scientific reports

Check for updates

OPEN

Improving privacy-preserving multi-faceted long short-term memory for accurate evaluation of encrypted time-series MRI images in heart disease

Lenka Čepová[1], Muniyandy Elangovan[2,3]✉, Janjhyam Venkata Naga Ramesh[4,5], Mandeep Kaur Chohan[6,7], Amit Verma[8] & Faruq Mohammad[9]

In therapeutic diagnostics, early diagnosis and monitoring of heart disease is dependent on fast time-series MRI data processing. Robust encryption techniques are necessary to guarantee patient confidentiality. While deep learning (DL) algorithm have improved medical imaging, privacy and performance are still hard to balance. In this study, a novel approach for analyzing homomorphically-encrypted (HE) time-series MRI data is introduced: The Multi-Faceted Long Short-Term Memory (MF-LSTM). This method includes privacy protection. The MF-LSTM architecture protects patient's privacy while accurately categorizing and forecasting cardiac disease, with accuracy (97.5%), precision (96.5%), recall (98.3%), and F1-score (97.4%). While segmentation methods help to improve interpretability by identifying important region in encrypted MRI images, Generalized Histogram Equalization (GHE) improves image quality. Extensive testing on selected dataset if encrypted time-series MRI images proves the method's stability and efficacy, outperforming previous approaches. The finding shows that the suggested technique can decode medical image to expose visual representation as well as sequential movement while protecting privacy and providing accurate medical image evaluation.

Keywords Heart Disease, MRI Images, Encryption, Multi-faceted long short-term memory (MF-LSTM)

Early detection and monitoring of cardiac disease are crucial in therapeutic diagnostics, necessitating the fast processing of time-series MRI data. But, due to the sensitive nature of this data, strict privacy controls are required to ensure affected person confidentiality[1]. Utilizing an innovative encryption strategy is important due to this demand for privacy. Despite advances in Deep learning (DL) algorithms for scientific imaging, achieving a stability between enhancing image quality and protection affected person privacy remains a major difficulty. Medical imaging is a rapidly evolving field of which has rewarding effects on diagnosing and managing fairly many conditions, particularly cardiovascular diseases. Among the minimally invasive, a crucial element is Magnetic Resonance Imaging, MRI with a particular focus on the field of cardiovascular pathology. This means that patient's privacy is a significant concern and there is rising need for technologies that can ensure privacy of the medical information[2]. For the encryption of time series MRI images, the deep learning method seems to offer a very promising area for accurate evaluation. This has brought about the answer to the usage of encryption

[1]Department of Machining, Assembly and Engineering Metrology, Faculty of Mechanical Engineering, VSB-Technical University of Ostrava, 70800 Ostrava, Czech Republic. [2]Department of Biosciences, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Chennai 602 105, India. [3]Applied Science Research Center, Applied Science Private University, Amman, Jordan. [4]Department of CSE, Graphic Era Hill University, Dehradun 248002, India. [5]Department of CSE, Graphic Era Deemed To Be University, Dehradun, Uttarakhand 248002, India. [6]Department of Computer Science and Engineering, Faculty of Engineering and Technology, Jain (Deemed-to-Be) University, Bengaluru, Karnataka, India. [7]Department of Computer Science and Engineering, Vivekananda Global University, Jaipur, India. [8]University Centre for Research and Development, Chandigarh University, Gharuan, Mohali, Punjab, India. [9]Department of Chemistry, College of Science, King Saud University, P.O. Box 2455, Riyadh 11451, Kingdom of Saudi Arabia. ✉email: muniyandy.e@gmail.com

systems to preservation of privacy. It is important to note that even though these techniques can be effective for data protection, they may bring some changes in the methods of carrying out the diagnostic evaluations[3]. The use of deep learning can also help in extracting detailed features and patterns from encrypted data; it provides a solution for this particular problem. Since medical information, in general, is sensitive, in questions related to heart health, the matter of privacy preservation is paramount[4]. MRI data is very specific in case of patients and contains a lot of valuable information regarding temporal characteristics of certain heart morphology/physiology. Digital frameworks within the healthcare industry continue to expand at newer rates, thus increasing the need to safeguard such information from unauthorized access[5]. Traditional methods work well to keep data and information confidential they do not allow researchers to carry out analytical work effectively. That is why sometimes presence of such information in the encrypted form can interfere with extraction of therapeutically relevant information[6]. Detection is a difficult problem, especially when using encrypted data which cannot be processed directly by deep learning models The use of deep learning models that are able to process encrypted data while at the same time maintaining its confidentiality can help solve this problem. Another great advance of the field is the combination of deep learning procedures to decrypted time-series MRI images[7]. This makes it possible to analyse the raw data in order to make conclusions without compromising on the data's confidentiality. Coupling with encrypted data is possible through deep learning networks with homomorphic encryption structures included. This permits key diagnostic information to be obtained from the outputs without the need to decrypt the results[8]. Moreover, the application of deep learning within this certain framework can lead to improvement in diagnostic assessments primarily based on these results. Through neural networks, the encrypted time-series MRI images with multiple layers can be decrypted and the existence of complicated patterns will be detected by medical practitioners, which gives medical practitioners an understanding of how cardiovascular diseases evolve[9]. Concerning the two criteria, the combination of the two, that is, of privacy preservation and the diagnostic precision in this respect helps to satisfy one of the major requirements of the medical domain, contributing to the development of a stronger and more effective system for handling private cardiac information[10]. For time-series MRI data under homomorphic encryption, we have presented a unique technique in the study termed Multi-Faceted Long Short-Term Memory (MF-LSTM). Ensuring the patients confidentiality in this approach assist in accurate prognosis of cardiac diseasesmaking the results more interpretable this makes this approach to underline good performance in estimating encrypted medical images.

Medical imaging analysis faces challenges in balancing data security with performance, particularly in handling sensitive patient information, and traditional methods struggle to maintain strict privacy while achieving high diagnostic accuracy.Addressing these challenges motivates the development of innovative approaches like MF-LSTM, which combines homomorphic encryption with LSTM networks to preserve patient privacy while achieving high accuracy in medical imaging analysis.The major challenges addressed in this paper is enhancing the evaluation of encrypted time-series MRI data for heart disorder prediction even as making sure patient privacy.

Specifically, the studies question is: "How can a DL model be designed to appropriately classify and predict heart disease from encrypted MRI statistics without compromising privacy?".

Contribution of this study

- Propose a novel Multi-Faceted Long Short -Term Memory (MF-LSTM) method that integrates privacy protection with accurate heart disease categorization and prediction.
- Make use of Generalized Histogram Equalization (GHE) to enhance the quality and evaluation of encrypted MRI images.
- Implement segmentation algorithms to improve the interpretability of pathogenic modifications in encrypted images.
- Demonstrate the approach's effectiveness via great experimentation, attaining advanced performance metrics as compared to existing strategies, with an accuracy, precision, recall, and F1-score.

This examine presents a strong framework for retaining affected person privacy even as reaching excessive accuracy in clinical photograph evaluation, addressing an important need inside the area of therapeutic diagnostics.

Parts of the article: In "Related works", there is a list of related works. Presenting the proposed techniques is "Methodology". Section "Result and discussion" presents the results and discussion. Section "Conclusion" contains the final findings of the recommended research.

