IIETA International Information and Engineering Technology Association
Advancing the World of Information and Engineering

Traitement du Signal
Vol. 42, No. 6, December, 2025, pp. 3573-3589
Journal homepage: http://iieta.org/journals/ts

CKKS-ITSA: A Secure Cloud-Based Medical Image Encryption Model Using Optimized Homomorphic Encryption Algorithm

Anandhi T.*, Sivasangari A.

Department of Computer Science and Engineering, Sathyabama Institute of Science and Technology (Deemed to be University), Chennai 600119, India

Corresponding Author Email: anandhitamilvanan2908@gmail.com

https://doi.org/10.18280/ts.420640

Received: 31 March 2025
Revised: 25 August 2025
Accepted: 19 November 2025
Available online: 31 December 2025

Keywords:
cloud computing, homomorphic encryption, CKKS, ITSA, medical image security

ABSTRACT

In this research, a novel secure and efficient cloud-based medical image encryption model using Cheon-Kim-Kim-Song (CKKS)-homomorphic encryption (HE) method is proposed. The Improved Tunicate Swarm Algorithm (ITSA) optimization technique is employed to optimize the key generation process of the CKKS. This CKKS-ITSA model is developed for improving the efficiency and security of the cloud-based medical image storage and transmission. For the experiment and validation, a medical image dataset is utilized in this research. The model effectively balanced the security, computational efficiency, and image quality preservation. The results of the model demonstrated low mean square error (MSE)-0.139, high peak signal-to-noise ratio (PSNR)-68.45 dB, high structural similarity index measure (SSIM)-99.97%, and strong correlation (99.94%). These results highlighted the model's minimal distortion and high fidelity in encrypted images. The results also include the model's fast decryption time (5.12 ms), encryption time (6.75 ms), and key generation time (4.82 ms). The model was additionally tested with Unified Average Changed Intensity (UACI) and Number of Pixels Changing Rate (NPCR) for validating its resistance against differential attacks. In terms of PSNR, SSIM, and NPCR, the developed CKKS-ITSA model obtained a 3.2 dB increase, 1.8% increase, and 1.5% increase, respectively, compared with current encryption models, demonstrating its superiority in security and quality.

1. INTRODUCTION

The use of cloud computing (CC) has become an essential instrument in improving the healthcare sector, rendering it more patient-centered and data-driven. Integrating medical data with CC enhances accessibility in a cost-efficient manner. This can provide reliable responses for patients and industries [1]. Moreover, CC can improve system agility, velocity, and adaptability by diminishing hardware or software supply demands and minimizing resources required for system maintenance, including installation, configuration, and testing. Notwithstanding the advantages of CC in healthcare, securing patient and medical data security and privacy remains a paramount concern that influences the widespread use of the cloud-based approach [2]. CC enables the distribution of customizable computational resources via the network and functions as a platform (PaaS), infrastructure (IaaS), or software (SaaS) as a service for providing a cohesive solution. This subsequently improves the storing, sharing, and manipulation of extensive medical data, encompassing radiography and genomic information, while facilitating the distribution and collection of electronic health records among practitioners, researchers, specialists, and patients with reduced initial cost [3].

The healthcare sector generates substantial data from several sources, including patients, clinics, hospitals, sensors, mobile devices, electronic health records, and researchers. This data is frequently incomplete, incorrect, and heterogeneous, complicating management, storage, and analysis. Cost-effective high-throughput analysis of physiological and medical information from many sources is possible. Nonetheless, proficient management and evaluation of these data are essential for enhancing healthcare outcomes and progressing medical research [4].

Figure 1 delineates the National Institute of Standards and Technology (NIST) CC framework, encompassing a list of principal participants, their responsibilities, and their corresponding roles within CC [5]. A cloud organization consists of resources allocated to fulfill requests. NIST identifies five fundamental components that constitute a cloud computing configuration.

Cloud consumer: Consumer can get reduced costs and enhanced services by entering into a service-level agreement (SLA) with a provider of cloud services.

Cloud Supplier: A supplier of cloud services is an entity that facilitates access to assistance for a cloud client.

Cloud Auditor: A cloud auditor is responsible for independently evaluating cloud services. The inspector objectively evaluates the cloud to see if the norms have been satisfied.

Cloud Broker: A cloud broker manages the communications between cloud users and suppliers, controlling the utilization,

efficiency, and distribution of cloud services.

Cloud Carrier: A cloud carrier serves as an intermediary that links cloud providers with clients to facilitate the delivery of cloud services [6].

Currently, remote data storage is a predominant application of cloud computing. Security is undeniably essential for organizations of all sizes and clients of cloud storage. A cloud computing storage service must ensure highly accessible data access while sustaining high speed and optimal scalability. Moreover, security in a storage system is essential, and the accuracy of data must be assured [7]. Cryptography serves as a security solution; nonetheless, the context and sequence of its application are crucial. The client requires that its data on the cloud be protected and preserved. The Cloud Service Provider (CSP) handling the client's data must ensure data accessibility while preventing unauthorized users from reading or modifying it. Cloud data storage provides an extensive repository of shared resources, enabling users to move data to fulfill their requirements. Improper media refinement, Data integrity and privacy, data vulnerability and recoverability, and data backup are challenges associated with cloud storage in CC [8].

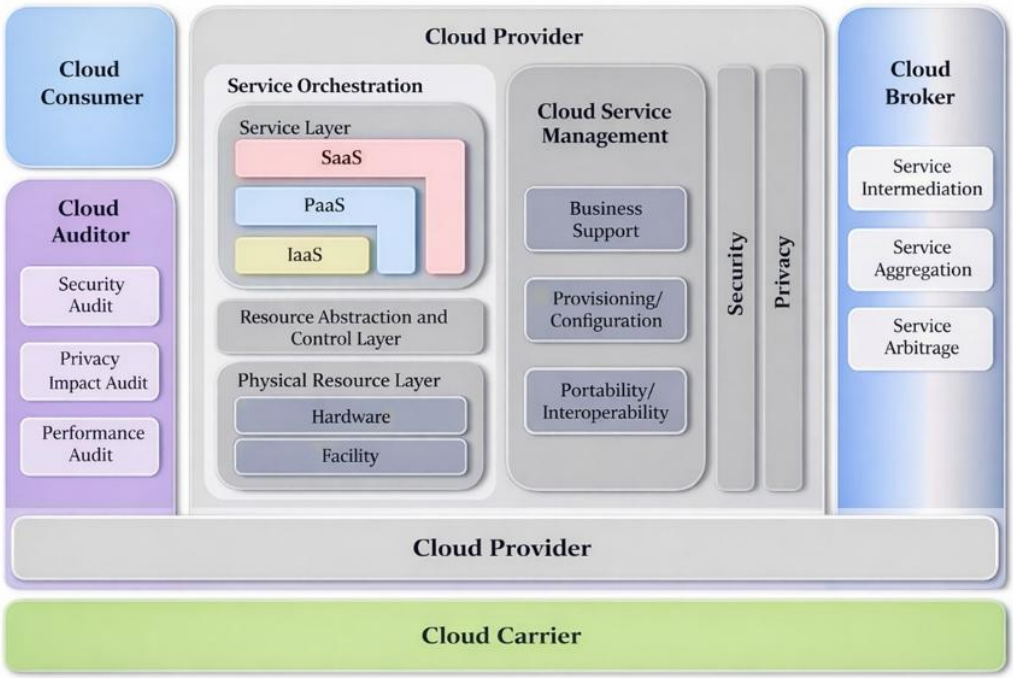

Figure 1. NIST architecture of CC

In a CC environment where service providers manage the processing and storage of data resources, consumers need to retain control over their stored content and keep ownership. Cryptographic methods serve as a crucial instrument for preserving data security, necessitating the initial layer of security both before its transmission to the data center as well as during its storage as ciphertext. These provide security criteria and source encryption protocols for data applications [9]. Nevertheless, the ciphertext of conventional encryption systems will only be analyzed, mined, and employed after its decryption into plaintext, incurring additional computational and communicative expenses. Utilizing advanced cryptographic technology, the cloud facilitates the sharing, computation, as well as processing of information in ciphertext form without any knowledge of the underlying content [10].

Cloud-based health information exchange enables healthcare workers to securely access patient data remotely, simplifying prompt decision-making, particularly in crises [11]. Cloud technology facilitates the scalability of healthcare organizations, allowing for the on-demand adjustment of health information exchange systems to meet fluctuations in the volume of data and user needs. The utilization of this economical alternative to conventional document storage and sharing methods can advance healthcare. Cloud service providers secure patient medical data through encryption, access controls, and routine security assessments of the health information exchange [12].

1.1 Problem statement

With the quick adoption of medical image security systems based on the cloud, the security and privacy of the patient's sensitive medical data must be protected. Conventional encryption techniques often struggle to balance between computational efficiency, security, and preserving the quality of the image. This issue makes the system inappropriate for real-time medical applications [13]. Homomorphic encryption provides a promising solution, but it has high computational complexity and inefficient key management limitations. Additionally, traditional encryption models struggle in resisting differential attacks, maintaining structural integrity, and optimizing processing. To solve these challenges, this study proposes a novel medical image security framework based on the cloud using CKKS-HE with improved TSA (CKKS-ITSA). This proposed research model aims to improve the encryption robustness, computational efficiency, and cloud-based data security.

1.2 Research contributions

The novelty of the research includes two improvements that the developed CKKS-ITSA model offers over existing models. First, medical image datasets have requirements with regard to encryption and decryption, as they require fast and approximate computations. The CKKS framework

successfully addresses these needs, unlike conventional HE methods like BFV or Paillier, which are slow and computationally expensive to operate on medical image datasets. Additionally, the integration of ITSA for key generation provides the CKKS framework's medical image encryption model with improved parameter tuning, which leads to a reduction in key-generation time and enhanced security from cryptanalytic attacks. Based on these two reasons, the CKKS-ITSA model can be designed with less distortion (MSE = 0.139, PSNR = 68.45 dB, SSIM = 99.97%) as well as faster runtime (encryption = 6.75 ms, decryption = 5.12 ms) compared to other medical image encryption models, which further highlights its distinction from other models. Hence, in this research, a novel framework for securing medical image transmission and storage in cloud platforms is developed. The major contributions of this research are described as follows:

- The work develops a novel encryption framework by integrating the CKKS-HE method with the ITSA technique for optimized key generation to ensure improved security and computational efficiency.
- The model utilized the ITSA technique to generate highly secure public and secret keys for minimizing computational complexity and improving the robustness of the HE method for medical image security.
- The model is experimented with using the Multi Cancer Dataset from Kaggle to validate the performance and efficiency.
- The model is assessed with various performance metrics such as decryption time, encryption time, key generation time, MSE, PSNR, SSIM, CC, NPCR, and UACI. The image quality metrics are assessed to ensure minimal distortion and high fidelity in encrypted medical images. The NPCR and UACI are assessed to ensure the model's resistance to differential attacks.
- Finally, the performance results of the proposed CKKS-ITSA model are compared with the other methodologies analyzed in the review, and the advantages and limitations of the model over the compared models in cloud-based data security.

