remote sensing

Article

Block-Scrambling-Based Encryption with Deep-Learning-Driven Remote Sensing Image Classification

Faisal S. Alsubaei [1], Amani A. Alneil [2], Abdullah Mohamed [3] and Anwer Mustafa Hilal [2,*]

[1] Department of Cybersecurity, College of Computer Science and Engineering, University of Jeddah, Jeddah 21959, Saudi Arabia
[2] Department of Computer and Self Development, Preparatory Year Deanship, Prince Sattam Bin Abdulaziz University, AlKharj 16278, Saudi Arabia
[3] Research Centre, Future University in Egypt, New Cairo 11845, Egypt
* Correspondence: a.hilal@psau.edu.sa

Abstract: Remote sensing is a long-distance measuring technology that obtains data about a phenomenon or an object. Remote sensing technology plays a crucial role in several domains, such as weather forecasts, resource surveys, disaster evaluation and environment protection. The application of remote-sensing images (RSIs) is extensive in some specific domains, such as national security and business secrets. Simple multimedia distribution techniques and the development of the Internet make the content security of RSIs a significant problem for both engineers and scientists. In this background, RSI classification using deep learning (DL) models becomes essential. Therefore, the current research article develops a block-scrambling-based encryption with privacy preserving optimal deep-learning-driven classification (BSBE-PPODLC) technique for the classification of RSIs. The presented BSBE-PPODLC technique follows a two-stage process, i.e., image encryption and classification. Initially, the RSI encryption process takes place based on a BSBE approach. In the second stage, the image classification process is performed, and it encompasses multiple phases, such as densely connected network (DenseNet) feature extraction, extreme gradient boosting (XGBoost) classifier and artificial gorilla troops optimizer (AGTO)-based hyperparameter tuning. The proposed BSBE-PPODLC technique was simulated using the RSI dataset, and the outcomes were assessed under different aspects. The outcomes confirmed that the presented BSBE-PPODLC approach accomplished improved performance compared to the existing models.

Keywords: remote-sensing images; image encryption; deep learning; privacy-preserving; hyperparameter tuning; security

check for updates

Citation: Alsubaei, F.S.; Alneil, A.A.; Mohamed, A.; Mustafa Hilal, A. Block-Scrambling-Based Encryption with Deep-Learning-Driven Remote Sensing Image Classification. *Remote Sens.* **2023**, *15*, 1022. https://doi.org/10.3390/rs15041022

Academic Editors: Gyanendra Prasad Joshi, Shankar Kathiresan and Seifedine Kadry

Received: 11 January 2023
Revised: 26 January 2023
Accepted: 31 January 2023
Published: 12 February 2023

1. Introduction

Remote-sensing images (RSIs) have become significant carriers of geospatial information. Their military and economic value are important and serve a crucial role in various domains, such as reconnaissance, surveying and mapping, monitoring and navigation [1]. Though the open network environment and digital storage technique help in realizing rapid communication and effective sharing of RSIs, it brings new difficulties in terms of security for the image datasets. Recently, ownership violations, data leakage and illegal tampering against RSIs have been repetitively prohibited [2,3]. Cloud storage is a cost-effective service that provides huge storage space and provides a lot of new opportunities for huge RSIs. Owing to the openness of Cloud technology, the information that is stored in the Cloud is at risk of malicious damage or deletion by the Cloud service providers [4]. In this background, ensuring the safety of RSIs saved in Cloud storage has been a hot research topic in recent years.

RSIs capture sensitive data, such as military places, oilfields and airports, which are at the risk of being misused and stolen. Further, when such images are processed without safety precautions, it eases the extraction process and provides seamless access to sensitive data that in turn may be exploited for illegal activities. This scenario suggests the requirement for developing a reliable privacy approach that ensures the encryption of large-scale RSIs on the Cloud server without being compromised. Privacy preservation in RSIs is essential as they frequently contain sensitive data of the individuals and their properties. This data may be exploited for unauthorized surveillance, theft of identity and other malicious actions. Moreover, the release of such sensitive data is unethical and illegal and violates an individual's right to privacy. Thus, it is essential to protect the individual's privacy and their properties in RSIs by executing a few methods such as access control, data masking and data encryption.

Encryption acts as a potential means of security. If the encoded data are stored in Clouds, it is simple to tamper with the cipher text, and the encrypted outcomes may not be restorable [5,6]. To avoid this situation, many backups of secret information are needed. In [7], the author presented an overview of the privacy-preservation deep learning (PPDL) method that was implemented to protect the privacy of businesses or individual users. This work deceptively argues that the PPDL approaches benefitted from public data analytics. Further, the approaches also thwarted data leakage and maintained the privacy of delicate data from illegal use and unauthorized access [8,9]. DL is typically utilized to build prediction methods for speech and text recognition applications and image processing. Such methods are highly accurate and particularly trained on large datasets [10]. Prediction techniques learn from the existing available datasets and utilize the knowledge to generate novel data that were once inaccessible. In several cases, such information even comprises delicate data that require preservation. Thus, there is a significant challenge existing here, i.e., to protect the privacy of the data if it is transferred to the public Cloud for analysis and processing [11,12]. In most cases, personal computers are not capable of processing huge satellite images. Thus, to extract the insights and valuable knowledge from such huge RS datasets, there comes a higher demand for the execution of big data analytics utilizing public Cloud servers [13]. As mentioned earlier, the satellite images may contain delicate and confidential data, such as military locations, oilfields and airports that can be misused and stolen. Similarly, if these images are processed without protection, it becomes easy to derive the delicate data and exploit it for illegal purposes [14,15]. Hence, it is both a challenging and a rewarding task to explore the possible PPDL approaches to implement them in the satellite images.

Al-Khasawneh et al. [16] described a novel chaos-related encryption method that utilizes Gauss-iterated maps, an external secret key, Henon and Logistic. The presented encryption technique was able to effectively encode a large number of images. If the number of images increases, though the images are smaller in size, the technology becomes impractical or inefficient. This study also analyzed the parallel image encryption technique on a huge number of RSIs in Hadoop. Zhang et al. [17] devised a QAPP method, i.e., quality-aware and privacy-preserving medical image release technique, which efficiently compiled DCT with differential privacy (DP). To be specific, QAPP had three stages. Initially, DCT was implemented in all the medical images to gain its cosine coefficients matrix. Secondly, the original cosine coefficients matrixes were compressed into k*k cosine coefficients matrixes which retained the core features of all the images. Thirdly, a suitable Laplace noise was injected into the formed k*k matrixes to attain differential privacy. Then, the noise-added coefficients were utilized for building the noise-added healthcare images using inverse DCT.

In [18], a new biometric-related authentication mechanism was modelled utilizing two servers, such as the untrusted storage server and a crypto-match server. This mechanism used the Paillier cryptosystem, the biometric image cryptosystem and cryptographic hashing. In the presented cryptosystem, the keystreams were generated from both logistic maps and Henon. It is possible to compute the control variables of such chaotic maps from the input biometric images. Abd EL-Latif et al. [19] presented a new encryption system for a privacy-preserving IoT-related healthcare mechanism in order to protect the privacy of the patients. Decryption or encryption processes depend on controlled alternate quantum walks. The presented cryptosystem method had two stages, such as permutation and substitution, and both were related to independently computed quantum walks. In the study conducted earlier [20], the authors used the BC to build a new privacy-preserving remote data integrity checking technique for IoT information management mechanism without the inclusion of trusted third parties. This technique used BC, a lifted EC-ElGamal cryptosystem and bilinear pairing to protect the security and data privacy of the IoT mechanisms and also to support an effective public batch signature verification.

Qin et al. [21] devised a privacy-preserving image retrieval technique related to adaptive weighted fusion and DL. At first, the authors derived the high-level semantic features of the images, low-level feature edge histogram descriptors and the BOW (bag of words). Then, a pre-filter table was built for the fusion features in order to enhance the search efficiency by the locality-sensitive hashing (LSH) technique. Both the logistic encryption method and the KNN technique were utilized in this study to protect the privacy of the fused images and features, correspondingly. In [22], a privacy-preserving effective and secure remote user authentication method was proposed to be applied in agricultural WSN. The presented technique was formally assessed through a probabilistic random-oracle-model (ROR) to emphasize the robustness of the method. In addition, the technique was also simulated through the AVISPA tool to exhibit its effectiveness in terms of security.

Yang and Newsam [23] examined the bag-of-visual-words (BOVW) systems for land-use classifiers from high-resolution overhead images. The authors assumed a typical non-spatial representation in which the frequency can be utilized for segregation amongst the analogous classes' and not the places of quantized image features. The proposed feature was used to determine how words can be exploited in the text document classifier without considering their order of presentation. In [24], the authors concentrated entirely on the existing approaches that manage the RSI scene classifier on restricted labelled instances. The authors classified literary works under three broad categories, such as algorithm-level, data-level and model-level. Zhou et al. [25] conducted a systematic review of the presently established RSIR approaches and benchmarks using over 200 papers. In particular, the authors grouped the RSIR approaches under different hierarchical models based on label, modality and image source. Zhu et al. [26] aimed at assisting this work by systematically examining the DL approaches and their applications across different sensor schemes. The authors also offered a detailed summary of the DL execution tips and connection to tutorials, open-source codes and pre-trained approaches that act as great self-contained reference materials for DL practitioners and individuals who are looking forward to being introduced to DL.

Numerous automated tools are available in the literature for effective detection and classification of RSIs. Despite the presence of ML and DL models in the earlier studies, there is still a need to enhance the classification performance along with security. Due to the continuous deepening of the models, the number of parameters in DL models increases too quickly, which results in a model overfitting issue. At the same time, different hyperparameters exert significant impact on the efficiency of the CNN model. Particularly, a few hyperparameters, such as epoch count, batch size and learning rate selection are essential to attain effective outcomes. Since the trial-and-error method for hyperparameter tuning is a tedious and erroneous process, the metaheuristic algorithms are applied. Therefore, in this work, the artificial gorilla troops optimizer (AGTO) algorithm is employed for parameter selection of the DenseNet model. The inclusion of the automated hyperparameter tuning techniques helps reduce the computation time and improve RSI classification performance. In addition, the inclusion of the encryption technique results in enhanced security of the RSIs.

