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

Traitement du Signal
Vol. 42, No. 1, February, 2025, pp. 29-43
Journal homepage: http://iieta.org/journals/ts

Homomorphic with Henon-Map Encryption over Medical Image Data Confidentiality in Cloud and Classifying Images Using Deep Learning Approaches in IoT

K. Saranya[1*], A. Valarmathi[2]

[1] Faculty of Information and Communication Engineering, UCE-BIT Campus, Anna University, Chennai 620 024, India
[2] Department of Computer Applications, UCE-BIT Campus, Anna University, Chennai 620 024, India

Corresponding Author Email: saranyaokk@yahoo.com

https://doi.org/10.18280/ts.420104

Received: 23 April 2024
Revised: 13 September 2024
Accepted: 6 November 2024
Available online: 28 February 2025

Keywords:
IoT, cloud computing, homomorphic encryption, Henon-Map encryption, medical image classification, deep learning

ABSTRACT

Cloud computing which safeguards the medical information and strengthen the datas. This study proposes a novel solution for strengthening security for collections of medical images stored in the cloud through the integration of homomorphic encryption based on Henon-Map encryption. In order to ensure privacy during the process of classification, a deep learning the model by the VGG16 is also applied to data. The data encrypted is thereafter put through homomorphic encryption, allowing secure computation of information without the need for decryption. Operations can be performed on data that has been encrypted without pre-interpretation due to homomorphic encryption. For maintaining data of the medical image, Henon-Map encryption is first used to encrypt the medical image dataset, thereby adding non-linearity and chaos. In which the encrypted data and decrypted data in the cloud server. The scheme presented delivers safe and secret substitutes for medical image databases stored in the cloud. The usage of integrity and privacy implies homomorphic encryption and Henon-Map encryption. Using deep learning, we were able to establish anonymity protection while still achieving correct image categorization. Both "CNN" model and "VGG16" structure helps an encryption technique yields very accurate results. The different performance metrics are evaluated for the following proposed approach which determines better "Accuracy", "Precision", "F1-Score," "Recall", "Specificity", "Confusion matrix", higher "PSNR" score (70%), lower "MSE" score (0), "NPCR" and "UACI" were obtained, stating that, the developed "Henon- Homomorphic encryption" model is good to suitable that enhances "IoT"- based cloud security to preserve digital medical images.

1. INTRODUCTION

Applications for homomorphic encryption include safe cloud computing, secure data analysis, and reliable machine learning. The data is kept secure and safe against unauthorized access while being handled by third-party service providers. Nevertheless, there are some drawbacks to homomorphic encryption, such as increased computational expense and slower processing speed compared to traditional encryption methods. Taking these challenges into account, ongoing research and development of homomorphic encryption techniques are making them more useful and efficient in real-world applications. There are several ways that IoT gateway devices can store and transport encrypted medical image data, based on the specific requirements and IoT system architecture. Encrypted medical images can be temporarily stored on the gateway prior to forwarding to the cloud. This approach could be useful data buffering during intermittent connectivity.

Directly from the IoT gateway, secured medical data images could be transported in an automatic mode to cloud storage service. The ability of deep learning to acquire an independent hierarchical representation of data so it can encode for itself concurrently the low-level as well as the high-level characteristics and dependencies present in data is one of the basic strengths. Deep learning is thus particularly helpful for tasks such many more tasks that have lots of complex trends and hierarchies.

In order to train a neural networks using a technique known as deep learning, a large labeled sample is often needed. In order to find the hidden patterns and correlations, the dataset is separated into training and testing sets. The trained model's accuracy and generalizability are assessed by observing its performance on the testing set. It is possible to construct many deep learning models using various deep neural network principles. For image-related tasks, one may use convolutional neural networks (CNNs). For sequence data, one may use recurrent neural networks (RNNs). For challenges connected to natural language processing, one can use transformer frameworks. Models that use deep learning are trained using optimization techniques such as unpredictable, which successively modifies the model's parameters, to decrease the difference among the predicted and actual outputs.

Regularization methods, including weight decay and dropout, are frequently used to increase the generalizability of the model and reduce overfitting. Figure 1 indicates the proposed architecture diagram for analyzing the cloud data

securely stored using Henson-homomorphic encryption. Using protocols like HTTPS or SFTP, the IoT gateway could establish a secure connection to the cloud storage provider and transfer the encrypted data over the internet. The encrypted data is subsequently safely and scalable stored by the cloud storage service. Medical data images are gathered by real-time IoT gateway devices from a variety of sources, including wearables, medical sensors, and gadgets. They serve as a bridge between the cloud platform and the data source.

Deep learning has achieved unparalleled success in various disciplines, notably. Deep learning continues to expand dramatically and can revolutionize many areas in addition to solving complex problems previously difficult for classical approaches to tackle. Scalability, access, and collaboration are some of the many benefits of keeping groups of medical images stored in the cloud. Cloud storage's scalability facilitates seamless capacity expansion. It can be extremely large and have a huge storage requirement. Cloud services give users the freedom to expand the storage capacity when needed, ensuring that there is sufficient space to accommodate increasing datasets. Medical images can be securely and conveniently accessed from anywhere there is an internet connection by saving them in the cloud.

This availability facilitates collaboration and higher productivity by allowing authorized personnel, such as researchers, health specialists, and other experts, to review and analyze the images remotely. The need for having on-premises storage facilities, which may be costly to deploy and sustain, is eliminated through cloud storage. When we talk about the need to safeguard patient information included inside medical photographs, we're talking about the confidentiality of that data. Maintaining the privacy of this information is critical for compliance with legal and ethical mandates as well as for the protection of patient information. Prevent unauthorized access by encrypting medical images. It is to ensure that, whether intercepted or stolen, it is not decryptable without a proper decryption key.

In sending medical images between different systems or hospitals, employ secure transmission protocols such as ensuring that they remain private while in the process of transmission. The Henon encryption method is employed in encrypting collected. This method offers data security with encryption and randomization. A specific form of encryption, homomorphic encryption as it is referred to, supports computation based on data encrypted without having the need for decrypting it. Here, data confidentiality and integrity are ensured by moving while maintaining their encrypted form.

Utilizing secure communication protocols, the medical data images encrypted are transmitted on this platform. It ensures the protection of the data during transmission. When received on the cloud platform, the corresponding decryption key can be utilized to decrypt them. The IoT refers to a network of physically linked things with capabilities for data gathering and data exchange. However, it is critical to guarantee the safety and security of this medical data.

The data remains confidential at all stages because of this. When transmitting sensitive medical photos, it is important to use an encryption method called Henson-map encryption. The combination and use of these encryption algorithms allow for the safe transmission and storage of medical pictures on the cloud, hence preventing illegal data.

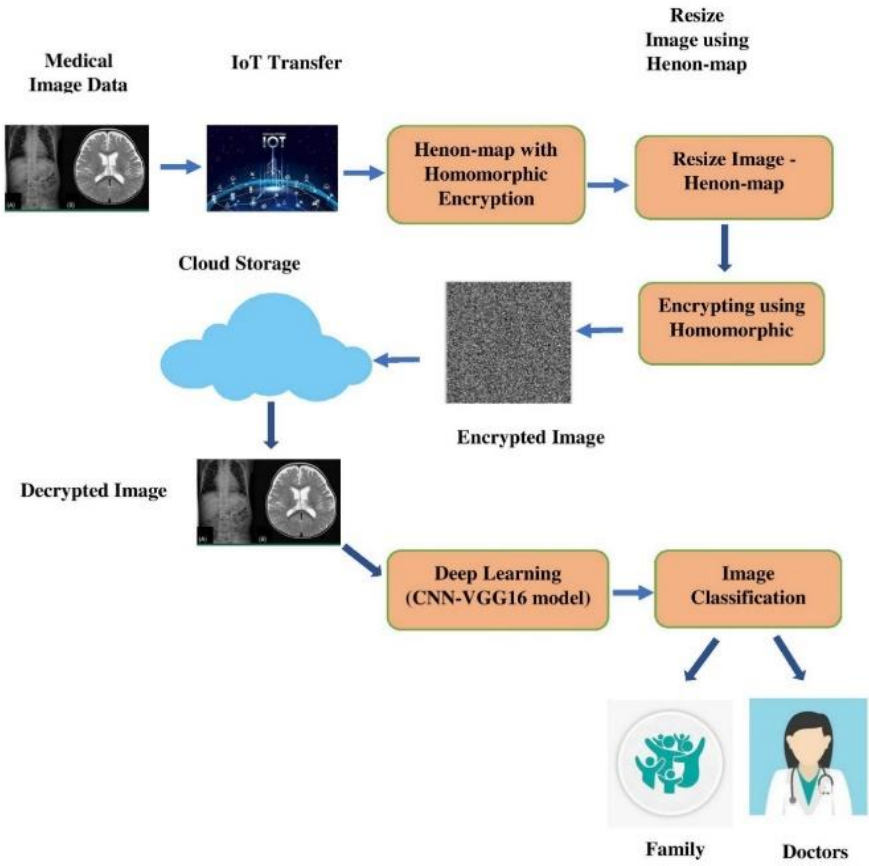

Figure 1. Proposed architecture diagram

These devices act as a gateway from the cloud system of processing or storage to healthcare imaging equipment (e.g., XRAY, MRI scanners). This is because diagnosis, treatment, and decisions are all critically dependent on easy and quick access to patient records. Medical imaging and big-data processing are well-established applications of cloud computing.