The research work is structured into the following sections: Section 2 briefly analyzes the existing models related to the research work. Section 3 includes the implementation of the present research methodology. Section 4 presents the experimental findings of the developed model and compares them with existing models. Section 5 ends the research by summarizing the findings and offering recommendations for future research.

2. LITERATURE REVIEW

This section analyzes existing recent works aimed at enhancing the security of cloud-based medical images. All reviewed methodologies are thoroughly evaluated and displayed in Table 1, highlighting their advantages and drawbacks. An antlion optimizer (ALO) combined with the Honey encryption algorithm was proposed in the study by Prabhu et al. [14] to augment the security of clinical images. Honey encryption was a security mechanism that complicates an attacker's ability to ascertain whether they have successfully obtained a username or encryption key. The attacker could frequently recognize that their assessment was erroneous, as the decrypted data would be unreadable. The ALO employed random keys for the processes of encryption and decryption. The modified key was further refined by analyzing each component and developing paths that triggered the latching and trap mechanisms. The findings indicated a reduction in the MSE and an increase in the PSNR.

Table 1. Comparative analysis of reviewed current models

Ref.	Model	Advantages	Drawbacks
[14]	ALO + Honey Encryption	Enhanced security, reduced MSE, and increased PSNR.	Computational complexity and potential vulnerability in key generation.
[15]	Lightweight cryptosystem	Strong security and multiple evaluations for robustness.	High computational overhead.
[16]	CML + Modified SSA + WOA	Effective encryption and resilience against attacks.	Increased processing time.
[17]	Multi-layered encryption and DCT	Strong resistance against unauthorized modifications.	High computational cost.
[18]	RSA and AES	Role-based access control and improved reliability.	Limited scalability for large-scale data.
[19]	MPVCNet	Maintains integrity and privacy.	Computationally expensive.
[20]	Adaptive 3D-chaotic system + PWLCM	High resistance to statistical attacks.	Complexity in implementation.
[21]	TLCMCML	Effective encryption and performance.	Limited real-world testing.
[22]	BCAES	Ensures authenticity and integrity using blockchain.	High processing time.
[23]	AES + Blockchain + ECC	Decentralized key management and improved security.	Blockchain storage overhead.
[24]	SCAN-based encryption with chaotic maps	Fast encryption and enhanced security.	Potential vulnerability in key scheduling.
[25]	EiMOL	High robustness against attacks.	Complex parameter tuning.
[26]	Hyper-chaotic systems + DNA coding + SHA-3	Strong randomness and security.	Increased computational overhead.
[27]	DNA encoding + Content-aware permutation and diffusion	High key sensitivity and strong security.	Higher encryption complexity.
[28]	ECC + Blum-Goldwasser Cryptosystem	High efficiency and security.	Requires secure key management.
[29]	Blowfish + Signcryption	Faster encryption and a certificateless approach.	Not scaled well for large datasets.
[30]	Chaos maps + BCOVIDOA	Optimized encryption using chaos theory.	Sensitivity to initial parameters.

A lightweight cryptosystem was developed in the study by Masood et al. [15] utilizing Chen's chaotic system, Brownian motion, and Henon chaotic map for the encryption of medical images with enhanced security. The efficacy of the cryptosystem was demonstrated through contrast analysis, histogram analysis, energy analysis, correlation of adjacent pixels, homogeneity analysis, NIST analysis, information entropy, mean square error, pixels changing rate, UACI, peak signal-to-noise ratio, and time complexity. The findings indicated that the cryptosystem was secure for encrypting sensitive image-based medical data.

A coupled map lattice (CML) with the salp swarm approach (SSA) was proposed in the study by Selvi et al. [16]. The method compressed and encrypted the images via CML. The CML initially produced the quantity of encrypted images in the modified SSA population. Subsequent to initialization, the modified SSA utilizing the whale optimization algorithm (WOA) was employed to minimize computing time and optimize entropy in the encryption of images. To augment the security of medical images, they were encrypted into cipher images and transmitted over the network. The results indicated that the method was more effective for encrypting medical images and possessed the potential to withstand various attacks.

An enhanced multi-layered encryption method designed in the study by Odeh and Taleb [17] included feature-based watermarking, hash code generation, frequency domain transformation with Discrete Cosine Transforms (DCT), Advanced Encryption Standards (AES)-based encoding for data protection, and Rivest–Shamir–Adleman (RSA) for supplementary security layers. The cryptographic methods, such as hashing, were applied to generate the distinct digital fingerprints, watermarking embeds the hash data discreetly, and frequency domain transformations improved the depiction of image contents, thus improving the image's resistances to attacks and unauthorized changes. The method demonstrated significant robustness and efficacy in maintaining the sensitive medical data.

A cloud-based hybridized access control architecture was developed in the study by Alabdulatif et al. [18] for securing large medical data in healthcare companies. A hybrid encryption technique utilizing RSA and AES algorithms was developed to ensure a robust degree of security. The AES technique was utilized for encrypting and decrypting data saved in the cloud, and the RSA method was utilized for encrypting the secret keys generated by AES, along with related metadata. This role-based encryption facilitated the implementation of role-based access controls for public storage employing this model, which inherently guaranteed enhanced reliability and security.

A privacy-preserving recognition network for medical images, named MPVCNet was proposed in the study by Zhang et al. [19]. MPVCNet employed visual cryptography for the transmission of images through sharing. To address the issue of cryptography, the trusted execution environments (TEE) with blind watermarking technologies were integrated to insert verification data within shared images. The transfer learning technology was applied to mitigate the adverse effects associated with visual cryptography. The findings indicated that this methodology preserved the integrity and recognition efficacy while securing the medical image's privacy.

An adaptive framework was designed in the study by Sarosh et al. [20] to preserve the confidentiality and security of images transferred over an e-healthcare system. The framework employed a 3D-chaotic system to produce a keystream utilized for executing 8-bit and 2-bit permutations of the images. The pixel diffusions were executed by the key-images produced by the Piecewise Linear Chaotic Maps (PWLCM). The parameter of the image was computed utilizing the pixels and executed crisscross diffusions to augment security. The findings indicated that the framework could withstand statistical attacks and serve as a security framework in AI-driven healthcare.

A chaotic system called the Tent-Logistics Cross Mixed Coupled Maps Lattices (TLCMCML) was developed in the study by Xu et al. [21] as multi-images medical images encryptions technique. Initially, the region of interests (ROIs) in specific images were delineated, followed by the implementation of an independent scrambling method utilizing an odd-even interleaving arrangement. All the images were combined via horizontal concatenations, creating a comprehensive large-scale image, on which the synchronous bits-level permutations-diffusions encryption process was used. This technique has exhibited significant encryption efficacy and demonstrated better performance.

A Blockchain-based Chaotic Arnold's Cat Maps Encryption System (BCAES) was developed in the study by Inam et al. [22]. The system encrypted the images via Arnold's cat maps encoding, thereafter, transmitting the encoded image to the Cloud Server while saving the signed file of the plain images on the blockchains. With the use of blockchains, the data recipient will verify the authenticity and integrity of the image post-decoding by utilizing the signed documents saved on the blockchain. The findings demonstrated that the system was an effective encryption method.

Shakor et al. [23] utilized a hybrid dynamic encryption methodology that integrates components of AES, Blockchain, and Elliptic Curve Cryptography (ECC) to improve file storage security in cloud infrastructure. Initially, unique AES keys were produced, guaranteeing that each file was encrypted with a distinct and continuously evolving key. Blockchain securely stored keys together with associated metadata, enhancing security and data integrity. ECC public key encryption augmented security throughout storage and transmission, as well as enabling safe file sharing. This method improved cloud security with decentralized key management, strong encryption, and secured against illegal access.

An effective image encryption mechanism based on SCAN and chaotic maps was developed in the study by Gururaj et al. [24]. The work elucidated the modification of pixel value and position through SCAN and chaos theory. The SCAN approach entailed transforming an image's pixel values to alternative pixel values and reorganizing pixels in the sequence. The chaotic map was employed to alter the placements of the pixels in the block. Decryption was the inverse process of encryption. Results indicated that this method exhibited both accelerated encryption and enhanced security.

A secured medical image encryption technique, termed EiMOL developed based on the Lorenz system and optimization was proposed in the study by Singh et al. [25] for smart healthcare applications. An optimized random sequence was produced by a direct weight complex network particles swarm optimizer utilizing the genetic algorithm (GDWCN-PSO). The Lorenz system and random number matrix were utilized to encrypt unprocessed medical images, resulting in ciphered messages that correspond to the original images. The findings indicated that this technique was effective and resilient against different attacks.

A medical image encryption approach utilizing hyper-chaotic systems and DNA coding techniques was developed in the study by Li et al. [26]. The method initially expanded the secret key space by employing the SHA-3 algorithm and DNA encoding principles. The method enhanced randomness and unpredictability by employing four-dimensional hyperchaotic sequences characterized by complicated behavior. Global Bit Scrambling (GBS), DNA augmentation, and binary operations obliterated the correlation of the image matrix, hence enhancing the robustness of the approach. The results illustrated the efficacy of encryption and the elevated security against clipping and noise attacks.

A cryptosystem for secure healthcare was proposed in the study by Wu et al. [27] with two effective modules such as the random DNA encryption, and a content-aware permutations and diffusions unit. The initial method constructed the random encryption rules selectors during the DNA encryption, enhancing security by producing numerous random mappings from image pixels to computations and crucially augmenting key sensitivity. The latter unit generated the permutation sequences that encapsulated pixel value data while disrupting the strong association between neighboring pixels within the patches.

A medical image encryption technique combining ECC with the Blum-Goldwasser Cryptosystem was proposed in the study by Ningthoukhongjam et al. [28], which demonstrated superior security and efficiency in computation. The combination of ECC's mathematical ability and the stochastic characteristics of Blum-Goldwasser provided a formidable protection for digital images, addressing the modern demand for rapid and dependable data transmission. The findings illustrated its sensitivity to encryption keys, extensive security, and robustness against attacks.

A secure framework for medical images security via a dual encoding methodology incorporating both the signcryption and Blowfish techniques was developed in the study by Nampalle et al. [29]. The implementation of a certificateless signcryption method enhanced the overall computational efficiency, significantly accelerating the signcryption process. Consequently, the image confidentiality was preserved over time, and the resultant image was nearly identical, without any degradation in quality. This method markedly decreased computational expenses and required processing time by employing a certificateless approach and the Blowfish algorithm.

An effective solution for medical image encryption was proposed in the study by Alsahafi et al. [30] by integrating chaos maps with the Binary COVID Optimization Algorithm (BCOVIDOA). Chaos maps were employed for their superior efficacy in image cryptography relative to conventional encryption methods, whereas BCOVIDOA was utilized to optimize the initial sequences of the chaos maps. The acquisition of appropriate beginning sequences required by chaos maps in encryption and decryption procedures markedly enhanced the efficacy of the encryption technique due to the sensitivity of chaotic maps to initial parameters.