The current research article develops a block-scrambling-based encryption with privacy preserving optimal deep-learning-driven classification (BSBE-PPODLC) technique for the classification of RSIs. The presented BSBE-PPODLC technique initially encrypts the RSI using the BSBE technique, which enables the secure communication of the images in a wireless medium. During the reception process, both decryption and image classification processes occur. In the presented BSBE-PPODLC technique, the image classification process encompasses three sub-processes, namely, densely connected network (DenseNet) feature extraction, extreme gradient boosting (XGBoost) classifier and AGTO-based hyperparameter tuning. The proposed BSBE-PPODLC technique was simulated using the RSI dataset, and the results were assessed under several aspects.

2. The Proposed Model

The current research paper introduces an effective BSBE-PPODLC approach for encryption and classification of the RSIs. The presented BSBE-PPODLC technique initially encrypts the RSIs using the BSBE technique, which enables the secure communication of the images in a wireless medium. During the reception process, both decryption and image classification processes occur. In the presented BSBE-PPODLC technique, the image classification process encompasses three sub-processes, namely DenseNet feature extraction, XGBoost classifier and AGTO-based hyperparameter tuning. Figure 1 represents the block diagram of the proposed BSBE-PPODLC approach.

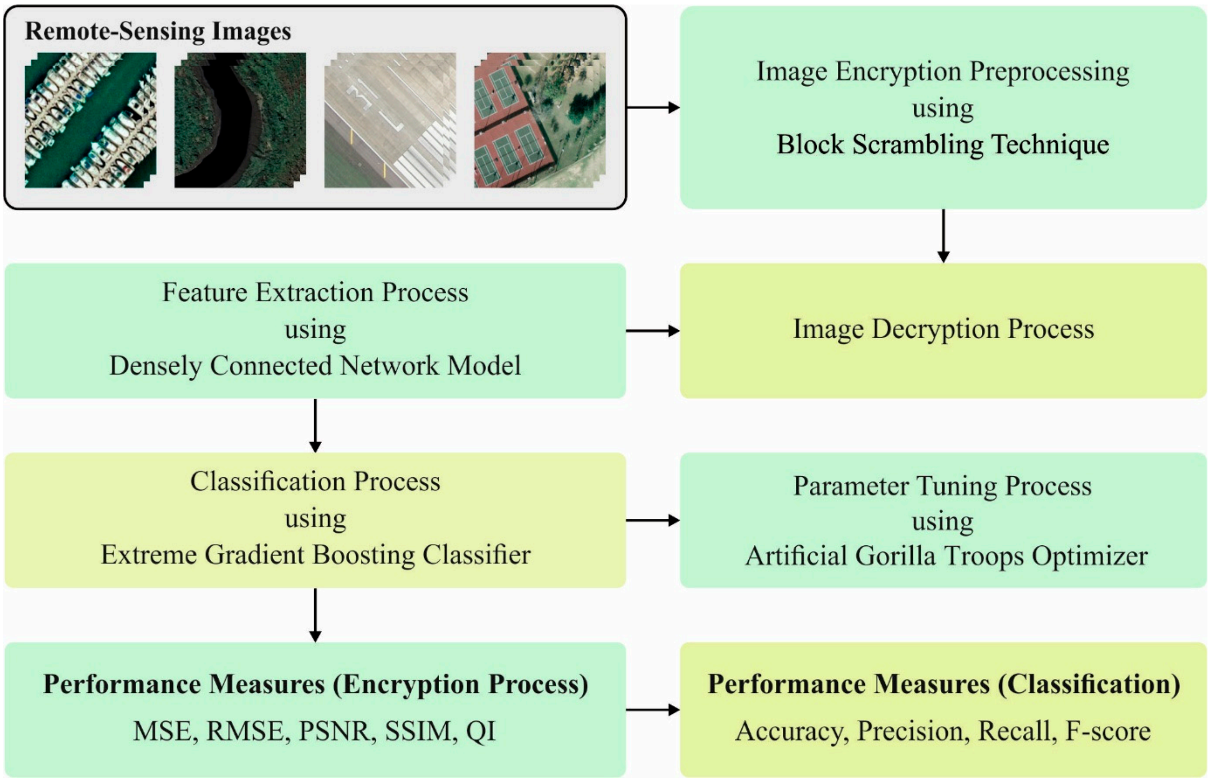
Remote-Sensing Images
Image Encryption Preprocessing using Block Scrambling Technique
Feature Extraction Process using Densely Connected Network Model
Image Decryption Process
Classification Process using Extreme Gradient Boosting Classifier
Parameter Tuning Process using Artificial Gorilla Troops Optimizer
Performance Measures (Encryption Process)
MSE, RMSE, PSNR, SSIM, QI
Performance Measures (Classification)
Accuracy, Precision, Recall, F-score

Figure 1. Block diagram of BSBE-PPODLC system.

2.1. Encryption Using the BSBE Technique

The BSBE technique is employed in this study for secure encryption of the RSIs. In the BSBE technique, a user may want to securely transmit image I to viewers using social networking service (SNS) providers [27]. While the consumer does not provide the confidential key K to the SNS provider, the privacy of the image that was shared under the control of the users is secured, even if the SNS provider recompresses image I. Thus, the consumer is assured of the privacy by him/herself. In case of CtE methods, the consumer is bound to disclose the unencrypted images to recompress them.

In this method, an image with $X \times Y$ pixels is primarily separated into non-overlapped blocks with $B_x \times B_y$; afterwards, four block-scrambling-based processing stages are executed to separate the images. The process to execute the image encryption to generate the encryption image I_e is provided as follows:

Step 1: Separate the image into $X \times Y$ pixels as blocks and each block with $B_x \times B_y$ pixels. Then, permute the separated blocks arbitrarily with the help of an arbitrary integer created by a confidential key K_1, L bit per pixel. During this work, the occurrence value K_1 has generally been utilized for every color element.

Step 2: Rotate and invert all the blocks arbitrarily by utilizing an arbitrary integer created by the key K_2, whereas K_2 has generally been utilized for every colour element as well.

Step 3: Execute negative–positive alteration for all the blocks by K_3, whereas K_3 is generally utilized for every colour element.

During this stage, the transformed pixel value from i^{th} block B_i, p', is calculated as given below.

$$p' = \begin{cases} p & (r(i) = 0), \\ p \oplus (2^L - 1) & (r(i) = 1). \end{cases} \tag{1}$$

Here, $r(i)$ implies an arbitrary binary integer created by K_3 *and* $p \in B_i$ signifies the pixel value of a novel image with L bit per pixel. During this work, the value of the occurrence probability $P(r(i)) = 0.5$ is utilized for inverting the bits arbitrarily.

Step 4: Shuffle three color elements from all the blocks by utilizing an integer that is arbitrarily chosen amongst six integers by key K_4.

An instance of the encryption image is $\left(B_x = B_y = 16\right)$. During this case, it is concentrated on the block-scrambling-based image encrypt for subsequent reasons.

(a) The encrypted image is well-suited for JPEG standards.
(b) The compression efficacy to encrypt the images is almost similar to the original ones in the JPEG standard.
(c) Robustness against several attacks is established.

2.2. Image Classification Module

During the classification process, the BSBE-PPODLC technique encompasses three sub-processes, namely DenseNet feature extraction, XGBoost classifier and AGTO-based hyperparameter tuning. XGBoost is chosen due to the following advantages: high accuracy, fast training speed, scalability, robustness and flexibility.

2.2.1. Feature Extraction

For the feature extraction process, the DenseNet model is exploited in the current study [28]. DenseNet was chosen due to its efficiency on a combination of features from many layers. Further, it also enables better feature representation and reduces the risk of overfitting. The DenseNet model links every layer with another one in a feedforward manner, thus generating a dense block of layers. It enables the free movement of the data and their gradients via the network and enables robust learning of the features. It requires fewer parameters than the classical CNN, which in turn minimizes the risk of overfitting and makes it computationally efficient.

DenseNet differs from ResNet in the way how the data are passed. In DenseNet, the feature map of the output layer is concatenated with the incoming feature maps instead of adding them. Therefore, the equation is transformed as follows.

$$x_l = H_l([x_0 + x_1 + \ldots + x_{l-1}]) \tag{2}$$

The same problem has been confronted in the studies conducted on ResNet in which it is not possible to combine or concatenate the activities of feature maps since they are of distinct sizes despite. So, it is not practical to either concatenate or add the feature maps in ResNet. DenseNet is separated into dense blocks. In this regard, the dimension of the feature map remains unchanged, whereas the number of filters changes between them. The layer that exists between the dense blocks is termed a transition layer. It can be utilized for downsampling through 2 × 2 pooling, batch normalization and 1 × 1 convolutional layers.

The channel dimension increases at all the layers due to the concatenation of the feature map; 'k' represents the growth rate hyperparameter which maintains the quantity of the data that is saved in all the layers of the network. When $H_{-}1$ produces k feature maps, the generalized formula to determine the number of feature maps using the l-th layer is demonstrated in the above formula.

A feature map acts as the data or learning data of the network. All the layers have access to the feature map of the preceding layers due to which it possesses collective knowledge. All the layers add feature maps or new data to this collective knowledge in a concrete k feature map of the data. Consequently, DenseNet saves and utilizes the data from the preceding layers which is not so in the case of conventional ConvNet and ResNet models.

2.2.2. Hyperparameter Tuning

To adjust the hyperparameter values of the DenseNet method, the AGTO algorithm is used in this study. The knowledge of the group performances in wild gorillas inspires the AGTO technique [29]. Initializing, global exploration and local exploitation are three stages which make up the AGTO, similar to other intelligent approaches.

Initialization Phase

Assume that a D-dimensional space has N gorillas. To identify the position of the i^{th} gorilla in the universe, it is expressed as $X_i = (x_{i,1},\ x_{i,2},\ \ldots x_{i,\ D})$, in which $I = 1, 2, \ldots N$ and is determined as follows:

$$X_{N\times D} = rand(N,\ D) \times (ub - lb) + lb \tag{3}$$

where $rand\ ()$ lies between 0 and 1. The searching range is defined based on the upper as well as lower limits, ub and lb, respectively. The matrix X has A arbitrary value in the range of 0 and 1, and it is assigned to every element of N rows and D columns from the matrix signified as $rand\ (N,\ D)$.

