drones

MDPI

Article

Artificial Intelligence-Based Secure Communication and Classification for Drone-Enabled Emergency Monitoring Systems

Fatma S. Alrayes [1], Saud S. Alotaibi [2], Khalid A. Alissa [3], Mashael Maashi [4], Areej Alhogail [5], Najm Alotaibi [6], Heba Mohsen [7] and Abdelwahed Motwakel [8,*]

[1] Department of Information Systems, College of Computer and Information Sciences, Princess Nourah Bint Abdulrahman University, P.O. Box 84428, Riyadh 11671, Saudi Arabia
[2] Department of Information Systems, College of Computing and Information System, Umm Al-Qura University, P.O. Box 715, Mecca 24381, Saudi Arabia
[3] Networks and Communications Department, College of Computer Science and Information Technology, Imam Abdulrahman Bin Faisal University, P.O. Box 1982, Dammam 31441, Saudi Arabia
[4] Department of Software Engineering, College of Computer and Information Sciences, King Saud University, P.O. Box 103786, Riyadh 11543, Saudi Arabia
[5] Department of Information Systems, College of Computer and Information Sciences, King Saud University, P.O. Box 103786, Riyadh 11543, Saudi Arabia
[6] Prince Saud AlFaisal Institute for Diplomatic Studies, P.O. Box 51988, Riyadh 11553, Saudi Arabia
[7] Department of Computer Science, Faculty of Computers and Information Technology, Future University in Egypt, New Cairo 11835, Egypt
[8] Department of Computer and Self Development, Preparatory Year Deanship, Prince Sattam bin Abdulaziz University, Alkharj 16278, Saudi Arabia
* Correspondence: a.ismaeil@psau.edu.sa

check for updates

Citation: Alrayes, F.S.; Alotaibi, S.S.; Alissa, K.A.; Maashi, M.; Alhogail, A.; Alotaibi, N.; Mohsen, H.; Motwakel, A. Artificial Intelligence-Based Secure Communication and Classification for Drone-Enabled Emergency Monitoring Systems. *Drones* **2022**, *6*, 222. https://doi.org/10.3390/drones6090222

Academic Editors: Alessandro Giuseppi, Francesco Liberati and Vishal Sharma

Received: 16 July 2022
Accepted: 19 August 2022
Published: 26 August 2022

Abstract: Unmanned Aerial Vehicles (UAVs), or drones, provided with camera sensors enable improved situational awareness of several emergency responses and disaster management applications, as they can function from remote and complex accessing regions. The UAVs can be utilized for several application areas which can hold sensitive data, which necessitates secure processing using image encryption approaches. At the same time, UAVs can be embedded in the latest technologies and deep learning (DL) models for disaster monitoring areas such as floods, collapsed buildings, or fires for faster mitigation of its impacts on the environment and human population. This study develops an Artificial Intelligence-based Secure Communication and Classification for Drone-Enabled Emergency Monitoring Systems (AISCC-DE2MS). The proposed AISCC-DE2MS technique majorly employs encryption and classification models for emergency disaster monitoring situations. The AISCC-DE2MS model follows a two-stage process: encryption and image classification. At the initial stage, the AISCC-DE2MS model employs an artificial gorilla troops optimizer (AGTO) algorithm with an ECC-Based ElGamal Encryption technique to accomplish security. For emergency situation classification, the AISCC-DE2MS model encompasses a densely connected network (DenseNet) feature extraction, penguin search optimization (PESO) based hyperparameter tuning, and long short-term memory (LSTM)-based classification. The design of the AGTO-based optimal key generation and PESO-based hyperparameter tuning demonstrate the novelty of our work. The simulation analysis of the AISCC-DE2MS model is tested using the AIDER dataset and the results demonstrate the improved performance of the AISCC-DE2MS model in terms of different measures.

Keywords: security; image encryption; emergency monitoring system; drones; data classification; deep learning

1. Introduction

Aerial images captured by unmanned aerial vehicles (UAVs) are used for several applications such as urban planning, real-estate management, disaster evaluation, traffic congestion management, road network detection, vehicle detection, etc. [1]. Analyzing aerial images can be useful for pattern recognition and the decision-making process. Recent advances in machine learning (ML) and deep learning (DL) can be used to extract meaningful data from aerial images. At the same time, Traditional ML methods involve functions such as feature selection and extraction. Feature selection and extraction layers were manual processes in traditional ML, and such layer necessities were automated in ML algorithms related to DL [2,3]. The automation of such layers is regarded as a benefit of DL networks, but it also has the drawback that DL networks necessitate more training datasets. The commonly utilized technique in DL-related image classifiers studies is the convolutional neural network (CNN). CNN with DL-related networks is a hastily emerging technology and is becoming a more extensive approach for image data-type classifiers studies [4]. The renowned image classifications competition in recent years is the IMAGENET large-scale visual recognition challenge (ILSVRC). The highest-ranked participants employed CNN-related approaches in ILSVRC. CNN networks have two core structures: the pooling and convolution layers [5,6]. The convolution layer contains feature maps that are connected to each other and a series of weights, and connect to functions such as a rectified linear unit (RELU).

Generally, a UAV has an LTE or Wi-Fi communication device, flight control computers, and mission computers for sending and receiving drone data to the drone operating system or ground control station [7]. On the other hand, the aerial images hold useful data relevant to confidential sites which need secure processing. It is of utmost importance to assure the security of transmission and processing of images acquired by aerial photography technologies as these images may contain crucial data concerning national security. Image encryption is a major and effective means to protect the security of image information [8]. In simple terms, drones without security operations are utilized for criminal acts such as information theft, safety threats, invasion of privacy, and security threats. For prevention of such cybersecurity susceptibilities, special purpose drones deployed by military drones or state agencies for attack purposes, surveillance, and reconnaissance require data encrypting technology for protecting not just transmission data but also delicate data stored in the drone [9,10].

The encryption process can be executed by every device within the UAV depending on the data type that needs encryption [11]. Flight control or communication data encryption can be processed in the flight control mechanism, and transmission data encrypting for the mission can be processed in the mission computers. Particularly, the drone has an encrypting operation in the transmission device, permitting all transmission data to be encrypted irrespective of data types [12]. In the case of drone data encryption, there exists a technique of applying encrypting software on particular devices of the drones or attachment of hardware modules that have an encrypting function in the device for managing encryption just as in hardware modules. The software encrypting technique is based on hardware characteristics and the operating system of the mission-and-flight control computer. Moreover, many drone producers offer data encryption in a simple method by not altering the source code of prevailing drone flight control systems [13].

This study develops an Artificial Intelligence-based Secure Communication and Classification for Drones Enabled Emergency Monitoring Systems (AISCC-DE2MS). The proposed AISCC-DE2MS technique applies an artificial gorilla troops optimizer (AGTO) algorithm with an ECC-Based ElGamal Encryption technique to assure security. For emergency situation classification, the AISCC-DE2MS model encompasses densely connected network (DenseNet) feature extraction, penguin search optimization (PESO)-based hyperparameter tuning, and long short-term memory (LSTM)-based classification. The simulation analysis of the AISCC-DE2MS model is tested using the AIDER dataset.

2. Literature Review

Sarkar et al. [14] introduced a new Energy-aware Secure Internet of Drone (ESIoD) structure. A decisive research complexity tackled by this study is the way in which faster on-board processing can be accomplished and diminishes battery use for a drone for extending the flight duration while retaining data security of drone-captured images. In particular, UAV-captured realistic images were encoded by utilizing either RSA or AES techniques and offloaded by the on-board computers to a server to process cognitive activities, leveraging advanced faster R-CNN and standard Haar cascade classifiers. Ismael [15] modelled an authentication and security mechanism related to the stream cipher lightweight HIGHT method and chaotic maps. The presented mechanism is particularly projected with an aim to decrease the less and computational use of UAV resources, and handles one drone and one ground control station (GCS) with several fly sessions. In [16], the author indicates the drone map planner is a fog-related and service-oriented drone management mechanism that communicates, controls, and monitors drones across the network. Such a planner permits interaction with many UAVs on the internet that can be controlled anytime and anywhere without long-distance boundaries. The abovementioned planner offers access to fog computing sources for UAVs to heavy load computation.

Bera et al. [17] devised a new access control technique for unauthorized drone detection and mitigation in an IoD environment, named ACSUD-IoD. By using the blockchain (BC)-related solution inculcates in ACSUD-IoD, the transaction data with the abnormal data for detecting unlicensed drones by the GSS were saved in a private BC, which are genuine and normal secure data from drones to the Ground Station Server (GSS). Ajmal [18] presents an enhanced version of HEVC for encryption of multimedia data based on motion and texture energy estimation. For every frame of the video, the quantized and transformed coefficients were computed along with motion vectors. In the presented method, the energy can be computed for every block, and a comparison is made for threshold values in selecting the suitable encrypting method. Here, the author has employed the Advanced Encryption Standard (AES) as an encrypting method and devised for encrypting the most significant bits (MSB) as most of the data exist in MSB.

