



ARTICLE

Computational Intelligence Driven Secure Unmanned Aerial Vehicle Image Classification in Smart City Environment

Firas Abedi¹, Hayder M. A. Ghanimi², Abeer D. Algarni³, Naglaa F. Soliman^{3,*}, Walid El-Shafai^{4,5}, Ali Hashim Abbas⁶, Zahraa H. Kareem⁷, Hussein Muhi Hariz⁸ and Ahmed Alkhayyat⁹

¹Department of Mathematics, College of Education, Al-Zahraa University for Women, Karbala, Iraq

²Biomedical Engineering Department, College of Engineering, University of Warith Al-Anbiyaa, Karbala, Iraq

³Department of Information Technology, College of Computer and Information Sciences, Princess Nourah bint Abdulrahman University, P.O. Box 84428, Riyadh, 11671, Saudi Arabia

⁴Security Engineering Lab, Computer Science Department, Prince Sultan University, Riyadh, 11586, Saudi Arabia

⁵Department of Electronics and Electrical Communications Engineering, Faculty of Electronic Engineering, Menoufia University, Menouf, 32952, Egypt

⁶College of Information Technology, Imam Jaafar Al-Sadiq University, Al-Muthanna, 66002, Iraq

⁷Department of Medical Instrumentation Techniques Engineering, Al-Mustaqbal University College, Hillah, 51001, Iraq

⁸Computer Engineering Department, Mazaya University College, Dhi Qar, Iraq

⁹College of Technical Engineering, The Islamic University, Najaf, Iraq

*Corresponding Author: Naglaa F. Soliman. Email: nfsoliman@pnu.edu.sa

Received: 05 January 2023 Accepted: 11 April 2023 Published: 09 November 2023

ABSTRACT

Computational intelligence (CI) is a group of nature-simulated computational models and processes for addressing difficult real-life problems. The CI is useful in the UAV domain as it produces efficient, precise, and rapid solutions. Besides, unmanned aerial vehicles (UAV) developed a hot research topic in the smart city environment. Despite the benefits of UAVs, security remains a major challenging issue. In addition, deep learning (DL) enabled image classification is useful for several applications such as land cover classification, smart buildings, etc. This paper proposes novel meta-heuristics with a deep learning-driven secure UAV image classification (MDLS-UAVIC) model in a smart city environment. The major purpose of the MDLS-UAVIC algorithm is to securely encrypt the images and classify them into distinct class labels. The proposed MDLS-UAVIC model follows a two-stage process: encryption and image classification. The encryption technique for image encryption effectively encrypts the UAV images. Next, the image classification process involves an Xception-based deep convolutional neural network for the feature extraction process. Finally, shuffled shepherd optimization (SSO) with a recurrent neural network (RNN) model is applied for UAV image classification, showing the novelty of the work. The experimental validation of the MDLS-UAVIC approach is tested utilizing a benchmark dataset, and the outcomes are examined in various measures. It achieved a high accuracy of 98%.

KEYWORDS

Computational intelligence; unmanned aerial vehicles; deep learning; metaheuristics; smart city; image encryption; image classification



1 Introduction

The concept of a smart city has become a prominent research field worldwide. The number of stationary sensors and the amount of data gathered by a surveillance camera and other devices placed in a smart city are massive. Using a mobile platform to replace them might decrease resource and energy costs [1]. The smart city paradigm directly connects the telecommunication industry to sustainable economic growth and better living standards with advanced techniques such as unmanned aerial vehicles (UAVs). Over the last few years, the advancement of UAVs has gained considerable attention due to essential characteristics like the ability to establish line of sight (LOS) links with the user, mobility, and easy deployment [2]. Generally, UAVs are categorized into fixed-wing and rotary-wing UAVs. All kinds of UAV are adapted to a particular kind of application. For instance, fixed-wing UAV is best suited for the type of mission whereby stationarity is not needed, for example, military applications, namely surveillance and attack. But rotary-wing UAV has increasingly complex aerodynamics [3]. Also, they can remain stationary at a specified location, but they cannot implement long-range missions [4]. Affordability and ease of use are two major elements for the extensive usage of UAVs in military and civilian applications [5]. Images taken through UAVs are utilized for geographical information system databases, data collection for agricultural mapping, land use, automatic decision-making, urban planning, environmental monitoring and assessment, and land cover detection [6]. Because of the quality of UAV images at present, abstracting reliable characteristics for forming data collection is less of a problem. Illustration of these features island cover characteristics (spectral and geometrical) from hyperspectral data and Light Detection and Ranging (LiDAR) [7]. In addition, the amalgamation of various sources (passive or active sensors) or multimodal data (data with distinct features) is suggested for improving land cover categorisation.

