IEEE Access
Multidisciplinary : Rapid Review : Open Access Journal

Received 14 September 2023, accepted 6 October 2023, date of publication 12 October 2023, date of current version 3 November 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3324068

RESEARCH ARTICLE

Rider Optimization With Deep Learning Based Image Encryption for Secure Drone Communication

N. KANNAIYA RAJA[1], E. LAXMI LYDIA[2], THUMPALA ARCHANA ACHARYA[3], K. RADHIKA[4], EUNMOK YANG[5], AND OKYEON YI[5]

[1]Department of Computer Science, IoT–HH Campus, Ambo University, Ambo 0610, Ethiopia
[2]Department of Computer Science and Engineering, Vignan's Institute of Information Technology, Visakhapatnam 530049, India
[3]Vignan's Institute of Information Technology, Visakhapatnam 530049, India
[4]AI&DS Department, Chaitanya Bharathi Institute of Technology, Gandipet, Hyderabad 500075, India
[5]Department of Financial Information Security, Kookmin University, Seoul 02707, South Korea

Corresponding author: Okyeon Yi (oyyi@kookmin.ac.kr)

This work was supported by the Institute for Information and Communications Technology Promotion (IITP) Grant funded by the Korea Government (MSIP) (Research on Security Technology for 6G Telecommunication with 5G+) under Grant 2020-0-00085.

ABSTRACT In recent years, drones or Unmanned Aerial Vehicles (UAVs) got significant attention among researchers because of their extensive application in commercial applications, border surveillance, etc. As the conventional terrestrial communication system does not work effectively on heavy calamities namely floods, landslides, cyclones, earthquakes, etc., UAVs can offer a potential solution for inexpensive, rapid, and wireless communication. Despite the drones' benefits in emergency monitoring, security is been a main factor because of the existence of wireless connections for transmission. Therefore, this article introduces optimal deep learning with image encryption-based secure drone communication (ODLIE-SDC) technique. The major intention of the ODLIE-SDC technique lies in the effectual secure communication and classification process in emergency monitoring scenarios. To accomplish this, the presented ODLIE-SDC technique designs a hyperchaotic map-based image encryption technique and its optimal keys are produced by the use of a rider optimization algorithm (ROA). The image classification process is performed encompassing EfficientNet-B4-CBAM feature extraction and enhanced stacked autoencoder (ESAE) classification. Finally, the hyperparameter tuning of the EfficientNet-B4-CBAM technique takes place using the Bayesian optimization (BO) algorithm. The experimental validation of the ODLIE-SDC technique is tested on the AIDER dataset. The comprehensive comparative analysis reported the enhanced performance of the ODLIE-SDC technique over other existing approaches.

INDEX TERMS Drones, image classification, secure communication, encryption.

I. INTRODUCTION

The reliance and usage of drones have been steadily increasing in various fields. This is because of the drones' capability to provide image capture, live-stream and real-time video, in conjunction with the capability to fly and transport goods [1]. Consequently, over 10,000 drones come into existence for commercial usage within the next five years. This is primarily a result of their benefits over commercial helicopters when it comes to budget and costs. Furthermore, technological development allows easier manipulation through smartphones to fly mini-drones rather than using remote controllers. Indeed, the usage of drones is not constrained to commercial and personal purposes [2]. Currently, drones are described as aircraft that fly with no pilots at the controls but are instead supported by automated flight or ground operators without human interference. Now, they are available for different applications and are utilized for crop monitoring,

The associate editor coordinating the review of this manuscript and approving it for publication was Engang Tian.

vegetation mapping, habitat destruction assessment, marine fauna detection, and surveillance of crime scenes. In addition, drone mapping has a large number of applications in different fields involving infrastructure inspection, construction, agriculture, and mining [3]. In recent times, the application of drones to humanitarian relief [4], [5]. Precise collection of data might be highly complicated in an emergency due to the lack of coordinated action by different agencies during the emergency [6]. Nevertheless, it was recommended that to enhance efficiency of the emergency management, recent technologies and methodologies are needed to conceptualize systems that integrate a mixture of spatial/temporal-oriented, telecommunication tools, and remote sensing databases. Even though this application was most promising to offer comfort and safety to all, it could bring disastrous results if the drone transmission link was misused and hacked [7].

Being resource-constraint, drones are extremely vulnerable to cyber and physical threats or attacks [8]. The battery and storage capacity of drones is limited and if appropriate management is not provided, it becomes easier to hack the sensors and the chips installed on the drone circuits to attain the information stored. As a result, it is extremely imperative to emphasise the safety requirements for drone transmission as their application increases [9]. The reliance on wireless communication makes drones vulnerable to different attacks. This type of attack might have dramatic effects, involving commercial and non-commercial losses. In that regard, there is a lack of clear understanding on how hacker hijacks a drone and performs their attacks, to crash or even interrupt it [10]. Indeed, drones could also be compromised for malicious purposes.

This article introduces optimal deep learning with image encryption-based secure drone communication (ODLIE-SDC) technique. The presented ODLIE-SDC technique designs a hyperchaotic map-based image encryption technique and its optimal keys are produced by the use of a rider optimization algorithm (ROA). The image classification process is performed encompassing EfficientNet-B4-CBAM feature extraction and enhanced stacked autoencoder (ESAE) classification. Finally, the hyperparameter tuning of the EfficientNet-B4-CBAM technique takes place using the Bayesian optimization (BO) algorithm. The experimental validation of the ODLIE-SDC technique is tested on the AIDER dataset

II. RELATED WORKS

Alrayes et al. [11] establish an AI-oriented Secure Communication and Classification for Drone-Enabled Emergency Monitoring System (AISCC-DE2MS). This system mostly utilizes encrypt and classifier methods for emergency conditions. Primarily, the proposed technique utilizes an artificial gorilla troops optimizer (AGTO) technique with an ECC-related ElGamal Encryption system for accomplishing security. For the emergency condition classifier, the proposed scheme includes a DenseNet extraction feature, penguin search optimizer (PESO) based hyperparameter tuning, and LSTM-based classifier. Rabieh et al. [12] present a proxy re-encryption-based sharing method for enabling 3rd party for accessing only restricted videos with no need for an original encrypted key. The expensive pairing functions in proxy re-encrypt could not be utilized for allowing quick access and delivery of surveillance video for 3rd party. The basic management was controlled by a trusted control centre that performs as a proxy to re-encryption the data.

Ingle et al. [13] examined an earlier fusion-based video synopsis. Primarily, the authors fused the 2-D camera and 3-D LIDAR point cloud data; secondarily, the authors executed abnormal object recognition utilizing a customized sensor on the integrated dataset and lastly extracting only the basic information to create a synopsis. In [14], the authors examine that UAVs are utilized for distributing virus-related tests to probably sick patients. A new technique which the authors present is to utilize the present drone structure for performing this task, whereas drones maintained and worked by distinct private and public entities can be retrofitted for the distribution of necessities in crises. Miao et al. [15] introduce a drone-supported smart air agent from a 6-G edge fusion scheme. Primarily, the energy-effective dynamic routing scheme dependent upon a joint air-ground control optimizer was planned for improving fusion sensing efficacy and extending service hours of drone swarms. Eventually, an airborne data fusion scheme dependent upon multiple source sensing was planned for solving the connected cognitive optimizer issue for multi-modal data.