Zhang et al. [19] propose a lightweight AKA method where there were only bitwise XOR operations and secure one-way hash functions when users and drones jointly authenticate one another. The presented method could reach AKA-security in the random oracle method and endure several renowned assaults. At the same time, the security comparison validates this presented method and offers security in a better way. Khan et al. [20] designed an identity-related proxy signcryption method for addressing such complexities. At the time of data transfer among UAVs and to cloud servers, the devised method supports member revocation and outsourcing decryption. The projected technique depends upon the notion of Hyper-Elliptic-Curve-Cryptography (HECC) that enhances the efficiency of network computations. The author employs the Random Oracle Model (ROM) along with formal security analysis for assessing security toughness. Though several methods have been available in the literature, it is still needed to develop effective models for drone communication security and classification. Besides, the hyperparameter tuning of the DL models is not taken into account in the existing models, which needs to be addressed. Therefore, this work makes use of the PESO algorithm for the hyperparameter tuning of the DenseNet model.

3. Materials and Methods

In this study, a new AISCC-DE2MS technique has been developed for secure communication and classification of drone-based emergency monitoring systems. The proposed AISCC-DE2MS technique performed image encryption at the preliminary stage using the AGTO algorithm with an ECC-Based ElGamal Encryption technique in which the optimal key generation procedure takes place via the AGTO algorithm. To classify the images, the AISCC-DE2MS model encompasses DenseNet feature extraction, PESO-based hyperparameter tuning, and LSTM-based classification. Figure 1 depicts the block diagram of the AISCC-DE2MS approach.

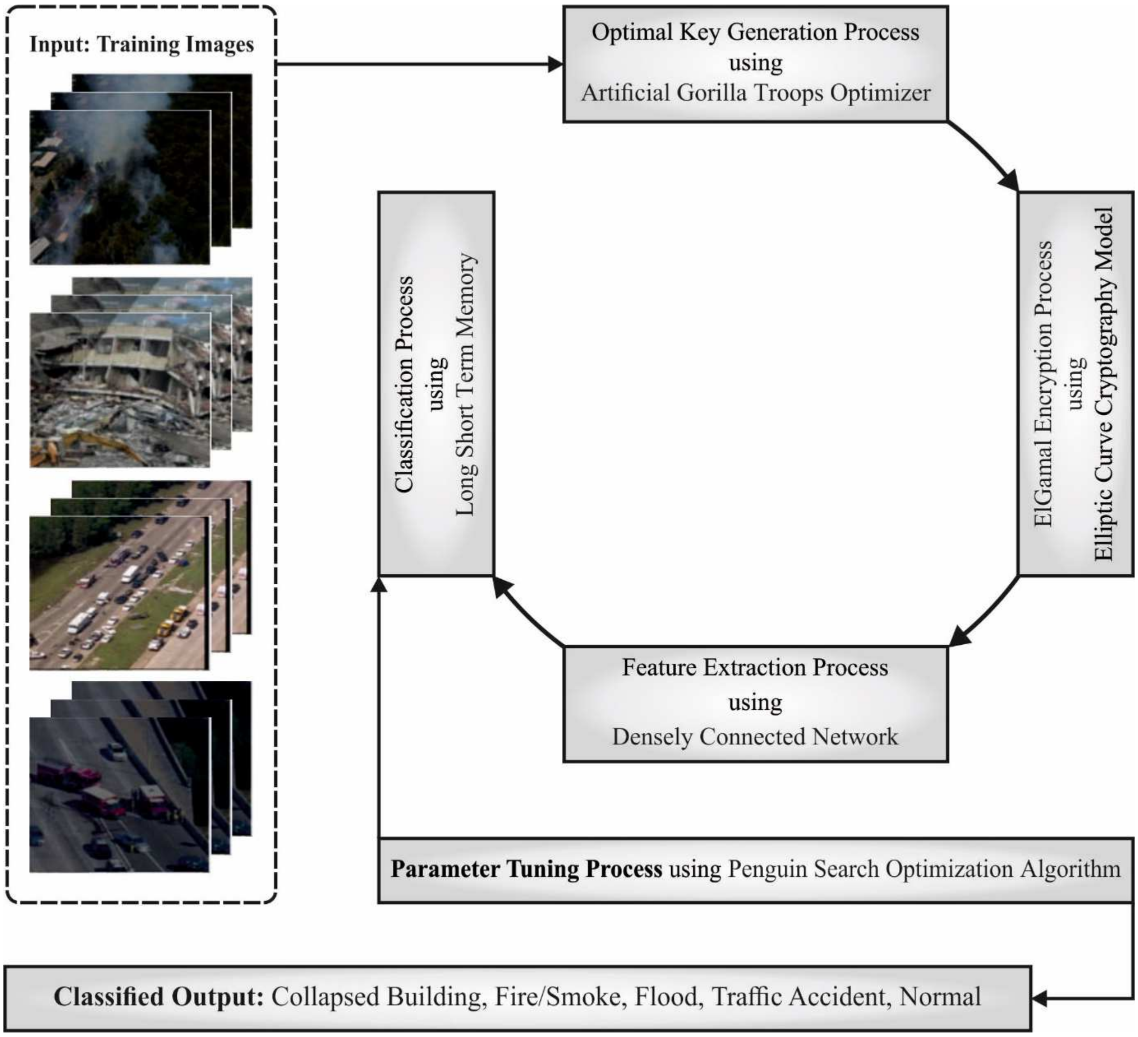

Input: Training Images
Optimal Key Generation Process using Artificial Gorilla Troops Optimizer
ElGamal Encryption Process using Elliptic Curve Cryptography Model
Feature Extraction Process using Densely Connected Network
Classification Process using Long Short Term Memory
Parameter Tuning Process using Penguin Search Optimization Algorithm
Classified Output: Collapsed Building, Fire/Smoke, Flood, Traffic Accident, Normal

Figure 1. Block diagram of AISCC-DE2MS approach.

3.1. Data Used

In this work, the experimental validation of the AISCC-DE2MS model is tested using the AIDER dataset [21]. The aerial images for disaster events are gathered from several online sources (for instance, news agencies, YouTube, Google images, web sites, bing images, and so on) utilizing the keywords “UAV” or “Drone” or “Aerial View” and events such as “Earthquake”, “Highway accident”, “Fire”, and so on. Images were primarily of distinct sizes compared to the standardized ones prior to training. Every image examined primarily comprises the events concerned. Next, the event was centered in the image so that some geometric transformations in augmentation could not eliminate it in the image view. In the data gathering method, several disaster events with distinct resolutions are taken, and in several conditions, in terms of viewpoint and illumination. In this study, a total of 8540 images under five classes are used for experimentation. Table 1 provides a detailed description of the dataset.

Table 1. Dataset details.

Class	Description	No. of Samples
C-1	Collapsed Building/Rubble	700
C-2	Fire/Smoke	740
C-3	Flood	700
C-4	Traffic Accidents	700
C-5	Normal	5700
Total No. of Samples		**8540**

3.2. Image Encryption Suing AGTO-ElGamal Technique

In this study, the AISCC-DE2MS technique makes use of AGTO with the ECC-based ElGamal encryption technique to accomplish security. The ECC-based ElGamal encryption with several parameters and steps utilized are given as follows [22].

The additive homomorphic approach grasps by succeeding Equation (1),

$$E(m_1) + E(m_2) = E(m_1 + m_2) \tag{1}$$

whereas + symbol is intended for the additive homomorphic and the public key is E. InECC, additive homomorphic encryption can be assumed. According to the elliptic curve's (ECs) algebraic infrastructure on finite domains, ECC-based ElGamal was explained. The finite fields were separated into two types such as prime and binary fields 2_n. During this current analysis, ECs over prime fields were examined. The special class of EC demonstrated in Equation (2) was utilized in EC over real numbers as

$$y^2 = x^3 + ax + b \tag{2}$$

$E_r(a,\ b)$ refers to the resultant curve where modulus is r, and the altered co-efficient of formula assumed a and b. The value of x ranges from 0 to r but not on every point on the curve. Even with lesser bit size, the ECC also projected a similar security level by processing an overhead decrease when compared to homomorphic and RSA techniques. For the optimal key generation process, the AGTO algorithm is used in this study.