Over the past few years, the arrival of deep learning (DL) methods has provided strong and brilliant techniques for enhancing the mapping of the earth's surface [8]. DL is an artificial neural network (ANN) technique of deeper combinations and numerous hidden layers accountable for maximizing and returning superior learning models over a general ANN. A splendid volume of revision materials exists in the scientific chronicles describing DL-related methods, common usage, and its historical evolution, along with that briefing functions and networks [9]. In recent years as computer processing and labeled instances (i.e., samples) are highly more accessible, the outcomes of deep neural networks (DNNs) raise in image-processing applications. DNN has been implemented in data-driven approaches successfully. But more should be covered under this to understand its efficiency and restrictions [10]. From this point of view, various studies on the application of DL in remote sensing have been advanced in general as well as in specific contexts to describe its significance in a better way.

There are some restrictions that can be associated with the use of computational intelligence techniques for secure unmanned aerial vehicle (UAV) image classification in a smart city environment:

- Limited availability of UAVs: UAVs may not be readily available or accessible in all smart city environments, which can limit the effectiveness and feasibility of implementing a UAV image classification system.
- Cost: The cost of acquiring and maintaining UAVs and associated equipment can be prohibitive for some cities and organizations, especially for those with limited budgets.
- Limited battery life and range: UAVs have limited battery life and range, which can restrict the amount of time they can be used for image classification and the distance they can travel to collect data.

- Technical expertise: Implementing a UAV image classification system requires technical expertise in areas such as machine learning, computer vision, and UAV operation. This expertise may not be available or accessible to all organizations.
- Public perception: The use of UAVs in a smart city environment may be perceived as intrusive or invasive by members of the public, which can lead to opposition and negative public sentiment.
- Weather conditions: Adverse weather conditions such as strong winds, heavy rain, and low visibility can restrict the use of UAVs, limiting the reliability and effectiveness of image classification systems.
- Regulatory challenges: The use of UAVs is subject to regulatory challenges, including airspace regulations, licensing requirements, and data privacy laws. Compliance with these regulations can be time-consuming and complex.

This study designs a novel metaheuristic with a deep learning-driven certain UAV image classification (MDLS-UAVIC) model in a smart city environment. The proposed MDLS-UAVIC model uses the signcryption technique to encrypt UAV images effectively. Next, the image classification process involves an Xception-based deep convolutional neural network for the feature extraction process. Finally, shuffled shepherd optimization with a recurrent neural network model is applied for UAV image classification. The experimental validation of the MDLS-UAVIC approach was tested employing a benchmark dataset, and the outcomes are examined in various measures.

2 Related Works

This section offers a brief review of existing UAV-based image classifier approaches. Raj [11] employed the blockchain method to gather healthcare information from the user and save them on a nearby server is presented. The UAV communicates with body sensor hives (BSH) via a low power secured method. This technique can be recognized by a token where the UAV establishes relationships with the BSH. Shibli et al. [12] introduced an AI drone-based encrypted ML of image classifier with a pertained CNN and image encrypt-decrypt using XOR-Secret-Key block cipher cryptology and singular value decomposition (SVD). Firstly, a pre-trained convolution neural network (CNN) is widely employed for extracting and classifying image features exploiting ML training tool features.