Nedelea et al. [16] examine the real possibility of utilizing drones in rescue operations, along with in non-segregated airspace, to attain solutions to monitor aerial work and activities supporting the public health system in an emergency. The particularity of the concept system was the usage of the "swarm" of fast drones for an aerial investigation that operates together, thereby enhancing the identification and search time while rising the operability of the system and the information area. Whenever required, a carrier drone with portable devices or medical supplies is incorporated that could also provide two-way video and audio transmission abilities. Mershad et al. [17] developed a technique which allows the drone to store significant information that it necessitates during its flight within the lightweight blockchain (BC) mechanism. Furthermore, the author proposed a new BC consensus model where different miners produce the block simultaneously that reduces the time required to securely add transactions to BC and meets the requirements of delay-sensitive applications.

III. THE PROPOSED MODEL

In this article, we have developed a new ODLIE-SDC method for effectual secure communication and classification processes in emergency scenarios. The ODLIE-SDC technique encompasses hyperchaotic map-based encryption, ROA-based key generation, EfficientNet-B3-CBAM feature extraction, BO-based hyperparameter optimizer, and ESAE classification. Fig. 1 demonstrates the overall procedure of the presented ODLIE-SDC algorithm.

A. IMAGE ENCRYPTION PROCESS

In this work, the encryption of the images captured by the drones takes place using hyperchaotic map-based encryption [18]. To enhance secrecy, the optimal keys can be produced by the ROA.

1) ENCRYPTION PROCEDURE

In this section, the process involved in the transformation of the input image into a cipher image is discussed.

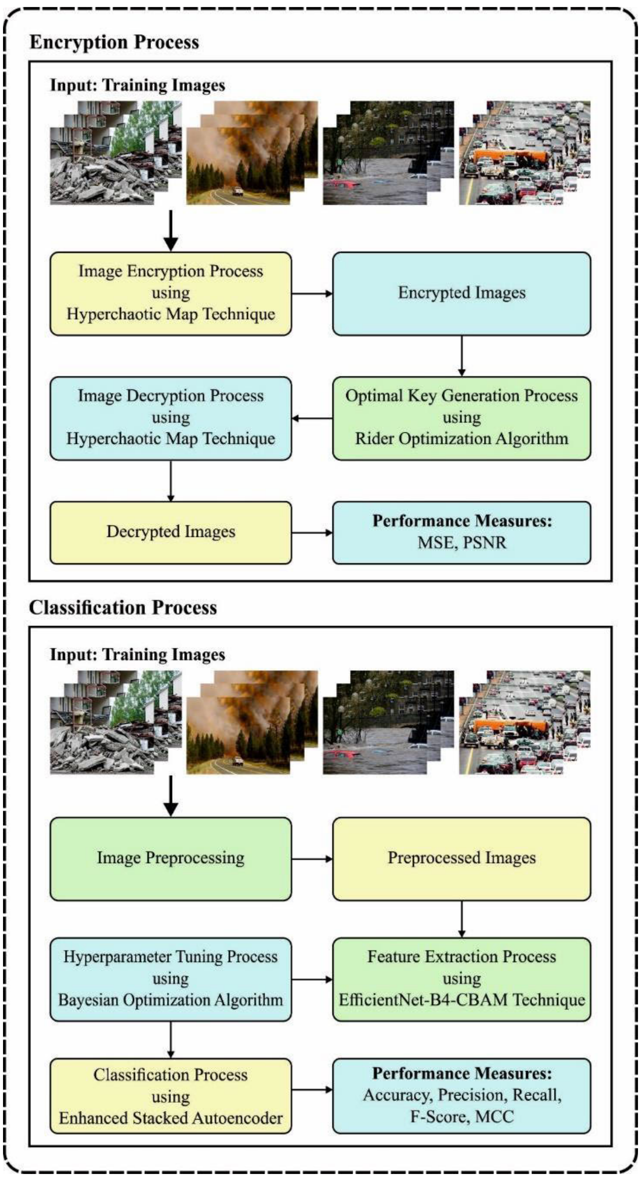


FIGURE 1. The overall procedure of the ODLIE-SDC system.

Step 1: Read a plain image (I_m) of size $m \times n$.

Step 2: Change I_m in 2D into 1D for more processing.

Step 3: Create optimum primary parameters like v_1, v_2, v_3, v_4, v_5, k, and l; and encrypted features (viz, α and β).

Step 4: Create confidential keys v_1', v_2', v_3', v_4', and v_5' using $5D$ hyper-chaotic map.

Step 5: Utilize v_1' and v_2' for changing the pixel value of I_m as

$$\begin{aligned} S &= mod\left(I_m + v_1', 256\right) \\ R &= mod(S + v_2', 256) \end{aligned} \tag{1}$$

At this point, R refers to the upgraded image.

Step 6: Afterward, the pixel of R was permutation utilizing v_3'. Primarily, v_3' has been arranged and it can be obtained v_3. Next, it is determined the value position of v_3'' in v_3' and keep the different positions in C_p. Afterwards, the element of R can be permutation by employing C_p as

$$R'(j) = R\left(C_p(j)\right), \quad j = 1, 2, \ldots, m \times n \tag{2}$$

In which R' indicates the permutation image.

Step 7: The permutation image R' is again permutation utilizing v_4' to optimum confusion. Similar to Step 6, sorting was executed on v_4' and the resultant matrix was kept in v_4. Afterwards, the value position of v_4'' is initiated in v_4' and altered positions are kept in C_p'. After that, every element of R' is permutation by utilizing C_p' as

$$R''(j) = R'\left(C_p'(j)\right), \quad j = 1, 2, \ldots, m \times n \tag{3}$$

Step 8: Diffusion was carried out on R'' utilizing v_5' and encrypt feature β for obtaining the encrypted image EN'.

$$EN'(j) = mod\left(v_5' \times R''(j) + (1 - \beta) \times v_5', 256\right) \tag{4}$$

Step 9: Again more than one level of diffusion is applied on EN' to optimum security. A key K is established in the groups of all 5 confidential keys. At that moment, K was utilized with another encrypted feature α for performing diffusion on EN' for obtaining the last encryption image.

$$\begin{aligned} K &= mod\left(v_1' \oplus v_2' \oplus v_3' \oplus v_4' \oplus v_5', 256\right) \\ EN(j) &= mod(K \times EN'(j) + (1 - \alpha) \times K, 256) \end{aligned} \tag{5}$$

Step 10: Change 1D EN into a 2D matrix and send it to the receiver.

