applied sciences

MDPI

Article

Internet of Medical Things with a Blockchain-Assisted Smart Healthcare System Using Metaheuristics with a Deep Learning Model

Ashwag Albakri [1,*] and Yahya Muhammed Alqahtani [2]

[1] Department of Computer Science, College of Computer Science & Information Technology, Jazan University, Jazan 45142, Saudi Arabia
[2] Department of Information Technology, College of Computer Science and Information Technology, Jazan University, Jazan 45142, Saudi Arabia; yalqahtani@jazanu.edu.sa
* Correspondence: aoalbakri@jazanu.edu.sa

Abstract: The Internet of Medical Things (IoMT) is a network of healthcare devices such as wearables, diagnostic equipment, and implantable devices, which are linked to the internet and can communicate with one another. Blockchain (BC) technology can design a secure, decentralized system to store and share medical data in an IoMT-based intelligent healthcare system. Patient records were stored in a tamper-proof and decentralized way using BC, which provides high privacy and security for the patients. Furthermore, BC enables efficient and secure sharing of healthcare data between patients and health professionals, enhancing healthcare quality. Therefore, in this paper, we develop an IoMT with a blockchain-based smart healthcare system using encryption with an optimal deep learning (BSHS-EODL) model. The presented BSHS-EODL method allows BC-assisted secured image transmission and diagnoses models for the IoMT environment. The proposed method includes data classification, data collection, and image encryption. Initially, the IoMT devices enable data collection processes, and the gathered images are stored in BC for security. Then, image encryption is applied for data encryption, and its key generation method can be performed via the dingo optimization algorithm (DOA). Finally, the BSHS-EODL technique performs disease diagnosis comprising SqueezeNet, Bayesian optimization (BO) based parameter tuning, and voting extreme learning machine (VELM). A comprehensive set of simulation analyses on medical datasets highlights the betterment of the BSHS-EODL method over existing techniques with a maximum accuracy of 98.51%, whereas the existing methods such as DBN, YOLO-GC, ResNet, VGG-19, and CDNN models have lower accuracies of 94.15%, 94.24%, 96.19%, 91.19%, and 95.29% respectively.

Keywords: Internet of Medical Things; smart healthcare; blockchain; security; key generation; image encryption

Citation: Albakri, A.; Alqahtani, Y.M. Internet of Medical Things with a Blockchain-Assisted Smart Healthcare System Using Metaheuristics with a Deep Learning Model. *Appl. Sci.* **2023**, *13*, 6108. https://doi.org/10.3390/app13106108

Academic Editors: Do-Young Kang, Sangjin Kim and Hyuntae Park

Received: 23 February 2023
Revised: 27 April 2023
Accepted: 14 May 2023
Published: 16 May 2023

1. Introduction

Smart healthcare is the advancement of conventional healthcare with advanced internet technologies. It incorporates various technologies to render real-time health-relevant data collected from patients utilizing smart wearable devices and detection of health problems in real time from the collected data [1]. The Internet of Medical Things (IoMT) plays a crucial role in the medical field to increase electronic devices' throughput, precision, and consistency. Due to the outbreak of the coronavirus pandemic, visiting a doctor becomes a high risk for a person with small problems [2]. With the help of IoMT devices, it becomes easy to monitor health records daily, and preventive measures can be taken on our own. An IoMT-based smart healthcare system refers to a collection of several smart medical devices linked within the network over the internet [3]. Analysis can be done by making use of proper AI-based data transformation and interpretation methods after getting the medical dataset. However, easy access to healthcare applications and services has increased

the risks and vulnerabilities that hinder smart healthcare systems' performance. Also, many more heterogeneous devices collect data that differ in formats and size, making it a challenge to manage the data in the healthcare repositories and secure it from attackers who seek to profit from the data [4]. Therefore, smart healthcare schemes are prone to several security risks and threats, such as network attacks, software and hardware-based attacks, and system-level attacks, which put the lives of patients at risk.

Developing technologies, namely blockchain (BC), were utilized for providing cutting-edge solutions in several settings [5], one among them being the healthcare sector. BC technology is used in the medical field to guarantee the security of patient reports and rationalise data sharing amongst pharmaceutical companies, health care providers, and labs [6]. In the medical world, applications (apps) built on BC technology can detect significant and even hazardous errors [7]. Thus, it is capable of enhancing the openness, efficacy, and safety of the systems to exchange healthcare data in the medical field. Medical institutions are aided by BC technology to obtain insight and enhance medical record analysis. Then, the healthcare support system demands a new processing method with delay-sensitive monitoring which should be smart and managed stably [8].

Deep learning (DL) related medical diagnosis in the IoMT signifies the use of machine learning (ML) and artificial intelligence (AI) approaches to examine medical datasets collected from different devices connected to the internet, namely medical equipment and wearable devices [9]. It enhances the precision level of diagnostic decisions, helps identify trends and patterns in patient data, and enables efficient and more personalized healthcare delivery [10]. Simultaneously, hyperparameter tuning of the DL models becomes essential to improve the overall classification performance. Since trial-and-error hyperparameter selection is a challenging task, metaheuristic optimization techniques are used. In addition, image encryption schemes can be used to securely transmit healthcare data in the IoMT encryption. Furthermore, the key generation process is critical to the security of an encryption algorithm, as the strength of the key directly impacts the security of the encrypted data. Therefore, it is important to use strong and secure key generation methods and to properly manage and protect the keys.

This article develops an IoMT with a blockchain-based smart healthcare system using encryption with an optimal deep learning (BSHS-EODL) model. The presented BSHS-EODL technique comprises a few processes: data collection, image encryption, and data classification. Initially, the IoMT devices enable data collection processes, and the gathered images are stored in BC for security. Then, image encryption is employed to encrypt the data, and its key generation process is performed via the dingo optimization algorithm (DOA). Finally, the BSHS-EODL technique performs disease diagnosis comprising SqueezeNet, Bayesian optimization (BO) based parameter tuning, and voting extreme learning machine (VELM). A comprehensive set of simulation analyses is performed on medical datasets.

The rest of the paper is organized as follows: Section 2 discusses the related works, Section 3 demonstrates the proposed approach, performance validation is depicted in Section 4, and the conclusion is shown in Section 5.

2. Related Works

Almaiah et al. [11] present a DL framework based on BC that offers a dual level of security and privacy. Initially, a BC technique was modelled in which each participating entity was verified, validated, and registered by making use of a smart contract related enhanced proof-of-work to reach the target of privacy and security. Then, a DL approach including bidirectional long short-term memory (BLSTM) for a variational autoencoder (VAE) and intrusion detection systems for privacy were devised. Khan et al. [12] introduced BIoMT, a BC Hyperledger fabric-assisted consortium architecture which offers transparency, security, and integrity to health-oriented transactions and interchanges delicate medical data in serverless peer-to-peer (P2P) secured network settings. A consensus was devised and constituted to decrease rate of BC resource limitations on the IoMT.

In [13], suggesting a BC-based secured data management framework (BSDMF) for medical data related to the IoTs to exchange patients' data securely and improve data accessibility and scalability. To assure data management and data transmission security among associated nodes, the IoMT-related security structure uses BC. In [14], this study evaluated offloading and scheduling issues for medical workflow in IoMT fog-cloud platforms. Thus, this study addressed the issue as an offloading and scheduling issue and developed deep reinforcement learning (DRL) as a Markov problem. This study designed an innovative DRL and BC-based system which contained multi-criteria offloading depending on DRL policies.

Lakhan et al. [15] developed an LSEOS method called lightweight secure efficient offloading scheduling. LSEOS has lightweight and secured offloading and scheduling methodologies whose offloading delay will be lesser compared to prevailing techniques. The end goal of LSEOS is to run the application over other nodes and diminish the delay and security threats in the mechanism. The metaheuristic LSEOS has the elements they are scheduling with neighbourhood search schemes, adaptive deadlines, and sorting. Kumar and Tripathi [16] offered an innovative contract-based consortium BC technique. The authors compiled interplanetary file systems (IPFS) and cluster nodes where smart contracts are deployable in the early phase. The IPFS cluster node assures the authentication and security of gadgets and even offers safe storage in IoMT based health care systems. Alqaralleh et al. [17] designed DL with BC-based secured image transmission and diagnosis system for the IoMT environment. The elliptic curve cryptography (ECC) was implemented in the initial stage, and then by combining grasshopper and fruit fly optimization (GO-FFO) system, ECC's optimum key generation is taken. Finally, a method called a deep belief network (DBN) is applied to find the existence of disease. In [18], a novel secure authentication method utilizing ML was presented. To find the attack authentication and detection in an IoMT platform, this study applies ML and k-nearest neighbour (KNN) with smart contract (KNN-MLSC).