The researchers in [13] focused on the structure of the share creation (SC) system using the social spider optimization based ECC method named SC-SSOECC for a secured image communication system in UAV. Initially, the presented method separates the color bands (RGB) for all the images. Next, the generation of the SC system occurs for all the images, making it difficult for the hacker to retrieve the original images. Mardiyanto et al. [14] proposed an analogue video communication security for UAVs using assembling arbitrary image pieces using the Linear Feedback Shift Register approach and image encryption technique with Pseudo Random Number Generator. The LFSR is a seed that acts as a key to the randomization pattern from the image processed by software and taken by the camera on Raspberry Pi.

Abualsaud [15] classified and analyzed the study on the UAV IoT framework and recognized the solution to the problem associated with the security comprising privacy of the framework. In this study, an optimal solution for different reliability and security problems in UAV-assisted IoT applications is presented that uses the combination of different techniques merging blockchain-based techniques. Punithavathi et al. [16] introduced an optimum dense convolution network (DenseNet) using a BiLSTM-based image classifier method named optimum DenseNet (ODN)-Bi-LSTM for UAV-based ad-hoc network. Kumar et al. [17] projected a secure privacy-preserving framework (SP2F)

for intelligent agriculture UAV technique. The presented architecture contains a DL-based anomaly detection technique and a two-level privacy system.

3 The Proposed Model

This study establishes a novel MDLS-UAVIC algorithm to securely encrypt the images and classify them into distinct class labels in the smart city environment. The MDLS-UAVIC model encompasses a series of processes: signcryption, Xception-based feature extraction, RNN classification, and SSO-based hyperparameter optimization. Fig. 1 illustrates the overall MDLS-UAVIC technique.

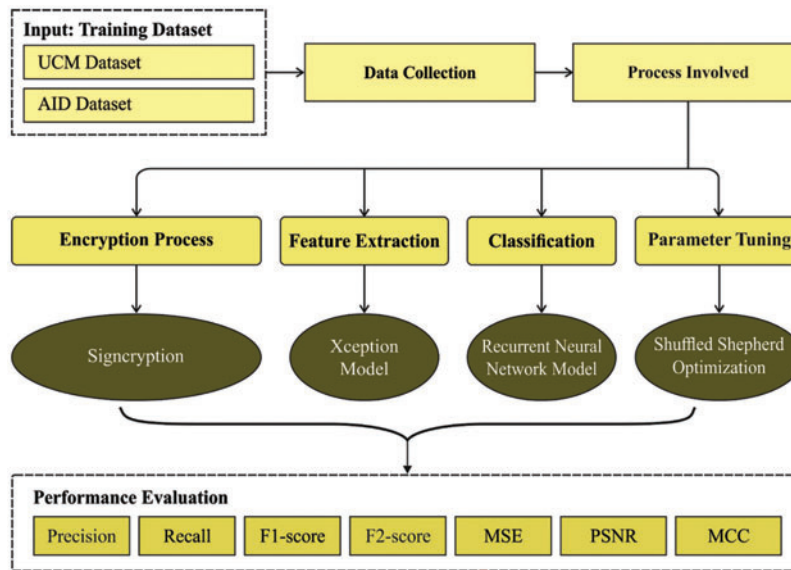


Figure 1: Working process of MDLS-UAVIC technique

3.1 Image Encryption Module

At the primary level, the proposed MDLS-UAVIC approach uses encryption techniques to encrypt the UAV images effectively. The security system is a public key encryption technique using a digital signature that might increase availability, confidentiality, integrity, authenticity, and non-repudiation [18]. A single session key is used again for encryption to obtain an effective presentation for name encryption compared to the encryption technique. The encryption technique has three phases: encryption, des encryption, and key generation. A signature provides authenticity, and encryption provides confidentiality simultaneously. It includes encryption, des encryption, generation of keys, and parameter initialization phase. Initially, the signature-based security analysis assigns certain parameters, namely large prime numbers for sender and receiver keys, key generation, and hash values. The initial parameter is Sr_1 , Su_1 , Rr_2 , and Ru_1 .

- Signcryption Phase

(i) This encryption technique transfers the information to the receiver after security analysis; at this point, motion vectors, hash, and one-key hash value-based encryption data are considered. The transformation of plain data to ciphered data can be defined as follows. Firstly, the sender transmits the data with a proper value A ranging from $[1 \dots PF - 1]$.

