Electronic ISSN: 2327-4697 CD: 2334-329X WORLDWIDE: +1 732 981 0060
IEEE Transactions on Network Science and Engineering, [doi: 10.1109/TNSE.2022.3199235]

https:// ieeexplore.ieee.org

基于混沌的新型癌症诊断隐私保护深度学习模型*

Mujeeb Ur Rehman , Arslan Shafique , Yazeed Yasin Ghadi , Wadii Boulila, Sana Ullah Jan, Member, IEEE, Thippa Reddy Gadekallu , Senior Member, IEEE, Maha Driss, and Jawad Ahmad , Senior Member, IEEE

摘　要: 早期癌症识别被认为是医疗届在癌症预防方面面临的一个具有挑战性的问题。此外，随着医疗数据共享的需求日益增长，确保医疗数据的隐私保护变得更加困难。本研究提出了一种利用深度学习（DL）的新型非入侵式隐私保护癌症检测方法。最初，用于诊断目的的临床数据利用互联网通过无线信道进行收集。确保个人临床数据的安全至关重要，以防未经授权的用户窃取并利用这些数据谋取个人利益。因此，收集到的数据在通过信道传输之前会进行加密，以防止数据被盗。我们采用了各种安全措施，包括相关性、熵、对比度、结构内容和能量，来评估所提出的加密方法的效率。在本文中，我们提出了使用基于卷积神经网络（CNN）的模型和磁共振成像（MRI）的不同技术，包括迁移学习，微调和 K 折分析癌症检测。为了评估所提出的 DL 技术与决策树（DT）、朴素贝叶斯（NB）、随机森林（RF）和支持向量机（SVM）等传统机器学习方法的性能，我们进行了广泛的实验。结果表明，基于 CNN 的模型取得了 98.9%的准确率，并且优于传统的 ML 算法。进一步的实验证明了这两种加密方案的效率，熵值、对比度和能量分别为 7.9999，10.9687 和 0.0151。

关键词: 癌症诊断;卷积神经网络;混沌模型;数据安全

Manuscript received 10 May 2022; revised 6 July 2022; accepted 7 August 2022. Date of publication 17 August 2022; date of current version 28 October 2022. This work was supported by Prince Sultan University in Saudi Arabia. Recommended for acceptance by Dr. Sahil Garg. (Corresponding author: Thippa Reddy Gadekallu.)

Mujeeb Ur Rehman is with School of Computing, Edinburgh Napier University, EH10 5DT Edinburgh, U.K, and also with the Department of Electrical Engineering, Riphah International University, Islamabad 46000, Pakistan (email: mujeeb.rehman@riphah.edu.pk).

Arslan Shafique is with the Department of Electrical Engineering, Riphah International University, Islamabad 46000, Pakistan (e-mail: arslan.shafique@riphah. edu.pk).

Yazeed Yasin Ghadi is with the Department of Computer Science, Software Engineering, Al Ain University, Abu Dhabi 122612, UAE (e-mail: yazeed. ghadi@aau.ac.ae).

Wadii Boulila is with the Robotics, Internet of Things Lab, Prince Sultan University, Riyadh 12435, Saudi Arabia, and also with the RIADI Laboratory, University of Manouba, Manouba 2010, Tunisia (e-mail: wboulila@psu.edu.sa).

Sana Ullah Jan is with the School of Computing, Edinburgh Napier University, EH10 5DT Edinburgh, U.K. (e-mail: s.jan@napier.ac.uk).

Thippa Reddy Gadekallu is with the School of Information Technology Engineering, Vellore Institute of Technology, Vellore, Tamil Nadu 632014, India (e-mail: thippareddy.g@vit.ac.in).

Maha Driss is with the RIADI Laboratory, University of Manouba, Manouba 2010, Tunisia, and also with the Security Engineering Lab, CCIS, Prince Sultan University, Riyadh 12435, Saudi Arabia (e-mail: mdriss@psu.edu.sa).

Jawad Ahmad is with School of Computing, Edinburgh Napier University, EH10 5DT Edinburgh, U.K (e-mail: j.ahmad@napier.ac.uk).

Digital Object Identifier 10.1109/TNSE.2022.3199235

* 基金项目: 10.13039/501100012639-Prince Sultan University
收稿时间: 2022-05-10; 修改时间: 2022-07-06; 采用时间: 2022-08-07

A Novel Chaos-Based Privacy-Preserving Deep Learning Model for Cancer Diagnosis

Mujeeb Ur Rehman , Arslan Shafique , Yazeed Yasin Ghadi , Wadii Boulila, Sana Ullah Jan, Member, IEEE, Thippa Reddy Gadekallu , Senior Member, IEEE, Maha Driss, and Jawad Ahmad , Senior Member, IEEE

Abstract: Early cancer identification is regarded as a challenging problem in cancer prevention for the healthcare community. In addition, ensuring privacy-preserving healthcare data becomes more difficult with the growing demand for sharing these data. This study proposes a novel privacy-preserving noninvasive cancer detection method using Deep Learning (DL). Initially, the clinical data is collected over the Internet via wireless channels for diagnostic purposes. It is paramount to secure personal clinical data against eavesdropping by unauthorized users that may exploit it for personalized interests. Therefore, the collected data is encrypted before transmission over the channel to prevent data theft. Various security measures, including correlation, entropy, contrast, structural content, and energy, are used to assess the proposed encryption method's efficiency. In this paper, we proposed using the Convolutional Neural Network (CNN)-based model and Magnetic Resonance Imaging (MRI) with different techniques, including transfer learning, fine-tuning, and K-fold analysis cancer detection. Extensive experiments are carried out to evaluate the performance of the proposed DL techniques with regard to traditional machine learning approaches such as Decision Tree (DT), Naive Bayes (NB), Random Forest (RF), and Support Vector Machine (SVM). Results show that the CNN-based model has achieved an accuracy of 98.9% and outperforms conventional ML algorithms. Further experiments demonstrate the efficiency of both encryption schemes, achieving entropy, contrast, and energy of 7.9999, 10.9687, and 0.0151, respectively.

Key words: Diagnosis, convolutional neural networks, chaos, data security.

1 引言

众所周知，癌症很难在早期阶段发现。而且如果在特定阶段后才被发现，癌症在治疗后更容易复发。医学成像分析通常用于检测人体中的异常，如血癌[1][2][3]、皮肤癌[4]、脑肿瘤[5]、肺癌[6]和乳腺癌[7]等。癌症实际上是一种由器官病变引发的肿瘤，被认为是全球范围内导致死亡的主要原因之一[8]。统计数据显示，2018 年一年中约有 1810 万癌症确诊病例，导致 960 万人死亡[9]。这些研究报告指出，肺癌是最主要的死亡原因，占全部死亡人数的 18.4 %。其他死因包括结肠癌(5.8 %)，乳腺癌(6.6 %)，皮肤癌(黑色素瘤与非黑色素瘤) (1.3 %)，前列腺癌(3.8 %)[10]。

早期发现癌症对治疗做出反应的几率更高，因此生存的可能性更大，发病率更低，治疗费用也更低[11]。目前有不同的筛查方法可以检测出身体中表明癌症或癌前病变(出现癌症症状之前)，例如乙型肝炎病毒(Hepatitis B Virus，HPV)检测、醋酸染色肉眼观察(VIA)和乳腺 X 光检查。癌症的主要症状包括疲劳或极度疲劳、进食困难、身体部位肿块或增厚、疼痛、黄疸、咳嗽或声音嘶哑、发烧、头痛以及视力或听力问题等[12]。此外，对癌症预后进行可靠和明确的预测也非常具有挑战性。某些类型的癌症对早期诊断来说更具挑战性，因为它们的症状模糊不清，而且它们在乳房 X 光检查和扫描的诊断迹象也不精确。因此，利用多元数据和高分辨率的诊断方法改进预测模型在临床癌症研究中至关重要[13]。

过去几十年中发展起来的大多数分类模型都是基于监督学习的，其中数据集起着至关重要的作用[14]。这些数据集都是可以被攻击者或者窃听者破坏的图像或文件表格形式。直观上，一系列精确的数据增强了基于监督学习的模型的准确性。因此，数据安全是一个至关重要的方面，可以通过对图像数据进行加密来实现。目前有许多图像加密方法被设计用于保护数字图像，同时这些方法也带来了加密、计算机或安全相关的问题[15] [16] [17] [18] [19] [20] [21]。因此，设计一种能够以较低的计算复杂度为数字图像提供一定安全级别的加密方案是至关重要的。

本文从两个方面对癌症检测模型的隐私保护做出了贡献。首先，通过使用混沌、DWT 和位平面提取方法增强了临床数据的安全性。其次，利用基于 CNN 的深度学习模型开发了癌症诊断模型。MRI 图像的临床数据是在一个诊断中心(中心 A)获得的，然后这些数据通过互联网的无线信道传输到另一个缺乏无创诊断设备的诊断中心(中心 B)。数据可能通过电子邮件传输，电子邮件本身是安全的，但不足以保证数据的隐私性。因此，采用图像加密技术实现 MRI 图像的安全传输。这些图像在接收端使用提出的加密算法的逆版本进行解

密。此外，接收端的病人报告在发送到另一端之前也要经过加密。患者最初的报告是文本格式的，但在发送到传输端之前，必须扫描并转换成图像格式。因此，患者的报告也可以使用所提出的加密算法进行加密。然后将数据输入到提出的非侵入式模型中，用于分类正常者或癌症阳性患者。结果经过加密并发送回诊断中心（中心 A），在中心 A 对其解密后进行会诊。所提出的方法的流程图如图 1 所示。

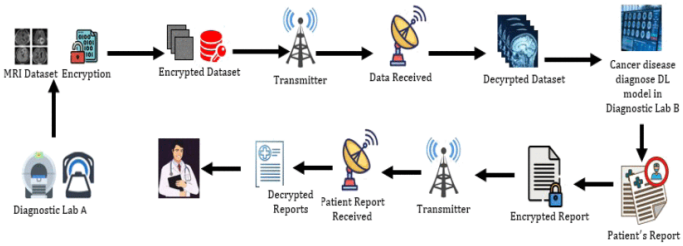


图 1　研究内容概述

本文其余部分的内容组织如下：第一章对加密方案和疾病诊断方法以及漏洞和潜在问题解决方案进行了文献综述。第二章阐述了为确保数据安全而提出的加密方案，第三章和第四章分别介绍了基于 CNN 的癌症诊断模型的理论基础和诊断方法。第五章对实验结果进行了讨论，最后第六章对全文进行了总结。

2　相关工作

传统的加密方案，如高级加密标准（AES）[22]和数据加密标准（DES）[23]，由于数据高度相关且加密轮数较多，并不适合保护图像免受网络攻击。因此，这些方案增加了计算时间，不适合实时应用。此外，在过去的几十年中，机器学习已被广泛用于疾病检测[24][25][26][27][28][29][30]。本章概述了近期文献中现有的图像加密和疾病诊断方法，并在后续章节中给出了解决方案。

2.1　数据加密技术

Romi 等人[31]提出的多轮图像加密被认为是一种安全的多信道方法。具体来说，这种方法旨在处理少量的数据或图像。具有高度相关数据的图像计算时间长、安全性弱都是需要克服的风险。选择性加密可以用于加速整体加密计算速度，同时对这些缺陷保持警惕。为了解决这些问题，Yinan 等人[32]提出了 DNA 折纸加密法（DOC）作为一种安全通信的安全技术。然而，较小的密钥规模使其容易受到暴力破解攻击，但这种策略行之有效，并在整个通信过程中提供了足够的完整性。为了防御暴力破解攻击，Alvazari[33]建议使用 2^{100} 的密钥空间来对抗暴力破解。因此，需要提高密钥的大小来提高安全性。

