SSRG International Journal of Electronics and Communication Engineering
ISSN: 2348-8549/ https://doi.org/10.14445/23488549/IJECE-V12I5P127

Volume 12 Issue 5, 310-326, May 2025

Original Article

VFHE-DWOA: A Cloud-Based Secure Medical Data Storage and Transmission Model

T. Anandhi[1], A. SivaSangari[2]

[1,2]*Department of Computer Science and Engineering, Sathyabama Institute of Science and Technology (Deemed to be University), Chennai, Tamil Nadu. India.*

[1]*Corresponding Author : anandhitamilvanan2908@gmail.com*

Received: 18 March 2025 Revised: 20 April 2025 Accepted: 21 May 2025 Published: 27 May 2025

Abstract *- As the need for Cloud Computing (CC) increases, security becomes more crucial for people as well as organizations, particularly in the medical sector. The secure storage and distribution of healthcare data have emerged as a significant concern due to their escalating use in the treatment and diagnosis of multiple diseases. Medical images include patients' personal data, and any unauthorized access to or alteration of these images might result in significant consequences. This research proposes a cloud-based security model using the Verifiable Fully Homomorphic Encryption (VFHE) with the Differential Whale Optimization Algorithm (DWOA) technique for secure medical image storage and transmission. The VFHE technique is applied to encrypt the medical images before storing them in the cloud. The DWOA algorithm is utilized to optimize the key generation process for improved efficiency and security. The encrypted images are uploaded to the cloud database, where the cloud storage enables remote access for legal users with security. The legal users are allowed to have access to the cloud storage through an internet portal. When a legal user requests access, the encrypted images are retrieved from the cloud. Using the VFHE-DWOA method, the encrypted image is decrypted back to its original form for further use. The results show that the VFHE-DWOA model achieves efficient encryption, decryption, and key generation time. The image quality assessment highlights superior performance, with the model achieving the lowest Mean Squared Error (MSE) of 0.214, the highest Peak Signal-to-Noise Ratio (PSNR) of 64.35 dB, and Structural Similarity Index Measure (SSIM) of 99.91% and Correlation Coefficient (CC) of 99.93%, ensuring minimal distortion and high image fidelity post-decryption. The VFHE-DWOA model outperformed the current models and demonstrated itself as a secure cloud-based medical image storage and transmission model.*

Keywords *- Cloud computing, Cloud security, DWOA, Homomorphic encryption, Medical image, VFHE.*

1. Introduction

CC is an emerging technology that will significantly influence daily activities. This technology enables access to computational resources and facilities at any time and from any location. The field of healthcare is perpetually transforming, and the upcoming healthcare model is expected to be information-centric. The industry could utilize cloud technology to deal with change and complexities [1]. The cloud facilitates the management, storage, sharing, protection, and Electronic Health Records (EHRs) archiving, pharmacy information systems, laboratory data systems, and medical images. Individuals would receive enhanced care due to current health records and ongoing communication among various healthcare providers. In addition to the lack of regulations, standards, and interoperability challenges, the primary barriers impeding the extensive adoption of cloud technology by medical organizations are security, confidentiality, and trust concerns [2]. CC possesses five primary characteristics: shared resources, wide network accessibility, elasticity, on-demand self-service, and measured service.

- Shared resources: clients can concurrently utilize resources such as networks, servers, storage, software, memory, and processing power. Providers can assign resources dynamically based on demand changes, while the consumer remains oblivious to the locations of their services.
- Wide network accessibility: the cloud facilitates widespread access to the network via the Internet from any device.
- Elasticity: the cloud exhibits flexibility and configurability. Clients perceive resources as limitless.
- On-demand self-services: Users could autonomously set up the cloud as required, without the involvement of service assistance. Users execute scheduling and determine the necessary storage and computational resources.
- Measured services: many cloud services could be evaluated utilizing distinct parameters. Comprehensive use records are produced to protect the interests of clients and providers [3].

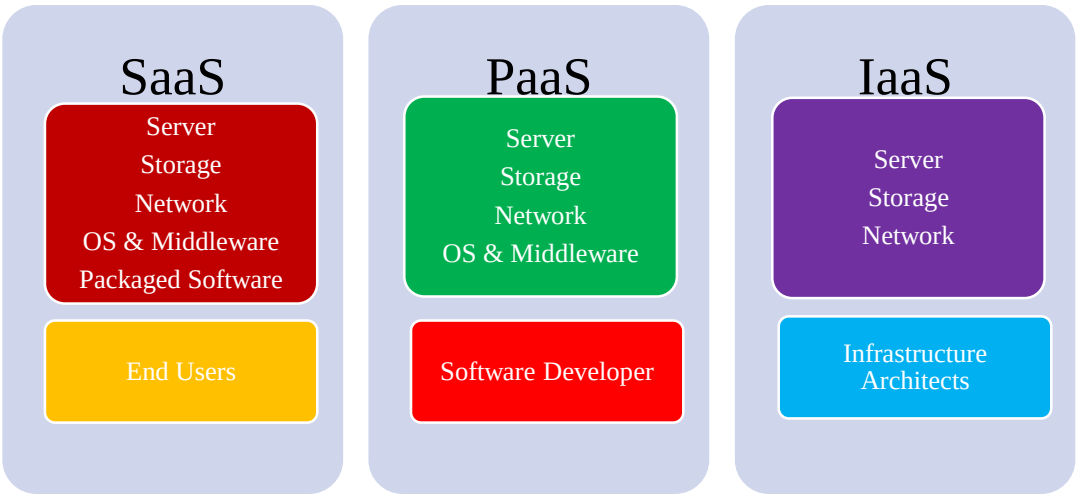

Fig. 1 Cloud service models

As shown in Figure 1, the CC has three key service models: Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). Recently, alongside the key service models, new Cloud service models have emerged, including Identity as a Service (IDaaS), Data as a Service (DaaS), Business Process as a Service (BPaaS), and Connectivity as a Service (CaaS).

- SaaS: This is the predominant cloud service, with the software hosted on the platform of providers. The user might utilize the software via the internet browsers or through the Application Programming Interfaces (API). It operates on a pay-per-use system of operation. Users need not concern themselves with updates and support; a limited capacity for application configuration may be accessible to them.
- PaaS: It offers platforms for development and testing. The consumer creates their own application on a server that is virtual and possesses access to the application hosting environment, especially regarding the application and data, thereby accelerating the development, testing, and deployment processes.
- IaaS: It offers the infrastructure, operating systems, and applications. This service is preferred by organizations lacking the resources for new hardware. Customers are charged based on usage [4].

The CC infrastructure uses four primary deployment types, which are:

- PUBLIC CLOUD: This model is characterized by a cloud infrastructure that is available to the public and managed by an organization or third-party cloud service provider.
- PRIVATE CLOUD: Private entities are accountable for the management and operation of this sort of cloud. The primary aim of the cloud business model is to uphold a consistent standard of security and privacy.
- COMMUNITY CLOUD: This architectural model facilitates the shared infrastructure among organizations or communities with identical purposes and visions, including security and control. Businesses and external entities can manage these services.
- HYBRID CLOUD: This deployment paradigm integrates two or more cloud architectures; they are interconnected while remaining distinct entities [5].

CC and cloud storage have significantly transformed data processing and utilization. The accessibility and availability of resources, in addition to a significant reduction in workforce, are a primary catalyst for the cloud transformation. The CC revolution has significantly increased the demand for outsourced applications. The client utilizes the service by transferring their information to the cloud and then receiving the processed results. It significantly advantages users; nevertheless, it also compromises important information to third-party companies that provide services [6]. In the healthcare sector, medical data of patients is digital files detailing an individual's medical history maintained by healthcare providers or hospitals. Patient medical files are maintained in data centers for processing and storage purposes. Before executing computations on data, conventional encryption methods decode the data to its original state. Consequently, confidential medical data is leaked [7].

Effective data security and protection are critical concerns in contrast to conventional on-premise computing. Numerous techniques exist for protecting data in the cloud, with encryption being the most effective method. Cryptography provides several security attributes, like authentication, confidentiality, integrity, and availability [8]. Data security is crucial for protecting the diverse services and benefits offered by CC. Utilizing encryption algorithms ensures data secrecy over networks. Cryptography is a reliable measure to guarantee secure communication. The predominant approach for mitigating the security gaps is the encryption of centrally stored data. An ever-changing cloud environment constitutes a substantial challenge to outsourcing calculations [9].

