Vol.67: e24240214, 2024
https://doi.org/10.1590/1678-4324-2024240214
ISSN 1678-4324 Online Edition

BABT
Brazilian Archives of Biology and Technology

Article - Engineering, Technology and Techniques

Blockchain Enabled Secure Medical Data Transmission and Diagnosis Using Golden Jackal Optimization Algorithm with Deep Learning

Kiruthikadevi Kulandaivelu[1*]
https://orcid.org/0009-0009-6010-3160

SivarajRajappan[1]
https://orcid.org/0000-0001-8170-5130

Vijayakumar Murugasamy[2]
https://orcid.org/0000-0002-5901-8980

[1]Nandha College of Technology, Department of CSE, Erode, Tamilnadu, India; [2]Sasurie College of Engineering, Department of CSE, Tamilnadu, India.

Editor-in-Chief: Alexandre Rasi Aoki
Associate Editor: Fabio Alessandro Guerra

Received: 04-Mar-2024; Accepted: 13-May-2024

*Correspondence: kiruthikadevi.k@outlook.com; (K.K.).

HIGHLIGHTS

- BGJOA-DLSMTD algorithm is to analyze the disease with a high detection rate.
- GJOA with a homomorphism encryption system is employed.
- DL techniques leverage intricate patterns within healthcare information to enhance the accuracy.

Abstract: The incorporation of deep learning (DL) and blockchain (BC) technologies in healthcare revolutionizes disease diagnoses and improves data security. The tamper-resistant and decentralized nature of BC safeguards the integrity and confidentiality of medical records, alleviating the risk of any unauthorized access. At the same time, DL techniques leverage intricate patterns within healthcare information to enhance the accuracy and speed of disease diagnoses. With this motivation, this article proposes a new BC with a golden jackal optimization algorithm enabled DL assisted secure medical data transmission and diagnoses (BGJOA-DLSMTD). The objective of the BGJOA-DLSMTD algorithm is to analyze the disease with a high detection rate and securely transfer the medical images. The BGJOA-DLSMTD algorithm integrates various levels of operations namely encryption, image acquisition, BC, and diagnostic process. Initially, GJOA with a homomorphism encryption system is employed for the process of image encryption wherein the optimum keys could be produced by the GJOA technique. Also, BC is implemented to store the encrypted imageries. Next, the diagnostic method includes Bayesian optimization algorithm (BOA) based hyper parameter tuning, deep belief network (DBN)-based classification, and CapsNet-based feature extraction. The empirical analysis of the proposed BGJOA-DLSMTD algorithm has been demonstrated by means of standard medical images and the outcomes underlined the superior achievement of the BGJOA-DLSMTD algorithm.

Keywords: Blockchain; Medical Data; Internet of Things; Homomorphic Encryption; Golden Jackal Optimization; Hyper parameter Tuning.

INTRODUCTION

The IoT has developed conventional medical systems into intelligent systems by permitting constant monitoring and remote access to patient information [1]. For instance, the wearable, and numerous IoT-enabled medical devices have been employed for gathering real-time physiological information from patients like blood glucose levels, body temperature, and alternative relevant data [2]. In fact, the IoT will support the medical sector with respect to remotely fast diagnosis and efficient medical treatment. However, the IoT nodes in an IoT-assisted medical system have been linked around the clock by employing an open unprotected public channel constructing the whole network susceptible to eavesdropping, data processing, and alternative safety-relevant problems [3]. Particularly, security issue occurs because of incapacitated safety concerns in communication protocols. By employing rapid expansion in hacking methods in which attacker's efforts to compromise the reliability, integrity, and accessibility of IoT devices and data [4]. Such attacks have not only been conducted under medical network constituents employing malicious or malware software however, they will be established in actual IoT devices with targets to temper its functionality [5]. Privacy complexity in IoT networks describes compromised sensitive, private data by executing active and passive (for example, data poisoning attack) attacks. The active attack targets to get access to collect or modify private data [6]. It provides less resource utilization by the contributing devices in the network and disturbances in their flow of normal communication, whereas the passive attack comprises sniffing important public data contents.

In order to deal with the above-mentioned issues, BC and DL are incorporated to offer a noticeable solution in IoT-assisted medical systems [7]. The main benefits of BC technology in the medical field were the subject of this exploration. The various abilities, accelerators, and combined workflows of BC and how they may increase healthcare distribution all over the world have been figured out and reviewed [8]. A fundamental role in recognizing and preventing misrepresentation in medical analysis, and it will improve data efficacy in the medical industry. Concerns concerning data manipulation in the medical sector could be alleviated by the system's establishment of categories of computer storage patterns and preservation of the highest potential security [9]. Accessibility to data can be interoperable, dynamic, authenticated, and responsible. Various causes why it will be essential for protecting the confidentiality of patients' medical data. Risk mitigation and decentralized data protection have been enhanced by employing BC technology in the medical field [10-11].

This article proposes a new BC with a golden jackal optimization algorithm enabled DL-assisted secure medical data transmission and diagnoses (BGJOA-DLSMTD). The objective of the BGJOA-DLSMTD algorithm is to analyze the disease with a high detection rate and securely transfer the medical images. Initially, GJOA with a homomorphic encryption system is implemented for the process of image encryption where the optimum keys could be produced by the GJOA technique. Also, BC is implemented to store the encrypted imageries. Next, the diagnostic method includes Bayesian optimization algorithm (BOA) based hyperparameter tuning, deep belief network (DBN)-based classification, and CapsNet-based feature extraction. The empirical analysis of the proposed BGJOA-DLSMTD algorithm has been demonstrated by means of standard medical images and the outcomes underlined the superior achievement of the BGJOA-DLSMTD algorithm.

LITERATURE WORKS

In an introduced BC-driven privacy-preserving; EHR analysis employing a sine cosine algorithm (SCA) with a DL model called the BPEHR-SCADL method. This technique mainly designs an artificial fish swarm algorithm (AFSA) with a signcryption method. Moreover, the BPEHR-SCADL method employs BC technology. Additionally, the SCA with a deep feedforward-NN (DFFNN) architecture was utilized for classification. Likewise, the SCA was implemented to optimally adjust the weight and bias values of the DFFNN technique. Neelakandan and coauthors [12] presented an innovative BC with DL supported safe medical data transmission and diagnosis (BDL-SMDTD) system. Mainly, moth flame optimizing with elliptic curve cryptography (MFO-ECC) method was implemented where ECC's optimal key is given by employing MFO. Moreover, BC was employed to save the encoded imaging. Next, the diagnosis method comprises support vector machine (SVM)-enabled classifying, Inception with ResNetv2 and histogram-assisted extracting and segmenting process. Rajasekaran and Duraipandian [13] developed BC and DL techniques, comprising three stages. Primarily, the Efficient Key-assisted Rivest Shamir Adelman (EKRSA) was employed, where keys could be produced by employing circle chaotic map and linear inertia weight-assisted honey badger optimizer (CLHBO) system. A radial basis kernel-assisted linear discriminant analysis (RBKLDA) technique was also implemented. Lastly, the classification was achieved by optimum parameter-centered bidirectional-LSTM (OPCBLSTM).

Lin and coauthors [14] projected an encrypted K-means cluster-assisted stellar consensus protocol (EKMC-SCP) technique. This model implements common client verification dependent upon the elliptic curve Menezes–Qu–Vanstone-assisted message authenticating code (ECMQV-MAC) method in a protective information storage employing Deltoid curve-assisted Pallier cryptosystem (DC-PC) and key generating methods utilizing the Dixon's algorithm assisted Blum–Goldwasser cryptosystem, (DM-BGC). Lastly, data transfer was executed employing EKMC-SCP in the BCN. Kumar and coauthors [15] aimed to permission for BC and smart contracts with DL methods. Particularly, PBDL is initially a BC method. Next, the authenticated data have been employed to develop an innovative DL method that must combine stacked sparse variational-AE with self-attention-assisted BLSTM (SSVAE-BiLSTM). Besides, SSVAE encrypts or converts medical data into new formats. In [16], an IoMT with a BC-assisted SHS employing encryption with an optimum DL (BSHS-EODL) technique was introduced. Primarily, the IoMT devices allow methods of gathering the data, image encryption was utilized, and its key generation technique was executed through the dingo optimizer algorithm (DOA). Lastly, this approach executes disease analysis including voting extreme learning machine (VELM), Bayesian optimization (BO) based parameter tuning, and SqueezeNet.

Sachidananda Murthy and Prasad [17] examined an innovative technique that integrates BC technology with DL methods. The DL technique utilizes advanced-NN models like recurrent and convolutional neural networks RNNs and CNNs for analyzing huge information. By leveraging the robustness of DL, this technique will be automatedly extracting related factors and patterns from intricate neurological data. In [18] a data offloading system dependent upon BC was developed. Notably, a smart contract was developed to confirm protective data offloading. Also, the method develops the rate complexity as a Markov Decision method, resolved by search-assisted deep reinforcement learning (DRL) method wherein the system mutually regards offloading decisions, distributing the radio transmission bandwidth and computational resources, and BC data security controls.

THE PROPOSED METHOD

In this article, we have presented an innovative BGJOA-DLSMTD model. The objective of the BGJOA-DLSMTD algorithm is to diagnose the disease with a high detection rate and securely transfer the medical images. The BGJOA-DLSMTD algorithm integrates various levels of operations namely encryption, image acquisition, BC, and diagnostic process. Figure 1 demonstrates the workflow of BGJOA-DLSMTD methodology.

Image Encryption

The ciphertext can be functioned directly without decryption by Homomorphic encryption [19]. Context encryption function denotes$\mathrm{E_{k1}}$, the decryption function represents $\mathrm{D_{k2}}$, and plaintext will be described $\mathrm{M} = \mathrm{m_1}, \mathrm{m_2}, \cdots, \mathrm{m_n}.\alpha$ and β describe the operation. When the encryption and decryption process fulfill Homomorphic encryption properties and after that, the next formula will be accurate.

$$\alpha\left(\mathrm{E_{k1}}(\mathrm{m_1}), \mathrm{E_{k2}}(\mathrm{m_2}), \cdots, \mathrm{E_{kn}}(\mathrm{m_n})\right) = \beta\left(\mathrm{E_{k1}}(\mathrm{m_1}, \mathrm{m_2}, \cdots, \mathrm{m_n})\right) \quad (1)$$

While data $m_1, m_2, \cdots, m_n$carriesβfunction without leaking, we will encrypt it as $(E_{k1}(m_1), E_{k2}(m_2), \cdots, E_{kn}(m_n)$, and execute$\alpha$ operation for it. The solution must be decoded as $\beta m_1, m_2, \cdots, m_n$. The multiplication homomorphism and addition homomorphism will be given below:

$$\mathrm{m_1}+\mathrm{m_2}+\cdots+\mathrm{m_n} = \mathrm{D_k}(\mathrm{E_k}(\mathrm{m_1})+\mathrm{E_k}(\mathrm{m_2})+\cdots+\mathrm{E_k}(\mathrm{m_n})).$$

$$\mathrm{m_1}\cdot\mathrm{m_2}\cdots\mathrm{m_{n=\ D_k}}(\mathrm{E_k}(\mathrm{m_1})\cdot\mathrm{E_k}(\mathrm{m_2})\cdot\cdots\cdot\mathrm{E_k}(\mathrm{m_n}))$$

To optimally generate the keys for encrypting procedure, the GJOA is used. The GJOA appeals to motivation from the organic populace behaviors and predatory actions of GJs [20]. It is a new meta-heuristic model that uses mathematical models to pretend the hunting behavior of GJ populations, including tracking, searching for prey, encircling, and attacking methods by following the prey-iterative search (PIS). Every individual within the population signifies an early possible solution. The method repeatedly upgrades such population, pretending the behaviors of GJ population till the pack effectively arrests its prey, creating the condition of the algorithm's stopping. Once this condition happens, it specifies no important variation among

the preceding and subsequent groups of the populace, indicating the detection of the best solution. This technique includes 4 leading processes which are mentioned below.