Exploration Phase

$$\begin{gathered} GX(t+1) = (ub - lb) \times r2 + lb,\ r1 < p \\ (r3 - C) \times XA(t) + L \times Z \times X(t),\ r1 \geq 0.5 \\ X(t) - L \times (L \times (X(t) - XB(t)) + r4 \times (X(t) - XB(t)))r1 < 0.5. \end{gathered} \tag{4}$$

At this point, t implies the iteration time, $X(t)$ signifies the gorilla's predefined position vector, and $GX(t+1)$ refers to the position of the potential searching agent during the subsequent iteration. Additionally, the arbitrary numbers $r1$, $r2$, $r3$ and $r4$ imply the number value between 0 and 1. Two places between the predefined gorillas' population, $XA(t)$ and $B(t)$, are chosen arbitrarily; p stands for a fixed value. With the employment of the problem dimensional as an index, Z indicates the row vector, whereas the element value is developed arbitrarily in $[-C,\ C]$. In addition, C is expressed as follows

$$C = (\ \cos\ (2 \times r5) + 1) \times \left(1 - \frac{t}{Maxiter}\right) \tag{5}$$

At this point, cos $(\bullet)$ implies the cosine function, r_5 stands for positive real numbers between zero and one, and $Maxiter$ implies the highest iteration number. The following equation is used to determine L.

$$L = C \times l \tag{6}$$

At this point, l represents an arbitrary value in the range of -1 and 1. Then, all the probable $GX(t+1)$ solutions are created because of the exploration, and the fitness value is related to them. If GX demonstrates X, then it is retained and employed in the place of X. It can be demonstrated as a condition $(GX) < F(X)$. Here, F refers to the fitness function for the problem in question (t). Furthermore, an optimum option that exists at the time is assumed to be the silverback.

Exploitation Phase

If a novel gorilla troop is generated, the silverback is the leading male which is at its peak health and strength. It is followed by blackback gorillas as they forage for food. Certainly, silverbacks tend to age and die, and younger blackbacks from the troops fight other males and occupy and control the troops. The exploitation step in this AGTO model follows the silverback gorillas and plays for adult female gorillas. W is projected to control these moves. Once C in Equation (6) is superior to W, then the silverback primary method is followed.

$$GX(t+1) = L \times M \times (X(t) - Xsilverback) + X(t) \tag{7}$$

In this case, a better solution initiated is represented by the X silverback, the predefined position vector is demonstrated as (t) and L is evaluated using Equation (7). The values of M are determined as follows.

$$M = \left(\frac{\sum_{i=1}^{n} xi(t)}{N \left|_{\frac{xi(t)}{N}} \right|^{2} l} \right) \frac{1}{2l} \tag{8}$$

where N signifies the entire individual number, and $Xi(t)$ refers to the vector that illustrates the position of the gorilla.

$$GX(t+1) = Xsilverback - (Xsilverback \times Q - X(t) \times Q) \times A \tag{9}$$

$$Q = 2 \times r6 - 1 \tag{10}$$

$$A = \phi \times E, \tag{11}$$

$$E = \begin{cases} N1, \; r7 \geq 0.5 \\ N2, \; r7 < 0.5 \end{cases} \tag{12}$$

It can be a pre-determined place as signified by (t) and the influence force, Q, which is estimated by Equations (9) and (10). An arbitrary value within 0 and 1 is employed for $r6$ in Equation (6).

2.2.3. Image Classification

For image classification, the XGBoost model is used. Due to its accurate and fast performance, XGBoost is regarded as a robust ensemble-learning-based classifier [30]. The ensemble architecture is designed based on various decision tree algorithms. In this model, the trees are added to the parent model by training to fit into accurate prediction and to remove the error that results from the preceding trees. In order to overcome the loss function, the gradient descent optimization technique is utilized. The loss gradient diminishes as the model becomes trained accurately, and the process is called gradient boosting. The XGBoost classifier from the Python repository was utilized in this study, in its initial condition, to check for efficiency. The efficiency of the built-in mechanism is estimated concerning cross-entropy loss, called log loss. The more accurate the classification, the lesser the log loss values are.

$$\log \; loss = y \ln{(p)} + (1-y) \ln{(1-p)} \tag{13}$$

where $p = \frac{1}{1+e^{-x}}$, y indicates the actual label within {0, 1} and p represents the probability score.

The system efficiency of the inbuilt XGBoost classifiers are examined, and the variation in the inherent parameter can be performed to minimize the log loss as defined earlier.

3. Results and Discussion

In this section, the proposed BSBE-PPODLC method was experimentally validated using the UCM dataset (http://weegee.vision.ucmerced.edu/datasets/landuse.html), accessed on 14 September 2022. The UCM dataset comprises a set of aerial images of land use in the UC Merced area. It was developed by researchers at the University of California, Merced and is frequently utilized as a benchmark dataset to evaluate the performance of land-use classification tasks. The UCM dataset includes 21 classes of land use, including agriculture, bare land, buildings, forests, grassland, highways and water bodies. It includes 2100 images, each with a size of 256 × 256 pixels and is divided into training and test datasets. The images in the dataset were collected using aerial imagery from the National Agricultural Imagery Program (NAIP). Figure 2 illustrates some of the sample images. Figure 3 demonstrates the original and the encrypted images.

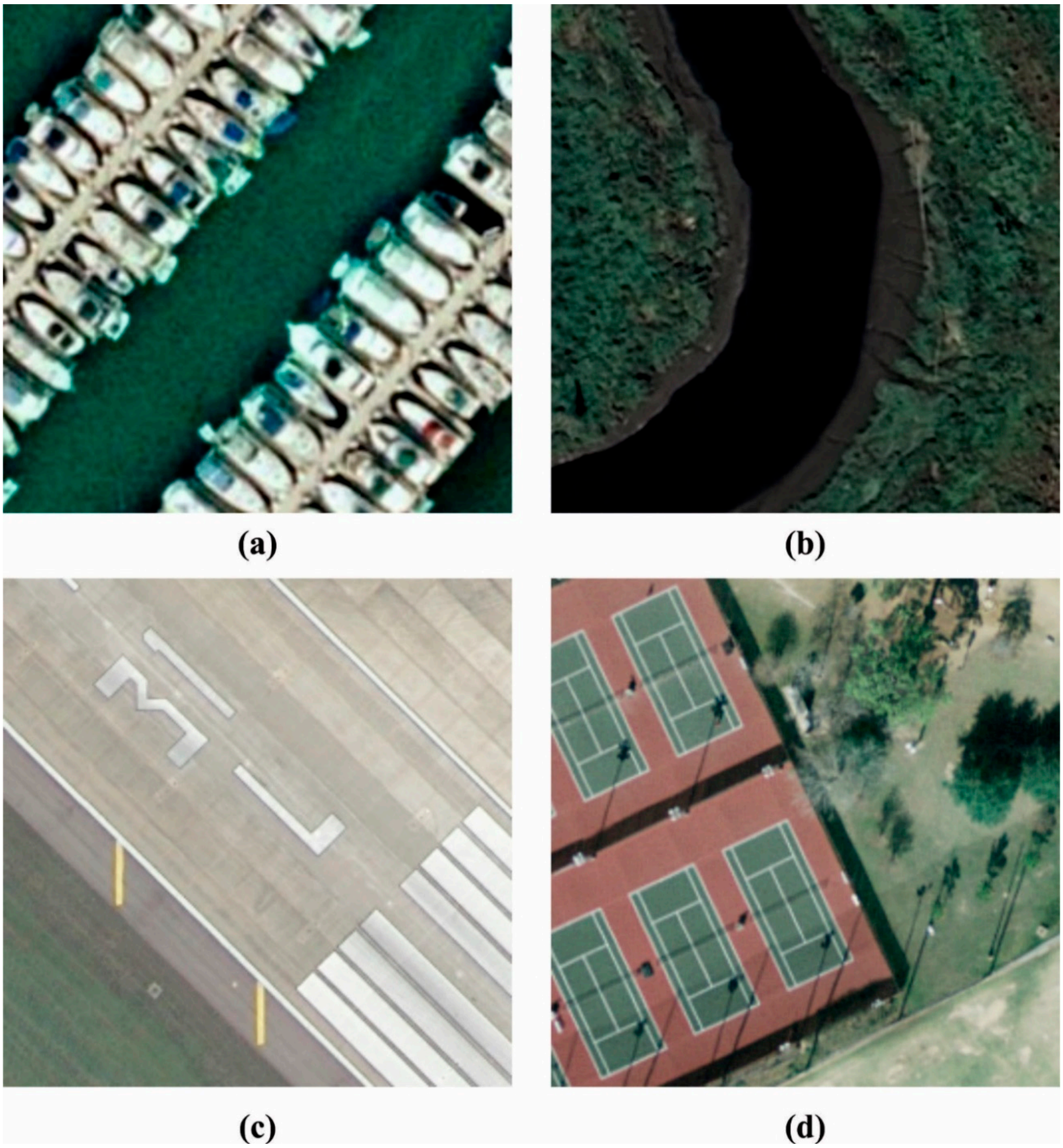

Figure 2. Sample images: (**a**) harbor; (**b**) river; (**c**) runway; (**d**) tennis court.