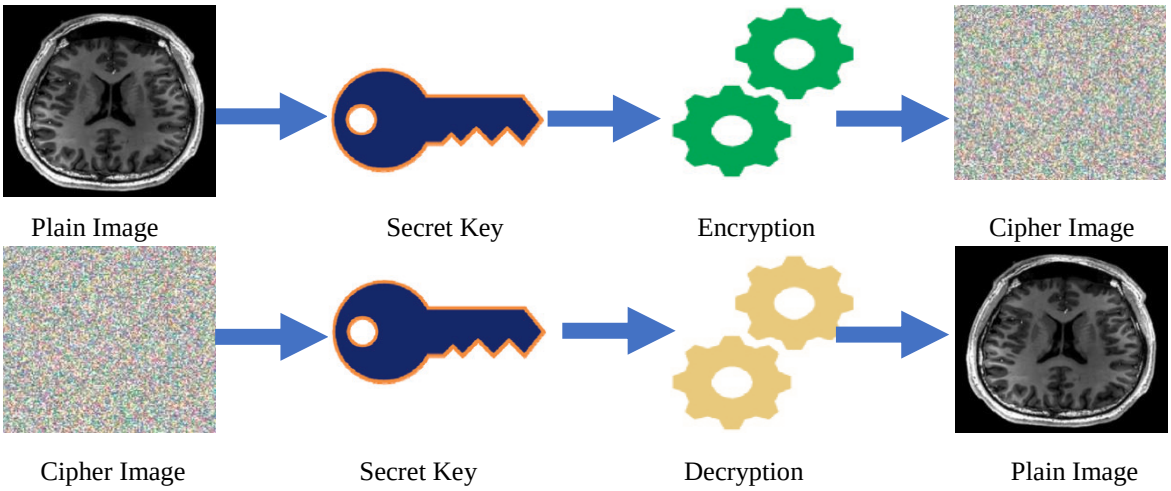

Fig. 2 Fundamental process of image encryption and decryption

As shown in Figure 2, the fundamental terms employed in encryption include:

- Plain Images: The original image that needs protection during distribution over the public networks. It is additionally called the source or input images.
- Cipher Images: An image that has been transformed into an unreadable format after undergoing encryption.
- Encryption: The procedure of transforming the plaintext images into the encrypted images using a specific encryption algorithm and secret keys.
- Decryption: The process at the receiver's end where the encrypted images are restored to their original plaintext form using a decryption algorithm and the corresponding secret key.
- Key: A crucial component of encryption security, which can be either numeric or alphanumeric. The key is essential for performing both encryption and decryption operations. Robust keys are essential for enhancing information security [10].

Encryption methods can generally be classified into two primary categories: asymmetric and symmetric procedures. To secure an image with symmetric encryption, it is crucial to preserve a single key. In contrast, the application of asymmetric approaches requires the maintenance of two separate keys. The measure of protection against unauthorized access, utilization, and manipulation of cloud resources is termed security in CC [11].

1.1. Problem Statement

Security risk pertains to many forms of attacks, threats, vulnerabilities, and additional concerns. Consequently, it is crucial to exercise caution while choosing or constructing a system for a business or client. Consequently, the cloud provider employs distinct security standards, methodologies, and frameworks to fulfill the client's specifications. Diverse strategies are utilized to counteract these attacks in the cloud, encompassing encryption, zero-trust architecture, intrusion detection systems, and antivirus software, among others [12]. The protection of individuals' data should be the primary determination. The data has to be protected by comprehensive security, encryption, authentication of users, and application protection by implementing present security standards and validating techniques. Security concerns, such as the manipulating of patient data from the cloud, breaches of data privacy, and unauthorized usage of data, pose significant challenges to cloud-based healthcare systems [13]. Hence, a novel approach to secure medical image transmissions in CC systems is proposed.

1.2. Research Objectives

The novelty of the developed VFHE-DWOA model for cloud-based medical image security is based on its integration of two different techniques. The research model integrates VFHE with DWOA for secure and effective medical image transmission. Compared to other encryption models, the implemented VFHE allows computations directly on encrypted images while ensuring verifiability. The implementation of DWOA improves the key generation and minimizes computational complexity. The primary objectives of this research are defined as follows:

- To develop a novel cloud-based medical image security model using the VFHE and the DWOA technique.
- To implement the VFHE technique to provide end-to-end privacy and security for medical images stored in the cloud.
- To integrate the DWOA technique to optimize and improve the VFHE's key generation for securing the cryptographic key selection.
- To assess the VFHE-DWOA model's efficiency using evaluation metrics like encryption time, decryption time, MSE, PSNR, and SSIM.
- To validate the efficiency of the developed model with the current models discussed in the related works based on performance comparison.

The paper is organized into the subsequent sections. Section II succinctly examines the current models relevant to the research study. Section III encompasses the implementation of the developed research methodology. Section IV highlights the experimental results of the research model and a comparison with current models. Section V concludes the research with an overview of the findings and recommendations for subsequent research initiatives.

2. Related Works

In this section, a review of current works applied to improving the cloud-based medical image security has been analyzed. All the reviewed current models are critically analyzed and presented in Table 1 with their advantages and limitations. The review of the related works is as follows: A rapid and safe encryption technique for medical images utilizing the 1D logistic map in conjunction with pseudo-random numbers was proposed in [14]. The technique integrated the two fundamental qualities, namely diffusion and confusion, which were requisite for any encryption scheme. Rows and columns derived from images and pseudo-random numbers were incorporated to mitigate chosen and differential-image attacks. The technique was rapid and efficient regarding computational time. The technique was resilient to noise and cropping attacks.

An approach designed to improve security protocols in the cloud was proposed in [15]. The approach was based on a lightweight homomorphic cryptography approach featuring dual layers of encryptions. The initial layer employed a lightweight cryptographic method, while the subsequent layer implemented multiplicative homomorphic algorithms to enhance data security in CC. The approach provided features of both asymmetric and symmetric cryptography. The findings of the approach demonstrated a significant enhancement in security, as well as improvements in encryption execution time, throughput, and memory utilization.

A secure system for authentication and encryption utilizing Improved Elliptic Curve Cryptography (IECC) was developed in [16] for IoT-based healthcare data. To transmit the data securely, the system employed the Substitution-Caesar cipher and IECC. The authentication framework utilizes the SHA-512 algorithm to integrate biometric parameters alongside the user's details. To augment the ECC's security, a secret key was provided to fortify the model's protection. Consequently, the complexity of the two phases was enhanced. The results demonstrated minimal encryption and decryption durations, as well as reduced communication overhead.

A medical image cipher technique utilizing a cascade quantum walk in combination with the Chebyshev map was proposed in [17]. To achieve an improved sensitivity of the plaintext image for the cipher mechanism, the SHA256 hashing method was applied to the plaintext medical image, and the resultant hash value was employed to modify the initial settings. Utilizing these revised parameters, the quantum walks were implemented to generate a distribution of probability vectors, which was subsequently employed alongside the modified initial scenario for iterating the Chebyshev map and yielded a chaotic sequence dependent on quantum walks and the original images. The results demonstrated higher levels of efficiency and security.

CloudSec, a compact and agile image encryption technique that integrates the hashing functions, a multi-wing chaotic map approach, and a genetic algorithm, was developed in [18]. A secret key with certain attributes served as the seeding values to produce the key DNA images from the hyper-chaotic approach, thereby eliminating the correlations within adjacent pixels through the chaotic sequences. The intricate dynamic behaviours of the chaotic maps produced a stochastic sequence for imaging diffusions. The transmission of data in the permuted DNA images and the key DNA images was accomplished using DNA operations.

The findings demonstrated that the technique effectively authenticated and secured images within healthcare data systems. The research in [19] examined the security of medical images in the IoT with a cryptography approach and optimization techniques. A framework for the efficient storages and secure transmission of individual's information and medical images for the management and optimization of keys were implemented using the Obstruction Bloom Breeding Optimization (OBBO), Hostile Orchestration (HO), and Rivest–Shamir–Adleman (RSA)-based Arnold Map (AM) to enhance the security of the decryption and encryption operations. The framework was clearly inadequate in security since it has never yielded significant results.

The encryption methods Data Encryption Standard (DES), Triple-DES (3DES), Advanced Encryption Standard (AES), Blowfish, Rivest Cipher-4 (RC4), and Rivest–Shamir–Adleman (RSA) were analyzed in [20] with their performance and security of imaging information in the CC. This analysis demonstrated that in cloud-based image cryptography, the approaches AES, Blowfish, RC4, and triple DES exhibited better performance. Although RC4 excelled in execution speed, it provided minimal security for images. Nonetheless, the approaches Blowfish, RSA, and AES generated the most secure ciphers for images in the CC.

A Fractional Ordered Lorenz Scheme and the Matrix Scramble Methodology (FOLS-MSM) was proposed in [21] to optimize medical image encryptions, ensuring enhanced correlations, high resolutions, and reliability. The Arnold map was employed to scramble the initial values. The tent maps were employed to ascertain the state value necessary for identifying the location of the pixels of plaintexts. The FOLS utilized the molded pixels as inputs, employing a matrix

approach to achieve scrambling and enhance confusion. Furthermore, it produced the pseudo-random sequences necessary for executing the cross-diffusions procedure to acquire the encrypted images. The findings validated that the data entropy of the enhanced FOLS-MSM was improved.

The model integrated 2D-Discrete Wavelet Transform-1 Level (2D-DWT-1L) or 2D-DWT-2L steganography with the hybrid encryption technique was proposed in [22]. The hybrid encryption model was constructed by methodically employing the AES and RSA algorithms to protect diagnostic data, which was integrated with the red, green, and blue channels of a cover image. The implementation of an Adaptive Genetics Algorithm for Optimal Pixels Adjustments Process (AGA-OPAP), which enhanced data hiding capabilities and imperceptibility attributes. The findings indicated that the model securely transferred medical data.

An image encryption method for healthcare IoT networks utilizing compressed sensing and the modified 7D hyper chaotic maps was developed in [23]. The 7D hyperchaotic map was initially adjusted to provide more protection and an intricate secret key. The SHA-512 was employed to establish the starting parameters for the model, hence guaranteeing its responsiveness to incoming images. Improvements in compressive sensing were attained through the application of the Non-Subsampled Contourlet Transform (NSCT), followed by the generation of measurement matrices utilizing secret keys derived from the model. To produce the encrypted image, diffusions and permutations were executed both row-wise and column-wise on images utilizing a secret key derived via the model. The results demonstrated that the model attained superior performance.

