FMDB *Transactions on Sustainable Health Science Letters*

Securing Ovarian Cancer Detection Using an EfficientNet Model and Patient Data Privacy Based on Lightweight Encryption

Thirumalraj Karthikeyan[1,*], V. Revathi[2], Swathi Baswaraju[3], S. Venkatasubramanian[4], Kawsher Rahman[5]

[1]Quest Technologies Research Labs, Quest Technologies, Trichy, Tamil Nadu, India.
[2]Department of Research and Development, New Horizon College of Engineering, Bengaluru, Karnataka, India.
[3]Department of Computer Science and Engineering, New Horizon College of Engineering, Bengaluru, Karnataka, India.
[4]Department of Computer Science and Business Systems, Saranathan College of Engineering, Trichy, Tamil Nadu, India.
[5]Department of General Medicine, Beanibazar Cancer and General Hospital, Sylhet, Bangladesh.
thirumalraj.k@gmail.com[1], revshank153@gmail.com[2], baswarajuswathi@gmail.com[3], veeyes@saranathan.ac.in[4], drkawsher.rahman@gmail.com[5]

Abstract: Women often die from ovarian cancer (OC). Recent studies show deep learning can better predict OC phases and subtypes. This study predicts OC phases using a free Cancer Genome Atlas dataset (TCGA-OV) website. Pre-processing uses Mean-Median-Gaussian (MMG), a new hybrid filtering approach. The predictive model is strengthened and more accurate by combining three basic filtering approaches. Key data is collected via Faster SqueezeNet. This feature speeds up the extraction of information from complex genetic data. Ovarian cancer stages are then accurately classified using the EfficientNet-V2 network. This improves diagnosis. Understanding the importance of patient data security, this research proposes a simple, lightweight image encryption method. The Lorenz Chaotic System and DNA coding are combined. This concealment strategy protects patient data during the investigation. There's also optimal key selection using the Child Drawing Development Optimisation Algorithm. Better encryption keys boost safety. Ovarian cancer detection is complete with these approaches. It diagnoses accurately and protects patient data. The Proposed EfficientNet model achieves 98.88% accuracy in ovarian cancer classification, outperforming other models in terms of precision, recall, specificity, and F1 score. The suggested Lightweight Encryption model offers high security, an entropy of 6.9, a PSNR of 40.5, and efficient encryption and decryption.

Keywords: Ovarian Cancer; Mean Median; Gaussian Filter; Squeeze Network; Efficient Net; DNA Coding; Child Drawing; Development Optimisation; Lorenz Chaotic System, Hybrid Filtering.

Received on: 03/09/2024, **Revised on:** 20/11/2024, **Accepted on:** 04/01/2025, **Published on:** 05/06/2025

Journal Homepage: https://www.fmdbpub.com/user/journals/details/FTSHSL

DOI: https://doi.org/10.69888/FTSHSL.2025.000459

Cite as: T. Karthikeyan, V. Revathi, S. Baswaraju, S. Venkatasubramanian, and K. Rahman, "Securing Ovarian Cancer Detection Using Efficientnet Model and Patient Data Privacy Based on Lightweight Encryption," *FMDB Transactions on Sustainable Health Science Letters*, vol. 3, no. 2, pp. 65–79, 2025.

1. Introduction

*Corresponding author.

The fifth most frequent cause of cancer-related mortality among women is ovarian cancer (OC), which occurs in most cases (75%) after menopause. Approximately 40 cases occur per 100,000 people aged 50 and above each year. Spotting sickness early on greatly increases the chance of living 5 years, from just 3% at stage 4 to 90% at stage 1. Checking samples under a microscope is a better path to finding out if someone has ovarian cancer. It is identified into histological types. Interpretation of cellular structure helps to understand the different types of OC and directs them. Making a treatment plan, which skilled doctors do best for ovarian tumours. But some differences in how observer grades have been noticed [24]. Different methods of reading a sample of cells under a microscope can lead to incorrect decisions about the future, ineffective treatments, and a lower quality of life [3]; [4]. This suggests that we need to develop computer methods that can accurately predict OC. To achieve this goal, various OC diagnosis models have been developed over the past decade. They used just one kind of picture from a test called histopathology [5]. This type of picture shows how a cell looks, which is very connected to the aggressiveness of OC. Additionally, it is known that changes in gene expression and alterations in gene function can indirectly affect cancer growth by accelerating cell proliferation and modifying the tumour microenvironment [6]. Therefore, genetic features are key indicators that guide medical testing. They include a list of gene activity marks, changes in DNA nucleotide sequences, local differences in the copy amounts of DNA parts, and the extent of methylation changes. This is in accordance with research [7].

Recent advancements in certain types of deep learning models, such as CNNs, have a significant impact on medical diagnosis. A significant challenge in the deep learning field is improving model performance. Currently, deep learning methods are being explored to address the issues of ML algorithms [8]. Currently, various applications of deep learning are very popular. These include things like CNN, RNN, and a special type of memory called LSTM. All of them are recognised for their contributions to the classification of medical images. DL methods can accurately identify an important collection of sample features without expert assistance [4]. Deep learning (DL) and object detection algorithms both mimic the way the human brain functions when recognising and categorising a wide range of concepts by observing examples of them [9]. Encryption is crucial for safeguarding the confidentiality and privacy of cancer image classification data [10].

As the medical field advances, the need to maintain the confidentiality of private patient details becomes increasingly important. Encryption serves as a safety shield, protecting sensitive medical images from unauthorised access and ensuring their privacy. Healthcare workers and scientists can prevent unauthorised access and protect patient information by using strong codes [5]. This way, they can reduce the risk of patients' details being accessed by unauthorised individuals [12]. This is very important in cancer picture sorting. Accurate diagnosis and treatment plans require an understanding of and the ability to read medical images [13]. The use of encryption technologies makes important data more secure. It also helps patients and doctors trust that private medical information will be handled rightly and privately [10].

1.1. Motivation

These studies are mainly about changing how it finds out about ovarian cancer. They really care about keeping patient information safe. The study aims to improve medical testing [21]. It aims to establish a model that safeguards patients' private information [17]. The aim is to improve the detection of ovarian cancer and ensure patient confidentiality through innovative methods in cancer detection and data protection. This will help the healthcare field grow, increase trust in medical work, and establish new guidelines for handling genetic information [23].

1.2. Main Contributions

- **Hybrid Filtering Technique (MMG):** Begin by exploring a novel approach to cleaning the TCGA-OV dataset using the Mean-Median-Gaussian hybrid filter. This method gives good results.
- **Feature Extraction with Faster SqueezeNet:** Using the faster SqueezeNet model to spot important parts of DNA that help guess the correct stages of ovarian cancer.
- **EfficientNet-V2 Classification:** Utilising the EfficientNet-V2 network enables the accurate and rapid identification of the different stages of ovarian cancer. This leads to better diagnosis.
- **Secure Patient Data Encryption:** Developing a Lightweight Lorenz Chaotic System and DNA Coding Image Encryption Scheme. This guarantees strong secrecy and safety of patient information during analysis.
- **Optimal Key Selection with CDDOA:** Starting the Child Drawing Development Optimisation Algorithm (CDDOA) helps to pick the best keys in the secret codes. This enhances the safety of patient data in studies on ovarian cancer.

1.3. Organisation of the Paper

The study's remaining sections are structured using shadows: the works that matter are summarised in Section 2, the suggested model is briefly explained in Section 3, the findings and validation analysis are presented in Section 4, and the summary and conclusion are provided in Section 5.