The AGTO approach consists of exploitation and exploration phases [23]. Equations (3)–(13) describe the major concept of the presented model. The exploration phase is used primarily to implement a global search for space. It makes use of three major models such as moving to the position of other gorillas, migrating to an unknown position, and migrating to a known position. The exploitation phase can be expressed in the following:

$$GX(t+1) = \begin{cases} (ub - lb) \times r_1 + lb, & r < p, \\ (r_2 - C) \times X_r(t) + L \times H, & r \geq 0.5, \\ X(i) - L \times (L \times (X(t) - GX_r(t)) + r_3 \times (X(t) - GX_r(t))), & r < 0.5. \end{cases} \tag{3}$$

Here, $X(t)$ is the gorilla's existing location, and $GX(t+1)$ represents the gorilla's location in the $t+1$ iteration. p defines a variable among [0, 1] that defines the migration method to be selected. lb and ub refer to the lower and upper limits, correspondingly. X_r stands for a randomly designated gorilla member from the population and GX_r denotes the randomly chosen gorilla candidate location vector. r_1, r_2, r_3, and r show the random value within [0, 1] upgraded on all the iterations. Furthermore, C, L, and H are evaluated as follows:

$$C = F \times \left(1 - \frac{It}{\text{Max } It}\right), \tag{4}$$

$$F = cos(2 \times r_4) + 1, \tag{5}$$

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

$$H = Z \times X(t), \tag{7}$$

$$Z = [-C,\ C]. \tag{8}$$

From the expression, It stands for the existing iteration count and Max It refers to the overall iteration amount. In Equations (5) and (6), r_4 and l denotes random values among [0, 1] upgraded on all the iterations. In Equation (8), Z shows the random number that lies within $-C$ to C. Eventually, in the exploration stage, the algorithm evaluates the fitness value of each GX solution, and the fitness value is $GX(t) < X(t)$, and the $X(t)$ solution is substituted with the $GX(t)$ solution.

The exploitation stage of AGTO makes use of two strategies, competing for adult female gorillas and following silverback gorillas. The approach is chosen by comparing the C value with the variable W set. When $C \geq W$, the AGTO exploits the following silverback gorilla strategy; when $C < W$, competing for adult female gorillas is preferred. Following the silverback gorilla is formulated as follows:

$$GX(t+1) = L \times M \times (X(t) - X_{silverback}) + X(t), \tag{9}$$

$$M = \left(\left|\frac{1}{N}\sum_{i=1}^{N} GX_i(t)\right|^{g}\right)^{\frac{1}{g}}, \tag{10}$$

$$g = 2^{L}. \tag{11}$$

In Equation (9), $X_{silverback}$ denotes the silverback gorilla location. In Equation (10), $GX_i(t)$ indicates the location of every candidate gorilla in the t iteration and N refers to the overall amount of gorillas. Competition with adult female gorillas is expressed below.

$$GX(i) = X_{silverback} - (X_{silverback} \times Q - X(t) \times Q) \times A, \tag{12}$$

$$Q = 2 \times r_5 - 1, \tag{13}$$

$$A = \beta \times E, \tag{14}$$

$$E = \begin{cases} N_1, & r \geq 0.5, \\ N_2, & r < 0.5. \end{cases} \tag{15}$$

In Equation (13), r_5 denotes a random value within [0, 1] upgraded on all the iterations. In Equation (14), β refers to a variable. In Equation (15), when rand ≥ 0.5, E denotes a random number in the standard distribution and the dimension of the problem; when rand < 0.5, E indicates a random number selected from a standard distribution. Eventually, in the exploitation stage, the algorithm evaluates the fitness value of each GX solution. Where $GX(t) < X(t)$, then the $X(t)$ solution is substituted with the $GX(t)$ solution, and the optimum solution chosen in the whole population is considered as a silverback gorilla.

In this study, the AGTO algorithm derives a fitness function for the maximization of the PSNR value.

$$Fitness = max\ (PSNR) \tag{16}$$

3.3. Image Classification Model

In this study, the AISCC-DE2MS model performs image classification via three major processes such as DenseNet feature extraction, PESO-based hyperparameter tuning, and LSTM-based classification.

3.3.1. DenseNet Feature Extraction

DenseNet is a novel addition to the NN applied to visual object detection. DenseNet169 is a procedure of DenseNet [24,25]. DenseNet is intended for the implementation of an image classifier. DenseNet169 is higher than the remaining DenseNet. Generally, in DenseNet, each image has been trained. An ImageNet image database is trained using the methodology and tested and stored by loading that saved methodology instead of ImageNet. Now, the outcomes of the initial layer are attained and concatenated with the upcoming layer in DenseNet. DenseNet has demonstrated an ability to decrease the accuracy from a high level NN generated by gradient vanishing, whereas there exists a long path between the input and output layers and the information attained vanishes just prior to accomplishing its target. DenseNet is a kind of typical network. According to the novel statistics, a convolutional layer is accurate and more effective once it is short and connected amongst layers such as input and closer output. Now, DenseNet was applied to connect each layer in feedforward manner. Usually, a traditional convolutional network contains L layers. Furthermore, L linking exists amongst the L layer. That characterizes one link amongst each layer and the subsequent layers.

It takes $L\ (L + 1)/2$ direct connections from the network. For each layer as input, each presiding layer is exploited. To input each subsequent layer, the FM is employed. Various advantages are attained from DenseNet. It reduces the gradient vanishing problem. The feature propagation is reinforced, feature reprocessing is stimulated, and it reduces the parameter number. The suggested method is evaluated on the highly competitive image detection benchmark ImageNet and also it uses the load and saved function. The incorporation of the layer was possible as described when there is whole similarity from the FM dimension during addition or concatenation. DenseNet is separated into DenseBlock with a dissimilar filter count, but within the block, the dimension is similar. Batch normalization (BN) was implemented with the help of down-sampling with transition layers and it is considered to be a crucial phase with CNN. As per the development of the channel dimension, the number amongst the DenseBlocks of filter variation, and growth rate can be denoted as K. It acts as a significant part of the generalizing I^{th} layer. Further, the data count is essential from each layer and has been evaluated as follows:

$$k_l = k_0 + k \times (l - 1) \tag{17}$$

3.3.2. Hyperparameter Tuning Using PESO Algorithm

For optimal tuning of the hyperparameters related to the DenseNet model, the PESO algorithm is exploited. A beneficial search activity of an animal is described as search activity from which the energy gain is moderately significant to that of the energy consumed [26]. For penguins, breathing ability remains a base factor while diving since the dive is based on reserve oxygen. The more they consume oxygen, the more depth and speed they gain, and the trip time begins to decrease. Food needed by a massive amount of groups differs by availability of food, species, and age within the area of concern. An optimization has been straightforwardly developed using the hunting strategy of penguins. To design the model, the penguin position within the area of concern is represented by "i". The distribution of the group is accomplished by the existence of food sources within the area of interest. Fundamental steps are established by employing these rules and are summarized as a pseudo-code demonstrated in Algorithm 1.

By considering the search space as a multi-dimension search space, the optimal solution is proposed by utilizing the food distribution probability to accomplish an optimum value and attain the maximal food quantity. Each member of a group utilizes a similar solution within the searching space. Generally, all the groups perform different dives on the basis of the probability of food expediency and the amount of reserve oxygen within the search space.

Penguins tends to switch essential data for determining an optimum solution and relocate the groups afterward carrying out multiple dives within the area of concern. The accomplishment of the global optimal without trapping in the local optimum after multiple iterations allows the PESO to implement better than traditional population-based techniques.

Algorithm 1: Penguin Search Optimization Algorithm (PESO)

```
Produce a random population of P penguins in groups
Initialize the probability of the existence of fish in the levels and holes
For i = 1 to the number of generations
    For every individual $i \in P$
    While oxygen reserves are not exhausted
    Take a random step
Enhance the penguin position using the location upgrade formula
Upgrade the quantity of fish eaten using this penguin
            End While
     End For
    Upgrade the quantity of eaten fish in the levels, holes, and best groups
    Reallocate the probability of penguins in the levels and holes
    Upgrade the optimal solution
End For
```

The PESO method makes a derivation of a fitness function (FF) that results in enhanced classifier performance. In this article, the reduction of the classifier error rate can be regarded as the FF, as presented in Equation (18).

$$fitness(x_i) = ClassifierErrorRate(x_i) = \frac{number\ of\ misclassified\ samples}{Total\ number\ of\ samples} \times 100 \tag{18}$$

3.3.3. LSTM Based Classification

Finally, the LSTM model is applied to allocate proper diverse class labels such as Collapsed Building, Fire/Smoke, Flood, Traffic Accident, and Normal. This is a gradient-based recurrent neural network structure that resolves the gradient disappearing problem. Long-term dependency in texts is a problem that advances at the training stage of a traditional RNN, whereas backpropagation through the time gradient descent tends to evaporate, or in rare situations, exponentially explode.