(1) Population initializes

Like other meta-heuristic techniques, the GJO algorithm's initial populace is arbitrarily spread over the search space. It is definite as:

$$Y_0=Y_{min}+rand(Y_{max}-Y_{min}) \quad (2)$$

Whereas Y_0 signifies the initial population. $Y_{\min}$and$Y_{\max}$denotes the search space's lower and upper boundaries, correspondingly. $rand$ represents an arbitrarily generated number within the interval of $[0\ and\ 1]$.

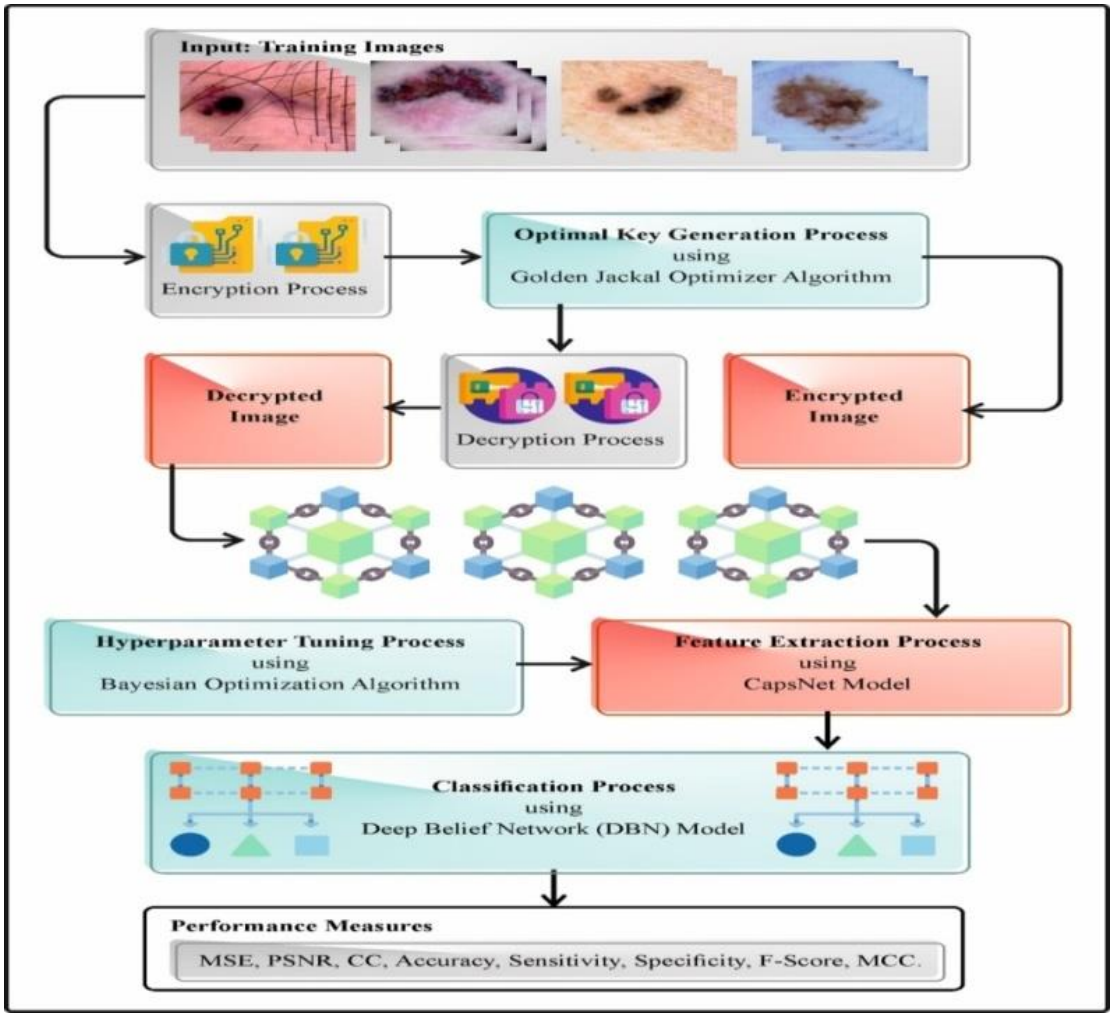

Figure 1. Workflow of BGJOA-DLSMTD methodology

The prey initial matrix is specified as:

$$Prey=\begin{bmatrix} Y_{1,1} & Y_{1,2} & \cdots & Y_{1,d} \\ Y_{2,1} & Y_{2,1} & \cdots & Y_{2,d} \\ \vdots & \vdots & \vdots & \vdots \\ Y_{n,1} & Y_{n,2} & \cdots & Y_{n,d} \end{bmatrix} \quad (3)$$

Here, $y_{i,j}$ denotes the j^{th} dimension value for the i^{th} prey, $Prey$ signifies the prey matrix, n represents the prey counts, and d is the dimensional. Frome the model's iterative procedure, every prey fitness value can be intended to utilize a correct fitness function. So, all the prey fitness values can be stated as below:

$$F_{OA}=\begin{bmatrix} f(Y_{1,1};Y_{1,2};\ldots;Y_{1,d}) \\ f(Y_{2,1};Y_{2,1};\ldots;Y_{2,d}) \\ \vdots \\ f(Y_{n,1};Y_{n,2};\ldots;Y_{n,d}) \end{bmatrix} \quad (4)$$

While f refers to the fitness function and F_{OA} denotes the fitness value matrix.

(2) Searching the prey

GJs show essential independent prey opinion and following abilities naturally. When the existence of prey is confirmed, then the male jackal will take up the leader role and guide the female jackal for searching the prey. The procedure is denoted over the mathematical model as below:

$$Y_1(t)=Y_M(t)-E\cdot|Y_M(t)-rl\cdot Prey(t)| \quad (5)$$

$$Y_2(t)=Y_{FM}(t)-E\cdot|Y_{FM}(t)-rl\cdot Prey(t)| \quad (6)$$

Whereas, $Prey(t)$ refers to the prey location at the t^{th} iteration. t denotes the existing iteration count. $Y_M(t)$ and $Y_{FM}(t)$ denote the locations of male and female jackals at the t^{th} iteration, correspondingly. $Y_2(t)$ and $Y_1(t)$ epitomize the upgraded locations of the female and male jackal. E represents the prey energy function evading the GJ is definite as:

$$E=E_1\cdot E_0 \quad (7)$$

$$E_0=2r-1 \quad (8)$$

$$E_1=c_1(1-(t/T)) \quad (9)$$

Whereas, E_1 embodies the energy decay method of the prey. E_0refers to the prey's initial energy state. r denotes a random number among [0,1]. $c_1$describes a constant value of 1.5. T denotes the highest iteration count.

In Eqs. (5) and (6), rl denotes a randomly formed number from the Levy distribution, and is evaluated utilizing the below-mentioned formulation:

$$rl=0.05LF(y) \quad (10)$$

Where LF is the function of Levy flight that is defined as:

$$LF(y)=0.01\times(\mu\times\sigma)/(|v^{(1/\beta)} \quad (11)$$

Whereas ν and μ are randomly produced numbers among [0, 1]. $\beta = 1.5$.

(3) Encircling and hunting the prey

The prey-lessening escape energy keys to a slow encircling and violence through the populace of GJs. This procedure is exactly signified as:

$$Y_1(t)=Y_M(t)-E\cdot|rl\cdot Y_M(t)-Prey(t)| \quad (12)$$

$$Y_2(t)=Y_{FM}(t)-E\cdot|rl\cdot Y_{FM}(t)-Prey(t)| \quad (13)$$

(4) Comprehending the prey-model termination

The GJ populace helpfully encircles and attacks the target, which finally results in the effective arrest. This method is described as follows:

$$Y(t+1)=\frac{Y_1(t)+Y_2(t)}{2} \quad (14)$$

Whereas $Y(t+1)$depicts the GJ position at the $(t+1)^{th}$ iteration. The parameters $Y_1(t)$ and $Y_2(t)$ do not modify extensively. Also, if $Y(t+1)$ and $Y(t)$ do not change considerably, the GJ effectively arrests the prey, so the algorithm iteration ends, and then it discovers the optimum solutions.

BC Technology

BC technology is used for storing the encrypted images. BC is a unique application model that integrates peer-to-peer transmission, consensus mechanism, encryption algorithm, decentralized data storage, and

alternative techniques for health-related data search technique and also records the storage, which leverages BC [21]. Due to the immutability of BC, the BC-based data storage could not be changed at random. It is utilized as evidence to verify the originality and fluidity of the information. The IPFS, EHR, BC, and data users are four different classes of entities. The IPFS stores the information generated by the healthcare system while safeguarding its search ability, verifiability, and privacy. Through a chain of blocks, a list of records is connected together. This can be reliant on the BC that have a decentralized database. Certain transaction details are maintained in the blocks and a single entity is defined as sets. BC maintains an improved list of records, which can be distributed and immutable. Based on BC technology, the secured asset distribution can be obtained among the non-trusted users by the different systems.

The individual block is formed in the BC network by together chaining the proceedings from genesis (initial block) to the present disseminated block. This block including data of the whole event, is transmitted to the network. The chain will be designed to not be removed, updated, or changed from user's request initiation until the moment the information is received. Once the client disrupts the group's data handling strategies or malicious threat is identified, then it enhances data traceability and performs data forensics in the event. The event lasts until the blocks are distributed into the BC, from the moment a request is made, and a block consists of a singular event. The demand was made and permission should be granted to explore the irregularity as soon as authorized entities want to look into systemic irregularity. The consensus node's responsibility is to report and investigate the outcome of this abnormality. This is due to the fact that blocks are related to the appealing aspect of BC immutability.

Diagnosis Process

Next, the diagnostic method includes BOA-based hyperparameter tuning, DBN-based classification, and CapsNet-based feature extraction.