Uppal et al. [19] proposed an interplanetary file system (IPFS) enabled model for secure healthcare system. It enables the client to continuously upload the healthcare information gathered by IoT devices and to add to the BC transactions. The authors in [20] developed a BC based electronic medical records (EMR) management model for a smart healthcare system. The privacy of the healthcare data can be accomplished using BC technology. It offers off-chain storage for the records and assuring the authenticity and integrity of the health records. In [21], a new hybrid Elman Neural-based Blowfish BC approach has been introduced for the security of the healthcare data in the IoT environment. The Elman network offered continual monitoring to predict abnormal activities in the trained multimedia data. The authors in [22] developed a Lionized Golden Eagle based Homomorphic Elapid Security (LGE-HES) technique with blockchain in healthcare network. The blockchain provides the privacy of the medical images using hash operations.

Although several encryption techniques have been presented in the literature, security performance still needs to be improved. Since the images encompass a massive quantity of data, high redundancy rate, and increased correlation between neighboring pixels, classical encryption models cannot be used to resolve the requirements of the image encryption technique. Therefore, several approaches have been presented based on chaotic concepts, pixel swapping, etc. On the other hand, the continuous deepening of the DL model has resulted in the model overfitting issue. In addition, various hyperparameters have provided a substantial impact on the performance of the CNN model. In particular, the hyperparameters such as learning rate, batch size, and number of epochs are important to attain effectual outcome. As the trial-and-error technique for hyperparameter tuning is a challenging and erroneous procedure, a BO algorithm is used in this study.

3. The Proposed Model

In this paper, we develop a new BSHS-EODL method for secured medical image transmission and analysis in the IoMT environment. The presented BSHS-EODL technique enables BC assisted secured image communication and detection models for the IoMT

environment. The proposed method includes data classification, data collection, and image encryption. At the initial stage, the IoMT devices enable data collection processes, and the gathered images are stored in BC for security. Once the images are gathered, they are encrypted using effective image encryption technique with a DOA based key generation process. Next, the encrypted image was securely transferred using BC technology. At the receiver end, the image decryption was implemented, and the disease diagnosis process was later. Figure 1 demonstrates the working process of the BSHS-EODL method.

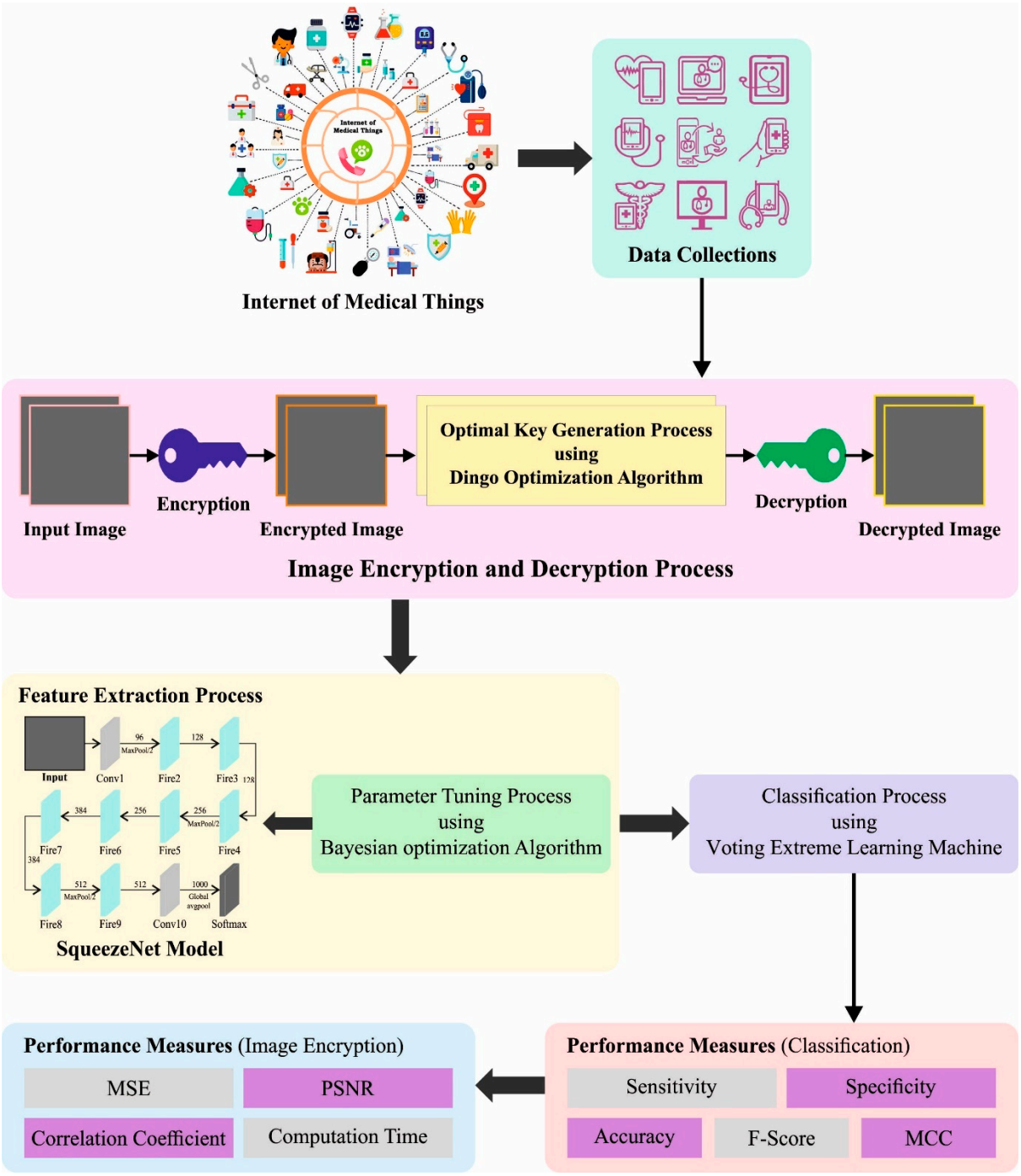

Figure 1. Working process of BSHS-EODL approach.

3.1. Image Encryption

In this work, image encryption method takes place to secure medical images. The image encryption procedure mostly comprises key selection, chaotic sequence pre-processing, diffusion, block scrambling, confusion, and expansion [23]. The chaotic sequence preprocessing makes the sequence more arbitrary. Block scrambling has been separated, as intra- and inter-block scrambling decrease the correlation and offer optimum protection against statistical attack. The expansion stage enhances arbitrary numbers to novel images towards all the encryption and thus gains a distinct ciphertext image that is optimally prepared to resist chosen plaintext attack. Diffusion and confusion complicate the connection amongst ciphertext and keys, which make it complex for adversaries to decrypt a ciphertext image and that improves the resistance of such scenarios.

Key Selection

Optimizing values x_0, y_0, μ_1, μ_2, λ_1, and λ_2 created by the DOA technique can be utilized as the keys for 2-D logistic maps. For avoiding transient impact, the first 200 points can be discarded and generate 2 chaotic sequences $\{x_n\}$, $\{y_n\}$ that are of length MN.

Chaotic Sequence Preprocessing

The 2 chaotic sequences $\{x_n\}$, $\{y\}$ can be pre-processed based on Equation (1).

$$\begin{array}{c} x_1(i) = 10^q \cdot x_n(i) - round(10^q \cdot x_n(i)) + 0.5 \\ y_1(i) = 10^q \cdot y_n(i) - round(10^q \cdot y_n(i)) + 0.5 \end{array} \quad (1)$$

whereas $x_1(i)$ and $y_1(i)$ implies the chaotic sequences $\{x_n\}$, $\{y\}$ pre-processed sequence, whereas $q = 8$.

Image Scrambling

The 16 sub-blocks $B(i), i = 1, 2, \ldots, 16$ of similar sizes can be separated by the new image P_1, and the remaining 16 numbers of sequences $x(i)$ are acquired for composing a sequences $D(i)$. The acquired integer sequence $S(i)$ was sorted, and inter-block scrambling was attained based on Equation (2).

$$\begin{array}{c} S(i) = floor\big(mod\big(D(i) \times 10^{14}, 16\big)\big) + 1 \\ [s, l] = sort(S) \\ B1 = B(l) \end{array} \quad (2)$$

Sequences t_1 and t_2 refer to the collection of 8 sequence values from the mid sequences $x(i)$ and (i), correspondingly and a novel sequence t was created based on Equation (3). All the sub-blocks were disordered t_j times by intra-block scrambling established to process the novel disordered sixteen sub-blocks.

$$\begin{cases} t(2(i-1)+1) = floor\big(mod\ \big(t1 \times 10^{14}, 3\big)\big) + 4 \\ t(2i) = floor\big(mod\ \big(t2 \times 10^{14}, 3\big)\big) + 4 \end{cases} \quad (3)$$

Finally, the 16 sub-blocks can be combined with procedure image P_2.

Image Expansion

The R_0 and R_1 are 2 random matrices created, whereas the sizes of R_0 and R_1 are $4 \times (N + 4)$ and $M \times 4$, correspondingly. Develop image P_2 based on the system for forming an expanded image P_3.