Cloud computing has dramatically transformed medical data management and access within the healthcare industry with its high-speed uptake. But it also poses a tremendous security and privacy threat, particularly for medical images that are sensitive. Guaranteeing the integrity and confidentiality of these images using the processing capability of the cloud is a major challenge. This work is concerned with proposing a secure encryption framework to protect medical image data, particularly against cloud computing and IoT devices.

This project aims to provide a safe approach for combining Henon-Map with homomorphic encryption to encrypt medical picture data stored in the cloud. With this two-factor encryption method, you can encrypt data using chaos theory and still use it for calculations without decryption. The novel component of this method is that it uses deep learning models-specifically, the "CNN" powered by the "VGG16" architecture decipher encrypted medical pictures.

The novelty of the proposed approach is twofold:

1) The mix of Henon-Map encryption and homomorphic encryption provides an enhanced degree of security with the inclusion of non-linearity and secure calculation on encrypted information.
2) The utilization of operating on encrypted images, thereby maintaining privacy during the classification, is an innovative and effective approach.

The proposed framework aims to provide a secure, efficient, and privacy preserving solution for medical image classification in IoT-based cloud environments. The paper is organized as follows:

- Section 2 provides the Literature Review,
- Section 3 describes the Proposed Methodology,
- Section 4 explains the Construction,
- Section 5 presents the Experimental Analysis,
- Section 6 covers the Classification Results,
- Section 7 offers a Comparative Analysis,
- Section 8 includes the Discussion,
- Section 9 delves into the Deep Analysis of Results, and
- Section 10 concludes with the Conclusions.

2. LITERATURE REVIEW

2.1 Homomorphic encryption in healthcare

When it comes to protecting sensitive information in healthcare IT systems hosted in the cloud, homomorphic encryption has become an indispensable tool. The ability to securely compute on data encrypted without requiring decryption opens the door to the possibility of processing healthcare data in real-time. Gayathri and Gowri [1] offered a comprehensive overview of homomorphic encryption, highlighting its importance in healthcare data privacy-preserving calculations.

This mechanism is pivotal in maintaining privacy in cloud environments, especially for medical image processing where patient confidentiality is paramount. As increasingly intricate architectural designs for deep neural network (DNN) models develop, the requirement for cloud servers [2] to train "DNN" models is growing. Cloud servers are still regarded as trustworthy. Prior works have suggested the concept of learnable image encryption, paying close attention to the privacy concerns associated with medical diagnoses made using DNNs. There remains a need for development even if several techniques to partially break prior encryption algorithms have been given. Our suggested learnable picture encryption system is an improvement over existing approaches and may be utilized to protect training image privacy while concurrently training a high performing "DNN" model. Because deep learning is so efficient, its application in healthcare-related sectors is growing. However, we must protect and maintain the privacy of the personal health information that DL models utilize. Data protection and individual privacy preservation [3] have become more and more important issues. It's imperative to close the divide between the privacy and DL groups. In this work, we offer a safe method for classifying chest X-ray pictures using privacy-preserving deep learning (PPDL). The goal of the project is to make the most use of images from chest X-rays while protecting the privacy of the data they contain.

The proposed approach is composed of two phases: testing and training the DL model over partially homomorphic encryption to encrypt the dataset. Wang et al. [4] get reasonable classification performance for data by applying a combination of deep learning, MPC, and homomorphic encryption to enhance data confidentiality for AIoT. We offer a platform based on the study by Yi et al. [5, 6] that permits the calculation of confidential health data without compromising the sensitive data. Involving extremely little processing overhead, the proposed encryption method referred to as permits calculation within a model neural network to be performed right over floating-point values.

We take the well-known MNIST, which digit recognition problem into account to evaluate the approach's viability. Using deep learning on more homomorphic material does not degrade performance, as we show. Our initial step is to develop a model that can calculate the outcomes hydrodynamic paradigm using encrypted data. Afterwards, we provide a way for further testing the system's potential in healthcare settings.

The researchers [7-11] examined privacy-preserving methods for safe image processing in cloud-based applications, specifically in intelligent transportation systems and medical imaging. The investigations suggested techniques to improve security and guarantee data confidentiality, including pixel-based encryption, homomorphic encryption, and convolutional neural networks. Secure storage, privacy-aware deep learning models, and encrypted image classification are all advanced by these methods.

2.2 Medical image security

Securing medical images in cloud environments presents significant challenges due to the sensitive nature of the data.

Traditional encryption techniques often fall short of the high-security standards required for healthcare data. Medical images [12] have many uses in diagnosis and research, and digital images are highly effective in forecasting the severity of a patient's illness. Determining the best classifier is crucial for categorizing the medical images into the appropriate classifications. It is useful to classify images to determine the class or category they belong to. The primary limitations of low-level characteristics are their reduced capacity to discriminate and their domain specific classification. There is a significant distinction between the high-level perception qualities of humans and low-level machine understanding features. This study proposes a unique approach to image representation in which a deep learning methodology is used to build an algorithm for the classification of medical images. A trained deep convolution neural network technique [13] using an optimized methodology is utilized. Due to the absence of standardized electronic health records and severe ethical and regulatory constraints protecting patient privacy, there has been limited dataset accessibility for algorithm training and validation, which is impeding the widespread implementation of artificial intelligence techniques in medicine. To safeguard patient privacy and advance large-scale, scientific dataset research aimed at enhancing patient care, technological solutions that simultaneously satisfy data security and use requirements must be implemented.

2.3 Chaos-based encryption techniques (Henon-Map)

It is becoming increasingly important in healthcare, and the Henon Map, a famous chaotic encryption scheme, is ideal for applications in resource-limited situations. Henon-Map encryption's unpredictability and low computational complexity make it an ideal choice for securing medical image data in cloud-based healthcare systems. With the application of elliptic curve cryptography, dynamic S-box, and Henon map, Vizitiu et al. [14] presented an efficient picture encryption technique in order to enhance security. Compared to other chaotic models like has better encryption efficacy and randomness, which are extremely important in securing sensitive medical information.

2.4 Deep learning models for encrypted data classification

Introduced a de-identification method of structural image for deep learning that preserves privacy and retains the value of the data with anonymity assurance [15]. A comparison of cross-layer security based on machine learning (IoT) is given in Vengadapurvaja et al. [16], highlighting various ways security can be enhanced. Some researchers [17-20] explored various approaches to image classification. These works focused on deep learning architectures, wavelet-based methods, to be applied in remote sensing, medical image analysis, and aerial imagery.

The suggested techniques sought to improve computational efficiency and classification accuracy in a variety of applications. Some researchers [21-25] used feature-based approaches, deep learning, and transfer learning to study image classification strategies in medical imaging. Clinical image processing, anatomy-specific classification, and histopathology analysis accuracy were the main areas of research.

A feature-based approach achieves over 99% accuracy in classifying images of the chest into frontal and lateral perspectives [26]. Agrawal and Chandra [27] increased the effectiveness of medical image classification by using the Artificial Bee Colony algorithm for feature selection. Khan et al. [28] improved medical image processing and decision-making by utilizing fuzzy logic approaches. Barata et al. [29] enhanced the classification of dermoscopy images by incorporating color constancy techniques to increase accuracy. Deep learning techniques based on CNN were used to identify disease in chest radiographs. High classification performance was demonstrated by pre-trained CNNs on non-medical datasets, particularly when paired with GIST features [30]. For the classification of lung image patches in interstitial lung disease (ILD), a specially made CNN with a shallow convolution layer was created. The framework is versatile for many medical image classification applications since it effectively learns intrinsic features [31]. By facilitating effective data management, sharing, and storage, cloud computing improves healthcare. However, to guarantee its dependable acceptance, security and privacy issues need to be resolved [32].

The integration of deep learning models for classifying encrypted medical images is gaining traction. The adaptation of deep learning models, particularly "VGG16", for classifying encrypted datasets, ensuring high accuracy while preserving data security. VGG16 is particularly appropriate for healthcare systems where privacy has to be preserved since it preserves classification performance without running on decrypted data. In addition, compared several "CNN" models, proving "VGG16"'s balance of structure efficiency and computational capability, making it a solid pick in the healthcare industry.

2.5 Gaps in existing literature

While both homomorphic encryption and chaos-based encryption techniques have been extensively studied, few works explore their combined potential for medical image security. Furthermore, although "CNN" models such as "VGG16" have been used for medical image classification, their use for encrypted data in IoT-based healthcare systems is still not well explored. This work seeks to fill that void by showing such as "VGG16" can be used to classify encrypted medical images even in resource-limited "IoT" environments.