2. Related Works

The study by Ziyambe et al. [2] described a novel algorithm for ovarian cancer diagnosis and prediction using convolutional neural networks (CNNs) to address these issues. A dataset of histopathological images was used in this work to train a CNN. The dataset was pre-augmented and separated into validation and training subsets. The model's accuracy rate was impressive, at 94%, correctly classifying 93.02% of healthy cells and accurately identifying 95.12% of cancer instances. This study is important because it addresses issues like increased rates of misclassification, variability among observers, and extended periods of analysis resulting from human expert review. This work offers a more precise, effective, and trustworthy method for ovarian cancer diagnosis and prognosis. The aim of the study by Binas et al. [4] was to provide medical professionals and biomedical engineers with a tool for personalised medicine by introducing a novel technique that utilises quantitative features extracted from medical images to assess intratumoral cellularity. This method is also referred to as sophisticated image processing, radiomics, and algorithms for artificial intelligence. The findings show that within the population under study (n = 22), the suggested method's average accuracy rating was above 85%.

The article by Sundari and Brintha [16] presented the IEDL-OVD model, a novel Internet Explorer that utilises deep learning to diagnose ovarian tumours. The IEDL-OVD model aims to enhance the quality of the input medical image, resulting in more accurate diagnostic results. An IE technique based on black widow optimisation is included in the recommended IEDL-OVD method. The ovarian tumour is detected using a stacked autoencoder (SAE) as a classification model and the VGG16 model as a feature extractor. Through a thorough experimental analysis, the diagnostic results of the IEDL-OVD model are investigated, and the findings are evaluated in relation to various assessment parameters. The IEDL-OVD model achieved better recall and precision rates of 0.612 and 0.735, respectively, with 100 photos. With the use of quality IE, the black widow optimisation algorithm (BWOA) produced results with a homogeneity of 0.94, a weighted peak signal-to-noise ratio (WPSNR) of 20.43, a high contrast of 0.97, and a contrast-to-noise ratio (CNR) of 92.74%. In the paper by Acharya et al. [20] on Kaggle, a deep convolutional neural network architecture was proposed for predicting ovarian cancer using a dataset comprising 349 patient instances. Subsequently, the dataset underwent a suite of feature extraction techniques and data-cleaning procedures [25].

Additionally, the model's efficacy has been demonstrated by contrasting it with seven conventional machine learning classifiers, including Linear Discriminant Analysis, Multilayer Perceptron, Random Forest, Gradient Boosting Tree, AdaBoost, XGBoost, and Decision Tree. The analysis of the results shows that the F1 score, ROC-AUC, recall, and precision are all higher for the proposed CNN architecture. The model by Maria et al. [8] integrated the effectiveness of the YOLO v5 detection model and the accuracy of the U-Net segmentation model in identifying malignant ovarian tumours on computed tomography images. Clinical data is used to validate the performance of this model, and an analysis has been conducted on its performance metrics. Simulated results indicate that ovarian tumours can be effectively treated using the proposed model with high accuracy and Dice scores. The YOLO v5 model detected the ovarian tumours with 98% accuracy, and the U-Net segmented them with 99.2% accuracy, as found. Radiologists can diagnose ovarian cancer with the use of this computer-aided diagnosis system. The security of the Internet of Things for medical images employs optimisation techniques and a novel cryptographic model. A distinct framework is required for the safe and efficient exchange of medical image data and patient data. Using the Rivest-Shamir-Adleman (RSA-AM) based Arnold map, it will select the supervisor responsible for overseeing and enhancing the security of lock and unlock processes.

This will involve optimisation of flower raising bitterness (OBBO) and hostile team direction (HO). The optimal metrics to assess the effectiveness of the proposed scheme are the peak signal-to-noise ratio (PSNR), entropy, bit error rate (BER), structural similarity index (SSI), mean square error (MSE), and correlation coefficient (CC). Research suggests that a low-cost technique for encrypting multiple images in a medical setting has a computational cost comparable to that of encrypting a single image [18]. It can use a single encryption operation to both encrypt and decrypt an unlimited number of medical images of various sizes. To guarantee that every plaintext image is the same size, the various-sized plaintext images are filled at the bottom and right of the image. After that, each filled image is stacked to produce a superimposed image. Using the algorithm for linear congruence, the original key is the first step in creating the encryption key sequence, produced by the SHA-256 algorithm. Next, the superimposed image is encrypted using the cypher picture using DNA encoding and the encryption key. Incorporating a method for decrypting the image independently can further strengthen the algorithm's security by reducing the possibility of data loss during decryption.

2.1. Research Gaps

They did not extensively discuss how well their ovarian cancer CNN performed with different datasets and its generalizability beyond its original training context. This made it hard to use. Binas et al. [4] have suggested that we need to explore tools for personalised medicine. It must consider how large they can be, utilise them in real-life scenarios, and ensure they work effectively on multiple patients to demonstrate their reliability [16]. The IEDL-OVD model has potential, but it hasn't been checked completely on different sets of data and compared to existing ways for finding out if someone has ovarian cancer.

CNN for ovarian cancer doesn't understand how it works, possible unfair actions, or right and wrong issues. Resolving these would make it more trusted. Mixed YOLO v5 and U-Net model. It seems good, but some issues need to be addressed in medical use, practical usefulness in real life, and integrating such technology into their system. Selvaraj et al. [10] stated that the security model for IoT should be tested using real health data and examined for its potential growth. They identified areas where it might be vulnerable, along with strategies to protect against them. Wu et al. [11] made a low-cost image scrambling solution. It requires further testing to determine its speed, identify potential weaknesses, and assess its resilience against various attacks before it can be deployed in real-life applications.

3. Proposed Methodology

Figure 1 shows the workflow of the proposed model.

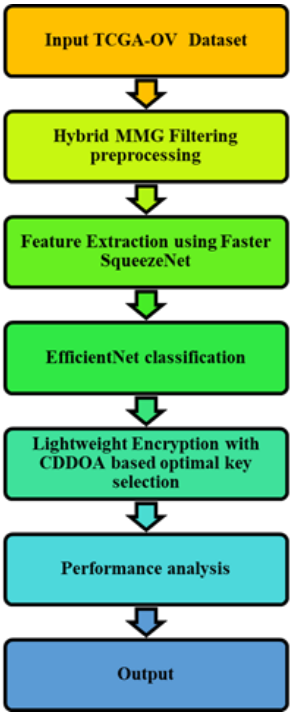

Figure 1: Block diagram

3.1. Dataset Description

For OC stage prediction, a publicly available dataset from the Cancer Genome Atlas portal accessed on March 2, 2021, was used. More specifically, the TCGA-OV can be found at https://portal.gdc.cancer.gov/. Data on copy number variants and gene expressions from 587 OC patients are included in the dataset. Every patient also has many pathological images. One modality type is associated with the coloured pathology images, whereas the gene expression and copy variant data have a single dimension. It refers to them as pathology image modal and gene modal in this work, respectively [18]. Table 1 lists all the features of the multimodal TCGA-OV dataset. It displays the number of patients' samples corresponding to each OC stage. Approximately 6,426 data indicators were included in the gene expression data, while approximately 24,776 data indicators were included in the copy number variants data. Additionally, for every patient, one to ten pathological images were available.