2) DECRYPTION PROCEDURE

In this section, the process involved in the reconstruction of the input image from the cipher image is discussed. To decipher a novel image, the receiver requires the similar primary parameters of a $5D$ hyper-chaotic map and encrypted features (α and β) which are utilized in encrypting. So, it can be essential to transfer the desired parameters with a receiver on a secured channel. The decrypt method is just the inverse of encrypt method. The steps of the decrypt method are discussed as follows

Step 1: The receiver received an encrypted image EN on a public network. The vital primary parameters v_1, v_2, v_3, v_4,

v_5, k, l, α, and β are received by the receiver with a secured channel.

Step 2: Confidential keys (v'_1, v'_2, v'_3, v'_4, *and* v'_5) are established.

Step 3: Create a key K by XORing every confidential key. Besides, change the EN in the 2D to 1D matrix.

$$K = mod\left(v'_1 \oplus v'_2 \oplus v'_3 \oplus v'_4 \oplus v'_5, 256\right) \tag{6}$$

Step 4: Execute α and K on EN to decipher and obtain EN'.

$$EN' = EN - (1-\alpha) \times \frac{K}{\alpha} \tag{7}$$

Step 5: Execute β and v'_5 on EN' and obtain decipher image (R'').

$$R'' = EN' - (1-\beta) \times \frac{v'_5}{\beta} \tag{8}$$

Step 6: Implement sorting on v'_4 and supply the resultant into v_4 Afterwards, determine the position of elements of v''_4 in v'_4 and keep them into C'_p. Then, R'' is permutation as

$$R'(j) = R''\left(C'_p(j)\right) \tag{9}$$

Step 7: Implement sorting on v'_3 as completed in Step 6 and kept the transformed position from C_p. Next, R' is permutation as

$$R(j) = R'\left(C_p(j)\right) \tag{10}$$

Step 8: Execute v'_1 and v'_2 on R for obtaining the last decrypt image DN.

$$\begin{aligned} S &= mod\left(R - v'_2, 256\right) \\ DN &= mod(S - v'_1, 256) \end{aligned} \tag{11}$$

3) OPTIMAL KEY GENERATION PROCEDURE

In this work, the optimal key generation process of the hyperchaotic maps can be produced by the use of the ROA. ROA is designed on the concept of a rider being aggregated to accomplish their goal [19]. The groups of riders include follower, bypass rider, attacker, and overtaker. Each rider was arranged and later divided into groups. Every group generates their performance individually to accomplish the target. This process pursues a sequential process in a step-by-step way. Initially, parameter initialization of groups and riders have been taken place. In the ROA technique, the defined group was denoted as T and randomly take the location. Therefore, the mathematical formula for the procedure of group initialization is shown as follows:

$$G^t = \left\{G^t(S_a, S_b)\right\}; \quad 1 \le S_a \le NR_t, \quad 1 \le S_b \le DI_t \tag{12}$$

Now, NR_t indicates the number of riders existing in the race concerning time, DI_t signifies the dimension concerning time t. The location of the rider is represented as $G^t(S_a, S_b)$. The notation denotes the overall amount of riders namely bypass rider, follower, overtaker, and attacker BR, F, O, and AT, whereby ($T = BR + F + O + AT$). The parameter that is regarded are acceleration, steering angle, brake, and the gear, and they are installed in all the groups of rider. The steering angle (SA^t) can be mathematically expressed as follows:

$$SA^t = \left\{SA^t_{S_a,S_b}\right\}; \quad 1 \le S_a \le NR_t; \quad 1 \le S_b \le DI_t \tag{13}$$

Let $SA^t_{S_a,S_b}$ be the steering angle of the existing rider and the initial phase of the steering angle is demonstrated below:

$$SA^{t=0}_{S_{a'}S_b} = \begin{cases} \theta_a; & if\ S_b = 1 \\ SA^{t=0}_{S_{a'}S_b} = 1 + \alpha & if\ S_b \ne 1 \\ 0; & Otherwise \end{cases} \tag{14}$$

The angle of the present rider is denoted as θ_a and the term α indicates the existing rider location. The group leader is created for measuring the success rate. The leader was centralized and utilized the concept of arbitrary search in each direction which reflect in the improvement of the success rate. The key parameter considered for measuring success rate is distance and it can be mathematically expressed as follows:

$$CR_{dis} = \frac{S_a + D_v}{S_a - D_v} \tag{15}$$

From the expression, S_a indicates the position of the existing rider and D_v shows the destination. The rate of the leader detection process is preceded to increase the success. The central concept behind the leader selection process is that leader that is selected has minimal distance (highest success rate) from the destination and they are dynamic, differing based on the time, speed, and position. Then, the location updating takes place based on the group of riders. Initially, the location updating of the bypass rider is formulated as follows:

$$\begin{aligned} G^{BRj}_{t+1}(S_a, S_b) = \gamma \big[& G^t(\eta, S_b) \times \mu(S_b) + G^t(e, S_b) \\ & \times [1 - \mu(S_b)] \big] \end{aligned} \tag{16}$$

Now, γ indicates an arbitrary value that lies within [0, 1], η represents the random number that ranges from 1 to T, and μ signifies a random number ranging between 0 and 1 of size $1 \times D$. Next, location updating of follower rider is given below:

$$\begin{aligned} G^F_{t+1}(S_{a'}S_b) = {} & G^{L_{index}}(L_{index}, c) \\ & + \left[\cos\left(SA^{t=0}_{S_{a'}S_b}\right) \times G^{L_{index}}(L_{index}, c) \times d^t_{S_a}\right] \end{aligned} \tag{17}$$

Here, $G^{L_{index}}$ denotes the leader position, L_{index} shows the leader index, $SA^{t=0}_{S_a,S_b}$ represents the existing rider steering angle, and $d^t_{S_a}$ indicates additional distance required for covering the existing rider. Next, the location updating of the overtaker rider is formulated as.

$$G^O_{t+1}(S_a, S_c) = G_t(S_a, S_c) + [Y^I_t(S_a) * G^{L_{index}}(L_{index}, S_c) \tag{18}$$

where, $G_t(S_a, S_c)$ represents the existing rider position, and $Y^I_t(S)$ shows the existing rider direction. Lastly, the location updating of the attacker riders is formulated by

$$G_{t+1}^{AT}(S_{a'}S_c) = G^{L_{index}}(L_{index}, S_b) + \left[\cos\left(SA_{S_{a'}S_b}^{t=0}\right) \times G^{L_{index}}(L_{index}, S_b)\right] + d_{S_a}^t \tag{19}$$

where, $G^{L_{index}}(L_{index}, S_b)$ indicates the leader location and $SA_{S_a,S_b}^{t=0}$ signified steering angle of existing riders. Afterwards the computation of the group update, the success rate was evaluated amongst the riders. Based on the measurement, the new position and the leader were selected.