(ii) Evaluate hash values of the sender applied by the receiver Ru_2 and A . The output O_H_o of the hash value is 128-bit. The mathematical expression of the hash value has been given in the following:

$$O_H_o = HASH (Ru_2^A * mod PN) . \quad (1)$$

iii) The resultant value of 128 bits is divided into 2 bits of sixty-four bits, as O_H_o1 and O_H_o2 .

iv) The sender encrypts the data for encryption E and O_H_o1 . The cipher information C_i is defined in the following:

$$C_i = EO_H_o1 (info) . \quad (2)$$

v) Next, the O_H_o2 value is employed efficiently from the one-key hash function K_H_o to hash the information that results in a 128-bit hash as follows:

$$F = K_H_o2 (info) . \quad (3)$$

vi) Lastly, the encryption of the information is evaluated, and the cipher data are given in the following:

$$S = A / (F + A_{O_H_o1})^{mod PF} \quad (4)$$

vii) From the calculation, three different values, F and C_i , are transmitted to the sender as well as the receiver.

- **Unsignryption Phase**

i) In the receiver end, the decryption method, that is, the unsignryption technique, is implemented afterwards after receiving the encrypted information, that is, F and C_i . The receiver is capable of decrypting the subsequent steps.

ii) The receiver keys Su_1 and Sr_1 with encryption data are transformed to 128-bit output decrypted data.

$$O_H_o = HASH ((Ru_1 * i^F) * Sr_2 mod PN) . \quad (5)$$

iii) The inverse operation of encryption can be executed; that is, 128-bit data is separated into sixty-four bits of 2 key pairs.

$$O_H_o1 \text{ and } O_H_o2 . \quad (6)$$

iv) The receiver uses the output key O_H_o1 for decrypting the cipher data C_i , and then the decrypted data is described by $= DO_H_o1 (C_i)$.

v) After completing the abovementioned process, valid data had attained as:

$$K_H_o O_H_o2 (info) = F . \quad (7)$$

vi) If it is equal, the message is considered a verified message; otherwise, it is invalid.

3.2 Image Classification Module

For the image classification process, the MDLS-UAVIC approach comprises feature extraction, classification, and parameter optimization. The working process of each module is elaborated in the following sections.

3.2.1 Feature Extraction

The Xception approach is used in this work to develop a helpful feature vector group. Xception [19] represents “extreme inception”. Xception was proposed in 2016. The Xception module is thirty-six layers deep, except for the fully connected (FC) layer at the end. Different from inceptionV3, the Xception parcel input record as a compacted lump also map the spatial connection for all the channels separately, and a 1×1 depthwise convolutional layer is implemented for catching cross channel relationship. This work introduces a pre-trained Xception method (trained on ImageNet data). Then, the module is fine-tuned on UAV images. During Fine-tuning, Xception gives an input image of $224 \times 224 \times 3$ that goes with shortcuts and a depthwise separable layer.

3.2.2 Image Classification Using RNN Model

For the image classification procedure, the derived features are passed into the RNN approach, which assigns proper class labels. RNN is extensively utilized for analyzing sequence datasets, namely machine translation and speech recognition, considering that sequential dataset $x = (x_1, x_2, \dots, x_T)$, whereas $x_t, t \in \{1, 2, \dots, T\}$ denotes the data at t -th time step. While using RNN to HSI classifications, x_t corresponds to the spectral values at t -th band. In RNN, the output of the hidden state at time t can be expressed as follows [20]:

$$h_t = \varphi (W_{hi}x_t + W_{hh}h_{t-1} + b_h) \quad (8)$$

whereas b_h represents a bias vector, φ denotes a non-linear activation function, namely hyperbolic tangent or logistic sigmoid functions, W_{hi} and W_{hh} denote the weight matrix from the existing input to hidden layers and preceding hidden layers to existing hidden layers, h_{t-1} indicates the output of hidden state at the prior time, correspondingly. We observed from the formula that the context relationship in the time domain would be created using a recurrent connection. Usually, h_T captures maximum time data for the sequential dataset. For classifier tasks, h_T is frequently fed into the output layer, in addition to the possibility that a softmax function derives the sequence belonging to i -th class. This process is expressed in the following:

$$O_T = W_{oh}h_T + b_o$$

$$P(\tilde{y} = i|\theta, b) = \frac{e^{\theta_i O_T + b_i}}{\sum_{j=1}^c e^{\theta_j O_T + b_j}} \quad (9)$$