Table 1: An explanation of the multimodal TCGA-OV dataset

Clinical Characteristics	Number of Samples
Patients with Serous Ovarian Carcinoma Having Clinical Data	N = 587
Stage Not Available	5(0.85%)
Stage IV	89(15.16%)
Stage III	446(75.98%)
Stage II	30(5.11%)

Stage I	17(2.90%)
Data Category	**Number of Attributes**
Gene expressions	6426
Pathology images for each sample	1375 images
Copy number variants	$1-10$ images

3.2. Preprocessing Using MMG Filter

First, a sample image was used to calculate the kernel matrix size. In the study's methodology section, a 3 × 3 kernel matrix is provided as an illustration. The sample image was subjected to Gaussian filters with a 3x3 matrix size, using the kernel described in [1]. One image was produced by calculating the resultant vectors of the same pixels from the images to which the mean, median, and Gaussian filters were applied. A mathematical formula was used to normalise the image that was obtained by taking the resultant vectors. Normalisation was carried out by computing the resultant vector of the pixel values corresponding to the three filtering techniques using Equation (1).

$$\mathrm{MMG_{i,j}} = 255 \cdot \frac{\sqrt{\left(\mathrm{Mean\ _{i,j}}\right)^2+\left(\mathrm{Median\ _{i,j}}\right)^2+\left(\mathrm{Gaussian\ _{i,j}}\right)^2}}{\mathrm{Max}\left(\mathrm{MMG_{i,j}}\right)} \quad (1)$$

The new image that has been softened by a filter is represented by MMG in the equation $Max\left(MMG_{i,j}\right)$ Represents, before normalisation, the maximum pixel value that could be extracted from the resultant vector. The research findings section contains the results of testing the MMG hybrid filter's performance using a sample image.

3.3. Extraction Using Faster Squeezenet

A faster SqueezeNet was introduced in this study to enhance the efficiency and precision of OC feature extraction. The authors incorporated Batch Normalisation and residual frameworks to prevent overfitting. Concat was also used in tandem with DenseNet to link different layers, thereby enhancing the expressiveness of the first layer. Fast SqueezeNet consists of three block layers: four convolution layers, a global average pooling layer, and a BatchNorm layer. The main improvements to Fast SqueezeNet are listed below. (1) To further improve the data flow between the layers, the current study offers a novel connection mode while imitating the DenseNet architecture [15]. This is made up of a pooling layer and a fire module. Finally, the convolutional layer that followed was also connected to the two concatenated layers. Every feature map from the previous layer is obtained by the current layer, which then uses $x_0, \ldots, x_{l-1}$ as the input, following x_l is shown as indicated by equation (2) below.

$$\mathrm{x_l} = \mathrm{H_l}([\mathrm{x_0}, \mathrm{x_1}, \ldots, \mathrm{x_{l-1}}]) \quad (2)$$

where $[x_0, x_1, \ldots, x_{l-1}]$ depicts the relationship between the layer's feature graph created, $0,1, \ldots, l-1$ and H_l represents the concatenation of multiple inputs. Moreover, the maximum pooling layer can be found by x_0 , x_1 denotes the Fire layer, while x_l Stands for the Concat layer. Considering the number of network parameters, efficiency can still be maximised early on. Data can be simultaneously transported directly over any two-layer network. (2) A fire module and a pooling layer were presented to distinct components after a thorough understanding of the ResNet architecture to ensure a successful network convergence. Lastly, two layers were appended and connected to the subsequent convolution layer. A common representation of the fundamental mapping is $H(x)$. To fit alternative mappings of the stacked non-linear layer, $F(x) := H(x) - x$. The initial mapping is arranged differently into $F(x) + x . F(x) + x$ is implemented as a shortcut connection structure. It utilises ResNet's residual architecture to address issues such as gradient degradation and vanishing gradients without introducing additional network variables.

3.4. Classification Using EfficientNet Framework

To achieve better classification results, a robust set of image features is necessary, as it directly aids in differentiating between the various image data groups. Dense deep learning networks can be used to compute a set of more efficient features, which in turn raises the recall rate of these techniques [22]. When deep networks are used, the models' computational capabilities are limited by the memory and processing power requirements, which significantly impact how these CNN techniques are applied. As such, there are always trade-offs between the evaluation's outcomes and computing costs. Therefore, it is necessary to develop an OC diagnosis system that exhibits increased precision in classification without incurring higher computational costs. To improve model performance, this study provides a simple and reliable computational method for classifying. An enhanced version of the EfficientNetV2-B4 model, referred to as EfficientNet, is presented for detecting OC. An enhanced version of EfficientNet is called EfficientNetV2. In essence, to maintain a high recall rate and expand the pool of resources, the improved

EfficientNetV2 model is provided. A rapid and efficient composite scaling technique was employed to develop the improved EfficientNetV2 model, enabling a standard ConvNet to be modified for any resource constraints without compromising its functionality. Consequently, the suggested method provides the best option for network architecture, including network layers and feature vector size, as well as the most effective way to calculate costs. Using a few model parameters, the EfficientNetV2 technique performs classification operations with robustness.

To detect OC, EfficientNet-V2 with dense layers was developed because it is a lightweight, efficient method with fewer parameters and a lower training time requirement. Using neural architecture search, the EfficientNetV2 method decreases training time and feature vector size while improving classification accuracy (NAS). Furthermore, the architecture of EfficiceiNetV2 maximises the operational power and makes effective use of mobile or server accelerators by incorporating the Fused-MBConv (FMBConv) blocks. In contrast, the primary building block of an MBConv block is used in the traditional EfficientNet approach, which exclusively employs depth-wise convolutions. Convolutions that are depth-wise minimise the quantity of operations required, but they don't make full use of newly created hardware accelerators. To optimise computing gains, the EfficientNetV2 technique fully utilises the MBConv and FMBConv blocks. The FMBConv substitutes standard 3x3 convolution layers for depth-wise 3x3 convolution.

The primary objective is to execute the method as efficiently as possible while maintaining accurate classification results. To complete the sorting process, it employed EfficientNetV2 with the B4 structure. The primary cause for the B4 base was chosen because it offers a better balance between the complexity of time and the model's ability to sort things out. Swish activation, MBConv blocks with 3x3 and 5x5 convolutions, and squeeze-and-excitation blocks (SEB) are utilised in the updated EfficientNet-V2 model, which is a sophisticated design. FMBConv blocks are utilised in the lower layers. MBConv blocks uphold a close relationship with the SEB and guarantee accurate classification outcomes. The ReLU activation function (ReLUAF) is replaced within the architecture by the Swish activation function (SAF) because ReLU eliminates negative values and discards a significant portion of the crucial ECG signal. Equation (3) can be utilised to find the SAF:

$$\mathrm{SAF}\ (x) = X.\,\mathrm{Sigmoid}\ (x) \tag{3}$$

To further reduce the input image sizes, the framework was extended with an initial batch normalisation layer. This is because only three of the many parameters available to FMBConv blocks for large values of O were used. To mitigate the problem of overfitting and reduce the model parameters, a layer of global average pooling was added following the MBConv framework. Two additional dense inner layers were added, in addition to dropout and ReLU AF layers, which help calculate the more efficient gathering of image attributes through their efficient arrangement. A 30% dropout rate was selected at random to enhance the model's performance. Ultimately, a layer of softmax was used to categorise OC. A detailed view of the enhanced EfficientNetV2 method is provided in Table 2.