To achieve a better outcome, it is crucial to define an effective objective function. The ROA derived a fitness function by the maximization of the PSNR. The keys with maximum PSNR values can be chosen as optimal keys by the ROA.

$$fitness = \max\{PSNR\} \tag{20}$$

B. IMAGE CLASSIFICATION PROCESS

To recognize the different classes, an image classification process is performed encompassing EfficientNet-B4-CBAM feature extraction, BO-based hyperparameter optimization, and ESAE classification.

1) FEATURE EXTRACTION

For feature vector generation, the EfficientNet-B4-CBAM model is employed here. EfficientNet is an extremely correct network acquired with a machine search [20]. It utilizes an easy and effectual compound co-efficient for equally scaling the resolution, width, and depth of networks. Besides, related to other CNN techniques which reach the same accuracy on ImageNet database, EfficientNet is much lesser. For precisely identifying several classes, a novel DL technique named EfficientNet-B4-CBAM was generated merging the EfficientNet-B4 and CBAM components EfficientNet-B4-CBAM method was mostly collected from the EfficientNet-B4 method and CBAM component. During the EfficientNet-B4-CBAM method, the EfficientNet-B4 technique has accountable for extracting features, but the CBAM component has responsible to realize the refinement of extraction features. The EfficientNet-B4 technique encompasses generally a mobile inverted bottleneck convolutional, with a 3-channel image with a pixel resolution of 380 × 380 as input and detection outcome as output. Pointwise convolutional, depthwise convolutional, and squeeze-and-excitation (SE) components are the 3 primary modules of MBConv. Afterwards, a 5 × 5 depthwise convolutional was executed, and then the overview of the SE component for boosting the expressiveness of the method. Afterwards, 1 × 1 pointwise convolutional has been utilized for returning the feature mapping to their novel channel dimensional. Eventually, drop connect was applied, and skip connection of input was executed.

Finally, the hyperparameter tuning of the EfficientNet-B4-CBAM technique takes place using the BO algorithm. BO is one of the robust methods for resolving functions which is computationally expensive for finding the extrema [21]. It is used for resolving the function without closed-form expression. Also, it is applied for the non-convex function or the expensive function to compute; the derivative is difficult to assess. In the presented work, the optimization aims at finding a maximal value at the sample point for the f unknown function.

$$x^+ = \arg\max_{x \in A} f(x). \tag{21}$$

In Eq. (21), A shows the search space of x. BO derived from the Bayes theorem:

$$P(M \mid E) \propto P(E \mid M \parallel) P(M). \tag{22}$$

The abovementioned equation reflects the fundamental idea of BO. BO aims to integrate the priori distribution of function f(x) with the sampling dataset to attain the posterior function; next, the posterior data is applied to finding the function f(x), where it is maximized based on the criterion. The function u defines the next sample point for maximizing the predicted utility. While searching the sampling region, it is essential to consider exploitation (sample from that with higher value) and exploration (sample from an area of high uncertainty). This might assist in reducing the sampling count. Additionally, the performance would be enhanced even while the function has local maxima.

Besides the sampling data, BO relies on the prior distribution of function f, which is an essential component in statistical inference. Generally, the Gaussian function is presumed to be very suitable for BO's priori distribution. The Gaussian function is easy to handle and extremely flexible. Hence the BO employs the Gaussian function to fit data and upgrade the posterior distribution.

Where $D_{1:f-1} = \{x_n, y_n\}_{n=1}^{t-1}$ characterizes the training data that comprises of $t-1$ observation of f function. As mentioned above, the process comprises two parts: maximizing the acquisition function (step 2) and updating the posterior distribution (steps 3 and 4). As the observation accumulates, the posterior distribution is constantly upgraded; based on the new posterior. The entire procedure is reiterated until the difference between the present and the optimum values attained so far is lesser than the predetermined threshold or the maximal amount of iterations is attained. It is worth noting that BO doesn't need the explicit expression of the function f more than that of other optimization techniques, namely the gradient descent algorithm. Hence, it has a large number of applications.

The BO algorithm derives a fitness function from accomplishing superior classification performance. It defines the positive integer to illustrate the superior performance of candidate solutions. The reduction of classification error rate is viewed as a fitness function, as follows.

$$fitness(x_i) = ClassifierErrorRate(x_i) = \frac{number\ of\ misclassified\ samples}{Total\ number\ of\ samples} * 100 \tag{23}$$

Algorithm 1 Bayesian Optimization

For $t = 1, 2, \cdots$

Find x_t by augmenting acquisition function u over function f.

$x_t = \arg\max_x u(x|D_{1:t-1})$.

Sampling the objective function: $y_t = f(x_t)$.

Increase the data $D_{1:t} = \{D_{1:t-1}, (x_t, y_t)\}$ and upgrade the posterior of function f.

End for

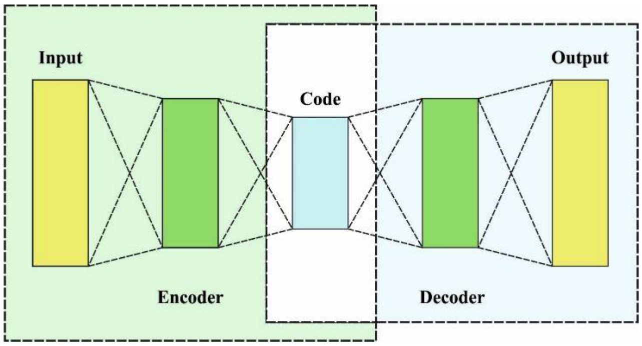


FIGURE 2. The architecture of SAE.

2) IMAGE CLASSIFICATION

Here, the classification of distinct kinds of classes takes place using the ESAE model. SAE could efficiently extract the deep feature in the dataset and has the features of faster convergence based on its underlying concept [22]. However, based on the theory of information bottleneck, still, the capability of feature extraction can be optimized. When the depth of NN is increased, the pertinent data of the extracted features by the network and original data will be decreased. Consequently, the study presents an ESAE model to preserve more original information during feature extraction. The model trains the original information as further data of the hidden layer (HL) in the pretraining phase. It could make original information wholly participate in the coding process so that additional data based on the original information are retained during the process of feature extraction.

ESAE is the same as SAE during the process of training, separated into reverse finetuning and pretraining. During the pretraining, the HL information of every AE is exploited as input for the following AE. Furthermore, the original information is included to improve training procedures. In the pretraining technique, ESAE first input the original information x_{data} into AE1 to train for obtaining the HL dataset $h^{(1)}$ of the $AE1$. Next, *the* $h^{(1)}$ hidden layer of AE1 is integrated into the original dataset as the input $x^{(2)} = [h^{(1)}, x_{data}]$ of $AE2$. Similarly, the AE2 trained as AE1 to attain $h^{(2)}$ hidden layer. The abovementioned steps are repeated to attain the depth of the model set. During the ESAE reverse finetuning, the network parameter attained in the network pretraining is exploited as an initialization parameter to build a deep network with several HLs. Fig. 2 depicts the infrastructure of SAE.