CapsNet Model

The study proposes a computer vision (CV) technique using CapsNet for improving the recognition procedure's recognition and overcome the limitations of traditional CNN [22]. Before compressing the result into a small vector of highly informative output, Caps Net performs a significant internal computation that has a group of neurons. If installed, this model is based on a Mini column where the capsule learns to find different visual entities through an inadequate set of deformations and observing conditions. The detection probability of capsules will be encoding the factors as output vector length. For instantiation, the factors identified can be directed to the parameter. Subsequently, the feature is transferred via the image. The probability has remained unchanged (the vector's length), but the orientation of the vector changes. Hinton represents the movement as activities equivariant once the object "moves through the diverse of possible arrivals" from the image. At the same time, the detection probability has remained unchanged, which is the type of invariance that we can endeavor instead of the type specified by the CNN with max pooling. The non-linear function named squashing" was applied in Eq. (15) for keeping the direction and length of the input vector within $[0,1]$ to ensure the likelihood of an object or the vector length remains between 0 and 1.

$$R_j=\frac{||p_j||^2}{1+||p_j||^2}\frac{p_j}{||p_j||} \quad 5)$$

In Eq. (15),p_i denotes the input R_j indicates the vector output, and capsules j. The overallcapsuleinputP_j is a weight sum over "prediction vector," $\hat{o}_{j|i}$. By increasing the W_{ij} weight matrix through the capsuleoutput o_i, this capsule in the prior layer was evaluated

$$p_j=\sum_{i=1}^{N} c_{ij}\,\hat{o}_{j|i} \quad (16)$$

$$\hat{o}_{j|i}=W_{ij}o_i \quad (17)$$

Here, c_{ij} indicates "coupling coefficient" attained in the dynamic routing method, the "coupling coefficients" amongi^{th} capsules and capsules layer greater the total to 1 will be defined by softmax which represents the primarylog_bitsb_{ij} of the preceding probability of capsule that must be combined to capsule j.

$$c_{ij}=\frac{\exp(b_{ij})}{\sum_{k}^{} \exp(b_{ij})} \quad (18)$$

Hyperparameter Tuning using BOA

The BOA is utilized for enhancing the black box function which can be a major advantage within its abilities to define the global optimum with some experimental rounds, thereby making it especially suitable for the tasks that need various tests like training architecture of SWMM [23]. The BOA model obtains this proficiency by making a Gaussian process to determine the distribution probability function to be enhanced. Next, exploitation and exploration are balanced by choosing the subsequent experimentation points and iteratively processing the global optima. The advantage of BOA technique includes prior parameter data, which necessitate their robustness and some iterations. The BOA model is mathematically modelled below:

$$P(X|Y)=\frac{P(Y|X)P(X)}{P(Y)} \quad (19)$$

In Eq. (19),$P(X)$ denotes the preceding probability of occurrence X, like the probability of the event of X, $P(Y)$ signifies the probability of existence event Y,X, and Y are two random events; $P(X|Y)$ denotes the posterior probability of occurrence X provided the arise of event Y, like the conditional probability, and$P(Y|X)$ indicates the conditional probability of occurrence Y offered the event of event X.

This BOA method is classified into two primary processes: at first, modelling the objective process that includes evaluating the variance and mean of function value at each point, usually obtained by Gaussian regression process; and next, making an acquisition function that is used to find the succeeding sample point. The techniques find novel search points depending on the prior search point to optimize the effectiveness and accuracy of the model via Gaussian regression and acquisition function.

$$f(x) \approx N\left(\mu(x), \sigma^2(x)\right) \quad (20)$$

In Eq. (20),$\mu(x)$ and$\sigma^2(x)$describe the mean and the variance and N indicates the Gaussian distribution.

The posterior probability of FF values at any discrete could be measured by applying Gaussian process regression. Then, an acquisition function was made depending on the posterior probability that could detect the highest function point as the succeeding search point. The optimal solution could be achieved by iterating this process.

The BOA acquires a fitness function (FF)for the achievement of improved classification effectiveness. This can be determined as a positive numeral for signifying the excellent efficacy of the candidate outputs. In this study, the decrease in the rate of error of the classification can be measured as the FF and is also expressed in Eq. (21).

$$\text{fitness}(x_i)=\text{Classifier Error Rate }(x_i)=\frac{\text{Number of mis classified samples}}{\text{Over all samples}}*100 \quad (21)$$

DBN based Classification

The DL method has been employed for stacking shallow models and accomplishing robust solutions because of improving the depth of the model [24]. The DBNs have been comprised of Restricted Boltzmann Machines (RBMs). During the deep networking, instead of employing one layer of RBM, these will be attached over one another, named a DBN. The word ‘belief’ in mathematics may be created misperception. Normally, a certainty is approximately that one has confidence in, like a divinity, believing astrology, science, and so on. But, in DBNs, the word ‘belief’ defines the data that one can have a faulty subjected assumption regards the objective sign. A DBN has a category of DL-based deterministic-NN and elects weights in a smart manner following the activation functions. Figure 2 depicts the infrastructure of DBN.

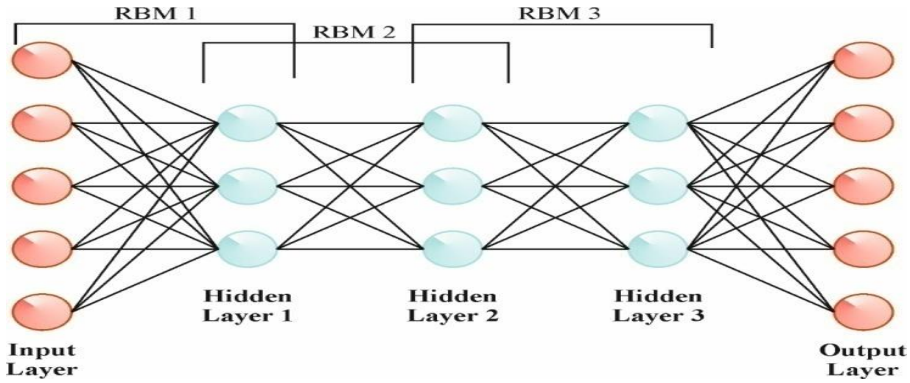

Figure 2. Architecture of DBN

The major inspiration after the DL utilization is to achieve a hierarchical data representation for a specified issue like ranking, regression, classification, and clustering. Mainly, a DBN method for the execution of DLmodels. Nevertheless, it was complex to create it effort while its improvement. As regards the Bayesian network, connects task probabilistic dependency, but, in a NN, there is a neuron correlation. The DBN layers are learned as a hierarchical representation and obtained by RBMs stacked over each other. Alternatively, an RBM was determined in each level of the DBN according to distinctive features. Generally, an unsupervised technique has been employed for training a DBN stage by stage. If the primary RBM has been trained, an alternative one will be loaded on top, and also method must be repeated. The gathering of RBMs to develop a DBN is similar to collecting AE for training a SAE. Meanwhile, DBNs have generative probabilistic methods, developed by making the latent representation in the existing level by taking from the previous stage as the input, producing them capable of dynamic data allocations.

RESULT ANALYSIS AND DISCUSSION

The performance analysis of the BGJOA-DLSMTD approach occurs using the ISIC dataset [25]. Figure 3 depicts the sample imageries.

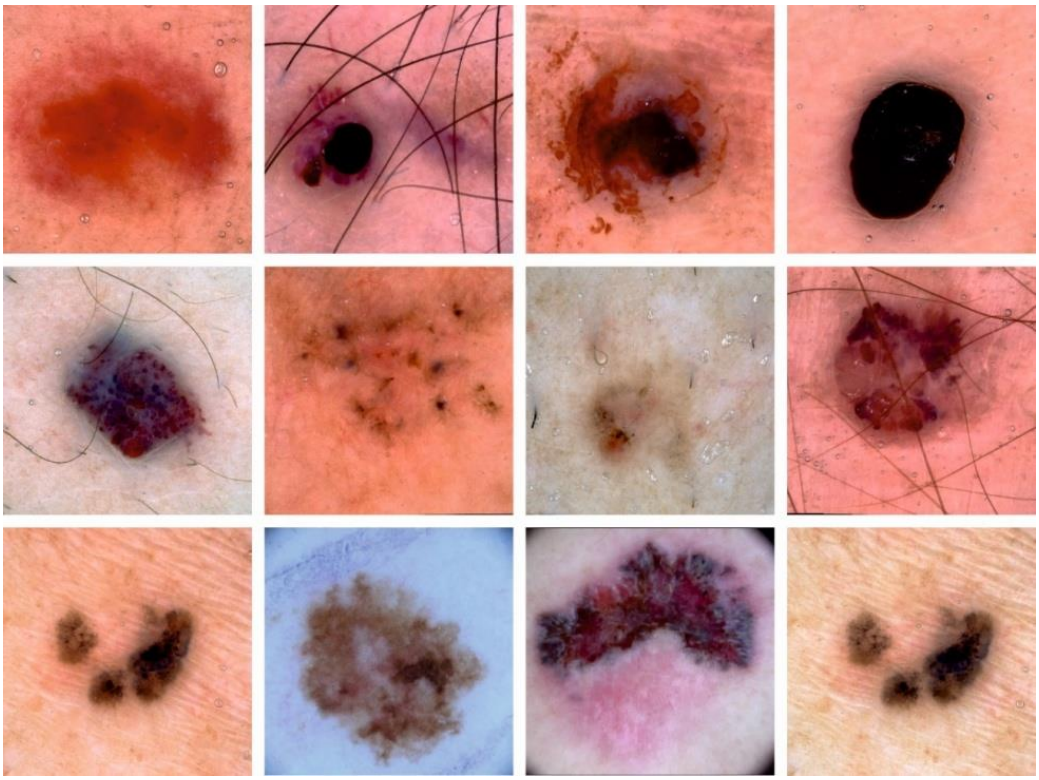

Figure 3. Sample Images

In Table 1, a detailed MSE and PSNR investigation of the BGJOA-DLSMTD method with present approaches is made.

Table 1. MSE and PSNR outcomes of the BGJOA-DLSMTD model with other algorithms under distinct images

Sample Images	BGJOA-DLSMTD		BSHS-EODL		HOCE-ECC		GO-FFO		GO-PSO		GWO	
	MSE	PSNR	MSE	PSNR	MSE	PSNR	MSE	PSNR	MSE	PSNR	MSE	PSNR
Image 1	0.05	61.14	0.07	59.56	0.11	57.64	0.13	56.93	0.17	55.80	0.20	55.19
Image 2	0.04	61.90	0.06	60.57	0.08	58.94	0.12	57.38	0.15	56.31	0.17	55.78
Image 3	0.06	60.07	0.08	59.21	0.12	57.41	0.15	56.31	0.19	55.39	0.22	54.71
Image 4	0.09	58.59	0.10	58.04	0.13	56.99	0.16	56.17	0.18	55.48	0.21	54.91
Image 5	0.06	60.65	0.07	59.62	0.11	57.84	0.13	57.06	0.17	55.96	0.19	55.44

In Figure 4, the comparative MSE outputs of the BGJOA-DLSMTD model are studied. The results denote that the GWO, GO-PSO, and GO-FFO models have reached increased MSE values. Moreover, the BSHS-EODL and HOCE-ECC methods are reported somewhat reduced MSE values. But, the BGJOA-DLSMTD method attains maximum achievement with the least MSE of 0.05, 0.04, 0.06, 0.09, and 0.06 in accordance with images 1-5, correspondingly.