Table 2: Specifics of the layers and blocks that make up the suggested model

No.	Layers
1	ConvL (3 × 3)
2	BatchNormalization
3	2 × FMBConv4 Block
4	3 × FMBConv4 Block
5	2 × FMBConv1 Block
6	Conv2d (1 × 1) Block
7	12 × MBConv6 Block
8	7 × MBConv6 Block
9	5 × MBConv4 Block
10	Dropout
11	Dense Layer
12	Dropout
13	Softmax Layer
14	Global average pooling
15	FC Layer
16	Dense Layer

3.4.1. Loss Function (LF)

Models use the loss function (LF) to evaluate their performance. Networks utilise automated learning to identify patterns and make predictions from massive volumes of data. Determining the degree of change between the expected and real values is the main objective of the LF. To lower error, the LF is continuously changed during the model training process until a robust fitting value is reached. To categorise distorted and high-quality samples, an output neuron and the last layer of the EfficientNet model are utilised. As a result, the framework's hyperparameters were chosen empirically. In the suggested method, a learning score of 0.1 is used in conjunction with the model's training. Additionally, it used twenty epochs to train the model. In tasks involving classification, the cross-entropy LF assesses the difference between the actual and calculated values using the Softmax function. In equation (4), the cross-entropy LF can be computed using the following formula:

$$\mathrm{LF} = \frac{1}{\mathrm{N}}\sum_{\mathrm{k=1}}^{\mathrm{n}} \log\left(\frac{\mathrm{e}^{\mathrm{s_j}}}{\sum_{\mathrm{i}} \mathrm{e}^{\mathrm{s_k}}}\right) \quad (4)$$

Here, N represents all neurons, and s_k Regarding the vector input, sj is the approximate label. Only 20% of the framework's parameters can be changed by the model, leaving the other 80% unchanged. Using a validation set ensured that issues related to model overfitting were prevented. Estimating Adaptive Moments was used to determine the learning rate value against each parameter. Equations (5) and (6), respectively, show how the impulse approach is used in this method to keep the prior gradient's exponential decay stored.

$$\mathrm{M_t} = \mathrm{b1M_t} - 1 + (1 - \mathrm{b1})\mathrm{G_t} \quad (5)$$

$$\mathrm{V_t} = \mathrm{b2V_t} - 1 + (1 - \mathrm{b2})\mathrm{G^2t} \quad (6)$$

Here, $b1$, and $b2$ are constants; the gradient score corresponds to 0.9 and 0.999, respectively, and is shown by G, and M_t and V_t show the vectors at the initial and subsequent moments. Each of these factors' values shows how the updated and earlier gradient values are similar. Greater values for these parameters indicate a high correlation between the old and new gradient values. Given that the two moments' initial values are set to zero, the factors used to correct for bias are needed $b1$ and $b2$, to keep the zero biases away. Through the use of the formulas (7) and (8), which calculate the bias-corrected Mt, such biases can be eliminated:

$$\mathrm{M_t} = \mathrm{M_t} - (\mathrm{bt1}) \quad (7)$$

$$\mathrm{V_t} = \mathrm{V_t} - (\mathrm{bt2}) \quad (8)$$

Equation (9) is used in the optimisation process of the model to update the gradient value.

$$\mathrm{W_{t+1}} = \mathrm{W_t} - \eta/(\mathrm{V_t} + \epsilon\mathrm{M})^{0.5}\mathrm{t} \quad (9)$$

Here, ϵ is a constant, η is the learning rate used to prevent the denominator from going to zero, with a value of 0.00001, and W(t+1) represents the parameters of the framework at a specific moment $(\mathrm{t}+1)$.

3.5. Lightweight Encryption Model

3.5.1. Lorenz Chaotic System

A pseudorandom source that can be generated at both the sending and receiving ends is required for the proposed cryptography system. Euler's method is used to digitise the chaotic system, bringing it to life in the digital realm [14]. The following equations give the Lorenz chaotic system's Eulerian solution:

$$\mathrm{X_{n+1}} = \mathrm{X_n} + \mathrm{h}\sigma(\mathrm{Y_n} - \mathrm{X_n}) \quad (10)$$

$$\mathrm{Y_{n+1}} = \mathrm{Y_n} + \mathrm{h}(\rho\mathrm{X_n} - \mathrm{Y_n} - \mathrm{X_nZ_n}) \quad (11)$$

$$\mathrm{Z_{n+1}} = \mathrm{Z_n} + \mathrm{h}(\mathrm{X_nY_n} - \beta\mathrm{Z_n}) \quad (12)$$

Wherein h is the size of the step, σ, ρ, and β are the parameters of the system, and $\mathrm{X_0}, \mathrm{Y_0}$, and $\mathrm{Z_0}$ are the variables in the system.

3.5.2. DNA Coding

The value of each pixel is concealed using the DNA encoding technique. In a DNA sequence, the four potential nucleic acid bases are adenine (A), guanine (G), thymine (T), and cytosine (C); "A" is always complementary to "T," and "C" is always complementary to "G". The connections between the binary codes and the different DNA bases that correspond to them are shown in Table 3. Considering the complementary characteristics of the binary stream and the nucleic acid bases, there are eight appropriate coding rules. Guidelines for encoding and decoding DNA are compiled for the suggested cryptography system, as shown in Table 3.

Table 3: Binary codes for DNA and the rules governing their decoding and encoding

DNA Base	Binary Code		Rules							
			8	7	6	5	4	3	2	1
C	11	C	A	G	T	G	C	T	A	C
T	10	T	C	T	C	A	A	G	G	T
A	01	A	G	A	G	T	T	C	C	A
G	00	G	T	C	A	C	G	A	T	G

3.6. Cryptography Algorithm

3.6.1. Encryption

- **Step 1:** First, determine the total number of pixels in the picture to get P_{Sum}.
- **Step 2:** Determine P, which is equivalent to $\mathrm{mod}(P_{Sum}, 16)$.
- **Step 3:** Eight keys, each with 32 bits, should be created from the input key. $(Key_1 \ldots Key_8)$.
- **Step 4:** To create the starting circumstances surrounding the chaotic sequence, XOR the keys together.
- **Step 5:** After executing the Lorenz chaotic system with the starting parameters from the preceding step, eliminate the redundant outputs by discarding the first 200 generated outputs.
- **Step 6:** Utilise the outputs of the chaotic system to produce $X_{bin1}, X_{bin2}, X_{bin3}, X_{bin4}, Y_{bin1}, Y_{bin\,2}, Y_{bin\,3}, Y_{bin\,4}$ such that Y_{bin} is similar to X_{bin} and Z_{bin}.
- **Step 7:** To complete the process of pixel confusion, the value of P. If P is even, the picture is encrypted in the typical manner; if not, it is reversed before encryption. This is an easy way to modify the pixel locations for each iteration.
- **Step 8**: Use $X_{bin1}, X_{bin2}, X_{bin3}$, and X_{bin4} as each of the input image's two bits' DNA encoding rule.
- **Step 9:** Use $Y_{bin\,1}, Y_{bin2}, Y_{bin\,3}$, and $Y_{bin\,4}$ as each of the two pieces of the previously mentioned DNA decoding rule generated DNA-encoded bits.
- **Step 10:** XOR the step 8's produced 8-bit output with Z_{bin} and mask, where mask is initialised with zero and holds the earlier output from step 10. Following this, $P = P - 1$; repeat step 5 until you reach $P = 0$.

Algorithm 1 provides more details on the encryption algorithm. If an image with LW pixels serves as the algorithm's input, the estimated time complexity is limited to $O(LW)$.