IV. PERFORMANCE VALIDATION

The proposed model is simulated using Python 3.6.5 tool on PC i5-8600k, GeForce 1050Ti 4GB, 16GB RAM, 250GB SSD, and 1TB HDD. The parameter settings are given as follows: learning rate: 0.01, dropout: 0.5, batch size: 5, epoch count: 50, and activation: ReLU. The experimental validation of the ODLIE-SDC technique is tested by utilizing the AIDER Dataset [23]. The dataset holds 8540 samples with five classes as represented by Table 1. Fig. 3 illustrates the sample images.

A set of measures used to examine the performance of the proposed model are mean square error (MSE), peak signal-to-noise ratio (PSNR), accuracy, precision, recall, F-Score, MCC, and computation time (CT).

TABLE 1. Details of dataset.

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

FIGURE 3. Sample images.

In Table 2, a brief study of the ODLIE-SDC technique with other methods in terms of MSE and PSNR is given. Fig. 4 examines a comparative MSE examination of the ODLIE-SDC technique. The results signify that the ODLIE-SDC technique reaches effectual outcomes with minimal values of MSE. For instance, on IMG-1, the ODLIE-SDC technique results in a reduced MSE of 0.038 while the

AISCC-DE2MS, GA, and CSA models attain increased MSE of 0.042, 0.060, and 0.120 respectively. Simultaneously, on IMG-3, the ODLIE-SDC technique results in a reduced MSE of 0.059 while the AISCC-DE2MS, GA, and CSA techniques attain increased MSE of 0.063, 0.078, and 0.099 correspondingly. Concurrently, on IMG-5, the ODLIE-SDC approach results in reduced MSE of 0.096 while the AISCC-DE2MS, GA, and CSA techniques attain increased MSE of 0.101, 0.142, and 0.219 correspondingly.

TABLE 2. MSE and PSNR analysis of the ODLIE-SDC algorithm with different test images.

No. of Test Images	ODLIE-SDC		AISCC-DE2MS		Genetic Algorithm		Cat Swarm Algorithm	
	MSE	PSNR	MSE	PSNR	MSE	PSNR	MSE	PSNR
TEST IMG-1	0.038	62.33	0.042	61.898	0.060	60.349	0.120	57.339
TEST IMG-2	0.072	59.56	0.086	58.786	0.096	58.308	0.153	56.284
TEST IMG-3	0.059	60.42	0.063	60.137	0.078	59.210	0.099	58.174
TEST IMG-4	0.087	58.74	0.091	58.540	0.131	56.958	0.211	54.888
TEST IMG-5	0.096	58.31	0.101	58.088	0.142	56.608	0.219	54.726

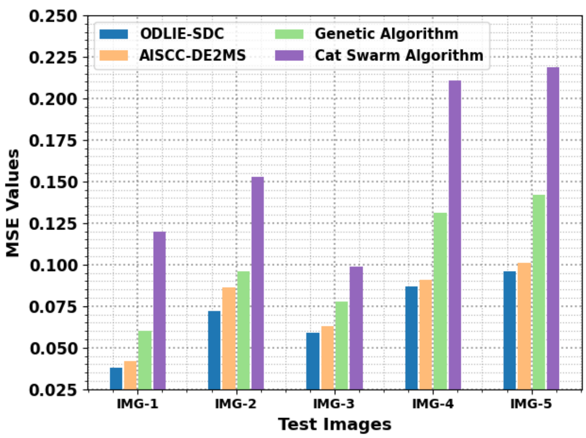


FIGURE 4. MSE analysis of the ODLIE-SDC algorithm with different test images.

In Fig. 5, a comparative PSNR study of the ODLIE-SDC technique is made under various images. The obtained values demonstrate that the ODLIE-SDC technique gains higher values of PSNR over other models. For instance, on IMG-1, the ODLIE-SDC technique obtains an increased PSNR of 62.33dB while the AISCC-DE2MS, GA, and CSA models reach decreased PSNR of 61.898dB, 60.349dB, and 57.339dB correspondingly. Meanwhile, on IMG-3, the ODLIE-SDC method attains an increased PSNR of 60.42dB while the AISCC-DE2MS, GA, and CSA techniques reach decreased PSNR of 60.137dB, 59.210dB, and 58.174dB correspondingly. Eventually, on IMG-5, the ODLIE-SDC method obtains an increased PSNR of 58.31dB while the AISCC-DE2MS, GA, and CSA methodologies reach

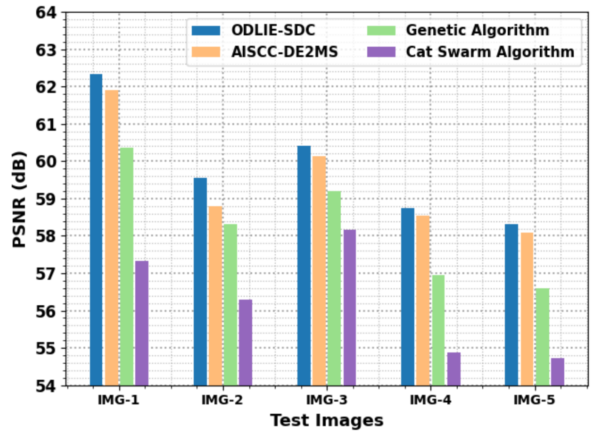


FIGURE 5. PSNR analysis of the ODLIE-SDC algorithm with different test images.

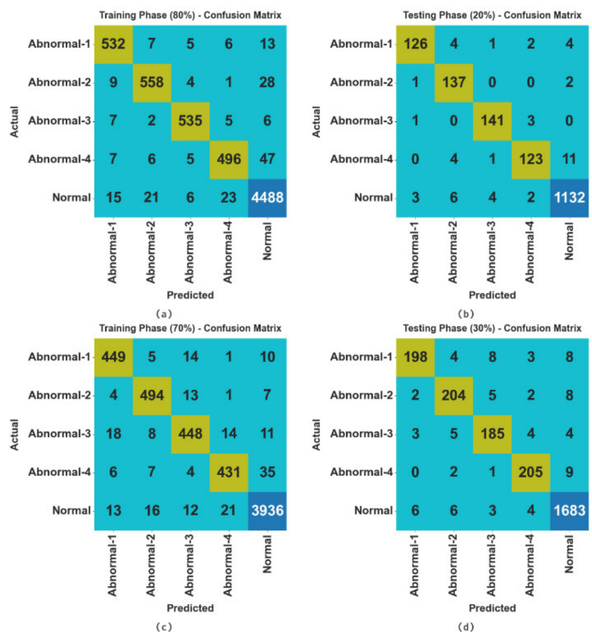


FIGURE 6. Confusion matrices of ODLIE-SDC approach (a-b) TRS/TSS of 80:20 and (c-d) TRS/TSS of 70:30.

decreased PSNR of 58.088dB, 56.608dB, and 54.726dB correspondingly.