Li 等人[34]介绍了一种基于混沌的图像加密技术，该技术结合了动态变量选择和轨道扰动过程。为了获得随机数，利用 Logistic 映射和混沌正弦映射扩展密钥空间，使其足以抵御暴力攻击。在保持安全等级的同时，这两种混沌映射[35][36]是按顺序而不是并行实现的。因此，执行时间过长将对实际应用带来许多不便。Sivakumar 等人[37]利用混沌理论生成的扫描模式和真实随机流，提出了一种基于混沌的图像加密方案。采用扫描模式对图像像素进行置换。此外，使用基于光子学的技术创建一个随机密钥，然后使用该密钥执行 XOR 操作，并逐位执行该操作以生成最终的加密图像。由于作者仅通过置换操作降低了他们所提出的加密技术的时间复杂度，因此安全级别被降低主要有两个原因。首先，他们提出的方法仅仅使用了一些基本的数学运算，第二，没有包含扩散操作。根据 Claud Shannon 的混淆和扩散准则[38]，一个加密系统必须同时具有混淆和扩散操作才能是安全的。Kaur 等人[39]提出了一种基于混沌的图像加密方案，该方案利用分段线性混沌映射（PWLCM）产生随机数用于置乱和混淆。与一维混沌映射如混沌 logistic 映射[40]不同，PWLCM 是一种高维混沌映射，其性能优于所有其他一维混沌映射[41][42][43][44]。Kamrani 等人[45]利用两个混沌 logistic 映射提出了一个基于混淆和扩散操作的加密系统。为了加强其提出的加密算法的安全性，作者满足了 Shannon 关于混淆扩散机制的标准。然而，由于这两个过程都是顺序执行的，因此在他们提出的工作中完成所有的数学运

算需要很长的时间。

Rehman 等人[46]提出了一种针对 MRI 和 X 射线等医学影像的图像加密方案，但该方案密钥空间小，缺乏安全性。混沌和替代盒(S-boxes)被用来解决这两个问题。为了扩大密钥空间，使用了多个混沌映射，其中六个密钥参数和每个密钥的灵敏度都是 10^{15}，这意味着总的密钥空间至少要达到 2^{200}，这足以抵抗暴力攻击。此外，S-boxes 根据替换算法对图像像素进行替换，增强了加密图像的安全性。Guodong 等人[47]开发了一种基于频率和空间加密的图像加密方案。离散余弦变换用于频域加密，而替换-置换过程用于空间域加密。该方法能够对数字图像进行快速加密，并在更高层次上对其进行安全保护。统计分析，如相关性，熵，对比度和能量分析，用于证明安全水平。这种方法提供了令人信服的结果，然而，它对噪声或裁剪攻击不具有鲁棒性。在文献[48]中，提出了一种利用 Lyapunov 图、相图和分岔图加密多幅图像的方法。在该方案中，为了保证原始图像的完整性，将大量的灰度照片融合在一起。使用加密轮数众多的超混沌系统，创建随机序列进行置乱，导致较高的加密计算时间。

2.2 基于机器学习的疾病检测

在文献[49]中，Onur 等人提出了一种基于三维卷积神经网络的结节性肺病检测和诊断方法，使用 Kaggle 上公开的数据集来训练模型。在单独开发检测和诊断系统的同时，人们发现将检测和诊断组件连接起来是至关重要的。通过利用这种连接，创建了一个性能更好、更持久的端到端系统，从而避免了结节识别过程中假阳性减少阶段的需要。系统的总体准确率为 95 %，这对于宣誓实例的情况来说是不够的，例如涉及肺癌患者。在[50]中，Rishav 等人讨论了不平衡数据集，以突出其相关问题。例如，他们发现如果一个特定类别的总体案例数量显著高于可接受的数量，这可能会导致不准确的分类。基于迁移学习的图像分类可以用来解决这个问题。

著名的 VGG - 19 也被认为可以提高系统的效率。VGG - 19 是一个卷积神经网络，共有 19 层[51]。这是通过使用 ImageNet 数据集，并应用机器学习技术来识别各种受试者，如乳腺癌患者或正常受试者。为了使采集的正常受试者和患者图像保持接近 1∶1 的比例，共采集了 277 524 张图像。当比较各种方法时，文献[50]提供的方法更优，准确率为 90.3 %。在[52]中，提出了一种基于堆叠稀疏自编码器(Stacked Sparse Autoencoder，SSAE)的深度学习方法，用于在高分辨率的乳腺癌组织病理学图像中有效地检测细胞核。为了确定核团的区分特征，SSAE 仅从像素强度中学习高级特征。图像块由来自自编码器的高级特征表示，然后输入到一个分类器，该分类器将每个图像块分类为核或非核。虽然文献[52]提出的方法能够对其进行分类，但总体准确率为 78.83 %，这在敏感医疗决策中是不可接受的。在文献[14]中，Yi 等人提出了一种使用自动乳腺超声(ABUS) 检测乳腺癌的方法，其中包含了一个 3D 卷积神经网络。具体来说，提出了一种监督方法，使用多层架构对癌症患者和健康受试者进行分类。该数据集由 899 例病例组成，其中 754 例来自癌症患者，144 例来自健康人群。使用准确率、精确率、F1 值、召回率等多个指标对系统性能进行测试。实验结果表明，该系统能够以高达 95 %的准确率进行分类。

除了 CNN，深度信念网络(DBN)、循环神经网络(RNN)和深度玻尔兹曼机(DBM)等几种不同的深度学习模型也被用于疾病诊断等医学应用中。在[53]中，Altan 等人提出了一种使用 DBN 检测乳腺癌的方法，其中使用不同的医学图像作为数据集。为了检测乳腺癌，从数据集中使用的图像中提取统计特征和生理特征。该模型的准确率为 96.4 %，这对于有效地检测恶性疾病来说是相当不充分的。在文献[54]中，Patil 等人使用图像处理、分割和 RNN 从医学图像中检测乳腺癌。此外，为了增强所提出的工作，还集成了一个优化的混合分类器。原始医学图像中含有大量的噪声，因此，对数据集中的图像使用中值滤波去除噪声，使得模型更加优化和准确。Li 等人[55]开发了一个使用 DBM 检测早期癌症疾病的未来预测系统。没有分割或降噪，这降低了他们提出的模型的准确性，这对于实时癌症疾病诊断来说是不可接受的。Antropova 等人[56]提出了一种基于循环神经网络和卷积神经网络的乳腺病变分类技术。训练阶段用于开发长短时记忆(LSTM)。为了捕获病灶增强中的局部变化，从大量预训练的 CNN 中提取特征。此外，将 LSTM 的性能与 CNN 进行比较，LSTM 的性能优于 CNN，他们计划的工作准确率为 93 %。

考虑到文献中指出的挑战，本文提出了新颖的数据加密和疾病诊断技术。下面总结本文工作的主要贡献。

2.3 主要贡献

根据世界卫生组织的报告，有效的癌症检测和诊断对于降低由此造成的伤亡率至关重要[57]。本文的主要贡献如下。

1） 为了增强医疗数据的安全性，提出了一种基于混沌的图像加密技术，并与现有方案进行了比较，证明了所提加密方案的有效性。

2） 主要的临床数据从巴基斯坦拉沃尔品迪和伊斯兰堡的三家医院收集。

3） 我们设计了一种准确预测癌症发生的方法，可以使用智能手机应用程序部署。所提出的技术使用 CNN 作为分类算法。

4） 使用 K - fold 分析和投票技术来选择特定的数据子集，因此，所提出的模型提供了更高的准确性。

5） 除了常用的准确性指标外，还使用了诸如精确率、召回率和 F1 分数等各种性能指标来验证所提出的模型。此外，迁移学习和微调技术用于进一步的性能增强。

3 数据加密方案

本文提出的数据安全算法包含 4 个主要部分：(a)位平面提取，(b)离散小波变换(dwt)，(c)混淆(置换)；和(D)扩散(使用替换盒(S-box)进行替换) 。如文献[58][59][60]所述，基于混沌的加密方案具有对初始条件敏感、难以预测、密钥空间大等优点，比基于频率的加密具有更好的加密效果。因此，基于混沌的加密被用于将所提工作中使用的医疗数据保证其适当的安全程度。文献[61]对基于混沌和基于频率的加密方案进行了数值分析，并且明确指出，基于混沌的加密方案可能比基于频率的加密方案产生更多的随机加密图像。

为了生成随机序列，采用了一维的 Cubic Logistic 混沌映射(CLCM)。这里值得一提的是，高维混沌映射的安全性更高，但是执行起来也需要更多的时间。因此，为了减少时间，在提出的加密算法中考虑了一个低维的混沌映射。然而，为了增强加密医学图像的安全级别，使用了诸如位平面提取、混沌理论、混淆和扩散等多种加密方法。

为了降低所提出的加密方案的时间复杂度，只考虑低频段和最高有效位平面。因为低频段和最重要的比特包含了大部分的明文信息。所提出的加密技术的框图如图 2 所示，图 3 分别为原始图像和对应的 4 幅加密图像。

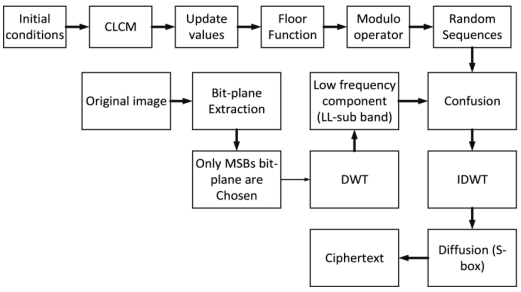


图 2 所提出的加密技术框图

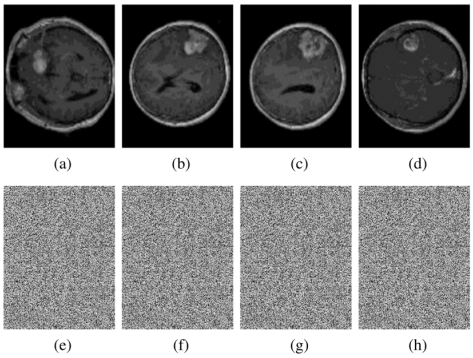


图 3 原始图像及其对应的加密图像

3.1 位平面提取

从原始图像中提取二值平面的过程称为位平面提取。位平面提取的理论表示如式(1)所示：

$$\mathbf{I}=\frac{1}{2^{\mathbf{L}}}\sum_{a=0}^{2^{\mathbf{L}}-1}\sum_{b=0}^{2^{\mathbf{L}}-1}I_{a,b}^{\mathbf{L}}\times 2^{\mathbf{L}} \tag{1}$$

其中 $\mathbf{L}$ 代表二进制位平面的总数，其数值范围：$\left\{L|\ L\in W\wedge 0\le n\le 7\right\}$ 。单个位平面可提取为 $\mathbf{I}_{a,b}^{'7}\times 2^7$，$\mathbf{I}_{a,b}^{'6}\times 2^6$，$\mathbf{I}_{a,b}^{'5}\times 2^5$，$\mathbf{I}_{a,b}^{'4}\times 2^4$，$\mathbf{I}_{a,b}^{'3}\times 2^3$，$\mathbf{I}_{a,b}^{'2}\times 2^2$，$\mathbf{I}_{a,b}^{'1}\times 2^1$ 和 $\mathbf{I}_{a,b}^{'0}\times 2^0$。其中 $I_{a,b}^{'7}\times 2^7$ 代表第 8 个位平面，以此类推。如图 4 所示，每个位平面中的明文信息量可能各不相同。