3.6.1.1. Algorithm 1: Encryption Process

Input: Input image I, and encryption key K
Output: Encrypted image E, and the 16-bit value P
1: $P = \mathrm{mod}(SU(I), 16)$
2.$P = P$//Divide the key into four $32 -$ bit keys.
3. $\{Key_1, \ldots, Key_s\} = K$
// Set up the chaotic system's initial parameters.
4: while $P > 0$ do
5. $x_0 = Key_1 \otimes Key_2 \otimes KeyK_3 \otimes Key_4$
6. $Y_0 = Key_3 \otimes Key_4 \otimes Key/5 \otimes Key_6$;
for $i = 1$ to $(200 + L \times W)$ do
$X = X_0 + h\sigma(Y_0 - X_0)$;
$Y = Y_0 + h(\rho X_0 - Y_0 - X_0 Z_0); Z = Z_0 + h(X_0 Y_0 - \beta Z_0); X_0 = X; Y_0 = Y_i Z_0 = Z_i$
if $i > 200$ then
$$X_{bim\,1} = \mathrm{mod}(\mathrm{fix}(X \times 2^{13}), 8) + 1$$

$X_{bin\,2} = \mathrm{mod}(\mathrm{fix}(X \times 2^{16}), 8) + 1;$
$X_{bin\,3} = \mathrm{mod}(\mathrm{fix}(X \times 2^{19}), 8) + 1;$
$X_{bin\,4} = \mathrm{mod}(\mathrm{fix}(X \times 2^{22}), 8) + 1 Y_{bin\,1} = \mathrm{mod}(\mathrm{fix}(Y \times 2^{13}), 8) + 1 Y_{bin2}$
$= \mathrm{mod}(\mathrm{fix}(Y \times 2^{16}), 8) + 1; Y_{bin3}$
$= \mathrm{mod}(\mathrm{fix}(Y \times 2^{19}), 8) + 1; Y_{bin\,4}$
$= \mathrm{mod}(\mathrm{fix}(Y \times 2^{22}), 8) + 1; Z_{bin} = \mathrm{mod}(\mathrm{fix}\,(Z \times 2^{22}), 8) + 1;$
if $\mathrm{mod}(P, 2) == 0$ then
$I = L_i$
else
$I = 1_{(L \times W) - i^*}$
end if
$D = DNA_{encode}\,(I, X_{bin1}, X_{bin2}, X_{bin3}, X_{bin\,4});$
$T = DNA_{decode}\,(D, Y_{bin1\,1}, Y_{bin2}, Y_{bin3}, Y_{bin4\,4});$
$I(i) = Z_{bin} \oplus T \oplus \mathrm{mask};$
$\mathrm{mask} = I(i);$
$P = P - 1$
end if
end for
$I = I;$
end while
$E = I;$
Return E, P

3.6.2. Decryption

The process of decryption is the inverse of encryption. The primary distinction is that P is transmitted to the receiving side along with the key rather than being calculated.

3.6.3. Optimal Key Selection Using CDDO Algorithm

In this paper, CDDOA is utilised for optimal key selection of the encryption model. While optimisation approaches seek the best scenario, which, using an evaluation function, can be used to determine the global optimum, artistic works aim to achieve the most aesthetically pleasing state, which is influenced by the artwork's use of the golden ratio. Throughout the drawing process, the artist makes several suggestions that ultimately determine the final drawing. Here, for example, a metaheuristic algorithm was formed using the components that influence a child's drawing throughout the various stages of their artistic development. The new Human behaviour-inspired algorithm's mathematical equations were developed with inspiration from the behaviour of children and the solid mathematical justification for the golden ratio presented in the previous section [19]. The following subsections will provide a thorough explanation of each section in relation to the golden ratio, pattern memory, mathematical equations, drawing properties (such as length and width) and group member cooperation.

3.6.4. CDDO Stages

Each step's specific explanation is provided below:

The First Stage (The Scribble): Most of a child's early drawings are just random marks made during their learning process. At this age, the child is learning about hand pressure and movement by observing it. Since the child is learning that hand movements with liners create lines and any additional hand movement produces curves, random motion can be both linear and curved. It is currently too forceful when holding the hand; in subsequent stages, it will be adjusted through trial and error, taking into account other factors, including whether it is excessively high or low. -launch Xij for $i = 1$ to N solution. X, when a child's drawing contains several factors that can be chosen from, such as the number of parameters, the length, width, golden ratio, and hand pressure reported, the current solution is represented by j.

The Second Stage (Exploitation): The youngster gains control over their direction and mobility, allowing them to create shapes during this stage. At this point, the drawings are more uniform and replicated, and the child is defining the best sketched drawing thus far and comparing it to the best pattern they have learned. In addition, they are creating new scribbles by copying the top local artists and comparing them to the best-sketched drawing that has been produced as a group, thus far. Hand pressure is one factor that is used to categorise a child's work. The child's level is high, despite the significant hand pressure. Meanwhile, that shows that a child is proficient enough to draw a picture using the correct golden ratio and little force. First, a Random

Hand Pressure (RHP) is produced. The hand pressure of a current solution is evaluated using a factor called RHP, which was developed to measure hand pressure (HP). The number that separates the problem's lower boundary (LB) from the solution's upper boundary (UP) is arbitrary. Equations (13) and (14) will be used to select HP from among when Hand pressure is represented by HP, and the parameters are gathered by *j* for the current solution, or the set of solution parameters.

$$\mathrm{RHP} = \mathrm{rand}\,(\mathrm{LB}, \mathrm{UP}) \quad (13)$$

$$\mathrm{HP} = \mathrm{X}(\mathrm{i}, \mathrm{rand}\,(\mathrm{j})) \quad (14)$$

Third Stage (Golden Ratio): The child is now applying the abilities they have gained from experiences by imitating, practising, and being enthusiastic (with trial). They attempt to decipher the drawings by looking for patterns in the real photos based on the feedback they receive. Before implementing these behaviours, measure the child's hand pressure HP to gauge their level of proficiency. When evaluating the relationship between the RHP and the present hand pressure, using equation (15), if it is less than the RHP will be updated to account for the child's arbitrary level rate (LR) and skill rate (SR), that start at zero and go up to 1, as well as whether the child displays relevant hand pressure, between 0.6 and 1. The child's knowledge and skill rate is accurate when SR and LR are set to high (0.6–1), even though it can be improved by accounting for the GR factor. The Golden Ratio (GR) is an additional element used to enhance performance and update the solution. GR represents the proportion of the two factors chosen for the solution, the child's drawing's width and length in equation (16). Equation (17) is utilised from all the components of the problem, to randomly select each of these two factors.,

$$\mathrm{X_{i+1}} = \mathrm{GR} + \mathrm{SR} \cdot * \left(\mathrm{X_{ilbest}} - \mathrm{X_i}\right) + \mathrm{LR} \cdot * \left(\mathrm{X_{igbest}} - \mathrm{X_i}\right) \quad (15)$$

$$\mathrm{X_{iGR}} = \frac{\mathrm{X_{iL}} + \mathrm{X_{iW}}}{\mathrm{X_{iL}}} \quad (16)$$

$$\mathrm{L}, \mathrm{W} = \mathrm{rand}\,(0, \mathrm{j}) \quad (17)$$

$\mathrm{X_{ilbest}}$ it is the young artist's finest drawing to date, and it represents the best option in the area. and $\mathrm{X_{igbest}}$ are the kids seeing the world's best solution in their surroundings? In addition, the child's drawing's length (L) and width (W) ratio is known as the Golden Ratio (GR).