A pigeon-based Optimizer with Encryptions-based Secured Medicinal Images Management (PIOE-SMIM) approach was developed in [24]. The methodology primarily focused on developing the process of Secret Share Creation (SSC) and the encryption procedure. The images were transformed into a set of 12 shares utilizing the SSC method. An ECC method was utilized for the encryption procedure. For optimizing the key generation processes in the ECC models, the PIO technique was employed for maximizing PSNR. On the recipient's end, the decryption and sharing reconstruction process was executed to recreate the real image. The findings indicated that the model has achieved improved security in the transmission of medical images.

The research in [25] presented a quantum chaos-based encryption system, termed QMedShield, for medical imaging. The model employed bit-plane scrambling, a three-dimensional quantum logistic map, quantum operations during the diffusion phase, a hybrid chaotic map, and DNA encoding in the confusion phase to convert the plain medical image into a ciphered medical image. The findings exhibited the model's resilience to various challenges, guaranteeing safe storage of healthcare images in the cloud.

An effective cryptosystem for securing medical images by leveraging the benefits of deoxyribonucleic acid (DNA) principles and chaotic mappings was proposed in [26]. The cryptosystem utilized the logistic chaos maps, Piece Wise Linear Chaotic Maps (PWLCM), and DNA encoding. PWLCM was applied to produce the secret key images. The rules of DNA were applied for encoding the secret key images and the input plain images by rows, utilizing the logistic chaos maps for encoding. The logistic maps were utilized to produce the intermediate images, serving as additional secret key images to systematically apply DNA functions to the encoded original image, followed by the decoding of the intermediate image. The preceding processes were reiterated through the image columns to acquire the optimal ciphered image. The findings indicate that the cryptosystem exhibited robust security alongside a better processing duration.

An encryption model that applied a chaotic map, DNA encoding, and bit planes scrambling was developed in [27]. The encryption scheme integrated bit planes scrambling with the chaotic map for safe healthcare image storage in the CC. The model employed a 4D hyperchaotic map for the purpose of confusion, and Henon maps and Tent maps were employed for diffusion processes. Experiments demonstrated that the model was resilient to various threats. A secure medical imaging system based on blockchain that ensured anonymity was developed in [28]. The system was an intelligent integration of fog nodes, edge layer nodes, cloud service providers, and blockchain technology. Lightweight cryptographic methods were proposed utilizing ECC alongside the Elliptic Curve Diffie-Hellman (ECDH) and Elliptic Curve Digital Signature (ECDS) algorithms to ensure the security of biomedical image processing while preserving privacy. The results illustrated the system's robustness and security.

2.1. Research Gap Analysis

Based on the analysis of current models for cloud-based medical image security, it is evident that current models commonly struggle in obtaining the optimal balance between encryption/decryption and computational efficiency. Conventional models like AES, DES, and RSA were robust, but these models lack effective key management and verification. This limitation makes them less suitable for sensitive and resource-based applications like medical data sharing. However, the homomorphic encryption allows computations on encrypted images, but it is computationally intensive and underperforms in verification. Hence, to bridge these gaps from current models, this research aims to develop a hybrid model called VFHE-DWOA for optimizing key generation, improving security, and computational efficiency in cloud-based medical image security.

Table 1. Critical analysis of analyzed related works

Ref.	Models	Application	Advantages	Disadvantages
[14]	1D Logistic Map with Pseudo-Random Numbers	Medical Image Encryption	High efficiency, resilient to noise & cropping attacks.	Vulnerable to key prediction if not properly randomized.
[15]	Lightweight Homomorphic Cryptographic Technique	Cloud Security	Enhances security, improves encryption execution time, and memory utilization.	Complexity increases with multiple encryption layers.
[16]	IECC + Substitution-Caesar Cipher	IoT-based Medical Data Encryption	Strong authentication, reduced communication overhead.	Increased computational complexity due to the added secret key.
[17]	Cascade Quantum Walk + Chebyshev Map	Medical Image Cipher	High sensitivity, robust against attacks.	Quantum implementation complexity.
[18]	CloudSec	Healthcare Image Security	Eliminates pixel correlation, stochastic sequences for diffusion.	Complexity in key management.
[19]	RSA-based AM + Optimization (HO, OBBO)	IoT Medical Image Security	Attempts key management optimization.	Inadequate security performance.
[20]	Comparative Study	Cloud-based Image Cryptography	AES, Blowfish, and RSA provided high security.	RC4 exhibited fast execution but weak security.
[21]	FOLS + Matrix Scrambling	Medical Image Encryption	Improved data entropy, high correlation, and reliability.	Increased computational overhead.
[22]	Hybrid Encryption (AES + RSA) + 2D-DWT Steganography	Medical Data Protection	Secure transfer, enhanced data hiding.	Increased processing time.
[23]	Modified 7D Hyperchaotic Map + Compressive Sensing	Medical IoT Image Encryption	High security, improved key complexity.	Computationally expensive.
[24]	PIO + ECC Encryption	Management of Secure Medical Images	Improved PSNR, optimized key generation.	Increased encryption time.
[25]	QMedShield	Medical Image Security in the Cloud	Strong resilience to threats.	Complexity in implementation.
[26]	DNA Encoding + Chaotic Mapping	Medical Image Cryptosystem	Robust security, better processing duration.	Vulnerable to chosen-plaintext attacks if not properly implemented.
[27]	DNA Encoding + Chaotic Maps + Bit Plane Scrambling	Medical Image Storage in the Cloud	High confusion and diffusion.	Key sensitivity may impact performance.
[28]	ECC, ECDH, and ECDS	Privacy-Preserving Medical Image Security	Robust security, anonymity are ensured.	Increased computational overhead due to blockchain.

3. Materials and Methods

This research proposed a cloud-based medical image security model using the VFHE with the DWOA technique for secure medical image storage and transmission. The developed research model's pipeline was depicted in Figure 3. As shown in the figure, initially, the medical images are collected from the hospital. The medical images are sensitive patient medical records, which must be stored and processed securely. For this task, the VFHE technique is applied to encrypt the medical images before storing them in the cloud. The DWOA algorithm is additionally utilized to optimize the key generation process for improved efficiency and security. The ciphered (encrypted) images were uploaded to the cloud database, where the cloud storage enables remote access for legal users with security. The legal users, such as doctors, patients, lab experts, and researchers, are allowed to have access to the cloud storage through an internet portal. The portal provides a secure platform for doctors and medical staff to retrieve and analyze the medical images without exposing them. When a legal user requests access, the encrypted images are retrieved from the cloud. Using the VFHE-DWOA method, the encrypted image is decrypted back to its original form for further use. The security of the image is maintained throughout the process and prevents from illegal access.

3.1. Data Collection

For validating the proposed research model, a Multi-Cancer Dataset from the Kaggle repository is collected. This data collection comprises images of many cancer kinds, collated for academic and research objectives. It encompasses eight cancer types: Acute Lymphoblastic Leukemia, Brain Cancer, Breast Cancer, Cervical Cancer, Kidney Cancer, Lung Cancer, Colon Cancer, Lymphoma, and Oral Cancer. This dataset comprises a total of 130,000 images, including 20,000 images depicting benign and various stages of leukemia, 15,000 images representing three primary types of brain cancer, 10,000 images illustrating benign and malignant breast cancer types, 25,000 images encompassing various cervical cell types, 10,000 images of normal and tumorous kidney tissues, 25,000 images covering different tissue types in the lung and colon, 15,000 images across three subclasses of lymphoma, and 10,000 images of normal and cancerous oral tissues. Figure 4 depicts the sample images from the dataset [29].

3.2. Preprocessing and Normalization

The preprocessing process is necessary for this research to enhance the image security prior to encryption, which ensures effective storage and transmission in the cloud. In this preprocessing stage, enhancement and normalization processes are performed. Contrast enhancement is performed using the Contrast-Limited Adaptive Histogram Equalization (CLAHE) technique to enhance contrast for better analysis after decryption.

For normalization, the Min-Max technique is used. The normalization is performed to ensure that all the medical images have a uniform size, format, and intensity range to avoid inconsistencies in encryption and storage.