Now W_{oh} denotes the weight matrixes from hidden to output layers, b_o indicates a bias vector, θ and b represent variables of softmax function, C signifies the class count to differentiate. The succeeding loss function is given as follows:

$$\mathcal{L} = -\frac{1}{N} \sum_{i=1}^N [y_i \log(\tilde{y}_i) + (1 - y_i) \log(1 - \tilde{y}_i)] \quad (10)$$

Here, N indicates the number of trained instances, \tilde{y}_i and y_i corresponding to the predicted and true labels of the i -th trained instance.

3.2.3 Hyperparameter Optimization

Finally, the SSO technique has been employed to adjust the RNN model’s hyperparameters properly. SSO technique is a multi-community (MC) population-based metaheuristic algorithm that imitates the nature of a shepherd. The steps included in the SSO approach are shown in [21]. Initially, the SSO approach starts by arbitrarily creating members of the community (MOC) in the search space

as follows:

$$MOC_{ij}^0 = MOC_{\min} + rand \times (MOC_{\max} - MOC_{\min});$$

$$i = 1, 2, \dots, m \text{ and } j = 1, 2, \dots, n \tag{11}$$

Here, *rand* indicates arbitrary number lies within [0, 1]; MOC_{\min} and MOC_{\max} correspondingly signify lower and upper limits; *m* denotes community amount, and *n* indicates the number of members. With this regard, it is considered that the total amount of members of the community can be obtained using the following equation:

$$nMC = m \times n \tag{12}$$

In the shuffling method, the *m* member of the community is selected based on its objective function and arranged randomly in the first column of the MC matrix as the first members of the community. Next, generate the second column of MC; the *m* member is chosen corresponding to the preceding step and arranged randomly in the column. The process is implemented in *n* time separately until the MC matrix is generated as:

$$MC = \begin{bmatrix} MOC_{1,1} & MOC_{1,2} & \dots & MOC_{1,j} & \dots & MOC_{1,n} \\ MOC_{2,1} & MOC_{2,2} & \dots & MOC_{2,j} & \dots & MOC_{2,n} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ MOC_{i,1} & MOC_{i,2} & \dots & MOC_{i,j} & \dots & MOC_{i,n} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ MOC_{m,1} & MOC_{m,2} & \dots & MOC_{m,j} & \dots & MOC_{m,n} \end{bmatrix} \tag{13}$$

A step size of motion for each community member can be estimated based on the 2 vectors. It is expressed in the following:

$$stepsize_{i,j} = stepsize_{i,j}^{Worse} + stepsize_{i,j}^{Better} \quad i = 1, 2, \dots, m \text{ and } j = 1, 2, \dots, n \tag{14}$$

whereas $stepsize_{i,j}^{Worse}$ and $stepsize_{i,j}^{Better}$ are defined as follows:

$$stepsize_{i,j}^{Worse} = \alpha \times rand_1 \times (MOC_{i,w} - MOC_{i,j}) \tag{15}$$

$$stepsize_{i,j}^{Better} = \beta \times rand_2 \times (MOC_{i,b} - MOC_{i,j}) \tag{16}$$

Now, $rand_1$ and $rand_2$ characterize arbitrary vectors; $MOC_{i,w}$ (chosen sheep) and $MOC_{i,b}$ (chosen horse) denote optimum and worse member-based objective function values associated with $MOC_{i,j}$ (shepherd). It is worth declaring that the primary member of *ith* community ($MOC_{i,1}$) does not take a member better than itself. Hence, $stepsize_{i,1}^{Better}$ is equal to zero. On the other hand, $MOC_{i,n}$ does not have a member worse than itself because of the last member of *i-th* community. Therefore, $stepsize_{i,1}^{Worse}$ is equal to zero. Moreover, α and β indicate factors that manage the exploitation and exploration stage. It is defined as follows:

$$\alpha = \alpha_0 - \alpha_0 \times t; \quad t = \frac{\text{iteration}}{\text{Max iteration}} \tag{17}$$

$$\beta = \beta_0 + (\beta_{\max} - \beta_0) \times t \tag{18}$$

According to the previous step, the novel position of MOC_{ij} can be estimated as follows. Later, the position of MOC_{ij} is upgraded, or else the objective old function value can be given as:

$$\text{newMOC}_{ij} = MOC_{ij} + \text{stepsize}_{ij} \quad (19)$$

The optimisation process would be terminated when the predetermined iteration number is reached, or the ending conditions are accomplished. Otherwise, it returns to step 2 for the new iteration. The SSO method progresses a fitness function (FF) for attaining effective classification efficiency. It resolves the positive integer for representing the best performance of the candidate solution.

$$\begin{aligned} \text{fitness}(x_i) &= \text{ClassifierErrorRate}(x_i) \\ &= \frac{\text{number of misclassified samples}}{\text{Total number of samples}} * 100 \end{aligned} \quad (20)$$

Algorithm 1: Pseudocode of SSO algorithm

Begin

1. Initialization of the problem and determine the parameter.
2. Arbitrarily estimate the group of elements.
3. Category the group elements from the ascending order dependent upon the objective function.
4. Generate the sorted subset was dependent upon 2 stages.
 - i) Create the step size matrix.
 - ii) Create a novel group of elements.
5. Evaluate the novel group of elements.
6. Execute the replacement approach amongst the novel and upgrade the group of elements.
7. Report the optimum element.

End

4 Experimental Validation

The performance validation of the MDLS-UAVIC approach is tested utilizing a benchmark dataset, namely UCM dataset (<http://weegeevision.ucmerced.edu/datasets/landuse.html>) and the AID dataset (<https://captain-whu.github.io/AID/>). The results are investigated under two aspects such as security and image classification. A few sample images are displayed in Fig. 2.

Table 1 provides a qualitative result analysis of the MDLS-UAVIC model on distinct sample test images. The outcomes showed that the MDLS-UAVIC approach has achieved an effective encryption process with maximal values of PSNR and CC under all images. At the same time, the MDLS-UAVIC approach has resulted in lower values of MSE under the very image.

Table 2 illustrates a detailed MSE and PSNR inspection of the MDLS-UAVIC model with existing models under distinct sample images [22]. Fig. 3 reports a comparative MSE assessment of the MDLS-UAVIC approach with recent algorithms under dissimilar images. The figure depicted that the MDLS-UAVIC algorithm has obtained enhanced performance with lower values of MSE. For instance, with sample image 1, the MDLS-UAVIC system has provided a minimal MSE of 0.047, whereas the AIUAV, CSO, and GWO processes have obtained increased MSE of 0.060, 0.189, and 0.288, correspondingly. Also, with sample image 3, the MDLS-UAVIC approach provided the least MSE

of 0.035, but the AIUAV, CSO, and GWO approach obtained maximum MSE of 0.049, 0.206, and 0.237, correspondingly. In addition, with sample image 5, the MDLS-UAVIC algorithm has provided a lesser MSE of 0.108, but the AIUAV, CSO, and GWO methods have gained higher MSE of 0.135, 0.183, and 0.234, correspondingly.