Fourth Stage (Creativity): Every child possesses the creativity and abilities they have acquired via experience and observation of their surroundings. The quality of creativity adds to the visual appeal of any work of art. At this point, the child is updating the golden ratio-containing solutions or is very close to it by combining information. The answer, however, lacks the appropriate hand pressure to indicate that a child's ability is still developing and should be improved by utilising both the golden ratio and the creative factor. Furthermore, a child will attempt to replicate the most effective learning strategies to improve their performance. To achieve this, a Pattern Memory (PM) is generated for every algorithmic solution; the size of the pattern varies depending on the specific issues at hand. But one way to speed up the rate of convergence of the algorithm and, in practice, help kids learn more quickly, is to choose a randomly selected PM array solution to update the underperforming solutions. Equation (18), which updates the present solution and converges towards the ideal solution, applies both CR and PM. The creativity factor is added, adding to the improvement. After much trial and error, a fixed value of CR = 0.1 was established. At a later time, when both SR and LR are low (0-0.5), the child's rate of knowledge and skill acquisition is inaccurate. However, it can be improved by taking their creativity and pattern memory into account.

$$\mathrm{X_{i+1}} = \mathrm{X_{iMP}} + \mathrm{CR} * \left(\mathrm{X_{igbest}}\right) \quad (18)$$

Fifth Stage (Pattern Memory): Employing past knowledge and experience, supplementing with additional details, increasing precision, and cross-referencing with all of the best drawings. Using a random selection from the top ten child drawings, the algorithm updates the existing illustration, which disregards hand pressure while keeping an exact golden ratio. The stage mainly focuses on the minute details in inches of the drawings. Given that the behaviour is displayed by the most effective updating system on the agent, it is applied in the algorithm. If a better solution becomes available, it will be updated accordingly. This also applies to updating the world's best solution for the population. This conduct will likewise be valid when each iteration's pattern memory is updated with the best global solution currently found.

3.6.5. The Steps of CDDOA

The steps and procedure of the following are the recently suggested algorithms:

- Set up the drawing population for a child.
- Assess drawings and select the best individual and collective drawings.

- Determine each drawing's golden ratio.
- Select the best drawing to use as the starting point for initial pattern memory when making changes to the current drawing.
- Update the drawings based on the child's hand pressure, using either pattern memory or the golden ratio.
- Update the child's level and skill rates.
- Assess the cost values and make updates to the individual, collective, and pattern memory.

4. Results and Discussions

4.1. Experimental Setup

A PC equipped with an Intel(R) Core (TM) i7-10700KF @ 3.80 GHz CPU, 32.0 GB RAM, six CPUs, and one NVIDIA GeForce RTX 3060 GPU is used to conduct the experimental study.

4.2. Classification Analysis

The efficacy of the suggested pipeline is evaluated using several criteria, including precision, Matthew's correlation coefficient (MCC), sensitivity, F1-score, specificity, and accuracy. These metrics are computed using the following formulas (19)– (23). Additionally, the receiving operating characteristic (ROC) and the confusion matrix are computed.

$$\text{Accuracy} = \frac{TP+TN}{TN+FP+FN+TP} \quad (19)$$

$$\text{Sensitivity} = \frac{TP}{TP+FN} \quad (20)$$

$$\text{Precision} = \frac{TP}{TP+FP} \quad (21)$$

$$\text{F1} - \text{Score} = \frac{2*\text{Precision}*\text{Recall}}{\text{Precision}+\text{Recall}} \quad (22)$$

$$\text{Specificity} = \frac{TN}{TN+FP} \quad (23)$$

The percentage of samples that are accurately identified as negative is known as the true positive (TP), the false negative (FN), the true negative (TN), the proportion of samples misclassified as positive, and the proportion of samples wrongly classified as positive is known as the false positive (FP).

Table 4: Classification analysis of the proposed Efficient Net model

Models	ACC	PR	RC	SPEC	F1
ANN	91.61	92.14	93.15	91.33	92.23
AlexNet	94.53	93.25	95.47	93.55	93.34
VGG16	96.34	94.58	96.33	95.62	95.26
ResNet	97.65	96. 67	97.65	97.56	97.61
Proposed EfficientNet model	98.88	98.87	98.23	98.55	98.56

To compare different models for classifying OC tasks, as shown in Table 4, measurements of their effectiveness were taken. Included were accuracy (ACC), precision (PR), recall (RC), specificity (SPEC) and F1 score. The Artificial Neural Network (ANN) performed well, achieving an accuracy of 91.61%. Its scores for precision, recall, specificity, and F1 were 92.14%, 93.15%, 91.33%, and 92.23%, respectively. The AlexNet network worked better. It got 94.53% correct answers. Its precision, recall, specificity, and F1 score were 93.25%, 95.47%, 93.55%, and 93.34%, respectively.

VGG16 outperformed earlier models with an accuracy of 96.34%. It achieved strong results for precision, recall, specificity, and F1 score, with values of 94.58%, 96.33%, 95.62%, and 95.26%, respectively. The ResNet model further improved performance. It achieved 97.65% accuracy, with 96.67% precision, 97.65% recall, 97.56% specificity, and a F1 score of 97.61%. Lastly, the suggested EfficientNet model did very well. It outperformed all other models with an accuracy rate of 98.88%. These numbers for the model were equally good, with precision, recall, specificity, and F1-score at 98.87%, 98.23%, 98.55%, and 98.56%, respectively.

4.3. Privacy Validation

Entropy Analysis: Entropy measures the level of uncertainty or randomness in the hidden image from the encrypted picture. More mixing and puzzling occur during the locking process, as indicated by a higher entropy.

$$H(X) = -\sum_{i=1}^{N} P(x_i) \cdot \log_2 \left(P(x_i)\right) \quad (24)$$

Peak Signal-to-Noise Ratio (PSNR): When comparing the encrypted picture with the original one, PSNR measures the quality of the encrypted image. Higher PSNR values show better preservation of image quality.

$$PSNR = 10 \cdot \log_{10} \left(\frac{Max^2}{MSE}\right) \quad (25)$$

Correlation Coefficient: A correlation coefficient is used to determine how closely the first and coded pictures resemble each other. A lower correlation number means stronger encryption.

$$\text{Correlation Coefficient} = \frac{\sum_{i=1}^{N}(X_i - \bar{X})(Y_i - \bar{Y})}{\sqrt{\sum_{i=1}^{N}(X_i - \bar{X})^2 \cdot \sum_{i=1}^{N}(Y_i - \bar{Y})^2}} \quad (26)$$

Number of Pixels Change Rate (NPCR): The difference between the original and hidden images is measured by how many pixels are different. This is called NPCR. A higher NPCR indicates a more even distribution of pixel values.

$$NPCR = \frac{1}{N \times M} \sum_{i=1}^{N} \sum_{j=1}^{M} \delta_{i,j} \quad (27)$$

where $\delta_{i,j}$ is zero if the corresponding pixels of the original and encrypted images match, and one if they do not.

Unified Average Changing Intensity (UACI): The difference in brightness between matching pixels in the hidden and original photos is measured by using UACI. A smaller UACI indicates that the encryption is working more effectively.

$$UACI = \frac{1}{N \times M} \sum_{i=1}^{N} \sum_{j=1}^{M} \frac{|I_{i,j} - E_{i,j}|}{255} \quad (28)$$

Table 5: Encryption validation analysis of the proposed lightweight model

Models	Entropy	PSNR	CC	NPCR (%)	UACI
AES	6.2	35.4	0.92	95.2	0.012
RSA	6.6	35.8	0.93	96.5	0.009
Blowfish	6.7	36.3	0.95	97.2	0.008
Twofish	6.7	38.6	0.96	98.4	0.006
Proposed Lightweight Encryption Model	6.9	40.5	0.98	99.6	0.001

In the analysis of different encryption types using important measures from Table 5 and Figure 2, natural cryptography methods were tested. The Advanced Encryption Standard (AES) achieved an entropy of 6.2, a PSNR of 35.4, a CC of 0.92, an NPCR of 95.2%, and a UACI of 0.012. The RSA encryption model yielded a slightly higher number, with an entropy of 6.6, a PSNR of 35.8, a CC of 0.93, an NPCR of 96.5%, and a UACI of 0.009.