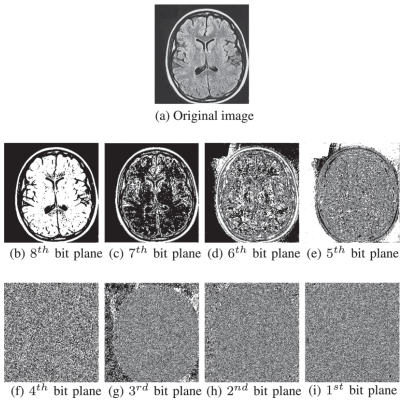


图 4 从原始图像中提取的二元平面

第 8 位包含的明文信息比例最高，第 1 位包含的明文信息最少。表 I 显示了各个位平面所含信息的百分比，可以用（2）[62]来确定。

$$\mathbf{I}=\frac{2^{\mathbf{L}-1}}{\sum_{\mathbf{L}=0}^{7}2^{-1}} \tag{2}$$

表 1 单个二进制位平面的信息量百分比

位平面索引	信息量百分比	位平面索引	信息量百分比
0	0.3000	4	6.2500
1	0.7900	5	12.2300
2	1.4200	6	25.7000
3	3.1200	7	50.2000

从提取的所有二进制位平面中重建原始图像形式如下：：

$$[b]\mathbf{I}_{a,b}=\mathbf{I}_{a,b}^{'7}\times 2^7+\mathbf{I}_{a,b}^{'6}\times 2^6+\mathbf{I}_{a,b}^{'5}\times 2^5+\mathbf{I}_{a,b}^{'4}\times 2^4+$$

$$\mathbf{I}_{a,b}^{'3}\times 2^3+\mathbf{I}_{a,b}^{'2}\times 2^2+\mathbf{I}_{a,b}^{'1}\times 2^1+\mathbf{I}_{a,b}^{'0}\times 2^0 \tag{3}$$

原始图像的大部分信息都存在于第 8 个二进制位平面。因此，为了提高图像的安全性，其余的加密步骤只考虑最重要的二进制位面（第 8、7、5 和 4 位平面）。

3.2 离散小波变换

可以利用小波变换可以提取信号的小波分量。利用小波可以分离出音频信号的精确特征[63]。例如，小波可以用来从低频分量中分离出精细的细节(边缘)。小波函数和大波函数分别用于分离细、粗细节。

所提出的加密技术使用 Haar 小波将明文转换为各种频率。可以通过应用离散小波变换(DWT)对明文图像进行分解来提取 LL 、 LH 、 HL 和 HH 等子带。

Harr 小波可以表示为 $W = HOH^T$ 。其中， O 表示具有相同行数（R）和列数（C）的原始图像， H 表示与原始图像大小相等的 Harr 变换矩阵， W 表示持有 Harr 基函数 $h_f(z)$ 的变换矩阵，其中 $z \in [01]$ 和 b 可定义为 $b \mid b \in N \wedge 0 \le b \le C-1$ 。可以用（4）对其进行唯一分解。

$$b = 2^e + s \tag{4}$$

这里， e 和 s 分别代表 2 的最大幂和余数（ $s = 2^e$ ）。根据 (5)，haar 有一个基函数。

$$h_b(z) = \frac{1}{\sqrt{C}} \begin{cases} 1 & \text{if } b = 0 \ \ \& \ \ 0 \le f < 1 \\ 2^{e/2} & \text{if } b > 0 \ \ \& \ \ s/2^e \le f < \dfrac{s+0.5}{2^e} \\ -2^{e/2} & \text{if } b > 0 \ \ \& \ \ (s+0.5)/2^e \le f < \dfrac{s+1}{2^e} \\ 0 & \text{anywhere} \end{cases} \tag{5}$$

(6) 提供了变换内核的逆版本，将其替换可生成二维离散哈尔小波变换 (DHWT)。

$$h'(z,b) = \frac{1}{\sqrt{C}} h_b(z/M) \quad for\ z = 0,1,2,\ldots,C-1 \tag{6}$$

其中， $h_a(w)$ 的定义为：

$$h_b(z) = H' = \begin{Bmatrix} h_0(\frac{0}{C}) h_0(\frac{1}{C}) \ldots h_0(\frac{C-1}{C}) \\ h_1(\frac{0}{C}) h_1(\frac{1}{C}) \ldots h_1(\frac{C-1}{C}) \\ h_2(\frac{0}{C}) h_2(\frac{1}{C}) \ldots h_2(\frac{C-1}{C}) \\ \cdot \quad \cdot \quad \cdot \\ \cdot \quad \cdot \quad \cdot \\ \cdot \quad \cdot \quad \cdot \\ h_{C-1}(\frac{0}{C}) h_{C-1}(\frac{1}{C}) \ldots h_{C-1}(\frac{C-1}{C}) \end{Bmatrix} \tag{7}$$

最后， $b = 0,1,2,\ldots,C-1$ 的变换矩阵为：

$$H = \frac{1}{\sqrt{C}} H' \tag{8}$$

在二维信号（$I(R,C)$ 图像）的情况下，使用高通和低通滤波器对水平方向上的每个像素行进行评估，结果是图像 L_r 和 H_r，大小为 $\frac{R}{2^1}\times\frac{C}{2^1}$。然后，使用高通和低通滤波器对新图像（$L_r$ 和 H_r）进行垂直方向的分析，称为 $\alpha(C)$ 和 $\beta(C)$。由此产生 LL_1、LH_1、HL_1 和 HH_1 频子带。图 5 显示了应用 2DHWT 后产生的四个频率子带。

(a) Original image

(b) LL (c) LH (d) HL (e) HH

图 5 使用 DWT 从摄影师图像中提取的频带

3.3 混淆过程

如图 5 所示，低频子带(LL 子带)包含了原始图像中的大部分信息。因此，在所提出的加密方案中，混淆过程仅在该子带上进行，以减少加密所需的整体计算时间。通过结合算法 1，根据使用混沌生成的随机序列应用混淆过程。

算法 1：随机序列生成模块

1：输入 CLCM 和随机数种子值（η_1，ζ_1（用于在行中创建混淆），η_2 和 ζ_2（用于在列中创建混淆），其中 $\zeta\in$（0 1）和[1.41 1.63)）。CLCM 方程如下：

$$\zeta_{i+1}=\eta*\zeta_i(1-\zeta_i)*(2+\zeta_i) \tag{9}$$

2：输出：τ = mod (σ , 256)

3：利用输入生成与 $LLsub-band$ 带中行数相等的随机值。

4：将随机值存储在一个数组中，假设为 K 。

5：更新 K 如下：

$$\varrho=K_i\times D_{num}$$

D_{num} 可以是任何大数字，例如 999。

6：要将小数值转换为实数，请应用向下取整函数。

7：要将值限制在 [0 255] 范围内，请对应用向下取整函数后生成的值取模，将整数值保存在数组中（σ）。

8：将 τ 序列应用在行和列中造成混乱 $LLsub-band$ 带。行列置乱的随机序列如图 6 所示。

9：结束

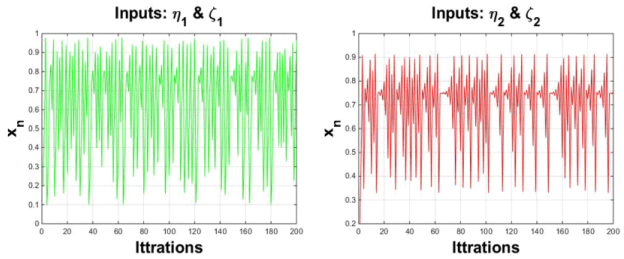


图 6 使用 CLCM 生成的随机序列

3.4 置换过程

由于混淆的比特平面由几个频率组成，因此需要使用逆离散小波变换（IDWT）将它们转换为八位整数值，以进行替换过程。这些整数值将被表 2 中给出的 S 盒值所取代。在提出的工作中使用的 S 盒是由 Hussain 等人提出的[64]。替换过程在示例 1 中解释：

表 2 S-Box 值

254	132	255	222	122	15	53	115	145	150	225	175	78	64	184	93
87	19	27	95	246	252	113	59	228	207	101	180	161	154	152	149
238	85	229	91	89	37	26	143	114	123	0	190	51	164	75	237
249	240	82	28	196	209	230	203	105	6	31	217	72	118	226	176
42	253	116	108	163	120	80	131	221	16	97	8	88	153	169	170
198	34	11	21	46	247	67	20	125	36	76	155	104	102	128	179
139	214	148	50	121	12	158	216	189	210	185	232	197	110	231	146
5	109	244	127	77	3	1	107	174	117	181	61	142	124	168	172
41	62	239	29	10	58	25	66	151	47	52	43	212	79	191	173
200	65	39	242	7	166	233	201	219	74	177	144	71	183	63	171
137	2	204	24	14	248	73	135	81	17	178	136	157	167	156	165
9	35	130	235	90	40	133	251	182	140	193	100	55	79	220	162
86	213	23	70	111	194	245	38	186	4	224	147	22	223	98	159
250	112	84	141	18	57	160	205	60	199	99	211	13	92	94	187
40	56	241	234	54	68	33	126	45	138	32	48	206	208	96	188
202	69	30	106	134	227	83	236	192	129	103	215	243	218	119	195

示例 1：让我们来看一张在进行 IDWT 后生成的图像的一小部分：

$$I=\begin{bmatrix} 80 & 156 & 205 \\ 246 & 90 & 50 \\ 183 & 120 & 165 \end{bmatrix}$$

将图像 I 的像素值转换为二进制值：

$$\begin{bmatrix} 01010000 & 10011100 & 11001101 \\ 11110110 & 01011010 & 00110010 \\ 10110111 & 01111000 & 10100101 \end{bmatrix}$$

将每个像素的所有八位转换为包含每组四位的两组。

$$\begin{bmatrix} \{(0101),(0000)\} & \{(1001),(1100)\} & \{(1100),(1101)\} \\ \{(1111),(0110)\} & \{(0101),(1010)\} & \{(0011),(0010)\} \\ \{(1011),(0111)\} & \{(0111),(1000)\} & \{(1010),(0101)\} \end{bmatrix}$$

$$\begin{bmatrix} \{R:5,C:0\} & \{R:9,C:12\} & \{R:12,C:13\} \\ \{R:15,C:6\} & \{R:5,C:12\} & \{R:3,C:2\} \\ \{R:11,C:7)\} & \{R:7,C:8\} & \{R:10,C:6\} \end{bmatrix}$$

用相应的 S 盒值替换数值，以在输入数值中创建扩散。加密后的矩阵将是：

$$\begin{bmatrix} 198 & 71 & 79 \\ 83 & 104 & 82 \\ 251 & 174 & 73 \end{bmatrix}$$

所提出的加密方案选择低频带和最显著的比特平面的目的是为了减少整体加密计算时间。低频带和最显著的比特包含大部分明文信息。因此，除了 LL 子频带和最显著的比特平面之外，没有必要加密所有子频带和比特平面。

接收端不会有信息丢失，因为 DWT 和比特平面提取方法都具有逆过程，能够恢复数字图像的确切像素值，原始信息正在被恢复。

4 卷积神经网络

近年来提出了几种利用机器学习（ML）算法检测肿瘤的方法[65][66][67]。从文献中可以看出，使用 ML 算法达到的准确性是不可接受的。因此，一种称为 CNN 的深度学习算法被用来增强所提出的分类任务的性能。

CNN 在近年来主导了机器视觉领域。CNN 包括多个层：隐藏层、输入层和输出层。CNN 通常使用卷积、池化、全连接和归一化层作为隐藏层。额外的层可能用于更高级的模型。图 7 展示了传统 CNN 的示例[68]。