Related works

Study	Method	Advantage	Disadvantage
[11]	Deep Convolution Neural Network (DCNN) with Residual Number System (RNS)	High classification performance on encrypted data	Complex setup with RNS; Limited scalability
[12]	Faster R-CNN (SecRCNN)	Lightweight, improved accuracy and reduced computation time	Requires fine-tuning for specific tasks; Potential accuracy trade-offs
[13]	Homomorphic encryption algorithm with CaRENets (CNN)	Efficient inference and memory usage on encrypted images	Computational overhead; Complex integration

Study	Method	Advantage	Disadvantage
14	Homomorphic Residue Number System-Convolutional Neural Network (HoRNS-CNN)	Promising results for dyslexia neural biomarker classification	Promising results in privacy; Limited scalability
15	Adaptive Sigma Filterized Synorr Certificate Less Sign Cryptive Levenshtein Entropy Coding (ASFSCSLEC-DNL)	Improved privacy of transmitted medical images, competitive results	Competitive privacy results; Effective compression
16	Perceptual Encryption (PE) method for color and grayscale images with JPEG compression	High security, no quality loss in lossy compression	Enhanced security; Lossless compression
17	Medi-Sec-Fed framework for federated education	Enhanced privacy and security, outperforms FedAvg	Outperforms FedAvg; Secure knowledge distillation
18	Chaotic system and ANN-based crypto-compression technique	High-quality and secure compressed images	High privacy protection; Maintains image quality
19	Deep learning-based key generation network (DeepKeyGen)	Superior security compared to existing methods	Superior security; Efficient key management
20	Neural network with key creation using Region of Interest (ROI)	Greater encryption and key strength	Strong encryption strength; Tailored security
21	Deep learning-based image encryption system	High security against statistical and differential attacks	Strong encryption; Comparative analysis
22	DeepFixCX privacy-preserving image compression	Enhanced predictive ability, unsupervised image compression	Enhances DL-based classification; Privacy-enhanced
23	FEDResNet framework	High level of security, strong encryption network	High security; Parallel dissemination
24	Generally Nuanced Deep Learning Framework (GaNDLF)	Comprehensive solution for clinical operations	Scalable; Supports diverse medical imaging tasks
25	Two-stage Generative Adversarial Neural Network (ToStaGAN)	Superior performance in brain tumor segmentation	High performance; Contextual autoencoder integration
26	Progressive Generative Adversarial Network (PG-GAN)	Generates realistic cardiac MRI images	Generates realistic images; Useful for rare diseases
27	Deep learning for Cardiac MRI (CMR) analysis	High-precision automated analysis	Largest annotated dataset; Automated diagnosis
28	Deep learning for cardiac MRI imaging plane recommendation	Accurate imaging plane approximation	Precision in imaging; Automatic generation
29	Deep learning structure for myocardial infarction image categorization and localization	High-level feature representation, accurate predictions	High-level feature representation; Clinical relevance
30	Deep Convolutional Neural Network (DCNN) for image quality assessment	High agreement with human experts	Automated assessment; Agreement with experts
31	Multiscale Residual Attention-UNet (MRA-UNet)	Achieves state-of-the-art results in brain tumour segmentation, particularly in core and tumour area improvement	Specific dataset dependency; performance may vary on other datasets
32	Dense Attention Mechanism Network (DAM-Net)	Uses dense layers, channel attention, adaptive downsampling, and label smoothing for high accuracy in detection	Requires large, diverse dataset for robust generalization; computational intensity due to complex architecture
33	Semi-supervised Multitask Learning with Unlabeled Data (Kaggle-EyePACS)	Enhances performance using unlabeled data; improves resilience and generalization	Dependency on availability and quality of unlabeled data; complexity in multitask training
34	Deep learning and hybrid techniques	Efficient and accurate brain tumor detection and classification. Reduces reliance on manual segmentation Improves diagnostic speed and consistency	Requires large annotated datasets. Potential overfitting with complex models. Interpretability challenges for clinical acceptance
35	Radiomics approach with advanced ML algorithms for microcalcification detection	Effective decision support for radiologists, Improves efficiency in early breast cancer screening	Complexity in implementing contourlet transform and parameter tuning for radiomic fusion algorithm
36	Advanced deep learning using transfer learning (SE-ResNet152, modified VGGNet). To detect lesions, use Chaotic Leader Selective Filler Swarm Optimisation (cLSFSO). grading and diagnosis using hybrid models (CNN + SVM, CNN + LSTM)	Enhanced accuracy in lesion detection and classification, Reduced false positives, Improved risk assessment, Faster convergence rates	Complexity in integrating multiple deep learning models, Potential overfitting despite regularization, High computational resource requirement
37	Deep learning approaches for breast cancer prognosis, integrating multi-imaging modalities, segmentation, feature extraction, and classification	Improved diagnostic accuracy, leveraging complex data patterns and multi-modal information to reduce misinterpretations and unnecessary biopsies	Requires large annotated datasets, significant computational resources, potential for overfitting, and challenges in validation and clinical interpretability

Problem statements

Balancing information privacy and high-performance predictive modeling in medical imaging is a essential venture. existing methods like DCNN with RNS and SecRCNN provide high accuracy however be afflicted by complexity and confined scalability. Homomorphic encryption with CNNs and HoRNS-CNNs enhance

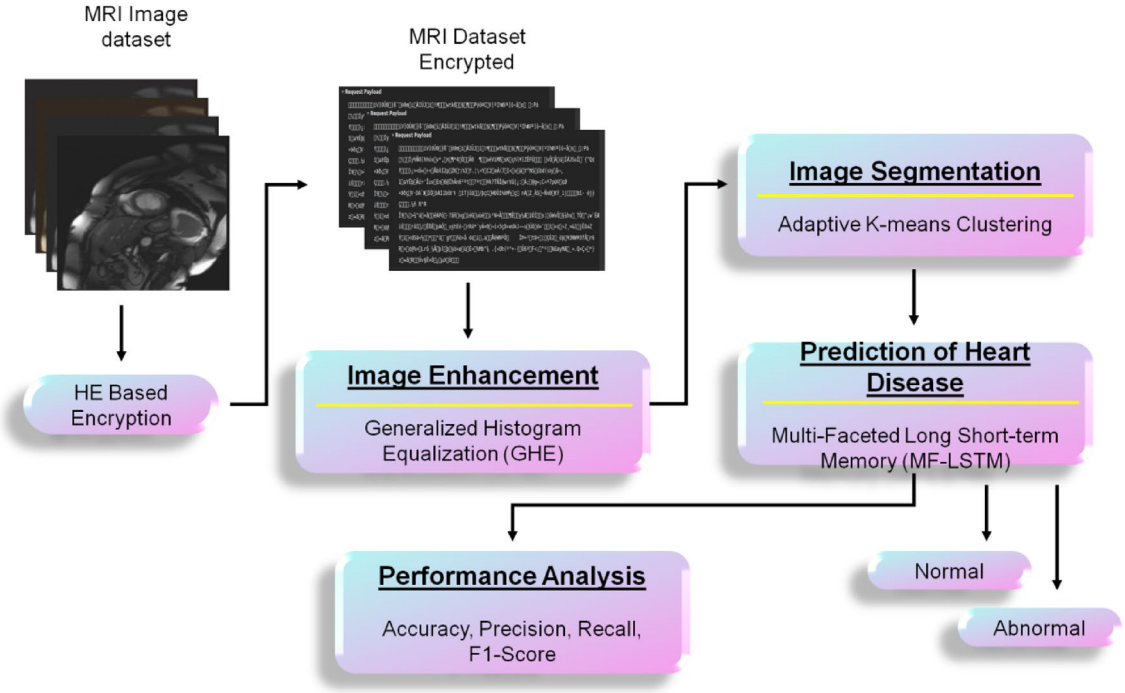

Fig. 1. Overview of the suggested model for encrypted MRI images in heart disease.

privacy however introduce computational complexity. Adaptive filtering and encryption-compression techniques enhance protection. Butcomputationally in depth and dataset-dependent. therefore, there can be a need for innovative strategies that combine superior encryption, effectivedata processing, and specific deep learning-model to ensurescalable, robust and secure clinical diagnostics.