Blowfish made more improvements. It reached an entropy of 6.7, a PSNR of 36.3, a CC of 0.95, an NPCR of 97.2%, and a UACI of 0.008. Two fish followed this pattern, with an entropy of 6.7, a PSNR of 38.6, a CC of 0.96, an NPCR of 98.4%, and a UACI of 0.006. Importantly, the proposed Lightweight Encryption model proved to be the most effective. It had an entropy of 6.9, a PSNR of 40.5, a CC of 0.98, an NPCR of 99.6%, and a UACI of 0.001. This demonstrates that the proposed Lightweight encryption method outperforms others. It offers better security, is more secure, and maintains image quality. This makes it an excellent choice for simple encryption situations.

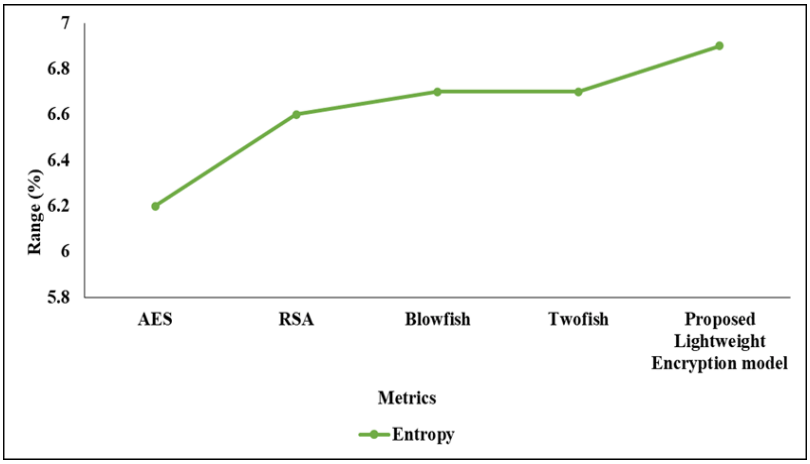

Figure 2: Entropy analysis

When it examined the performance of different encryption models using Table 6 and Figure 3, it determined the average time required for encrypting and decrypting the information. This was measured in a tiny part of a second, called milliseconds. The AES (Advanced Encryption Standard) showed that it takes about 2.45 milliseconds to encrypt information and 2.12 milliseconds to decrypt it. Likewise, the RSA code showed times of 2.36 milliseconds for encoding and 2.05 milliseconds for decoding. Blowfish showed better speed.

Table 6: Computation time analysis of the proposed lightweight encryption model

Models	Average Encryption time (ms)	Average Decryption time (ms)
AES	2.45	2.12
RSA	2.36	2.05
Blowfish	2.21	1.58
Twofish	1.85	1.46
Proposed Lightweight Encryption Model	1.21	1.08

It had an average time to make messages secret (encryption) of 2.21 milliseconds, and an average time to make them normal again (decryption) of 1.58 milliseconds. Twofish further enhanced these performance measures. On average, it took 1.85 seconds for encryption and 1.46 seconds less for decryption. The Lightweight Encryption model that was suggested worked better than all others. This was because it took a very small amount of time to encrypt, with an average of 1.21 milliseconds. It also took the smallest amount of time to decrypt, which was just 1.08 milliseconds. These results demonstrate that the light encryption model is extremely fast and effective in solving problems. This makes it the best choice when you need to encrypt or decode things quickly.

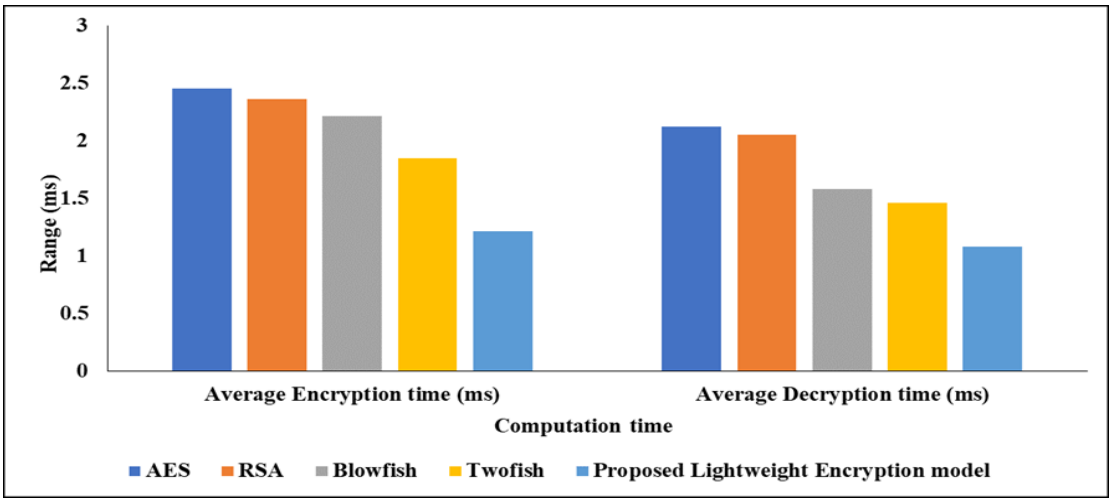

Figure 3: Computation time analysis

5. Conclusion

Ultimately, this research has developed a method for detecting ovarian cancer using the TCGA-OV data and introduced a new technique called Mean-Median-Gaussian (MMG) filtering. It utilises the Faster SqueezeNet model to extract features and then employs the EfficientNet network to classify them. This indicates that it improves diagnosis. The commitment to protecting patient information is evident in the new Lightweight Image Encryption Scheme. It utilises DNA coding and the Lorenz Chaotic System to safeguard data. Using the Child Drawing Development Optimisation Algorithm (CDDOA) for optimal key selection enhances the strength of this encryption method. These efforts represent a significant step forward in ensuring accuracy and safety in ovarian cancer research. They set an example for combining new technology in medical gene studies. This big plan helps us learn more about ovarian cancer. It also makes a guide for proper and safe data handling in medical studies. The proposed EfficientNet model achieves outstanding ovarian cancer classification metrics, with an accuracy of 98.88%, a precision of 98.87%, a recall of 98.23%, a specificity of 98.55%, and an F1 score of 98.56%. Additionally, the proposed Lightweight Encryption model demonstrates superior security, with an entropy of 6.9, a PSNR of 40.5, and remarkable efficiency, achieving an average encryption time of 1.21 milliseconds and an average decryption time of 1.08 milliseconds. Future work may focus on refining the Mean-Median-Gaussian hybrid filtering, adjusting model settings, and expanding the suggested protection plan. Using new technologies and bigger data sets can help us make improvements.

Acknowledgement: The authors sincerely acknowledge Quest Technologies, New Horizon College of Engineering, Saranathan College of Engineering, and Beanibazar Cancer and General Hospital for their valuable support, guidance, and collaboration in the successful completion of this research work.

Data Availability Statement: The data supporting this study are available upon reasonable request from the corresponding author, subject to ethical and institutional data-sharing policies.

Funding Statement: This research received no specific grant or financial support from any funding agency or organisation.

Conflicts of Interest Statement: The authors declare no financial or personal conflicts of interest that could have influenced this work.

Ethics and Consent Statement: The study adhered to institutional ethical standards, with approval obtained and informed consent obtained from all participants.