Confusion and Diffusion

The chaotic scheme comprises two stages: diffusion and confusion. Confusion seeks to obscure and confound the relationships among key and the cipher images. Diffusion aims to obscure the relationships among the cipher and plain images by making it as convoluted. Principally, the swapping operation on the rows and the columns was performed for

the realization of the confusion effects. Primarily, compute the novel row index $r(i) = ceil(x_1(i) \times (M+4))$ utilizing $x_1(i)$, followed by related row i with row indexes $r(i)$.

$$\begin{gathered} if\ r(i) < i,\ then \\ r(i) = i \end{gathered} \tag{4}$$

Secondly, the parameters k_{11}, k_{12} are computed utilizing $x_1(i)$.

$$\begin{aligned} k_{11}(i) &= mod\big(floor\big(x_1(i) \times 10^8\big), 256\big) \\ k_{12}(i) &= mod\big(floor\big(x_1(i) \times 10^9\big), 256\big) \end{aligned} \tag{5}$$

Thirdly, accomplish a bitwise XOR function on the expansion image P_3 with parameters k_{11}, k_{12}.

If $= r(i)$, then

$$\begin{gathered} P_{30}(i,:) = P_3(i,:) \oplus k_{11}(i) \\ if\ \neq r(i),\ then \\ P_{30}(i,:) = P_3(i,:) \oplus k_{11}(i) \\ P_{30}(r(i),:) = P_3(r(i),:) \oplus k_{12}(i) \end{gathered} \tag{6}$$

At the fourth stage, swap the ith and $r(i)$th row of P_{30} for obtaining P_{31}.

$$\begin{gathered} temp = P_{30}(i,:) \\ P_{30}(i,:) = P_{30}(r(i),:) \\ P_{30}(r(i),:) = temp \\ P_{31} = P_{30} \end{gathered} \tag{7}$$

In the fifth, the first and last columns of P_{31} can be computed to obtain P_4.

$$P_4(i,\ 1) = mod\ (P_{31}(i,\ 1) + P_{31}(i,\ N+4), 256) \tag{8}$$

At the sixth stage, the other columns of P_{31} and P_4 can be computed.

$$P_4(i,j) = mod\ (P_{31}(i,j) + P_4(i,j-1), 256) \tag{9}$$

The diffusion and confusion of columns are related to the row, but that sequence $y_1(i)$ was utilized rather than sequence $x_1(i)$. The particular computation process was projected in Algorithm 1.

Algorithm 1: Column confusion and diffusion

Input: Image P_4 and pre-processed chaotic sequence $y_1(i)$
Output: Image P_5
for $j = 1$ to $N+4$
$q(j) = ceil((N+4) \cdot y_1(j))$,
$k_{21}(j) = mod\ \big(floor\big(10^8 \times y_1(j)\big), 2^8\big)$,
$k_{22}(j) = mod\ \big(floor\big(10^9 \times y_1(j)\big), 2^8\big)$,
if $q(j) < j$ then
$q(j) = j$,
end if
if $q(j) = j$ then
$P_4(:,j) = k_{21}(j) \oplus P_4(:,j)$,
else if
$P_4(:,j) = k_{21}(j) \oplus P_4(:,j)$,
$P_4(:,q(j)) = k_{22}(j) \oplus P_4\ q(j))$,
end if
$temp = P_4(:,j)$,
$P_4(:,j) = P_4(:,q(j))$,
$P_4(:,q(j)) = temp$,

$$P_{41} = P_{4;}$$

for $i = 1$ *to* $M + 4$

$$P_5(1, j) = mod\ \left(P_{41}(1, j) + P_{41}(M + 4, j), 2^8\right),$$
$$P_5(i, j) = mod\ \left(P_5(i - 1, j) + P_{41}(i, j), 2^8\right),$$

end for

end for

3.2. Key Generation Process

The DOA is used for an effective key generation process. The DOA is a metaheuristic approach stimulated by the hunting behaviours of dingo. DOA is chosen for key generation due to its following advantages: high convergence, robust, global optimization, a smaller number of parameters, simplicity, and highly versatile. This strategy includes scavenging nature, attack by persecution, and assembling procedures [24]. Australian dingo dogs are in danger of extermination. Consequently, the survival rate of dingo is regarded in the DOA. The mathematical expression of DOA is given in the following. In general, dingoes meet in groups during hunting. They then find the prey location and surround it using the following equation:

$$\vec{x}_i(t+1) = \beta_1 \sum_{k=1}^{na} \frac{\left[\vec{\varphi_k}(t) - \vec{x}_i(t)\right] \frac{\setminus}{\phi_k(t)}}{na} - \vec{x}_{i*}(t) \tag{10}$$

In Equation (10), $\vec{x}(t+1)$ represents the new prey location of the searching agent, na denotes the random integer generated within [2, $\frac{SizePop}{2}$], where SizePop indicates overall dingo population size. $\vec{\varphi}_k(t)$ shows the subset of search agent where $\phi \subset X$, X denotes the randomly generated dingo population, $\vec{x}_i(t)$ specifies the existing search agent, $\vec{x}_i(t)$ signifies the best possible searching agent attained from prior iteration, and β_1 is a consistently produced arbitrary number within $[-2, 2]$. Typically, dingoes hunt tiny prey and chase it till it gets caught. These characteristics are expressed as follows:

$$\vec{x}_i(t+1) = \vec{x}_*(t) + \beta_1 * e^{\beta_2} * \left(\vec{x}_{r_1}(t) - \vec{x}_i(t)\right) \tag{11}$$

In Equation (11), $\vec{x}(t+1)$ describes the movement of the dingo, $\vec{x}_i(t)$ shows existing search agents, $\vec{x}_*(t)$ means best possible search agent obtained from the previous iteration, r_1 represents randomly produced numbers from the interval 1 to the size of maximal of the search agent, and $\vec{x}_{r1}(t)$ shows the $r_1 -$ th selected search agent, where $i \neq r_1$.

Scavenger is characterized as a dingo finding meat to eat if they get a random walk in the habitat.

$$\vec{x}_i(t+1) = \frac{1}{2}[e^{\beta_2} * \vec{x}_{r_1}(t) - \left(-1\right)^{\sigma} * \vec{x}_i(t)\Big] \tag{12}$$

In Equation (12), $\vec{x}(t+1)$ denotes the dingo progress, β_2 has equivalent value as in Equation (12), r_1 represents the randomly generated number within [1, max_size of searching agent] interval, $\vec{x}_{r_1}(t)$ indicates the r_1^{th} selected search agent, $\vec{x}_i(t)$ denotes the existing search agent, where $i \neq r_1$, and σ signifies the arbitrarily created binary number. Finally, the survival rate of the dingoes is expressed as follows:

$$survival\ (i) = \frac{fitness_{\max} - fitness(i)}{fitness_{\max} - fitness_{\min}} \tag{13}$$

In Equation (13), $fitness_{\max}$ and $fitness_{\min}$ correspondingly represent poor and optimum fitness values in the present round. $fitness(i)$ signifies existing fitness value of *i-th* searching agent. The survival vector in Equation (13) encompasses the normalizing fitness value within $[0, 1]$. Equation (14) is used for attaining lower survival rate.

$$\vec{x}_i(t) = \vec{x}_*(t) + \frac{1}{2}[\vec{x}_{r_1}(t) - \left(-1\right)^{\sigma} * \vec{x}_{r_2}(t)] \quad (14)$$

In Equation (14), $\vec{x}_i(t)$ represents that search agent with minimal survival rate is upgraded. In addition, r_1 and r_2 denote the randomly produced numbers within [1, max_size of searching agent] interval, $\vec{x}_*(t)$ specifies best possible searching agent accomplished from previous iteration, and σ showing binary number of agents, with $r_1 \neq r_2$, $\vec{x}_{r_1}(t)$ and $\vec{x}_{r_2}(t)$, describes r_1, r_2 selected searching agent, $\vec{x}_*(t)$ indicates the best possible searching agent accomplished from previous iteration, and σ shows the randomly generated number.

The set of keys is preferred by considering the "fitness function" as a max key using peak signal-to-noise ratio (PSNR) for scrambling and unscrambling data from medical images. With the help of hybrid optimization, the organization has been developed, and it is given in the following:

$$Fitness = \max\{PSNR\} \quad (15)$$

3.3. Blockchain Technology

The proposed BSHS-EODL technique used BC technology for secure data transmission in the medical field. A BC is distributed data where a novel time-stamped transaction is grouped and appended to a hash-chain of blocks [25]. The BSHS-EODL technique comprises a data processing section, application server for data transmission and reception, BC enabled decentralized databases, application programming interface (API) management element, and data analytics unit. A few processes which take place in the system are Create_Patient_Data, Grant_Access_ToHCP, and Revoke_Access. The structured data of the patient gets saved in the classical dataset and the unstructured data gets stored in the data warehouse. The encrypted data gets saved in the distributed BC using preferrable smart contract. After the storage of data in the allotted BC, BSHS-EODL technique uses VELM classifier for classification process. The medical image is loaded into the decentralized BC, and the BSHS-EODL technique can be employed to the data fetched from the decentralized network. The BSHS-EODL technique operates in the following way. Ethereum BC network can be employed for patient data distribution. Each individual actor carries out various activities in the network and has access to the data for which they received access. The patients can generate the information and commit the transaction. When the transactions are committed in the BC, the altered transaction is dispersed over the Internet, verifying that each data existing in the network can be accessed by every actor in the network and cannot be changed by unintentional persons. The medical personnel can access the data only when the respective user provides access permissions. Healthcare professionals can access the patient data and perform disease diagnostic processes. If the healthcare professional receives a request from the patient, they can accept it and send a request to access the data to the specific person. Upon the acceptance of the request, they investigate the medical data for disease detection purposes.