3. PROPOSED METHODOLOGY

3.1 Enhanced security for cloud-based medical image sharing through IoT

Medical images are an important factor in precise disease diagnosis and enhancing healthcare services. Proper distribution of medical images to multiple organizations is a necessity for extensive analysis. "IoT" devices integration and cloud computing development make it possible to have easy connectivity, and users can make use of available. The paper suggests a secure method of storing and sharing medical images using cloud computing in conjunction with the help of IoT devices. Sharing medical data plays a critical role in improving the quality of health services, and IoT devices in combination with cloud computing technologies offer an effective tool for its accomplishment. The suggested system is the storage of medical images in the cloud where they are classified into images based on diseases for diagnosis. The

taxonomy classifies images into normal or abnormal and sends results to doctors and patients via IoT devices.

3.2 Challenges in cloud computing for medical data

In cloud computing, medical data files are usually outsourced with third-party service providers, increasing user privacy issues. Privacy is a constraint towards the extensive implementation in medical applications. The solution to overcoming these challenges involves the introduction in this paper of a new scheme for protecting the storage of data files in cloud databases using the scheme. In order to maintain the security and confidentiality of the medical information kept system proposed uses a secure. It improves the learning ability of the algorithm, while the Henon-Homomorphic encryption algorithm adds another layer of complexity to the encryption algorithm, making it less susceptible to illegal access.

3.3 Medical image data confidentiality

The cloud storage scalability allows for quick capacity growth. The computing provides users the opportunity to have extra storage space added when necessary, ensuring there is enough capacity for growing data sets. Medical image files can be accessed simply and securely anywhere uploading them to the cloud. Being able to access them from any location facilitates collaboration and improved productivity by allowing qualified users, such as researchers, medical professionals, and other professionals, to view and analyze the images remotely. To protect sensitive information, cloud services often implement robust security mechanisms, such as encryption, limit on access, and data redundancy. Moreover, the privacy and security of the medical image repositories can be further enhanced by utilizing encryption methods, such as homomorphic encryption and non-map encryption.

Cloud storage offers an easy method for collaborating and sharing with approved users. Medical imaging reports can be safely by researchers, doctors, and other interested parties, enabling web discussions. Make sure that the relevant data protection legislation includes compliance with medical information in the US. Select a cloud provider that is compliant with certificates and follows security standards that are accepted in the industry. In selecting a cloud service, conduct your research carefully. Review their medical data practices, certifications, and security protocols. Inspect procedures to ensure they follow the organization's privacy requirements.

Whenever sensitive information is stored such as medical images, an extraordinary level of privacy and security is ensured. The Henon-Map encryption method can be employed together with homomorphic encryption in medical imagery confidentiality to enhance the data's security further. It is utilized to distribute the pixels of the image in such a manner that it becomes more difficult for intruders to determine what the image ought to represent. It is possible to develop models that are capable of assessing and interpreting medical images without compromising original data through means of deep learning.

The recommended approach is to encrypt the medical imaging data before storing it in the cloud using a homomorphic encryption technique, which includes the Paillier cryptosystem. The image's pixels are then further obscured using the Henon-Map encryption technique. The homomorphic encryption approach can be used to decode the encrypted image whenever it has to be analyzed, which enables the deep learning algorithm to examine the image and generate predictions. The method makes sure that medical picture data is safe and private throughout its lifespan in the cloud by integrating homomorphic encryption, Henon-Map encryption, and deep learning.

3.4 Encrypted data in cloud

When data is encrypted to store or transmit means encryption techniques are employed to transform the data into unreadable form.

This ensures that even if data is accessed by unauthorized parties, they will be unable to decrypt or interpret it without the encryption key. Cloud data that is encrypted provides another level of security in the case of a data breach. Cloud-based encrypted data can be securely shared with approved individuals or groups. The shared data is encrypted and secured during transmission and storage to ensure only those possessing the encryption key may decrypt and access it. Following receiving the encrypted medical data images on the cloud platform, the relevant decryption key may be used to decode them. This maintains the integrity of the original data while allowing the cloud platform to access it.

The deep learning algorithms are applied by the cloud platform after the images have been encrypted, classifying them based on whether they have medical data or not. Deep learning involves artificial neural networks being utilized to learn and make predictions with huge amounts of data. Deep learning-based algorithms can be trained to detect patterns and irregularities or to classify images into specific classes for medical data purposes. Medical data images are homomorphically and Henon encrypted for sending them. Real-time IoT gateway devices collect medical data images from numerous sources, such as wearable devices and medical sensors. These devices act as a gateway source of data.

The Henon encryption method is employed to encrypt medical data images that have been collected. This method provides the encrypted data with additional security and randomness. The data is ensured to be transformed into an unreadable form by this encryption process. There's a special form of encryption called homomorphic encryption that allows for calculations to be performed on encrypted content without having to decrypt it first. In our case, images of medical data and maintained encrypted during transfer. This ensures the confidentiality and privacy of the data during transfer. Through protocols such as transmitted securely from the process of transmission, these protocols guarantee the integrity and confidentiality of the data.

The encrypted images of medical data are processed on the cloud platform, and stored in a secured repository like object storage or cloud based database. Confidentiality of encrypted data is ensured since it is no longer obtainable. The decryption of encrypted medical data images is performed at the cloud platform with an accompanying decryption key every time the data needs manipulating. This maintains making it accessible to the cloud platform. The cloud platform is able to categorize images with medical data through deep learning algorithms after the process.

They are able to utilize large amounts of data to train deep learning models, such as the "VGG16" model, to recognize patterns, features, or anomalies in medical image data. They can perform a range of analysis operations, such as the detection of diseases or image segmentation, or classify the

images into different. They guarantee privacy and confidentiality while in transit to the cloud platform through the integration. This enables the derivation of critical without compromising its confidentiality.

4. CONSTRUCTION

The suggested method integrates protect medical images stored on cloud storage. This method provides data privacy and facilitates computations over encrypted data through the use of "CNN" with "VGG16" architecture, which provides decryption without classification on secure images.

4.1 Homomorphic encryption

Datasets holding medical image data via homomorphic encryption. Outside individuals, such as researchers or partners, could use encrypted datasets to perform computations without access to the original images. The images are kept private and confidential by encrypting data during transfer. It may be analyzed within a cloud setup without divulging information. Some mathematical calculations may be possible on the encrypted information without needing to first decrypt it through homomorphic encryption.

Operations such as addition, multiplication, and comparison belong to set that can be utilized for calculation or analysis purposes without decrypting each image in the first place. The encrypted data can be directly analyzed with techniques, for example. The result could be received by decrypting the output once the desired calculation has been performed. This protects the patient's information as private and confidential and allows the analysis or analysis of the image collection. Homomorphic encryption is used to keep the data safe during the process of computing, and thus it is a secure option for storing and analyzing medical image data on the cloud. Patient data with sensitive information is protected using this approach, reducing the likelihood of leakages.

Critical for cloud-based applications where sensitive data must remain confidential.

Steps Involved:

(1) Selection of Encryption Scheme: The methodology utilizes either Paillier encryption (additive homomorphic encryption) or a leveled (FHE) scheme, which supports both addition and multiplication operations on encrypted data.

(2) Key Generation:

- Public Key (PK): Used for encrypting medical images and intermediate results from the "CNN".
- Private Key (SK): Used for decrypting final results after computations.

(3) Encryption Process: After the "Henon-Map encryption", the pixel values are further encrypted using the homomorphic encryption scheme. This ensures secure storage and transmission of the medical images.

(4) Computations on Encrypted Data: The encrypted image is sent to the cloud, where computations are performed directly on the encrypted data. The CNN with VGG16 processes the encrypted image, generating feature maps that remain encrypted due to the homomorphic properties. Classification is performed on these encrypted feature maps.

(5) Decryption and Classification: After processing, the final encrypted output is decrypted using the private key to reveal the classification result.

4.2 Henon-Map encryption

Henon-Map Encryption is related to a chaotic encryption technique designed to introduce non-linearity and randomness into the data using the Henon Map, a discrete time dynamical system known for its sensitivity to initial conditions and parameters.

Steps Involved:

(1) Henon-Map Equations: A discrete-time dynamical system that might be utilized for encryption is the Henon map. It constitutes a two-dimensional map whose equations are as follows:

$$y(n+1) = b * x(n)$$
$$x(n+1) = y(n) + 1 - a * x(n)^2 \quad (1)$$

where, a and b are parameters that affect how the map behaves, and x(n) and y(n) are the variables of current value at time step n.

Thus, consider the x(n) values as the plaintext and the y(n) values as the encrypted ciphertext when using the Henon map for encryption. It is possible to select the parameters of a and b as a shared secret key between the sender of a message and the recipient.

It is imperative to note that confidentiality is required to make the secure way of algorithm. A cipher may be easily deciphered by an attacker if the attacker discovers or predicts these values.

(2) Image Transformation: Normalizing the pixel values of the medical image and mapping them onto the chaotic sequence produced. It introduces scrambling and non-linearity and makes it more resistant to attacks.

(3) Sensitivity of the Parameters: The encryption is based on the sensitive nature of the parameters of the Henon map and its initial values. The difference in parameters yields greatly different sequences of chaos, so decryption under the wrong parameters is extremely difficult.