We developed an innovative method known as MF-LSTM in order to overcome these constraints.By utilizing an advanced encryption algorithm develop specifically for time-series MRI data, our suggested technique intends to improve privacy preserving method.

Methodology

The dataset of MRI images is encrypted with HE-based encryption. Generalized Histogram Equalization (GHE) is used for image enhancement. Adaptive K-means clustering was used for the segmentation process. The proposed MF-LSTM was employed to predict the time series MRI image. Figure 1 shows the suggested model's general flow.

Dataset

The dataset from https://github.com/lalaantika/HyperkinesiaML/tree/master/dataset, comprising data from 30 sufferers with 900 to 1200 image, faces boundaries and biases[38]. Its small sample size might not completely represent the variety of hyperkinesia. Potential biases in patient selection and variability in image satisfactory could have an effect on the reliability and generalizability of findings. Additionally, without detailed distribution facts, there is a danger of dataset imbalance. Addressing those issues requires cautious interpretation and validation on large, further diverse datasets to make sure robustness in analyses and model improvement.

Encryption using homomorphic encryption (HE)

Homomorphic encryption (HE) is a cryptographic technology that allows calculations on encrypted data without decrypting it, making it useful in data privacy-sensitive instances including healthcare applications like assessing MRI scans for heart disorder. HE improves privacy in assessing encrypted MRI images. It conserves privacy, enables accurate version evaluation, and guarantees affected person privacy without compromising diagnostic accuracy in healthcare packages.

The potential to carry out calculations on encrypted information homomorphic encryption (HE) protects magnetic resonance imaging (MRI) at the same time as preserving diagnostic integrity and retaining privacy. In this study, we employ the Paillier method to secure image encryption. Paillier ciphers are Partially Homomorphic Encryption (PHE) that could fulfill additive homomorphism. we can explain the essential ideas behind this research, which encompass key generation, encryption and homomorphic addition.

Key generation: The formula for computing (m, h) as the public key and (λ, μ) as the private key is as follows.

1. Find a pair of huge prime numbers, o and r, where their $gcd\big(oq, (o-1)(r-1)\big) = 1$.

2. Find the least common multiple (lcm) of the two numbers m and λ, where $m = or$ and $\lambda = lcm(o-1, r-1)$.
3. Decide on a number h at random.
4. Since $\mu = \left(K\left(h^{\lambda} mod m^2\right)\right)^{-1} mod m$ and $K(w) = \frac{w-1}{m}$, then calculate m.

Encryption: The cipher-text d can be calculated as follows: $d = h^n.q^m mod\ m^2$ *and* q is a number that is chosen at random $\left(0 < q < m \text{ and } \gcd(q, m) = 1\right)$.
Homomorphic addition: Two cipher-texts multiplied together will be decoded into their combined plaintext form: $C\left(F\left(n_1, q_1\right).F\left(n_2, q_2\right) mod\ m^2\right) = (n_1 + n_2)\ mod\ m$ and the decryption of a ciphertext multiplied by a plain-text will yield the sum of the plaintexts involved
$C\left(F\left(n_1, q_1\right).h^{n_2} mod\ m^2\right) = (n_1 + n_2)\ mod\ m$.

Homomorphic encryption (HE) is used to encrypt MRI images before transmission or storage, providing an extra layer of protection for patient's personal health data.

Image enhancement

Improvements in definition, contrast and resolution are part of the MRI enhancement process for heart disease. The diagnostic accuracy of cardiovascular examinations can be greatly improved by using better images help doctors to detect minor abnormalities.

Generalized histogram equalization (GHE)

Generalised Histogram Equalisation (GHE) improves image contrast by dispersing pixel concentrations. In privacy-preserving LSTM for encrypted MRI analysis, GHE improves image quality prior to encryption, increasing model accuracy in identifying heart disease from time-series MRI data. This method improves encrypted data reliability, which is critical for accurate medical diagnoses.

Through redistributing pixel intensities, Generalized Histogram Equalization (GHE) improves image contrast. It enhances detail visibility in different lighting circumstances, producing visually appealing and crystal-clear images.

To construct the histogram of the MRI image, the intensity transfer function for contrast enhancement is derived as

$$T(d) = d_{\min} + (d_{\max} - d_{\min}).\frac{\int_{d_{\min}}^{d} h(w)dx}{\int_{d_{\min}}^{d_{\max}} h(w)dx} \tag{1}$$

where d is the intensity value, d_{min} and d_{max} represent the minimum and maximum values of d, $h(w)$ is the image histogram and $T(d)$ is the intensity transfer function for contrast improvement. Naturally, an enormous point in a histogram creates an immediate rise in the cdf function. Therefore, more gray levels are assigned to more common intensity values, while fewer gray levels are assigned to less common intensity values.

This method of histogram equalization can be understood from a different angle, though. To visualize how likely it is that the intensity value w requires to be enlarged for image enhancement, $H(w)$ can be conceptualized as an expansion function. The magnitude of emphasis: We prefer to make this circle around w's intensity levels larger when w occurs more frequently. Hence, Eq. (1) can be construed as a reallocation of intensities based on the distribution of an expansion function $h(w)$.

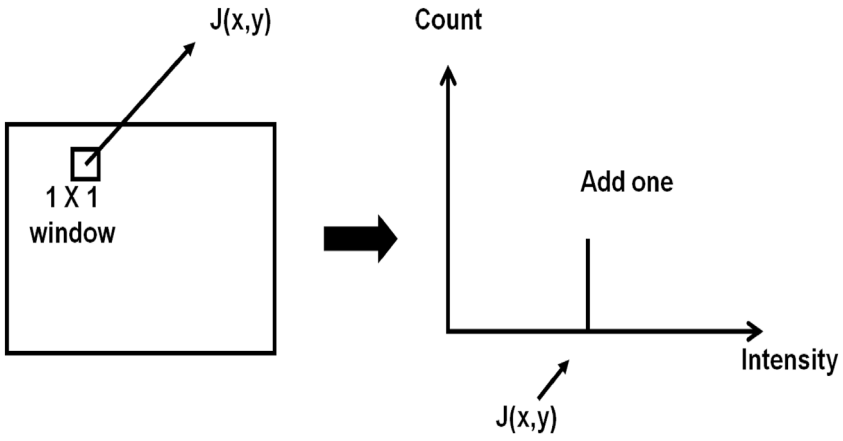

Fig. 2. The process of generating a histogram is demonstrated.

Onanother side, the construction of the histogram $h(w)$ can be seen as a masking-and-accumulating method. Let's pretend we're measuring the intensity of each pixel in the image by scanning it with a $1x1$ mask. The resulting $h(w)$ is an accumulation of these intensities. To produce the histogram function $h(w)$, we simply apply the masking and accumulation process throughout the entire image. In Fig. 2, we show an example of this masking and accumulation in action. The HE technique disregards information surrounding each pixel because of the small size of the $1x1$ mask. Therefore, the overall statistics of the image are contained in the histogram function $h(w)$.