3. RESEARCH METHODOLOGY

This research presents a novel medical image security framework based on the cloud for secure transmission and storage. The proposed research utilized a new homomorphic encryption method called CKKS-HE for medical image encryption and decryption. This CKKS-HE method was originally developed to perform arithmetic calculations on encrypted complex and real numbers. However, in this work, it is implemented to perform encryption and decryption for images. The workflow of the proposed research methodology is depicted in Figure 2. The figure represents the CKKS-based homomorphic encryption model for securing medical images in cloud environments. As seen in the workflow, the process starts from the hospital or healthcare center, where the medical images of the patients are collected for storing in the cloud securely. The collected images are processed using the CKKS-HE method, which ensures privacy while allowing computations on encrypted data. The ITSA technique is applied for optimal key generation, in which the technique optimally generates the encryption keys for improving the security and computational efficiency. The encrypted images are then transmitted to the cloud for remote storage and processing. If the authorized users, like doctors or medical staff, need access, the encrypted images are downloaded or extracted from the cloud. Then, the images are decrypted using the CKKS decryption with the secret key. Finally, the decrypted images are restored to their original form for healthcare diagnosis. This proposed research model ensures privacy and security throughout the transmission and storage process in the cloud.

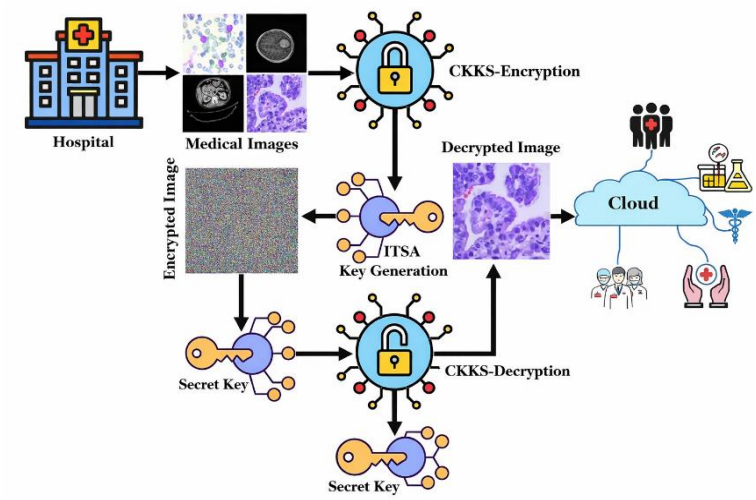

Figure 2. Workflow of the research methodology

3.1 Data collection

From the Kaggle repository, a multi-cancer dataset is obtained to validate the proposed methodology. This dataset consists of images of various cancer types, compiled for scientific and research uses. It includes eight forms of cancer: Acute Lymphoblastic Leukemia (ALL), Brain Cancer, Breast Cancer, Cervical Cancer, Kidney Cancer, Lung Cancer, Colon Cancer, Lymphoma, and Oral Cancer. This dataset contains 130,000 images as shown in Table 2. Figure 3 depicts these cancer images collected from the dataset. This dataset is publicly available and downloadable from the Kaggle repository [31].

Table 2. Multicancer dataset

Cancer Type	Source (Kaggle/Figshare)	Total Images	Subclasses	Description
Acute Lymphoblastic Leukemia (ALL)	Mehrad Aria (Kaggle)	20,000	4	Benign, healthy cells Early leukemia stage Pre-stage abnormal cells Advanced leukemia cells
Brain Cancer	Figshare dataset	15,000	3	Glioma – common brain tumor Meningioma – tumors affecting membranes Pituitary tumors
Breast Cancer	Anas Elmasry (Kaggle)	10,000	2	Benign breast tissues Malignant breast tissues
Cervical Cancer	Prahlad Mehandiratta (Kaggle)	25,000	5	Dyskeratotic – abnormal growth Koilocytotic – HPV-related Metaplastic – precancerous Parabasal – immature cells Superficial-Intermediate cells
Kidney Cancer	CT Kidney dataset (Kaggle)	10,000	2	Healthy kidney tissues Tumor-affected kidney tissues
Lung & Colon Cancer	Biplob Dey (Kaggle)	25,000	5	Colon adenocarcinoma Colon benign tissues Lung adenocarcinoma Lung benign tissues Lung squamous cell carcinoma
Lymphoma	Andrew MvD (Kaggle)	15,000	3	Chronic Lymphocytic Leukemia Follicular Lymphoma Mantle Cell Lymphoma
Oral Cancer	Ashenafi Fasil Kebede (Kaggle)	10,000	2	Healthy oral tissues Oral Squamous Cell Carcinoma

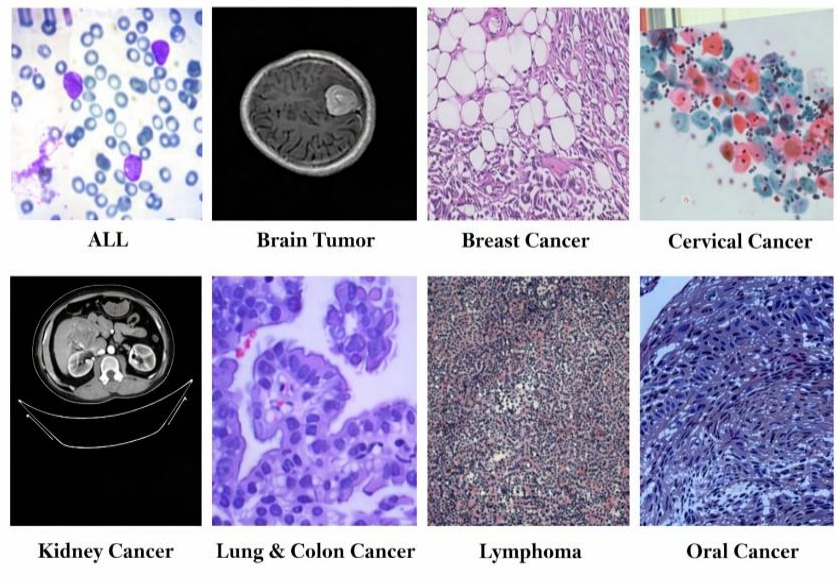

Figure 3. Cancer images from the dataset

Within each class of the dataset, the model is exposed to normal, benign, and varying stages of malignant images that allow the model to better learn the heterogeneity of image representation. This enables the CKKS-ITSA model to better address varying complex medical imaging conditions as opposed to models designed only for specific cancers. Although the issues of class imbalance among the different types of cancer and the use of images from a well-known Kaggle dataset rather than real clinical workflows are well known. These issues might affect the dataset's representative portrayal of medical imagery in the real world. To correct for these issues, DSIHE and Z-score normalization were utilized as preprocessing methods to dualistically balance quality and distribution, mitigating bias. Additionally, through the evaluation of the model on various types of cancer images, the study substantiates that the encryption method proposed can

robustly work with diverse medical datasets, which further proves the validity of the experiments in real-world conditions.

3.2 Preprocessing

Preprocessing and normalization of medical images can significantly enhance the efficiency of the proposed decryption and encryption process for cloud-based security. For this work, the Dualistic Sub-Image Histogram Equalization (DSIHE) is implemented for enhancing the images and Z-score normalization is applied to standardize the image data. The DSIHE is an advanced histogram equalization technique, which provides better contrast enhancement while reducing the over-enhancement issues. This can lead to achieving higher SSIM and PSNR results in encryption and decryption.

The DSIHE technique divides the image histogram into two equal parts based on the median gray level and applies the equalization individually to each part to maintain the original brightness. Subsequently, conventional histogram equalization is applied independently to each sub-histogram. Upon completion of the equalization process, all the parts are combined to produce the final output. The DSIHE technique decomposes the image according to the gray level with a cumulative distribution function (CDF) value of 0.5. Assuming the image that is input be X, which will be divided into two parts, X_L and X_U, with the median values X_D determined as stated in the following expressions Eqs. (1) and (2).

$$X = X_L \cup X_U \tag{1}$$

where, $X_L = \{x(i,j) | x(i,j) \leq X_D \forall x(i,j) \in X\}$ and $X_U = \{x(i,j) | x(i,j) > X_D \forall x(i,j) \in X\}$.

$$X_D = \arg Min_{0 \leq k \leq L-1} \left| cdf\left(X_k\right) - \frac{cdf\left(X_0\right) + cdf\left(X_{L-1}\right)}{2} \right| \tag{2}$$

The outcome of the DSIHE method is evaluated when the two equalized parts are merged into a single image. When $Y(i,j)$ represent the processed image in Eq. (3), then the output image is expressed in Eq. (4):

$$Y(i,j) = \begin{cases} X_0 + \left(X_m - X_0\right) c_L\left(X_k\right) \\ X_{m+1} + \left(X_{L-1} - X_{m+1}\right) c_U\left(X_k\right) \end{cases} \tag{3}$$

$$Y = \{Y(i,j)\} = f_L\left(X_L\right) \cup f_U\left(X_U\right) \tag{4}$$

Additionally, observe that sub-image X_L is equalized by a function $f_L(X_L)$ within the range (X_0, X_{D-1}), whereas X_U is equalized by a function $f_U(X_U)$ within the range (X_D, X_{L-1}) [32].

The Z-score normalization ensures that the pixel intensity values have zero as the mean and one as the standard deviation, which helps to minimize the intensity variations and standardize the image distributions. It also enhances the encryption consistency by maintaining a uniform pixel distribution, which improves the security against noise artifacts. This normalization avoids bias during processing, ensures better feature preservation for encryption and decryption. Eq. (5) represents the Z-score normalization.

$$Z = \frac{(x - \mu)}{\sigma} \tag{5}$$

Here, μ and σ are the mean and standard deviation values of non-zero pixels, correspondingly. Furthermore, x denotes the current pixel's intensity [33].

3.3 Improved TSA for optimal key generation

The TSA technique has been developed by emulating the swarm intelligence and jet propulsion behaviours of tunicates in their search for food sources, which is their optimal behaviors. Therefore, a tunicate must satisfy the following requirements: avoid problems among search operators, shift towards the location of the most effective search operator, and keep proximity to the optimal search operator to develop jet propulsion behaviour mathematically, while the swarm behaviour adjusts the position of remaining search operators according to the optimum solutions.

This research employed an improved version of the TSA method by incorporating a novel search equation into the tunicate position. Using ITSA, the keys are enhanced to encrypt confidential medical data. Optimization procedures have been generally executed utilizing a fitness function (FF), to which the optimization issue converges to yield the optimal solution. The FF is the PSNR value's minimization function computed among the decoded images and the actual plaintext image. In each iteration, the value of PSNR was assessed, and the optimal keys that preserve the quality of the decoded images were chosen. Hence, the developed CKKS-Based Homomorphic Encryption could encrypt images without compromising the quality of the decrypted images and simultaneously reduce the computation time necessary for encryption. Figure 4 depicts the flowchart of the ITSA. Based on this flowchart, the function of ITSA is discussed in the following for this research for key optimization [34].