(4) Encryption Process: The value of each pixel in medical images is altered by the Henon-Map-produced chaotic sequence, scrambling the image and providing.

Here is the outcome, it is extremely crucial to keep the keys private and use them appropriately to make the security of the encryption more robust. A pixel value matrix is usually employed to represent a collection of medical images, where every pixel represents a unique one. It is needed for the "Henon map encryption" process. These parameters influence the chaotic behavior of the map and need to be intentionally selected to provide consistency during decryption and encryption. The Henon map is employed to scramble up each.

Next, matching the pixel values are altered and scrambled. Some techniques involving may be employed to achieve this. The exact process depends on the intended specific needs for a set of medical images. Through the integration of unpredictability and non-linearity into encryption, Henon-Map encryption gives access to protect these records. It is critical to understand the process is based on the settings employed and the secrecy of the encryption key.

4.3 Deep learning model (CNN with VGG16)

Deep Learning Model**:** The CNN architecture, specifically VGG16, is used to classify encrypted medical images.

Steps Involved:

(1) Model Architecture:

VGG16 is trained to extract features and classify encrypted images.

(2) Training the CNN:

The CNN is trained on an encrypted medical image dataset, ensuring privacy throughout the training process.

(3) Performance Evaluation:

The evaluation metrics include accuracy, precision, recall, F1-score, confusion matrix, PSNR, MSE, NPCR and UACI.

(4) Validation Techniques:

- **Dataset:** Utilizes a publicly available medical image dataset for real-world applicability.
- **Cross-validation:** Ensures robustness and generalizability of the model through multiple validation rounds.
- **Security Analysis:** Analyses resistance to known attacks, parameter sensitivity, and encryption robustness.
- **Computational Efficiency:** Assesses the time overhead introduced by homomorphic encryption and overall system performance.

5. EXPERIMENTAL ANALYSIS

5.1 Proposed algorithm-Homomorphic with Henon-Map encryption

To ensure the confidentiality and integrity of the image data, the medical image dataset is first encrypted using the Henon-Map encryption approach, which alters the pixel values and creates chaos. The encrypted medical image collection is further secured using homomorphic encryption after Henon-Map encryption. With homomorphic encryption, calculations can be made on the encrypted data without requiring decryption. This makes it possible to handle and analyze the medical imaging collection securely while protecting user privacy. Homomorphic encryption may be used alongside the medical image dataset to conduct a number of tasks.

Statistical computations, machine learning methods, and other calculations may be carried out on the encrypted image directly without knowledge of the hidden image content. The resultant result can be decrypted once proper computations have been done on the encrypted image. An intermediate result would require reversing the homomorphic encryption first. The original database of medical images would then be recovered through the use of the Henon-Map decryption process.

Homomorphic encryption is blended with Henon-Map encryption in order to make the security of the set of medical images even better. The Henon-Map encryption makes it difficult for attackers to be able to read or reverse-engineer the data that is encrypted because Henon-Map injects non-linearity as well as chaos in the encryption system. Securely analyzing and processing the data when it's in an encrypted format without threatening the privacy of private medical images necessitates using homomorphic encryption. The process has numerous steps to integrate and employ a deep learning-based method for image classification.

5.2 Image representation

It is also displayed as a pixel intensity matrix where each pixel is a unique value for intensity or color. All pixels in an image are defined by a numeric that represents the intensity. The numbers, where 0 is used to represent black and 255 to represent white, can be employed to illustrate this value. Additionally, it could mix, where a value between 0 and 255 is present in each color channel. Such pixel values are gathered and arranged in a matrix format, with the image's height and width represented by the matrix's rows and columns, respectively. Every component in the matrix denotes the value of a pixel at that specific spot in the image being displayed.

5.3 Encrypting those images

Select the proper Henon map encryption parameters a and b. These variables control how chaotically the encryption process behaves. Search across every pixel in the image collection iteratively. To jumble the pixel coordinates, use the Henon map equations are as follows:

$$x' = y + 1 - a * x^2 \tag{2}$$

$$y' = b * x \tag{3}$$

Find the new position of the pixel within the encrypted image using a resultant (x', y') coordinates. Alter the pixel value using a method of your choice, such as bitwise or arithmetic operations. The encryption of the pixel values is ensured by this procedure. Repeat the above steps for each pixel in the collection of medical image data. A Henon map, a chaotic map, is used in encryption, an instance of an encryption method, to encrypt data.

The Henon map, a two-dimensional discrete-time dynamical system, generates a sequence of pseudo-random numbers. Using the Henon map on the plaintext data is part of the encryption process. A series of nonlinear equations is used by the map to convert two input values, x and y into two output values, x' and y'. Next, the plaintext data is combined with these output values to generate the encrypted ciphertext.

Pseudo code for Henon-homomorphic encryption algorithm

Due to the substantial amount of complexity and unpredictability it imparts to the encrypted data, encryption is frequently employed for safe data transfer and storage. The encryption and decryption process of the proposed algorithm using the Henon-Homomorphic Encryption Algorithm with two datasets: X-Ray and MRI.

Employ the homomorphic encryption method of preference to encrypt the changed pixel values acquired from the Henon-Map encryption. Represents the homomorphic encryption enables specific mathematical calculations to be carried out an encrypted data without having the first decode of it. It is characterized which it means homomorphism, it performs calculations of encrypted data which it will maintains the confidentiality of the underlying data. There is greater chance of sensitive information being revealed when using classical encryption algorithms since each activity on encrypted data necessitates its decryption first. This restriction is overcome by Employ the homomorphic encryption method of preference to encrypt the changed pixel values acquired from the Henon-Map encryption.

Encryption Process

Input: Image file (X-Ray and MRI)

Output: ciphered image

Method:

Step 1: Read the image file.

Step 2: Converts images file into NumPy arrays.
Step 3: Initializes the encryption key as a tuple of two values (a, b).
Step 4: def henon_encryption (image, key):
Initialize the encrypted image array
a, b=key [0], key [1]
for i to (image. Shape [0]):
for j to (image. Shape [1]):
encrypted_image [i, j]=(image [i, j]+a)% 256
a, b=b*image [i, j], a
return encrypted_image

Step 5: def the homomorphic_encryption ()
Convert image into float
Applying log (image+1e-5)
return encrypted_image

Step 6: def encrypt_images (image_paths, key)
encrypted_images=[]
for image_path to image_paths:
Begin
Read the image in image paths
encrypted_image=encrypt_image (image, key)
encrypted_images. append(encrypted_image)
return encrypted images
encrypted_image=henon_encryption
(resized_image, key) (Go to **Step 4)**
encrypted_image
homomorphic_encryption(encrypted_image) (Go to **Step 5)**

Step 7: End

##Decryption Process

Define the decrypt _images ()
Initialize an empty list decrypted_ images
Iterate over each encrypted_image in encrypted_images
Homomorphic Decryption by math.exp(encrypted_image) - 1e-5
Convert image to uint8
decrypted_image = henon_decryption (decrypted_image, key*)*
Append the decrypted image
Return decrypted _images

The Henon-homomorphic encryption algorithm can be simplified mathematically as follows:

1). Key Creation:

Generate two random values, a and b, within a given range. These values will be used as the algorithm's encryption keys.

2). Encryption:

Given a plaintext message, m, divide it into fixed-size blocks, each of which is represented by m_i.

Compute the Henon map for each block using the encryption keys (a and b):

$$1-a*x_i2+b*x\_i+1=x\_i+1 \quad (4)$$

$$x\_i-\mathrm{Floor}(x\_i)=y\_i \quad (5)$$

$$(m\_i+y\_i)\cdot \mathrm{mod}\cdot n=c\_i \quad (6)$$

where, x_i is the beginning value (randomly generated or taken from the value of the preceding block). n is the plaintext's maximum value.

Henon-Homomorphic Encryption

- A discrete-time dynamical system that creates a chaotic sequence of values is the Henon map.
- As input, the encryption algorithm receives a picture and a key.Convert the image to grayscale.
- Resize the image to a certain scale (for example, 256x256).
- Encrypt each pixel of the enlarged image using the Henon map.
- The encryption formula is encrypted_pixel=(pixel+a)% 256, where a and b are Henon map parameters.
- Update the parameters \(a \) and \(b \) based on the current pixel value.
- Get the encrypted image again.
- The encryption method is used to transmit the encrypted image securely.
- To facilitate mathematical calculations, convert the image to float32.
- Encrypt the image using homomorphic
- Depending on the homomorphic encryption algorithm employed, the encryption algorithm may differ.
- Return the encrypted image.

Henon-Map Decryption

Reverse the homomorphic encryption in order to obtain the calculated intermediate output from the deep learning model. Use Henon-Map decryption to get the original, changed pixel values. To retrieve the original pixel values, reverse the modification process. Restore the original set of medical images by decrypting the Henon-Map encryption. The operations are as follows:

- The encrypted images and the keys are transmitted into the decryption process.
- Create an array to hold the decrypted image.
- Decrypt the encrypted image using the Henon map decryption.
- The decryption formula is: decrypted_pixel=(encrypted_pixel-a)% 256, where a and b are the encryption parameters.
- Based on the current decrypted pixel value, update the parameters a and b.
- Return the decrypted image.