在卷积神经网络的学习过程中，可以应用向量微积分和链式法则。

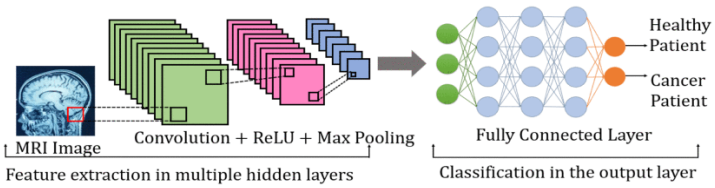


图 7 CNN 网络结构

将 $x \in R^X$ 和 S 视为向量，任意标量 $(i.eS \in R)$。则 S 对 w 的偏导数为：

$$\frac{\partial S}{\partial w} = \frac{\partial S}{\partial w_i} \tag{10}$$

w 和 $\frac{\partial S}{\partial w}$ 将具有相同的大小，$\frac{\partial S}{\partial w}$ 是第 i^{th} 个元素。此外，假设 $\mathbf{N} \in R^L$ 且 $\frac{\partial S}{\partial w^R} = \frac{\partial S}{\partial w})^R$。对于这种情况，$S$ 的偏导数将如下：

$$\left[\frac{\partial w}{\partial \mathbf{N}^R}\right]_{il} = \frac{\partial w_i}{\partial \mathbf{N}_i} \tag{11}$$

在（12）中定义。而 $\frac{\partial S}{\partial \mathbf{N}^R}$ 可以使用链式法则确定。

$$\frac{\partial S}{\partial \mathbf{N}^R}=\left[\frac{\partial S}{\partial \mathbf{N}^R}\right]\left[\frac{\partial w}{\partial \mathbf{N}^R}\right] \tag{12}$$

结果 $u,\mathbf{N}^1\rightarrow L^1,\mathbf{N}^2\rightarrow L^1,\cdots\mathbf{N}^L\rightarrow T^L=S$ 之间的差异和 $CNN's\ \mathbf{N}^M$ 可能通过使用损失函数即 $S=\left|u-\mathbf{N}^M\right|^2$ 来确定。因此，卷积被表述为：

$$w_{i^{k+1}.l^{l+1},c}=\sum_{i=0}^{Q}\sum_{l=0}^{L}\sum_{c=0}^{\mathbf{E}}h_{i.l.c}\times\mathbf{N}^M_{i^{k+1}+i,l^{k+1}+l,c} \tag{13}$$

卷积大小取决于滤波器的大小。即如果滤波器（ h ）的大小为（ $O\times L\times\mathbf{E}^k$ ），则卷积的大小将是：$(O-O+1)\times(L^k-L+1)$，其中 $\mathbf{E}$ 片表示在 $Q^{O^{k+1}\times L^{k+1}\times\mathbf{E}^{k+1}}$，$O^{k+1}=O^k-O+1$，$L^{k+1}=L^k-L+1$，$\mathbf{E}^{k+1}=\mathbf{E}$ 中的 $z(w^{k+1})$。

方程（14）可用于计算每个符号 $T\in\{1,2,3,\cdots T\}$ 在每个训练事件中出现的概率。

$$O(T\mid\mathbf{N})=\frac{exp(ST)}{\sum_{i}^{T}exp(S_i)} \tag{14}$$

在这里，非归一化对数概率由 S 表示。而所提出模型的交叉熵可以如下确定：

$$Entropy=\sum_{T=1}^{T}log(p(T)q(T)) \tag{15}$$

由于交叉熵损失在逻辑斯蒂克 S_T 中是可微的，所以可以实现对深度模型进行梯度训练。梯度范围从-1到+1，可能性增加了正确分类的机会。 过拟合梯度是 $\frac{\partial k}{\partial S_T}$。如果将交叉熵保持在尽可能低的水平，过拟合可以通过检查标签分布来避免，这些标签与具有平滑参数 eta 的训练示例 v(t)无关，其中 $p(T\mid\mathbf{N})=\ \sigma T,\mathbf{N}'$ 被修改如下：

$$p^{'T|\mathbf{N}}=(1-\eta)\varpi_{T,\mathbf{N}}+\eta\Xi(T) \tag{16}$$

$p^{'T|\mathbf{N}}$ 是 $q^{S|N}$ 和稳定分布 $\Xi(T)$ 的组合，其权重分别为(1 - η)和 η。当使用 $\Xi(T)\ =\ \frac{1}{T}$ 进行标签平滑

正则化时，$p^{'T|\mathbf{N}}$ 变为：

$$p^{'T|\mathbf{N}} = (1-\eta)\varpi_{T,\mathbf{N}} + \frac{\eta}{S} \tag{17}$$

方程（17）可以表示为熵的函数，如下所示：

$$q(p^{'},r) = -\sum_{t=1}^{J} log(p(t))p^{'(t)} = (1-\eta)q(p^{'},r) + \eta P(u,q) \tag{18}$$

换句话说，标签平滑正则化等同于通过用两个损失替换单个交叉熵损失来计算 Kullback-Leibler 散度，一个用于 $\mathbf{G}(p,r)$ 和一个用于 $\mathbf{G}(s,r)$ 。第二个损失惩罚预测的标签分布 r 偏离先验分布 s 的量，等于 $\frac{\eta}{(1-\eta)}$ 的形式化。在文献[69][70]中，可以找到其他 CNN 架构的数学公式。

4.1 迁移学习

脑肿瘤、肝肺疾病和其他疾病等预测任务可以通过使用迁移学习进行预测。也就是说，来自一个情境的数据可能被用于提高另一个情境的绩效。当预训练模型所使用的新数据集小于原始数据集时，迁移学习经常被使用。利用在 ImageNet 上训练的 Inception - v3 模型在新的数据集上学习特征进行训练是本项目(CIFAR - 10 和加州理工学院 Faces)的目标[71]。从 ImageNet 上获取的特征开始，使其适应新的数据集或任务，而不是从一开始就随机初始化权重，这是迁移学习的一个优势[72]。

4.2 微调技术

为了识别 ImageNet 中的 1000 个通用对象类，对提出的模型进行了修改。迁移学习是网络微调的基础。我们可以通过加强分类函数以减少错误来训练 CNN 学习各种领域的特征[73]。然后，在更新分类函数时，微调网络以减少更窄范围内的错误。在这种配置中，网络的功能和特性被分配给专门的领域。

CNN 分类功能，通常被称为“softmax”，在计算 ImageNet 数据集的 1000 个类别的可能性时使用。为了开始微调过程，在 softmax 分类器中删除旧值，并用新的随机值替换。然后使用反向传播技术和大量的癌症患者数据集从头开始训练一个新的 softmax 分类器。

每一层的学习率在进行微调的反向传播过程之前必须正确校准，这一点至关重要。为了本研究的目的，我们将顶部分类层的学习率增加到 10，将接下来的七个分类层的学习率降低到 0.1。使用反向传播技术优化网络参数，总共完成了五千轮次的随机梯度下降（SGD）[74]。

5 数据与方法

所提出的非侵入性癌症诊断方法补充了现有的诊断工具和机制，并帮助医学从业者更可靠和准确地诊断癌症。该数据集包含 4800 张经过认证的 MRI 图像，将用于计划中的研究。正常患者的 MRI 图像与出现肿瘤的图像不同。MRI 图像中的肿瘤具有不同的颜色强度，如图 8 所示。

图像被分成训练图像和患者测试图像。在开始分析 MRI 扫描之前，所有 X 光片都经过质量控制检查，任何质量低劣或无法阅读的扫描都被淘汰。随后，两名专业人员评估了这些图像，然后才被接受用于 AI 系统。最后，第三位专家检查了评估集，以确保不存在任何评分问题。

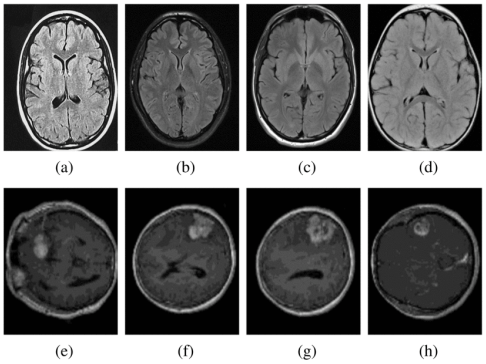


图 8 (a-d) 正常患者图像 (e-h) 癌症患者图像

所提出的工作旨在对健康和癌症患者进行分类，从而将他们彼此区分开来。为了达到这种分类，对分类性能进行了评估。图 9 给出了本文工作的结构示意图。

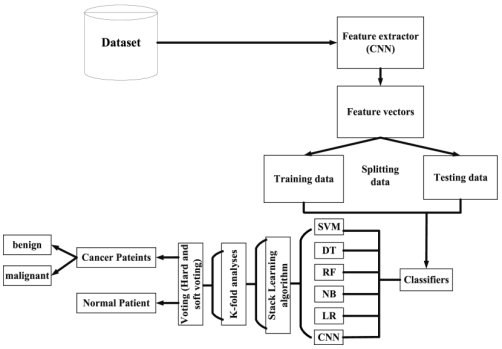


图 9 所提出的癌症诊断模型流程图。

数据是通过磁共振成像（MRI）扫描收集的。各种 MRI 扫描的尺寸不同；例如，A 和 B 分别表示图像像素的行和列。

图像预处理：图像预处理阶段对于生成清晰和清晰的图像至关重要。图像的预处理允许分类阶段。首先，主要使用了数据增强过程。该过程通过对初始输入执行多种转换来扩展数据集的容量。输入使用了几种转换技术进行复制，包括平移、对称和旋转。以下提到了预处理和增强所涉及的阶段。

图像被调整大小到特定的像素计数，并按指定方向定位。

居中每个图像的行和列都从其边缘移除。因此，可以获得各种尺寸的图像。随后，整个行和列宽度被剪裁，并统计图像的总数。

分割：需要提取和分类高质量图像。在对高分辨率图片进行分割时，出现了光谱混淆，描绘受损，图像精度降低的情况。此外，为了增强这一点，采用了面向对象的图像分割方法，从图像中去除盐和噪音，同时通过使用对象结构和光谱特征来提高其精度。

特征提取：通过使用各层提供的滤波器来检索特征。第一层（卷积和池化）中的滤波器用于提取低级特征，而高级特征则在上层卷积层中提取。

为每个 X 射线图像制作了不同的特征向量 $Z.V = Z_1, Z_2, Z_3 \cdots Z_{14}$。

提供的矩阵（ $Z.Vs$ ）仅包含从 MRI 扫描中收集的统计特征表示的向量。这些特征可以在单个数据集中表示，如（19）所示。

$$\begin{cases} Z.V_1 = Z_1, Z_2, Z_3 \ldots Z_{14} \\ Z.V_2 = Z_1, Z_2, Z_3 \ldots Z_{14} \\ Z.V_3 = Z_1, Z_2, Z_3 \ldots Z_{14} \\ \vdots \\ Z.V_n = Z_1, Z_2, Z_3 \ldots Z_{14} \end{cases} \tag{19}$$

这些检索到的特征随后通过全连接层的帮助发送给分类器进行决策。

数据集被分为两部分用于训练和测试。训练数据集包括健康和肺炎感染患者的组合，并且使用 CNN 对模型进行了训练。根据（20）中指定的，将近 80%的数据集被随机选择用于训练，考虑到健康和受污染的数据类型。用于训练和测试目的的数据的精确分配可能会有所不同。

此外，我们使用迁移学习和微调来提高建议模型的准确性。在微调后，模型的准确性被确定为 98%。此外，还添加了 K 折分析和投票程序以提高建议模型的准确性，最终成功达到 99.7%。