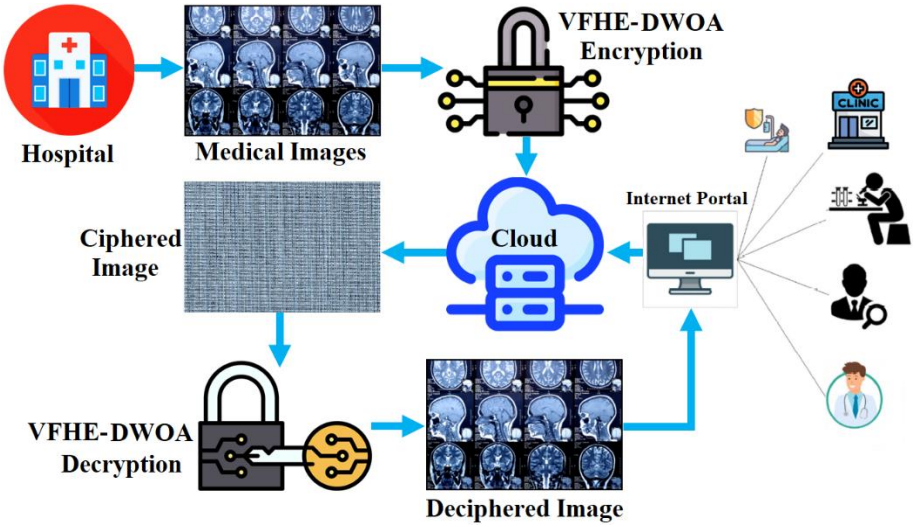

Fig. 3 Proposed cloud-based medical image security model

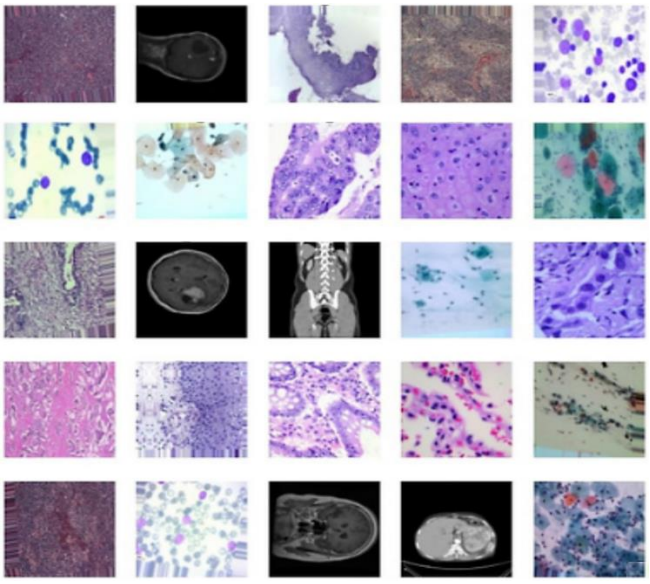

Fig. 4 Sample images from the dataset

CLAHE operates on localized regions of the image known as tiles, instead of the entire image. The disparity between every tile was enhanced to align the histograms of the output area with the histograms of each match. The adjacent tiles are subsequently merged using bilinear interpolation, which resamples data and inserts information into each pixel. Bilinear interpolation is a method used to calculate values of a matrix region based on nearby cells in the grid. The main distinction is that it employs the four nearest cell centers. Additionally, it employs the use of the 16 closest neighbouring pixels to effectively refine the surface of all pixels and eliminate erroneously established boundaries. The cumulative distribution of the histogram, denoted as represented as follows:

$$H'(i) = \sum_{0<j<i} H(j) \tag{1}$$

To utilize the equation provided as a remapping function, it is necessary to normalize the $H'(i)$ in a manner that the maximum value is equivalent to 255, or comparable to the highest intensity values found in images.

Image normalization is employed to enhance the rate at which the model converges, its accuracy, and stability by altering the distribution and range of pixel values in the image. The min-max normalization approach applies Equation (2) to process the intensity of all the pixels.

$$X_{norm} = \frac{X_i - \min(X)}{\max(X) - \min(X)} \tag{2}$$

In the given equation, X_i denotes the image's pixel intensity values, $\max(X)$ and $\min(X)$ denotes the maximum and minimum values of the image's pixel intensity values. X_{norm} denotes the normalized intensity of a pixel. Min-max normalization, represented by Equation (3), is a process where the minimum value of image intensity is set to 0 and the maximum value is set to 255.

$$X_{norm} = \frac{X_i}{255} \tag{3}$$

The initial pixel image's pixel intensity values ranged from 0 to 255. Min-max normalization is used to scale the image's intensity range, resulting in a smooth intensity distribution and a wider range of intensities [30].

As the proposed VFHE works on pixel-based data, this preprocessing phase will improve the images for better storage, security, and retrieval. This process ensures that the decrypted image retains high fidelity for accurate diagnosis while minimizing the complexity of encryption.

3.3. Differential Whale Optimization Algorithm

Many optimization problems can be solved with the assistance of an optimization algorithm. The objective of an optimization algorithm is to find the best possible solution by maximizing efficiency and success. This can be accomplished by either reducing or increasing the amount of complexity that is involved in overcoming the challenges. Meta-heuristics for decision-making have garnered a lot of research and interest recently, which is not surprising considering the increased complexity of models and the increased pressure to make decisions quickly in the healthcare industry. The image processing tasks have incorporated optimization since the advent of computers. One such optimization technique is the DWOA, which involves iteratively comparing different solutions until the most suitable solution is identified. This algorithm is specifically utilized to achieve an appropriate solution through the optimization process. After the best search agent has been determined, the next phase may involve the other search agents attempting to improve their rankings and become almost as good as the best search agent.

$$\vec{S} = \left|\vec{Y} \cdot \vec{B} * (u) - \vec{B}(u)\right| \tag{4}$$

$$\vec{B}(u+1) = \vec{B}(u) - \vec{K}\vec{S} \tag{5}$$

In the Equations (4) and (5), u denotes the current iteration, $\vec{K}$ and $\vec{Y}$ describe the coefficient vectors, B^* explains the best solution of the position vector that has previously been produced, $\vec{B}$ represents the absolute value of the position vector, and '$\cdot$' symbolizes the multiplication of one element by another.

$$\vec{K} = 2\vec{k} \cdot \vec{n} - \vec{r} \tag{6}$$

$$\vec{Y} = 2 \cdot \vec{n} \tag{7}$$

Here ($\vec{r}$) was a random vector with values in the range [0,1], and it declined linearly from 2 to 0 $\vec{k}$ iterations.

$$\vec{B}(u+1) = \overrightarrow{s'} \cdot i^{xv} \cdot COS(2\pi v) + \vec{B} * (u) \tag{8}$$

Here, the distant among the whale e and its prey is described by the equation $\vec{S'} = |\vec{B} * (u) - \vec{B}(u)|$, where x represents a constant for a logarithmic spiral shape and v represents a random number in the range [-1,1].

$$\vec{B}(u+1) = \begin{cases} \vec{B} * (u) - \vec{K} \cdot \overrightarrow{S} & if\ q \le 0.5 \\ \overrightarrow{S'} \cdot i^{xv} \cdot cos(2\pi v) + \vec{B} * (u) & if\ q \ge 0.5 \end{cases} \tag{9}$$

q represents a random number between 0 and 1.

$$\vec{S} = |\vec{Y} \cdot \vec{B}_{rand} - \overrightarrow{B}| \tag{10}$$

$$\vec{B}(u+1) = \vec{B}_{rand} - \vec{K}\vec{S} \tag{11}$$

A random whale position vector taken from the current

population is denoted by the variable $\vec{B}_{rand}$. After that, the data that was encrypted is decrypted whenever the user wants access to it [31]. In this research, the DWOA was applied for optimizing key generation in VFHE, improving computational efficiency and security.

3.4. Verifiable Fully Homomorphic Encryption

Homomorphic encryption has developed as a significant research domain in cryptography due to the increasing demand for data secrecy across various applications in everyday life. Homomorphic encryption aims to facilitate the calculation of encrypted data. This indicates that the data can stay confidential during processing, enabling critical operations to be executed utilizing data stored in untrusted locations. This is highly beneficial for heterogeneous networks and distributed computing. A homomorphic cryptosystem, comparable to conventional public encryption methods, utilizes a public key for encrypting data, guaranteeing that just an individual with the associated private key can access the decrypted data. It employs an algebraic approach to facilitate diverse calculations of encrypted data. Organizations can employ conventional encryption techniques to protect confidential information in cloud environments. However, if they want the analysis or validation of encrypted details stored in the cloud, they have to either decrypt the data or download and subsequently decrypt it [32].

Homomorphic encryption is classified into three categories. The fundamental distinction between them relies on the categories and frequencies of mathematical computations permissible on ciphertext.

- Partially Homomorphic Encryption (PHE): An encrypted data can undergo an infinite amount of addition or multiplication processes.
- Somewhat Homomorphic Encryption (SWHE): The quantity of multiplication and addition operations that can be executed is constrained.
- Fully Homomorphic Encryption (FHE) permits an encrypted message to perform an infinite number of multiplication and addition operations.

A verifiable encryption strategy is a cryptographic system that enables the demonstration of certain attributes of an encrypted value without revealing the value itself. When the verification option is integrated with homomorphic capabilities inside a single encryption scheme, it results in a VFHE. Thus, a VFHE scheme is an efficient method for outsourcing intricate calculations on sensitive data to a remote cloud server. It enables the client to validate the accuracy of their allocated computations. VFHE is defined by the combination of the concepts of FHE and verifiable computation. VFHE is built on two core cryptographic components: FHE, which allows computations on encrypted information, and Verifiable Computation (VC), which ensures correctness of encrypted computations.

For this research, let M be the space of medical image data, E_{VFHE} and D_{VFHE} let be the encryption and decryption functions of VFHE. p_k and s_k be the public and secret keys, optimized using the DWOA.