Image segmentation

In the case of heart illness, MRI segmentation is cutting up MRI scans of the heart into sections for more accurate study of the heart's architecture. This improves health care and the results for patients by facilitating accurate diagnosis of a variety of heart diseases.This research shows how the "Adaptive K-means clustering" technique can be used to classify heartMRI scans for the purpose of diagnosing cardiac disease.

Adaptive K-means clustering dynamically partitions encrypted time-series MRI images, assisting in feature extraction for LSTM models. This approach enhances privacy-preserving analysis by adapting clusters to varying data individualities, enhancing accuracy in diagnosing heart disease from encrypted medical imaging data.

Classification is where features like shape and brightness get their start.

Initialization stage: Goodness functions can be calculated after a number of rounds with the K-means image clustering method (where, n = 10). An earlier version of the suggested adaptive segmentation technique looked like this.

Adaptive classification stage: Heart illness is broken down into its component parts and image clustering techniques are applied. Starting with the initial iteration in the phase of initialization, K-means clustering is effective for a total number of iterations (n = 10). Many tiny processes are there in this process: feature-based calculation, feature-based evaluation method, new centers creating process and object selection.

Initialization stage

The first step of the adaptive segmentation strategy is the phase of initialization, during which K-means clustering is applied for n rounds. The core novel clusters are constructed with the help of newly disseminated midpoints. In this particular iteration, the evaluation of goodness occurs immediately. As the average roundness of complete consequences, the goodness functions are defined. The circularity ratio, defined by Eq. (2), is the ratio of the area enclosed by a contour to the area enclosed by a circle with its border.

$$e_{circ} = \frac{4\pi B}{O^2} \tag{2}$$

where B and O are two different regions of the object. For non-circular shapes, the e_{circ} function evaluates to a value less than 1, but for circular shapes, it evaluates to 1. The area is determined by adding the pixels in each alienated set. The following Eq. (3) is used to develop the quality measure:

$$\text{GOODNESS} = \frac{\sum_{j=1}^{N} e_{circ_j} B_j}{\sum_{j=1}^{N} B_j} \tag{3}$$

where e_{circ} are the aspect ratios of the jth object and B_j are the area of the jth object. Large object standards are raised and tiny object values are lowered thanks to the region's coupling via circularity ratio.

Classification stage

It plays a pivotal role in the anticipated algorithm. After the initialization step is complete, the K-means method can be used for another n iteration. Goodness is recalculated using an equation and the feature-based calculation approach. We compare our estimates of the present and past positions' goodness using this evaluation method. If

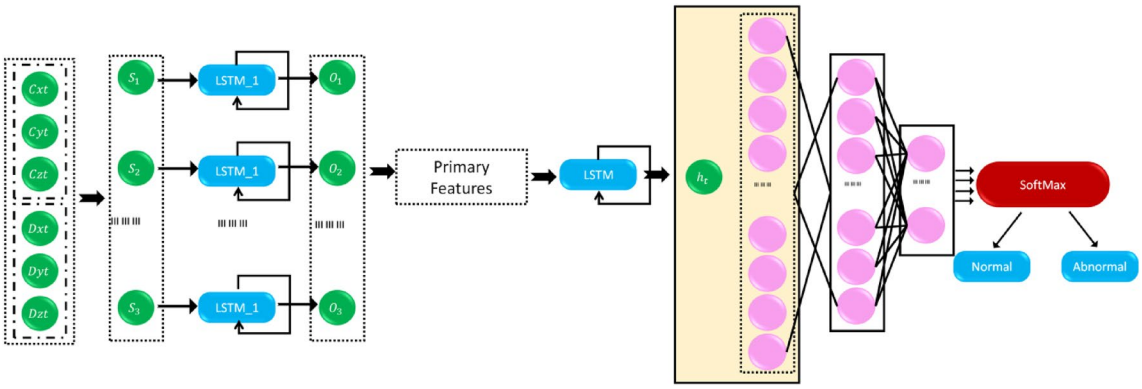

Fig. 3. Architectural design of the multi-faceted LSTM Network.

the current goodness is higher, the outputs from the past are discarded and the current location is used instead. If the current goodness is lower than the novel goodness, new clusters will be generated using the two brightest clusters as targets and the present clusters will be stored unaltered. These steps are repeated until no change occurs in the goodness output or N iterations have passed. Finally, the object selection technique is utilized to identify the most circular areas (those with a circularity ratio close to 1).

Prediction of heart disease

Through performing a sequential and multi-feature analysis of cardiac MRI images, the MF-LSTM algorithm for image segmentation improves accuracy, making it useful for the prediction of heart contamination.

Multi-faceted long short-term memory (MF-LSTM)

This study examine introduces a unique category algorithm for coronary heart sickness, especially the network of multifaceted long short-term memory (MF-LSTM).The properties of heart disease are extracted using aLong Short-Term Memory (LSTM) network, which makes use of time series data obtained from MRI images.Moreover, the activity classification of datainstances is accomplished by using a softmax category algorithm, which utilizes the given capabilities as its basis.A time series dataset may be expressed in a matrix format comprising MRI image data received over a selected time frame, encompassing many MRI images.This can be characterized as Eq. (4).

$$\begin{pmatrix} \boldsymbol{C}_{x0} & \boldsymbol{C}_{y0} & \boldsymbol{C}_{z0} & \boldsymbol{D}_{x0} & \boldsymbol{D}_{y0} & \boldsymbol{D}_{z0} & \dots \\ \boldsymbol{C}_{x1} & \boldsymbol{C}_{y1} & \boldsymbol{C}_{z1} & \boldsymbol{D}_{x1} & \boldsymbol{D}_{y1} & \boldsymbol{D}_{z1} & \dots \\ \boldsymbol{C}_{x2} & \boldsymbol{C}_{y2} & \boldsymbol{C}_{z2} & \boldsymbol{D}_{x2} & \boldsymbol{D}_{y2} & \boldsymbol{D}_{z2} & \dots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots \\ \boldsymbol{C}_{xt} & \boldsymbol{C}_{yt} & \boldsymbol{C}_{zt} & \boldsymbol{D}_{xt} & \boldsymbol{D}_{yt} & \boldsymbol{D}_{zt} & \dots \end{pmatrix} \tag{4}$$

In this context, C and D denote different sensors, whereas x,y and z indicate the three dimensions of each MRI image. Additionally, t represents the duration of a single activity. As previously stated, the task of processing a long-time-step input with a single LSTM neuron is a labor-intensive process. In our suggested technique, numerous Long Short-Term Memory (LSTM) units are employed to process distinct segments of the activity data. Fig 3 illustrates the architectural design of the multi-faceted LSTM Network. The architectural design consists of multiple components, including a layer of input, a layer of parallel LSTM, a layer of merging LSTM,layers that are fully connected and a layer of softmax.

During the signal's input phase, the time sequence signals are partitioned into n segments, denoted as $S_1 \sim S_n$, along the time dimension. Each segment consists of an equal number of time steps and there is no overlap between segments. In accordance with this, there exists a set of n LSTM units that are supplied with n segments, thereby forming the parallel LSTM layer. Each LSTM unit is equipped with identical hyper-parameters, including the number of neurons and the dropout rate to ensure equitable treatment of each segment. The Long Short-Term Memory (LSTM) unit processes segmented data in a chronological manner, iterating via a loop. The preliminary features, which consist of the outputs at the final stage of time of each Long Short-Term Memory (LSTM) unit, are gathered and merged to form a matrix of size $n \times h_1$. Here, h_1 variable denotes the quantity of hidden neuronsin each unit of LSTM. A layer of LSTM for merging is incorporated. The framework is provided with the initial characteristics and proceeds to iterate over the sequence of outputs from the preceding layer. In essence, the combining layer of LSTM operates in a sequential manner.