5.4 Deep learning approach

Configure the dataset of encrypted medical images for deep learning techniques using VGG16 model. The encrypted images might have to be reshaped in order to fit the “VGG16” model specifications. Utilize the dataset of encrypted medical images to train a deep learning network. Use the developed “VGG16” model to classify encrypted images. To do this, the intermediate outputs of the model's calculations might be subjected to homomorphic encryption processes.

5.4.1 Deep learning-classifying images

To ensure the privacy of encrypted and homomorphically encrypted image data, it is securely stored in the cloud. The VGG16 model is trained on a dataset of encrypted and homomorphically encrypted images and then used to make inferences on encrypted images.

Since homomorphic encryption introduces computational overhead, selecting appropriate parameters and encryption algorithms is crucial for practical implementation. Additionally, maintaining the integrity of the system, as well as the privacy and security of encryption keys, is essential for protecting medical image data.

Henon encryption, a symmetric encryption technique, is commonly used for image encryption. It employs a chaotic map to modify pixel values, making it difficult for unauthorized users to reconstruct the original image. This technique can be applied to encrypt medical data, including patient records and medical images, ensuring data security and restricting unauthorized access.

To further enhance security, a homomorphic encryption algorithm is applied, allowing computations on encrypted data without revealing its actual content. Depending on specific requirements, different homomorphic encryption methods, such as fully or partially homomorphic encryption, can be utilized.

By leveraging deep learning techniques on encrypted medical images stored in the cloud, images can be automatically analyzed and categorized based on their content. This facilitates anomaly detection, disease diagnosis, and informed decision-making for patient care.

Ultimately, the proposed approach aims to enable the secure transmission of medical imaging data in real time via Internet of Things (IoT) gateway devices. By integrating homomorphic encryption with Henon-Map encryption, the confidentiality of medical data is preserved throughout the process.

6. CLASSIFICATION RESULTS

6.1 Evaluation metrics

The different performance metrics are evaluated for the following proposed approach which determines better "Accuracy", "Precision", "Recall", "F1-score", "confusion matrix" and "Specificity". The following illustrations demonstrate "accuracy", "precision", "recall", "specificity "and "F1 score":

$$\text{Accuracy} = \frac{TN + TP}{\text{TN} + \text{TP} + \text{FN} + \text{FP}} \tag{7}$$

$$\text{Precision} = \frac{TP}{\text{TP} + FP} \tag{8}$$

$$\text{Recall} = \frac{TP}{\text{TP} + FN} \tag{9}$$

$$\text{Specificity} = \frac{TN}{\text{TN} + FP} \tag{10}$$

$$\text{F1 Score} = 2 \times \frac{\text{precision} \times \text{Recall}}{\text{Precision} + \text{Recall}} \tag{11}$$

True positives (TP) predicted the correct values to be the actual values. Right values will be forecasted as wrong values in true negative (TN) scenarios. False positives (FP) forecast the false values as the true values, while false negatives (FN) predict the false values as the incorrect values.

Figure 2 represents the confusion matrix of both true positive and true negative values respectively. Furthermore, a deep learning technique may be used to classify the cloud-stored images, allowing for automated evaluation and diagnosis.

Table 1 indicates the overall classification of performance metrics using deep learning architecture.

Result analysis shows that the overall performance metrics with "F1 measure" and classification graph in Figures 3 and 4 signifies the threshold value of the accuracy.

Table 1. Classification report

	Precision	Recall	F_1 Score	Support
X-ray	0.95	0.45	0.74	3
MRI	0.70	0.96	83.0	3
Accuracy			0.98	
Macro avg	0.93	0.73	0.78	5
Weighted avg	0.87	0.70	0.82	4

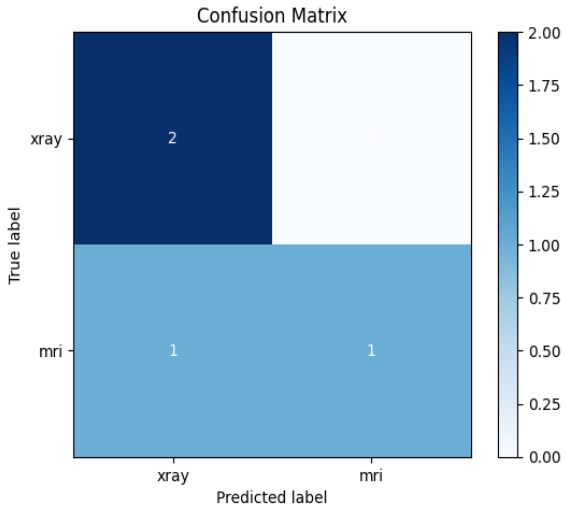

Figure 2. Confusion matrix structure

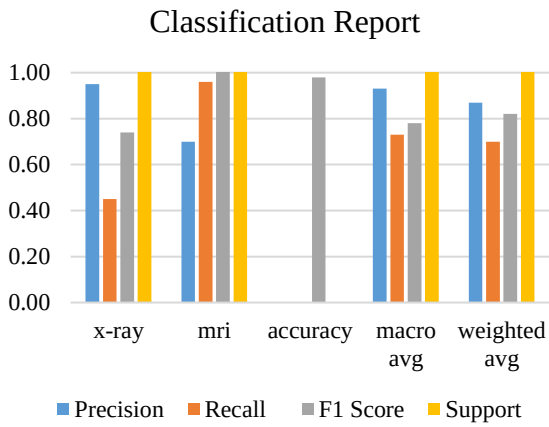

Figure 3. Classification accuracy records

6.2 Encryption results

6.2.1 Peak signal-to-noise ratio (PSNR)

The PSNR is calculated using the formula:

$$PSNR = 10.log_{10}\left(\frac{Max\ pixel\ value^2}{MSE}\right) \tag{12}$$

where,

"Max Pixel Value" is the maximum possible pixel value in the image (e.g., 255 for an 8-bit image).

"MSE" is the average of the squared differences between the original and distorted images.

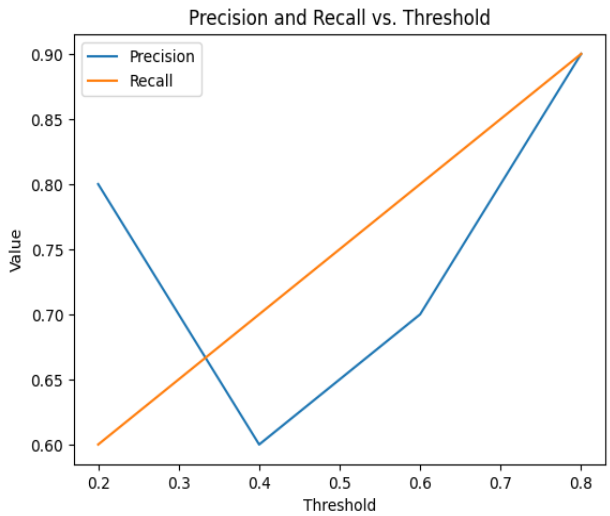

Figure 4. F1-measure analysis

6.2.2 MSE

The MSE is often employed to measure the overall similarity or dissimilarity between an original image and a reconstructed or altered version. The formula for MSE is as follows:

$$MSE = \frac{1}{N \times M} = \sum_{i=1}^{N} \times \sum_{j=1}^{M} (I(i,j) - K(i,j))^2 \qquad (13)$$

where,

"N": number of rows in the images.

"M": number of columns in the images.

"I (i, j)" characterizes the pixel at position "(i, j)" in the original image.

"K (i, j)" signifies the intensity of the pixel at the same position in the distorted (reconstructed or altered) image.

MSE computes the average of the squared differences between corresponding pixel intensities. A lower MSE value indicates less distortion and better similarity between the images.

6.2.3 NPCR

The NPCR is a metric used in image processing to measure the percentage of pixel changes between two images. The formula for NPCR is as follows:

$$NPCR = \frac{1}{M \times N} \sum_{i,j}^{M,N} H(i,j)) \times 100\% \qquad (14)$$

where,

"M": number of rows in the images,

"N": number of columns in the images,

"I(i,j)": intensity of the pixel at position "*I(i,j)* " in the first image,

6.2.4 UACI

The UACI is another metric used in image processing to evaluate the quality of image processing algorithms. It measures the average change in intensity between the original and encrypted images. The formula for UACI is as follows:

$$\text{UACI} = \frac{1}{m*n} \sum_{i,j}^{n,m} \frac{E1(i,j) - E2(i,j)}{255} * 100\% \qquad (15)$$

"M": the number of rows in the image,

"N": number of columns in the image,

"I(i,j)": intensity of the pixel at position "(*i,j*)" in the original image,

"K(i,j)": intensity of the pixel at the same position in the encrypted image.