P be the proof ensuring the computation integrity, and F represents the function applied to encrypted data. Key Generation: The security of VFHE is based on the key generation, which is optimized using the DWOA method. The optimal key pair is given as defined in the following Equation (12).

$$(p_k, s_k) = DWOA(\max\{S(p_k, s_k)\}) \tag{12}$$

Here, the variable $S(p_k, s_k)$ is the security level based on the key size and complexity [33].

```
Key Generation
VFHE_Key_Generation()
  Input: Security Parameters λ
  Output: Public Key (pk), Secret Key (sk)
  Initialize Key Space K with random keys
  for each iteration in DWOA_Max_Iterations do
    Evaluate Security Strength S(pk, sk) for current keys
    Update keys based on DWOA optimization rules
  end for
  (pk, sk) ← Best optimized keys from DWOA
  Return (pk, sk)
End
```

Encryption of Medical Images: Each medical image $I \in M$ is encrypted using the public key p_k, which results in an encrypted cipher image.

$$C = E_{VFHE}(p_k, I) \tag{13}$$

In this Equation (13), C denotes the ciphered image.

```
Encryption
VFHE_Encryption(I, pk)
  Input: Medical Image I, Public Key pk
  Output: Encrypted Image C
  B ← ConvertToBinary(I)
  C ← Encrypt(pk, B)
  Return C  # Ciphered Image
End
```

Homomorphic Computation: The homomorphic computation is performed on the encrypted images. Given two encrypted images C_1, C_2 and a function F, VFHE allows secure computations without decryption as computed using the following Equation (14).

$$C_{out} = Eval(p_k, F, C_1, C_2) \tag{14}$$

The cloud server computes C_{out} without assessing the images. Proof generation for verifiable computation is performed to ensure the computation's integrity, where the verifiable proof P is generated using the following Equation (15).

$$P = ProofGen(p_k, F, C_1, C_2) \quad (15)$$

The proof is transmitted along with the processed medical image data.

```
Homomorphic Computation
Homomorphic_Computation(C1, C2, pk, Function F)
  Input: Encrypted Images C1, C2, Public Key pk, Function F
  Output: Processed Encrypted Output C_out
  C_out ← Eval(pk, F, C1, C2)
  P ← ProofGen(pk, F, C1, C2, C_out)
  Return (C_out, P)
End
```

Decryption and Verification: The legal users, i.e., Doctors or patients, decrypt the processed image using the secret key s_k as given in Equation (16).

$$I_{out} = D_{VFHE}(s_k, C_{out}) \quad (16)$$

To verify the accuracy, the proof is checked using the following Equation (17).

$$Valid = Verify(p_k, F, C_1, C_2, C_{out}, P) \quad (17)$$

If the computation $Valid = 1$, the computation is correct and secure [34].

```
Decryption and Verification
VFHE_Decryption(C_out, sk, P, pk, F, C1, C2)
  Input: Encrypted Output C_out, Secret Key sk, Proof P, Public Key pk, Function F, Input Images C1, C2
  Output: Deciphered Image I_out, Verification Status
  I_out ← Decrypt(sk, C_out)
  isValid ← Verify(pk, F, C1, C2, C_out, P)
  if isValid = True then
    Return I_out  # Successfully decrypted and verified
  else
    Return "Verification Failed: Computation Not Trusted"
  end if
End
```

The advantages of the VFHE-DWOA include computations occurring on encrypted images, preventing data leaks, proofs ensure the correctness of cloud-based medical image analysis, and finally, DWOA enhances key generation and reduces computational complexity.

4. Results and Discussion

4.1. Experimental Setup

The performance evaluation of the proposed research model is conducted through experimental computation in this section. The experiments for this research were conducted using Python 3.8+, TensorFlow 2.8+, and Keras APIs. Additionally, cryptographic libraries such as PySEAL, TenSEAL, and PyCryptodome were utilized for implementing the VFHE scheme, while NumPy, SciPy, and DEAP were employed for optimizing key generation using the DWOA.

The research model was executed on a Google Colab platform equipped with an NVIDIA GTX 1050 4GB GPU. The experimental setup is outfitted with 16 gigabytes of RAM, a 1 terabyte hard disk drive, and a 256-gigabyte solid-state drive.

This extensive analysis focuses on the effectiveness of the proposed research model, considering many metrics like Encryption time, Decryption time, MSE, SSIM, PSNR, and Correlation Coefficient.

4.2. Performance Metrics

For evaluating the results of the VFHE-DWOA model in the implemented cloud-based medical image security system, the following metrics are considered:

Encryption Time: This measures the time required to encrypt the medical image using the VFHE-DWOA model.

$$ENC = T_{end} - T_{start} \quad (18)$$

Here, the variables T_{start} and T_{end} denote the encryption process's start and end times, respectively. Lower values indicate faster encryption.

Decryption Time: This measures the time required to decode the encrypted image and revert it to its actual form.

$$DEC = T_{end} - T_{start} \quad (19)$$

Here, the variables T_{start} and T_{end} denote the decryption process's start and end times, respectively. Lower values signify efficient decryption [16].

Mean Squared Error: This measures the pixel-wise error between the actual images and the decoded images.

$$MSE = \frac{1}{MN}\sum_{i=0}^{M}\sum_{j=0}^{N}(I(i,j) - I'(i,j))^2 \quad (20)$$

Here, M and N are the image dimensions. A lower MSE indicates better reconstruction.

SSIM: This evaluates the perceptual similarity between the original and decrypted images.

$$SSIM(I, I') = \frac{(2\mu_I\mu_{I'}+C_1)(2\sigma_{II'}+C_2)}{(\mu_I^2+\mu_{I'}^2+C_1)(\sigma_I^2+\sigma_{I'}^2+C_2)} \quad (21)$$

Where μ and σ are the mean and variance of images I and I', and C_1 and C_2 are constants. SSIM ranges from 0 to 1, with values closer to 1 indicating better quality.

PSNR: This measures the quality of the decrypted image in terms of signal strength relative to noise.

$$PSNR = 10log_{10}\left(\frac{MAX_I^2}{MSE}\right) \quad (22)$$

Here MAX_I is the maximum possible pixel intensity. Higher PSNR indicates better image quality.

Correlation Coefficient (CC): This measures the correlation within the actual and decoded images.

$$CC = \frac{\sum(I(i,j)-\mu_I)\left(I'(i,j)-\mu_{I'}\right)}{\sqrt{\sum(I(i,j)-\mu_I)^2\sum(I'(i,j)-\mu_{I'})^1}} \quad (23)$$

Here μ_I and $\mu_{I'}$ are the means of the original and decrypted images. CC values closer to 1 indicate higher similarity [27].

4.3. Performance Evaluation

This section presents the results of the proposed VFHE-DWOA model evaluated using the encryption time (ms), decryption time (ms), key generation time (ms), MSE, PSNR (dB), SSIM, and CC. Figure 5 depicts the results of the encrypted images using the research model.

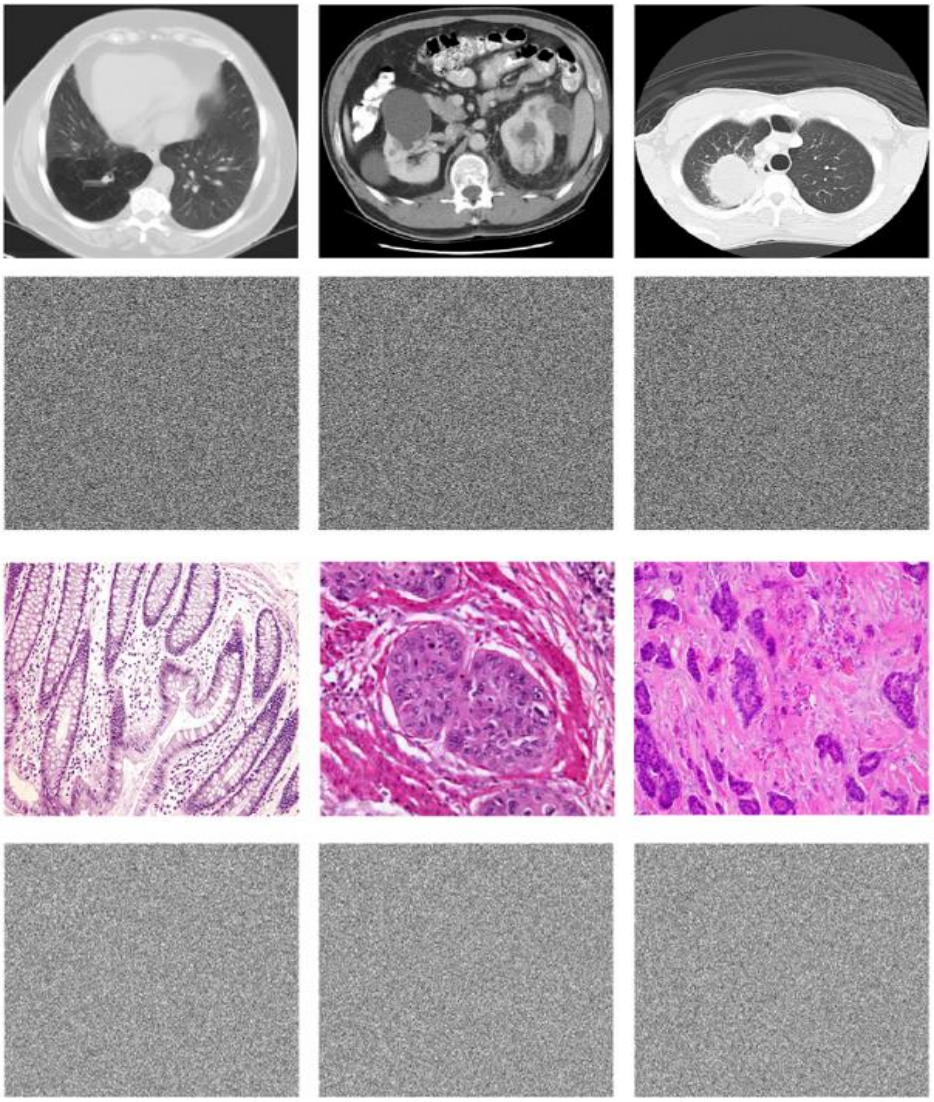

Fig. 5 Results of encrypted images

Table 2 presents the processing time results of the proposed VFHE-DWOA for six different images, evaluating encryption, decryption, and key generation times in Milliseconds (ms). The encryption time varies slightly across the images, ranging from 8.05 ms to 8.40 ms, indicating an efficient and stable encryption process with minimal fluctuations. The decryption time is consistently lower, ranging from 5.98 ms to 6.30 ms, demonstrating the model's ability to efficiently retrieve the original image with minimal computational overhead. The key generation time, which is crucial for secure encryption, remains within a narrow range of 5.72 ms to 6.01 ms, highlighting the optimization effectiveness of the DWOA in accelerating key computation. Figure 6 highlights the graphical chart of the VFHE-DWOA model's results in the encryption, decryption, and key generation time performance.