Figure 2 demonstrated the architecture of LSTM, and is capable of accurately managing long-term dependency in the text. Every LSTM is composed of forget, output, and input gates. Every gate is composed of pointwise multiplication operations and a sigmoid neural network layer. The input from the existing and hidden states of the preceding cell is first passed to the forget gate by utilizing X as an input vector at time t and N as a number of LSTM cells in the forward pass, to decide whether to discard it with an output of 0 or store the data with an output of 1 (Equation (19)). The main objective of the forget gate is to define either forget knowledge or not. The sigmoid function output (σ) of the product between the weights (W_f) and the sum of bias (b_f) and input $(h_{t-1},\ X_t)$ that encompasses the input from the preceding state (h_{t-1}) and the existing input (X_t) is the forget value (f_t) that lies within [0, 1].

$$f_t = \sigma(W_f \cdot [h_{t-1}, X_t] + b_f) \tag{19}$$

The next process is to exploit the update of cell state (C) based on Equation (20)

$$C_t = C_{t-1} \cdot f_t + N_t \cdot i_t \tag{20}$$

Let N_t be the output of the $\tan\text{h}$ function that exploits W_n, h_{t-1}, X_t, and b_n, expressed by

$$N_t = \tan\text{h}\ (W_n \cdot [h_{t-1},\ X_t] + b_n) \tag{21}$$

In Equation (21), i_t denotes the output of the sigmoid layer as follows:

$$i_t = \sigma(W_i \cdot [h_{t-1}, X_t] + b_i) \tag{22}$$

Then, the sigmoid activation output (O) is calculated by utilizing Equation (23) and based on bias (b_0), the existing input (X_t), prior state (h_{t-1}), and weights (W_0),

$$O_t = \sigma(W_0 \cdot [h_{t-1}, X_t] + b_0) \tag{23}$$

The next step is to upgrade the hidden state (h) by utilizing the below formula.

$$h_t = O_t \cdot \tan\text{h}\,(C_t) \tag{24}$$

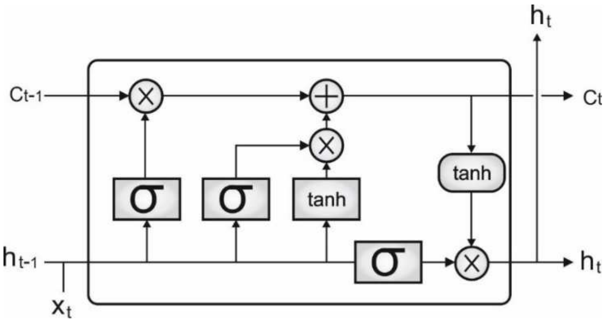


Figure 2. Framework of LSTM.

4. Results and Discussion

This section inspects the encryption and classification performance of the AISCC-DE2MS model [27]. A few sample images are demonstrated in Figure 3. The results are investigated in terms of mean square error (MSE), and peak signal-to-noise ratio (PSNR). It is defined as the ratio of the maximum possible value (power) of a signal and the power of distorting noise that influences the quality of its representation.

Figure 3. Sample images.

Table 2 offers a detailed encryption outcome of the AISCC-DE2MS model with other optimization algorithms. Figure 4 provides a comparative MSE examination of the AISCC-DE2MS model with other models. The experimental values inferred that the AISCC-DE2MS model gained minimal MSE values under all images. For instance, on image-1, the AISCC-DE2MS model obtained a lower MSE of 0.042, whereas the genetic algorithm (GA), crow search algorithm (CSA), and artificial bee colony (ABC) algorithms attained a higher MSE of 0.060, 0.120, and 0.165, respectively. Additionally, on image-2, the AISCC-DE2MS approach achieved a lesser MSE of 0.086 whereas the GA, CSA, and ABC algorithms gained a superior MSE of 0.096, 0.153, and 0.202 correspondingly. In line with, image-3, the AISCC-DE2MS approach reached a minimal MSE of 0.063, whereas the GA, CSA, and ABC systems attained a higher MSE of 0.078, 0.099, and 0.166, correspondingly.

Table 2. Encryption result analysis of AISCC-DE2MS approach with distinct images.

No. of Test Images	AISCC-DE2MS		Genetic Algorithm		Cat Swarm Algorithm		Artificial Bee Colony Algorithm	
	MSE	PSNR	MSE	PSNR	MSE	PSNR	MSE	PSNR
Image-1	0.042	61.898	0.060	60.349	0.120	57.339	0.165	55.956
Image-2	0.086	58.786	0.096	58.308	0.153	56.284	0.202	55.077
Image-3	0.063	60.137	0.078	59.210	0.099	58.174	0.166	55.930
Image-4	0.091	58.540	0.131	56.958	0.211	54.888	0.254	54.082
Image-5	0.101	58.088	0.142	56.608	0.219	54.726	0.244	54.257

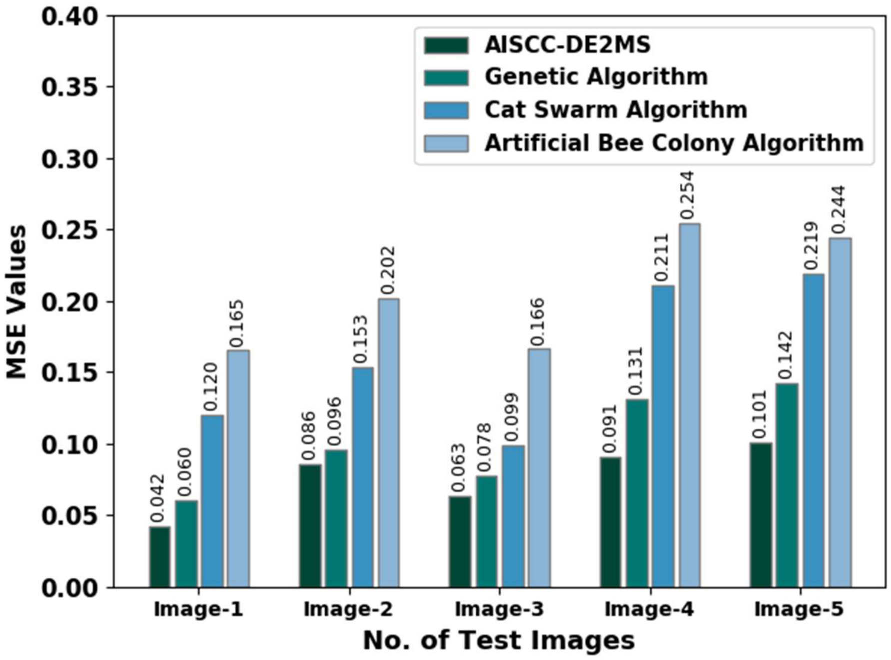


Figure 4. MSE analysis of AISCC-DE2MS approach with distinct images.

A comprehensive PSNR inspection of the AISCC-DE2MS model with recent models under diverse images is given in Figure 5. The results reported that the AISCC-DE2MS model showed improved values of PSNR under every image. For instance, on image-1, the AISCC-DE2MS model depicted a maximum PSNR of 61.898 dB, whereas the GA, CSA, and ABC algorithms exhibited a minimal PSNR of 60.349 dB, 57.339 dB, and 55.956 dB, respectively. Moreover, on image-2, the AISCC-DE2MS approach illustrated a maximal PSNR of 58.786 dB, whereas the GA, CSA, and ABC algorithms showcased a reduced PSNR of 58.308 dB, 56.2849 dB, and 55.077 dB, correspondingly. Eventually, in image-

3, the AISCC-DE2MS approach depicted a maximum PSNR of 60.137 dB, whereas the GA, CSA, and ABC systems outperformed the lower PSNR of 59.210 dB, 58.174 dB, and 55.930 dB, correspondingly.