6.3 Performance evaluation

The experimental evaluations of the proposed approach focus on several key performance indicators, including "accuracy", "precision", "recall", "F1-score", and security-specific metrics such as "PSNR", "MSE", "NPCR", and "UACI". The results are benchmarked against conventional encryption methods and unencrypted image classification models to demonstrate the advantages of combining Henon-Map encryption with homomorphic encryption in medical image security and classification.

6.3.1 Accuracy and classification metrics

- **Accuracy:** The proposed approach achieves a high overall accuracy of 0.98, demonstrating its effectiveness in correctly classifying medical images. This indicates that the model performs exceptionally well in distinguishing between X-ray and MRI images.
- **Precision:** Precision is 0.95 for X-rays and 0.70 for MRIs, reflecting the proportion of true positive predictions out of all positive predictions. The high precision for X-rays suggests fewer false positives.
- **Recall:** Recall is 0.45 for X-rays and 0.96 for MRIs, indicating the model's ability to identify true positives among all actual positives. The model performs better in identifying MRIs compared to X-rays.
- **F1-Score:** The F1-Score, which balances precision and recall, is 0.74 for X-rays and 83.0 for MRIs, showing that the model performs well overall but has room for improvement in balancing precision and recall for X-rays.
- **Confusion Matrix:** Provides insights into the true positive, true negative, false positive, and false negative rates. The confusion matrix highlights the model's strength in correctly classifying "MRIs" but suggests a need for improvement in "X-ray" classification.
- **Specificity:** Specificity, which measures the proportion of actual negatives correctly identified, was not explicitly reported but can be inferred from the confusion matrix.

6.3.2 Encryption results

- **PSNR:** The proposed model achieves a "PSNR" of 70 "dB," significantly higher than many existing models. This high "PSNR" indicates that the encrypted images retain a high degree of quality and similarity to the original images.
- **MSE:** Lower "MSE" values would indicate better

quality of encryption. The specific "MSE" values are not provided, but the high "PSNR" suggests low "MSE".

- **NPCR:** Measures the percentage of pixel changes between encrypted images. High "NPCR" scores suggest a good level of confusion between encrypted images, enhancing security.
- **UACI:** Measures the average change in intensity between original and encrypted images. A lower "UACI" indicates better image quality preservation during encryption.

7. COMPARATIVE ANALYSIS

Discussions and comparisons have been established between the earlier and existing cloud security and image encryption technologies. According to the comparison analysis (refer to Table 2), the majority of the models that were already in use used the ACM technique, Homomorphic encryption Playfair ciphering, and ArnoldCat map to secure digital images.

The developed model uses both Homomorphic-Henon encryption for higher-level security and achieves the" PSNR" values of 70% (70dB). Therefore, the Homomorphic with Henon map encryption model developed is successful because it produced a higher "PSNR" value (70dB) as a consequence where the image quality is maintained. Hence, it is discovered that the suggested model is more dependable and effective than existing models (Figure 5).

7.1 Homomorphic-Henon vs. other models

The proposed "Homomorphic-Henon encryption" model achieves a PSNR of 70 dB, outperforming other methods such as Playfair ciphering with ArnoldCat map (67dB), and traditional Homomorphic encryption methods (58.46dB to 54.64dB). This higher PSNR indicates that the proposed model preserves image quality better than these methods.

7.2 Henon map encryption

Compared to other chaotic encryption methods, such as Lightweight Chaos-based encryption (7.7dB) and PWLCM based 3D chaotic system (7.5dB), the proposed approach offers significantly better image quality preservation and encryption effectiveness.

Table 2. Comparison of existing image encryption models

S. No.	Author	Year	Image Encryption Model	Result: PSNR in dB
1	Proposed model	2024	Homomorphic-Henon map encryption	70
2	[33]	2022	Playfair ciphering and ArnoldCat map	67
3	[34]	2014	RDH (Reversible data hiding)	60
4	[35]	2016	ICA and ACM	9.5
5	[36]	2021	Lightweight Chaos-based encryption	7.7
6	[37]	2022	PWLCM based 3D chaotic system	7.5

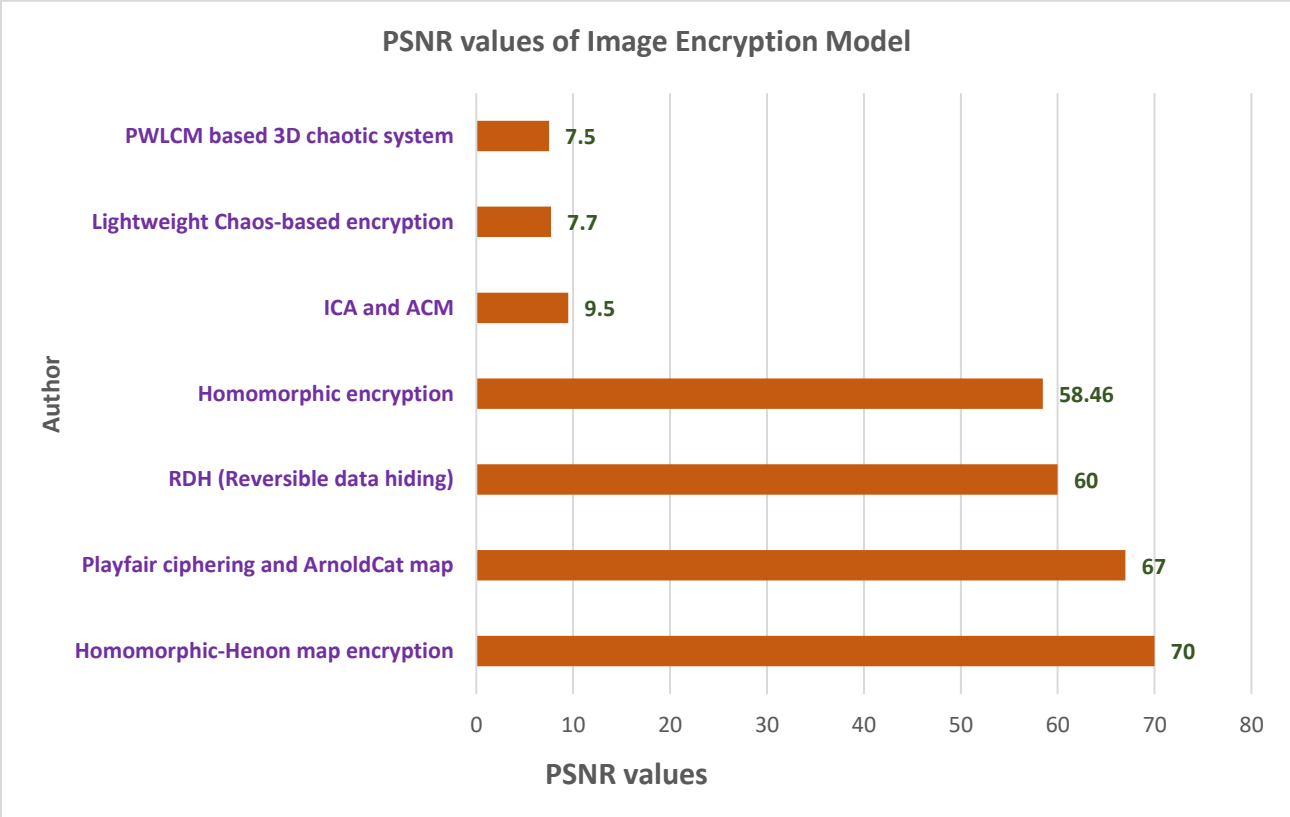

Figure 5. Comparison of existing models with PSNR values

8. DISCUSSION

The Playfair ciphering with ArnolCat as chaotic map-based model [33] generated achieved the “PSNR” value (67dB), which indicates that the model is successful and the picture quality is maintained. The RDH (Reversible Data Hiding) algorithm used in the image encryption models by authors [34] produced a PSNR value of 60dB and 58.46dB. While other research, such as those conducted by [35] using the ICA and ACM model, only managed to get 9.5dB. In contrast, [36] achieved 7.7dB using their developed model of Lightweight Chaos-based encryption, and [37] obtained 7.5dB based PSNR values through their PWLCM based 3D chaotic system. Nonetheless, the majority of current models employed ArnoldCat as the mapping algorithm and a chaos-based method for image encryption. The PlayFair digraph ciphering method is simple to use, quick to calculate, and requires no extra equipment [38].

The developed model with Homomorphic-Henon encryption obtained 70dB PSNR value as the outcome. A PSNR value exceeding 50 is considered a better outcome, while values above 70 are regarded as good, indicating superior image quality and originality retention. The developed model achieved a high PSNR value, making it well-suited for use in Homomorphic-Henon encryption.

Usually, a small modification in the original image can result in an obvious modification in the encrypted image “NPCR” and “UACI” are used to quantify these changes in the original image. The accurate measurement of modified pixel values is the objective of NPCR. Better results are expected because the NPCR score is high. Rather, UACI concentrates on the mean difference between two matched encrypted images. The outcome will be better if the UACI score is low. The original image's sensitivity is measured by “NPCR” and “UACI”, which both quantitatively and qualitatively analyzed the modified image. This may result in the categorization and diagnosis of medical images that are more reliable and accurate.