Table 2. Results of the VFHE-DWOA in processing time

Images	Encryption Time (ms)	Decryption Time (ms)	Key Generation Time (ms)
Image-1	8.23	6.12	5.87
Image-2	8.10	6.05	5.79
Image-3	8.35	6.20	5.92
Image-4	8.05	5.98	5.72
Image-5	8.40	6.30	6.01
Image-6	8.18	6.10	5.84

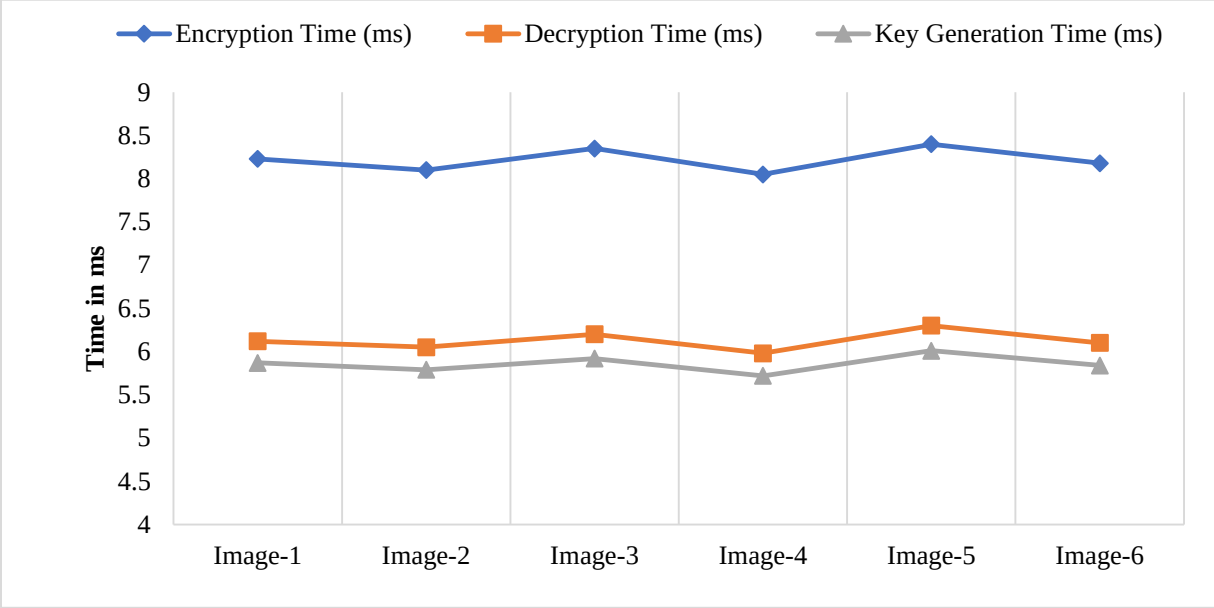

Fig. 6 Graphical illustration of VFHE-DWOA's processing time results

Table 3. Results of the VFHE-DWOA in image quality assessment

Image	MSE	PSNR	SSIM	CC
Image-1	0.0215	65.42	99.91	99.96
Image-2	0.0190	66.01	99.93	99.91
Image-3	0.0231	61.88	99.89	99.93
Image-4	0.0189	64.40	99.94	99.90
Image-5	0.0253	62.50	99.87	99.94
Image-6	0.0208	65.80	99.92	99.97

Table 3 presents the image quality assessment results of the proposed VFHE-DWOA across six images using four key evaluation metrics: MSE, PSNR, SSIM, and CC. The MSE values are extremely low, ranging from 0.0189 to 0.0253, indicating minimal distortion introduced by the encryption and decryption process. Correspondingly, the PSNR values remain high, between 61.88 dB and 66.01 dB, confirming that the reconstructed images retain high fidelity with negligible loss. The SSIM values, which measure structural similarity between the original and decrypted images, consistently exceed 99.87%, highlighting the model's ability to preserve important image features.

The CC values, which evaluate pixel-wise correlation between original and decrypted images, remain exceptionally high (99.90% to 99.97%), demonstrating a nearly perfect reconstruction. These results confirm that VFHE-DWOA maintains superior image quality with minimal encryption-induced degradation, making it highly suitable for secure medical image encryption and cloud storage applications. Figures 7, 8, and 9 depict the graphical chart of the MSE, PSNR, SSIM, and CC results.