3.4. Disease Classification Model

In this work, the BSHS-EODL technique performs disease diagnosis comprising SqueezeNet, BO based parameter tuning, and VELM.

3.4.1. Feature Extraction Using SqueezeNet

To produce feature vectors, the SqueezeNet model is used in this work. SqueezeNet is a small, efficient deep neural network structure [26]. It is intended to be faster and smaller than other architectures while accomplishing higher accuracy on image classification tasks. SqueezeNet exploits a technique named "squeeze-and-excitation" to decrease the parameter count in the network, enabling it to be more effective in terms of memory and computational requirements. It was specifically designed for use on embedded and mobile devices. The SqueezeNet architecture comprises a series of layers, including the following:

- Pooling layers, decrease the spatial dimension of the feature maps.
- The input layer takes in the image dataset.
- A sequence of FC layers categorises the image based on the extracted features through the convolution layer.
- A sequence of convolutional layers extracts features from the image. This layer uses "fire modules" that comprise the "expand" layer with a larger number of filters, followed by "squeeze" layer with smaller number of filters. This enables the network to maintain fewer parameters while still extracting relevant features from the image.

The architecture also includes a dropout layer and a softmax layer. Dropout is a regularization technique that prevents overfitting by randomly dropping out some neurons during training. The softmax layer creates a probability distribution over the feasible classes used to classify the image. The SqueezeNet architecture is designed to be small and efficient, with a total of only 1.2 million parameters. This makes it better suited for use on embedded and mobile devices with limited computational resources.

Here, the BO is utilized for the hyperparameter selection of SqueezeNet. A probabilistic method of the objective function (x) called the surrogate function can be created using BO technique [27]. Bayes' Theorem is the core of BO technique and computes the conditional probability of event A given another event B, $P(A|B)$,

$$P(A|B) = P(B|A) * \frac{P(A)}{P(B)} \tag{16}$$

Bayes' theorem is capable of being adjusted by neglecting the $P(B)$ marginal probability from the conditional probability for optimization problem using Equation (17):

$$P(A|B) = P(B|A) * P(A) \tag{17}$$

A new version of Bayes' theorem is given as follows:

$$Posterior = Likelihood * Prior \tag{18}$$

The conditional probability is a function that estimates the objective function and is utilized for sampling the searching space. The searching space in these problems is the SqueezeNet hyperparameter. BO algorithm, as an informed search technique, can be differentiated by using an acquisition function that exploits the posterior for sampling the searching area and selecting the succeeding sample to evaluate the objective function. In this study, the objective function can be denoted as a Gaussian method with the Matern 5/2 kernel. At first, random samples from the search space $(x_1, x_2, \ldots, x_n)$ are exploited for determining the $F(x)$ objective function at these samples. The assessments and samples are gathered in a consecutive way, which leads to a sequence of data points $S = \{x_i, F(x_j), \ldots x_n, F(x_n)\}$, where n denotes the number of samples. The set S defines the likelihood, and prior function can be described as follows:

$$P(F|S) = P(S|F) * P(S) \tag{19}$$

The posterior is updated afterwards with the evaluation of prior and probability. The acquisition function, C, is enhanced over the Gaussian algorithm for selecting the subsequent sample x_n, which can be represented as follows:

$$x_n = \text{argmax}_x C(x|S_{1:n-1}) \tag{20}$$

In this study, the acquisition function can be executed by the expected improvement algorithm, as defined below.

$$C(x) = E\left[\max\left(F(x) - P(x^+), 0\right)\right] \tag{21}$$

In Equation (21), $F(x)$ indicates the value of objective function for the better sample, E denotes the expectation operator, and x^+ shows the better sample location in the search range. Then, the sample selected can be assessed by the objective function, and these processes are repeated until the objective function attains its least or minimum objective within the given run time.

3.4.2. Image Classification Using VELM Model

Finally, the classification of medical images is performed by the VELM model. The VELM was utilized as a classifier in this work. The VELM is a significant ML model which enhances classification accuracy while maintaining high processing speeds and robustness to noise and outliers in the input data. An ELM is a type of artificial neural network (ANN) with a single hidden layer (HL) [28]. Here, the weight that connects input to the HL and HL to biases are randomized. The weights between the output and HLs are computed by the Moore–Penrose inverse, making the training model faster. Several ELMs can be used for classification to increase detection accuracy. Each individual ELM is trained using similar data. In the process of detection, the sample is used for all the ELMs and output is computed. Based on the majority voting, the last output is computed. Assume, an ELM with activation functions f and l hidden neurons in HL. If there is N training sample of the form $(x_i,\ t_i)$, where $x_i = [x_{i1},\ x_{i2},\ \ldots,\ x_{in}]^T \in R^n$ and $t_i = [t_{i1},\ t_{i2},\ \ldots,\ t_{im}]^T \in R^m$ $(m = 2)$ then the output can be represented as

$$0_i = \sum_{j=1}^{1} v_j f\left(u_j,\ b_j,\ x_i\right) \tag{22}$$

for, $i = 1, 2, 3, \ldots, N$.

Where $u_j \in R^n$ and $b_j \in R$ denote the learning parameters of jth hidden neuron. $v_j = [\nu_{j1},\ \nu_{j2},\ \ldots,\ \nu_{jm}]^T$ indicates the weight vector that connects jth hidden neurons to output neurons. This can be represented as follows:

$$O = HV \tag{23}$$

where,

$$H = \begin{bmatrix} f(u_1, b_1, x_1) & \ldots & f(u_l, b_l, x_1) \\ \vdots & \vdots & \vdots \\ f(u_1, b_1, x_N) & \ldots & f\left(u_l, b_|, x_N\right) \end{bmatrix}, V = \begin{bmatrix} v_1^T \\ \vdots \\ v_l^T \end{bmatrix} \text{and } O = \begin{bmatrix} o_1^T \\ \vdots \\ o_N^T \end{bmatrix}$$

The u_j and b_j parameters are randomly initialized for minimizing the error $||O - T||$, where $T = (t_1,\ t_2, \ldots, t_N)$, that is independent of input dataset. The output weights can be expressed by finding the least square solution,

$$V = H^+ T \tag{24}$$

where the symbol " $+$ " characterizes the Moore–Penrose generalized inverse of matrix. It implies ELM is trained. In V-ELM, k-th ELM is used. The equivalent number of hidden layers initialized this ELM. The learning parameter u_j and b_j of each ELM is initialized in a random fashion. Next, each ELM is trained on a similar dataset and the results are computed. In detection stage, a set of samples of the form $y_i = [y_{i1},\ y_{i2},\ \ldots,\ y_{in}]$ is used for each ELM. The output $0_i = [0,\ 1]$ or $0_i = [1,\ 0]$ of every individual ELM is taken, and majority voting receives the last output. For every i sample, a vector $C_i \in Z^2_{>=0}$ has been used for storing the class labels recognized by dissimilar ELMs. At first, C_i is initialized to zero $(C_i = [0, 0])$ once an ELM output takes place; the value of equivalent location in C_i can be raised by 1. For instance, assume output of ELM_1 is [1, 0] now C_i become [1, 0].

Output of ELM_2 is again $[1,\ 0]$, then C_i becomes $[2,\ 0]$. Output of ELM_3 is $[0,\ 1]$, then C_i becomes $[2,\ 1]$. Once each k output is reached, then the concluding output is evaluated.

4. Performance Validation

In this section, the experimental outcome of the BSHS-EODL technique is well studied on skin lesion images in the ISIC database. Figure 2 illustrates the sample images.