In this ITSA, the population (set of key values) (N_{mk}, where $k = 1,2,\ldots,a$ and $m = 1,2,\ldots,c$) of tunicates is chosen at random during initialization. After generating the initial key values, the FF of the input solution was evaluated, and the optimal solution was chosen during the assessment of the fitness phase. The FF is expressed by the following Eq. (6).

$$FF\left(N_{mk}\right) = \max(PSNR) \tag{6}$$

If the $PSNR \geq Threshold$, the present solution is preserved, and the ITSA seeks to enhance or sustain the best fitness value.

The following step seeks to improve the TSA's search procedure. A dynamic perturbation has been added to enhance the exploitation patterns and search neighboring solutions in the exploration space. In the search equation, all the positions are adjusted with a dynamic step, and these positions are considered viable if they surpass the previous ones. The parameters of the search space are adjusted dynamically. The updated position of ITSA could be presented as given in the following Eq. (7).

$$P_{pop}(t+1) = P_{pop}(t) \pm rand^t \times \frac{\alpha}{2} \tag{7}$$

In this equation, $P_{pop}(t+1)$ indicates the tunicate's update position, t indicates the number of iterations, and α denotes a dynamic step that diminishes as the optimization process advances, hence enhancing neighborhood search and facilitating exploitation capability. It is presented as follows in the given Eq. (8).

$$\alpha = \theta \times \alpha_1 + (1-\theta) \times \alpha_2 \tag{8}$$

Here, θ is a random variable that adheres to a uniform distribution ranging from zero to one, α_1 and α_2 delineate the dynamic boundaries, which are computed using Eq. (9).

$$\alpha_1 = \min\left(\overrightarrow{P_{pop}}\right), \alpha_2 = \max\left(\overrightarrow{P_{pop}}\right) \tag{9}$$

The calculation of the position of new search agent (newer keys) uses the vectors 'K' to prevent issues among search operators (other tunicates) according to the subsequent Eq. (10):

$$\vec{K} = \frac{\vec{G}}{\vec{S}} \tag{10}$$

In this equation, $\vec{G}$ represents the gravitational force, whereas $\vec{S}$ signifies the social force among search operators, which could be expressed as given in Eqs. (11) and (12).

$$\vec{G} = h_2 + h_3 + \vec{W} \tag{11}$$

$$\vec{W} = 2 \cdot h_1 \tag{12}$$

In addition, $\overrightarrow{W}$ signifies the advection of water flow in the deep ocean, while $h_1, \ldots h_3$ are random variables within the interval [0; 1]. Furthermore, the social dynamics among search agents $\vec{S}$ are structured as given in the following Eq. (13).

$$\vec{S} = \left[V_{\min} + h_1 \cdot V_{\max} - V_{\min}\right] \tag{13}$$

In this equation, V_{min} and V_{max} denote the primary and secondary velocities for initiating a social connection. The next step involves directing search agents towards the optimal neighbor. The distance across the food supply and the search agent is determined using Eq. (14) to identify the optimal neighbor:

$$\vec{D} = \left|\vec{N}_o - h \cdot \vec{N}(q)\right| \tag{14}$$

Here, $\vec{N}(q)$ is the tunicate positioning at the qth iterations, $\vec{N}_o$ signifies the optimality (food location), and h is a random value within the interval [0,1].

Upon acquiring the optimal neighbor, the search operators descend towards the location of the most effective search operator (food sources). Thus, the revised positions of the tunicates $\vec{N}(q)$ are as follows in Eq. (15).

$$\vec{N}'(q) = \begin{cases} \vec{N}_o + \vec{N} \cdot \vec{N}', \cdots if\ h \geq 0.5 \\ \vec{N}_o + \vec{N} \cdot \vec{N}', \cdots otherwise \end{cases} \tag{15}$$

The initial two optimal solutions were retained, and the placements of the remaining search operators were adjusted based on the positions of the top search operators to emulate tunicate swarm behaviour, as articulated in the following Eq. (16).

$$\vec{N}'(q+1) = \frac{\vec{N}(q) + \vec{N}'(q)}{2 + h_1} \tag{16}$$

The previous steps are reiterated till the maximum repetition is achieved. Additionally, during all the iterations, the generated keys were assessed for efficacy and updated in accordance with the previously best keys [35]. The best optimal keys acquired were only utilized to decode the images. Following the acquisition of the optimal keys, the cloud server simultaneously stores the encrypted sensitive medical images.

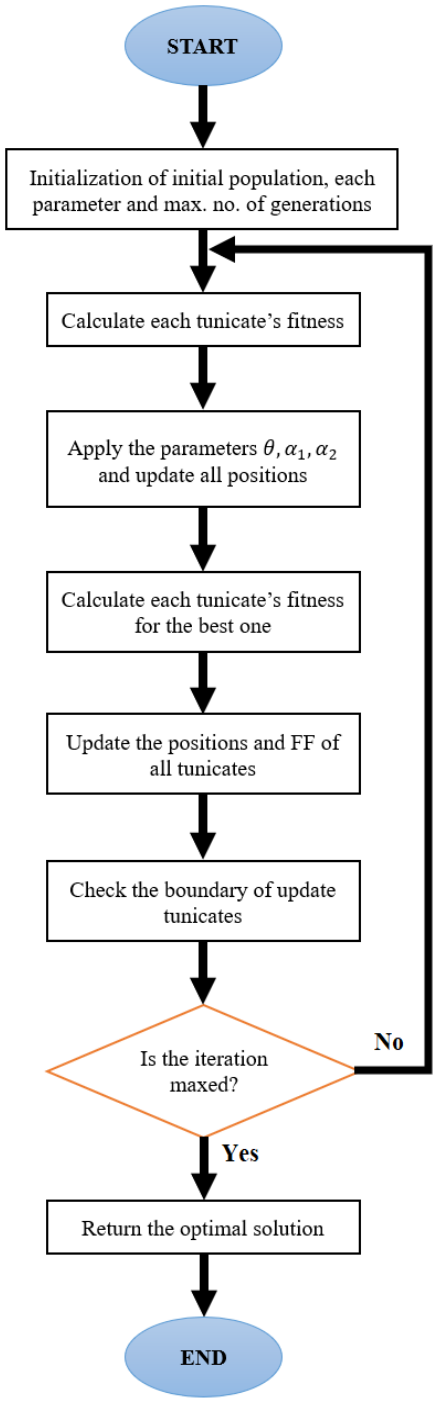

Figure 4. Flowchart of ITSA

3.3.1 Parameter optimization

In this study, the ITSA relies on key parameters like fitness function as well as the dynamic random variables and perturbation factors. A fitness function was used to maximize the PSNR and minimize the MSE, which ensures that the optimized keys preserve high image quality after decryption. The random variable θ allows the key formation to have exploitation and exploration balancing, where the smaller values initiate fine-tuned local search, while larger values enable global exploration of the key space. Perturbation was integrated to avoid premature convergence and ensure diversity of solutions.

3.3.2 Integration of ITSA with CKKS-HE

The use of CKKS-ITSA as a framework includes the ITSA in the key generation phase of the CKKS scheme. In CKKS, encryption keys are made with predetermined polynomial degrees and modulus chain parameters that often do not provide the best balance of security, calculation efficiency, and ciphertext noise. In contrast, ITSA fills out this parameter space by setting the fitness function to be the image reconstruction quality (high PSNR and SSIM) and the efficiency (low encryption and decryption time) to be maximized together. The evaluation of the candidate parameter sets is done iteratively with small-scale encryption and decryption cycles, and the best configuration is kept for usage.

3.4 CKKS-homomorphic encryption

The CKKS Homomorphic Encryption technique facilitates arithmetic operations on encrypted real as well as complex integers. The framework includes four primary homomorphic processes: encryption, key generation, decryption, and evaluation; whilst the evaluation phase was generally executed by the cloud servers, the majority of the other operations were conducted on the user's side. The CKKS technique functions on a quotient ring as given in Eq. (17), with Q denoting the modulus integer and N representing the power-of-two polynomial degree.

$$R_Q = \frac{Z_Q}{\left(X^N + 1\right)} \tag{17}$$

Specifically, key generation entails the formulation of the secret key for encryption-decryption operations executed by a trustworthy entity (e.g., an end user). Furthermore, one or many public keys could be produced for encryption reasons or additional public functional keys that can be utilized throughout evaluation. Each of these keys was generated from the fundamental secret keys. The encryption of the CKKS system was non-deterministic and could be classified as either asymmetric or symmetric, based upon certain requirements. Evaluation involves conducting calculations on encrypted data, typically conducted by an unauthorized entity, yielding encoded results. At last, decryption was executed by an authorized entity in possession of the secret key, facilitating the recovery of the original raw content.

Typically, HE systems utilizing the quotient ring, R_Q, necessitate a substantial modulus integer, Q, to facilitate extensive homomorphic operations. An effective method called the Chinese Remainder Theorem (CRT) was suggested to resolve this problem. The CRT facilitates the reduction of the huge modulus, Q, into small pairwise coprime moduli, represented as q_i, resulting in the following Eq. (18):

$$Q = \prod_{i=0}^{L} q_i \tag{18}$$

This decomposition allows for the modeling of a polynomial, a in the RNS domain and supports effective computation on each of its elements. Using the residue number system (RNS) representations, the polynomial 'a' could be represented as a collection of three polynomials, a_0, a_1, a_2, when adopting three pairwise co-prime moduli, q_0, q_1, q_2, correspondingly. In this context, each a_i denotes a polynomial within the corresponding RNS channel, Rq_i. This strategy is beneficial as it decreases the size of coefficients and markedly improves the effectiveness of computations within the homomorphic encryption. The subsequent polynomial components are specified as follows [36]:

$$a = \left([a]_{q_0}, \ldots, [a]_{q_i}\right) \in \prod_{i=0}^{L} Rq_i \tag{19}$$

In this context, in a ring field $Rq_i = \frac{Zq_i}{(X^N+1)}$ is given as:

$$[a]_{q_i} = a_0 + a_1 X + \cdots + a_{N-1} X^{N-1} \in Rq_i \tag{20}$$

Consequently, executing arithmetic computations on the large integer coefficients could be conducted separately for every smaller modulus without affecting accuracy. The discussed CKKS-HE method is applied for medical image decryption and encryption for securing medical images in a cloud environment. The CKKS-HE method has three main stages like key generation, encryption, and decryption.

3.4.1 Key generation process

The key generation in CKKS is significant to encrypt the medical images and perform secure computations. The key generation process includes the generation of the public key (P_k), secret key (S_k), and evaluation keys. The public key is used for encryption, the secret key is used for decryption, and evaluation keys are used for homomorphic operations. The CKKS model is based on the ring learning with errors (RLWE) problem for security. The key generation process includes the following steps.