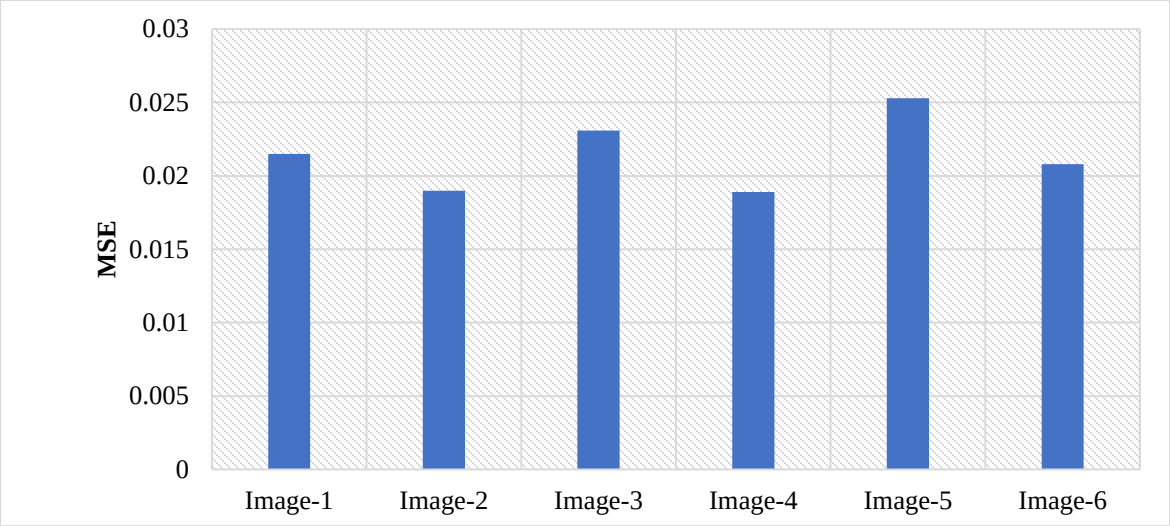

Fig. 7 Graphical illustration of VFHE-DWOA's MSE results

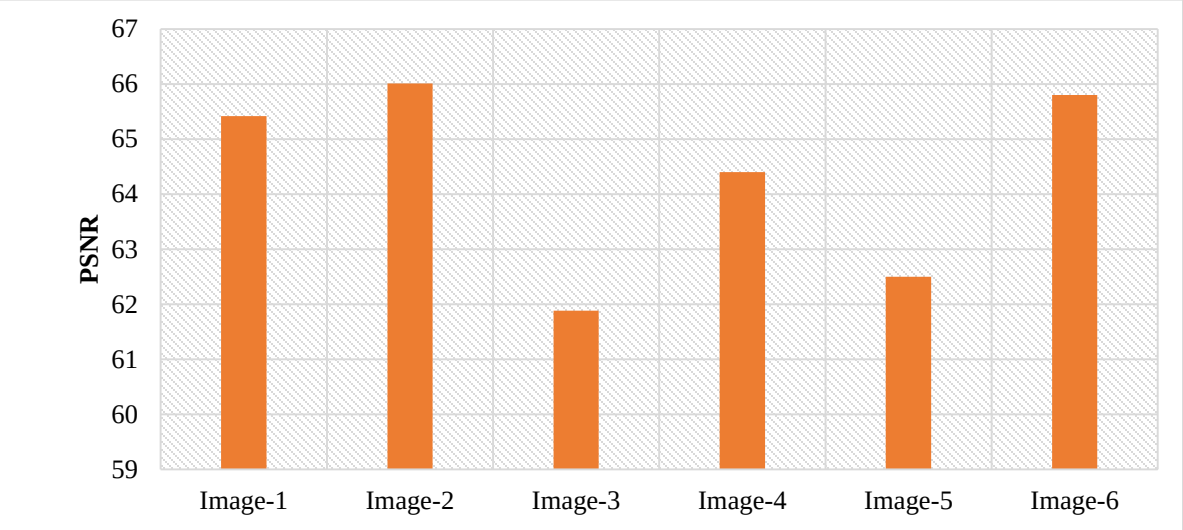

Fig. 8 Graphical illustration of VFHE-DWOA's PSNR results

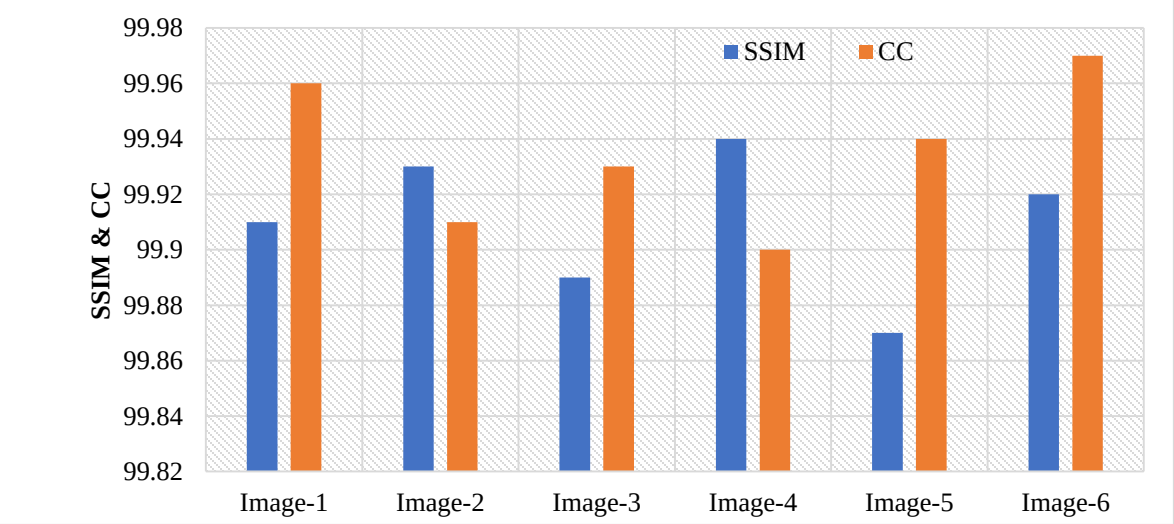

Fig. 9 Graphical illustration of VFHE-DWOA's SSIM and CC results

Table 4. Results comparison of VFHE-DWOA with current models

Models	MSE	PSNR	SSIM	CC
DES [20]	1.925	42.33	96.45	96.90
AES [20]	0.928	50.21	97.80	97.92
Blowfish [20]	0.825	51.40	98.32	98.40
RSA [20]	2.143	40.98	95.12	95.60
AES+RSA [22]	0.742	52.01	98.75	98.79
IECC + SCC [16]	0.610	53.45	98.98	99.01
Lightweight HE [15]	0.505	54.93	99.25	99.30
PIO + ECC [24]	0.342	58.45	99.60	99.65
Proposed VFHE-DWOA	0.214	64.35	99.91	99.93

Table 4 presents a comparative analysis of the proposed VFHE-DWOA against existing encryption models, evaluating their performance using MSE, PSNR, SSIM, and CC. The proposed VFHE-DWOA model outperforms all other encryption techniques, achieving the lowest MSE of 0.214, indicating minimal distortion. The PSNR of 64.35 dB is significantly higher than other models, demonstrating superior image quality preservation. Additionally, VFHE-DWOA achieves the highest SSIM (99.91%) and CC (99.93%), confirming that the decrypted images retain their structural integrity and pixel-wise correlation with the original images better than competing models. The VFHE-DWOA model highlights superior performance over current models with enhanced security, efficiency, and image quality assessments. Compared to other models, the proposed VFHE-DWOA model provides verifiable encrypted computations and simultaneously optimizes the key generation using the DWOA. This results in making the model secure, fast, and effective with improved results than other current models discussed and compared in this research.

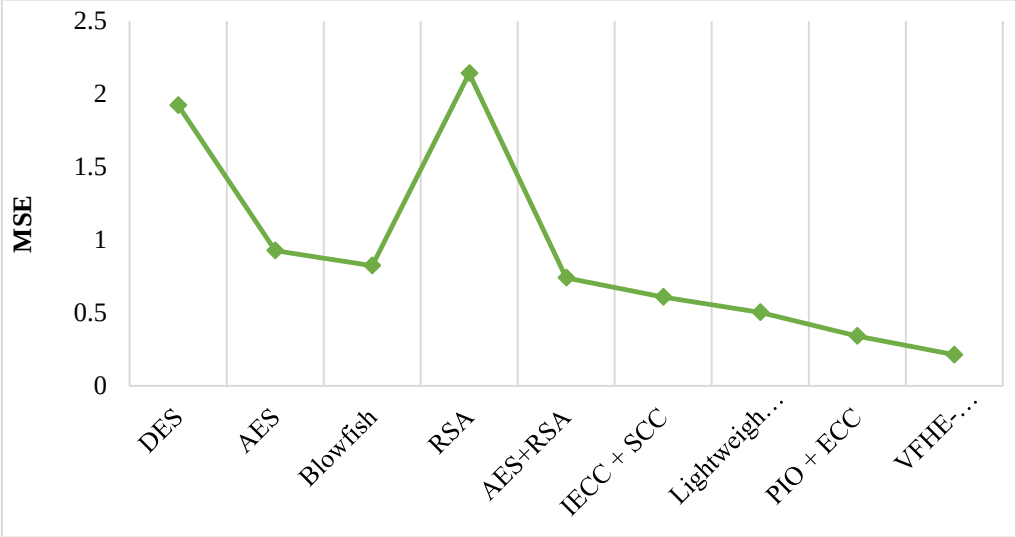

Fig. 10 Graphical illustration of MSE results comparison

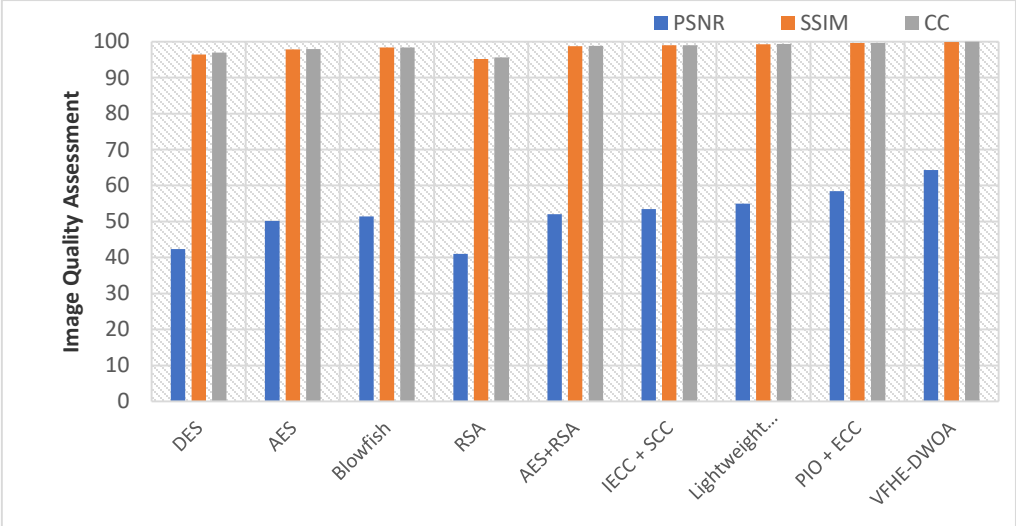

Fig. 11 Graphical illustration of PSNR, SSIM, and CC results comparison

In contrast, traditional encryption methods such as DES (MSE: 1.925, PSNR: 42.33 dB, SSIM: 96.45%) and RSA (MSE: 2.143, PSNR: 40.98 dB, SSIM: 95.12%) show lower performance due to higher image distortion. Hybrid models such as AES+RSA (MSE: 0.742, PSNR: 52.01 dB, SSIM: 98.75%) and PIO+ECC (MSE: 0.342, PSNR: 58.45 dB, SSIM: 99.60%) perform better than conventional methods but still fall short compared to VFHE-DWOA. These findings establish that VFHE-DWOA provides an optimal balance between security and image quality, making it highly effective for secure medical image encryption in cloud-based environments. Figures 10 and 11 depict the results comparison of the VFHE-DWOA model with the current models discussed in the related works section. The overall results of this research demonstrate the effectiveness of the VFHE-DWOA in ensuring secure and high-quality medical image encryption. The processing time analysis shows that VFHE-DWOA achieves efficient encryption, decryption, and key generation times, with encryption taking approximately 8.23 ms on average, decryption 6.12 ms, and key generation 5.87 ms, indicating its computational efficiency. The image quality assessment highlights superior performance, with the proposed model achieving the lowest MSE of 0.214, the highest PSNR of 64.35 dB, and SSIM of 99.91% and CC of 99.93%, ensuring minimal distortion and high image fidelity post-decryption. Comparative analysis with existing encryption models, including DES, AES, Blowfish, RSA, and hybrid techniques like AES+RSA and PIO+ECC, confirms that VFHE-DWOA outperforms all, providing the best balance between security, efficiency, and image quality preservation.