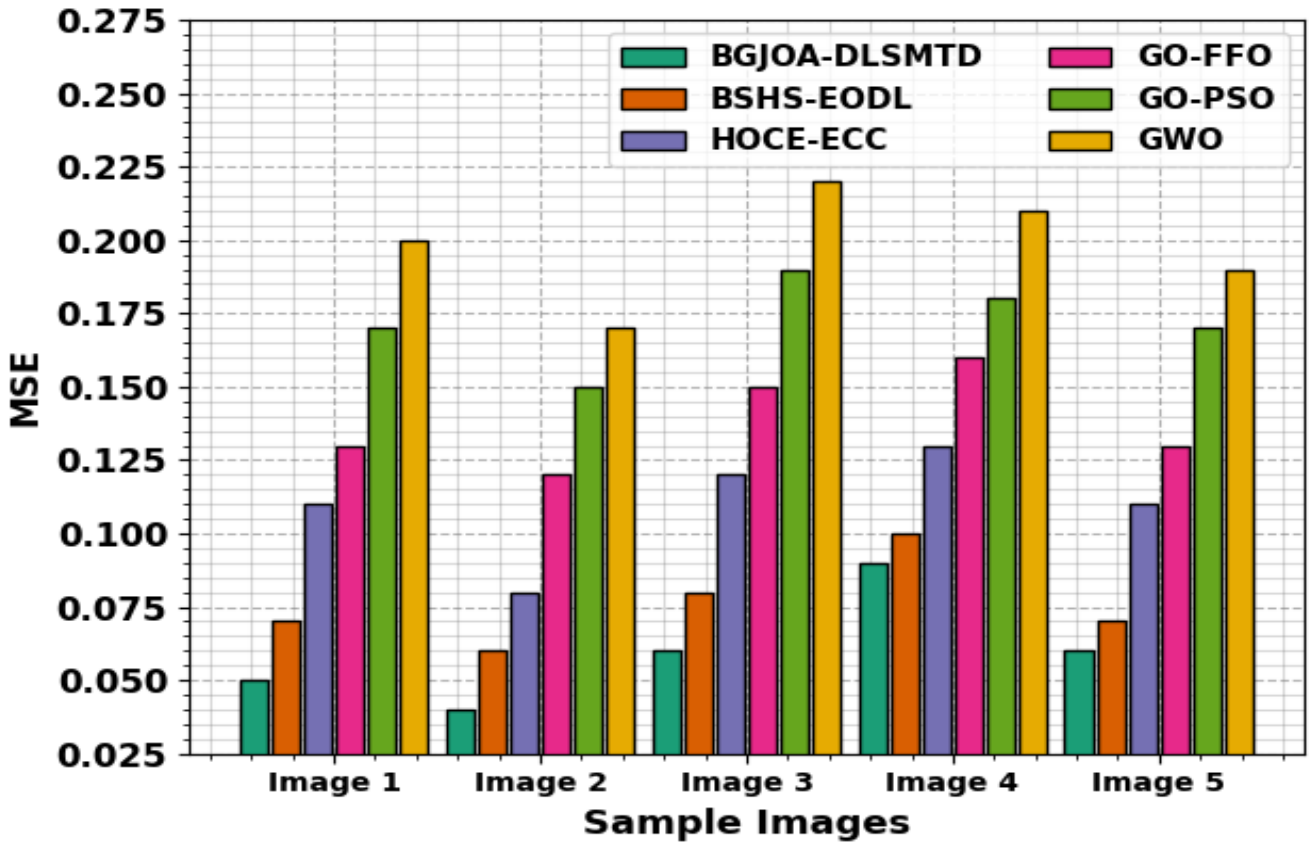

Figure 4. MSE outcome of BGJOA-DLSMTD method under distinct images

In Figure 5, the PSNR outputs of the BGJOA-DLSMTD approach are compared with other ones. These experimentation outcomes highlighted that the GWO, GO-PSO, and GO-FFO approaches have decreased PSNR values. Simultaneously, the BSHS-EODL and HOCE-ECC techniques have demonstrated moderately improved PSNR values. But the BGJOA-DLSMTD method achieves greater performance with increased PSNR of 61.14%, 61.90%, 60.07%, 58.59%, and 60.65% on images 1 to 5.

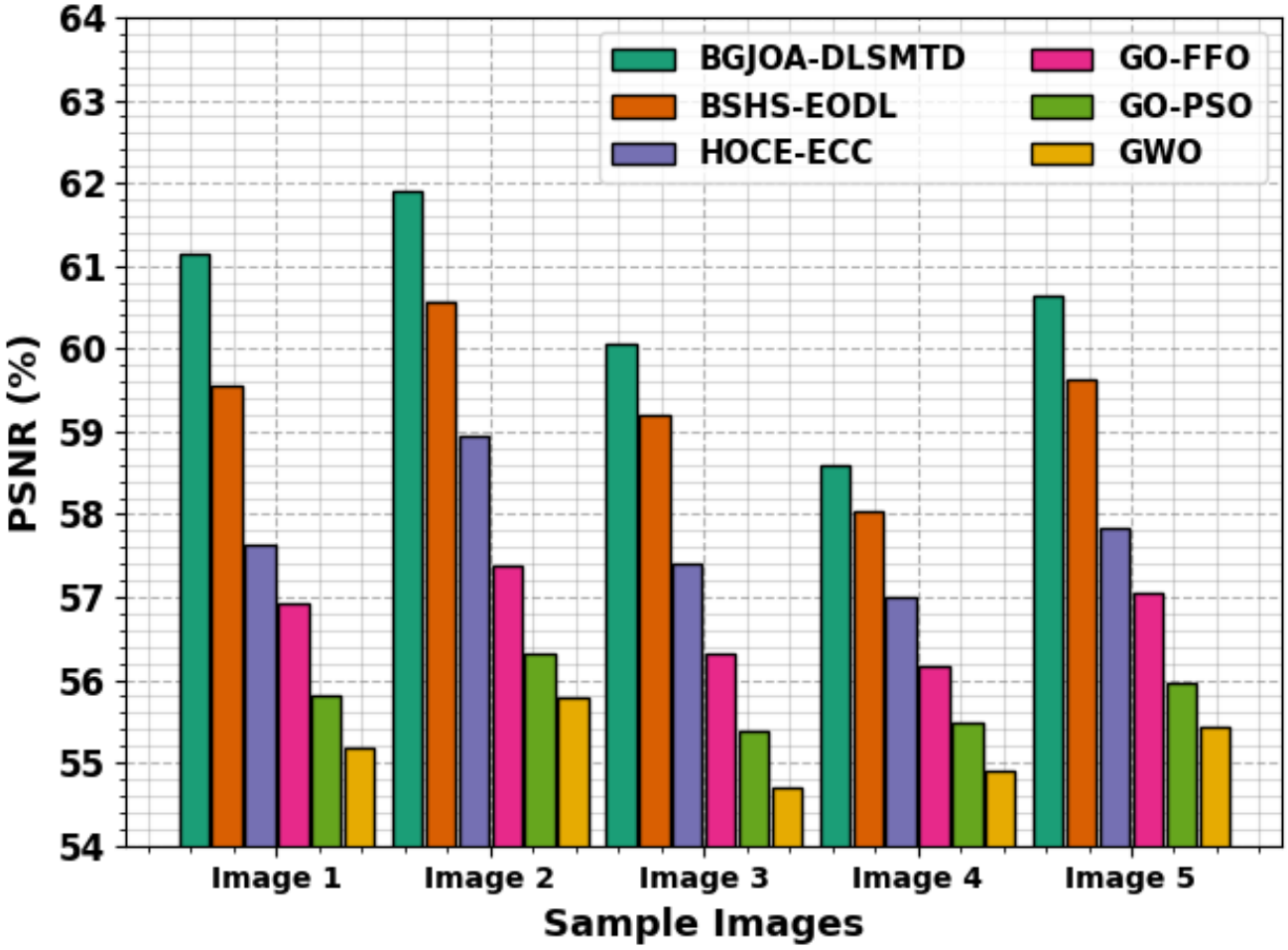

Figure 5. PSNR outcome of the BGJOA-DLSMTD system under distinct images

A comprehensive correlation coefficient (CC) outcome of the BGJOA-DLSMTD system has been compared with present models and illustrated in Table 2 and Figure 6. These accomplished findings emphasized that the GWO, GO-PSO, and GO-FFO algorithms provide minimized CC values. Next, the BSHS-EODL and HOCE-ECC systems have reported considerably boosted CC values. Nevertheless, the BGJOA-DLSMTD method accomplishes excellent performance with higher CC of 99.53%, 99.73%, 99.30%, 99.83%, and 99.79%under 1-5imaging, respectively.

Table 2. CC outcome of the BGJOA-DLSMTD method with other approaches under distinct images

Correlation Coefficient (%)						
Sample Images	**BGJOA-DLSMTD**	**BSHS-EODL**	**HOCE-ECC**	**GO-FFO**	**GO-PSO**	**GWO**
Image 1	99.53	99.42	98.93	98.49	98.16	97.70
Image 2	99.73	99.63	99.22	98.84	98.53	98.18
Image 3	99.30	99.21	98.76	98.45	97.98	97.54
Image 4	99.83	99.72	99.33	99.01	98.65	98.19
Image 5	99.79	99.68	99.37	99.04	98.54	98.22

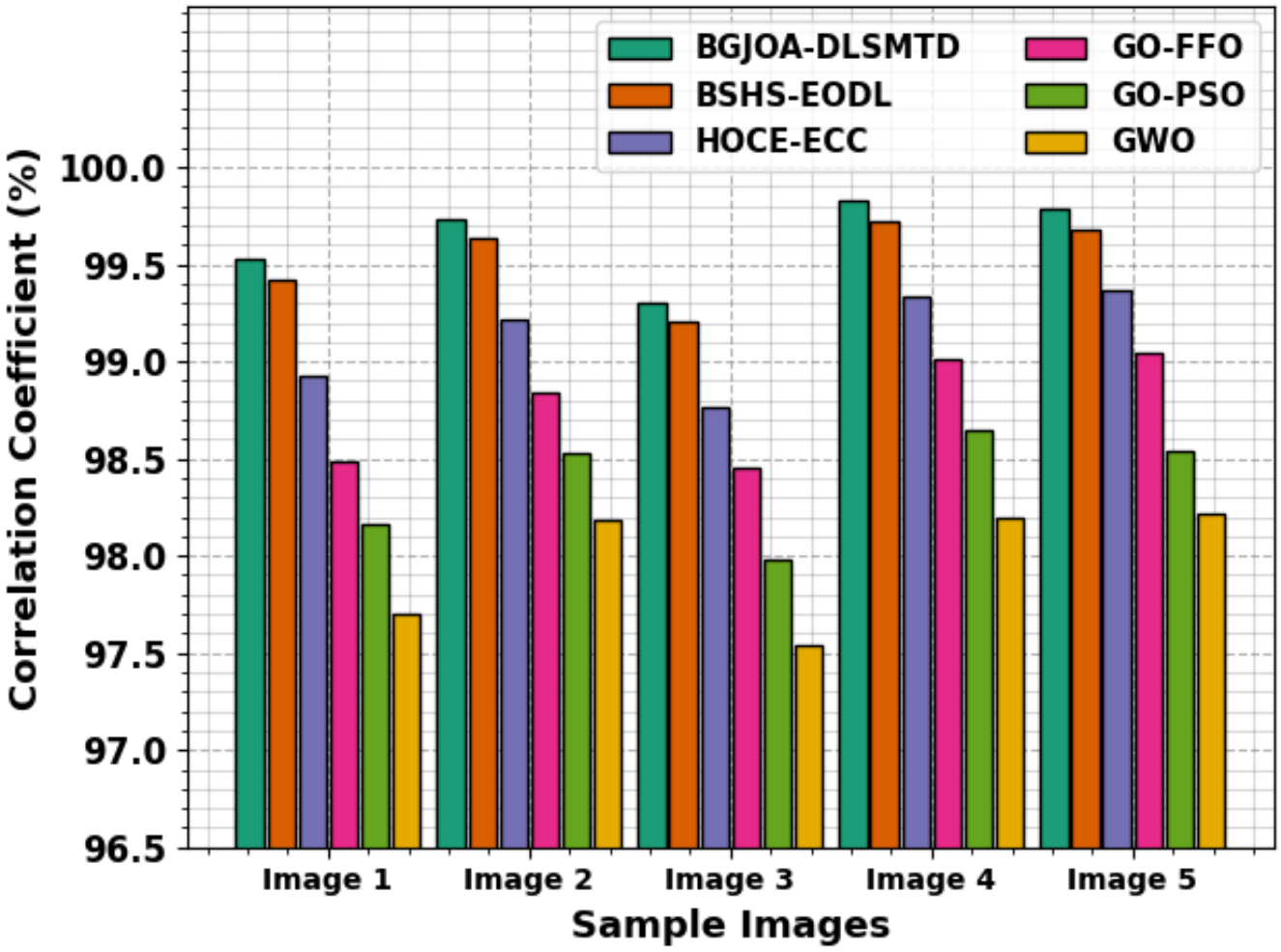

Figure 6. CC outcome of BGJOA-DLSMTD model under distinct images

In Table 3, a wide-ranging computation time (CT) and PSNR during attacks analysis of the BGJOA-DLSMTD method with recent algorithms are examined.