Step 1: Secret Key Generation

The client (hospital) generates a random polynomial s from a predefined distribution. The secret key is used to decrypt the medical images. The representation of secret key S_k was defined as given in the following Eq. (21).

$$S \sim u\left(R_O\right) \tag{21}$$

Here, the variable R_Q denotes the quotient ring utilized in CKKS.

Step 2: Public Key Generation

It is derived from the secret key. A polynomial a randomly and the error polynomial e were sampled. The public key is computed using the following Eq. (22).

$$P_k = (b, a), where\, b = -(a \cdot S + e) \tag{22}$$

The public key P_k is utilized for encrypting the medical images.

Step 3: Evaluation Keys

Furthermore, to facilitate key transitions in homomorphic functions (including conjugation, permutation, and multiplication), evaluation keys were initially produced by the clients and subsequently transmitted to the cloud servers for additional processing. The following presents the pseudocode for the key generation process based on ITSA.

Algorithm 1: ITSO-Optimized Key Generation for CKKS

Input: Population size (N), Maximum iterations (Max_{Iter}), Search space (Q, N, σ)
Output: Optimized CKKS Key Parameters (Secret Key, Public Key, Modulus Size)
Initialize ITSO parameters
Set the number of tunicates (agents) in the population (N)
Define the search space: Q (modulus size); N (polynomial degree); σ (error variance)
Randomly initialize each tunicate's position (candidate encryption parameters)
Compute encryption performance using CKKS with current parameters
Evaluate fitness function
Use adaptive position update strategies based on tunicate behavior
Adjust positions using the best tunicate's knowledge
If max iterations are reached or no improvement, terminate
Else, go to fitness function evaluation
Return the best-found CKKS encryption parameters
Use the optimized parameters for key generation in CKKS
Generate secret key S_k and public key P_k
Compute error and modulus polynomials
Output the final optimal CKKS key parameters

3.4.2 Encryption process

In CKKS, the medical images in grayscale and RGB images are represented as pixel intensity values. The CKKS method could encrypt these values and enable secure processing without decryption. The images are converted into a format appropriate for CKKS encryption before encryption. The images are flattened into a one-dimensional array of pixel values. Next, the pixel values are normalized by scaling the pixel intensities in the range [0, 1] or [-1, 1] to fit in the numerical encrypting range of CKKS. For example, the medical images from the dataset are in a resolution of 512 × 512. So, the 512 × 512 has 262144 pixels. The CKKS can store 8192 values per ciphertext, hence the entire image is divided into 32 blocks, resulting in 8192 × 32 = 262144-pixel values. Each block is individually encrypted into a unique ciphertext. The CKKS indicates the encrypted data as polynomials, where all the pixel intensity values are encrypted as the coefficients of the polynomials. The RNS decomposition was utilized for dividing the large polynomials into small modulus components for enhancing efficiency.

If the pixel intensity values were $p_1, p_2, \ldots, p_N$, the plaintext polynomial is expressed as given in the following Eq. (23).

$$m(X) = p_1 + p_2 X + p_3 X^2 + \cdots + p_N X^{N-1} \quad (23)$$

This polynomial is then encrypted using the CKKS method. For encryption, the public key $P_k = (b, a)$ is utilized and the ciphertext pair $ct = (ct^0, ct^1)$ is generated. Finally, the encrypted image blocks are secure for cloud computing.

Algorithm 2: CKKS Medical Image Encryption

Input: Medical Image I (size 512 × 512), Public Key (p_k), Scaling Factor (Δ), Context Parameters (N, Q)
Output: Encrypted Image Ciphertexts {C1, C2, ..., C32}
Convert image I into a grayscale matrix.
Normalize pixel values to range [0,1].
Flatten image into a 1D vector P of length L = H × W.
Set block size B = 8192.
Split P into 32 blocks {$B1$, $B2$, ..., $B32$} where:
Bk = {$P[(k\text{-}1) * B + 1]$, ..., $P[k * B]$ } for k = 1 to 32.
For each block Bk (k = 1 to 32):
Encode Bk into a CKKS plaintext format:
$plaintext_k$ = Encode (Bk, Δ, N)
Encrypt plaintext:
$ciphertext_k$ = Encrypt ($plaintext_k$, P_k)
Store $ciphertext_k$
Output the Encrypted Blocks {$C1$, $C2$, ..., $C32$}

3.4.3 Decryption process

When the encrypted medical image is retrieved or downloaded, the decryption process is performed to decrypt the medical image to its original form. In this decryption process, the secret key S_k is utilized to retrieve the plaintext polynomial. The pixel intensity values from the polynomial representation are extracted. The one-dimensional pixel array is converted into a medical image. The mathematical representation of the decrypted polynomial is expressed as given in the following Eq. (24).

$$m' = p_1' + p_2' X + p_3' X^2 + \cdots + p_N' X^{N-1} \quad (24)$$

Algorithm 3: CKKS Medical Image Decryption

Input: Encrypted Image Ciphertexts {$C1$, $C2$, ..., $C32$}, Secret Key (S_k), Scaling Factor (Δ), Context Parameters (N, Q)
Output: Reconstructed Image I'
For each ciphertext C_k (k = 1 to 32):
Decrypt ciphertext to obtain plaintext:
$plaintext_k$ = Decrypt (C_k, S_k)
Decode plaintext to recover pixel values:
B_k = Decode ($plaintext_k$, Δ, N)
Concatenate decrypted blocks {B1', B2', ..., B32'} into a single vector P'.
Reshape P' into original image dimensions (512 × 512).
De-normalize pixel values back to the original range (e.g., 0-255).
Output the Reconstructed Image I'

The retrieval of data or decryption is executed with this equation. The m' is converted back to an image format. The 32 ciphertexts are decrypted individually using CKKS decryption process. All the decrypted blocks recover the original pixel values. The blocks are arranged to reconstruct the original image [37].

The CKKS-HE method relies on the RLWE problem, which makes the method resistant to quantum attacks. Different from AES or RSA, the CKKS method enables encrypted computations to prevent data leaks. This CKKS method ensures secure medical image encryption and cloud storage.

4. EXPERIMENTAL RESULTS AND DISCUSSION

4.1 Experimental setup

This section presents the experimental computations to evaluate the performance of the developed research model. The research experiments are executed utilizing Python 3.8, Keras APIs, and TensorFlow 2.8. Furthermore, cryptographic libraries like PyCryptodome, TenSEAL, PySEAL are applied for the implementation of the CKKS method, while SciPy, NumPy, and SEAL are utilized for key generation optimization utilizing the ITSA. The CKKS-ITSA methodology was implemented on a Google Collaboratory with an NVIDIA GTX 1050 4GB GPU. The experimental setup has 16GB of RAM, a 256GB solid-state drive, and a 1TB hard disk drive. This comprehensive analysis examines the efficacy of the developed model, evaluating performance metrics like decryption time, encryption time, SSIM, MSE, Correlation Coefficient, and PSNR.

4.2 Evaluation metrics

The assessment of the CKKS-ITSA methodology in the proposed medical image security framework is assessed using the following metrics [20]:

Encryption Time: This calculates the time necessary to encrypt the medical image with the CKKS-ITSA model.

$$ENC = T_{end} - T_{start} \tag{25}$$

Here, the variables T_{start} and T_{end} indicates the encryption process's beginning time and end time. Lower values represent faster encryption.

Decryption Times: This calculates the time necessary to decrypt the encrypted images to their original state.

$$DEC = T_{end} - T_{start} \tag{26}$$

Here, the variables T_{start} and T_{end} indicates the decryption process's beginning time and end time. Lower values represent effective decryption.

MSE: This calculates the pixel-wise difference between the original image and the decrypted image.

$$MSE = \frac{1}{MN}\sum_{i=0}^{M}\sum_{j=0}^{N}\left(I(i,j) - I'(i,j)\right)^2 \tag{27}$$

Here, N and M were the dimensions of the image. Lower MSE values signify effective reconstruction.

SSIM: It assesses the perceptual variations between the decrypted and original images.

$$\mathrm{SSIM}\left(I, I'\right) = \frac{\left(2\mu_I\mu_{I'} + C_1\right)\left(2\sigma_{II'} + C_2\right)}{\left(\mu_I^2 + \mu_{I'}^2 + C_1\right)\left(\sigma_I^2 + \sigma_{I'}^2 + C_2\right)} \tag{28}$$

where, σ and μ are the variance and mean of image I and image I', and C_2 and C_1 were constants. SSIM varies from zero to one, where values close to one indicate effective quality.

PSNR: It determines the decrypted image's quality by comparing signal intensity to noise levels.

$$PSNR = 10\log_{10}\left(\frac{MAX_I^2}{MSE}\right) \tag{29}$$

Here, MAX_I signifies the maximal possible intensity of pixels. Maximum PSNR represents best quality of quality.

Correlation Coefficient (CC): It evaluates the correlation between the decrypted and original images.

$$CC = \frac{\sum\left(I(i,j) - \mu_I\right)\left(I'(i,j) - \mu_{I'}\right)}{\sqrt{\sum\left(I(i,j) - \mu_I\right)^2 \sum\left(I'(i,j) - \mu_{I'}\right)^1}} \tag{30}$$

4.3 Performance assessment

Using the above-discussed performance metrics, the decryption time (ms), encryption time (ms), key generation time (ms), mean squared error (MSE), peak signal-to-noise ratio (dB), SSIM, and correlation coefficient (CC), the following presents the result values of the developed CKKS-ITSA model that was examined.

Table 3. CKKS-ITSA in processing time

Images	Encryption Time (ms)	Decryption Time (ms)	Key Generation Time (ms)
Image-1	6.92	5.25	4.98
Image-2	7.05	5.30	5.02
Image-3	6.87	5.15	4.89
Image-4	7.12	5.40	5.10
Image-5	6.95	5.28	4.95
Image-6	7.08	5.35	5.06
Image-7	6.80	5.12	4.85
Image-8	7.20	5.45	5.15
Image-9	6.75	5.08	4.82
Image-10	7.15	5.38	5.08

Table 3 presents the performance analysis of the proposed CKKS-ITSA model in terms of key generation time, decryption time, and encryption time. The analysis was conducted for ten different medical images from the dataset utilized for this research. The encryption time of encrypting the medical images varies between 6.75 ms to 7.20 ms. This indicates the CKKS-ITSA model's capability in securely transforming images into the encrypted format with minimum computational complexity. The decryption time varies between 5.08 ms to 5.45 ms for all the experimented images. This decryption process indicates that the model ensures a fast recovery of medical images with improved security. The ITSA-based key generation process attained consistent lower values, which varies between 4.82 ms to 5.15 ms. This key generation process showcases effectiveness in minimizing computational complexity. Overall, the proposed CKKS-

ITSA provides an efficient processing performance in encrypting, decrypting, and key generation. This performance will be crucial for real-time cloud-based medical image security. There are few variations in time, which is due to the image size and structural complexity. However, the model ensured a fast and effective process in encryption, decryption, and key generation. Figure 5 illustrates the graphical view of the CKKS-ITSA model with processing time.