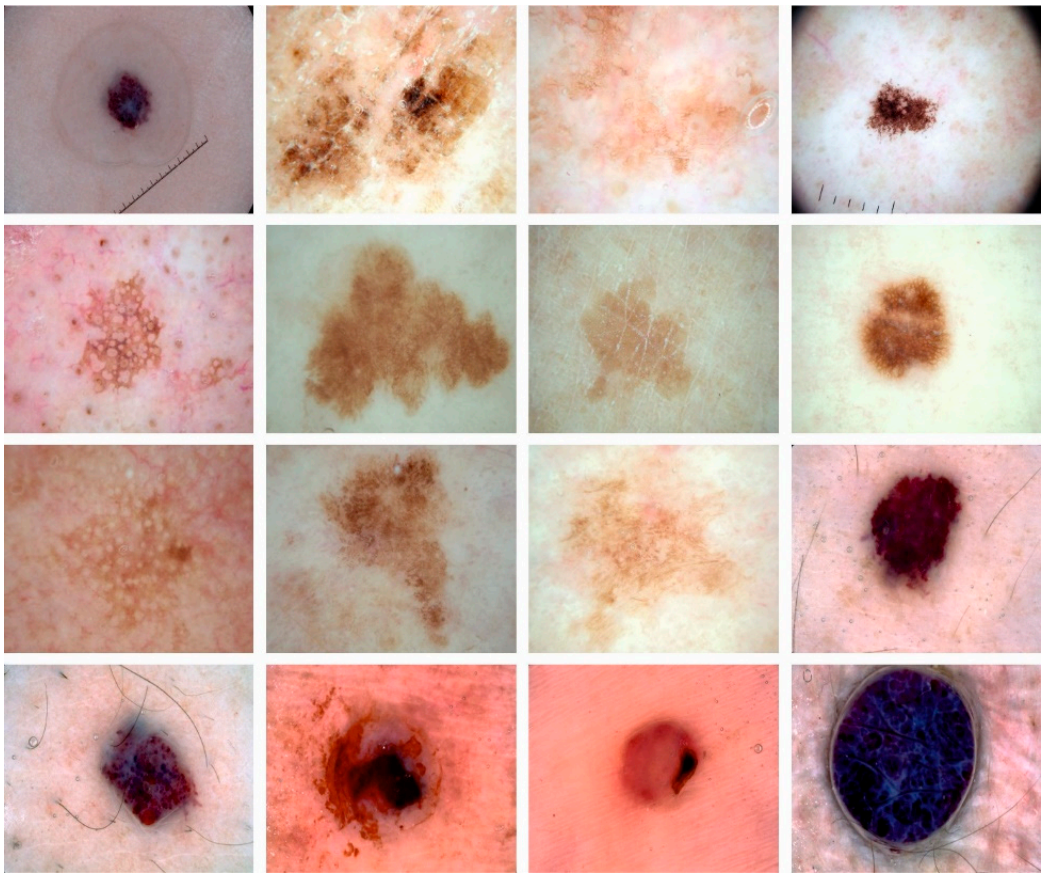

Figure 2. Sample Images.

Figure 3 shows the histogram analysis of the BSHS-EODL technique. Figure 3a,b show the original images and their corresponding histogram images. Similarly, Figure 3c,d demonstrate the encrypted images and their respective histograms.

Table 1 represents the comparative MSE and PSNR examination of the BSHS-EODL technique with existing techniques [17,29] on different images. The results indicate that the GWO and GO-PSO algorithms resulted in higher MSE values, while the GO-FFO and HOCE-ECC techniques led to considerable MSE values. However, the BSHS-EODL technique gains effective performance over other models with minimal MSE of 0.072, 0.057, 0.078, 0.102, and 0.071 under test images 1–5, respectively. The experimental outcomes indicate that the GWO and GO-PSO algorithms represented lower PSNR values than existing ones. Although the GO-FFO and HOCE-ECC models reach moderately improved PSNR values, the BSHS-EODL technique outperformed the existing models with a higher PSNR of 59.56 dB, 60.57 dB, 59.21 dB, 58.04 dB, and 59.62 dB under images 1–5 respectively.

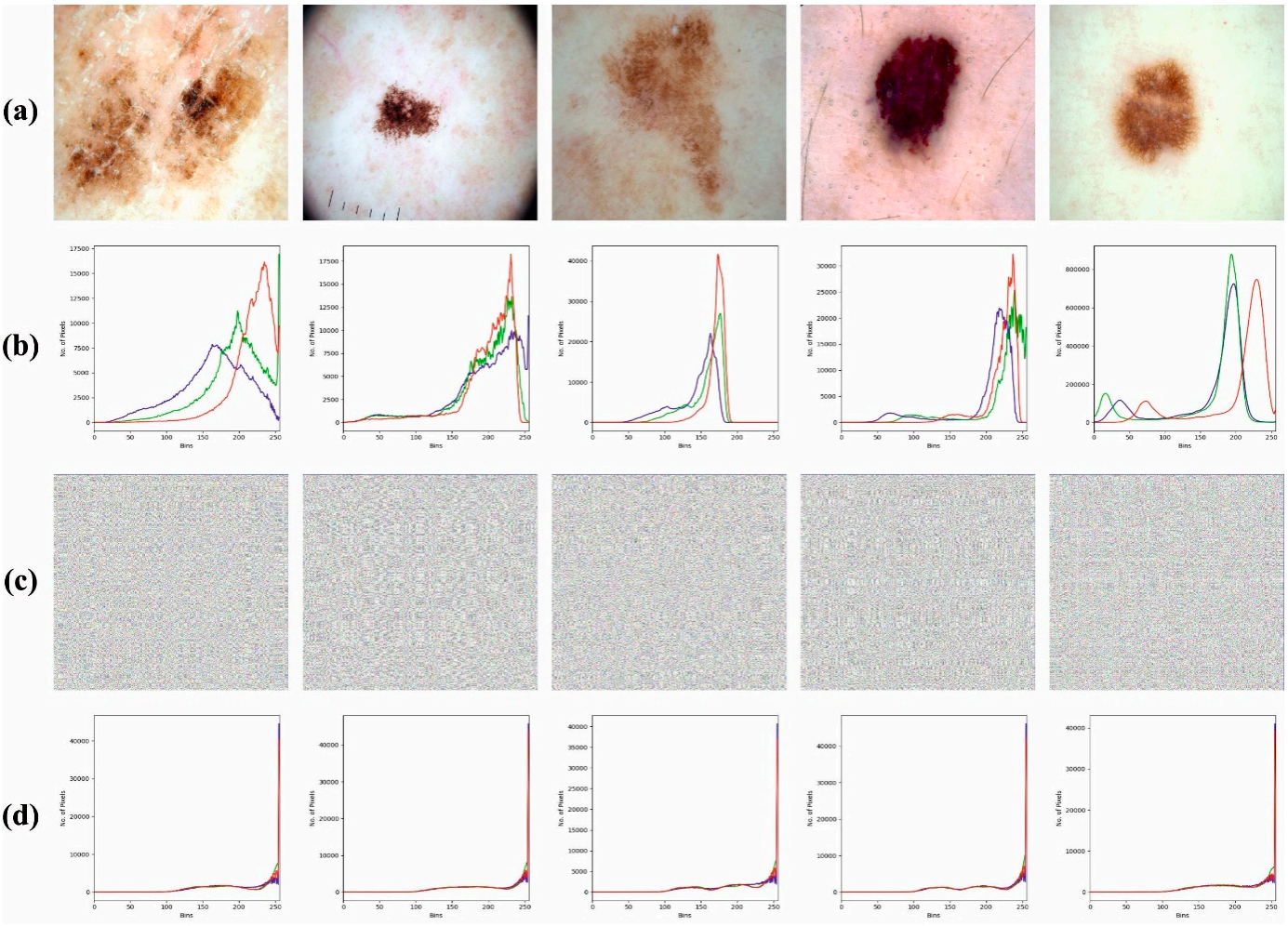

Figure 3. (**a**) Original Images (**b**) Histogram of Original Images (**c**) Encrypted Images (**d**) Histogram of Encrypted Images.

Table 1. MSE and PSNR analysis BSHS-EODL approach with other systems under varying images.

Sample Images	BSHS-EODL		HOCE-ECC [29]		GO-FFO [17]		GO-PSO [17]		GWO [17]	
	MSE	PSNR	MSE	PSNR	MSE	PSNR	MSE	PSNR	MSE	PSNR
Image 1	0.072	59.56	0.112	57.64	0.132	56.93	0.171	55.80	0.197	55.19
Image 2	0.057	60.57	0.083	58.94	0.119	57.38	0.152	56.31	0.172	55.78
Image 3	0.078	59.21	0.118	57.41	0.152	56.31	0.188	55.39	0.220	54.71
Image 4	0.102	58.04	0.13	56.99	0.157	56.17	0.184	55.48	0.210	54.91
Image 5	0.071	59.62	0.107	57.84	0.128	57.06	0.165	55.96	0.186	55.44

Table 2 shows a brief CC outcome of the BSHS-EODL system under several images. The experimental outcome stated that the GWO and GO-PSO algorithms represented lesser CC values over existing ones. However, the GO-FFO and HOCE-ECC models reach moderately enhanced CC values, and the BSHS-EODL approach outperformed the existing techniques with maximal CC of 99.42, 99.63, 99.21, 99.72, and 99.68 under images 1–5 correspondingly.

Table 2. CC analysis of BSHS-EODL approach with other techniques under varying images.