The characteristic of the activity determined the result that occurs at the last stage of the combining layer of LSTM is selected which incorporates the temporal relationship. The vector has a dimension of h_2, where h_2 denotes the number of hidden neurons in the combining unit of LSTM. Based on previous splitting and merging procedures, it is possible to extract the temporal dependency from the data. The initiation of signal processing can occur prior to the full completion of an activity, hence decreasing the duration of waiting time for activity detection in real-world scenarios.

Subsequently, a pair of fully-connected layers are employed to decrease the dimensionality of the features to a vector of size $1 \times m$, where m represents the total number of diseases. Next, the resulting output is sent into a layer of softmax regression using logistic regression, which generates the classification result. Algorithm 1 shows the process of MF-LSTM.

Hyper parameter	Typical values/Selection process
Number of LSTM layers (L)	2 layers
Hidden state size (H)	256
Batch size	16—128
Learning rate	Tuned via grid search or adaptive methods
Dropout rate	Empirically chosen (e.g., 0.2, 0.3)
Epochs	Typically 50 to 100, adjusted based on convergence and metrics

Table 1. Hyper parameter configuration.

```
Initialize parameters and hyperparameters for LSTM model training
Define encryption and decryption functions for privacy-preserving operations
functiontrain_lstm_encrypted(images, labels, encryption_key):
encrypted_images = encrypt(images, encryption_key)
model = MultiFacetedLSTM()
  model.initialize_parameters()
    for epoch in range(num_epochs):
encrypted_outputs = model.forward_pass(encrypted_images)
decrypted_outputs = decrypt(encrypted_outputs, encryption_key)
loss = calculate_loss(decrypted_outputs, labels)
model.backward_pass(loss)
model.update_parameters()
    return model
function encrypt(data, key):
encrypted_data = homomorphic_encrypt(data, key)
    return encrypted_data
function decrypt(encrypted_data, key):
decrypted_data = homomorphic_decrypt(encrypted_data, key)
    return decrypted_data
class MultiFacetedLSTM:
functioninitialize_parameters():
    function forward_pass(input_data):
    function backward_pass(loss):
functionupdate_parameters():
encryption_key = generate_encryption_key()
encrypted_images, labels = load_encrypted_data()
trained_model = train_lstm_encrypted(encrypted_images, labels,
encryption_key)
encrypted_test_images = load_encrypted_test_data()
encrypted_predictions = trained_model.predict(encrypted_test_images)
decrypted_predictions = decrypt(encrypted_predictions, encryption_key)
evaluate_performance(decrypted_predictions, true_labels)
```

Algorithm 1. The process of MF-LSTM.

Result and discussion

We implemented our privacy-preserving LSTM approach in python version 3.10 on system running window 10. An Intel Core i3 CPU and a specialized high-performance IRIS graphics card are part of the hardware setup, which maximizes processing power for demanding machine learning task. The effectiveness of the suggested method (MF-LSTM) was analyzed by applying a set of parameters such asaccuracy, precision, recall and F1-score are compared with existing methods KNN (k-Nearest Neighbor)[39], RF (Random forest)[40], and SVR (Support Vector Regression)[40] The hyper parameter used for training are described in Table 1.

Comparing MF-LSTM complexity with traditional LSTM

The computational complexity of the proposed Multi-Faceted Long Short-Term Memory (MF-LSTM) version exceeds that of conventional LSTM model because of its incorporation of a couple of layers, parallel processing paths, and potentially extra mechanisms like attention and adaptation. This complexity allows MF-LSTM to address diverse encrypted MRI data successfully, albeit requiring more computational assets for training and inference. Figure 4 shows the computational complexity of LSTM and MF-LSTM.

ROC (Receiver operating characteristic)

The Receiver operating characteristic (ROC) curve is a graphical illustration of a binary classifier machine's overall performance, plotting True Positive Rate (TPR) in opposition to False Positive Rate (FPR) at unique threshold settings. It is beneficial in comparing encrypted time-series MRI images for coronary heart disease detection, assessing the classifier's capacity to differentiate between positive and negative instances. Figures 5, 6 show the ROC results and the confusion matrix and the ROC results. The formula of ROC is shown in Eq. (5), (6). The TPR (Sensitivity) FPR (1- Specificity) is defined as:

- True positive rate (TPR)

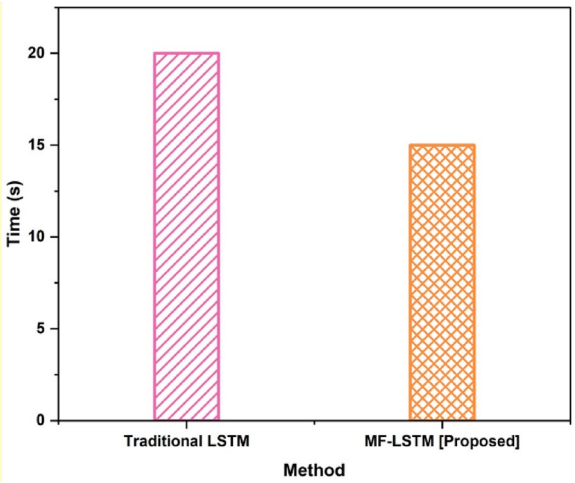

Fig. 4. Traditional LSTM vs MF-LSTM.

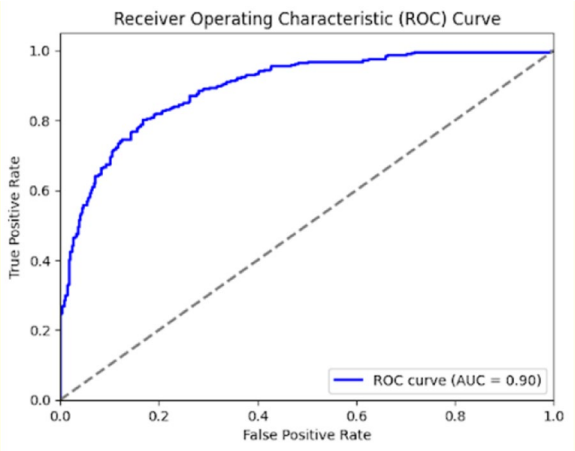

Fig. 5. Outcome of ROC.

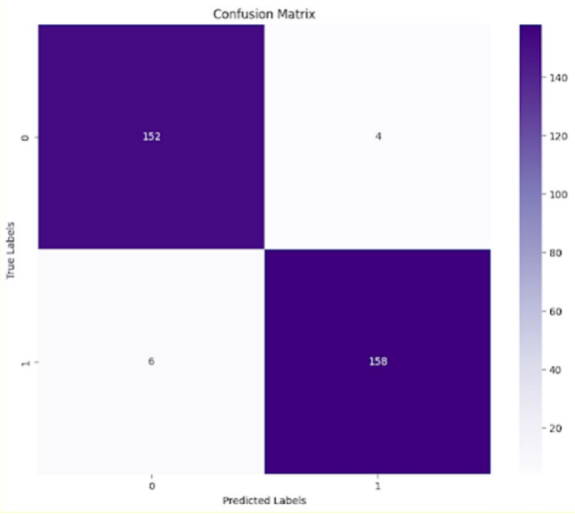

Fig. 6. Outcome of confusion matrix.