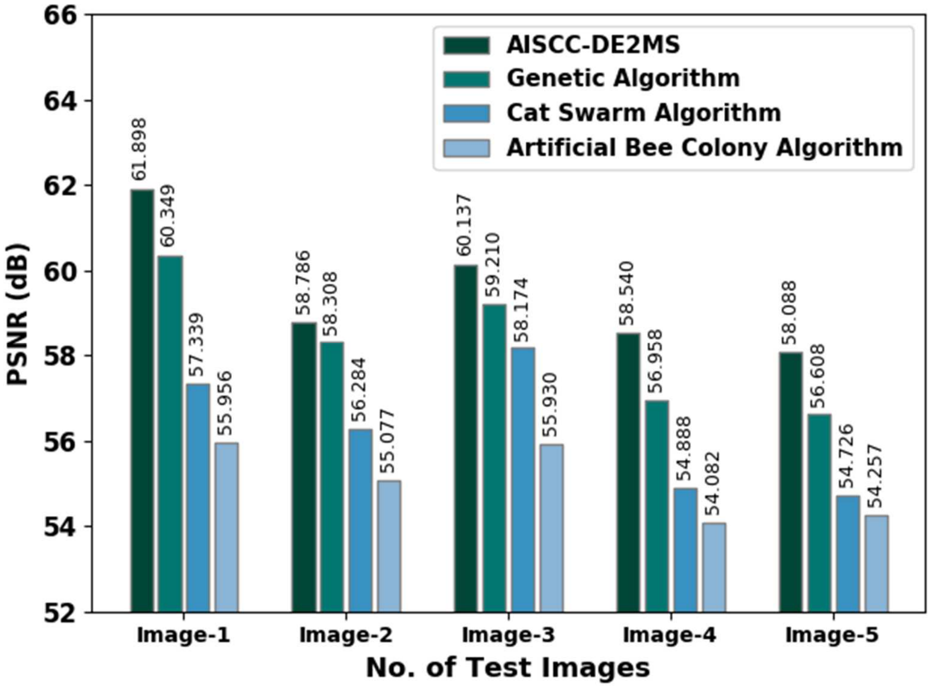


Figure 5. PSNR analysis of AISCC-DE2MS approach with distinct images.

The confusion matrices created by the AISCC-DE2MS model during the classification process are demonstrated in Figure 6. The figures reported that the AISCC-DE2MS model accurately classified all the samples into different classes under all runs.

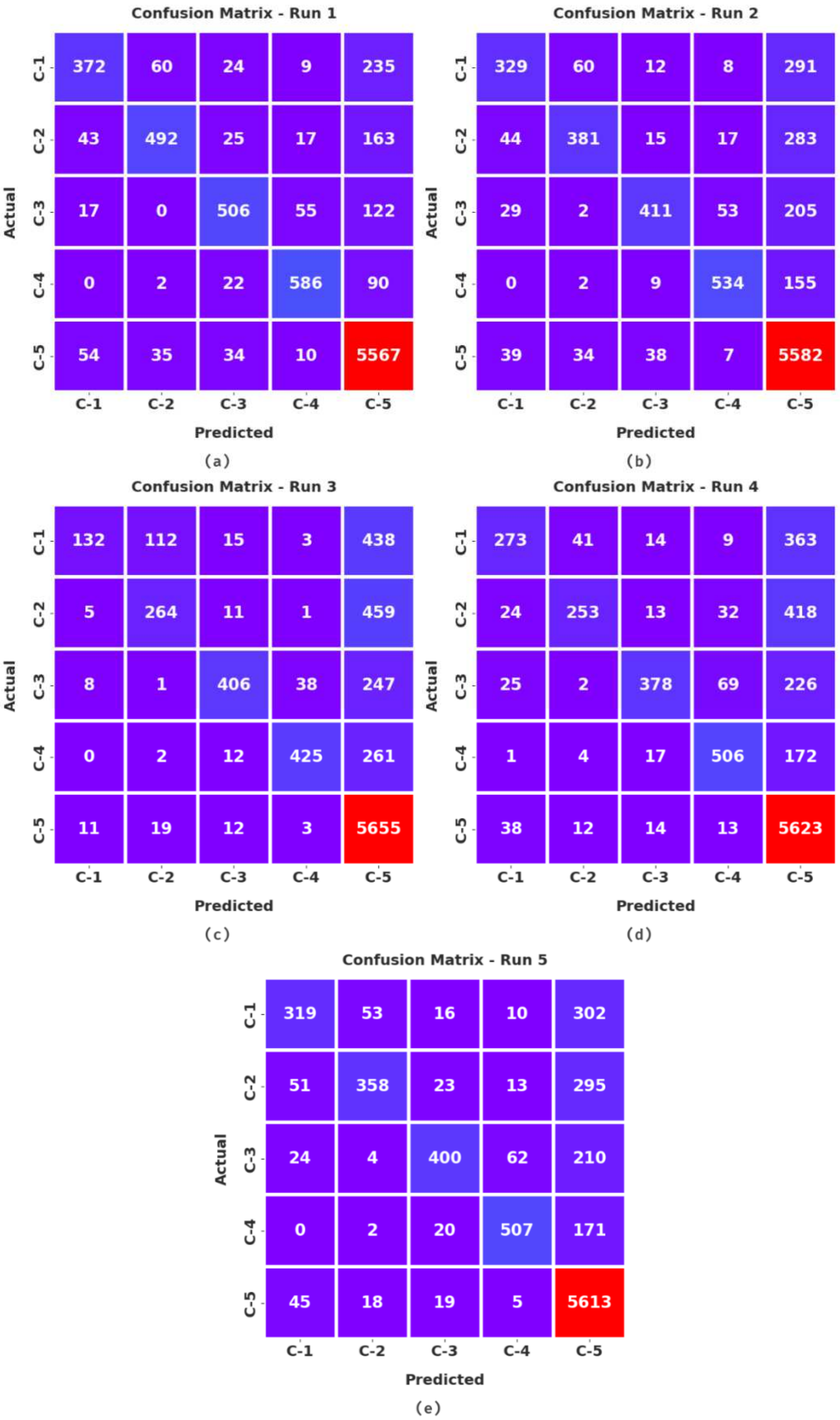
Table 3 and Figure 7 exhibit an overall classification performance of the AISCC-DE2MS model under distinct runs. The experimental outcomes highlighted that the AISCC-DE2MS model reached enhanced results under all classes. For instance, on run-1, the AISCC-DE2MS model offered an average $accu_y$, $prec_n$, $reca_l$, F_{score}, and AUC_{score} of 95.24%, 83.91%, 74.66%, 78.56%, and 84.66%, respectively. In line with run-2, the AISCC-DE2MS algorithm has an obtainable average $accu_y$, $prec_n$, $reca_l$, F_{score}, and AUC_{score} of 93.90%, 82.16%, 66.28%, 72.38%, and 79.38%, correspondingly. Afterward, on run-3, the AISCC-DE2MS system had an accessible average $accu_y$, $prec_n$, $reca_l$, F_{score}, and AUC_{score} of 92.23%, 82.10%, 54.49%, 61.75%, and 71.97%, correspondingly. At last, on run-4, the AISCC-DE2MS methodology provided an average $accu_y$, $prec_n$, $reca_l$, F_{score}, and AUC_{score} of 92.94%, 81.30%, 59.62%, 66.44%, and 75.24%, correspondingly.

The training accuracy (TRA) and validation accuracy (VLA) acquired by the AISCC-DE2MS approach on the test dataset is in Figure 8. The experimental result exposed that the AISCC-DE2MS system gained higher values of TRA and VLA. Specifically, the VLA looked superior to that of the TRA.

The training loss (TRL) and validation loss (VLL) accomplished by the AISCC-DE2MS approach on the test dataset are recognized in Figure 9. The experimental result stated that the AISCC-DE2MS system has reached decreased values of TRL and VLL. When predefined, the VLL is lesser than TRL.

An obvious precision-recall investigation of the AISCC-DE2MS system on test dataset is represented in Figure 10. The figure revealed that the AISCC-DE2MS algorithm has resulted in maximal values of precision-recall values under all classes.

A detailed ROC examination of the AISCC-DE2MS algorithm on the test dataset is demonstrated in Figure 11. The outcomes representing the AISCC-DE2MS system outperformed its capability in classifying various classes of test dataset.



Confusion Matrix - Run 1

(a)

Confusion Matrix - Run 2

(b)

Confusion Matrix - Run 3

(c)

Confusion Matrix - Run 4

(d)

Confusion Matrix - Run 5

(e)

Figure 6. Confusion matrices of AISCC-DE2MS approach. (**a**) Run1, (**b**) Run2, (**c**) Run3, (**d**) Run4, and (**e**) Run5.

Table 3. Result analysis of AISCC-DE2MS approach with distinct measures and runs.