Sample Images	BSHS-EODL	HOCE-ECC [29]	GO-FFO [17]	GO-PSO [17]	GWO [17]
Image 1	99.42	98.93	98.49	98.16	97.7
Image 2	99.63	99.22	98.84	98.53	98.18
Image 3	99.21	98.76	98.45	97.98	97.54
Image 4	99.72	99.33	99.01	98.65	98.19
Image 5	99.68	99.37	99.04	98.54	98.22

Table 3 represents the encryption outcomes of the BSHS-EODL method with existing models under the presence of attacks in terms of computation time (CT) and PSNR. The outcome inferred that the GWO and GO-PSO algorithms resulted in higher CT values, while the GO-FFO and HOCE-ECC approaches led to considerable CT values. The BSHS-EODL algorithm attains effectual performance over other systems with minimal CT of 0.20 s, 0.13 s, 0.16 s, 0.11 s, and 0.15 s under test images 1–5 correspondingly.

Table 3. CT and PSNR outcome of BSHS-EODL approach with other techniques under varying images.

Computation Time (s)					
Sample Images	**BSHS-EODL**	**HOCE-ECC [29]**	**GO-FFO [17]**	**GO-PSO [17]**	**GWO [17]**
Image 1	0.20	0.50	0.78	0.94	1.29
Image 2	0.13	0.31	0.51	0.70	1.05
Image 3	0.16	0.48	0.72	0.92	1.07
Image 4	0.11	0.45	0.59	0.89	1.03
Image 5	0.15	0.41	0.68	1.00	1.31
PSNR During Attacks (dB)					
Sample Images	BSHS-EODL	HOCE-ECC [29]	GO-FFO [17]	GO-PSO [17]	GWO [17]
Image 1	59.21	57.08	56.47	55.29	54.66
Image 2	60.17	58.34	56.90	56.01	55.48
Image 3	58.80	57.01	55.74	54.84	54.38
Image 4	57.71	56.44	55.61	54.91	54.44
Image 5	59.31	57.43	56.59	55.42	55.09

The experimental outcomes implied that the GWO and GO-PSO algorithms represented minimal PSNR values over existing ones. However, the GO-FFO and HOCE-ECC models reached moderately greater PSNR values, and the BSHS-EODL approach outperformed the existing approaches with enhanced PSNR of 59.21 dB, 60.17 dB, 58.80 dB, 57.71 dB, and 59.31 dB under images 1–5 correspondingly.

The classification performance of the BSHS-EODL technique can be tested on the ISIC 2017 Dataset, comprising 318 samples with seven classes, as defined in Table 4.

Table 4. Details of dataset.

Labels	Class	No. of Images
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 count of Images		318

The confusion matrices of the BSHS-EODL method are investigated under distinct sizes of TRS and TSS in Figure 4. The results demonstrated that the BSHS-EODL technique properly recognizes the samples under every class.

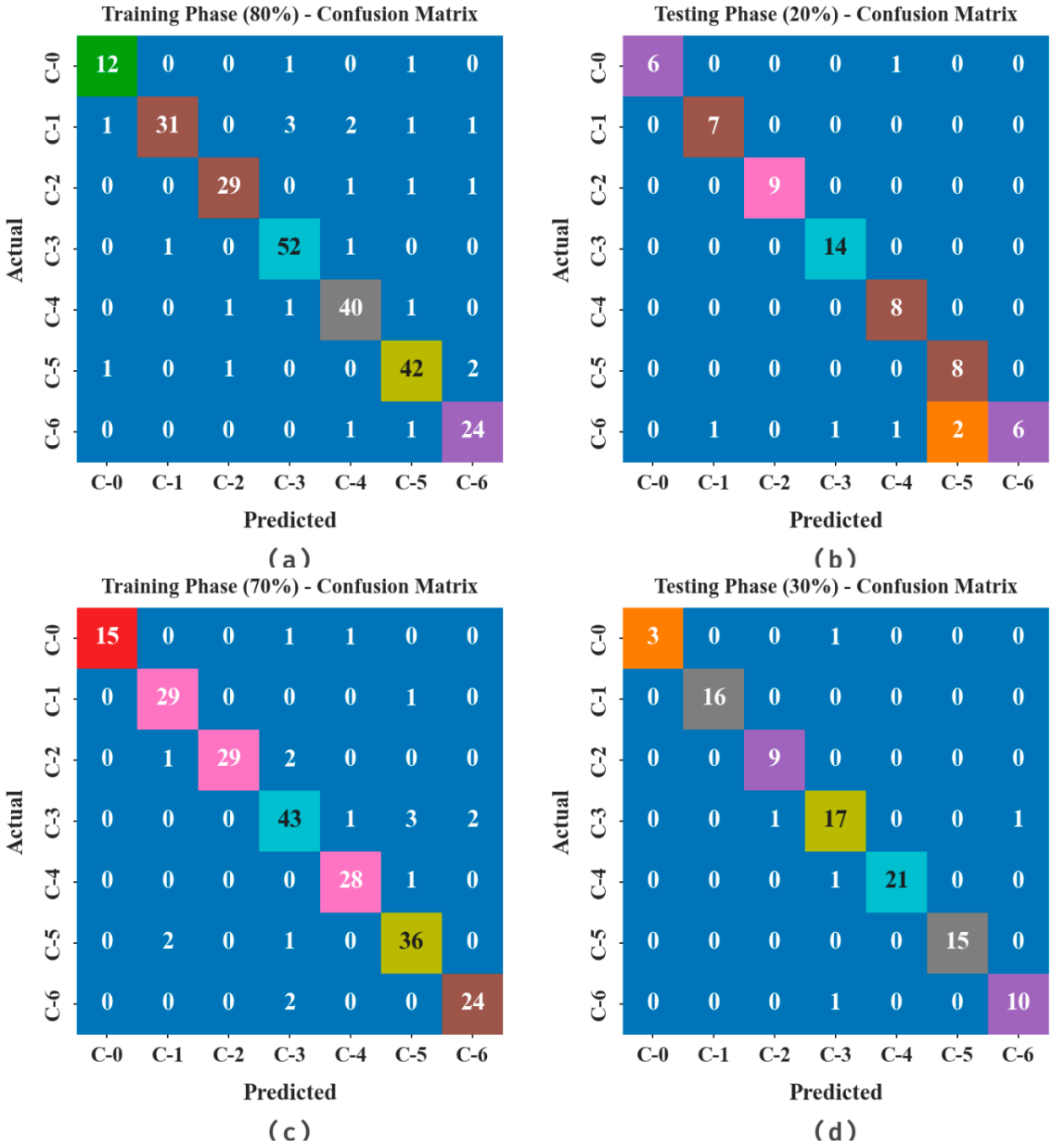

Figure 4. Confusion matrices of BSHS-EODL approach (**a**,**b**) TRS/TSS of 80:20 and (**c**,**d**) TRS/TSS of 70:30.

In Table 5, the overall results of the BSHS-EODL technique are demonstrated. The results indicate that the BSHS-EODL technique properly classified the images under all classes. For instance, with 80% of TRS, the BSHS-EODL technique reaches average $accu_{bal}$ of 97.30%. In addition, with 20% of TSS, the BSHS-EODL approach attains average $accu_{bal}$ of 97.32%. Meanwhile, with 70% of TRS, the BSHS-EODL system attains average $accu_{bal}$ of 97.68%. Finally, with 30% of TSS, the BSHS-EODL algorithm obtains average $accu_{bal}$ of 98.51%.

Table 5. Classifier outcome of BSHS-EODL approach with different metrics.

Labels	$Accu_y$	$Sens_y$	$Spec_y$	F_{score}	MCC
Training Phase (80%)					
C-0	98.43	85.71	99.17	85.71	84.88
C-1	96.46	79.49	99.53	87.32	85.85
C-2	98.03	90.62	99.10	92.06	90.96
C-3	97.24	96.30	97.50	93.69	91.99
C-4	96.85	93.02	97.63	90.91	89.04
C-5	96.46	91.30	97.60	90.32	88.16
C-6	97.64	92.31	98.25	88.89	87.64
Average	**97.30**	**89.82**	**98.40**	**89.85**	**88.36**
Testing Phase (20%)					
C-0	98.44	85.71	100.00	92.31	91.78
C-1	98.44	100.00	98.25	93.33	92.72
C-2	100.00	100.00	100.00	100.00	100.00
C-3	98.44	100.00	98.00	96.55	95.64
C-4	96.88	100.00	96.43	88.89	87.83
C-5	96.88	100.00	96.43	88.89	87.83
C-6	92.19	54.55	100.00	70.59	70.60
Average	**97.32**	**91.47**	**98.44**	**90.08**	**89.49**
Training Phase (70%)					
C-0	99.10	88.24	100.00	93.75	93.48
C-1	98.20	96.67	98.44	93.55	92.57
C-2	98.65	90.62	100.00	95.08	94.45
C-3	94.59	87.76	96.53	87.76	84.29
C-4	98.65	96.55	98.96	94.92	94.15
C-5	96.40	92.31	97.27	90.00	87.84
C-6	98.20	92.31	98.98	92.31	91.29
Average	**97.68**	**92.06**	**98.60**	**92.48**	**91.15**
Testing Phase (30%)					
C-0	98.96	75.00	100.00	85.71	86.14
C-1	100.00	100.00	100.00	100.00	100.00
C-2	98.96	100.00	98.85	94.74	94.32
C-3	94.79	89.47	96.10	87.18	83.96
C-4	98.96	95.45	100.00	97.67	97.05
C-5	100.00	100.00	100.00	100.00	100.00
C-6	97.92	90.91	98.82	90.91	89.73
Average	98.51	92.98	99.11	93.74	93.03

The training accuracy (TACY) and validation accuracy (VACY) of the BSHS-EODL method can be assessed in Figure 5. The figure inferred that the BSHS-EODL algorithm has demonstrated greater results with enhanced values of TACY and VACY. It can be noted that the BSHS-EODL system has obtained maximal TACY outcomes.