5.1 K折分析

K-fold 验证的目的是通过选择不同的 K 值（K = 10、K = 15、K = 20、K = 25、K = 30）来测试所提出的模型。这种验证方法利用数据集从整个数据集中选择不同的训练数据来训练模型。例如，如果 K 值为 10，将执行总共十次迭代，其中整个数据集的十分之一将被选中用于测试目的。即，在第一次迭代中，数据集的第 1 个 1/10 部分将用于测试目的。类似地，在第二次迭代中，第 2 个 1/10 部分将用于测试，而剩余的数据将用于训练。数学上可以写成：

$$\begin{cases} \text{if} \\ \text{Total test instances} \quad \text{T= 5000} \\ \text{Traininginstances} \quad \text{(Total instances) - (5000)} \end{cases} \tag{20}$$

当 K 设置为 10 时，评估模型时，将数据集分成十个部分。每个部分将在每次迭代中用作测试数据集。

5.2 表决技术

它是一个元分类器，结合了等效或优秀的机器学习分类器用于分类和检测[75]。它也被称为“集成投票分类器”。集成投票分类器分别用于进行“硬”和“软”投票。

(1) 硬投票

绝大多数投票的最简单示例是硬集成投票，这是最常见的投票方式。该策略基于获得多数票[76]。例如，在建议的研究中，为了提高模型的准确性，采用 k-fold 分析将事件分类为两类，具体取决于获得的多数票：A 和 B。图 10 显示了所有 k 个模型的准确性，可以观察到大多数模型更喜欢 A 类而不是 B 类。因此，在经过严格投票后，即将到来的样本将被分类为 A 类。所提出的工作应用的硬投票的详细流程图如图 10 所示。

(2) 软投票

分类器的预测概率，用 p 表示，用于预测哪些类别将被选中。图 11 描述了基于单个 k 模型[77]结果的特定类型发生概率的各种可能性。方程 21 可用于确定每个类别发生的概率。

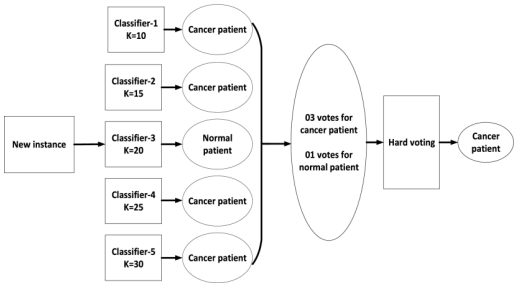


图 10 使用硬投票进行分类

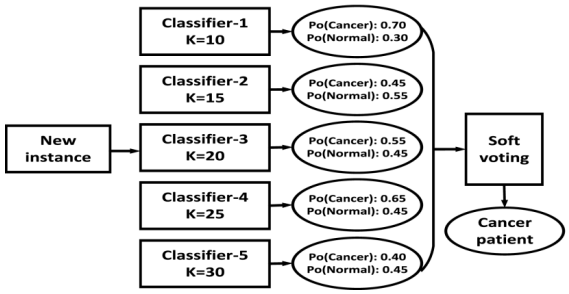


图 11 使用软投票进行分类

$$\text{Class cancer}(\mathbf{C}) = \frac{Po(\mathbf{C})_1 + Po(\mathbf{C})_2 + \cdots + Po(\mathbf{C})_N}{N} \tag{21}$$

$$\text{Class normal}(\mathbf{N}) = \frac{(\mathbf{N})_1 + Po(\mathbf{N})_2 + \cdots + Po(\mathbf{N})_N}{N} \tag{22}$$

$$\text{Class}(\mathbf{C}) = \frac{0.70 + 0.45 + 0.55 + 0.65 + 0.40}{5} \times 100 = 55 \tag{23}$$

$$\text{Class}(\mathbf{N}) = \frac{0.30 + 0.55 + 0.45 + 0.35 + 0.60}{5} \times 100 = 45\% \tag{24}$$

6 结果与讨论

下文解释了不同的性能测量参数，以评估所提出的两种模型的性能，包括用于数据安全的加密方案和用于癌症诊断的检测模型。

6.1 加密方案分析

为了分析和比较所提出的加密方案与现有技术，进行了熵、能量、相关性、同质性、结构内容和直方图分析等安全参数的分析。数学表示和与强安全性的关系在表 3 种给出，文献[78] [79] [80] [81] [82]中给出了类似分析的更多细节。从表 3 中可以看出，所提出的加密方案的安全数值比现有的方案要好许多。这是因为使用了大量的 DWT，混沌呵位平面提取方法来提高所提出的加密方案的性能。此外，DWT 和位平面提取的使用使得所提出的加密过程通过仅加密低频带呵最重要的位。表 4 中的结果表明，所提出的加密方案比现有的方案性能更好。

表 3 性能测量参数

参数	数学表达式	与强安全性的关系(S.S)	变量解释
Entropy	$Ent = -\sum O(p_i)\log_2 en(c_i)$	$Entropy \propto S.S$	$O(p_i)$ 表示发生的概率
Energy	$Energy = \sum O(a,b)^2$	$Energy \propto \frac{1}{S.S}$	$O(a,b)$ 表示一个原始图像

Correlation	$Co=\frac{\frac{1}{L}\sum_{j=1}^{L}(x_i-En(a))(y_i-En(b))}{\sigma_a\sigma_b}$ $\sigma_a=\sqrt{VARa},\sigma_b=\sqrt{VAR_b}$ $VAR(a)=\frac{1}{L}\sum_{j=1}^{L}(a_i-E(a))^2$ $VAR(b)=\frac{1}{L}\sum_{j=1}^{L}(b_i-E(b))^2$	$Correlation\propto\frac{1}{S.S}$	L:总像素 $E(a)$ 和 $E(b)$ 表示加密图像的水平和垂直方向
Contrast	$Cont=\sum\|a-b\|^2\ O(a,b)]$	$Contrast\propto S.S$	$O(a,b)$表示灰度同现矩阵
Homogeneity	$\sum_a\sum_b\frac{O(a,b)}{1+\|a-b\|}\Big]$	Homogeneity $\propto\frac{1}{S.S}$	//
S.C	$Sc=\frac{\sum_{a=1}^{M}\sum_{b=1}^{N}[O(a,b)]^2}{\sum_{a=1}^{M}\sum_{b=1}^{N}[En(a,b)]^2}$	$S.C\propto\frac{1}{S.S}$	En 表示加密图像

表 4 安全分析统计值

	Proposed work						
Encrypted MRI images	Homogeneity	SC	Entropy	Correlation	Energy	Contrast	Execution time (sec)
Normal MRI image$_1$	258	18	7.9992	0.0001	0.154	9.2413	0.021
Normal MRI image$_2$	259	15	7.9991	-0.0054	0.0156	10.7891	0.020
Normal MRI image$_3$	260	16	7.9988	0.0010	0.0155	10.1584	0.025
Normal MRI image$_4$	251	16	7.9991	0.0001	0.0155	10.7914	0.027
Cancer MRI image$_1$	251	19	7.9991	-0.0035	0.0152	10.7341	0.029
Cancer MRI image$_2$	256	17	7.9997	0.0006	0.0151	10.7982	0.030
Cancer MRI image$_3$	251	16	7.9992	-0.0015	0.0155	10.1351	0.022
Cancer MRI image$_4$	260	15	7.9990	0.0004	0.0154	10.7546	0.025
Average	260	15	7.9990	0.0004	0.0154	10.7546	0.025
	Comparison						
Existing schemes	MSE	PSNR	Entropy	Correlation	Energy	Contrast	Execution time (sec)
Ref [83]	249	20	7.9953	-0.0015	0.0156	9.9882	1.361
Ref [84]	248	25	7.9959	0.0006	0.0155	9.9783	1.399
Ref [85]	249	23	7.9925	-0.0075	0.0160	9.9944	2.978
Ref [86]	248	26	7.9944	-0.0050	0.0159	9.6986	2.036
Ref [87]	247	21	7.9972	0.0009	0.0158	9.9973	2.971

6.2 直方图分析

直方图可以显示图像上的像素分布[88]，图 12 表示具有多个峰值的原始图像的直方图。如图 12 所示，加密图像的像素分布均匀。加密图像的直方图必须接近平坦，并区分于原始图像的直方图，以提供安全的加密过程。从图 12 中可以明显看出，所提出的加密方案确实提供了令人满意的结果，并且满足直方图测试的最低要求。评估 ML/DL 检测系统得性能指标包括癌症检测的准确率、特异性/精确度、灵敏度、召回率、F1 评分和 AUC。对于这样的检测模型，不同的性能标准可能导致不同的结论。例如，在准确度方面，这通常是任何分类系统得主要评估措施，如果一个模型能够正确地进行模式识别，则可以获得极好的结果。表 5 列出了不同得性能参数及其相应的数学方程。

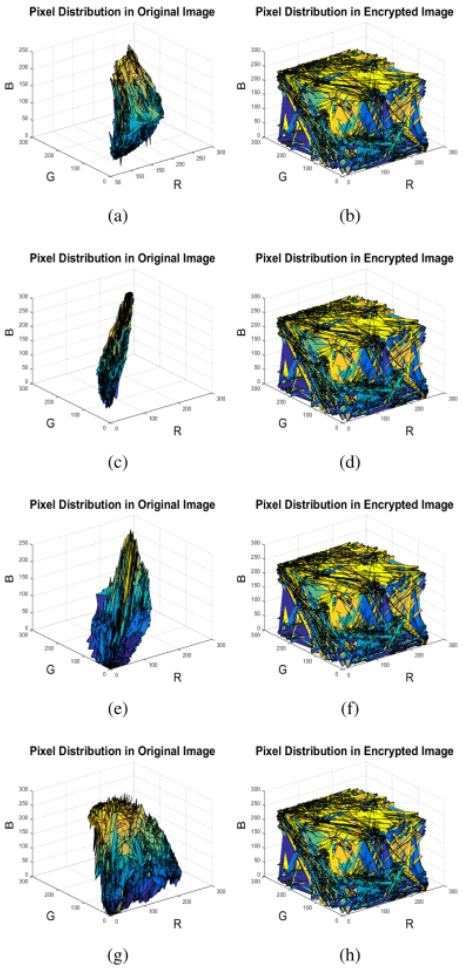


图 12 原始图像和加密图像中的像素分布

Total No. of Patients: 5000	Predicted NO (Normal Patient)	Predicted Yes (Cancer disease)
Actual NO (Normal Patient)	TP: 4364	FP: 85
Actual yes (Cancer disease)	FN: 55	TN: 496

(a) Confusion matrix for CNN model

Total No. of Patients: 5000	Predicted NO (Normal Patient)	Predicted Yes (Cancer disease)
Actual NO (Normal Patient)	TP: 4379	FP: 133
Actual yes (Cancer disease)	FN: 85	TN: 491

(b) Confusion matrix for Transfer model

Total No. of Patients: 5000	Predicted NO (Normal Patient)	Predicted Yes (Cancer disease)
Actual NO (Normal Patient)	TP: 3986	FP: 53
Actual yes (Cancer disease)	FN: 62	TN: 899

(c) Confusion matrix for Fine Tuning model

图 13 CNN、迁移学习和微调的提出模型的混淆矩阵

表 5 性能评估指标

指标参数	数学表达式
Accuracy	$\frac{\Gamma_P+\Gamma_N}{\Gamma_P+F_P+_N+F_N}$
Specificity/precison	$\frac{\Gamma_P}{\Gamma_P+F_N}$
Sensitivity	$\frac{\Gamma_N}{\Gamma_{N+F_P}}$
F1--Score	$2\times\left[\frac{\text{Sensitivity}\times\text{Specificity}}{\text{Sensitivity}+\text{Specificity}}\right]$