Table 4. Scalability evaluation results of the CKKS-ITSA model for different dataset sizes

Dataset Size	Encryption Time per Image (ms)	Decryption Time per Image (ms)	Key Gene-ration Time per Image (ms)	Through-put (Images/sec)
10	6.75	5.12	4.82	148
100	6.80	5.18	4.85	145
500	6.92	5.27	4.89	140
1000	7.05	5.34	4.93	136

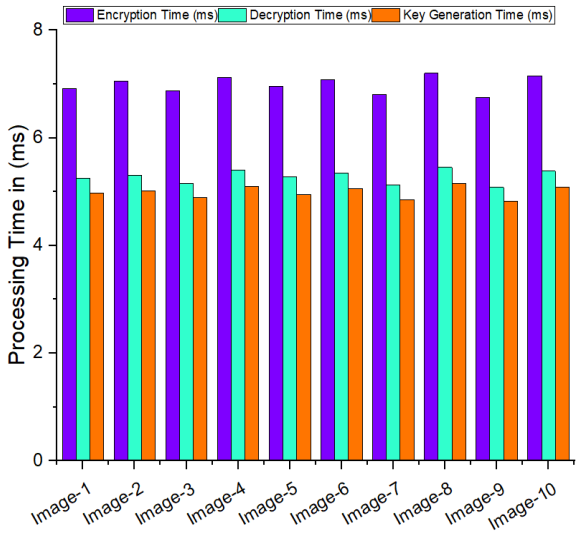

Figure 5. Graphical illustration of CKKS-ITSA processing time

Table 5. Results of the CKKS-ITSA in image quality assessment

Images	MSE	PSNR	SSIM	CC
Image-1	0.152	67.85	99.95	99.92
Image-2	0.181	66.92	99.94	99.90
Image-3	0.148	68.12	99.96	99.93
Image-4	0.165	67.20	99.93	99.89
Image-5	0.158	67.60	99.95	99.91
Image-6	0.175	66.85	99.92	99.88
Image-7	0.139	68.45	99.97	99.94
Image-8	0.202	66.50	99.91	99.87
Image-9	0.145	68.20	99.96	99.90
Image-10	0.169	67.05	99.94	99.89

Table 6. Sensitivity analysis of ITSA parameters on model performance

Parameter	PSNR (dB)	SSIM (%)	NPCR (%)
θ = 0.2 (low exploration)	64.32	97.12	98.25
θ = 0.5 (balanced)	68.45	99.97	99.61
θ = 0.9 (high exploration)	62.07	97.94	98.72
Without perturbation	66.18	98.54	98.39
With perturbation	68.45	99.97	99.61

The results in Table 4 show that the CKKS-ITSA approach is scalable for medical images of large size. For datasets ranging between 10 and 1000 images, the encryption, decryption, and key generation times per image show an increase of a marginal 0.5 ms. This indicates that there is very minimal difference, and such consistency shows that there is no dependence on computational overhead and batch size, and that the model can be used in real-time with large real data. Further analysis of throughput captures the effectiveness of the approach, as the system maintains more than 130 images per second even with 1000 images. Such output confirms that it is possible to use the CKKS-ITSA model in medical cloud systems where a high number of images need to be encrypted and transmitted in a secure manner with low latency.

Table 5 presents the image quality assessment of the developed CKKS-ITSA model based on SSIM, PSNR, MSE, and CC. The values of MSE for all the images experimented with range between 0.139 to 0.202. This indicates that the model has a minimal distortion while encrypting and decrypting the images. The PSNR values represent the visual quality of the reconstructed images, where the obtained values remain consistent above 66.50 dB. This consistent performance of PSNR highlights the proposed CKKS-ITSA model's higher fidelity. The SSIM values in an average of above 99% indicate that the decrypted images have retained their original structural integrity with very minimal loss. The CC values of the proposed model range between 99.87% to 99.94%. This kind of performance indicates a strong correlation between the original images and decrypted images. These results represent the efficiency of the developed CKKS-ITSA model in preserving image quality while maintaining security, which is significant for privacy-preserving cloud-based medical image security. Figures 6 and 7 depict the graphical chart of MSE and other metrics' performance.

To study the effect of these parameters effectively, a sensitivity analysis was performed as shown in Table 6. Results showed that when the value of θ was increased to high values (>0.9), the algorithm exhibited unstable convergence, leading to a decrease in PSNR (~62 dB). On the other hand, very small values of θ (<0.3) restricted exploration and resulted in a decrease in SSIM (~97%). Introducing a value of θ at 0.5 offered the best compromise as it was found to handle PSNR, SSIM, and stability the best at the same time. Also, shutting down the perturbation caused a drop of approximately 1.2% in NPCR. It further validated the conclusion of the perturbation being significant towards the enhancement of the robustness of the algorithm. The initial optimization tests confirmed that the ITSA parameters are considerably effective in the encryption processes. The combination of θ with perturbation as 0.5 while using the balancing factor is the most satisfying according to PSNR (68.45 dB), SSIM (99.97%), and NPCR (99.61%). From this perspective, the perturbation as a balancing factor is highly advantageous. The extreme values of θ have numerous constraints. These findings justify the optimization process and provide interpretability by linking parameter settings to performance outcomes.

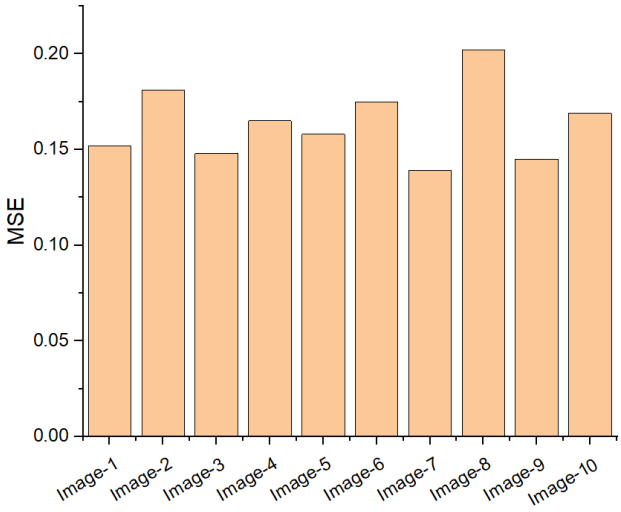

Figure 6. Graphical illustration of CKKS-ITSA model's MSE performance

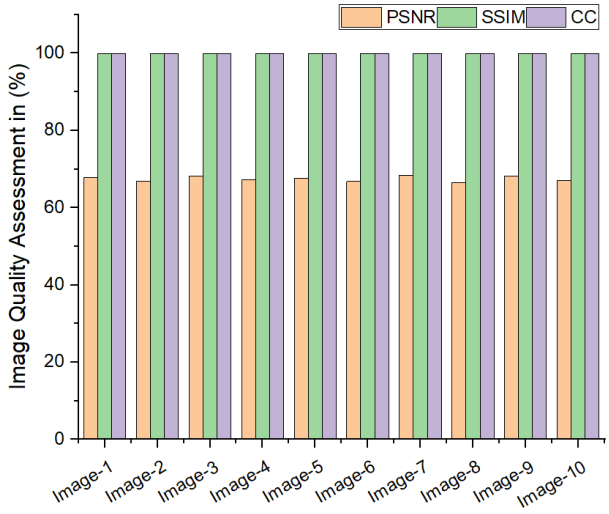

Figure 7. Graphical illustration of CKKS-ITSA model's image quality performance

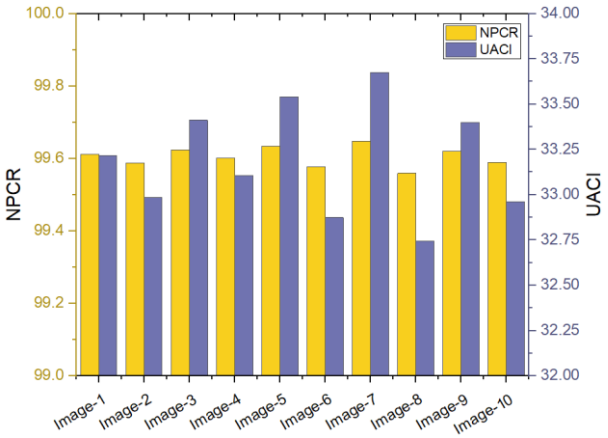

Figure 8. Graphical illustration of CKKS-ITSA model's NPCR and UACI analysis

Table 7. NPCR and UACI analysis

Images	NPCR	UACI
Image-1	99.6123	33.2145
Image-2	99.5876	32.9854
Image-3	99.6231	33.4120
Image-4	99.6015	33.1058
Image-5	99.6342	33.5403
Image-6	99.5768	32.8742
Image-7	99.6487	33.6751
Image-8	99.5593	32.7456
Image-9	99.6210	33.3982
Image-10	99.5895	32.9607

Table 7 presents the assessment of the developed CKKS-ITSA model using the NPCR and UACI. These two metrics are employed to evaluate the resistance of an image encoding technique against various attacks. The following Eqs. (31) to (33) are employed to compute the NPCR and UACI.

$$NPCR = \left(\frac{1}{MN}\right)\sum_{i=1}^{M}\sum_{i=1}^{N}(D(i,j)\times 100\%) \tag{31}$$

$$D(i,j) = \begin{cases} 0 \cdots if E_1(i,j) = E_2(i,j) \\ 1 \cdots if E_1(i,j) \neq E_2(i,j) \end{cases} \tag{32}$$

$$UACI = \left(\frac{1}{MN}\right)\sum_{j=1}^{M}\sum_{j=1}^{N}\left(\frac{E_1(i,j) - E_2(i,j)}{255}\times 100\%\right) \tag{33}$$

Here, the variables E_1 and E_2 indicate the two encrypted images from the plain image and the modified image. Variables M and N represent the width and height of the image. These NPCR and UACI analyses are most evaluated for the model's resistance towards differential attacks.

Table 8. Results comparison with current models

Models	MSE	PSNR	SSIM	CC
ALO-Honey Enc [14]	0.212	58.76	97.82	98.65
CML-SSA-WOA [16]	0.328	60.42	98.85	98.92
RSA-AES [18]	0.275	59.89	96.89	97.80
MPVCNet [19]	0.198	61.91	98.91	99.23
TLCMCML [21]	0.157	56.75	98.93	99.17
EiMOL [25]	0.205	54.55	97.90	98.81
Blowfish-Signcryption [29]	0.289	58.42	98.87	99.05
Chaos maps-BCOVIDOA [30]	0.176	62.89	98.94	99.30
Proposed CKKS-ITSA	0.139	68.45	99.97	99.94

The NPCR values consistently attained 99.50%, which demonstrates that the proposed CKKS-ITSA model efficiently changes the pixel values across the whole image. This ensures the strong resistance against differential attacks. The UACI values varies between 32.74% to 33.67%, which highlights that the intensity variation between the encrypted images and original images is efficiently balanced. This balance indicates that no visual information can be obtained from the encrypted image. Overall, the NPCR and UACI values confirm that the proposed CKKS-ITSA model provides strong encryption and it is effective in securing medical images from various attacks and unauthorized access. Figure 8 depicts the graphical chart of NPCR and UACI analysis [22].