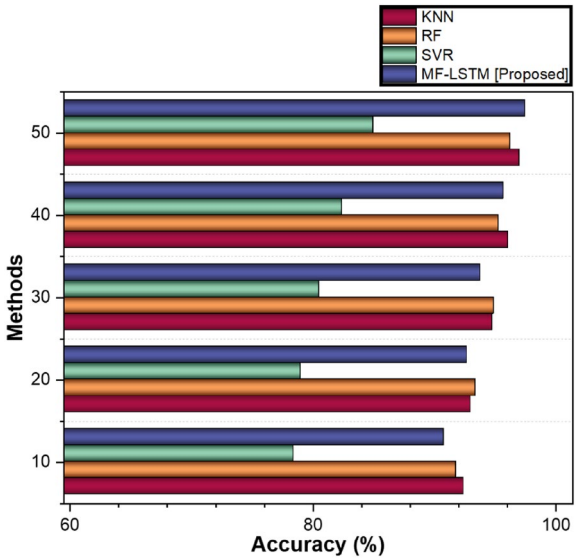

Fig. 7. Comparison of accuracy.

Methods	Accuracy (%)			
	KNN[39]	RF[40]	SVR[40]	MF-LSTM [Proposed]
10	92.4	91.8	78.4	90.8
20	93	93.4	79	92.7
30	94.8	94.9	80.5	93.8
40	96.1	95.3	82.4	95.7
50	97	96.28	84.97	97.5

Table 2. Comparison of accuracy.

$$\text{Sensitivity} = \frac{TP}{TP + FN} \tag{5}$$

- False positive rate (FPR)

$$\text{Specificity} = \frac{TN}{TN + FP} \tag{6}$$

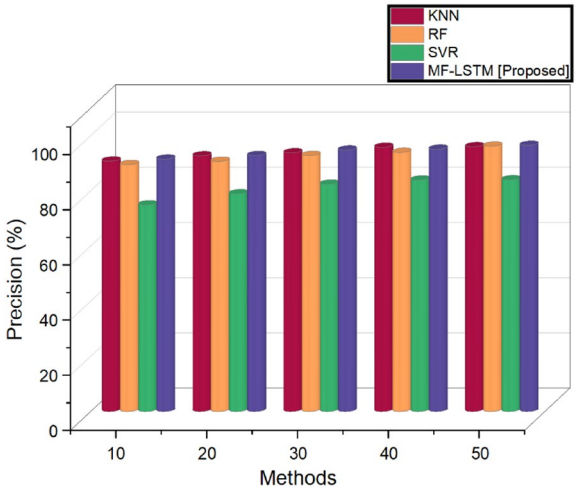

Fig. 8. Comparison of precision.

Methods	Precision (%)			
	KNN[39]	RF[40]	SVR[40]	MF-LSTM [Proposed]
10	90.8	89.5	74.9	91.5
20	92.7	90.7	78.9	92.8
30	93.8	92.8	82.4	94.8
40	95.8	93.9	83.9	95.1
50	96	96.2	84	96.5

Table 3. Comparison of precision.

ROC analysis is essential for validating the accuracy and reliability of diagnostic models, ensuring robustness in clinical imaging packages including heart disease detection the usage of encrypted MRI data.

Accuracy

Accuracy assesses the model's overall correctness in categorization or prediction. The comparisonof accuracy is displayed in Fig. 7 and Table 2.The existing KNN, RF and SVR algorithms achieve 97%, 96.28% and 84.97% accuracy, while the proposed MF-LSTM achieves 97.5%.The proposed method shows the higher accuracy scoreis able to identify diseased cardiac images as distinct from healthy ones.The increased accuracy shows how well the MF-LSTMmodel can recognize and separate healthy from sick cardiac images.The formula of accuracy is shown in Eq. (7).

$$Accuracy = \frac{Number\ of\ Correct\ Predictions}{Total\ Number\ of\ Predictions} \tag{7}$$

Precision

Precision measures the model's accuracy in making beneficial predictions. Precision in medical imaging refers to how many of the displayed cases of heart disease actually occur as true positives. The comparison of precision is displayed in Fig. 8 and Table 3. Here, compared to the existing KNN (96%), RF (96.2%) and SVR (84%) methods, our proposed method MF-LSTM has a much higher precision value of 96.5%.The higher precision score of our

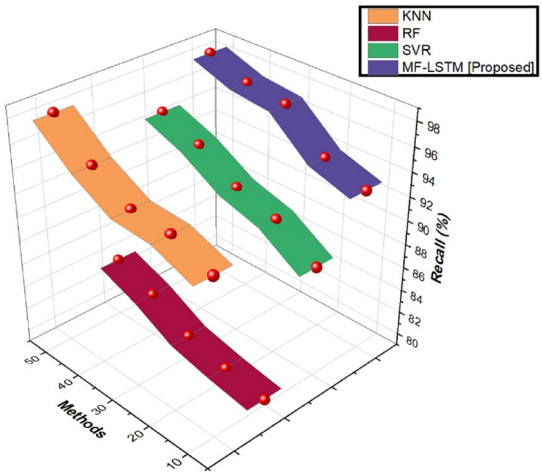

Fig. 9. Comparison of recall.

Methods	Recall (%)			
	KNN[39]	RF[40]	SVR[40]	MF-LSTM [Proposed]
10	92.4	79.5	88.5	92.7
20	93.7	80.1	90.7	93.8
30	93.9	80.9	91.7	96.7
40	95.7	82.7	93.7	97.1
50	98.3	84	95	98.3

Table 4. Comparison of Recall.

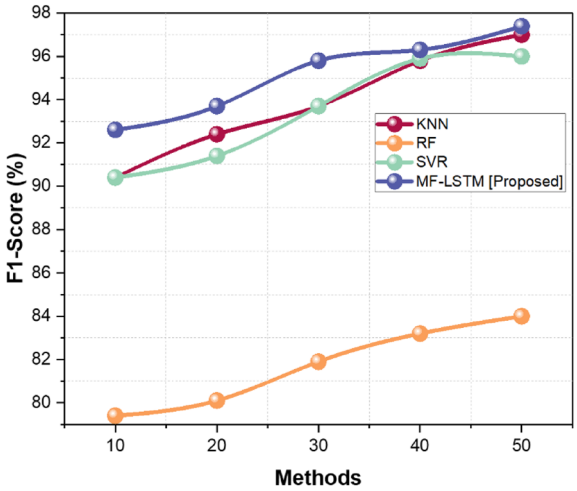

Fig. 10. Comparison of F1-score.