Labels	Accuracy	Precision	Recall	F-Score	AUC Score
			Run-1		
C-1	94.82	76.54	53.14	62.73	75.84
C-2	95.96	83.53	66.49	74.04	82.62
C-3	96.50	82.82	72.29	77.19	85.47
C-4	97.60	86.56	83.71	85.11	91.28
C-5	91.30	90.12	97.67	93.74	88.09
Average	**95.24**	**83.91**	**74.66**	**78.56**	**84.66**
			Run-2		
C-1	94.34	74.60	47.00	57.67	72.79
C-2	94.65	79.54	51.49	62.51	75.12
C-3	95.75	84.74	58.71	69.37	78.89
C-4	97.06	86.27	76.29	80.97	87.60
C-5	87.68	85.67	97.93	91.39	82.52
Average	**93.90**	**82.16**	**66.28**	**72.38**	**79.38**
			Run-3		
C-1	93.07	84.62	18.86	30.84	59.28
C-2	92.86	66.33	35.68	46.40	66.98
C-3	95.97	89.04	58.00	70.24	78.68
C-4	96.25	90.43	60.71	72.65	80.07
C-5	83.02	80.10	99.21	88.64	74.87
Average	**92.23**	**82.10**	**54.49**	**61.75**	**71.97**
			Run-4		
C-1	93.97	75.62	39.00	51.46	68.94
C-2	93.61	81.09	34.19	48.10	66.72
C-3	95.55	86.70	54.00	66.55	76.63
C-4	96.29	80.45	72.29	76.15	85.36
C-5	85.29	82.67	98.65	89.95	78.57
Average	**92.94**	**81.30**	**59.62**	**66.44**	**75.24**
			Run-5		
C-1	94.13	72.67	45.57	56.01	72.02
C-2	94.63	82.30	48.38	60.94	73.70
C-3	95.57	83.68	57.14	67.91	78.07
C-4	96.69	84.92	72.43	78.18	85.64
C-5	87.53	85.16	98.47	91.34	82.02
Average	**93.71**	**81.75**	**64.40**	**70.88**	**78.29**

Finally, a detailed comparative study of the AISCC-DE2MS model with other existing models is offered in Table 4 [28]. The experimental values implied that the SCNet, SCFCNet, baseNet, and MobileNet models have shown lower performance over other models. Next to that, the ERNet and VGG16 models have certainly demonstrated improved outcomes.

However, the AISCC-DE2MS model has ensured better performance over other models with higher $accu_y$ of 95.24% and processing time of 11.13 ms. Therefore, the presented

AISCC-DE2MS model can be employed for the effectual classification model on the drone's environment.

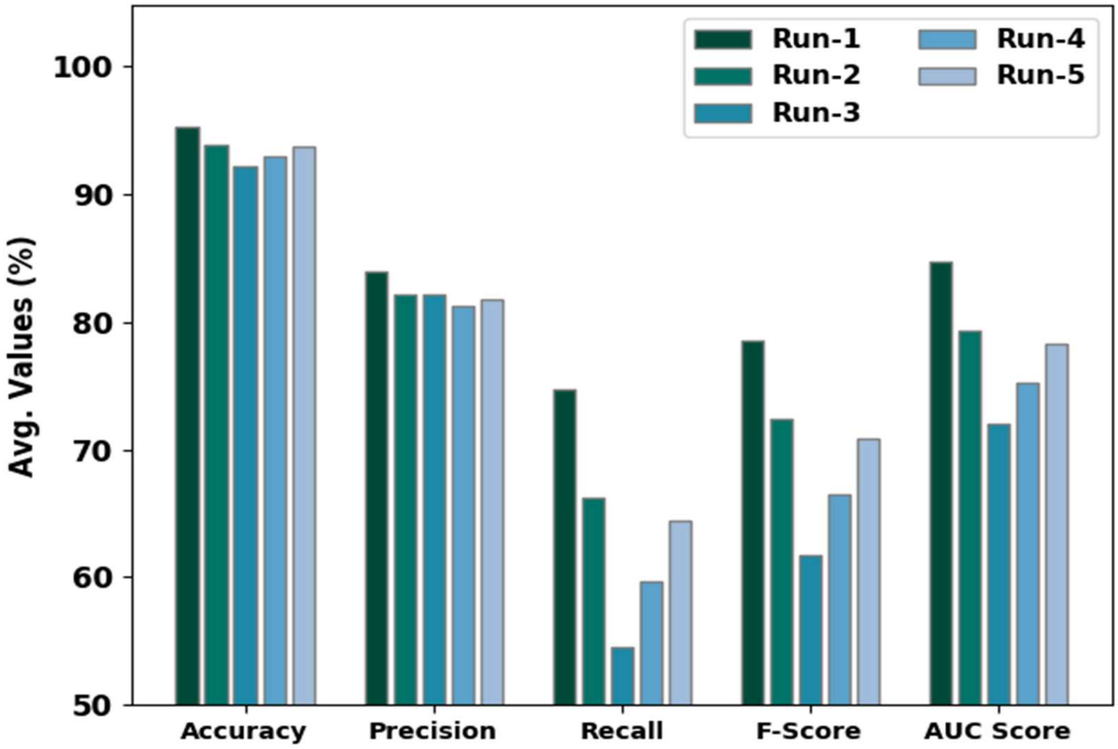


Figure 7. Average analysis of the AISCC-DE2MS approach with distinct runs.

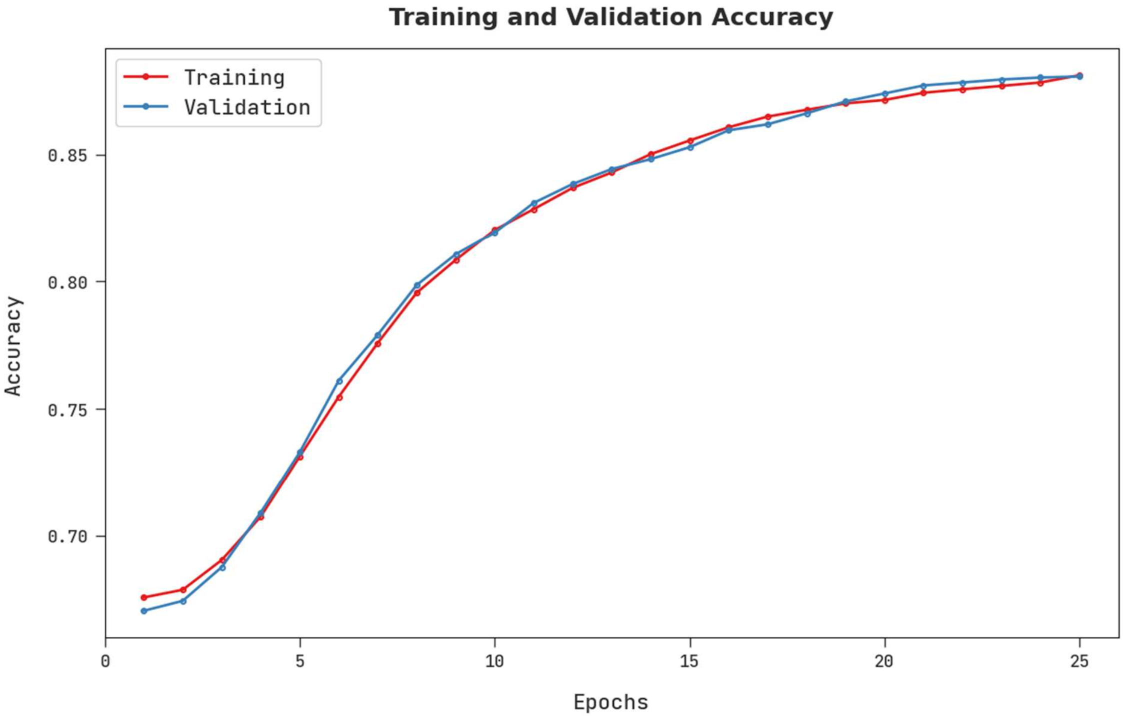


Figure 8. TRA and VLA analysis of AISCC-DE2MS approach.