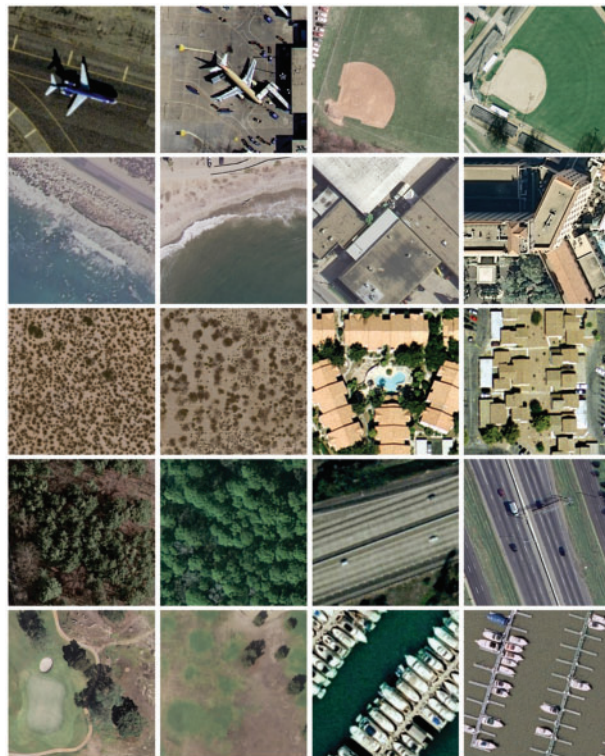

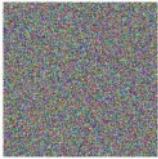


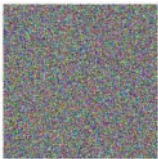



Figure 2: Sample UAVs images

Table 1: Visualization of proposed MDLS-UAVIC methodology on sample images

Input images	Encrypted images	Decrypted images	MSE	PSNR	CC
			0.047	61.410	99.910
			0.059	60.422	99.990

(Continued)

Table 1 (continued)


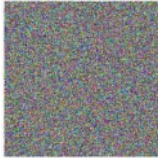


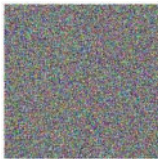

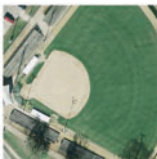

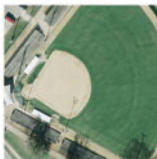
Input images	Encrypted images	Decrypted images	MSE	PSNR	CC
			0.035	62.690	99.910
			0.105	57.919	99.920
			0.108	57.797	99.930

Table 2: MSE and PSNR analysis of MDLS-UAVIC technique with various sample images

Sample images	MDLS-UAVIC		AIUAV model		CSO algorithm		GWO algorithm	
	MSE	PSNR	MSE	PSNR	MSE	PSNR	MSE	PSNR
Sample 1	0.047	61.410	0.060	60.371	0.189	55.373	0.288	53.538
Sample 2	0.059	60.422	0.080	59.089	0.176	55.666	0.232	54.472
Sample 3	0.035	62.690	0.049	61.273	0.206	54.994	0.237	54.391
Sample 4	0.105	57.919	0.130	56.981	0.215	54.815	0.262	53.956
Sample 5	0.108	57.797	0.135	56.827	0.183	55.509	0.234	54.439

A detailed PSNR examination of the MDLS-UAVIC model with current models is provided in Fig. 4. The experimental values specified that the MDLS-UAVIC system had improved PSNR values under every sample image. For sample, with sample image 1, the MDLS-UAVIC model has increased PSNR by 61.410 dB, whereas the AIUAV, CSO, and GWO algorithms have provided reduced PSNR of 60.371, 55.373, and 53.538 dB, respectively. Meanwhile, with sample image 3, the MDLS-UAVIC technique has accessible increased PSNR of 62.690 dB. In contrast, the AIUAV, CSO, and GWO algorithms have provided lesser PSNR of 61.273, 54.994, and 54.391 dB, correspondingly. Eventually, with sample image 5, the MDLS-UAVIC method has enhanced SNR of 57.797 dB, whereas the AIUAV, CSO, and GWO approaches have provided reduced PSNR of 56.827, 55.509, and 54.439 dB.