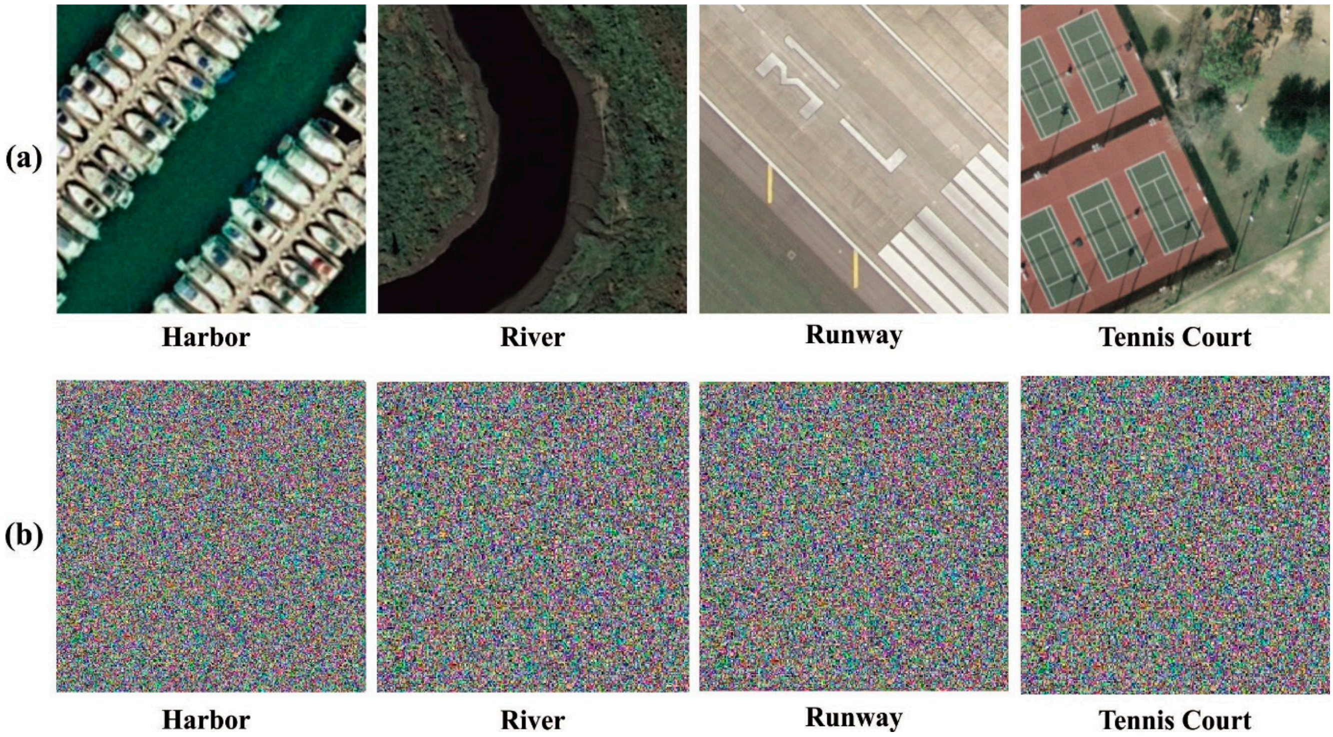

Figure 3. (**a**) Original images; (**b**) encrypted images.

Table 1 represents the overall encryption results achieved by the proposed BSBE-PPODLC model. The experimental outcomes show that the proposed BSBE-PPODLC method achieved effectual performance under all the images. For example, with the harbor test image, the BSBE-PPODLC technique gained an MSE of 0.1956, RMSE of 0.4423, PSNR of 55.22 dB, SSIM of 99.83% and a QI of 99.97%. Meanwhile, with the river test image, the BSBE-PPODLC technique obtained an MSE of 0.2794, RMSE of 0.5286, PSNR of 53.67 dB, SSIM of 99.80% and a QI of 99.90%. Eventually, with the runway test image, the BSBE-PPODLC method reached an MSE of 0.3465, RMSE of 0.5886, PSNR of 52.73 dB, SSIM of 99.80% and a QI of 99.97%.

Table 1. Overall encryption outcomes of the proposed BSBE-PPODLC approach under distinct test images.

Test-Image	MSE	RMSE	PSNR (dB)	SSIM (%)	QI (%)
Harbor	0.1956	0.4423	55.22	99.83	99.97
River	0.2794	0.5286	53.67	99.80	99.90
Runway	0.3465	0.5886	52.73	99.80	99.97
Tennis Court	0.2909	0.5394	53.49	99.81	99.91

In Table 2 and Figure 4, the overall MSE analysis outcomes achieved by the proposed BSBE-PPODLC model and other existing models are given. The outcomes display that the HBMO-LBG and the QPSO-LBG methods attained a poor performance with maximum MSE values. Next, the FF-LBG model and the CS-LBG methods reached moderately low MSE values. Although the SSA-LBG model tried to attain a reasonable MSE value, the BSBE-PPODLC model exhibited the maximum performance with a minimal MSE of 0.1956 for the Harbor image, 0.2794 for the River image, 0.3465 for the runway image and 0.2909 for the tennis court image.

Table 2. MSE analysis results of the proposed BSBE-PPODLC method with other methods for distinct test images.

MSE						
Test-Image	**BSBE-PPODLC**	**SSA-LBG**	**CS-LBG**	**FF-LBG**	**HBMO-LBG**	**QPSO-LBG**
Harbor	0.1956	0.2723	0.3302	0.3780	0.4251	0.4907
River	0.2794	0.3601	0.4269	0.4969	0.5779	0.6400
Runway	0.3465	0.4168	0.4909	0.5477	0.5888	0.6496
Tennis Court	0.2909	0.3752	0.4305	0.4836	0.5706	0.6339

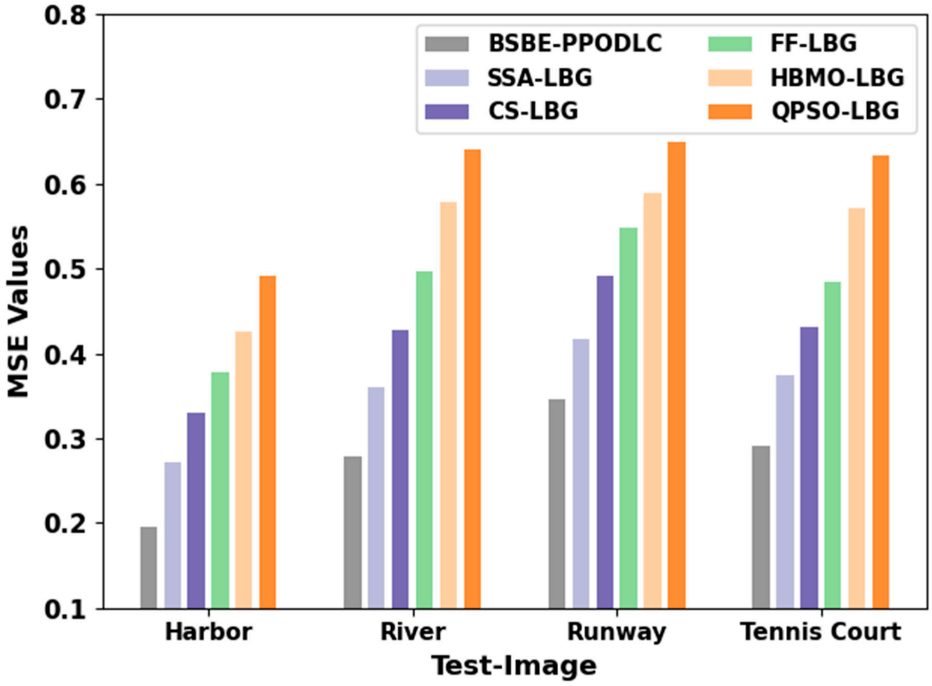

Figure 4. MSE analysis outcomes of the proposed BSBE-PPODLC method for distinct test images.

In Table 3 and Figure 5, the overall PSNR study outcomes accomplished by the proposed BSBE-PPODLC approach and other existing methods are portrayed. The outcomes show that the HBMO-LBG and the QPSO-LBG algorithms achieved a poor performance with minimal PSNR values. Then, the FF-LBG model and the CS-LBG approaches reached moderately increased PSNR values. Although the SSA-LBG technique attempted to achieve a reasonable PSNR value, the proposed BSBE-PPODLC algorithm exhibited improved results with a maximum PSNR of 55.22 dB in the case of the harbor image, 53.67 dB for the river image, 0.3465 for the runway image and 0.2909 for the tennis court image.

Table 3. PSNR analysis outcomes of the proposed BSBE-PPODLC method with other methods for distinct test images.

PSNR (dB)						
Test-Image	**BSBE-PPODLC**	**SSA-LBG**	**CS-LBG**	**FF-LBG**	**HBMO-LBG**	**QPSO-LBG**
Harbor	55.22	53.78	52.94	52.36	51.85	51.22
River	53.67	52.57	51.83	51.17	50.51	50.07
Runway	52.73	51.93	51.22	50.75	50.43	50.00
Tennis Court	53.49	52.39	51.79	51.29	50.57	50.11