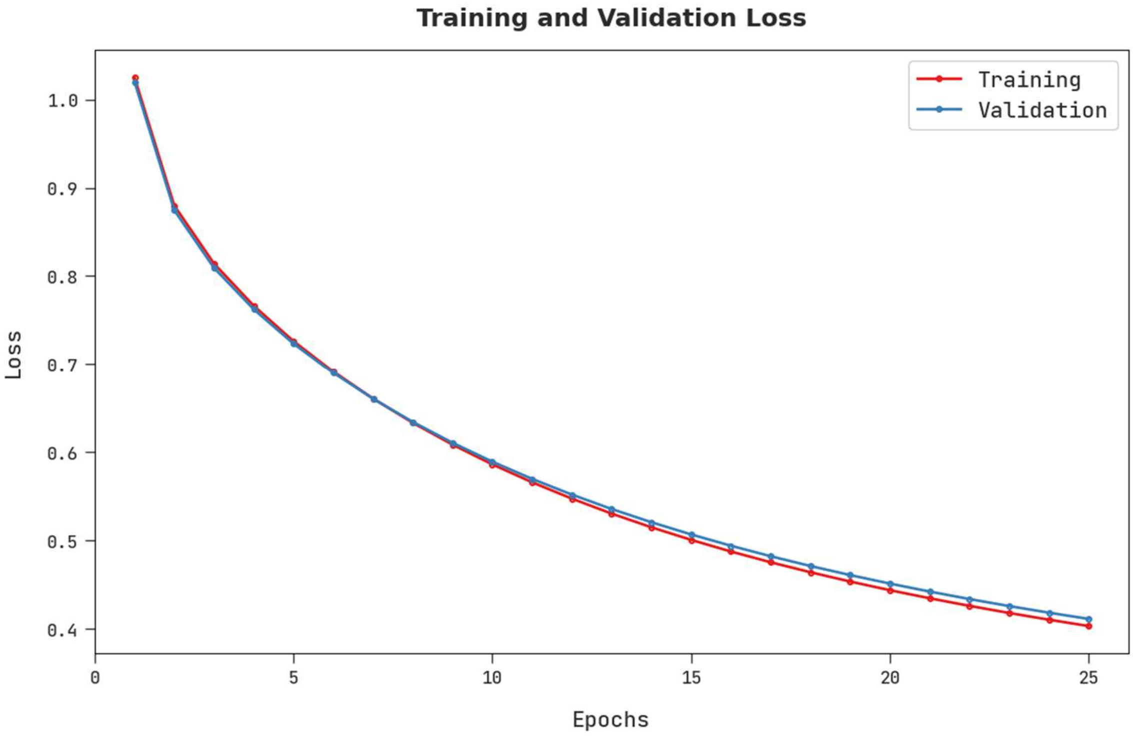


Figure 9. TRL and VLL analysis of the AISCC-DE2MS approach.

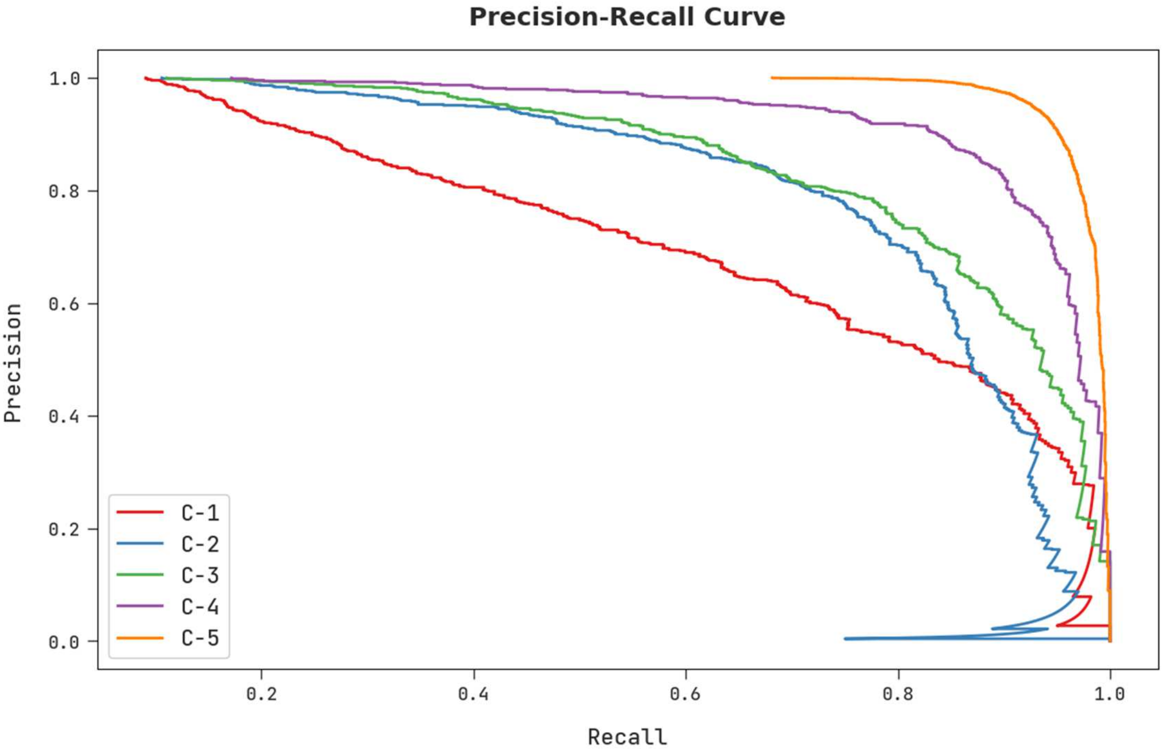


Figure 10. Precision-recall analysis of AISCC-DE2MS approach.

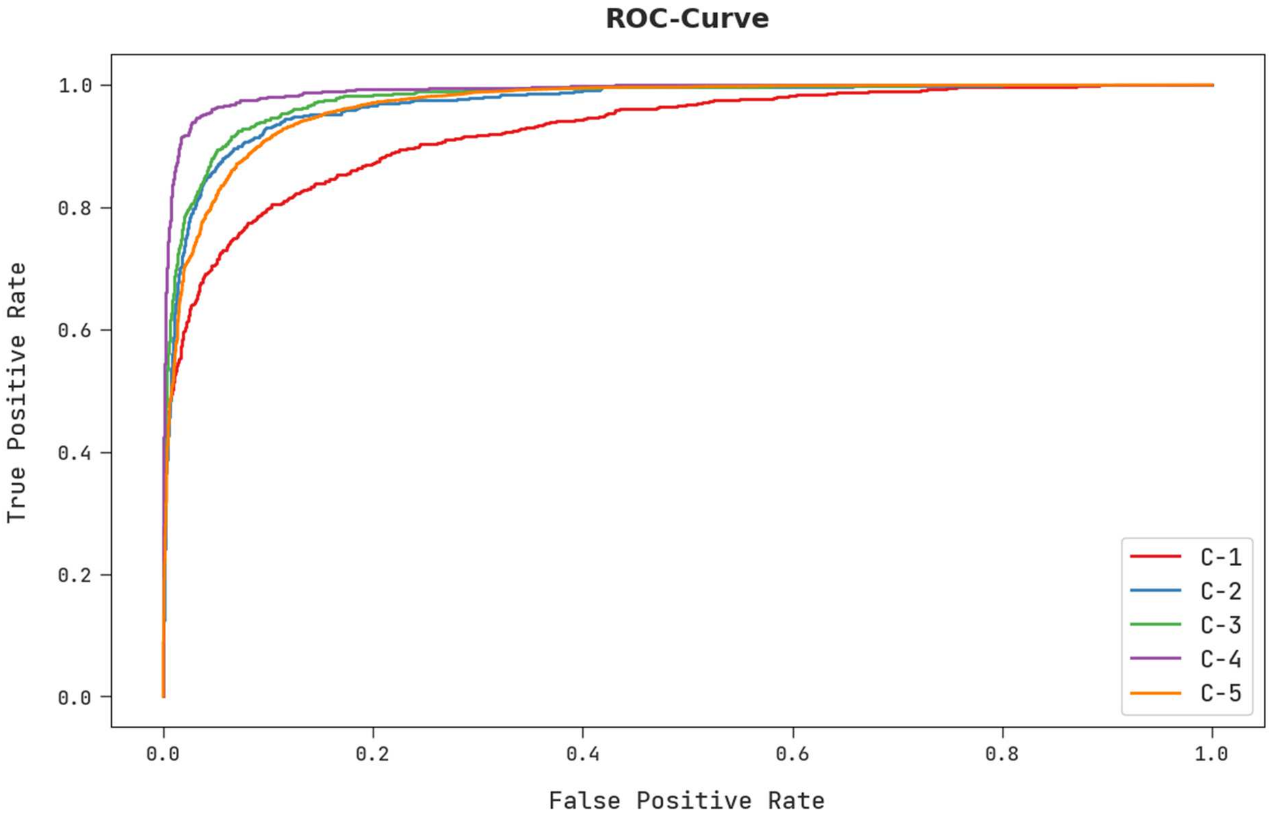


Figure 11. ROC analysis of the AISCC-DE2MS approach.

Table 4. Comparative analysis of the AISCC-DE2MS approach with recent algorithms.

Methods	Accuracy (%)	Processing Time (ms)
AISCC-DE2MS	95.24	11.13
ERNet Model	90.16	19.46
SCFCNet Model	87.11	14.14
SCNet Model	85.70	14.18
baseNet Model	88.34	21.12
VGG16 Model	91.25	347.22
ResNet50 Model	89.61	257.48
MobileNet Model	88.55	47.63

5. Conclusions

In this study, a new AISCC-DE2MS algorithm was projected for secure communication and classification on drone-based emergency monitory systems. The proposed AISCC-DE2MS technique performed image encryption at the preliminary stage using the AGTO algorithm with an ECC-Based ElGamal Encryption technique in which the optimal key generation procedure takes place via the AGTO algorithm. To classify the images, the AISCC-DE2MS model encompasses DenseNet feature extraction, PESO-based hyperparameter tuning, and LSTM-based classification. The simulation analysis of the AISCC-DE2MS model is tested by making use of the AIDER dataset and the results demonstrate the improved performance of the AISCC-DE2MS model with an accuracy of 95.24% and a processing time of 11.13 ms. Thus, the AISCC-DE2MS method can be utilized as a proficient tool for secure communication and classification in the drone's environment. In the future, the performance of the presented model can be extended by image steganographic techniques.