Table 3. CT and PSNR during attacks of BGJOA-DLSMTD algorithm with recent systems under distinct images

			CT (s)			
Sample Images	**BGJOA-DLSMTD**	**BSHS-EODL**	**HOCE-ECC**	**GO-FFO**	**GO-PSO**	**GWO**
Image 1	0.15	0.20	0.50	0.78	0.94	1.29
Image 2	0.06	0.13	0.31	0.51	0.70	1.05
Image 3	0.09	0.16	0.48	0.72	0.92	1.07
Image 4	0.05	0.11	0.45	0.59	0.89	1.03
Image 5	0.10	0.15	0.41	0.68	1.00	1.31
			PSNR During Attacks (dB)			
Image 1	60.50	59.21	57.08	56.47	55.29	54.66
Image 2	61.37	60.17	58.34	56.90	56.01	55.48
Image 3	60.09	58.80	57.01	55.74	54.84	54.38
Image 4	58.86	57.71	56.44	55.61	54.91	54.44
Image 5	60.52	59.31	57.43	56.59	55.42	55.09

An extensive comparative computational time (CT)outcome of the BGJOA-DLSMTD technique is studied and described in Figure 7. These experimentation outcomes indicate that the GWO, GO-PSO, and GO-FFO algorithm gains improved CT values. Meanwhile, the BSHS-EODL and HOCE-ECC methods have described slightly diminished CT values. However, the BGJOA-DLSMTD system offers maximum performance with decreased CT of 0.15s, 0.06s, 0.09s, 0.05s, and 0.10s under images 1-5.

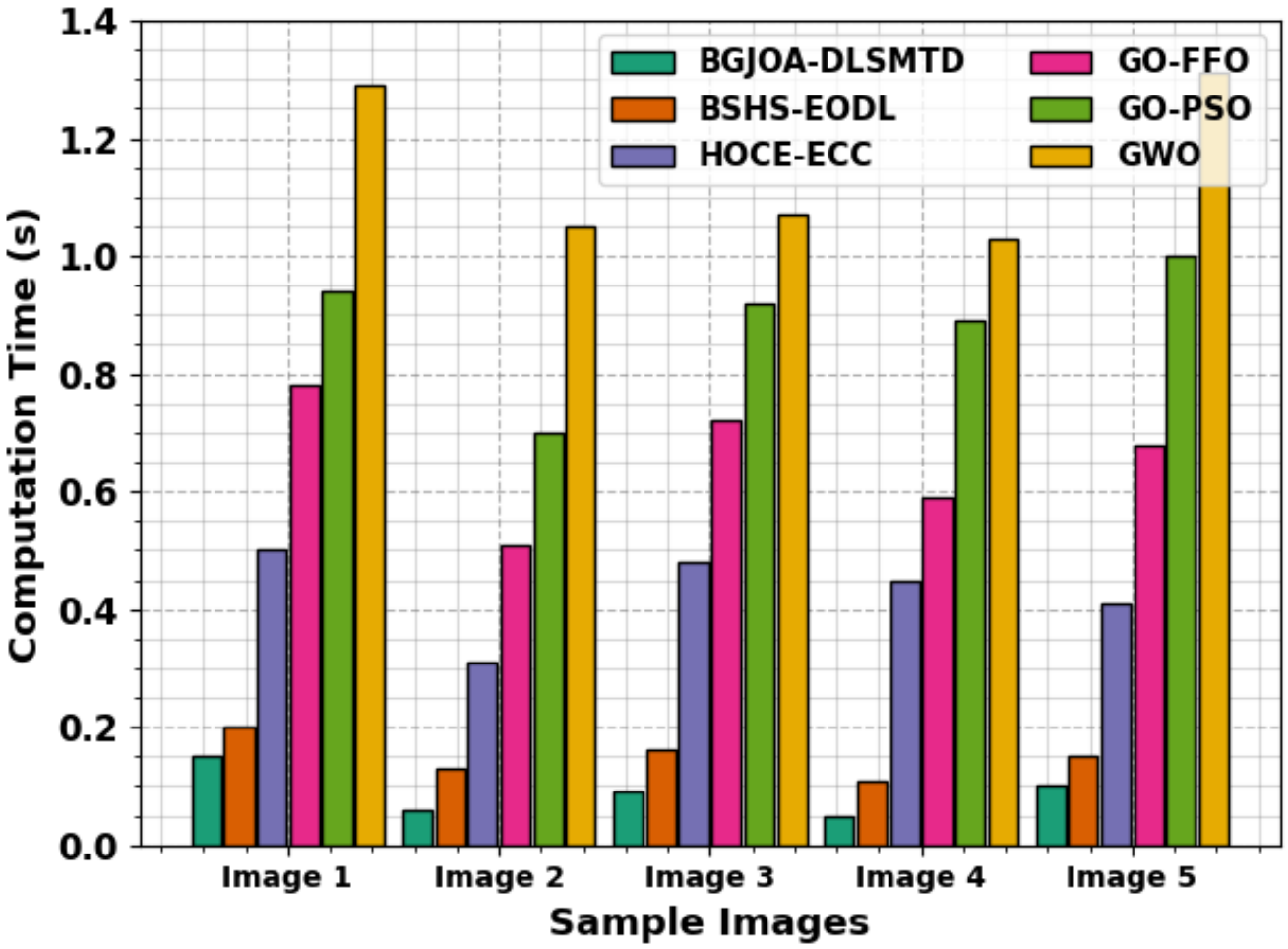

Figure 7. CT outcome of the BGJOA-DLSMTD method under distinct images

In Figure 8, the PSNR during attacks result of the BGJOA-DLSMTD method is compared with existing ones. These obtained results underscored that the GWO, GO-PSO, and GO-FFO techniques have reduced PSNR during attack values. Concurrently, the BSHS-EODL and HOCE-ECC algorithms offer moderately higher PSNR during attack values. But the BGJOA-DLSMTD method attains superior performance with boosted PSNR during attacks of 60.50dB, 61.37dB, 60.09dB, 58.86dB, and 60.52dB on images 1-5, correspondingly.

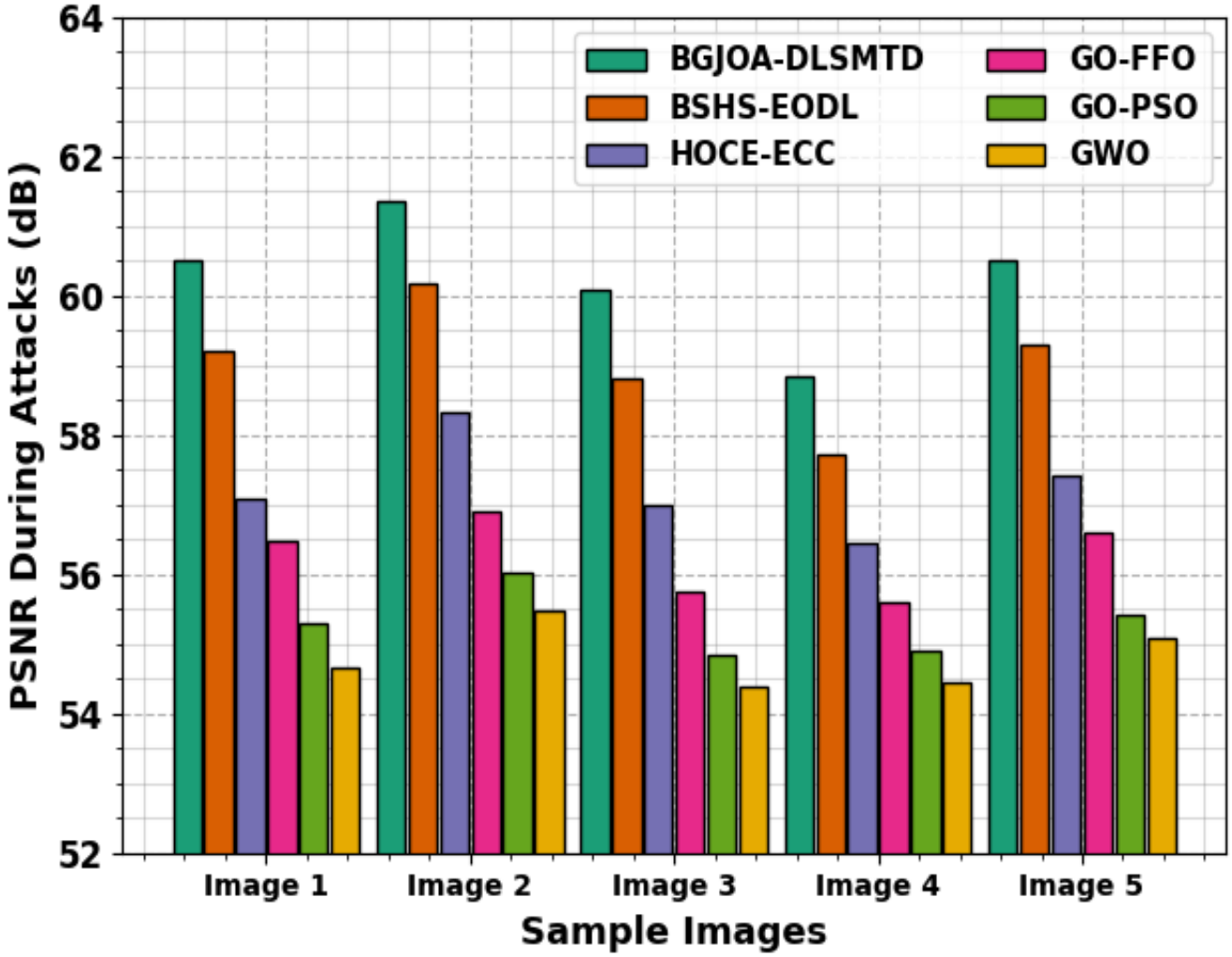

Figure 8. PSNR during attacks of BGJOA-DLSMTD model under distinct images

The dataset encompasses 318 sample images under seven class labels as demonstrated in Table 4.