The confusion matrix of the ODLIE-SDC technique on the classification procedure is depicted in Fig. 6. The results assured that the ODLIE-SDC technique can recognize different kinds of class labels accurately.

Table 3 exhibits comprehensive classification outcomes of the ODLIE-SDC technique. The results inferred that the ODLIE-SDC technique reaches effectual results under all aspects. For instance, with 80% of TRS, the ODLIE-SDC technique attains average $accu_y$ of 98.69%, $prec_n$ of 95.01%, $reca_l$ of 94.18%, F_{score} of 94.58%, and MCC of 93.42%. Meanwhile, with 20% of TSS, the ODLIE-SDC method reaches average $accu_y$ of 98.85%, $prec_n$ of 95.19%, $reca_l$ of 94.85%, F_{score} of 94.96%, and MCC of 94.01%.

TABLE 3. Classification outcome of the ODLIE-SDC system with a distinct measure.

Labels	Accuracy	Precision	Recall	F-Score	MCC
Training Phase (80%)					
Abnormal-1	98.99	93.33	94.49	93.91	93.36
Abnormal-2	98.86	93.94	93.00	93.47	92.84
Abnormal-3	99.41	96.40	96.40	96.40	96.08
Abnormal-4	98.54	93.41	88.41	90.84	90.09
Normal	97.67	97.95	98.57	98.26	94.75
Average	98.69	95.01	94.18	94.58	93.42
Testing Phase (20%)					
Abnormal-1	99.06	96.18	91.97	94.03	93.55
Abnormal-2	99.00	90.73	97.86	94.16	93.69
Abnormal-3	99.41	95.92	97.24	96.58	96.26
Abnormal-4	98.65	94.62	88.49	91.45	90.78
Normal	98.13	98.52	98.69	98.61	95.75
Average	98.85	95.19	94.85	94.96	94.01
Training Phase (70%)					
Abnormal-1	98.81	91.63	93.74	92.67	92.03
Abnormal-2	98.98	93.21	95.18	94.18	93.63
Abnormal-3	98.43	91.24	89.78	90.51	89.65
Abnormal-4	98.51	92.09	89.23	90.64	89.85
Normal	97.91	98.42	98.45	98.44	95.28
Average	98.53	93.32	93.28	93.29	92.09
Testing Phase (30%)					
Abnormal-1	98.67	94.74	89.59	92.09	91.41
Abnormal-2	98.67	92.31	92.31	92.31	91.58
Abnormal-3	98.71	91.58	92.04	91.81	91.11
Abnormal-4	99.02	94.04	94.47	94.25	93.72
Normal	98.13	98.31	98.88	98.59	95.79
Average	98.64	94.19	93.46	93.81	92.72

FIGURE 7. TACC and VACC outcome of ODLIE-SDC algorithm.

Eventually, with 70% of TRS, the ODLIE-SDC method gains average $accu_y$ of 98.53%, $prec_n$ of 93.32%, $recal_l$ of 93.28%, F_{score} of 93.29%, and MCC of 92.09%. Finally, with 30% of TSS, the ODLIE-SDC algorithm achieves average $accu_y$ of

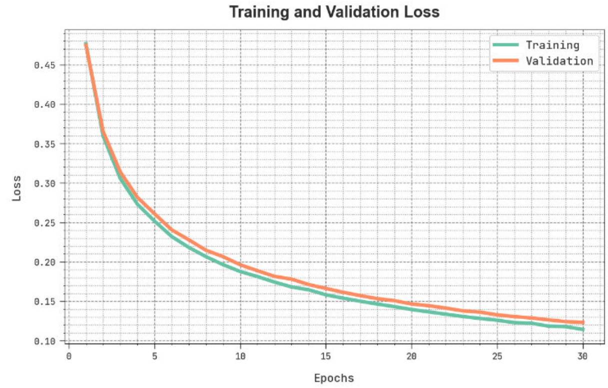


FIGURE 8. TLS and VLS outcome of ODLIE-SDC algorithm.

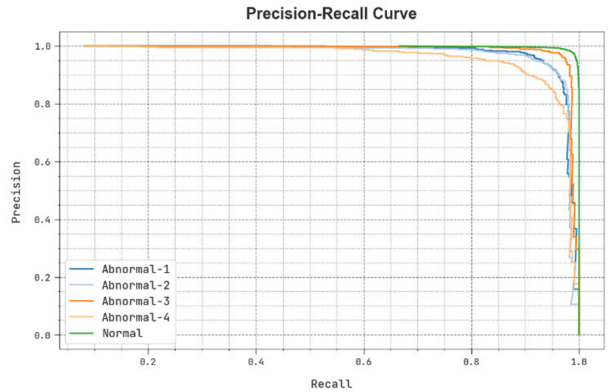


FIGURE 9. The precision-recall outcome of the ODLIE-SDC algorithm.

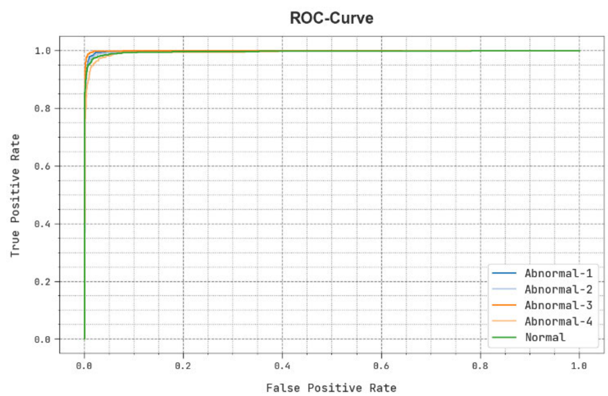


FIGURE 10. ROC outcome of ODLIE-SDC algorithm.

98.64%, $prec_n$ of 94.19%, $recal_l$ of 93.46%, F_{score} of 93.81%, and MCC of 92.72%.

The TACC and VACC of the ODLIE-SDC approach are investigated on classification performance in Fig. 7. The figure displayed that the ODLIE-SDC approach has improved performance with increased values of TACC and VACC. Notably, the ODLIE-SDC methodology has reached maximum TACC outcomes.

The TLS and VLS of the ODLIE-SDC approach are tested on classification performance in Fig. 8. The figure inferred that the ODLIE-SDC system has better performance with the

TABLE 4. Comparative analysis of the ODLIE-SDC system with other recent techniques.