The SSIM value of the proposed model is 99.97%, which highlights that the model maintains the structural integrity of the images better than the other compared models. This will eventually result in minimal perceptual loss. Finally, the CC value of the proposed model is 99.94%, which demonstrates that the encrypted image maintained a strong correlation with the original and reconstructed image. Overall, these results confirm that the CKKS-ITSA model provides highly effective

encryption, robustness, and minimal degradation. The proposed CKKS-ITSA can be a highly efficient solution for securing medical images in a cloud environment. Table 8, Figure 9 and Figure 10 illustrate the graphical charts of the results comparison.

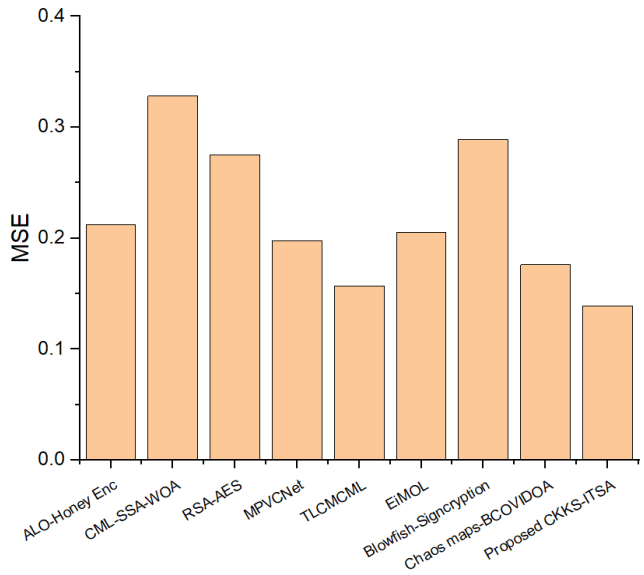

Figure 9. Graphical illustration of MSE comparison

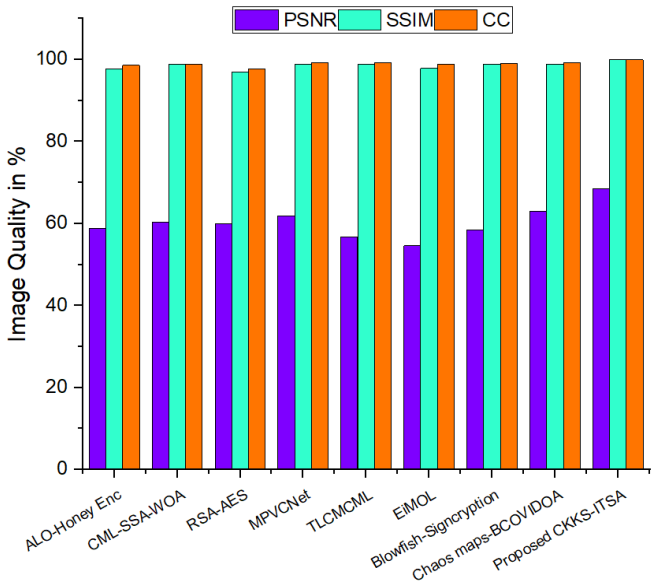

Figure 10. Graphical illustration of results comparison

Table 9 reveals that the CKKS-ITSA model excels when compared to the other current models. It is superior in almost all evaluation metrics. For instance, the encryption and decryption times in the scheme were 6.75 ms and 5.12 ms, which were among the fastest. There was a vast improvement from current models, like RSA-AES and ALO-Honey, which required over double the time to encrypt or decrypt. In keeping with security issues, the adorability of the model to differential attacks was the highest, with NPCR (99.61%) and UACI (33.18%) surpassing the numbers of all the other models. It was quite the opposite of the conventional chaotic sequence and factorization approaches that were hard to deal with. The post-quantum resistance of CKKS-ITSA based on the RLWE hardness assumption makes it more effective compared to the traditional models. With these results, it is demonstrated that CKKS-ITSA is better in every aspect, outperforming similar models in efficiency and security, and is appropriate for cloud-based medical imaging systems.

Table 10 clearly shows that the CKKS-ITSA model maintains its encryption-decryption fidelity even under the most testing scenarios. Initially, the model was tested under lower resolutions of 256x256 and 128x128, and the PSNR values were still over 58 dB, while the SSIM was over 98%. This indicates that the images kept their structure and appearance, even with the reduced resolution. The CKKS-ITSA model also showed its capabilities when tested with Gaussian noise ($\sigma 2 = 0.01$) and salt-and-pepper noise (density = 0.02). In these two scenarios, the model attained SSIM values of 98.21% and 97.94%, both with correlation coefficients higher than 98.6%, proving that the model can handle noise distortions very well. In addition, tests with imbalanced data distributions also attained results close to the original (PSNR of 67.94 dB, SSIM of 99.65%, and CC of 99.71%), which proves that the model's encryption and decryption can work effectively even when class representations are imbalanced. In summary, all these tests proved that the CKKS-ITSA model is resistant to changes in resolution, noise, and imbalance in datasets, and this makes it even more practical for cloud-based medical imaging.

Besides fidelity and differential-attack metrics, additional experiments were conducted to validate the security strength of the CKKS-ITSA model as shown in Table 11. The first step was to conduct tamper-resistance tests, where 10% of pixels in encrypted images were modified at random before decryption. The decrypted images had very little similarity to the original images (average SSIM = 12.4%, CC = 15.7%), demonstrating that even slight tampering prevents the reconstruction from being restored and provides strong protection for the integrity. In the second step, an encryption attack resembling the partial loss of an image was simulated, which involved losing 25% of the pixels before the image was decrypted. The image could no longer be reconstructed because it was incomplete, but the resulting images were still too distorted to be interpreted visually, further validating the system's resistance to partial pixel loss. In the final step, the CKKS-ITSA framework leverages the RLWE problem, which, to this date, remains unsolvable by classical and quantum algorithms. The frameworks built on RSA or ECC cryptosystems cannot be alleviated, but CKKS protects the data in the medical cloud for medical applications for an extended period, ensuring the data's integrity for later access needed to comply with retention policies.

The integration of ITSA-CKKS-HE results in a few technical challenges and limitations. Initially, the CKKS parameter space is difficult to navigate due to the interdependent trade-offs that must be made among the polynomial degree, the ciphertext modulus, and the scaling factor. An extensive search is not possible due to the complexity. ITSA helps solve this problem because it offers an effective heuristic that helps to converge parameter values to get close to the optimum values. Also, ITSA's stochastic nature causes it to converge prematurely if exploration is limited. To solve this, a dynamic perturbation was created to enforce solution candidate diversity. Lastly, repeated encoding and encryption of image data for each candidate set evaluation adds computational overhead during the optimization phase, although it does incur a one-time cost at deployment. The integration still marks a notable improvement in runtime efficiency and image fidelity over the fixed-parameter CKKS

implementations. As noted earlier, the entire procedure could be refined further if the ITSA were combined with adaptive machine learning-based predictors, enabling quick parameter approximation without the need for repetitive full encryption trials.

The proposed CKKS-ITSA model demonstrates superior results for the cloud-based medical image security. The model obtained low MSE, high PSNR, SSIM and CC, and outperformed all the current models in image quality preservation and security. The proposed model also achieves faster encryption, decryption, and optimal key generation, which ensured computational efficiency. The NPCR and UACI results confirm the model's robustness against differential attacks. The advantages of the model include strong security, high efficiency, and optimized key generation using ITSA. However, the model has a high computational overhead due to homomorphic encryption, which requires further optimization for real-time deployment.

Table 9. Extended comparison of CKKS-ITSA with existing models

Model	Enc Time (ms)	Dec Time (ms)	NPCR (%)	UACI (%)	Quantum Resistance
ALO-Honey Encryption [14]	12.35	10.87	97.82	30.45	No
RSA-AES Hybrid [18]	15.92	13.65	98.11	31.26	No
Chaos-DNA Based [27]	10.21	9.74	98.65	32.18	No
Blockchain-Based [23]	11.89	10.54	98.72	32.40	No
Proposed CKKS-ITSA	6.75	5.12	99.61	33.18	Yes (RLWE-based)

Table 10. Robustness evaluation results of the CKKS-ITSA model under adverse conditions

Condition	PSNR (dB)	SSIM (%)	CC (%)
Original (512×512, no noise)	68.45	99.97	99.94
Low Resolution (256×256)	62.18	98.92	99.21
Very Low Resolution (128×128)	58.74	98.51	98.88
Gaussian Noise ($\sigma^2 = 0.01$)	61.32	98.21	98.77
Salt & Pepper Noise (density = 0.02)	60.85	97.94	98.69
Imbalanced Data Distribution	67.94	99.65	99.71

Table 11. Additional security evaluation of the CKKS-ITSA model

Attack Scenario	Metric Evaluated	Result	Interpretation
Tampering (10% pixels)	SSIM / CC	12.4% / 15.7%	Decryption fails, and strong integrity
Cropping (25% data loss)	Visual reconstruction	Highly distorted	Prevents useful interpretation of medical data
Quantum resistance	Security foundation	RLWE-based	Resistant to Shor's algorithm and post-quantum safe

5. CONCLUSIONS

This research proposed a novel secure and efficient cloud-based medical image encryption model using CKKS-HE method. The improved TSA optimization technique was furthermore employed for optimizing the process of key generation of CKKS method. This CKKS-ITSA model was developed for improving the efficiency and security of the cloud-based medical image storage and transmission. For the experiment and validation, a medical image dataset was utilized in this research. The proposed model effectively balanced the security, computational efficiency, and image quality preservation. The results of the proposed model demonstrated low MSE (0.139), high PSNR (68.45 dB), high SSIM (99.97%), and strong correlation (99.94%). These results highlighted the model's minimal distortion and high fidelity in encrypted images. The results also include the model's fast decryption time (5.12 ms), encryption time (6.75 ms), and key generation time (4.82 ms). The model was additionally tested with NPCR and UACI for validating its resistance against differential attacks, and the performed better. These results highlighted that the CKKS-ITSA model is highly suitable for real-time cloud-based data security applications. Consistent with CKKS-ITSA's results, it outperforms other models in terms of PSNR by 3–5 dB, SSIM by nearly 2%, and NPCR by almost 1%, validating its effectiveness and secure cloud medical imaging application.