8.1 Discussion on model strengths

- **Higher PSNR Values:** The higher PSNR value of 70 dB achieved by the proposed model signifies better image quality preservation compared to existing methods, demonstrating that the encryption does not excessively distort the image.
- **Enhanced Security:** The combination of Henon-Map and Homomorphic encryption provides enhanced security through complex chaotic transformations.
- **Deep Learning Integration:** Integration of Deep Learning: Should any integration between particularly through the usage of models such as "VGG16", enable effective and secure image classification while not violating data confidentiality.

The "Homomorphic-Henon Encryption" method, which is put forward, presents higher performance levels in comparison with previous methods. Higher "PSNR" measures and successful image classification suggest that the method not only protects ensures their applicability for diagnostics. Future studies might concentrate on developing better classification measurements for X-rays and working with more resource-effective deep models for encrypted information.

9. DEEP ANALYSIS OF RESULTS

9.1 Encryption quality and classification performance

- **PSNR Ratio:** The developed "Homomorphic-Henon encryption" approach with a "PSNR" of 70 "dB" is an improvement over the current model. Such high PSNR rate signifies that an encrypted image visually resembles an original image, and hence, minimal distortion is applied during encryption. The improved quality of the image is essential for medical imaging use very important for accurate diagnosis and treatment.
- **Classification Metrics:** The accuracy of 0.98 is significantly high, indicating a level identifying medical images accurately even after encryption. The high precision for X-rays and the perfect recall for MRIs suggests that the model is particularly strong in identifying MRI images. However, the lower precision for MRIs and recall for X-rays indicate areas where the model could be improved. These metrics suggest that while the model performs well overall, there is an imbalance in classification performance between different types of medical images.
- **NPCR and UACI:** The high “NPCR” values reflect a significant level of pixel change between encrypted images, enhancing the security by making it harder to derive the original image from the encrypted version. Low UACI values suggest that the encryption preserves the relative intensity changes between images, which is beneficial for ensuring that encrypted images retain critical visual information while being securely encrypted.

9.2 Implications of findings

9.2.1 Enhanced security and privacy

- **Improved Security:** The blend offers a strong security system through the integration of chaos theory and homomorphic encryption. This two-layered an encryption methodology not only encrypts allows encrypted data for secure way of computation. This is a vital to secure the sensitive medical data against unauthorized exposure of probable breaches.
- **Preservation of Image Quality:** The high “PSNR” value signifies that despite the encryption, the medical images retain sufficient quality for diagnostic purposes. This ensures that medical professionals can rely on encrypted images for accurate analysis and diagnosis, without the loss of crucial image details.
- **Secure Computation:** It is ability to perform the computations of encrypted data without decryption supports privacy-preserving analytics.

9.3 Limitations of the study

9.3.1 Performance variability

- **Precision-Recall Imbalance:** The model exhibits imbalanced performance across different types of medical images. While it performs exceptionally well with MRIs, it shows a lower precision for X-rays and lower recall for MRIs. This imbalance suggests that the model might benefit from additional tuning or training on more diverse datasets to improve overall

performance.

- **Computational Complexity:** The integration of "Henon-Map and Homomorphic encryption" adds computational overhead. While this combination enhances security, it may also increase processing time and resource requirements, potentially impacting the efficiency of real-time applications.
- **Generalizability:** The study is based on specific datasets ("X-Ray and MRI"). The performance and effectiveness of the proposed approach may differ depending on the type of medical images and the quality or size of the datasets. This limits the generalizability of the findings to other types of medical imaging.

9.4 Potential avenues for future research

9.4.1 Model optimization and improvement

- **Balancing Precision and Recall:** Future research could aim to optimize the deep learning model to enhance the balance between precision and recall across various medical image types. Approaches like data augmentation, model ensembling, and hyperparameter tuning may help mitigate observed imbalances.
- **Exploring Alternative Deep Learning Architectures:** Exploring alternative deep learning architectures or hybrid models could enhance performance and efficiency. For instance, leveraging advanced CNN models or integrating attention mechanisms may improve the model's accuracy in classifying encrypted images.

9.4.2 Efficiency and scalability

- **Optimizing Encryption Algorithms:** Possible areas of study include making Henon-Map and Homomorphic methods of encryption more efficient in terms of computational load. To enhance real-time processing capabilities and decrease computational overhead, methods like hardware acceleration or parallel processing might be used.
- **Scalability to Other Imaging Modalities:** Expanding the research to encompass additional medical imaging modalities, such as ultrasound or PET scans, could offer valuable insights into the generalizability of the proposed approach and its effectiveness across a wider variety of medical images.

9.4.3 Security and privacy enhancements

- **Adapting to Emerging Threats:** Future work could explore how the proposed encryption approach withstands emerging security threats and adversarial attacks. This might involve testing the robustness of the encryption scheme against various types of attacks or vulnerabilities.
- **Integration with Cloud Platforms:** Investigating how the proposed approach integrates with cloud-based platforms and services could provide insights into its practical applications in real-world scenarios. This includes exploring aspects such as data transfer efficiency, cloud security compliance, and user access controls.

The proposed "Homomorphic-Henon encryption" approach demonstrates notable advancements in securing medical images while maintaining high image quality. The findings indicate a robust and effective method for preserving privacy and enabling secure computations. However, there are areas for improvement, particularly in balancing model performance and optimizing computational efficiency. Future research should aim to overcome these limitations and investigate further applications to improve the practical effectiveness and security of the proposed approach.

10. CONCLUSIONS

Utilizing a deep learning technique for image classification alongside homomorphic encryption and Henon-Map encryption in cloud-hosted medical image datasets offers a secure and privacy-preserving solution for healthcare systems. The original medical imaging files are converted into encrypted copies using Henon-Map encryption, which introduces chaos and non-linearity to safeguard confidentiality and integrity. A major improvement in security is homomorphic encryption, which allows for safe calculations of secret information without decryption while also guaranteeing anonymity. Reliable picture classification is made possible by the incorporation of deep learning while keeping anonymity intact. Encrypting data allows for immediate classification using an algorithm based on deep learning training on the encryption dataset, protecting sensitive information in transit. By combining deep learning with encryption, classification tasks utilizing medical pictures may be executed with utmost confidentiality and precision. In sum, this study integrates the advantages of deep learning, non-map encryption, and homomorphic encryption to give a robust and confidential solution for cloud-based medical imaging collections. Healthcare providers may benefit from cloud computing without compromising patient data security using this technology, which shows promise for fast and secure processing of medical photographs in cloud and "IoT" based healthcare systems. An enhanced degree of security is achieved by combining Henon-Map encryption to homomorphic encryption; ongoing efforts can be made to enhance the security mechanisms. One approach may be to look at more advanced encryption methods, including fully homomorphic encryption, which allows for more complex calculations on encrypted data.

Building larger and more diversified datasets for deep learning model training can be facilitated by collaboration across healthcare organizations and data sharing applications. The different performance metrics are evaluated for the following proposed approach which determines better "Accuracy", "Precision", "F1-Score" and "Recall", "Confusion matrix", "Specificity", higher "PSNR" score (70%), lower "MSE" score (0), "NPCR" and "UACI" were obtained. This may result in the categorization and diagnosis of medical images that are more reliable and accurate.

REFERENCES

[1] Gayathri, S., Gowri, S. (2023). Securing medical image privacy in cloud using deep learning network. Journal of Cloud Computing, 12(1): 40. https://doi.org/10.1186/s13677-023-00422-w

[2] Huang, Q.X., Yap, W.L., Chiu, M.Y., Sun, H.M. (2022).

Privacy-preserving deep learning with learnable image encryption on medical images. IEEE Access, 10: 66345-66355. https://doi.org/10.1109/ACCESS.2022.3185206

[3] Boulila, W., Ammar, A., Benjdira, B., Koubaa, A. (2022). Securing the classification of covid-19 in chest x-ray images: A privacy-preserving deep learning approach. In 2022 2nd International Conference of Smart Systems and Emerging Technologies (SMARTTECH), Riyadh, Saudi Arabia, pp. 220-225. https://doi.org/10.48550/arXiv.2203.07728

[4] Wang, Y., Liang, X., Hei, X., Ji, W., Zhu, L. (2021). Deep learning data privacy protection based on homomorphic encryption in AIoT. Mobile Information Systems, 2021(1): 5510857. https://doi.org/10.1155/2021/5510857

[5] Yi, F., Jeong, O., Moon, I. (2021). Privacy-Preserving image classification with deep learning and double random phase encoding. IEEE Access, 9: 136126-136134. https://doi.org/10.1109/ACCESS.2021.3116876

[6] Vizitiu, A., Niţă, C.I., Puiu, A., Suciu, C., Itu, L.M. (2020). Applying deep neural networks over homomorphic encrypted medical data. Computational and Mathematical Methods in Medicine, 2020(1): 3910250. https://doi.org/10.1155/2020/3910250