References

1. B. Aksoy and O. K. M. Salman, “A new hybrid filter approach for image processing,” *Sakarya University Journal of Computer and Information Sciences,* vol. 3, no. 3, pp. 334–342, 2020.
2. B. Ziyambe, A. Yahya, T. Mushiri, M. U. Tariq, Q. Abbas, M. Babar, M. Albathan, M. Asim, A. Hussain, and S. Jabbar, “A deep learning framework for the prediction and diagnosis of ovarian cancer in pre- and post-menopausal women,” *Diagnostics,* vol. 13, no. 10, p. 1703, 2023.
3. C. C. Gajjela, M. Brun, R. Mankar, S. Corvigno, N. Kennedy, Y. Zhong, J. Liu, A. K. Sood, D. Mayerich, S. Berisha, and R. Reddy, “Leveraging mid-infrared spectroscopic imaging and deep learning for tissue subtype classification in ovarian cancer,” *Analyst*, vol. 148, no. 12, pp. 2699–2708, 2023.
4. D. A. Binas, P. Tzanakakis, T. L. Economopoulos, M. Konidari, C. Bourgioti, L. A. Moulopoulos, and G. K. Matsopoulos, “A novel approach for estimating ovarian cancer tissue heterogeneity through the application of image processing techniques and artificial intelligence,” *Cancers*, vol. 15, no. 4, p. 1058, 2023.
5. F. Castro, D. Impedovo, and G. Pirlo, “A medical image encryption scheme for secure fingerprint-based authenticated transmission,” *Applied Sciences,* vol. 13, no. 10, p. 6099, 2023.
6. H. Chen, B. -W. Yang, L. Qian, Y. -S. Meng, X. -H. Bai, X. -W. Hong, X. He, M. -J. Jiang, F. Yuan, Q. -W. Du, and W. -W. Feng, “Deep learning prediction of ovarian malignancy at US compared with O-RADS and expert assessment,” *Radiology*, vol. 304, no. 1, pp. 106–113, 2022.
7. H. Farahani, J. Boschman, D. Farnell, A. Darbandsari, A. Zhang, P. Ahmadvand, S. J. M. Jones, D. Huntsman, M. Köbel, C. B. Gilks, N. Singh, and A. Bashashati, “Deep learning-based histotype diagnosis of ovarian carcinoma whole-slide pathology images,” *Modern Pathology*, vol. 35, no. 9, pp. 1983–1990, 2022.
8. H. H. Maria, A. M. Jossy, and S. Malarvizhi, “A hybrid deep learning approach for detection and segmentation of ovarian tumours,” *Neural Computing and Applications,* vol. 35, no. 21, pp. 15805–15819, 2023.
9. J. Breen, K. Allen, K. Zucker, P. Adusumilli, A. Scarsbrook, G. Hall, N. M. Orsi, and N. Ravikumar, “Artificial intelligence in ovarian cancer histopathology: a systematic review,” *NPJ Precision Oncology*, vol. 7, no. 1, p. 83, 2023.

10. J. Selvaraj, W. C. Lai, B. P. Kavin, and G. H. Seng, “Cryptographic encryption and optimization for Internet of Things-based medical image security,” *Electronics,* vol. 12, no. 7, p. 1636, 2023.
11. J. Wu, J. Zhang, D. Liu, and X. Wang, “A multiple-medical-image encryption method based on SHA-256 and DNA encoding,” *Entropy,* vol. 25, no. 6, p. 898, 2023.
12. K. F. Handley, T. T. Sims, N. W. Bateman, D. Glassman, K. I. Foster, S. Lee, J. Yao, B. M. Fellman, J. Liu, Z. Lu, K. A. Conrads, B. L. Hood, W. Barakat, L. Zhao, J. Zhang, S. N. Westin, J. Celestino, K. M. Rangel, S. Badal, I. Pereira, P. T. Ram, G. L. Maxwell, L. S. Eberlin, P. A. Futreal, R. C. Bast Jr, N. D. Fleming, T. P. Conrads, and A. K. Sood, “Classification of high-grade serous ovarian cancer using tumor morphologic characteristics,” *JAMA Network Open*, vol. 5, no. 10, p. e2236626, 2022.
13. K. Lata and L. R. Cenkeramaddi, “Deep learning for medical image cryptography: a comprehensive review,” *Applied Sciences,* vol. 13, no. 14, p. 8295, 2023.
14. M. A. Fetteha, W. S. Sayed, and L. A. Said, “A lightweight image encryption scheme using DNA coding and chaos,” *Electronics,* vol. 12, no. 24, p. 4895, 2023.
15. M. Al Duhayyim, H. G. Mohamed, J. S. Alzahrani, R. Alabdan, A. S. A. Aziz, A. S. Zamani, I. Yaseen, and M. I. Alsaid, “Sandpiper optimization with a deep learning-enabled fault diagnosis model for complex industrial systems,” *Electronics*, vol. 11, no. 24, p. 4190, 2022.
16. M. J. Sundari and N. C. Brintha, “An intelligent black widow optimization on image enhancement with deep learning-based ovarian tumor diagnosis model,” *Computer Methods in Biomechanics and Biomedical Engineering: Imaging and Visualization,* vol. 11, no. 3, pp. 598–605, 2023.
17. M. Köbel and E. Y. Kang, “The evolution of ovarian carcinoma subclassification,” *Cancers*, vol. 14, no. 2, p. 416, 2022.
18. R. M. Ghoniem, A. D. Algarni, B. Refky, and A. A. Ewees, “Multimodal evolutionary deep learning model for ovarian cancer diagnosis,” *Symmetry,* vol. 13, no. 4, p. 643, 2021.
19. S. Abdulhameed and T. A. Rashid, “Child drawing development optimization algorithm based on child’s cognitive development,” *Arabian Journal for Science and Engineering*, vol. 47, no. 2, pp. 1337–1351, 2022.
20. S. Acharya, D. Ghosh, H. Swapnarekha, M. Mishra, and S. Nayak, “Integrative data analysis and automated deep learning technique for ovary cancer detection,” *in Computational Intelligence in Cancer Diagnosis*, *Academic Press,* Massachusetts, United States of America, 2023.
21. S. T. Ahmed, D. A. Hammood, R. F. Chisab, A. Al-Naji, and J. Chahl, “Medical image encryption: a comprehensive review,” *Computers,* vol. 12, no. 8, p. 160, 2023.
22. T. Nazir, M. M. Iqbal, S. Jabbar, A. Hussain, and M. Albathan, “EfficientPNet—an optimized and efficient deep learning approach for classifying disease of potato plant leaves,” *Agriculture,* vol. 13, no. 4, p. 841, 2023.
23. T. Saida, K. Mori, S. Hoshiai, M. Sakai, A. Urushibara, T. Ishiguro, M. Minami, T. Satoh, and T. Nakajima, “Diagnosing ovarian cancer on MRI: a preliminary study comparing deep learning and radiologist assessments,” *Cancers*, vol. 14, no. 4, p. 987, 2022.
24. U. M. Zamwar and A. P. Anjankar, “Aetiology, epidemiology, histopathology, classification, detailed evaluation, and treatment of ovarian cancer,” *Cureus*, vol. 14, no. 10, p. e30561, 2022.
25. Y. Jung, T. Kim, M. -R. Han, S. Kim, G. Kim, S. Lee, and Y. J. Choi, “Ovarian tumor diagnosis using deep convolutional neural networks and a denoising convolutional autoencoder,” *Scientific Reports*, vol. 12, no. 1, p. 17024, 2022.