Methods	F1-Score (%)			
	KNN[39]	RF[40]	SVR[40]	MF-LSTM [Proposed]
10	90.4	79.4	90.4	92.6
20	92.4	80.1	91.4	93.7
30	93.7	81.9	93.7	95.8
40	95.8	83.2	95.9	96.3
50	97	84	96	97.4

Table 5. Comparison of F1-score.

method will reduce the number of false positive patients thereby improving clinical outcome and the care of the diseases' patients.The proposed method shows the higher precision score is able to identify diseased cardiac images as distinct from healthy ones. The formula of precision is shown in Eq. (8).

$$Precision = \frac{True\ Positives}{True\ Positives + False\ Positives} \tag{8}$$

Recall

The metric referred to as recall, which is known as sensitivity or true positive rate, quantifies the model's capacity to detect every relevant incident, namely instances of heart disease in the domain of medical imaging. The comparison of recall is shown in Fig. 9 and Table 4. Our suggested **MF**-LSTM strategy has a high recall percentage of 98.3%, while the existing KNN, RF and SVR methods achieve 98.3, 84 and 95%, respectively. The proposed method shows the higher recall score is able to identify diseased cardiac images as distinct from healthy ones. High recall is crucial in medical imaging for heart disease diagnosis, minimizing false negative and ensuring accurate diagnosis and timely medical intervention.The formula of recall is shown in Eq. (9).

$$Recall = \frac{True\ Positives}{True\ Positives + False\ Positives} \tag{9}$$

F1-score

The F1-score is a balanced measure that includes the advantage of false positives and false negatives. It is a harmonic mean of precision and recall. The comparison of the F1-score is shownin Fig. 10 and Table 5. Compared to the traditional methodologies KNN (97%), RF (84%) and SVR (96%), our suggested method, MF-LSTM has a higher F1-score of 97.4%.Our proposed method outperforms the previous method by achieving a higher f1score, enhancing the identification of diseased cardiac images as distinct from healthy ones.The formula of recall is shown in Eq. (10).

$$f1 - score = \frac{2 \times (Precision \times Recall)}{Precision + Recall} \tag{10}$$

Discussion

The main disadvantages of KNN (k-Nearest Neighbor)[39], RF (Random forest)[40], and SVR (Support Vector Regression)[40]in the accurate assessment of encrypted time-series MRI images in coronary heart disorder stem from their inherent obstacles in managing complex, excessive-dimensional statistics and encrypted information. KNN suffers from scalability troubles and high computational costs as the dataset grows, making it inefficient for large-scale MRI data. RF, at the same time as strong, can struggle with overfitting, in particular with time-seriesdatathat might have temporal dependencies not easily captured by tree-based model. SVR, on the other hand, require for significant tuning of hyper parameters and it was sensitive to the selection of kernel functions, which could restrict its performance on encrypted datasets in which characteristic extraction and representation are critical. Those techniques commonly lack the functionality to absolutely exploit the temporal and spatial intricacies of MRI data, leads to suboptimal accuracy within the assessment of heart disorder while compared to more advanced deep learning strategies tailored for such tasks.

The Multi-Faceted Long Short-Term Memory (MF-LSTM) excels in accurately comparing encrypted time-series MRI images in coronary heart disorder via retaining temporal dependencies and shooting complicated styles, vital for retaining information integrity and diagnostic accuracy in sensitive clinical imaging application.

Practical implication

- **Enhance security:** Making sure sensitive patient data remains private while taking into account powerful evaluation and diagnosis the usage of superior deep learning models.
- **Advanced Diagnostic Accuracy:** Facilitating more particular detection and type of heart sickness situations from encrypted MRI data, assisting better affected patient care and treatment plans.
- **Facilitated data Sharing:** assist secure sharing of encrypted MRI data across healthcare provider and researchers, promoting collaborative efforts in medical research and diagnostics.
- **Regulatory Compliance:** Assembly regulatory requirements for affected person facts privacy ensuring ethical use of AI technologies in healthcare.

Those implications highlight the practical benefits of MF-LSTM in addressing the dual challenging situations of maintaining patient privacy and achieving accurate medical critiques in coronary heart disease analysis.

Conclusion

Wediscuss the importance of patient privacy in time-series magnetic resonance imaging for early diagnosis and monitoring of cardiac disease. In this paper, we introduce the Multi-Faceted Long Short-Term Memory (MF-LSTM) method that integrates privacy protection with the homomorphic-encrypted (HE) time-series MRI data. The suggested MF-LSTM architecture maintains the highest level of security while safeguarding patient privacy and enabling precise classification and prediction of heart disease scenarios. By distributing the intensity values to create a more harmonious and aesthetically pleasing representation, Generalized Histogram Equalization (GHE), a complex image enhancement technique, improves the contrast and overall quality of images. The identification of crucial regions in the encrypted MRI images is made possible by adaptive k means clustering, which enhances the interpretability of pathological alterations. Python software is used for simulation. Experimental findings value such as accuracy (97.5%), recall (98.3%), F1-score (97.4%) and precision (96.5%) were found to be best achieved by the proposed MF-LSTM method. The real-time assessment of medical images can be impacted by the computational overhead that privacy-preserving approaches impose. Create and investigate more sophisticated privacy-preserving methods that can improve the security of private medical data while retaining the accuracy of the model.

Limitation and future scope of this study

The study's application may be limited by the unique dataset employed and its representation of varied patient demographics and imaging procedures. Further investigation into the scalability and practical deployment aspects of the privacy-preserving MF-LSTM approach in clinical contexts, as well as the resolution of integration obstacles and performance evaluation on bigger and more diverse datasets, might be considered as future research.

Data availability

The data presented in this study are available through email upon request to the corresponding author.

Received: 13 March 2024; Accepted: 19 August 2024
Published online: 30 August 2024

References

1. Jeelani, H., Martin, J., Vasquez, F., Salerno, M. and Weller, D.S., 2018, April. Image quality affects deep learning reconstruction of MRI. In 2018 IEEE 15th international symposium on biomedical imaging (ISBI 2018) (pp. 357–360). IEEE.
2. Masutani, E. M., Bahrami, N. & Hsiao, A. Deep learning single-frame and multiframe super-resolution for cardiac MRI. *Radiology* **295**(3), 552–561 (2020).
3. Curiale, A. H., Colavecchia, F. D. & Mato, G. Automatic quantification of the LV function and mass: A deep learning approach for cardiovascular MRI. *Comput. Methods Progr. Biomed.* **169**, 37–50 (2019).