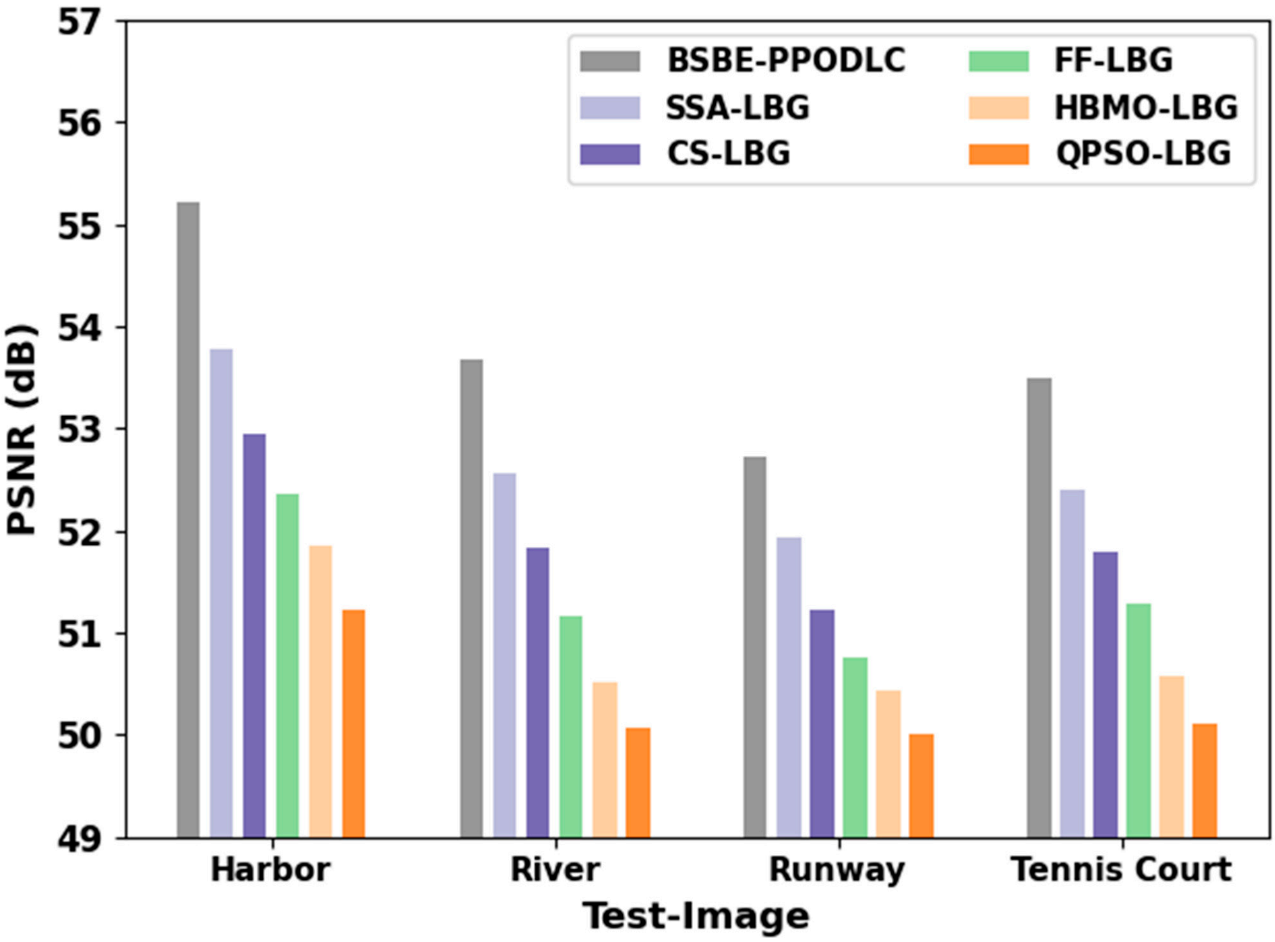

Figure 5. MSE analysis results of the BSBE-PPODLC approach under distinct test images.

In Figure 6, the RSI classification results attained by the proposed BSBE-PPODLC model are presented in the form of a confusion matrix. The results specify that the proposed BSBE-PPODLC method effectively identified four classes.

Table 4 and Figure 7 represent the classification performance of the BSBE-PPODLC model on 80:20 of TR/TS data. The obtained values show that the BSBE-PPODLC algorithm identified all the class labels on the RSIs. For example, with 80% of the TR database, the BSBE-PPODLC technique accomplished an average $accu_y$ of 99.06%, $prec_n$ of 98.18%, $reca_l$ of 98.09% and an F_{score} of 98.10%. Moreover, with 20% of the TS database, the BSBE-PPODLC method attained an average $accu_y$ of 98.12%, $prec_n$ of 96.26%, $reca_l$ of 96.43 % and an F_{score} of 96.25%.

Table 5 and Figure 8 show the classification performance accomplished by the proposed BSBE-PPODLC method on 70:30 of TR/TS data. The gained values show that the BSBE-PPODLC technique identified all the class labels on the RSIs. For example, with 70% of the TR database, the BSBE-PPODLC method established an average $accu_y$ of 98.39%, $prec_n$ of 96.90%, $reca_l$ of 96.77% and an F_{score} of 96.77%. Furthermore, with 30% of the TS database, the BSBE-PPODLC method accomplished an average $accu_y$ of 97.50%, $prec_n$ of 95.18%, $reca_l$ of 95.08 % and an F_{score} of 94.97%.

The TACC and VACC performance outcomes of the BSBE-PPODLC methodology, are shown in Figure 9. The figure implies that the BSBE-PPODLC technique achieved improved performance with increased TACC and VACC values. Notably, the BSBE-PPODLC method reached the maximum TACC outcomes.

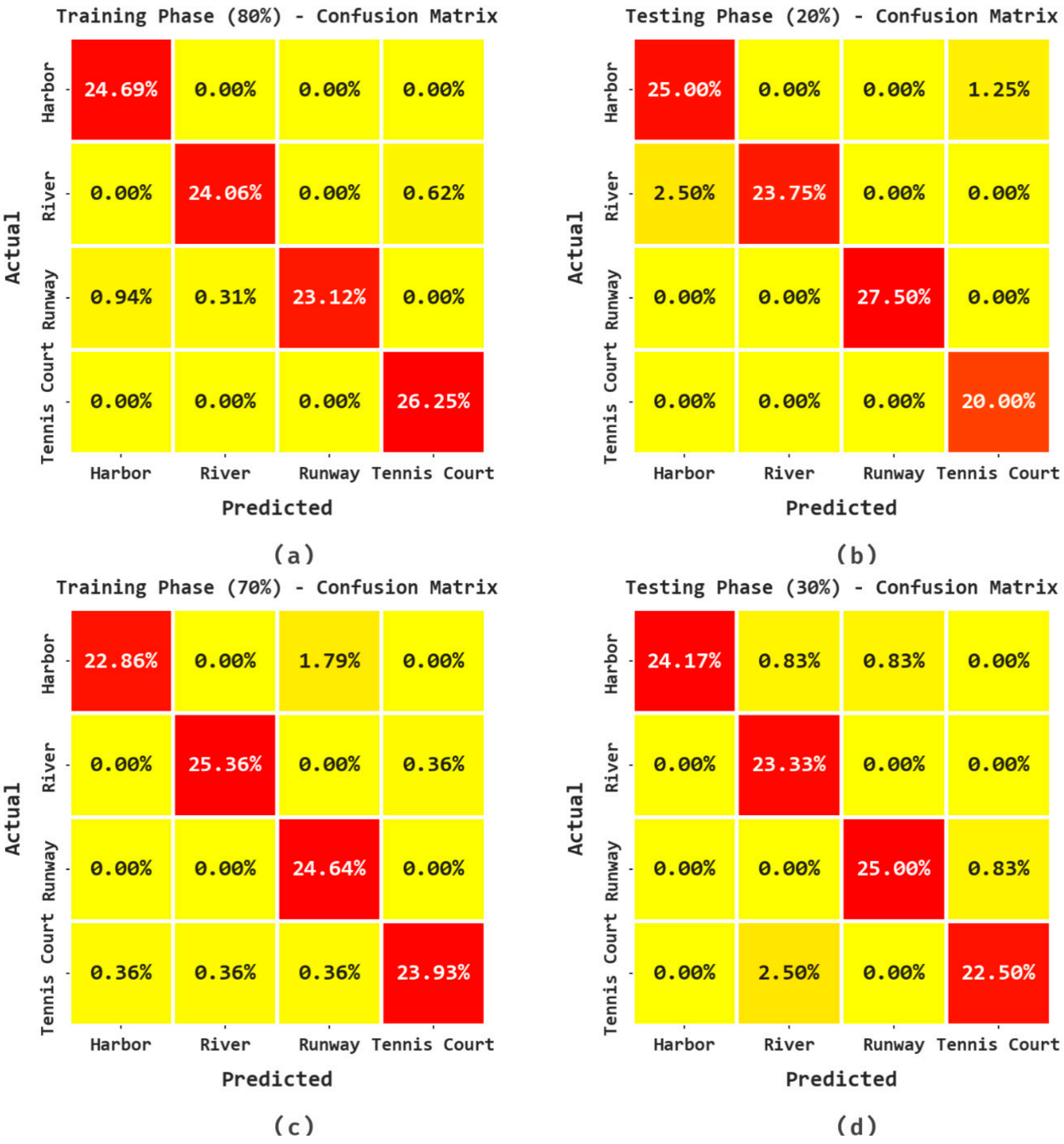

Figure 6. Confusion matrices of the BSBE-PPODLC approach: (**a**,**b**) TR and TS databases of 80:20; (**c**,**d**) TR and TS databases of 70:30.

Table 4. Classification outcomes of the proposed BSBE-PPODLC approach on 80:20 TR/TS datasets.

Class	$Accu_y$	$Prec_n$	$Reca_l$	F_{score}
Testing Phase (80%)				
Harbor	99.06	96.34	100.00	98.14
River	99.06	98.72	97.47	98.09
Runway	98.75	100.00	94.87	97.37
Tennis Court	99.38	97.67	100.00	98.82
Average	**99.06**	**98.18**	**98.09**	**98.10**

Table 4. *Cont.*

Class	$Accu_y$	$Prec_n$	$Reca_l$	F_{score}
Testing Phase (20%)				
Harbor	96.25	90.91	95.24	93.02
River	97.50	100.00	90.48	95.00
Runway	100.00	100.00	100.00	100.00
Tennis Court	98.75	94.12	100.00	96.97
Average	**98.12**	**96.26**	**96.43**	**96.25**