Methods	Accuracy (in %)	Computation Time (in ms)
ODLIE-SDC	98.85	8.95
AISCC-DE2MS Model	95.24	11.13
SCNet Model	85.70	14.18
SCFCNet Model	87.11	14.14
MobileNet Model	88.55	47.63
baseNet Model	88.34	21.12
ERNet Model	90.16	19.46

least values of TLS and VLS. Perceptibly, the ODLIE-SDC method has resulted in reduced VLS outcomes.

A clear precision-recall inspection of the ODLIE-SDC algorithm under the test database is given in Fig. 9. The figure designated that the ODLIE-SDC technique has resulted in enhanced values of precision-recall values under all classes.

The comprehensive ROC study of the ODLIE-SDC method under the test database is depicted in Fig. 10. The outcomes signified the ODLIE-SDC methodology has exposed its capability in classifying distinct classes.

Table 4 depicts the superiority of the ODLIE-SDC method, a widespread comparison study is made in terms of $accu_y$ and computation time (CT) [11].

The results represent that the ODLIE-SDC technique has obtained better performance over other DL models. Based on $accu_y$, the ODLIE-SDC technique has gained improvised $accu_y$ of 98.58% which is considerably higher than the existing models. Similarly, the ODLIE-SDC technique has obtained a CT of 8.95ms which is significantly lower than the compared methods. These results stated the supremacy of the ODLIE-SDC technique in disaster monitoring.

V. CONCLUSION

In this article, we have developed a new ODLIE-SDC method for effectual secure communication and classification processes. To accomplish this, the presented ODLIE-SDC technique designed a hyperchaotic map-based image encryption technique and its optimal keys are produced by the use of the ROA. The image classification process is performed encompassing EfficientNet-B4-CBAM feature extraction and ESAE classification. Finally, the hyperparameter tuning of the EfficientNet-B4-CBAM technique takes place with the BO algorithm. The experimental validation of the ODLIE-SDC method is tested on the AIDER dataset. The comprehensive comparative analysis stated the enhanced performance of the ODLIE-SDC technique over other existing methods.

The ODLIE-SDC technique can protect the data captured and transmitted by drones, avoiding unauthorized individuals or malicious actors from intercepting and decoding the data. This practical implication assures the privacy and security of the data collected by drones. The proposed ODLIE-SDC scheme can be optimized for real-time encryption and decryption, guaranteeing secure and timely communication between the drone and the ground station. This practical implication enables secure and responsive control and monitoring of drone operations. In future, the performance of the ODLIE-SDC method can be improvised by hybrid DL classification models. Besides, future work can explore new architectures, optimization techniques, or novel approaches to improve the security and efficiency of image encryption for drone communication. We also need to investigate the robustness of the ODLIE-SDC scheme against various attacks.

REFERENCES

[1] Y. Harbi, K. Medani, C. Gherbi, O. Senouci, Z. Aliouat, and S. Harous, "A systematic literature review of blockchain technology for Internet of Drones security," *Arabian J. Sci. Eng.*, vol. 48, pp. 1053–1074, Oct. 2022.

[2] S. H. Alsamhi, O. Ma, M. S. Ansari, and F. A. Almalki, "Survey on collaborative smart drones and Internet of Things for improving smartness of smart cities," *IEEE Access*, vol. 7, pp. 128125–128152, 2019.

[3] M. Zhang and X. Li, "Drone-enabled Internet-of-Things relay for environmental monitoring in remote areas without public networks," *IEEE Internet Things J.*, vol. 7, no. 8, pp. 7648–7662, Aug. 2020.

[4] A. Kumar, R. Krishnamurthi, A. Nayyar, A. K. Luhach, M. S. Khan, and A. Singh, "A novel software-defined drone network (SDDN)-based collision avoidance strategies for on-road traffic monitoring and management," *Veh. Commun.*, vol. 28, Apr. 2021, Art. no. 100313.

[5] M. Aliyari, B. Ashrafi, and Y. Z. Ayele, "Drone-based bridge inspection in harsh operating environment: Risks and safeguards," *Int. J. Transp. Develop. Integr.*, vol. 5, no. 22, pp. 118–135, 2021.

[6] M. R. A. Refaai, D. R. Rinku, I. Thamarai, S. Meera, N. K. Sripada, and S. Yishak, "An enhanced drone technology for detecting the human object in the dense areas using a deep learning model," *Adv. Mater. Sci. Eng.*, vol. 2022, pp. 1–12, Sep. 2022.

[7] C. Wankmüller, M. Kunovjanek, and S. Mayrgündter, "Drones in emergency response—Evidence from cross-border, multi-disciplinary usability tests," *Int. J. Disaster Risk Reduction*, vol. 65, Nov. 2021, Art. no. 102567.

[8] P. L. Mehta, R. Kalra, and R. Prasad, "A backdrop case study of AI-drones in Indian demographic characteristics emphasizing the role of AI in global cities digitalization," *Wireless Pers. Commun.*, vol. 118, no. 1, pp. 301–321, May 2021.

[9] X. Li, "Some problems of deployment and navigation of civilian aerial drones," 2021, *arXiv:2106.13162*.

[10] X. Ren, S. Vashisht, G. S. Aujla, and P. Zhang, "Drone-edge coalesce for energy-aware and sustainable service delivery for smart city applications," *Sustain. Cities Soc.*, vol. 77, Feb. 2022, Art. no. 103505.

[11] F. S. Alrayes, S. S. Alotaibi, K. A. Alissa, M. Maashi, A. Alhogail, N. Alotaibi, H. Mohsen, and A. Motwakel, "Artificial intelligence-based secure communication and classification for drone-enabled emergency monitoring systems," *Drones*, vol. 6, no. 9, p. 222, Aug. 2022.

[12] K. Rabieh, S. Mercan, K. Akkaya, V. Baboolal, and R. S. Aygun, "Privacy-preserving and efficient sharing of drone videos in public safety scenarios using proxy re-encryption," in *Proc. IEEE 21st Int. Conf. Inf. Reuse Integr. Data Sci. (IRI)*, Aug. 2020, pp. 45–52.

[13] P. Y. Ingle, Y. Kim, and Y.-G. Kim, "DVS: A drone video synopsis towards storing and analyzing drone surveillance data in smart cities," *Systems*, vol. 10, no. 5, p. 170, Sep. 2022.

[14] M. Kunovjanek and C. Wankmüller, "Containing the COVID-19 pandemic with drones—Feasibility of a drone enabled back-up transport system," *Transp. Policy*, vol. 106, pp. 141–152, Jun. 2021.

[15] Y. Miao, J. Xu, M. Chen, and K. Hwang, "Drone enabled smart air-agent for 6G network," in *Proc. IEEE Int. Conf. Commun.*, May 2022, pp. 1–6.

[16] P. L. Nedelea, T. O. Popa, E. Manolescu, C. Bouros, G. Grigorasi, D. Andritoi, C. Pascale, A. Andrei, and D. C. Cimpoesu, "Telemedicine system applicability using drones in pandemic emergency medical situations," *Electronics*, vol. 11, no. 14, p. 2160, Jul. 2022.