The training loss (TLOS) and validation loss (VLOS) of the BSHS-EODL approach are tested in Figure 6. The figure stated that the BSHS-EODL approach has demonstrated higher performance with decreasing TLOS and VLOS. Evidently, the BSHS-EODL algorithm has resulted in lesser VLOS outcomes.

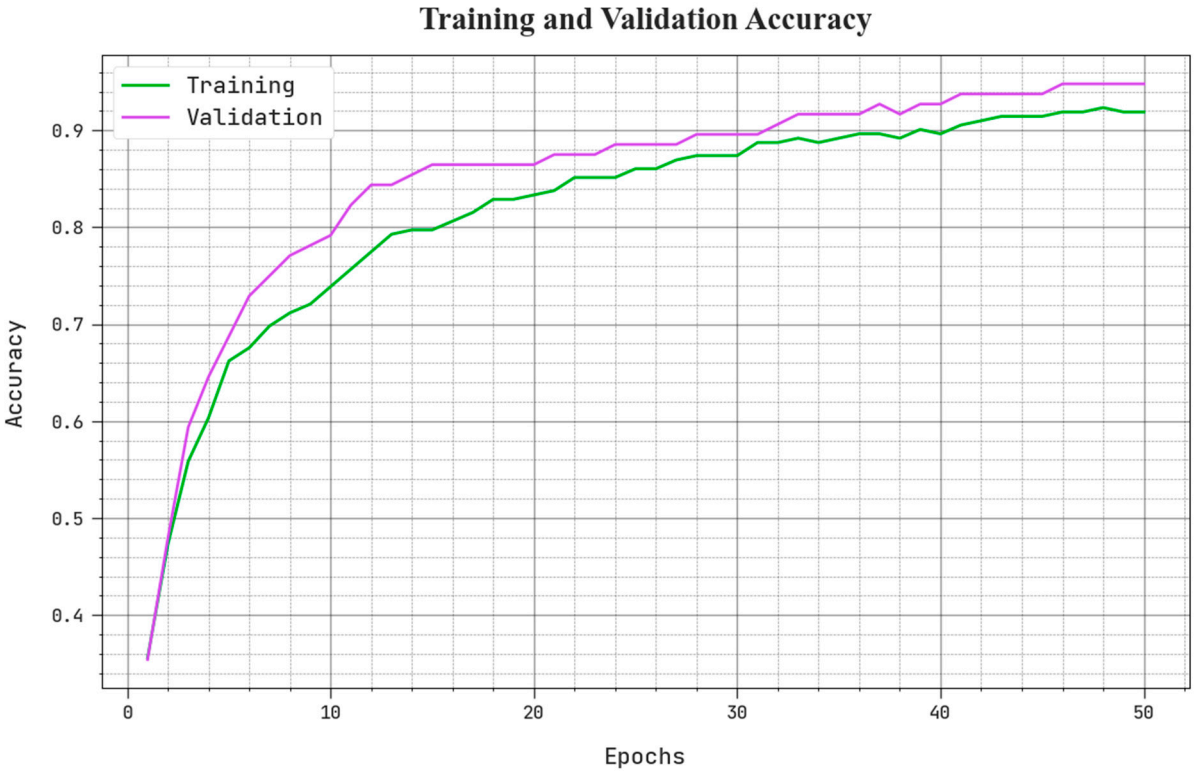

Figure 5. TACY and VACY analysis of BSHS-EODL method.

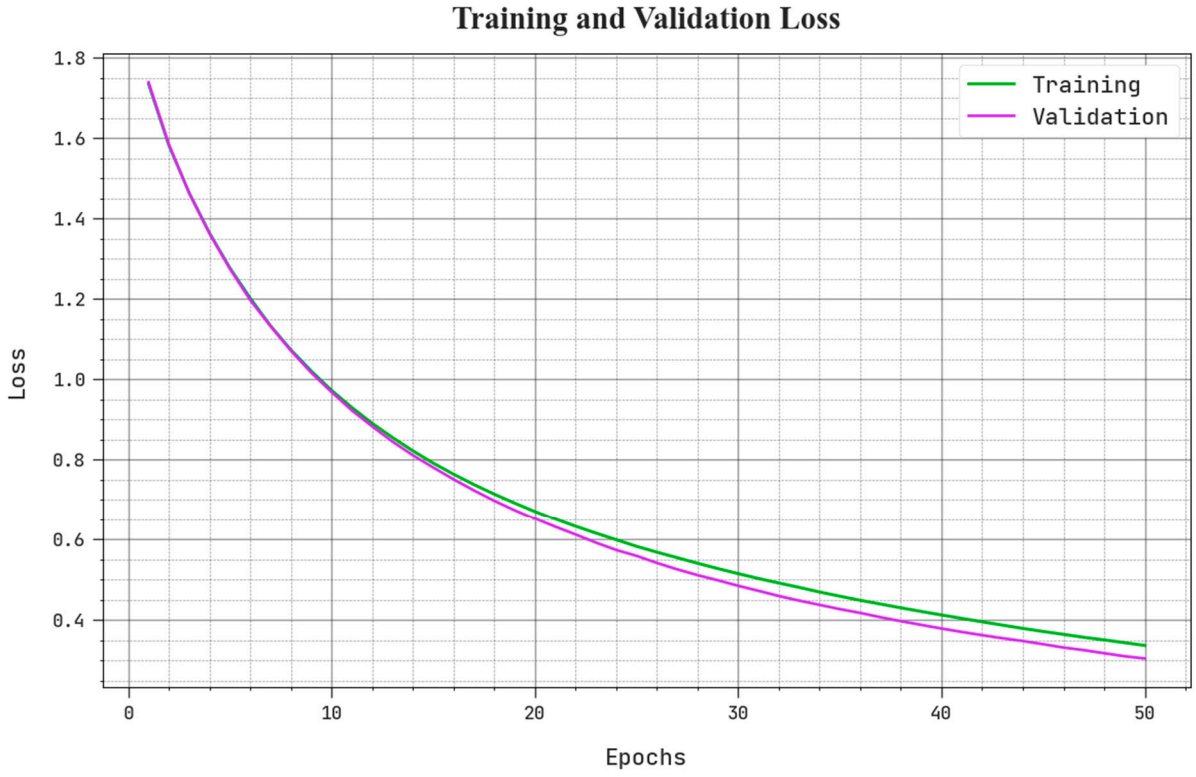

Figure 6. TLOS and VLOS analysis of BSHS-EODL approach.

The extensive comparative study of the BSHS-EODL technique takes place in Table 6 [17,30]. The results highlighted that the VGG-19 model shows least performance, whereas the DBN and YOLO-GC techniques reported moderately similar outcomes. In comparison, the ResNet and CDNN models attain a reasonable performance.

Table 6. Comparative outcome of BSHS-EODL method with other DL techniques.

Methods	Accuracy	Sensitivity	Specificity
BSHS-EODL	98.51	92.98	99.11
DBN [17]	94.15	91.40	90.98
YOLO-GC [17]	94.24	89.30	90.77
ResNet Model [17]	96.19	90.44	91.03
VGG-19 [30]	91.19	90.20	93.73
CDNN [17]	95.29	91.19	92.77

However, the BSHS-EODL technique gains maximum classification performance with $accu_y$ of 98.51%, $sens_y$ of 92.98%, and $spec_y$ of 99.11%. These outcomes ensured the betterment of the BSHS-EODL method over other existing techniques in the IoMT environment.

5. Conclusions

This article introduces a new BSHS-EODL technique for secure medical image transmission and analysis in the IoMT environment. The presented BSHS-EODL technique enables BC assisted secured image transmission and diagnosis models for the IoMT platform. The proposed method includes data classification, data collection, and image encryption. At the initial stage, the IoMT devices enable data collection processes, and the gathered images are stored in BC for security. Subsequently, image encryption is applied to encrypt the data and the key generation process is performed via the DOA. Finally, the BSHS-EODL technique performs disease diagnosis comprising SqueezeNet, BO based parameter tuning, and VELM. A comprehensive set of simulation analyses on medical datasets highlights the supremacy of the BSHS-EODL technique. In upcoming years, the performance of the proposed method can be tested on other disease diagnoses.