在表 5 中，分别代表真阳性，真阴性，假阳性，假阴性。这些术语的定义如下：

真阳性：表示患者患有癌症，并且模型正确检测出其患有癌症的情况。

真阴性：表示患者实际上未患有癌症的情况，并且模型正确地将其识别为健康的情况。

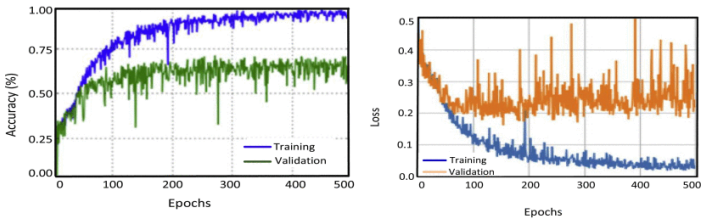
假阳性：表示患者是健康的，但模型将其识别为受癌症影响情况的情况。

假阴性：表示患者患有癌症的情况，然而模型将其识别为健康的情况。

表 5 中给出的参数可以使用混淆矩阵（包含的 2 维阵列）来确定。图 13 中给出了所提出的具有迁移学习呵微调的模型的混淆矩阵。此外，所提出的方案和现有方案的统计值表如表 6 所示，表面所提方案比现有方案更可靠。许多现有的模型，如 CNN，RF，NB 和 SCM，都被用来确定哪一个性能更好。近年来，已经提出了几种使用机器学习算法进行肿瘤检测的方法。根据文献，通过机器学习算法获得的准确度并不令人满意。因此，一种被称为 CNN 的深度学习技术被建议用来提高分类任务的性能。如表 6 所示，当使用 CNN 时，可以达到 97.2％的准确度。当 RF，NB 和 SVM 分别给出 98％，90％和 15％的准确度时，这反映出 CNN 时所提出的模型中更好的选择。除了 CNN，还分析了几种深度学习算法，如循环神经网络（RNNs）[89]，深度玻尔兹曼机（DBMs）[90]和深度信念网络（DBNs）[91]，以比较它们与 CNN 的性能。表 6 中给出了每个参数对应的不同统计值，表明 CNN 在其中具有更高的准确性。此外，精度和损失曲线如图 14 所示，最小损失表明所提出的模型在准确预测类别方面的能力。

表 6 所提出的方法与现有方法的性能比较

Schemes	CNN	Tranfer Learninng	Fine Tuning	DBN	RNN	DBM	RF	NB	SVM (sigmoid kernel)	SVM (linear kernel)	SVM (rbf kernel)	SVM (polynomial kernel)
								Accuracy (Ac_y)				
Proposed	97.2	97.4	97.7	95.3	95.6	97.1	98	90	15	53	95	96
Ref [92]	91	81	89	88	87	85	90	90	92	91	84	86
Ref [93]	86	93	92	90	89	91	.92	91	92	92	91	92
Ref [94]	95	75	77	78	79	86	79	73	74	82	84	86
Ref [95]	85	83	82	90	92	88	89	92	93	91	92	97
Ref [96]	92	86	82	86	82	90	92	92	94	91	92	93
								Precision ($Prec_y$)				
Proposed	0.97	0.98	0.98	0.96	0.95	0.93	0.89	0.99	0.32	0.35	0.99	0.97
Ref [92]	0.84	0.92	0.900.	0.79	0.86	0.89	0.85	0.86	0.87	0.89	0.92	0.89
Ref [93]	0.92	0.95	0.93	0.90	0.90	0.89	0.96	0.93	0.93	0.95	0.98	0.99
Ref [94]	0.97	0.95	0.96	0.95	0.93	0.90	0.98	0.96	0.99	0.98	0.99	0.98
Ref [95]	0.89	0.88	0.87	0.88	0.90	0.93	0.84	0.92	.97	0.98	0.97	0.98
Ref [96]	0.89	0.88	0.87	0.88	0.91	0.93	0.84	0.92	.97	0.98	0.97	0.98
								sensitivity (Sen_y)				
Proposed	0.97	0.98	0.99	0.97	0.95	0.93	0.96	0.80	0.15	0.87	0.92	0.85
Ref [92]	0.89	0.92	0.93	0.91	0.90	0.93	0.95	0.91	0.94	0.95	0.94	0.92
Ref [93]	0.92	0.94	0.91	0.90	0.91	0.93	0.90	0.98	0.94	0.95	0.92	0.91
Ref [94]	0.91	0.92	0.90	0.89	0.90	0.92	0.89	0.96	0.92	0.93	0.91	0.92
Ref [95]	0.97	0.91	0.92	0.91	0.93	0.90	0.91	0.92	0.96	0.95	0.92	0.96
Ref [96]	0.91	0.92	0.94	0.93	0.90	0.91	0.96	0.96	0.92	0.92	0.91	0.91
								F1 Score				
Proposed	0.98	0.99	0.98	0.95	0.96	0.93	0.96	0.89	0.22	0.45	0.94	91
Ref [92]	0.86	0.92	0.81	0.85	0.81	0.83	0.88	0.85	0.97	0.93	0.94	0.92
Ref [93]	0.92	0.92	0.83	0.83	0.90	0.91	0.92	0.93	0.91	0.98	0.96	0.94
Ref [94]	0.96	0.97	0.92	0.89	0.90	0.89	0.91	0.91	0.96	0.95	0.92	0.91
Ref [95]	0.91	0.90	0.92	0.91	0.90	0.93	0.93	0.92	0.91	0.95	0.96	0.99
Ref [96]	0.91	0.90	0.92	0.89	0.91	0.93	0.93	0.92	0.91	0.95	0.96	0.99



(a) Training and validation accuracy (b) Training and validation loss

图 14 准确率和损失曲线。

7 结论

本研究讨论了两个与癌症检测相关的关键问题：数据隐私保护和癌症诊断。使用 DWT、混沌和位平面提取的图像加密技术来传输数据，而不被攻击者操纵或未经授权的访问，从而保护用于癌症诊断的患者的敏感医学图像。在被用于癌症诊断之前，数据一旦以加密形式接收将会被破解。本研究的第二部分重点关注利用深度学习模型，即卷积神经网络对癌症诊断进行特征提取和分类。此外，采用迁移学习和微调方法来提高模型的整体精度，包括对精确率，准确率，F1 分数和召回率等指标进行分析，用于评估所提出的癌症诊断模型的性能，同时提供了一个全面的比较，以证明所提出的方法与现有技术相比的有效性。

8 未来研究方向

本文所提出的使用 CNNs 的方法具有 97.2%相对较高的准确性，但是未来通过采用以下的方法可能会进一步提高：

(1) 使用不同的预处理技术来清洗所需要的数据集，例如主成分分析(PCA) [97]和线性判别分析(LDA) [98]。

(2) 研究联邦学习的概念，它是一种有趣的方法，通过允许参与的设备自主地训练一个由集中式系统初始化的全局模型，以适应不同的分布式系统和应用[99]。

(3) 引入一种基于生成对抗网络的技术来增强所需数据集中的图像质量，可以提高癌症诊断精度并解决数据不平衡分布问题。

(4) 开发用于癌症早期检测的移动应用程序，患者只需要 MRI 图像作为输入。

参考文献:

[1] D. Tellez, G. Litjens, J. van der Laak and F. Ciompi, "Neural image compression for gigapixel histopathology image analysis", IEEE Trans. Pattern Anal. Mach. Intell., vol. 43, no. 2, pp. 567-578, Feb. 2021.

[2] T. Botterill, T. Lotz, A. Kashif and J. G. Chase, "Reconstructing 3-D skin surface motion for the DIET breast cancer screening system", IEEE Trans. Med. Imag., vol. 33, no. 5, pp. 1109-1118, May 2014.

[3] G. Litjens, O. Debats, J. Barentsz, N. Karssemeijer and H. Huisman, "Computer-aided detection of prostate cancer in MRI", IEEE Trans. Med. Imag., vol. 33, no. 5, pp. 1083-1092, May 2014.

[4] S. S. Mohamed and M. M. Salama, "Prostate cancer spectral multifeature analysis using TRUS images", IEEE Trans. Med. Imag., vol. 27, no. 4, pp. 548-556, Apr. 2008.

[5] A. Islam, S. M. Reza and K. M. Iftekharuddin, "Multifractal texture estimation for detection and segmentation of brain tumors", IEEE Trans. Biomed. Eng., vol. 60, no. 11, pp. 3204-3215, Nov. 2013.

[6] X. Wang et al., "Weakly supervised deep learning for whole slide lung cancer image analysis", IEEE Trans. Cybern., vol. 50, no. 9, pp. 3950-3962, Sep. 2020.

[7] X. Feng et al., "Accurate prediction of neoadjuvant chemotherapy pathological complete remission (pCR) for the four sub-types of breast cancer", IEEE Access, vol. 7, pp. 134697-134706, 2019.

[8] F. Bray, M. Laversanne, E. Weiderpass and I. Soerjomataram, "The ever-increasing importance of cancer as a leading cause of premature death worldwide", Cancer, vol. 127, pp. 3029-3030, 2021.

[9] S. H. Read and S. H. Wild, "Prevention of premature cardiovascular death worldwide", Lancet, vol. 395, no. 10226, pp. 758-760, 2020.

[10] L. A. Habel et al., "A population-based study of tumor gene expression and risk of breast cancer death among lymph node-negative patients", Breast Cancer Res., vol. 8, no. 3, pp. 1-15, 2006.

[11] V. Gausman et al., "Risk factors associated with early-onset colorectal cancer", Clin. Gastroenterol. Hepatol., vol. 18, no. 12, pp. 2752-2759, 2020.

[12] A. Rizzo et al., "Peripheral neuropathy and headache in cancer patients treated with immunotherapy and immuno-oncology combinations: The mouseion-02 study", Expert Opin. Drug Metab. Toxicol., vol. 17, pp. 1455-1466, 2021.

[13] A.-M. Yang, Y. Han, C.-S. Liu, J.-H. Wu and D.-B. Hua, "D-TSVR recurrence prediction driven by medical Big Data in cancer", IEEE Trans. Ind. Informat., vol. 17, no. 5, pp. 3508-3517, May 2021.

[14] Y. Wang et al., "Deeply-supervised networks with threshold loss for cancer detection in automated breast ultrasound", IEEE Trans. Med. Imag., vol. 39, no. 4, pp. 866-876, Apr. 2020.

[15] A. Shafique and F. Ahmed, "Image encryption using dynamic s-box substitution in the wavelet domain", Wireless Pers. Commun., vol. 115, no. 3, pp. 2243-2268, 2020.

[16] B. Bai, S. Nazir, Y. Bai and A. Anees, "Security and provenance for internet of health things: A systematic literature review", J. Softw. Evol. Process, vol. 33, no. 5, 2021.

[17] A. Shafique and J. Shahid, "Novel image encryption cryptosystem based on binary bit planes extraction and multiple chaotic maps", Eur. Phys. J. Plus, vol. 133, no. 8, pp. 1-16, 2018.

[18] T. A. Al-Maadeed, I. Hussain, A. Anees and M. T. Mustafa, "A image encryption algorithm based on chaotic lorenz system and novel primitive polynomial s-boxes", Multimedia Tools Appl., vol. 80, pp. 24801-24822, 2021.

[19] A. Shafique, "A new algorithm for the construction of substitution box by using chaotic map", Eur. Phys. J. Plus, vol. 135, no. 2, pp. 1-13, 2020.

[20] S. S. Jamal, A. Anees, M. Ahmad, M. F. Khan and I. Hussain, "Construction of cryptographic s-boxes based on mobius transformation and chaotic tent-sine system", IEEE Access, vol. 7, pp. 173273-173285, 2019.