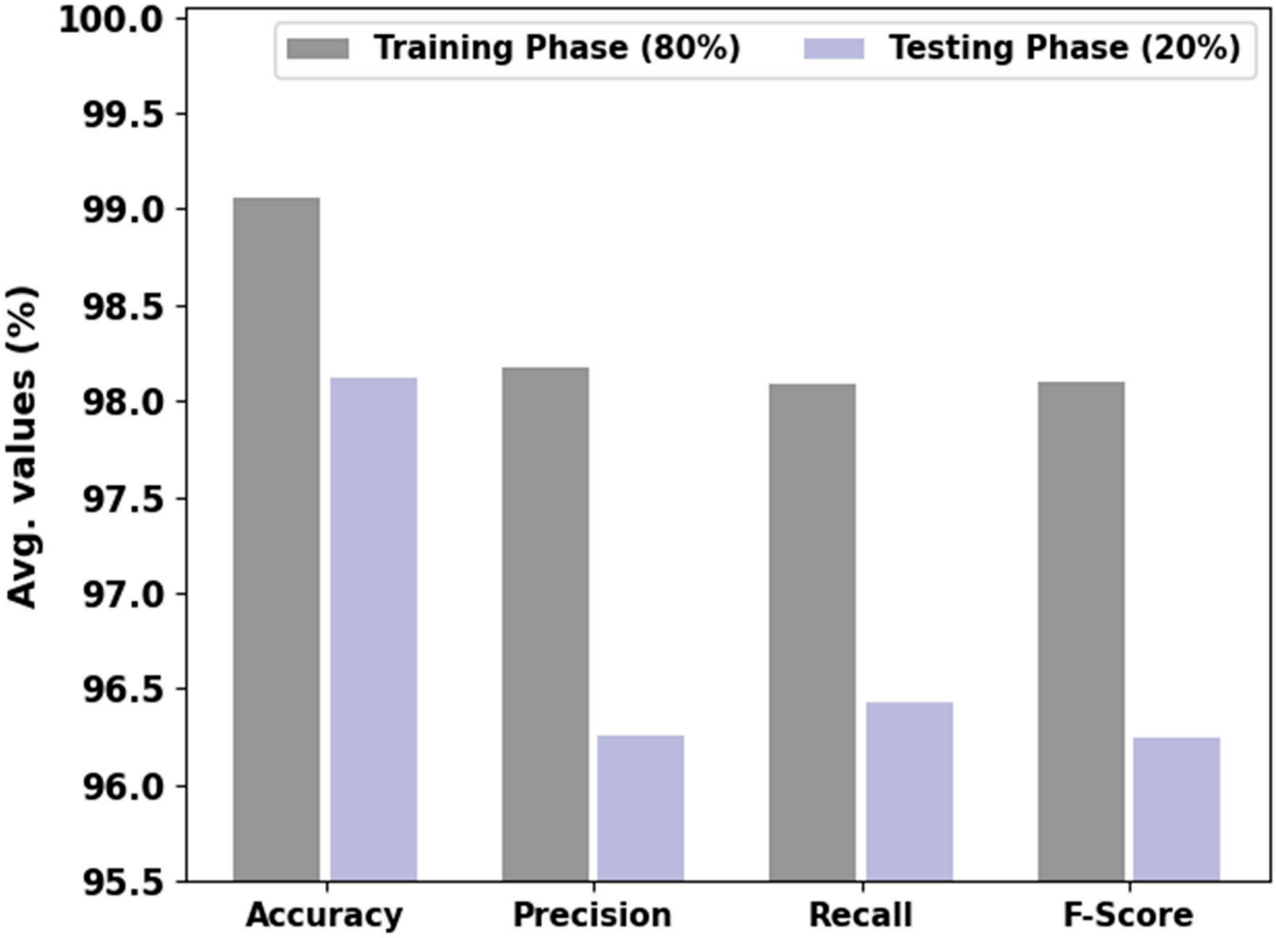

Figure 7. Average outcomes of the BSBE-PPODLC approach on 80:20 on TR/TS datasets.

Table 5. Classification results of the proposed BSBE-PPODLC approach on 70:30 on TR/TS datasets.

Class	$Accu_y$	$Prec_n$	$Reca_l$	F_{score}
Training Phase (70%)				
Harbor	97.86	98.46	92.75	95.52
River	99.29	98.61	98.61	98.61
Runway	97.86	92.00	100.00	95.83
Tennis Court	98.57	98.53	95.71	97.10
Average	**98.39**	**96.90**	**96.77**	**96.77**

Table 5. *Cont.*

Class	$Accu_y$	$Prec_n$	$Reca_l$	F_{score}
Testing Phase (30%)				
Harbor	98.33	100.00	93.55	96.67
River	96.67	87.50	100.00	93.33
Runway	98.33	96.77	96.77	96.77
Tennis Court	96.67	96.43	90.00	93.10
Average	**97.50**	**95.18**	**95.08**	**94.97**

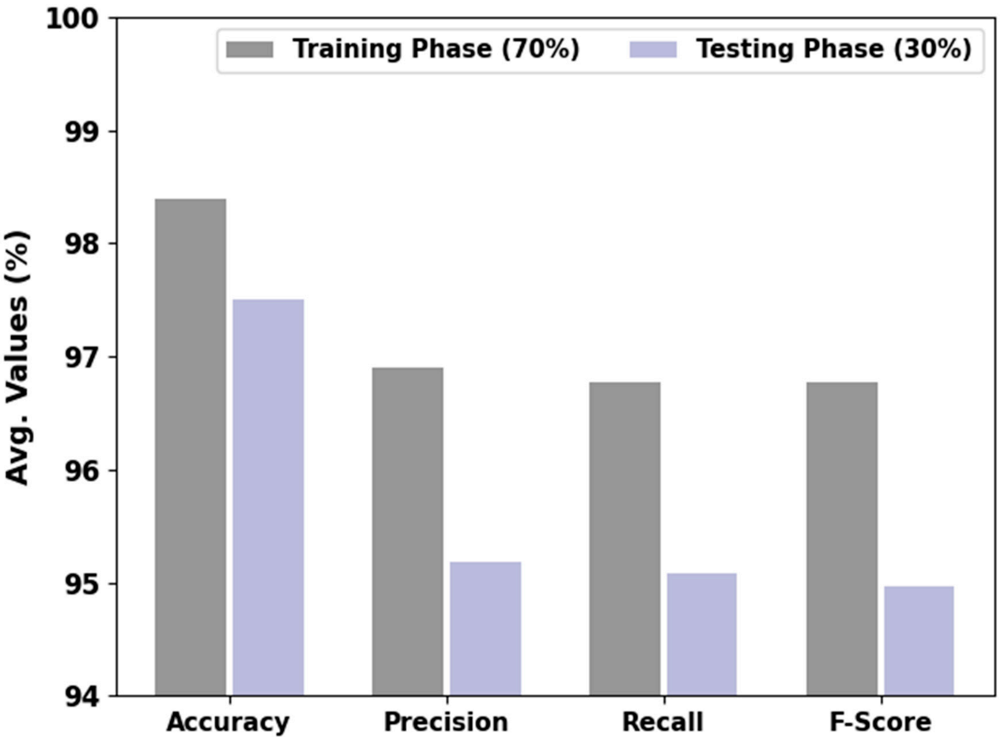

Figure 8. Average outcomes of the proposed BSBE-PPODLC approach on 70:30 on TR/TS datasets.

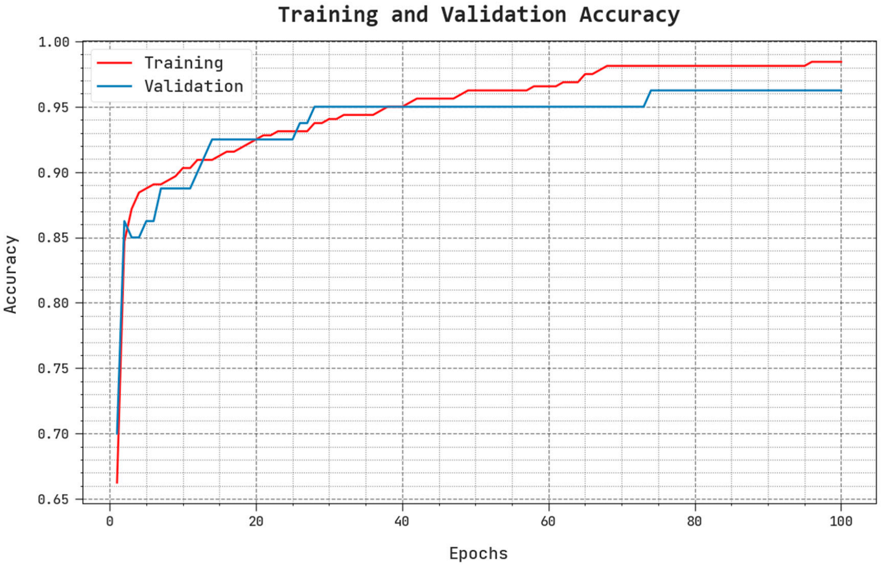

Figure 9. TACC and VACC outcomes of the BSBE-PPODLC approach.

The TLS and VLS performance results of the BSBE-PPODLC techniques are portrayed in Figure 10. The figure shows that the BSBE-PPODLC method had a better performance with the least TLS and VLS values. Seemingly, the proposed BSBE-PPODLC method achieved low VLS outcomes.

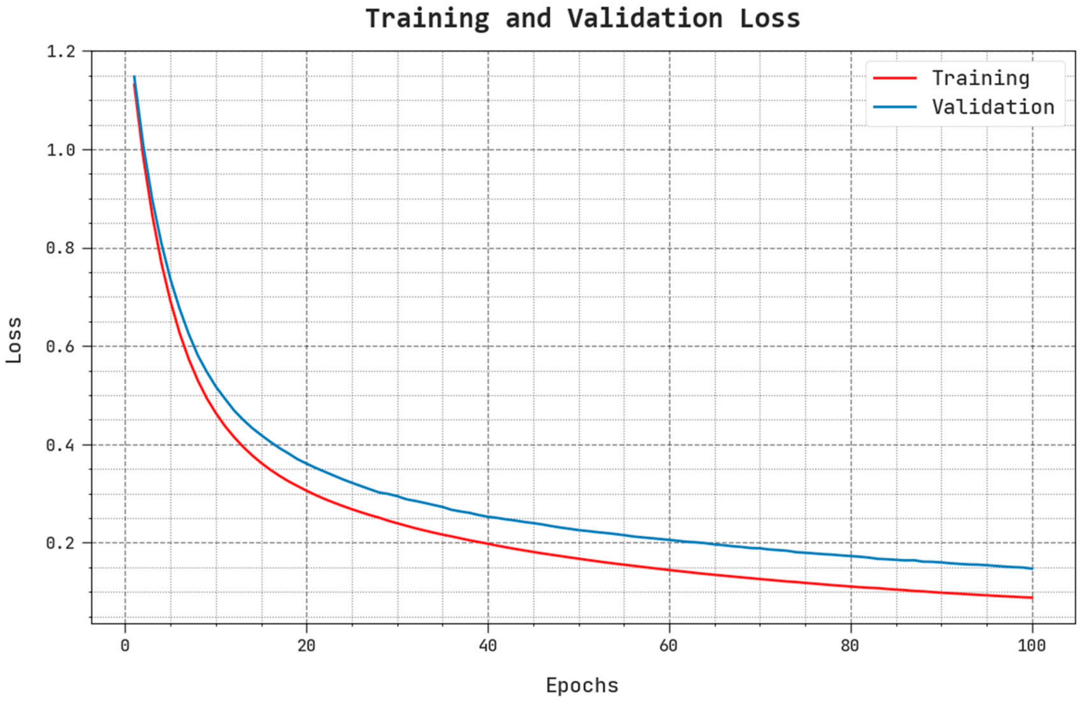

Figure 10. TLS and VLS outcomes of the BSBE-PPODLC approach.