5. Conclusion

This research proposed a cloud-based secure model for medical images storage and transmission using the VFHE with DWOA. The VFHE technique was implemented for encrypting the medical images before storing them in the cloud. The DWOA algorithm was additionally utilized to optimize the key generation process for improved efficiency and security. The encrypted images were uploaded to the cloud database, where the cloud storage enabled remote access for legal users with security. The legal users were allowed to have access to the cloud storage through an internet portal. The portal provides a secure platform for users to retrieve and analyze the medical images without exposing them. When a legal user requests access, the encrypted images are retrieved from the cloud. Using the VFHE-DWOA method, the encrypted image was decrypted back to its original form for further use. The security of the image was maintained throughout the process and prevents from illegal access. VFHE-DWOA achieved efficient encryption, decryption, and key generation times, with encryption taking approximately 8.23 ms on average, decryption 6.12 ms, and key generation 5.87 ms, indicating its computational efficiency. Further, the model achieved the lowest MSE of 0.214, the highest PSNR of 64.35 dB, and SSIM of 99.91% and CC of 99.93%, ensuring minimal distortion and high image fidelity post-decryption. Future work will focus on enhancing the efficiency and robustness of VFHE-DWOA by integrating quantum-resistant encryption techniques to ensure security against quantum attacks. Further, real-time implementation on cloud platforms and testing with diverse medical imaging modalities will be conducted to validate its adaptability and scalability in practical healthcare applications.

Acknowledgments

The authors would like to thank the Department of Computer Science and Engineering, Sathyabama Institute of Science and Technology, for their support and motivation throughout this research.

References

[1] Hadeel Amjed Saeed et al., "Survey on Secured Scientific Workflows Scheduling in Cloud Environment," *Future Internet*, vol. 17, no. 2, pp. 1-29, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[2] Giuseppe Agapito, and Mario Cannataro, "An Overview on the Challenge and Limitation using Cloud Computing in Healthcare Corporation," *Big Data and Cognitive Computing*, vol. 7, no. 2, pp. 1-19, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[3] Remya Sivan, and Zuriati Ahmad Zukarnain, "Security and Privacy in Cloud-Based E-Health Systems," *Symmetry*, vol. 13, no. 5, pp. 1-14, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[4] Smita Sharma, and Sanjay Tyagi, "Security and Privacy Preservations of Electronics Health Record in Cloud," *International Journal of Fuzzy Logics and Intelligent System*, vol. 24, no. 4, pp. 428-439, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[5] K. Sasikumar, and S. Nagarajan, "Comprehensive Reviews and Analysis of Cryptography Technique in Cloud Computing," *IEEE Access*, vol. 12, pp. 52325-52351, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[6] Yazan Al-Issa, Mohammad Ashraf Ottom, and Ahmed Tamrawi, "eHealth Cloud Security Challenge: A Survey," *Journal of Healthcare Engineering*, vol. 2019, no. 1, pp. 1-15, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[7] Priyanka, and Amit Kumar Singh "A Survey of Image Encryptions for Healthcare Application," *Evolutionary Intelligences*, vol. 16, pp. 801-818, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[8] K. Munjal, and R. Bhatia, "A Systematic Review of Homomorphic Encryption and its Contributions in Healthcare Industry," *Complex & Intelligent System*, vol. 9, pp. 3759-3786, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[9] Mandeep Kaur, Surender Singh, and Manjit Kaur, "Computational Images Encryption Technique: A Comprehensive Review," *Mathematical Problem in Engineering*, vol. 2021, no. 1, pp. 1-17, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[10] Hamed Taherdoost, Tuan-Vinh Le, and Khadija Slimani, "Cryptographic Technique in Artificial Intelligences Security: A Bibliometric Review," *Cryptography*, vol. 9, no. 1, pp. 1-16, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[11] Yousef Alghamdi, and Arslan Munir, "Image Encryptions Algorithm: A Survey of Designs and Evaluation Metric," *Journal of Cybersecurity and Privacy*, vol. 4, no. 1, pp. 126-152, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[12] Fei Yan et al., "Insight into Security and Privacy Issue in Smart Healthcare System based on Medical Image," *Journal of Information Security and Application*, vol. 78, pp. 1-15, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[13] Saja Theab Ahmed et al., "Medical Images Encryptions: A Comprehensive Review," *Computers*, vol. 12, no. 8, pp. 1-45, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[14] Manish Kumar, and Prateek Gupta, "A New Medical Image Encryption Algorithm based on the 1D Logistic Map Associated with Pseudo-Random Numbers," *Multimedia Tool and Application*, vol. 80, pp. 18941-18967, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[15] Fursan Thabit et al., "A Novel Effective Lightweight Homomorphic Cryptographic Algorithms for Data Security in Cloud Computing," *International Journal of Intelligent Network*, vol. 3, pp. 16-30, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[16] Mohammad Ayoub Khan et al., "A Secure Framework for Authentication and Encryption Using Improved ECC for IoT-Based Medical Sensor Data," *IEEE Access*, vol. 8, pp. 52018-52027, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[17] Fahad Alblehai et al., "Cascading Quantum Walk with Chebyshev Maps for Designing a Robust Medical Images Encryption Algorithms," *Scientific Report*, vol. 15, pp. 1-24, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[18] A. Mondal and P. S. Chatterjee, "CloudSec: A Lightweight and Agile Approach to Secure Medical Images Transmissions in the Cloud Computing Environments," *SN Computer Science*, vol. 5, no. 237, pp. 1-23, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[19] Jeeva Selvaraj et al., "Cryptographic Encryptions and Optimizations for Internet of Things based Medical Images Security," *Electronics*, vol. 12, no. 7, pp. 1-19, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[20] B. Rahul, and K. Kuppusamy, "Efficiency Analysis of Cryptographic Algorithm for Image Data Security in Cloud Environments," *IETE Journal of Research*, vol. 69, no. 9, pp. 6053-6064, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[21] P. Suhasini, and S. Kanchana, "Enhanced Fractional Orders Lorenz Systems for Medical Images Encryptions in Cloud-Based Healthcare Administrations," *International Journal of Computer Network and Application*, vol. 9, no. 4, pp. 424-437, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[22] R. Denis, and P. Madubala, "Hybrid Data Encryption Model Integrating Multi-Objective Adaptive Genetic Algorithm for Secure Medical Data Communication Over Cloud-Based Healthcare Systems," *Multimedia Tool and Application*, vol. 80, pp. 21165-21202, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[23] M. Kaur et al., "Lightweights Biomedical Images Encryptions Approach," *IEEE Access*, vol. 11, pp. 74048-74057, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[24] B.T. Geetha et al., "Pigeon Inspired Optimization with Encryption Based Secure Medical Image Management System," *Computational Intelligences and Neurosciences*, vol. 2022, no. 1, pp. 1-13, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[25] Arun Amaithi Rajan, and Vetriselvi Vetrian, "QMedShield: A Novel Quantum Chaos-Based Images Encryptions Scheme for Secured Medical Images Storages in the Cloud," *Journal of Modern Optics*, vol. 71, no. 13-15, pp. 524-542, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[26] Walid El-Shafai et al., "Robust Medical Image Encryption based on DNA-Chaos Cryptosystem for Secure Telemedicine and Healthcare Applications," *Journal of Ambient Intelligences and Humanized Computing*, vol. 12, pp. 9007-9035, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[27] Arun Amaithi Rajan, Vetriselvi Vetrian, and Aruna Gladys, "Secure Image Encryptions Models for Cloud-Based Health Care Storages using Hyper Chaos and DNA Encoding," *International Conferences on Computational Intelligences in Data Sciences*, pp. 89-103, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[28] Hemant B. Mahajan, and Aparna A. Junnarkar, "Smart Health Care Systems using Integrated and Lightweights ECC with Private Blockchains for Multimedia Medical Data Processing," *Multimedia Tool and Application*, vol. 82, no. 28, pp. 44335-44358, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[29] Obuli Sai Naren, Multi Cancer Dataset, Kaggle, 2022. [Online]. Avaliable: https://www.kaggle.com/datasets/obulisainaren/multi-cancer

[30] Xiaolong Pei et al., "Robustness of Machines Learning to Colors, Size Changes, Normalizations, and Images Enhancements on Micrograph Dataset with Large Samples Difference," *Material & Designs*, vol. 232, pp. 1-13, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[31] Tao Zheng et al., "Differential Whale Optimizations Algorithms," *2021 IEEE International Conferences on Networking, Sensing and Controls (ICNSC)*, Xiamen, China, pp. 1-6, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[32] Alexander Viand, Christian Knabenhans, and Anwar Hithnawi, "Verifiable Fully Homomorphic Encryptions," *arXiv Preprint*, pp. 1-18, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[33] Ruwei Huang, Zhikun Li, and Jianan Zhao, "A Verifiable Fully Homomorphic Encryptions Schemes," *Security, Privacy, and Anonymity in Computations, Communications, and Storages, SpaCCS 2019, Lecture Notes in Computer Sciences*, Atlanta, GA, USA, vol. 11611, pp. 412-426, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[34] Ahmed El-Yahyaoui, and Mohamed Dafir Ech-Cherif El Kettani, "A Verifiable Fully Homomorphic Encryptions Schemes for Cloud Computing Security," *Technologies*, vol. 7, no. 1, pp. 1-7, 2019. [CrossRef] [Google Scholar] [Publisher Link]