[17] K. Mershad, "PROACT: Parallel multi-miner proof of accumulated trust protocol for Internet of Drones," *Veh. Commun.*, vol. 36, Aug. 2022, Art. no. 100495.

[18] M. Kaur and D. Singh, "Multiobjective evolutionary optimization techniques based hyperchaotic map and their applications in image encryption," *Multidimensional Syst. Signal Process.*, vol. 32, no. 1, pp. 281–301, Jan. 2021.

[19] N. F. Abdulsattar, D. A. Mohammed, A. Alkhayyat, S. Z. Hamed, H. M. Hariz, A. S. Abosinnee, A. H. Abbas, M. H. Hassan, M. A. Jubair, F. H. Abbas, A. D. Algarni, N. F. Soliman, and W. El-Shafai, ''Privacy-preserving mobility model and optimization-based advanced cluster head selection (P2O-ACH) for vehicular ad hoc networks,'' *Electronics*, vol. 11, no. 24, p. 4163, Dec. 2022.

[20] X. Zhu, X. Zhang, Z. Sun, Y. Zheng, S. Su, and F. Chen, ''Identification of oil tea (*Camellia oleifera* C. Abel) cultivars using EfficientNet-B4 CNN model with attention mechanism,'' *Forests*, vol. 13, no. 1, p. 1, Dec. 2021.

[21] W. Jia, C. Xiu-Yun, Z. Hao, X. Li-Dong, L. Hang, and D. Si-Hao, ''Hyper-parameter optimization for machine learning models based on Bayesian optimization,'' *J. Electron. Sci. Technol.*, vol. 17, no. 1, pp. 26–40, 2019.

[22] B. Liu, Y. Chai, Y. Jiang, and Y. Wang, ''Industrial fault detection based on discriminant enhanced stacking auto-encoder model,'' *Electronics*, vol. 11, no. 23, p. 3993, Dec. 2022.

[23] K. Christos. *AIDER (Aerial Image Dataset for Emergency Response Applications)*. Accessed: Jun. 14, 2023. [Online]. Available: https://zenodo.org/record/3888300#.Ys_0h3ZByUk

N. KANNAIYA RAJA received the M.E. degree from Anna University and the Ph.D. degree from Manonmaniam Sundaranar University. He is a Professor with the Computer Science Department, Ambo University, HH-Campus, Ambo, Ethiopia. He is also a researcher in data science, natural language processing, and computer networks.

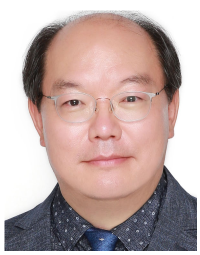
E. LAXMI LYDIA is a Professor of Department of Computer Science and Engineering, Vignan's Institute of Information Technology, India. She is a big data analytics online trainer for the international training organisation and she has presented various webinars on big data analytics. She is certified by Microsoft Certified Solution Developer (MCSD). She published more than 100 research papers in international journals in the area big data analytics and data sciences and she published ten research papers in international conference proceedings. She is an author for the big data analytics book and currently she is working on government DST funded project and she holds a patents.

THUMPALA ARCHANA ACHARYA received the M.B.A., S.E.T., M.Phil., and Ph.D. degrees. She is an Associate Professor with the Vignan's Institute of Information Technology. She completed a project on Sources and Applications of Funds in Public Sector Company (at post graduation), Financial Performance of Foreign Banks (at M.Phil.), and Business Process Re-Engineering in Commercial Banks (at Ph.D.). She has ten years of experience in teaching, 14 years of experience in research, and eight years of experience in different roles in academia administration. She handled courses related to banking and insurance management, international financial management, financial risk management, financial management, accounting for managers, for master's students; and managerial economics and financial analysis, management science, and entrepreneurship development, for bachelor's students. Her four publications have been indexed in international databases, such as Scopus and SCI. She has participated in and presented more than ten papers in international and national conferences. She has published 20 research papers in international and national reputed journals in the field of banking and application of technology in banking sector. In the field of higher education and corporate skills, she has published two book chapters at national level and applied for four projects, out of which one funded project Chunauthi 2.0 has been sanctioned. She has guided more than 75 projects at master's level. As part of various roles of administration, she is the Coordinator of APSSDC and ISRO-IIRS Outreach Programs and a member of the Idea Innovation Centre. As part of coordinator ship organized more than 20 workshops for B.Tech. students from APSSDC, 11 programs from ISRO, and six workshops of institute innovation cell. Her areas of research interests include banking–new application technologies, business analytics, big data, block chain technology, and soft computing techniques. She is a Life Member of CEGR and Institute of Engineers.

K. RADHIKA received the B.Tech. degree in EEE from V. R. Sidhartha Engineering College, Vijayawada, Andhra Pradesh, India, the master's degree in computer science and engineering (CSE) from JNTU, Hyderabad, and the Ph.D. degree from Osmania University, for her research work entitled ''Efficient Mobile-Centric Vertical Hand-off Decision Models for Heterogeneous Wireless Networks.''

She is currently a Professor with the Department of Artificial Intelligence and Data Science, Chaitanya Bharathi Institute of Technology, Hyderabad, Telangana, India. She has a total of about 28 years of experience in both industry and academia. She was the former Head of the Department of Information Technology, CBIT. She was instrumental in establishing a laboratory for big data analytics with the sponsorship of AICTE and another laboratory for the Internet of Things apart from modernizing the existing laboratories and creating other infrastructural facilities in the department. She has published around 20 research papers in national/international journals and conferences. She is currently guiding eight Ph.D. scholars. Her research interests include mobile computing, cloud computing, machine learning, data science, decision support systems, including game theory, multiple criteria decision making-MCDM, analytic hierarchy process-AHP, PCA for dimensionality reduction, and blockchain technology. She is a member of various professional bodies and was also a panel member and the session chair of various national and international conferences.

EUNMOK YANG received the M.S. degree from the Department of Computer Engineering, Kongju National University, Gongju, South Korea, in 2002, and the Ph.D. degree from the Department of Mathematics, Kongju National University, in 2016. In 2016, he was with the UbiTech Research Center. Since 2017, he has been a Researcher with Soongsil University's Industry–University Cooperation Foundation. Since 2020, he has been a Research Professor with the Department of Financial Information Security, Kookmin University. His research interests include security, artificial intelligence, data mining, machine learning, and network security.



OKYEON YI received the Ph.D. degree in mathematics from the University of Kentucky, in 1996. From July 1999 to August 2001, he was with the Electronics and Telecommunications Research Institute, Daejeon, South Korea, as a Team Leader of mobile information security. He is currently a Professor with Kookmin University, Seoul, South Korea. His research interests include the 5G, 5G+, 6G mobile telecommunication security, drone security, quantum cryptographic module security, quantum key distribution security, and post quantum cryptography security.