[21] A. Anees and I. Hussain, "A novel method to identify initial values of chaotic maps in cybersecurity", Symmetry, vol. 11, no. 2, 2019.

[22] J. Daemen and V. Rijmen, "Reijndael: The advanced encryption standard", Dr Dobb's J. Softw. Tools Professional Programmer, vol. 26, no. 3, pp. 137-139, 2001.

[23] D. E. Standard et al., Data Encryption Standard, New York, NY, USA:Federal Information Processing Standards Publication, vol. 112, 1999.

[24] M. U. Rehman et al., "Infrared sensing based non-invasive initial diagnosis of chronic liver disease using ensemble learning", IEEE Sensors J., vol. 21, no. 17, pp. 19395-19406, Sep. 2021.

[25] M. U. Rehman, A. Shafique, S. Khalid, M. Driss and S. Rubaiee, "Future forecasting of covid-19: A supervised learning approach", Sensors, vol. 21, no. 10, 2021.

[26] M. Safaei, E. A. Sundararajan, M. Driss, W. Boulila and A. Shapi'i, "A systematic literature review on obesity: Understanding the causes & consequences of obesity and reviewing various machine learning approaches used to predict obesity", Comput. Biol. Med., vol. 136, 2021.

[27] M. Al-Sarem, A. Alsaeedi, F. Saeed, W. Boulila and O. AmeerBakhsh, "A novel hybrid deep learning model for detecting covid-19-related rumors on social media based on lstm and concatenated parallel CNNs", Appl. Sci., vol. 11, no. 17, 2021.

[28] S. Ben Atitallah, M. Driss, W. Boulila, A. Koubaa and H. Ben Ghezala, "Fusion of convolutional neural networks based on dempster-shafer theory for automatic pneumonia detection from chest x-ray images", Int. J. Imag. Syst. Technol., vol. 32, no. 2, pp. 658-672, 2022.

[29] S. Ben Atitallah, M. Driss, W. Boulila and H. Ben Ghezala, "Randomly initialized convolutional neural network for the recognition of covid-19 using x-ray images", Int. J. Imag. Syst. Technol., vol. 32, no. 1, pp. 55-73, 2022.

[30] M. U. Rehman et al., "Novel privacy preserving non-invasive sensing-based diagnoses of pneumonia disease leveraging deep network model", Sensors, vol. 22, no. 2, 2022.

[31] R. Audhkhasi and M. L. Povinelli, "Generalized multi-channel scheme for secure image encryption", Sci. Rep., vol. 11, no. 1, pp. 1-9, 2021.

[32] Y. Zhang et al., "DNA origami cryptography for secure communication", Nature Commun., vol. 10, no. 1, pp. 1-8, 2019.

[33] G. Alvarez and S. Li, "Some basic cryptographic requirements for chaos-based cryptosystems", Int. J. Bifurcation Chaos, vol. 16, no. 8, pp. 2129-2151, 2006.

[34] H. Li, Y. Wang and Z. Zuo, "Chaos-based image encryption algorithm with orbit perturbation and dynamic state variable selection mechanisms", Opt. Lasers Eng., vol. 115, pp. 197-207, 2019.

[35] W. Wang, Z. Han, M. Alazab, T. R. Gadekallu, X. Zhou and C. Su, "Ultra super fast authentication protocol for electric vehicle charging using extended chaotic maps", IEEE Trans. Ind. Appl..

[36] C. Rupa, M. Harshita, G. Srivastava, T. R. Gadekallu and P. K. R. Maddikunta, "Securing multimedia using a deep learning based chaotic logistic map", IEEE J. Biomed. Health Informat..

[37] T. Sivakumar and P. Li, "A secure image encryption method using scan pattern and random key stream derived from laser chaos", Opt. Laser Technol., vol. 111, pp. 196-204, 2019.

[38] C. E. Shannon, "Communication theory of secrecy systems", Bell Syst. Tech. J., vol. 28, no. 4, pp. 656-715, 1949.

[39] G. Kaur, R. Agarwal and V. Patidar, "Chaos based multiple order optical transform for 2D image encryption", Eng. Sci. Technol. Int. J., vol. 23, no. 5, pp. 998-1014, 2020.

[40] Y. Luo, J. Yu, W. Lai and L. Liu, "A novel chaotic image encryption algorithm based on improved baker map and logistic map", Multimedia Tools Appl., vol. 78, no. 15, pp. 22023-22043, 2019.

[41] L. Liu and S. Miao, "A new simple one-dimensional chaotic map and its application for image encryption", Multimedia Tools Appl., vol. 77, no. 16, pp. 21445-21462, 2018.

[42] M. Z. Talhaoui, X. Wang and A. Talhaoui, "A new one-dimensional chaotic map and its application in a novel permutation-less image encryption scheme", Vis. Comput., vol. 37, no. 7, pp. 1757-1768, 2021.

[43] B. Yosefnezhad Irani, P. Ayubi, F. Amani Jabalkandi, M. Yousefi Valandar and M. Jafari Barani, "Digital image scrambling based on a new one-dimensional coupled sine map", Nonlinear Dyn., vol. 97, no. 4, pp. 2693-2721, 2019.

[44] M. Kumar, A. Saxena and S. S. Vuppala, "A survey on chaos based image encryption techniques" in Multimedia Security Using Chaotic Maps Principles and Methodologies, Berlin, Germany:Springer, pp. 1-26, 2020.

[45] A. Kamrani, K. Zenkouar and S. Najah, "A new set of image encryption algorithms based on discrete orthogonal moments and chaos theory", Multimedia Tools Appli., vol. 79, no. 27, pp. 20263-20279, 2020.

[46] M. U. Rehman, A. Shafique, S. Khalid and I. Hussain, "Dynamic substitution and confusion-diffusion-based noise-resistive image encryption using multiple chaotic maps", IEEE Access, vol. 9, pp. 52277-52291, 2021.

[47] D. Hyun, L. Abou-Elkacem, R. Bam, L. L. Brickson, C. D. Herickhoff and J. J. Dahl, "Nondestructive detection of targeted microbubbles using dual-mode data and deep learning for real-time ultrasound molecular imaging", IEEE Trans. Med. Imag., vol. 39, no. 10, pp. 3079-3088, Oct. 2020.

[48] G. Carneiro, J. Nascimento and A. P. Bradley, "Automated analysis of unregistered multi-view mammograms with deep learning", IEEE Trans. Med. Imag., vol. 36, no. 11, pp. 2355-2365, Nov. 2017.

[49] O. Ozdemir, R. L. Russell and A. A. Berlin, "A 3D probabilistic deep learning system for detection and diagnosis of lung cancer using low-dose CT scans", IEEE Trans. Med. Imag., vol. 39, no. 5, pp. 1419-1429, May 2020.

[50] R. Singh, T. Ahmed, A. Kumar, A. K. Singh, A. K. Pandey and S. K. Singh, "Imbalanced breast cancer classification using transfer learning", IEEE/ACM Trans. Comput. Biol. Bioinf., vol. 18, no. 1, pp. 83-93, Jan./Feb. 2021.

[51] M. S. M. Khan, M. Ahmed, R. Z. Rasel and M. M. Khan, "Cataract detection using convolutional neural network with VGG-19 model", Proc. IEEE World AI IoT Congr., pp. 209-212, 2021.

[52] J. Xu et al., "Stacked sparse autoencoder (SSAE) for nuclei detection on breast cancer histopathology images", IEEE Trans. Med. Imag., vol. 35, no. 1, pp. 119-130, Jan. 2016.

[53] G. Altan et al., "Breast cancer diagnosis using deep belief networks on ROI images", Pamukkale Univ. J. Eng. Sci., vol. 28, pp. 286-291, 2021.

[54] R. S. Patil and N. Biradar, "Automated mammogram breast cancer detection using the optimized combination of convolutional and recurrent neural network", Evol. Intell., vol. 14, no. 4, pp. 1459-1474, 2021.

[55] Y. Li, F. Fauteux, J. Zou, A. Nantel and Y. Pan, "Personalized prediction of genes with tumor-causing somatic mutations based on multi-modal deep boltzmann machine", Neurocomputing, vol. 324, pp. 51-62, 2019.

[56] N. Antropova, B. Huynh, H. Li and M. L. Giger, "Breast lesion classification based on dynamic contrast-enhanced magnetic resonance images sequences with long short-term memory networks", J. Med. Imag., vol. 6, no. 1, 2018.

[57] W. H. Organization et al., "Definition diagnosis and classification of diabetes mellitus and its complications: Report of a who consultation. part 1 diagnosis and classification of diabetes mellitus", vol. 2, 1999.

[58] G. Ye and X. Huang, "Spatial image encryption algorithm based on chaotic map and pixel frequency", Sci. China Inf. Sci., vol. 61, no. 5, pp. 1-3, 2018.

[59] L. Gao, L. Qi and L. Guan, "The property of frequency shift in 2D-FRFT domain with application to image encryption", IEEE Signal Process. Lett., vol. 28, pp. 185-189, 2021.

[60] M. A. S. Hassan and I. S. I. Abuhaiba, "Image encryption using differential evolution approach in frequency domain", 2011.

[61] M. Guan, X. Yang and W. Hu, "Chaotic image encryption algorithm using frequency-domain DNA encoding", IET image Process., vol. 13, no. 9, pp. 1535-1539, 2019.

[62] F. Francis-Lothai and D. B. Bong, "A fingerprint matching algorithm using bit-plane extraction method with phase-only correlation", Int. J. Biometrics, vol. 9, no. 1, pp. 44-66, 2017.

[63] A. Shafique, M. M. Hazzazi, A. R. Alharbi and I. Hussain, "Integration of spatial and frequency domain encryption for digital images", IEEE Access, vol. 9, pp. 149943-149954, 2021.

[64] I. Hussain, A. Anees, T. A. Al-Maadeed and M. T. Mustafa, "Construction of s-box based on chaotic map and algebraic structures", Symmetry, vol. 11, no. 3, 2019.

[65] J. Amin, M. Sharif, M. Raza, T. Saba and M. A. Anjum, "Brain tumor detection using statistical and machine learning method", Comput. Methods Programs Biomed., vol. 177, pp. 69-79, 2019.

[66] D. N. George, H. B. Jehlol and A. S. A. Oleiwi, "Brain tumor detection using shape features and machine learning algorithms", Int. J. Adv. Res. Comput. Sci. Softw. Eng., vol. 5, no. 10, pp. 454-459, 2015.

[67] P. R. Kshirsagar, A. N. Rakhonde and P. Chippalkatti, "MRI image based brain tumor detection using machine learning", Test Eng. Manage., vol. 81, pp. 3672-3680, 2020.

[68] R. Arandjelovic, P. Gronat, A. Torii, T. Pajdla and J. Sivic, "NetVLAD: CNN architecture for weakly supervised place recognition", Proc. IEEE Conf. Comput. Vis. Pattern Recognit., pp. 5297-5307, 2016.

[69] J. Wu, "CNN for dummies", 2015.

[70] C. Szegedy, V. Vanhoucke, S. Ioffe, J. Shlens and Z. Wojna, "Rethinking the inception architecture for computer vision", Proc. IEEE Conf. Comput. Vis. pattern Recognit., pp. 2818-2826, 2016.

[71] X. Xia, C. Xu and B. Nan, "Inception-v3 for flower classification", Proc. 2nd Int. Conf. Image Vis. Comput., pp. 783-787, 2017.

[72] M. Alkhelaiwi, W. Boulila, J. Ahmad, A. Koubaa and M. Driss, "An efficient approach based on privacy-preserving deep learning for satellite image classification", Remote Sens., vol. 13, no. 11, 2021.