Author Contributions: Conceptualization, F.S.A. and N.A.; methodology, S.S.A.; software, H.M.; validation, M.M.; A.A. and A.M.; formal analysis, A.M.; investigation, K.A.A.; resources, A.A.; data curation, M.M.; writing—original draft preparation, F.S.A., K.A.A. and S.S.A.; writing—review and editing, A.A. and H.M; visualization, A.M.; supervision, K.A.A.; project administration, S.S.A.; funding acquisition, F.S.A. and A.A. All authors have read and agreed to the published version of the manuscript.

Funding: Princess Nourah bint Abdulrahman University Researchers Supporting Project number (PNURSP2022R319), Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia. The authors would like to thank the Deanship of Scientific Research at Umm Al-Qura University for supporting this work by Grant Code (22UQU4210118DSR30).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

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

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

References

1. Kumar, A.; de Jesus Pacheco, D.A.; Kaushik, K.; Rodrigues, J.J. Futuristic view of the internet of quantum drones: Review, challenges and research agenda. *Veh. Commun.* **2022**, *36*, 100487. [CrossRef]
2. Jang, W.; Lee, S.Y. Partial image encryption using format-preserving encryption in image processing systems for Internet of things environment. *Int. J. Distrib. Sens. Netw.* **2020**, *16*, 1550147720914779. [CrossRef]
3. Rashmi, P.; Supriya, M.C.; Hua, Q. Enhanced Lorenz-Chaotic Encryption Method for Partial Medical Image Encryption and Data Hiding in Big Data Healthcare. *Secur. Commun. Netw.* **2022**, *2022*, 9363377. [CrossRef]
4. Yahuza, M.; Idris, M.Y.I.; Ahmedy, I.B.; Wahab, A.W.A.; Nandy, T.; Noor, N.M.; Bala, A. Internet of drones security and privacy issues: Taxonomy and open challenges. *IEEE Access* **2021**, *9*, 57243–57270. [CrossRef]
5. Abunadi, I.; Althobaiti, M.M.; Al-Wesabi, F.N.; Hilal, A.M.; Medani, M.; Hamza, M.A.; Rizwanullah, M.; Zamani, A.S. Federated learning with blockchain assisted image classification for clustered UAV networks. *Comput. Mater. Contin.* **2022**, *72*, 1195–1212. [CrossRef]
6. Koubâa, A.; Qureshi, B.; Sriti, M.F.; Allouch, A.; Javed, Y.; Alajlan, M.; Cheikhrouhou, O.; Khalgui, M.; Tovar, E. Dronemap Planner: A service-oriented cloud-based management system for the Internet-of-Drones. *Ad Hoc Netw.* **2019**, *86*, 46–62. [CrossRef]
7. Alohali, M.A.; Al-Wesabi, F.N.; Hilal, A.M.; Goel, S.; Gupta, D.; Khanna, A. Artificial intelligence enabled intrusion detection systems for cognitive cyber-physical systems in industry 4.0 environment. *Cogn. Neurodyn.* **2022**, 1–13. [CrossRef]
8. Allouch, A.; Cheikhrouhou, O.; Koubâa, A.; Toumi, K.; Khalgui, M.; Nguyen Gia, T. Utm-chain: Blockchain-based secure unmanned traffic management for internet of drones. *Sensors* **2021**, *21*, 3049. [CrossRef]
9. Al-Qarafi, A.; Alrowais, F.; Alotaibi, S.; Nemri, N.; Al-Wesabi, F.N.; Al Duhayyim, M.; Marzouk, R.; Othman, M.; Al-Shabi, M. Optimal machine learning based privacy preserving blockchain assisted internet of things with smart cities environment. *Appl. Sci.* **2022**, *12*, 5893. [CrossRef]
10. Tian, Y.; Yuan, J.; Song, H. Efficient privacy-preserving authentication framework for edge-assisted Internet of Drones. *J. Inf. Secur. Appl.* **2019**, *48*, 102354. [CrossRef]
11. Upadhyay, J.; Rawat, A.; Deb, D. Multiple Drone Navigation and Formation Using Selective Target Tracking-Based Computer Vision. *Electronics* **2021**, *10*, 2125. [CrossRef]
12. Singh, M.; Aujla, G.S.; Bali, R.S. A deep learning-based blockchain mechanism for secure internet of drones environment. *IEEE Trans. Intell. Transp. Syst.* **2020**, *22*, 4404–4413. [CrossRef]
13. Bera, B.; Chattaraj, D.; Das, A.K. Designing secure blockchain-based access control scheme in IoT-enabled Internet of Drones deployment. *Comput. Commun.* **2020**, *153*, 229–249. [CrossRef]
14. Sarkar, S.; Khare, S.; Totaro, M.W.; Kumar, A. A novel energy aware secure internet of drones design: Esiod. In Proceedings of the IEEE INFOCOM 2021-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), Vancouver, BC, Canada, 10–13 May 2021; pp. 1–6.
15. Ismael, H.M. Authentication and encryption drone communication by using HIGHT lightweight algorithm. *Turk. J. Comput. Math. Educ.* **2021**, *12*, 5891–5908.
16. Gorrepati, R.R.; Guntur, S.R. DroneMap: An IoT Network Security in Internet of Drones. In *Development and Future of Internet of Drones (IoD): Insights, Trends and Road Ahead*; Springer: Berlin/Heidelberg, Germany, 2021; pp. 251–268.
17. Bera, B.; Das, A.K.; Sutrala, A.K. Private blockchain-based access control mechanism for unauthorized UAV detection and mitigation in Internet of Drones environment. *Comput. Commun.* **2021**, *166*, 91–109. [CrossRef]

18. Ajmal, S. An Efficient Video Encryption Technique for Secure Transmission through Drones in IoMT. Ph.D. Thesis, The Islamia University of Bahawalpur, Bahawalpur, Pakistan, 2020.
19. Zhang, Y.; He, D.; Li, L.; Chen, B. A lightweight authentication and key agreement scheme for Internet of Drones. *Comput. Commun.* **2020**, *154*, 455–464. [CrossRef]
20. Khan, M.A.; Shah, H.; Rehman, S.U.; Kumar, N.; Ghazali, R.; Shehzad, D.; Ullah, I. Securing internet of drones with identity-based proxy signcryption. *IEEE Access* **2021**, *9*, 89133–89142. [CrossRef]
21. Available online: https://zenodo.org/record/3888300#.Ys_0h3ZByUk (accessed on 13 April 2022).
22. Reegan, A.S.; Kabila, V. Highly secured cluster based WSN using novel FCM and enhanced ECC-ElGamal encryption in IoT. *Wirel. Pers. Commun.* **2021**, *118*, 1313–1329. [CrossRef]
23. Abdollahzadeh, B.; Soleimanian Gharehchopogh, F.; Mirjalili, S. Artificial gorilla troops optimizer: A new nature-inspired metaheuristic algorithm for global optimization problems. *Int. J. Intell. Syst.* **2021**, *36*, 5887–5958. [CrossRef]
24. Hasan, N.; Bao, Y.; Shawon, A.; Huang, Y. DenseNet convolutional neural networks application for predicting COVID-19 using CT image. *SN Comput. Sci.* **2021**, *2*, 389. [CrossRef]
25. Xing, Z. An improved emperor penguin optimization based multilevel thresholding for color image segmentation. *Knowl.-Based Syst.* **2020**, *194*, 105570. [CrossRef]
26. Lei, J.; Liu, C.; Jiang, D. Fault diagnosis of wind turbine based on Long Short-term memory networks. *Renew. Energy* **2019**, *133*, 422–432. [CrossRef]
27. Kyrkou, C.; Theocharides, T. EmergencyNet: Efficient aerial image classification for drone-based emergency monitoring using atrous convolutional feature fusion. *IEEE J. Sel. Top. Appl. Earth Obs. Remote Sens.* **2020**, *13*, 1687–1699. [CrossRef]
28. Kyrkou, C.; Theocharides, T. Deep-Learning-Based Aerial Image Classification for Emergency Response Applications Using Unmanned Aerial Vehicles. In Proceedings of the CVPR Workshops, Long Beach, CA, USA, 16–20 June 2019; pp. 517–525.