A clear precision–recall study was conducted upon the proposed BSBE-PPODLC method under the test database and the results are shown in Figure 11. The figure shows that the proposed BSBE-PPODLC technique achieved enhanced precision–recall values under several classes.

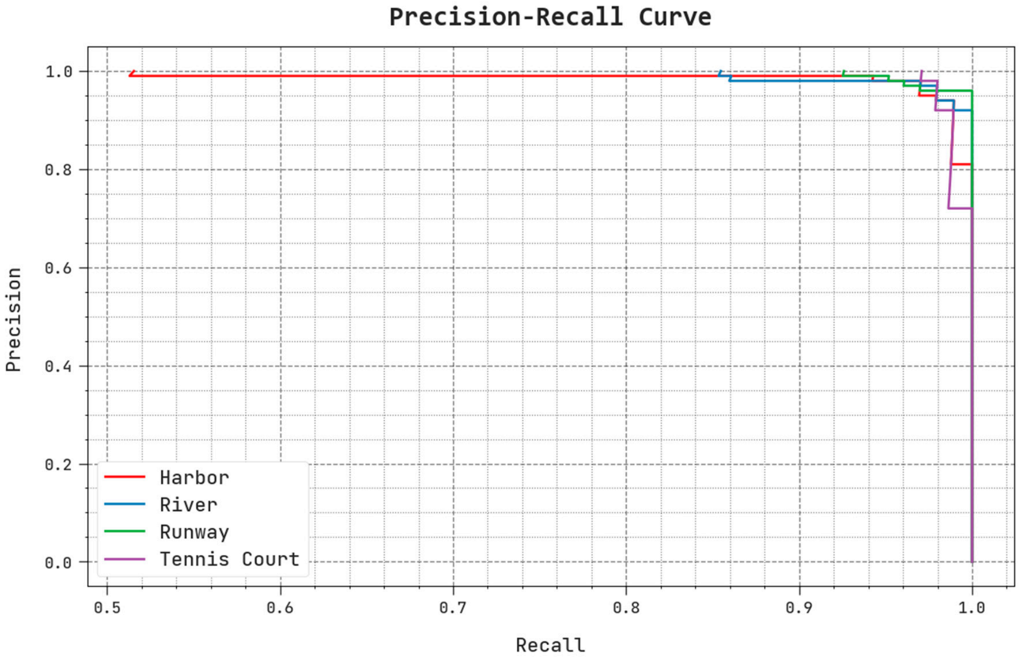

Figure 11. Precision–recall outcomes of the BSBE-PPODLC approach.

A comprehensive ROC study was conducted upon the BSBE-PPODLC technique with the test database and the results are detailed in Figure 12. The fallouts exhibited from the BSBE-PPODLC method established its ability in categorizing the test database into different classes.

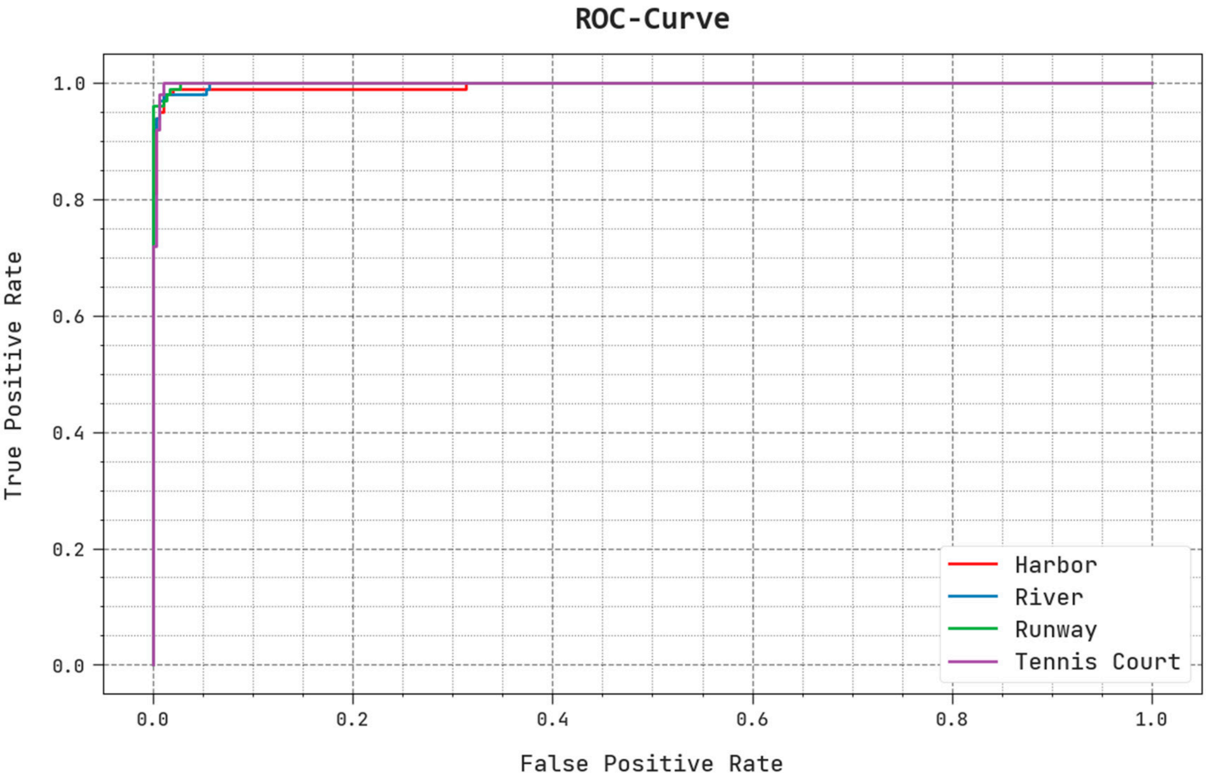

Figure 12. ROC outcomes of the BSBE-PPODLC approach.

In Table 6 and Figure 13, the RSI classification performance of the BSBE-PPODLC model and other DL models are portrayed [31,32]. The outcomes show that the ResNet50 and the DenseNet models offered the least classification performance. Next, the VGG16 and the Xception models reached moderately closer performance.

Table 6. Comparative analysis results of the BSBE-PPODLC approach and other systems.

Methods	Accuracy	Precision	Recall	F-Score
BSBE-PPODLC	99.06	98.18	98.09	98.10
VGG16	97.46	95.01	96.40	94.77
Xception	97.21	95.12	94.26	92.59
ResNet50	94.51	95.46	93.76	94.94
DenseNet121	94.18	93.82	94.88	94.36
PP-DL Model	98.40	97.20	97.11	96.48

In contrast, the PP-DL method achieved a reasonable performance with an $accu_y$ of 98.40%, $prec_n$ of 97.20%, $reca_l$ of 97.11% and an F_{score} of 96.48%. However, the proposed BSBE-PPODLC model exhibited its supremacy with an $accu_y$ of 99.06%, $prec_n$ of 98.18%, $reca_l$ of 98.09% and an F_{score} of 98.10%. These results confirmed the better performance of the proposed BSBE-PPODLC method over other DL approaches

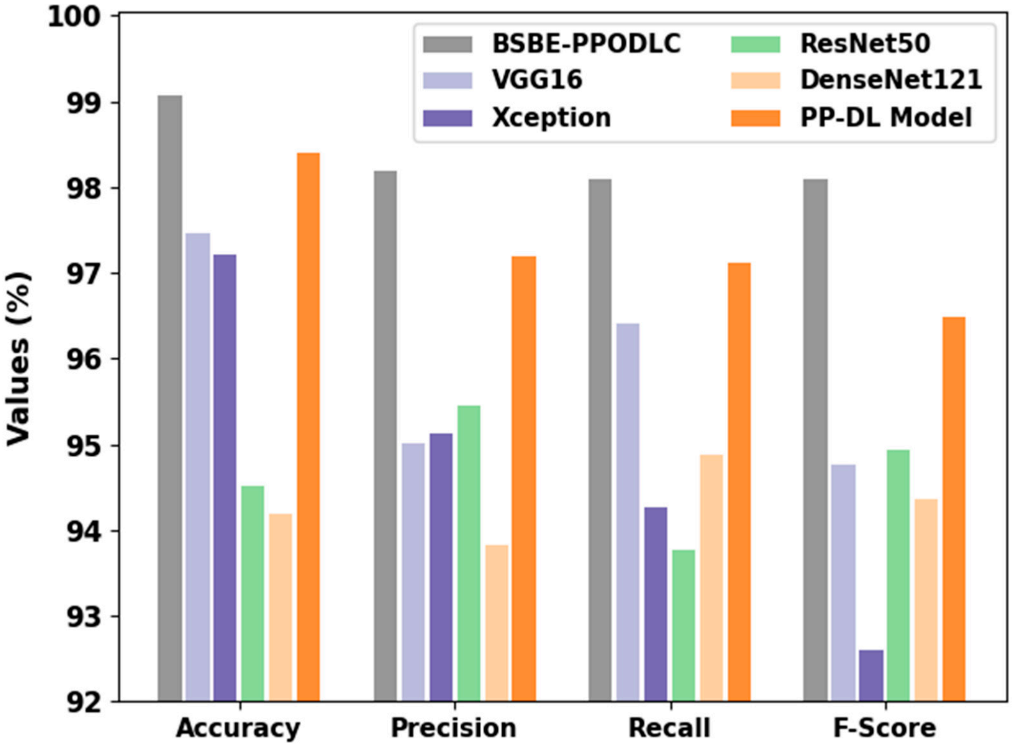

Figure 13. Comparative analysis outcomes of the BSBE-PPODLC approach and other systems.

4. Conclusions

The current research paper introduced an effective BSBE-PPODLC technique for encryption and classification of RSIs. The presented BSBE-PPODLC technique initially encrypts the RSIs using the BSBE technique, which enables secure communication of the images in a wireless medium. During the receipt process, both decryption and the image classification processes occur. In the presented BSBE-PPODLC technique, the image classification process encompassed three sub-processes, namely DenseNet feature extraction, XGBoost classifier and AGTO-based hyperparameter tuning. The simulation values of the BSBE-PPODLC approach were tested on the RSI dataset and the outcomes were assessed under different aspects. The simulation outcomes confirmed that the BSBE-PPODLC technique reached an improved performance over other models with a maximum accuracy of 99.06%. In future, the RSIs can be integrated into other kinds of data, such as LiDAR (light detection and ranging) or radar data, to enhance the image classification performance. In addition, the DL models can also use additional data sources in the classification process. Moreover, future works can focus on developing methods that make DL models highly interpretable. This phenomenon would be highly beneficial for applications in which it is important to understand the reasoning behind the model's decisions.