Table 4. Dataset specification

Labels	Class	Image Numbers
C-0	Angioma	21
C-1	Nevus	46
C-2	Lentigo NOS	41
C-3	Solar Lentigo	68
C-4	Melanoma	51
C-5	Seborrheic Keratosis	54
C-6	BCC	37
Total Image Counts		318

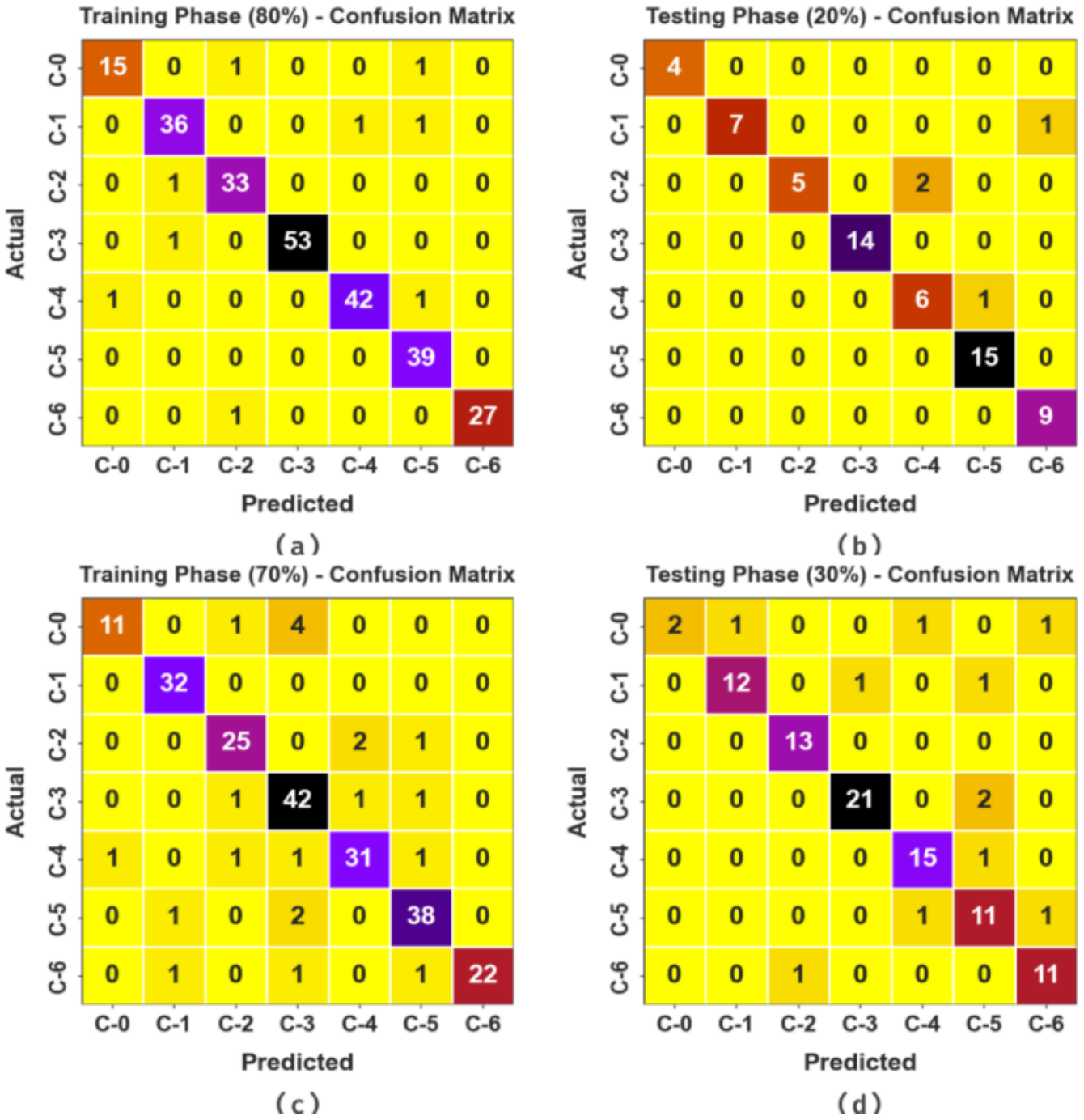

Figure 9. Confusion matrices (a-b) 80:20 and(c-d) 70:30TRAPH/TESPH

Figure 9 portrays the confusion matrices given by the BGJOA-DLSMTD methodat80:20 and 70:30 TRAPH/TESPH. These results indicate the effective recognition with the overall seven classes.

In Table 5 and Figure 10, the classifier values of the BGJOA-DLSMTD technique at 80:20 TRAPH/TESPH under distinct classes are given. These results demonstrate that the BGJOA-DLSMTD technique properly recognized the samples. Based on 80%TRAPH, the BGJOA-DLSMTD technique offers average $accu_y$, $sens_y$, $spec_y$, F_{score}, and MCC of 98.99%, 95.72%, 99.41%, 95.91%, and 95.35%, respectively.Additionally, with 20%TESPH, the BGJOA-DLSMTD method provides average $accu_y$, $sens_y$, $spec_y$, F_{score}, and MCC of 98.21%, 92.09%, 98.95%, 92.60%, and 91.89%.

Table 5. Classifier outcomes of BGJOA-DLSMTD method at 80:20TRAPH/TESPH

ClassLabels	$Accu_y$	$Sens_y$	$Spec_y$	F_{score}	*MCC*
			TRAPH (80%)		
C-0	98.82	88.24	99.58	90.91	90.33
C-1	98.43	94.74	99.07	94.74	93.81
C-2	98.82	97.06	99.09	95.65	94.98
C-3	99.61	98.15	100.00	99.07	98.82
C-4	98.82	95.45	99.52	96.55	95.85
C-5	98.82	100.00	98.60	96.30	95.69
C-6	99.61	96.43	100.00	98.18	97.98
Average	98.99	95.72	99.41	95.91	95.35
			TESPH (20%)		
C-0	100.00	100.00	100.00	100.00	100.00
C-1	98.44	87.50	100.00	93.33	92.72
C-2	96.88	71.43	100.00	83.33	83.07
C-3	100.00	100.00	100.00	100.00	100.00
C-4	95.31	85.71	96.49	80.00	77.58
C-5	98.44	100.00	97.96	96.77	95.83
C-6	98.44	100.00	98.18	94.74	94.00
Average	98.21	92.09	98.95	92.60	91.89

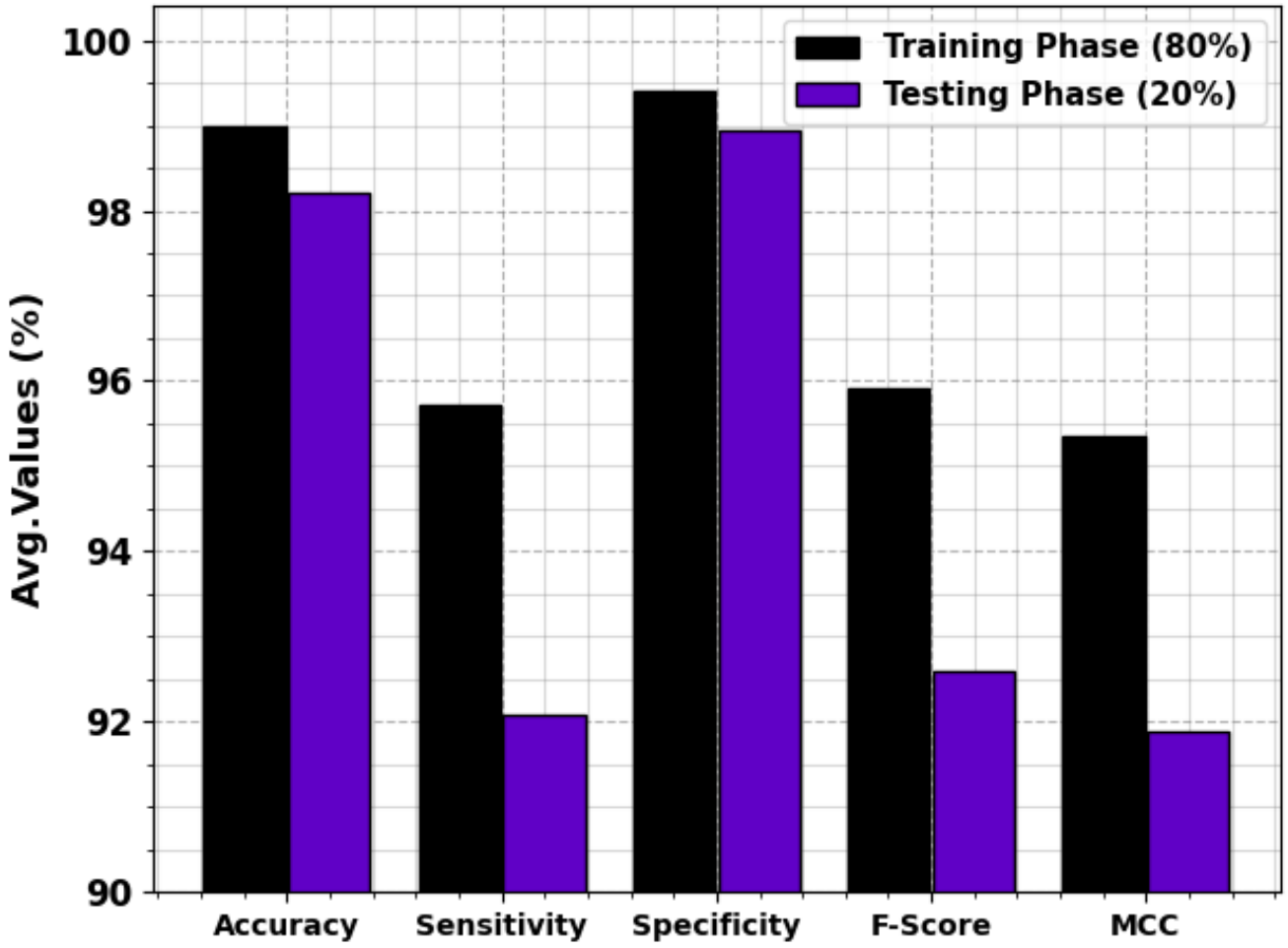

Figure 10. Average of the BGJOA-DLSMTD technique on 80:20 TRAPH/TESPH

Detailed classifier outcomes of the BGJOA-DLSMTD method at 70:30 TRAPH/TESPH and different classes are reported in Table 6 and Figure 11. These achieved outputs exhibit that the BGJOA-DLSMTD

system correctly identified the samples. According to 70%TRAPH, the BGJOA-DLSMTD algorithm obtains average$accu_y$, $sens_y$, $spec_y$, F_{score}, and MCC of 97.30%, 88.66%, 98.37%, 89.76%, and 88.36%, correspondingly. Additionally, with 30% TESPH, the BGJOA-DLSMTD approach gets average $accu_y$, $sens_y$, $spec_y$, F_{score}, and MCC of 96.73%, 83.86%, 98.07%, 84.73%, and 83.87%.