[73] E. C. Too, L. Yujian, S. Njuki and L. Yingchun, "A comparative study of fine-tuning deep learning models for plant disease identification", Comput. Electron. Agriculture, vol. 161, pp. 272-279, 2019.

[74] C. Käding, E. Rodner, A. Freytag and J. Denzler, "Fine-tuning deep neural networks in continuous learning scenarios", Proc. Asian Conf. Comput. Vis., pp. 588-605, 2016.

[75] N. Khuriwal and N. Mishra, "Breast cancer diagnosis using adaptive voting ensemble machine learning algorithm", Proc. IEEMA Engineer Infinite Conf., pp. 1-5, 2018.

[76] R. Atallah and A. Al-Mousa, "Heart disease detection using machine learning majority voting ensemble method", Proc. 2nd Int. Conf. New Trends Comput. Sci., pp. 1-6, 2019.

[77] J. Cao, S. Kwong, R. Wang, X. Li, K. Li and X. Kong, "Class-specific soft voting based multiple extreme learning machines ensemble", Neurocomputing, vol. 149, pp. 275-284, 2015.

[78] I. Hussain, A. Anees and A. Algarni, "A novel algorithm for thermal image encryption", J. Integrative Neurosci., vol. 17, pp. 3-4, 2018.

[79] I. Hussain, A. Anees, A. H. AlKhaldi, A. Algarni and M. Aslam, "Construction of chaotic quantum magnets and matrix lorenz systems s-boxes and their applications", Chin. J. Phys., vol. 56, no. 4, pp. 1609-1621, 2018.

[80] A. Anees, A. M. Siddiqui, J. Ahmed and I. Hussain, "A technique for digital steganography using chaotic maps", Nonlinear Dyn., vol. 75, no. 4, pp. 807-816, 2014.

[81] A. Anees, A. M. Siddiqui and F. Ahmed, "Chaotic substitution for highly autocorrelated data in encryption algorithm", Commun. Nonlinear Sci. Numer. Simul., vol. 19, no. 9, pp. 3106-3118, 2014.

[82] F. Ahmed, A. Anees, V. U. Abbas and M. Y. Siyal, "A noisy channel tolerant image encryption scheme", Wirel. Pers. Commun., vol. 77, no. 4, pp. 2771-2791, 2014.

[83] I. Hussain, A. Anees, A. H. Alkhaldi, M. Aslam, N. Siddiqui and R. Ahmed, "Image encryption based on Chebyshev chaotic map and S8 S-boxes", Optica Applicata, vol. 49, no. 2, 2019.

[84] S. Zhu, C. Zhu, Y. Fu, W. Zhang and X. Wu, "A secure image encryption scheme with compression-confusion-diffusion structure", Multimedia Tools Appl., vol. 79, no. 43, pp. 31957-31980, 2020.

[85] H. Liu, F. Wen and A. Kadir, "Construction of a new 2D Chebyshev-sine map and its application to color image encryption", Multimedia Tools Appl., vol. 78, pp. 15997-16010, 2019.

[86] L. Guo, H. Du and D. Huang, "A quantum image encryption algorithm based on the Feistel structure", Quantum Inf. Process., vol. 21, no. 1, pp. 1-18, 2022.

[87] Y. Luo, X. Ouyang, J. Liu, L. Cao and Y. Zou, "An image encryption scheme based on particle swarm optimization algorithm and hyperchaotic system", Soft Comput., vol. 26, pp. 5409-5435, 2022.

[88] D. S. Malik and T. Shah, "Color multiple image encryption scheme based on 3D-chaotic maps", Math. Comput. Simul., vol. 178, pp. 646-666, 2020.

[89] R. Pascanu, C. Gulcehre, K. Cho and Y. Bengio, "How to construct deep recurrent neural networks", 2013.

[90] Y. Zhang, R. Salakhutdinov, H.-A. Chang and J. Glass, "Resource configurable spoken query detection using deep boltzmann machines", Proc. IEEE Int. Conf. Acoust. Speech Signal Process., pp. 5161-5164, 2012.

[91] A.-r. Mohamed et al., "Deep belief networks for phone recognition", Proc. NIPS Workshop Deep Learn. Speech Recognit. Related Appl., 2009.

[92] P. Palimkar, R. N. Shaw and A. Ghosh, "Machine learning technique to prognosis diabetes disease: Random forest classifier approach", Proc. Adv. Comput. Intell. Technol., pp. 219-244, 2022.

[93] R. Bharti, A. Khamparia, M. Shabaz, G. Dhiman, S. Pande and P. Singh, "Prediction of heart disease using a combination of machine learning and deep learning", Comput. Intell. Neurosci., vol. 2021, 2021.

[94] T. M. Ghazal et al., "Alzheimer disease detection empowered with transfer learning", Comput. Mater. Continua, vol. 70, pp. 5005-5019, 2022.

[95] M. Elhoseny et al., "A new multi-agent feature wrapper machine learning approach for heart disease diagnosis", Comput. Mater. Contin, vol. 67, pp. 51-71, 2021.

[96] J. Rasheed, A. A. Hameed, C. Djeddi, A. Jamil and F. Al-Turjman, "A machine learning-based framework for diagnosis of covid-19 from chest x-ray images", Interdiscipl. Sci. Comput. Life Sci., vol. 13, no. 1, pp. 103-117, 2021.

[97] A. Maćkiewicz and W. Ratajczak, "Principal components analysis (PCA)", Comput. Geosciences, vol. 19, no. 3, pp. 303-342, 1993.

[98] P. Xanthopoulos, P. M. Pardalos and T. B. Trafalis, "Linear discriminant analysis", Proc. Conf. Robust Data Mining, pp. 27-33, 2013.

[99] M. Driss et al., "A federated learning framework for cyberattack detection in vehicular sensor networks", Complex Intell. Syst., pp. 1-15, 2022.

Mujeeb Ur Rehman received the Ph.D. degree (with distinction) from the Faculty of Engineering and Applied Sciences, Riphah International University, Islamabad, Pakistan, in 2022. He is currently a Researcher with the James Watt School of Engineering, University of Glasgow, Glasgow, U.K. He is a Lecturer with the Department of Electrical Engineering, Riphah International University.

He is also a Professional Engineer. His research interests include artificial intelligence, non-invasive health care, IoT, cyber security, and multimedia encryption.

Arslan Shafique received the B.E. degree in mechatronics engineering from Wah Engineering College, Wah Cantt, Pakistan, in 2014, and the M.S. degree in electrical engineering from Heavy Industries Taxila Education City University, Taxila, Pakistan, in 2017. He is currently working toward the Ph.D. degree with the Faculty of Engineering and Applied Sciences, Riphah International University, Islamabad, Pakistan. He is also a Research Associate with Riphaha International University. His research interests include cryptography, secure communication, and machine learning.

Yazeed Yasin Ghadi received the Ph.D. degree in electrical and computer engineering from The University of Queensland, Brisbane, QLD, Australia. He is currently an Assistant Professor of software engineering with Al Ain University, Al Ain, UAE. Before joining Al Ain university, he was a Postdoctoral Researcher with The University of Queensland. He has authored or coauthored more than 25 peer reviewed journals and conference papers and he holds three pending patents. His research interests include developing novel electro-acousto-optic neural interfaces for large-scale high-resolution electrophysiology and distributed optogenetic stimulation. His dissertation on developing novel hybrid plasmonicphotonic on-chip biochemical sensors was the recipient of the Sigma Xi Best Ph.D. Thesis Award. He was the Recipient of a number of awards.

Wadii Boulila received the B.Eng. degree (1st Class Hons. with distinction) in computer science from the Aviation School of Borj El Amri, in 2005, the M.Sc. degree in computer Science from the National School of Computer Science (ENSI), University of Manouba, Manouba, Tunisia, in 2007, and the Ph.D. degree in computer science conjointly from the ENSI and Telecom-Bretagne, University of Rennes 1, Rennes, France, in 2012. He is currently an Associate Professor of computer science with Prince Sultan University, Riyadh, Saudi Arabia. He participated in many research and industrial-funded projects. He was the recipient of the Award of the Young Researcher in computer scientist in Tunisia for the year 2021 from Beit El-Hikma. He was the Chair, a Reviewer, and a TPC Member of many leading international conferences and journals. He is a Senior Fellow of the Higher Education Academy, U.K.

Sana Ullah Jan (Member, IEEE) received the B.S. degree in electronic engineering from International Islamic University, Islamabad, Pakistan, in 2012, and the combined M.S./Ph.D. degree from the University of Ulsan, Ulsan, South Korea. He is currently a Lecturer with Edinburgh Napier University, Edinburgh, U.K. From 2012 to 2014, he was a Lab Engineer with the University of Lahore, Islamabad Campus, Islamabad, Pakistan. His research interests include wireless sensor networks, visible light communications, applications of bluetooth low energy, and machine learn ing-based sensor fault detection, isolation, and diagnosis applications.

Thippa Reddy Gadekallu is currently an Associate Professor with the School of Information Technology and Engineering, Vellore Institute of Technology, Vellore, India. He received the bachelor's in computer science and engineering from Nagarjuna University, India, the Master of Technology degree in computer science and engineering from Anna University, Chennai, India, and the Ph.D. degree from the Vellore Institute of Technology, Vellore, India. He has more than 14 years of experience in teaching. He has auhtored or coauthored more than 60 papers in reputed journals/conferences. His research interests include machine learning, Internet of Things, deep neural networks, block chain, and computer vision. He is an Academic Editor in journals like Peerj Computer Science, PLOS ONE, International Journal of Decision Support Sys tem Technology, International Journal of Organizational and Collective Intelligence, International Journal of Project Management and Productivity Assessment. He is also a Reviewer of many journals, like IEEE TII, IEEE ITS, IEEE Access, IEEE IOT Journal, IEEE Software, IEEE Consumer Electronic Magazine, Soft Computing, Applied Soft Computing, Future Generation Computer Systems, Multimedia Tools and Applications, Journal of Ambient Intelli gence and Humanized Computing, Wiley ETT, Wiley ITL, Ah HoC Networks, SUSCOM, COMNET, and COMCOM.

Maha Driss received the Engineering degree (Hons.) in computer science and the M.Sc. degree from the National School of Computer Science, University of Manouba, Manouba, Tunisia, in 2006 and 2007, respectively, and the Ph.D. degree conjointly from the University of Meyenne and University Rennes 1, Rennes, France, in 2011. From 2012 to 2015, she was an Assistant Professor of computer science with the National Higher Engineering School of Tunis, University of Tunis, Tunis, Tunisia. From 2015 to 2021, she was an Assistant Professor of computer Science with Taibah University, Medina, Saudi Arabia. She is currently an Assistant Professor of computer technology with Prince Sultan University, Riyadh, Saudi Saudi, and a Senior Researcher with the RIADI Laboratory, University of Manouba. She was a Reviewer in several world-leading high-impact jour nals and she has chaired tracks and participated as a Reviewer at a number of international conferences.

Jawad Ahmad (Senior Member, IEEE) is currently an experienced Researcher with more than ten years of cutting-edge research and teaching experience in prestigious institutes, including Edinburgh Napier University, Edinburgh, U.K., Glasgow Caledonian University, Glasgow, U.,K., Hongik University, Seoul, South Korea, and HITEC University, Taxila, Pakistan. He is also a Professor of various courses both at undergraduate and postgraduate levels during his career. He has coauthored more than 100 research articles, in international journals and peer-reviewed international conference proceedings. His research interests include cybersecurity, multimedia encryption, and machine learning and applications. He is an Invited Reviewer of numerous world-leading high-impact journals. He regularly organizes timely special sessions and workshops for several flagship IEEE conferences.