Author Contributions: Conceptualization, F.S.A. and A.M.; Methodology A.A.A.; Software, A.M.; Investigation, A.A.A.; Resources, A.M.; Data curation, A.M.; Writing—original draft, F.S.A., A.A.A. and A.M.H.; Writing—review & editing, A.A.A., A.M. and A.M.H.; Supervision, A.A.A.; Project administration, A.M.H.; Funding acquisition, F.S.A. All authors have read and agreed to the published version of the manuscript.

Funding: The authors extend their appreciation to the Deputyship for Research & Innovation, Ministry of Education in Saudi Arabia for funding this research work through the project number MoE-IF-UJ-R-22-0708-1.

Conflicts of Interest: The authors declare that they have no conflict of interest. The manuscript was written through the contributions of all authors. All authors have given approval for the final version of the manuscript.

References

1. Chouragade, P.M.; Ambhore, P.B. A Survey on Privacy Preserving Content Based Image Retrieval and Information Sharing in Cloud Environment. In Proceedings of the 2021 4th International Conference on Recent Trends in Computer Science and Technology (ICRTCST), Jamshedpur, India, 1–12 February 2022; IEEE: New York, NY, USA; pp. 238–245. [CrossRef]
2. Saravanan, K.; Suganthi, K.; Kalaiselvi, R.; Divya, B.; Kumar, S.D. Privacy Preserving On Remote Sensing Data Using Reversible Data Hiding. *J. Phys. Conf. Ser.* **2021**, *1979*, 012050. [CrossRef]
3. Yang, J.; Cheng, G.; Shen, M. Secure fusion of encrypted RSI based on Brovey. *Sci. China Inf. Sci.* **2021**, *64*, 1–3. [CrossRef]
4. Boulemtafes, A.; Derhab, A.; Braham, N.A.A.; Challal, Y. PReDIHERO–Privacy-Preserving Remote Deep Learning Inference based on Homomorphic Encryption and Reversible Obfuscation for Enhanced Client-side Overhead in Pervasive Health Monitoring. In Proceedings of the 2021 IEEE/ACS 18th International Conference on Computer Systems and Applications (AICCSA), Tangier, Morocco, 30 November–3 December 2021; IEEE: New York, NY, USA; pp. 1–8. [CrossRef]
5. Rajput, A.S.; Raman, B.; Imran, J. Privacy-preserving human action recognition as a remote cloud service using RGB-D sensors and deep CNN. *Expert Syst. Appl.* **2020**, *152*, 113349. [CrossRef]
6. Hasan, M.M.; Islam, M.U.; Sadeq, M.J.; Fung, W.K.; Uddin, J. Review on the Evaluation and Development of Artificial Intelligence for COVID-19 Containment. *Sensors* **2023**, *23*, 527. [CrossRef] [PubMed]
7. Xie, D.; Chen, F.; Luo, Y.; Li, L. One-to-many image encryption with privacy-preserving homomorphic outsourced decryption based on compressed sensing. *Digit. Signal Process.* **2019**, *95*, 102587. [CrossRef]
8. Du, G.; Zhou, L.; Li, Z.; Wang, L.; Lü, K. Neighbor-aware deep multi-view clustering via graph convolutional network. *Inf. Fusion* **2023**, *93*, 330–343. [CrossRef]
9. Sirisha, U.; Chandana, B.S. Privacy Preserving Image Encryption with Optimal Deep Transfer Learning Based Accident Severity Classification Model. *Sensors* **2023**, *23*, 519. [CrossRef] [PubMed]
10. Li, S.; Wu, L.; Meng, W.; Xu, Z.; Qin, C.; Wang, H. DVPPIR: Privacy-preserving image retrieval based on DCNN and VHE. *Neural Comput. Appl.* **2022**, *34*, 14355–14371. [CrossRef]
11. Jayaram, R.; Prabakaran, S. Onboard disease prediction and rehabilitation monitoring on secure edge-cloud integrated privacy preserving healthcare system. *Egypt. Inform. J.* **2021**, *22*, 401–410. [CrossRef]
12. Zhang, Z.; Zhou, F.; Qin, S.; Jia, Q.; Xu, Z. Privacy-Preserving Image Retrieval and Sharing in Social Multimedia Applications. *IEEE Access* **2020**, *8*, 66828–66838. [CrossRef]
13. Wang, X.; Li, J.; Yan, H. An improved anti-quantum MST3 public key encryption scheme for RSI. *Enterp. Inf. Syst.* **2021**, *15*, 530–544. [CrossRef]
14. Lee, T.; Lin, Z.; Pushp, S.; Li, C.; Liu, Y.; Lee, Y.; Xu, F.; Xu, C.; Zhang, L.; Song, J. Occlumency: Privacy-preserving remote deep-learning inference using SGX. In Proceedings of the 25th Annual International Conference on Mobile Computing and Networking, Los Cabos, Mexico, 21–25 October 2019; pp. 1–17.
15. Janani, T.; Brindha, M. Secure Similar Image Matching (SESIM): An Improved Privacy Preserving Image Retrieval Protocol over Encrypted Cloud Database. *IEEE Trans. Multimed.* **2021**, *24*, 3794–3806. [CrossRef]
16. Al-Khasawneh, M.A.; Uddin, I.; Shah, S.A.A.; Khasawneh, A.M.; Abualigah, L.; Mahmoud, M. An improved chaotic image encryption algorithm using Hadoop-based MapReduce framework for massive remote sensed images in parallel IoT applications. *Clust. Comput.* **2022**, *25*, 999–1013. [CrossRef]
17. Zhang, X.; Wang, Y.; Ma, J.; Jin, Q. QAPP: A quality-aware and privacy-preserving medical image release scheme. *Inf. Fusion* **2022**, *88*, 281–295. [CrossRef]
18. Falmari, V.R.; Brindha, M. Privacy preserving biometric authentication using chaos on remote untrusted server. *Measurement* **2021**, *177*, 109257. [CrossRef]
19. Abd EL-Latif, A.A.; Abd-El-Atty, B.; Abou-Nassar, E.M.; Venegas-Andraca, S.E. Controlled alternate quantum walks based privacy preserving healthcare images in internet of things. *Opt. Laser Technol.* **2020**, *124*, 105942. [CrossRef]
20. Zhao, Q.; Chen, S.; Liu, Z.; Baker, T.; Zhang, Y. Blockchain-based privacy-preserving remote data integrity checking scheme for IoT information systems. *Inf. Process. Manag.* **2020**, *57*, 102355. [CrossRef]
21. Qin, J.; Chen, J.; Xiang, X.; Tan, Y.; Ma, W.; Wang, J. A privacy-preserving image retrieval method based on deep learning and adaptive weighted fusion. *J. Real-Time Image Process.* **2019**, *17*, 161–173. [CrossRef]
22. Rangwani, D.; Sadhukhan, D.; Ray, S.; Khan, M.K.; Dasgupta, M. An improved privacy preserving remote user authentication scheme for agricultural wireless sensor network. *Trans. Emerg. Telecommun. Technol.* **2021**, *32*, e4218. [CrossRef]
23. Yang, Y.; Newsam, S. Bag-of-visual-words and spatial extensions for land-use classification. In Proceedings of the 18th SIGSPATIAL International Conference on Advances in Geographic Information Systems, San Jose, CA, USA, 2–5 November 2010; pp. 270–279.
24. Dutta, S.; Das, M. Remote sensing scene classification under scarcity of labelled samples—A survey of the state-of-the-arts. *Comput. Geosci.* **2023**, *171*, 105295. [CrossRef]
25. Zhou, W.; Guan, H.; Li, Z.; Shao, Z.; Delavar, M.R. Remote Sensing Image Retrieval in the Past Decade: Achievements, Challenges, and Future Directions. *IEEE J. Sel. Top. Appl. Earth Obs. Remote Sens.* **2023**, *16*, 1447–1473. [CrossRef]
26. Zhu, Y.; Wang, M.; Yin, X.; Zhang, J.; Meijering, E.; Hu, J. Deep Learning in Diverse Intelligent Sensor Based Systems. *Sensors* **2023**, *23*, 62. [CrossRef] [PubMed]

27. Chuman, T.; Sirichotedumrong, W.; Kiya, H. Encryption-Then-Compression Systems Using Grayscale-Based Image Encryption for JPEG Images. *IEEE Trans. Inf. Forensics Secur.* **2018**, *14*, 1515–1525. [CrossRef]
28. Nalluri, S.; Sasikala, R. A deep neural architecture for SOTA pneumonia detection from chest X-rays. *Int. J. Syst. Assur. Eng. Manag.* **2022**, 1–14. [CrossRef]
29. Alsolai, H.; Alzahrani, J.S.; Maray, M.; Alghamdi, M.; Qahmash, A.; Alnfiai, M.M.; Aziz, A.S.A.; Mustafa Hilal, A. Enhanced Artificial Gorilla Troops Optimizer Based Clustering Protocol for UAV-Assisted Intelligent Vehicular Network. *Drones* **2022**, *6*, 358. [CrossRef]
30. Li, S.; Qin, J.; He, M.; Paoli, R. Fast Evaluation of Aircraft Icing Severity Using Machine Learning Based on XGBoost. *Aerospace* **2020**, *7*, 36. [CrossRef]
31. Minu, M.S.; Canessane, R.A. An Efficient Squirrel Search Algorithm based Vector Quantization for Image Compression in Unmanned Aerial Vehicles. In Proceedings of the 2021 International Conference on Artificial Intelligence and Smart Systems (ICAIS), Coimbatore, India, 25–27 March 2021; IEEE: New York, NY, USA; pp. 789–793. [CrossRef]
32. Alkhelaiwi, M.; Boulila, W.; Ahmad, J.; Koubaa, A.; Driss, M. An Efficient Approach Based on Privacy-Preserving Deep Learning for Satellite Image Classification. *Remote Sens.* **2021**, *13*, 2221. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.