Table 6. Classifier outcomes of the BGJOA-DLSMTD system with 70:30 TRAPH/TESPH

Class Labels	$Accu_y$	$Sens_y$	$Spec_y$	F_{score}	MCC
		TRAPH (70%)			
C-0	97.30	68.75	99.51	78.57	78.07
C-1	99.10	100.00	98.95	96.97	96.50
C-2	97.30	89.29	98.45	89.29	87.74
C-3	95.05	93.33	95.48	88.42	85.47
C-4	96.85	88.57	98.40	89.86	88.00
C-5	96.85	92.68	97.79	91.57	89.64
C-6	98.65	88.00	100.00	93.62	93.10
Average	97.30	88.66	98.37	89.76	88.36
		TESPH (30%)			
C-0	96.88	40.00	100.00	57.14	62.23
C-1	96.88	85.71	98.78	88.89	87.15
C-2	98.96	100.00	98.80	96.30	95.78
C-3	96.88	91.30	98.63	93.33	91.33
C-4	96.88	93.75	97.50	90.91	89.08
C-5	93.75	84.62	95.18	78.57	75.20
C-6	96.88	91.67	97.62	88.00	86.30
Average	96.73	83.86	98.07	84.73	83.87

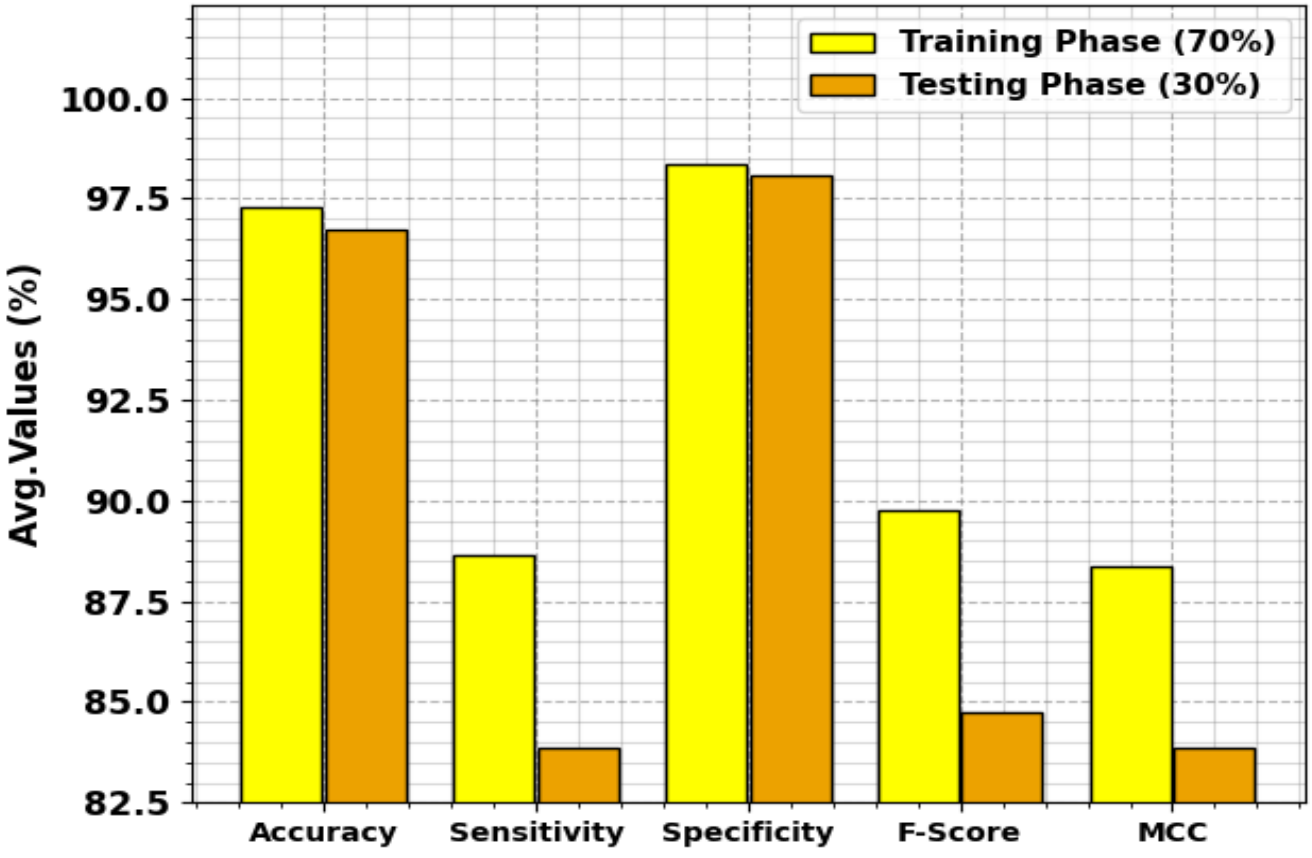

Figure 11. Average of the BGJOA-DLSMTD method on 70:30 TRAPH/TESPH

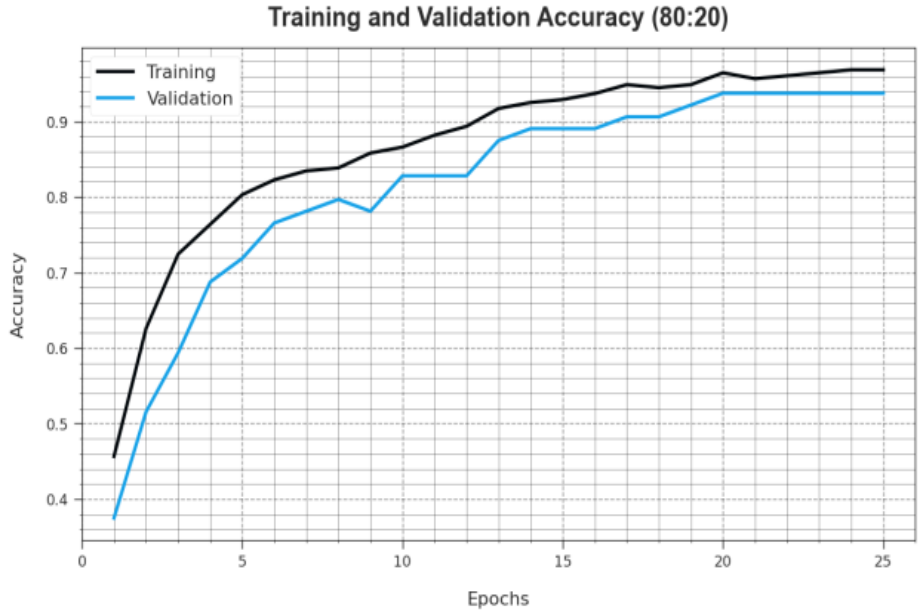

Figure 12. Accuracy curve of the BGJOA-DLSMTD method at 80:20 TRAPH/TESPH

The effectiveness of the BGJOA-DLSMTD approach with 80:20 TRAPH/TESPH is graphically presented in Figure 12 in the form of training accuracy (TRAA) and validation accuracy (VALA) curves. This figure exhibits useful analysis of the behaviour of the BGJOA-DLSMTD technique over varying epoch counts, signifying its learning process and generalization capabilities. Mainly, the figure infers a constant improvement in the TRAA and VALA with progress in epochs. It ensures the adaptive nature of the BGJOA-DLSMTD algorithm in the pattern recognition process under TRA and TES data. The higher trend in VALA outlines the capability of the BGJOA-DLSMTD system to adapt to the TRA data and also surpass to provide accurate classification on undetected data, pointing out the robust generalization abilities.

Figure 13 displays a wide-ranging representation of the training (TRLA) and validation (VALL) loss results of the BGJOA-DLSMTD model on 80:20 TRAPH/TESPH. The progressive result lessens in TRLA highlights the BGJOA-DLSMTD method enhancing the weights and minimizing the classification error on the TRA and TES data. The figure indicates a perfect understanding of the BGJOA-DLSMTD method relevant to the TRA data, highlighting its proficiency in capturing patterns. Significantly, the BGJOA-DLSMTD model incessantly improves its parameters in decreasing the variances among the prediction and real TRA class labels.

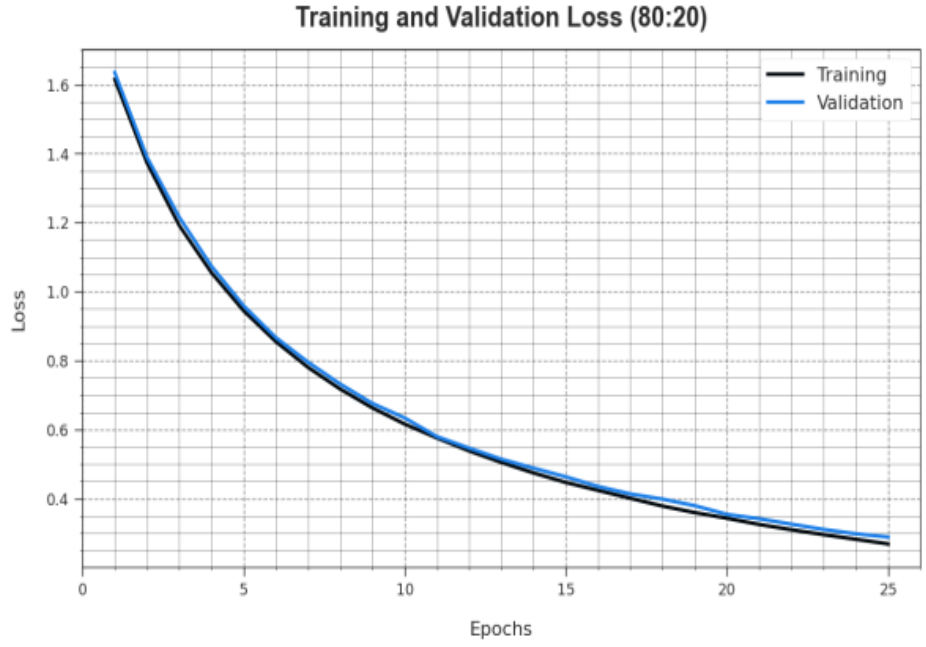

Figure 13. Loss curve of the BGJOA-DLSMTD technique on 80:20 TRAPH/TESPH

The classification results of the BGJOA-DLSMTD approach are compared with recent models in Table 7 [16]. In Figure 14, a relative result analysis of the BGJOA-DLSMTD technique is made in terms of $accu_y$. Based on $accu_y$, the BGJOA-DLSMTD technique gains increased $accu_y$ of 98.99% while the BSHS-EODL, DBN, YOLO-GC, ResNet, VGG19, and CDNN algorithms obtained reduced$accu_y$ of 98.51%, 94.15%, 94.24%, 96.19%, 91.19%, and 95.29%, respectively.