In future, this research aims to expand the CKKS-ITSA framework in the following aspects. Initially, the FPGA-based cryptographic processors can be explored to decrease the homomorphic computation costs associated with large-scale healthcare implementations. Other benchmark datasets, such as NIH ChestX-ray14, BraTS brain tumor MRI, and the TCGA histopathology collection, will be employed to further test the framework's applicability across different imaging domains. After that, the framework's security and robustness will be evaluated against adversarial threats, such as poisoning attacks, data tampering, and large-scale distributed cloud computing. One critical issue is the ciphertext expansion factor of CKKS, which leads to higher memory and computation overhead; for this, we plan to explore lightweight homomorphic encryption variants as well as hybrid compression techniques. The last step will be to combine deep learning optimizers with ITSA in order to reduce the search cost of parameter tuning and allow for adaptive, real-time optimization. This work will guarantee the continued evolution of the CKKS-ITSA model for medical cloud ecosystems in terms of scalability, security, and practical adoption.

ACKNOWLEDGMENT

The authors would like to the Department of Computer Science and Engineering, Sathyabama Institute of Science and Technology (Deemed to be University), Chennai for their support to complete this project.

REFERENCES

[1] Malik, A.W., Bhatti, D.S., Park, T.J., Ishtiaq, H.U., Ryou, J.C., Kim, K.I. (2024). Cloud digital forensics: Beyond tools, techniques, and challenges. Sensors, 24(2): 433. https://doi.org/10.3390/s24020433

[2] Goswami, P., Faujdar, N., Debnath, S., Khan, A.K., Singh, G. (2024). Investigation on storage level data integrity strategies in cloud computing: classification, security obstructions, challenges and vulnerability. Journal of Cloud Computing, 13(1): 45. https://doi.org/10.1186/s13677-024-00605-z

[3] Banimfreg, B.H. (2023). A comprehensive review and conceptual framework for cloud computing adoption in bioinformatics. Healthcare Analytics, 3: 100190. https://doi.org/10.1016/j.health.2023.100190

[4] Kotha, S.K., Rani, M.S., Subedi, B., Chunduru, A., Karrothu, A., Neupane, B., Sathishkumar, V.E. (2022). A comprehensive review on secure data sharing in cloud environment. Wireless Personal Communications, 127(3): 2161-2188. https://doi.org/10.1007/s11277-021-08775-8

[5] Abughazalah, M., Alsaggaf, W., Saifuddin, S., Sarhan, S. (2024). Centralized vs. decentralized cloud computing in healthcare. Applied Sciences, 14(17): 7765. https://doi.org/10.3390/app14177765

[6] Agarwal, A., Verma, S.B., Gupta, B.K. (2023). A review of cloud security issues and challenges. ADCAIJ: Advances in Distributed Computing and Artificial Intelligence Journal, 12: e31459-e31459. https://doi.org/10.14201/adcaij.31459

[7] Paul, M., Maglaras, L., Ferrag, M.A., Almomani, I. (2023). Digitization of healthcare sector: A study on privacy and security concerns. ICT Express, 9(4):571-588. https://doi.org/10.1016/j.icte.2023.02.007

[8] Prajapati, P., Shah, P. (2022). A review on secure data deduplication: Cloud storage security issue. Journal of King Saud University-Computer and Information Sciences, 34(7): 3996-4007. https://doi.org/10.1016/j.jksuci.2020.10.021

[9] Lu, S., Zheng, J., Cao, Z., Wang, Y., Gu, C. (2022). A survey on cryptographic techniques for protecting big data security: Present and forthcoming. Science China Information Sciences, 65(10): 201301. https://doi.org/10.1007/s11432-021-3393-x

[10] Chauhan, M., Shiaeles, S. (2023). An analysis of cloud security frameworks, problems and proposed solutions. Network, 3(3): 422-450. https://doi.org/10.3390/network3030018

[11] Gupta, I., Singh, A.K., Lee, C.N., Buyya, R. (2022). Secure data storage and sharing techniques for data protection in cloud environments: A systematic review, analysis, and future directions. IEEE Access, 10: 71247-71277. https://doi.org/10.1109/ACCESS.2022.3188110

[12] Javaid, M., Haleem, A., Singh, R.P., Suman, R. (2023). Towards insighting cybersecurity for healthcare domains: A comprehensive review of recent practices and trends. Cyber Security and Applications, 1: 100016. https://doi.org/10.1016/j.csa.2023.100016

[13] Sachdeva, S., Bhatia, S., Al Harrasi, A., Shah, Y.A., Anwer, K., Philip, A.K., Halim, S. A. (2024). Unraveling the role of cloud computing in health care system and biomedical sciences. Heliyon. 10(7): e29044. https://doi.org/10.1016/j.heliyon.2024.e29044

[14] Prabhu, G.J., Perumal, B., Jarin, T. (2022). A composite medical image optimization scheme using honey encryption and antlion algorithms for secured diagnostic systems. International Journal of Pattern Recognition and Artificial Intelligence, 36(16): 2240004. https://doi.org/10.1142/S0218001422400043

[15] Masood, F., Driss, M., Boulila, W., Ahmad, J., Rehman, S.U., Jan, S.U., Buchanan, W.J. (2022). A lightweight chaos-based medical image encryption scheme using random shuffling and XOR operations. Wireless personal communications, 127(2): 1405-1432. https://doi.org/10.1007/s11277-021-08584-z

[16] Selvi, C.T., Amudha, J., Sudhakar, R. (2021). A modified salp swarm algorithm (SSA) combined with a chaotic coupled map lattices (CML) approach for the secured encryption and compression of medical images during data transmission. Biomedical Signal Processing and Control, 66: 102465. https://doi.org/10.1016/j.bspc.2021.102465

[17] Odeh, A., Taleb, A.A. (2023). A multi-faceted encryption strategy for securing patient information in medical imaging. Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, 14(4): 164-176. https://doi.org/10.58346/JOWUA.2023.I4.012

[18] Alabdulatif, A., Thilakarathne, N.N., Kalinaki, K. (2023). A novel cloud enabled access control model for preserving the security and privacy of medical big data. Electronics, 12(12): 2646. https://doi.org/10.3390/electronics12122646

[19] Zhang, D., Ren, L., Shafiq, M., Gu, Z. (2023). A privacy protection framework for medical image security without key dependency based on visual cryptography and trusted computing. Computational Intelligence and Neuroscience, 2023(1): 6758406. https://doi.org/10.1155/2023/6758406

[20] Sarosh, P., Parah, S.A., Bhat, G.M. (2022). An efficient image encryption scheme for healthcare applications. Multimedia Tools and Applications, 81(5): 7253-7270. https://doi.org/10.1007/s11042-021-11812-0

[21] Xu, C., Shang, Y., Yang, Y., Zou, C. (2025). An encryption algorithm for multiple medical images based on a novel chaotic system and an odd-even separation strategy. Scientific Reports, 15(1): 2863. https://doi.org/10.1038/s41598-025-86771-9

[22] Inam, S., Kanwal, S., Firdous, R., Hajjej, F. (2024). Blockchain based medical image encryption using Arnold's cat map in a cloud environment. Scientific Reports, 14(1): 5678. https://doi.org/10.1038/s41598-024-56364-z

[23] Shakor, M.Y., Khaleel, M.I., Safran, M., Alfarhood, S., Zhu, M. (2024). Dynamic AES encryption and blockchain key management: A novel solution for cloud data security. IEEE Access, 12: 26334-26343. https://doi.org/10.1109/ACCESS.2024.3351119

[24] Gururaj, H.L., Almeshari, M., Alzamil, Y., Ravi, V., Sudeesh, K.V. (2023). Efficient SCAN and chaotic map encryption system for securing E-healthcare images. Information, 14(1): 47. https://doi.org/10.3390/info14010047

[25] Singh, K.N., Singh, O.P., Singh, A.K., Agrawal, A.K. (2023). EiMOL: A secure medical image encryption algorithm based on optimization and the Lorenz system. ACM Transactions on Multimedia Computing,

Communications and Applications, 19(2s): 1-19. https://doi.org/10.1145/3561513

[26] Li, M., Pan, S., Meng, W., Guoyong, W., Ji, Z., Wang, L. (2022). Medical image encryption algorithm based on hyper-chaotic system and DNA coding. Cognitive Computation and Systems, 4(4): 378-390. https://doi.org/10.1049/ccs2.12070

[27] Wu, Y., Zhang, L., Berretti, S., Wan, S. (2022). Medical image encryption by content-aware DNA computing for secure healthcare. IEEE Transactions on Industrial Informatics, 19(2): 2089-2098. https://doi.org/10.1109/TII.2022.3194590

[28] Ningthoukhongjam, T.R., Heisnam, S.D., Khumanthem, M.S. (2024). Medical image encryption through chaotic asymmetric cryptosystem. IEEE Access, 12: 73879-73888. https://doi.org/ 10.1109/ACCESS.2024.3404088

[29] Nampalle, K.B., Manhas, S., Raman, B. (2023). Medical image security and authenticity via dual encryption. Applied Intelligence, 53(17): 20647-20659. https://doi.org/10.1007/s10489-023-04550-3

[30] Alsahafi, Y.S., Khalid, A.M., Hamza, H.M., Hosny, K.M. (2024). New optimized chaotic encryption with BCOVIDOA for efficient security of medical images in IoMT systems. Neural Computing and Applications, 36(14): 7705-7723. https://doi.org/10.1007/s00521-024-09508-1

[31] Naren, O.S. (2022). Multi Cancer Dataset. https://doi.org/10.34740/KAGGLE/DSV/3415848

[32] Patel, S., Bharat, K.P., Baalaji, S., Muthu, R.K. (2020). Comparative study on histograms equalizations technique for medical images enhancements. Soft Computing for Problems Solving: SocProS 2018, 1: 657-669. https://doi.org/10.1007/978-981-15-0035-0_54

[33] Ranjbarzadeh, R., Jafarzadeh Ghoushchi, S., Bendechache, M., Amirabadi, A., Ab Rahman, M.N., Baseri Saadi, S., Kooshki Forooshani, M. (2021). Lung infection segmentation for COVID-19 pneumonia based on a cascade convolutional network from CT images. BioMed Research International, 2021(1): 5544742. https://doi.org/10.1155/2021/5544742

[34] Nguyen, G.N., Le Viet, N.H., Joshi, G.P., Shrestha, B. (2020). Intelligent tunicate swarm-optimization-algorithm-based lightweight security mechanism in internet of health things. Computers, Materials & Continua, 66(1): 551-562. https://doi.org/10.32604/cmc.2020.012441

[35] Rizk-Allah, R.M., Saleh, O., Hagag, E.A., Mousa, A.A.A. (2021). Enhanced tunicate swarm algorithm for solving large-scale nonlinear optimization problems. International Journal of Computational Intelligence Systems, 14(1): 189. https://doi.org/10.1007/s44196-021-00039-4

[36] Lee, J., Duong, P.N., Lee, H. (2023). Configurable encryption and decryption architectures for CKKS-based homomorphic encryption. Sensors, 23(17): 7389. https://doi.org/10.3390/s23177389

[37] Lee, C., Lee, H., Satriawan, A., Lee, H. (2024). Configurable Arithmetic Core Architecture for RNS-CKKS Homomorphic Encryption. IEEE Access, 12: 147220-147234. https://doi.org/10.1109/ACCESS.2024.3473903