Author Contributions: Conceptualization, A.A.; Methodology, A.A.; Software, Y.M.A.; Validation, Y.M.A.; Formal analysis, Y.M.A.; Writing—original draft, A.A.; Writing—review & editing, Y.M.A.; Visualization, A.A.; Funding acquisition, A.A. All authors have read and agreed to the published version of the manuscript.

Funding: This research work is funded by the Deputyship for Research & Innovation, Ministry of Education in Saudi Arabia by the grant number RUP3-1.

Institutional Review Board Statement: This article does not contain any studies with human participants performed by any of the authors.

Data Availability Statement: Data sharing is not applicable to this article as no datasets were generated during the current study.

Acknowledgments: The authors extend their appreciation to the Deputyship for Research & Innovation, Ministry of Education in Saudi Arabia, for funding this research work through project number RUP3-1.

Conflicts of Interest: The authors declare that they have no conflicts of interest.

References

1. 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*, 731–737. [CrossRef]
2. Garg, N.; Wazid, M.; Das, A.K.; Singh, D.P.; Rodrigues, J.J.; Park, Y. BAKMP-IoMT: Design of blockchain enabled authenticated key management protocol for internet of medical things deployment. *IEEE Access* **2020**, *8*, 95956–95977. [CrossRef]
3. Gul, M.J.; Rehman, A.; Paul, A.; Rho, S.; Riaz, R.; Kim, J. Blockchain expansion to secure assets with fog node on special duty. *Soft Comput.* **2020**, *24*, 15209–15221. [CrossRef]
4. Kagita, M.K.; Thilakarathne, N.; Gadekallu, T.R.; Maddikunta, P.K.R. A review on security and privacy of internet of medical things. *Intell. Internet Things Healthc. Ind.* **2022**, 171–187.
5. Dai, H.N.; Imran, M.; Haider, N. Blockchain-enabled internet of medical things to combat COVID-19. *IEEE Internet Things Mag.* **2020**, *3*, 52–57. [CrossRef]

6. Roshanzamir, M.; Darbandy, M.T.; Roshanzamir, M.; Alizadehsani, R.; Shoeibi, A.; Ahmadian, D. Swarm Intelligence in Internet of Medical Things. In Proceedings of the 2022 IEEE 10th Jubilee International Conference on Computational Cybernetics and Cyber-Medical Systems (ICCC), Reykjavík, Iceland, 6–9 July 2022; pp. 371–376.
7. Razdan, S.; Sharma, S. Internet of medical things (IoMT): Overview, emerging technologies, and case studies. *IETE Tech. Rev.* **2022**, *39*, 775–788. [CrossRef]
8. Egala, B.S.; Pradhan, A.K.; Badarla, V.; Mohanty, S.P. 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*, 11717–11731. [CrossRef]
9. Dwivedi, R.; Mehrotra, D.; Chandra, S. Potential of Internet of Medical Things (IoMT) applications in building a smart healthcare system: A systematic review. *J. Oral Biol. Craniofacial Res.* **2022**, *12*, 302–318. [CrossRef]
10. Lakhan, A.; Mohammed, M.A.; Elhoseny, M.; Alshehri, M.D.; Abdulkareem, K.H. 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*, 6429–6442. [CrossRef]
11. Almaiah, M.A.; Ali, A.; Hajjej, F.; Pasha, M.F.; Alohali, M.A. A lightweight hybrid deep learning privacy preserving model for FC-based industrial internet of medical things. *Sensors* **2022**, *22*, 2112. [CrossRef]
12. Khan, A.A.; Wagan, A.A.; Laghari, A.A.; Gilal, A.R.; Aziz, I.A.; Talpur, B.A. BIoMT: A state-of-the-art consortium serverless network architecture for healthcare system using blockchain smart contracts. *IEEE Access* **2022**, *10*, 78887–78898. [CrossRef]
13. Abbas, A.; Alroobaea, R.; Krichen, M.; Rubaiee, S.; Vimal, S.; Almansour, F.M. Blockchain-assisted secured data management framework for health information analysis based on Internet of Medical Things. *Pers. Ubiquitous Comput.* **2021**, 1–14. [CrossRef]
14. Lakhan, A.; Mohammed, M.A.; Kozlov, S.; Rodrigues, J.J. Mobile-fog-cloud assisted deep reinforcement learning and blockchain-enable IoMT system for healthcare workflows. *Trans. Emerg. Telecommun. Technol.* **2021**, e4363. [CrossRef]
15. Lakhan, A.; Sodhro, A.H.; Majumdar, A.; Khuwuthyakorn, P.; Thinnukool, O. A lightweight secure adaptive approach for internet-of-medical-things healthcare applications in edge-cloud-based networks. *Sensors* **2022**, *22*, 2379. [CrossRef]
16. Kumar, R.; Tripathi, R. Towards design and implementation of security and privacy framework for internet of medical things (iomt) by leveraging blockchain and ipfs technology. *J. Supercomput.* **2021**, *77*, 7916–7955. [CrossRef]
17. Alqaralleh, B.A.; Vaiyapuri, T.; Parvathy, V.S.; Gupta, D.; Khanna, A.; Shankar, K. Blockchain-assisted secure image transmission and diagnosis model on Internet of Medical Things Environment. *Pers. Ubiquitous Comput.* **2021**, 1–11. [CrossRef]
18. Al-Otaibi, Y.D. K-nearest neighbour-based smart contract for internet of medical things security using blockchain. *Comput. Electr. Eng.* **2022**, *101*, 108129. [CrossRef]
19. Uppal, S.; Kansekar, B.; Mini, S.; Tosh, D. HealthDote: A blockchain-based model for continuous health monitoring using interplanetary file system. *Healthc. Anal.* **2023**, *3*, 100175. [CrossRef]
20. Zakzouk, A.; El-Sayed, A.; Hemdan, E.E.D. A blockchain-based electronic medical records management framework in smart healthcare infrastructure. *Multimed. Tools Appl.* **2023**, 1–19. [CrossRef]
21. Karthik, G.M.; Kalyana Kumar, A.S.; Karri, A.B.; Jagini, N.P. Deep intelligent blockchain technology for securing IoT-based healthcare multimedia data. *Wirel. Netw.* **2023**, 1–13. [CrossRef]
22. Miriam, H.; Doreen, D.; Dahiya, D.; Rene Robin, C.R. Secured Cyber Security Algorithm for Healthcare System Using Blockchain Technology. *Intell. Autom. Soft Comput.* **2023**, *35*, 1889–1906. [CrossRef]
23. Hussain, M.; Iqbal, N.; Bashir, Z. A chaotic image encryption scheme based on multi-directional confusion and diffusion operations. *J. Inf. Secur. Appl.* **2022**, *70*, 103347. [CrossRef]
24. Almazán-Covarrubias, J.H.; Peraza-Vázquez, H.; Peña-Delgado, A.F.; García-Vite, P.M. An improved Dingo optimization algorithm applied to SHE-PWM modulation strategy. *Appl. Sci.* **2022**, *12*, 992. [CrossRef]
25. Maw, A.; Adepu, S.; Mathur, A. ICS-BlockOpS: Blockchain for operational data security in industrial control system. *Pervasive Mob. Comput.* **2019**, *59*, 101048. [CrossRef]
26. Shafiee, M.J.; Li, F.; Chwyl, B.; Wong, A. Squishednets: Squishing squeezenet further for edge device scenarios via deep evolutionary synthesis. *arXiv* **2017**, arXiv:1711.07459.
27. Atteia, G.; Alhussan, A.A.; Samee, N.A. BO-ALLCNN: Bayesian-Based Optimized CNN for Acute Lymphoblastic Leukemia Detection in Microscopic Blood Smear Images. *Sensors* **2022**, *22*, 5520. [CrossRef]
28. Kushwah, G.S.; Ranga, V. Voting extreme learning machine based distributed denial of service attack detection in cloud computing. *J. Inf. Secur. Appl.* **2020**, *53*, 102532. [CrossRef]
29. Padmavathi, U.; Rajagopalan, N. Blockchain Enabled Emperor Penguin Optimizer Based Encryption Technique for Secure Image Management System. *Wirel. Pers. Commun.* **2022**, *127*, 2347–2364. [CrossRef]
30. Yacin Sikkandar, M.; Alrasheadi, B.A.; Prakash, N.B.; Hemalakshmi, G.R.; Mohanarathinam, A.; Shankar, K. Deep learning based an automated skin lesion segmentation and intelligent classification model. *J. Ambient Intell. Humaniz. Comput.* **2021**, *12*, 3245–3255. [CrossRef]