4. Wang, Z., Peng, Y., Li, D., Guo, Y. & Zhang, B. MMNet: A multi-scale deep learning network for the left ventricular segmentation of cardiac MRI images. *Appl. Intell.* **52**(5), 5225–5240 (2022).
5. Liao, F., Chen, X., Hu, X. & Song, S. Estimation of the volume of the left ventricle from MRI images using deep neural networks. *IEEE Trans. Cybern.* **49**(2), 495–504 (2017).
6. Zhou, T. *et al.* Automatic segmentation of left ventricle in cardiac cine MRI images based on deep learning In medical imaging. *Image Process.*. **10133**(540), 547 (2017).
7. Abdeltawab, H. *et al.* A deep learning-based approach for automatic segmentation and quantification of the left ventricle from cardiac cine MR images. *Comput. Med. Imaging Graph.* **81**, 101717 (2020).
8. Zhang, N. *et al.* Deep learning for diagnosis of chronic myocardial infarction on nonenhanced cardiac cine MRI. *Radiology* **291**(3), 606–617 (2019).
9. Hauptmann, A., Arridge, S., Lucka, F., Muthurangu, V. & Steeden, J. A. Real-time cardiovascular MR with spatio-temporal artifact suppression using deep learning–proof of concept in congenital heart disease. *Magn. Reson. Med.* **81**(2), 1143–1156 (2019).
10. Küstner, T. *et al.* CINENet: Deep learning-based 3D cardiac CINE MRI reconstruction with multi-coil complex-valued 4D spatio-temporal convolutions. *Sci. Rep.* **10**(1), 13710 (2020).
11. Usman, O. L. & Muniyandi, R. C. CryptoDL: Predicting dyslexia biomarkers from encrypted neuroimaging dataset using energy-efficient residue number system and deep convolutional neural network. *Symmetry* **12**(5), 836 (2020).
12. Liu, Y., Ma, Z., Liu, X., Ma, S. & Ren, K. Privacy-preserving object detection for medical images with faster R-CNN. *IEEE Trans. Inf. Forensics Secur.* **17**, 69–84 (2019).
13. Chao, J., Badawi, A.A., Unnikrishnan, B., Lin, J., Mun, C.F., Brown, J.M., Campbell, J.P., Chiang, M., Kalpathy-Cramer, J., Chandrasekhar, V.R. and Krishnaswamy, P., 2019. CaRENets: Compact and resource-efficient CNN for homomorphic inference on encrypted medical images. arXiv preprint arXiv:1901.10074.
14. Usman, O.L., Muniyandi, R.C., Omar, K. and Mohamad, M., 2022, February. Privacy-Preserving Classification Method for Neural-Biomarkers using Homomorphic Residue Number System CNN: HoRNS-CNN. In 2022 International Conference on Business Analytics for Technology and Security (ICBATS) (pp. 1–8). IEEE.
15 Selvi, C. T., Amudha, J. & Sudhakar, R. Medical image encryption and compression by adaptive sigma filterized synorr certificate-less signcryptiveLevenshtein entropy-coding-based deep neural learning. *Multimed. Syst.* **21**(1056), 1074 (2021).
16. Ahmad, I. & Shin, S. A perceptual encryption-based image communication system for deep learning-based tuberculosis diagnosis using healthcare cloud services. *Electronics* **11**(16), 2514 (2022).
17. Kumar, A., Purohit, V., Bharti, V., Singh, R. & Singh, S. K. Medisecfed: Private and secure medical image classification in the presence of malicious clients. *IEEE Trans. Ind. Inf.* **18**(8), 5648–5657 (2021).
18. Hajjaji, M. A., Dridi, M. & Mtibaa, A. A medical image crypto-compression algorithm based on neural network and PWLCM. *Multimed. Tools Appl.* **78**, 14379–14396 (2019).
19. Ding, Y. *et al.* DeepKeyGen: a deep learning-based stream cipher generator for medical image encryption and decryption. *IEEE Trans. Neural Netw. Learn. Syst.* **33**(9), 4915–4929 (2021).
20. Krishna, A.A., Arikutharam, V., Ramnan, K.V., Bharathi, H. and Chandar, T.S., 2022, May. Dynamic Image Encryption using Neural Networks for Medical Images. In 2022 IEEE IAS Global Conference on Emerging Technologies (GlobConET) (pp. 739–745). IEEE.
21. Panwar, K. *et al.* Encipher GAN: An end-to-end color image encryption system using a deep generative model. *Systems* **11**(1), 36 (2023).
22. Gaudio, A., Smailagic, A., Faloutsos, C., Mohan, S., Johnson, E., Liu, Y., Costa, P. and Campilho, A., 2023. DeepFixCX: Explainable privacy-preserving image compression for medical image analysis. Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery, p.e1495.
23. Zhu, L., Qu, W., Wen, X. & Zhu, C. FEDResNet: a flexible image encryption and decryption scheme based on end-to-end image diffusion with dilated ResNet. *Appl. Opt.* **61**(31), 9124–9134 (2022).
24. Pati, S. *et al.* GaNDLF: the generally nuanced deep learning framework for scalable end-to-end clinical workflows. *Commun. Eng.* **2**(1), 23 (2023).
25. Ding, Y. *et al.* ToStaGAN: An end-to-end two-stage generative adversarial network for brain tumor segmentation. *Neurocomputing* **462**, 141–153 (2021).
26. Diller, G. P. *et al.* Utility of deep learning networks for the generation of artificial cardiac magnetic resonance images in congenital heart disease. *BMC Med. Imaging* **20**, 1–8 (2020).
27. Bernard, O. *et al.* Deep learning techniques for automatic MRI cardiac multi-structures segmentation and diagnosis: Is the problem solved?. *IEEE trans. Med. Imaging* **37**(11), 2514–2525 (2018).
28 Blansit, K., Retson, T., Masutani, E., Bahrami, N. & Hsiao, A. Deep learning–based prescription of cardiac MRI planes. *Radiol. Artif. Intell.* **1**(6), 180069 (2019).
29. Chen, M., Fang, L., Zhuang, Q. & Liu, H. Deep learning assessment of myocardial infarction from MR image sequences. *Ieee Access* **7**, 5438–5446 (2019).
30 Piccini, D. *et al.* Deep learning to automate reference-free image quality assessment of whole-heart MR images. *Radiol. Artif. Intell.* **2**(3), 190123 (2020).
31. Ullah, Z., Usman, M., Jeon, M. & Gwak, J. Cascade multiscale residual attention cnns with adaptive roi for automatic brain tumor segmentation. *Inf. Sci.* **608**, 1541–1556 (2022).
32. Ullah, Z., Usman, M., Latif, S. & Gwak, J. Densely attention mechanism based network for COVID-19 detection in chest X-rays. *Scientific Reports* **13**(1), 261 (2023).
33. Ullah, Z., Usman, M., Latif, S., Khan, A. & Gwak, J. SSMD-UNet: Semi-supervised multi-task decoders network for diabetic retinopathy segmentation. *Sci. Rep.* **13**(1), 9087 (2023).
34. Ali, S. *et al.* A comprehensive survey on brain tumor diagnosis using deep learning and emerging hybrid techniques with multi-modal MR image. *Archives Comput. Methods Eng.* **29**(7), 4871–4896 (2022).
35. Mahmood, T. *et al.* An automatic detection and localization of mammographic microcalcifications ROI with multi-scale features using the radiomics analysis approach. *Cancers* **13**(23), 5916 (2021).
36. Mahmood, T., Saba, T., Rehman, A. & Alamri, F. S. Harnessing the power of radiomics and deep learning for improved breast cancer diagnosis with multiparametric breast mammography. *Expert Syst. Appl.* **249**, 123747 (2024).
37. Mahmood, T. *et al.* A brief survey on breast cancer diagnostic with deep learning schemes using multi-image modalities. *IEEE Access* **8**, 165779–165809 (2020).
38. Sharma, L., Gupta, G. and Jaiswal, V., 2016, December. Classification and development of tool for heart diseases (MRI images) using machine learning. In 2016 Fourth International Conference on Parallel, Distributed and Grid Computing (PDGC) (pp. 219–224). IEEE.
39. Obayes, H. K. & Al-Shareefi, F. Secure heart disease classification system based on three pass protocol and machine learning. *Iraqi J. Comput. Sci. Math.* **4**(2), 72–82 (2023).
40. Hassan, C. A. U. *et al.* Effectively predicting the presence of coronary heart disease using machine learning classifiers. *Sensors* **22**(19), 7227 (2022).

Acknowledgement
The KSU author acknowledges funding from Researchers Supporting Project number (RSP2024R355), King Saud University, Riyadh, Saudi Arabia.

Author contributions
Conceptualization, L.C, M.E, J.N.R, M.K, A.V, and F.M Formal analysis, L.C, M.E, J.N.R, M.K, A.V, and F.M Investigation, L.C, M.E, J.N.R, M.K, A.V, and F.M Methodology, L.C, M.E, J.N.R, M.K, A.V, and F.M Software, L.C, M.E, J.N.R, M.K, A.V, and F.M Writing – original draft, L.C, M.E, J.N.R, M.K, A.V, and F.M Writing – review & editing, L.C, M.E, J.N.R, M.K, A.V, and F.M.

Funding
European Union under the REFRESH,CZ.10.03.01/00/22_003/0000048.

Competing interests
The authors declare no competing interests.

Additional information
Correspondence and requests for materials should be addressed to M.E.

Reprints and permissions information is available at www.nature.com/reprints.

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.