Table 7. Comparative outcomes of the BGJOA-DLSMTD system with other algorithms

Methods	$Accu_y$	$Sens_y$	$Spec_y$
BGJOA-DLSMTD	98.99	95.72	99.41
BSHS-EODL	98.51	92.98	99.11
DBN	94.15	91.40	90.98
YOLO-GC	94.24	89.30	90.77
ResNet	96.19	90.44	91.03
VGG-19	91.19	90.20	93.73
CDNN	95.29	91.19	92.77

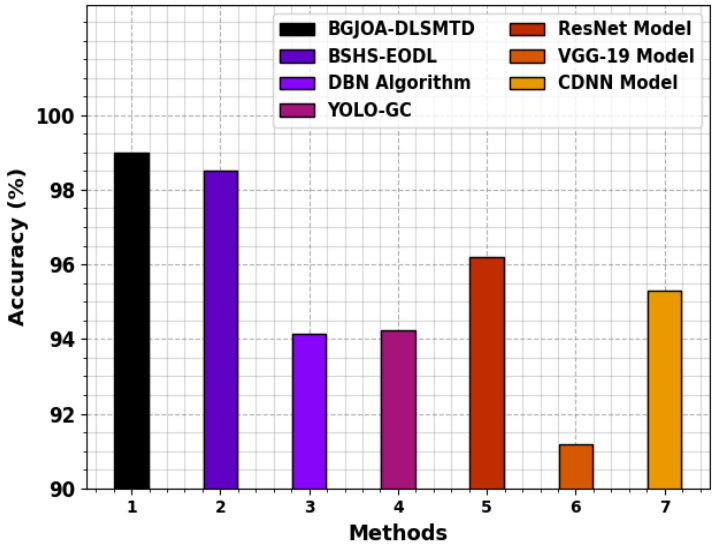

Figure 14. Accuracy result of the BGJOA-DLSMTD model with other methods

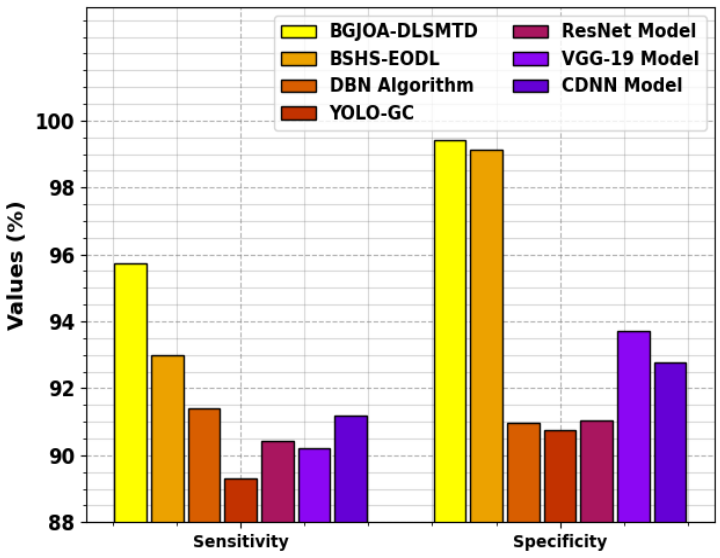

Figure 15. Sensitivity and Specificity result of BGJOA-DLSMTD technique with recent systems

An extensive comparative outcomes of the BGJOA-DLSMTD method has been achieved with respect to$sens_y$ and $spec_y$ as described in Figure 15. According to$sens_y$, the BGJOA-DLSMTD method provides higher $sens_y$ of 95.72% however, the BSHS-EODL, DBN, YOLO-GC, ResNet, VGG19 and CDNN algorithms acquires minimized $sens_y$ of 92.98%, 91.40%, 89.30%, 90.44%, 90.20%, and 91.19%.Similarly, based on$spec_y$, the BGJOA-DLSMTD system got boosted $spec_y$ of 99.41% whereas the BSHS-EODL, DBN, YOLO-GC, ResNet, VGG19 and CDNN techniques gained diminished $spec_y$ of 99.11%, 90.98%, 90.77%, 91.03%, 93.73%, and 92.77%. These experimentation outcomes confirmed the enhanced performance of the BGJOA-DLSMTD method in the healthcare environment.

CONCLUSION

In this article, we have presented an innovative BGJOA-DLSMTD methodology. The objective of the BGJOA-DLSMTD algorithm is to diagnose the disease with a high detection rate and securely transfer the medical images. The BGJOA-DLSMTD algorithm integrates various levels of operations namely encryption, image acquisition, BC, and diagnostic process. Initially, GJOA with homomorphic encryption system is employed for the process of image encryption where the optimum keys are produced by the GJOA technique. In addition, BC technology is implemented for storing the encrypted images. Next, the diagnostic method includes BOA-based tuning, DBN-based classification, and CapsNet-based feature extraction. The empirical analysis of the proposed BGJOA-DLSMTD algorithm has been demonstrated employing standard medical images and the outcomes underlined the superior achievement of the BGJOA-DLSMTD algorithm.

Funding: The authors declare they have no funding applied.
Conflicts of Interest: The authors declare they have no conflicts of interest to report regarding the present study.

REFERENCES

1. Almaiah MA, Ali A, Hajjej F, Pasha MF, Alohali MA. A lightweight hybrid deep learning privacy preserving model for FC-based industrial internet of medical things. Sensors (Basel). 2022;22(6):2112. https://doi.org/10.3390/s22062112.
2. Khan AA, Wagan AA, Laghari AA, Gilal AR, Aziz IA, Talpur BA. BIoMT: A state-of-the-art consortium serverless network architecture for healthcare system using blockchain smart contracts. IEEE Access. 2022;10:78887–98. https://doi.org/10.1109/ACCESS.2022.3194195.
3. Abbas A, Alroobaea R, Krichen M, Rubaiee S, Vimal S, Almansour FM. Blockchain-assisted secured data management framework for health information analysis based on Internet of Medical Things. Pers Ubiquitous Comput. 2021;1–14. https://link.springer.com/article/10.1007%2Fs00779-021-01626-0.
4. Garg N, Wazid M, Das AK, Singh DP, Rodrigues JJ, Park Y. BAKMP-IoMT: Design of blockchain enabled authenticated key management protocol for internet of medical things deployment. IEEE Access. 2020;8:95956–77. https://doi.org/10.1109/ACCESS.2020.2995917.
5. Kalimuthu VK, Velumani R. Modeling of Intrusion Detection System Using Double Adaptive Weighting Arithmetic Optimization Algorithm with Deep Learning on Internet of Things Environment. Braz Arch Biol Technol. 2024;67. https://doi.org/10.1590/1678-4324-2024231010.
6. Razdan S, Sharma S. Internet of medical things (IoMT): Overview, emerging technologies, and case studies. IETE Tech Rev. 2022;39:775–88. https://doi.org/10.1080/02564602.2021.1927863.
7. Egala BS, Pradhan AK, Badarla V, Mohanty SP. Fortified-chain: A blockchain-based framework for security and privacy assured internet of medical things with effective access control. IEEE Internet Things J. 2021;8:11717–31. https://doi.org/10.1109/JIOT.2021.3058946.
8. Parameswari A, Bhavani S, Vinoth Kumar K. A Convolutional Deep Neural Network Based Brain Tumor Diagnoses Using Clustered Image and Feature-Supported Classifier (CIFC) Technique. Braz Arch Biol Technol. 2023;66. https://doi.org/10.1590/1678-4324-2023230012.
9. Lakhan AR, Mohammed MA, Elhoseny M, Alshehri MD, Abdulkareem KH. Blockchain multi-objective optimization approach-enabled secure and cost-efficient scheduling for the Internet of Medical Things (IoMT) in fog-cloud system. Soft Comput. 2022;26:6429–42. http://dx.doi.org/10.1007/s00500-022-07167-9.
10. Vaiyapuri T, Binbusayyis A, Varadarajan V. Security, privacy and trust in IoMT enabled smart healthcare system: A systematic review of current and future trends. Int J Adv Comput Sci Appl. 2021;12:731–7. https://dx.doi.org/10.14569/IJACSA.2021.0120291.
11. Parameswari A, Bhavani S, Vinoth Kumar K. A Deep Learning Based Glioma Tumour Detection Using Efficient Visual Geometry Group Convolutional Neural Networks Architecture. Braz Arch Biol Technol. 2024;67. https://doi.org/10.1590/1678-4324-2024230705.
12. Neelakandan S, Beulah JR, Prathiba L, Murthy GLN, Irudaya Raj EF, Arulkumar N. Blockchain with deep learning-enabled secure healthcare data transmission and diagnostic model. Int J Model Simul Sci Comput. 2022;13(04):2241006. https://doi.org/10.1142/S1793962322410069.

13. Rajasekaran P, Duraipandian M. Secure cloud storage for IoT based distributed healthcare environment using blockchain orchestrated and deep learning model. J Intell Fuzzy Syst. 2024;1:1069–84. https://doi.org/10.3233/jifs-234884.
14. Lin Q, Li X, Cai K, Prakash M, Paulraj D. Secure Internet of medical Things (IoMT) based on ECMQV-MAC authentication protocol and EKMC-SCP blockchain networking. InfSci (N Y). 2024;654:119783. http://dx.doi.org/10.1016/j.ins.2023.119783.
15. Kumar R, Kumar P, Tripathi R, Gupta GP, Islam AN, Shorfuzzaman M. Permissioned blockchain and deep learning for secure and efficient data sharing in industrial healthcare systems. IEEE Trans Ind Inform. 2022;18(11):8065-73. http://dx.doi.org/10.1109/TII.2022.3161631.
16. Albakri A, Alqahtani YM. Internet of Medical Things with a Blockchain-Assisted Smart Healthcare System Using Metaheuristics with a Deep Learning Model. Appl Sci (Basel). 2023;13(10):6108. https://doi.org/10.3390/app13106108.
17. Sachidananda Murthy KB, Prasad SN. Blockchain-Enabled Detection of Neurological Disorders Using a Deep Learning Approach. Eng Proc. 2024;59(1):187. https://doi.org/10.3390/engproc2023059187.
18. He Q, Feng Z, Fang H, Wang X, Zhao L, Yao Y, et al. A Blockchain-Based Scheme for Secure Data Offloading in Healthcare With Deep Reinforcement Learning. IEEE/ACM Trans Netw. 2023. https://doi.org/10.1109/TNET.2023.3274631.
19. Yin S, Liu J, Teng L. Improved Elliptic Curve Cryptography with Homomorphic Encryption for Medical Image Encryption. Int J NetwSecur. 2020;22(3):419-24. https://doi.org/10.6633/IJNS.202005 22(3).07.
20. Liu G, Guo Z, Liu W, Jiang F, Fu E. A feature selection method based on the Golden Jackal-Grey Wolf Hybrid Optimization Algorithm. PLoS One. 2024;19(1). https://doi.org/10.1371/journal.pone.0295579.
21. Sonkamble RG, Bongale AM, Phansalkar S, Sharma A, Rajput S. Secure Data Transmission of Electronic Health Records Using Blockchain Technology. Electronics (Basel). 2023;12(4):1015. https://doi.org/10.3390/electronics12041015.
22. Abouelmagd LM, Shams MY, Marie HS, Hassanien AE. An optimized capsule neural networks for tomato leaf disease classification. EURASIP J ImageVideoProcess. 2024;2024(1):2. http://dx.doi.org/10.1186/s13640-023-00618-9.
23. Jiawei G, Yu L, Ruilong Z, Xin L, Liang J. Automatic SWMM parameter calibration method based on the differential evolution and Bayesian optimization algorithm. Authorea Preprints. 2023. https://doi.org/10.22541/au.169011560.08999787/v1.
24. Kale AP, Wahul RM, Patange AD, Soman R, Ostachowicz W. Development of Deep Belief Network for Tool Faults Recognition. Sensors (Basel). 2023;23(4):1872. https://doi.org/10.3390/s23041872.
25. Kim Y, Lee SO, Ko K. Secure Outsourced Blockchain-Based Medical Data Sharing System Using Proxy Re-Encryption. Appl Sci. 2021;11(20):9422. https://doi.org/10.3390/app11209422.