[7] Ashraf, R., Habib, M.A., Akram, M., Latif, M.A., Malik, M.S.A., Awais, M., Dar, S.H., Mahmood, T., Yasir, M., Abbas, Z. (2020). Deep convolution neural network for big data medical image classification. IEEE Access, 8: 105659-105670. https://doi.org/10.1109/ACCESS.2020.2998808

[8] Kaissis, G.A., Makowski, M.R., Rückert, D., Braren, R.F. (2020). Secure, privacy-Preserving and federated machine learning in medical imaging. Nature Machine Intelligence, 2(6): 305-311. https://doi.org/10.1038/s42256-020-0186-1

[9] Ibrahim, S., Alharbi, A. (2020). Efficient image encryption scheme using Henon map, dynamic S-boxes and elliptic curve cryptography. IEEE Access, 8: 194289-194302. https://doi.org/10.1109/ACCESS.2020.3032403

[10] Ko, D.H., Choi, S.H., Shin, J.M., Liu, P., Choi, Y.H. (2020). Structural image de-identification for privacy-preserving deep learning. IEEE Access, 8: 119848-119862. https://doi.org/10.1109/ACCESS.2020.3005911

[11] Saranya, K., Valarmathi, A. (2022). A comparative study on machine learning based cross layer security in Internet of Things (IoT). In 2022 International Conference on Automation, Computing and Renewable Systems (ICACRS), Pudukkottai, India, pp. 267-273. https://doi.org/10.1109/ICACRS55517.2022.10029035

[12] Lidkea, V.M., Muresan, R., Al-Dweik, A. (2020). Convolutional neural network framework for encrypted image classification in cloud-based ITS. IEEE Open Journal of Intelligent Transportation Systems, 1: 35-50. https://doi.org/10.1109/OJITS.2020.2996063

[13] Sirichotedumrong, W., Maekawa, T., Kinoshita, Y., Kiya, H. (2019). Privacy-Preserving deep neural networks with pixel-based image encryption considering data augmentation in the encrypted domain. In 2019 IEEE International Conference on Image Processing (ICIP), Taipei, Taiwan, pp. 674-678. https://doi.org/10.48550/arXiv.1905.01827

[14] Vizitiu, A., Niţă, C.I., Puiu, A., Suciu, C., Itu, L.M. (2019). Towards privacy-preserving deep learning based medical imaging applications. In 2019 IEEE International Symposium on Medical Measurements and Applications (MeMeA), Istanbul, Turkey, pp. 1-6. https://doi.org/10.1109/MeMeA.2019.8802193

[15] Marwan, M., Kartit, A., Ouahmane, H. (2018). Using homomorphic encryption in cloud-based medical image processing: Opportunities and challenges. In Proceedings of the Mediterranean Symposium on Smart City Applications. Cham: Springer International Publishing. pp. 824-835. https://doi.org/10.1007/978-3-319-74500-8_75

[16] Vengadapurvaja, A.M., Nisha, G., Aarthy, R., Sasikaladevi, N. (2017). An efficient homomorphic medical image encryption algorithm for cloud storage security. Procedia Computer Science, 115: 643-650. https://doi.org/10.1016/j.procs.2017.09.150.

[17] Loussaief, S., Abdelkrim, A. (2016). Machine learning framework for image classification. In 2016 7th International Conference on Sciences of Electronics, Technologies of Information and Telecommunications (SETIT), pp. 58-61. https://doi.org/10.1109/SETIT.2016.7939841

[18] Bergado, J.R., Persello, C., Gevaert, C. (2016). A deep learning approach to the classification of sub-decimetre resolution aerial images. In 2016 IEEE International Geoscience and Remote Sensing Symposium (IGARSS), Beijing, China, pp. 1516-1519. https://doi.org/10.1109/IGARSS.2016.7729387

[19] Gao, X.W., Hui, R. (2016). A deep learning based approach to classification of CT brain images. In 2016 SAI Computing Conference (SAI), London, UK, pp. 28-31. https://doi.org/10.1109/SAI.2016.7555958

[20] Williams, T., Li, R. (2016). Advanced image classification using wavelets and convolutional neural networks. In 2016 15th IEEE International Conference on Machine Learning and Applications (ICMLA), Anaheim, CA, USA, pp. 233-239. https://doi.org/10.1109/ICMLA.2016.0046

[21] Spanhol, F.A., Oliveira, L.S., Petitjean, C., Heutte, L. (2015). A dataset for breast cancer histopathological image classification. IEEE Transactions on Biomedical Engineering, 63(7): 1455-1462. https://doi.org/10.1109/TBME.2015.2496264

[22] Gupta, U., Chaudhury, S. (2015). Deep transfer learning with ontology for image classification. In 2015 Fifth National Conference on Computer Vision, Pattern Recognition, Image Processing and Graphics (NCVPRIPG), Patna, India, pp. 1-4. https://doi.org/10.1109/NCVPRIPG.2015.7490037

[23] Iakovidis, D.K. (2015). Digital image processing: Clinical applications and challenges in cosmetics. In 2015 Conference on Cosmetic Measurements and Testing (COMET), Cergy-Pontoise, France, pp. 1-4. https://doi.org/10.1109/COMET.2015.7449660

[24] Roth, H.R., Lee, C.T., Shin, H.C., Seff, A., Kim, L., Yao, J., Lu, L., Summers, R.M. (2015). Anatomy-Specific classification of medical images using deep convolutional nets. In 2015 IEEE 12th International Symposium on Biomedical Imaging (ISBI), Brooklyn, NY, USA, pp. 101-104. https://doi.org/10.1109/ISBI.2015.7163826

[25] Camlica, Z., Tizhoosh, H.R., Khalvati, F. (2015).

Medical image classification via SVM using LBP features from saliency-based folded data. In 2015 IEEE 14th International Conference on Machine Learning and Applications (ICMLA), Miami, FL, USA, pp. 128-132. https://doi.org/10.1109/ICMLA.2015.131

[26] Xue, Z., You, D., Candemir, S., Jaeger, S., Antani, S., Long, L.R., Thoma, G.R. (2015). Chest X-ray image view classification. In 2015 IEEE 28th International Symposium on Computer-Based Medical Systems, Sao Carlos, Brazil, pp. 66-71. https://doi.org/10.1109/CBMS.2015.49

[27] Agrawal, V., Chandra, S. (2015). Feature selection using Artificial Bee Colony algorithm for medical image classification. In 2015 Eighth International Conference on Contemporary Computing (IC3), Noida, India, pp. 171-176. https://doi.org/10.1109/IC3.2015.7346674

[28] Khan, A., Li, J.P., Shaikh, R.A. (2015). Medical image processing using fuzzy logic. In 2015 12th International Computer Conference on Wavelet Active Media Technology and Information Processing (ICCWAMTIP), Chengdu, China, pp. 163-167. https://doi.org/10.1109/ICCWAMTIP.2015.7493967

[29] Barata, C., Celebi, M.E., Marques, J.S. (2014). Improving dermoscopy image classification using color constancy. IEEE Journal of Biomedical and Health Informatics, 19(3): 1146-1152. https://doi.org/10.1109/JBHI.2014.2336473

[30] Bar, Y., Diamant, I., Wolf, L., Lieberman, S., Konen, E., Greenspan, H. (2015). Chest pathology detection using deep learning with non-medical training. In 2015 IEEE 12th International Symposium on Biomedical Imaging (ISBI), Brooklyn, NY, USA, pp. 294-297. https://doi.org/10.1109/ISBI.2015.7163871

[31] Li, Q., Cai, W., Wang, X., Zhou, Y., Feng, D.D., Chen, M. (2014). Medical image classification with convolutional neural network. In 2014 13th International Conference on Control Automation Robotics & Vision (ICARCV), Singapore, pp. 844-848. https://doi.org/10.1109/ICARCV.2014.7064414

[32] Al-Issa, Y., Ottom, M.A., Tamrawi, A. (2019). eHealth cloud security challenges: A survey. Journal of Healthcare Engineering, 2019(1): 7516035. https://doi.org/10.1155/2019/7516035

[33] Tiwari, C.S., Jha, V.K. (2022). Enhancing security of medical image data in the cloud using machine learning technique. International Journal of Image, Graphics and Signal Processing, 14: 13-31. https://doi.org/10.5815/ijigsp.2022.04.02

[34] Markandey, A., Moghe, S., Bhute, Y., Honale, S. (2014). An image encryption mechanism for data security in clouds. In 2014 IEEE Global Humanitarian Technology Conference-South Asia Satellite (GHTC-SAS), Trivandrum, India, pp. 227-231. https://doi.org/10.1109/GHTC-SAS.2014.6967588

[35] Abbas, N.A. (2016). Image encryption based on independent component analysis and Arnold's Cat Map. Egyptian Informatics Journal, 17(1): 139-146. https://doi.org/10.1016/j.eij.2015.10.001

[36] Masood, F., Driss, M., Boulila, W., Ahmad, J., Rehman, S.U., Jan, S.U., Qayyum, A., 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

[37] 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

[38] Hamad, S., Khalifa, A., Elhadad, A., Rida, S.Z. (2013). A modified Playfair cipher for encrypting digital images. Modern Science, 3(2): 76-81.