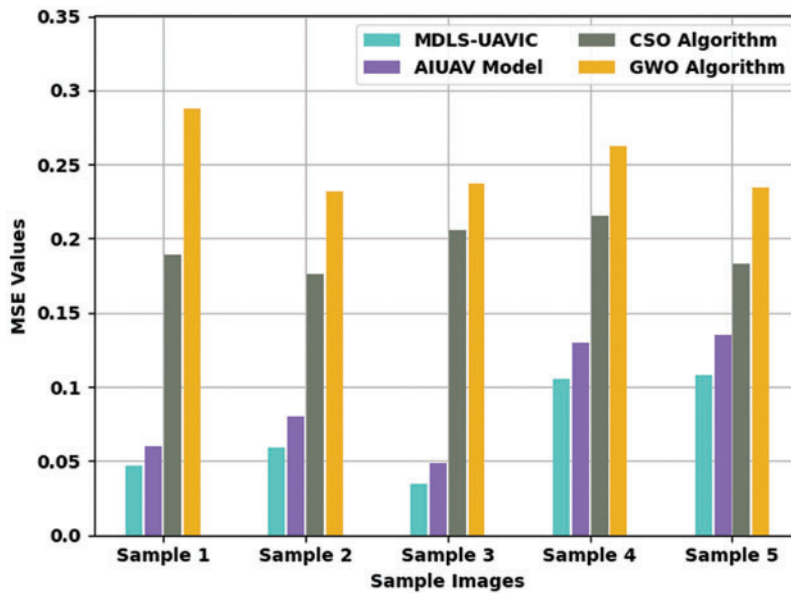


Figure 3: MSE analysis of MDLS-UAVIC approach with distinct sample images

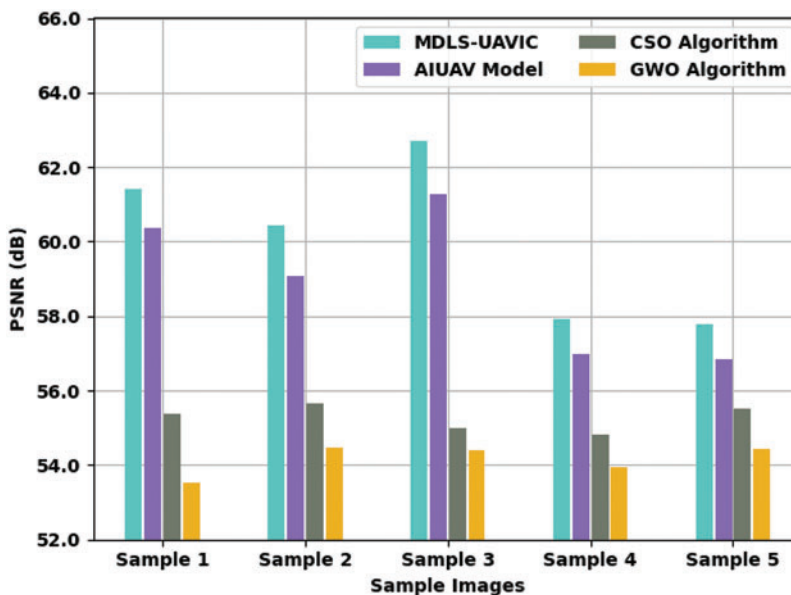


Figure 4: PSNR analysis of MDLS-UAVIC approach with distinct sample images

A detailed CC examination of the MDLS-UAVIC approach with current algorithms is provided in Table 3 and Fig. 5. The experimental values show that the MDLS-UAVIC system has gained enhanced CC values under every sample image. For instance, with sample image 1, the MDLS-UAVIC technique has obtainable increased CC of 99.910, whereas the AIUAV, CSO, and GWO techniques have provided lower CC of 99.700, 99.470, and 99.240, respectively. In the meantime, with sample image 3, the MDLS-UAVIC model has existing increased CC of 99.910, whereas the AIUAV, CSO, and GWO algorithms have provided reduced CC of 99.710, 99.460, and 99.210, respectively. At last, with sample

image 5, the MDLS-UAVIC model has obtainable maximal CC of 99.930, whereas the AIUAV, CSO, and GWO techniques have provided lower CC of 99.650, 99.360, and 99.160, correspondingly.

Table 3: Correlation coefficient (CC) analysis of MDLS-UAVIC system with various sample images

Sample images	MDLS-UAVIC	AIUAV model	CSO algorithm	GWO algorithm
Sample 1	99.910	99.700	99.470	99.240
Sample 2	99.990	99.740	99.500	99.220
Sample 3	99.910	99.710	99.460	99.250
Sample 4	99.920	99.650	99.450	99.210
Sample 5	99.930	99.650	99.360	99.160

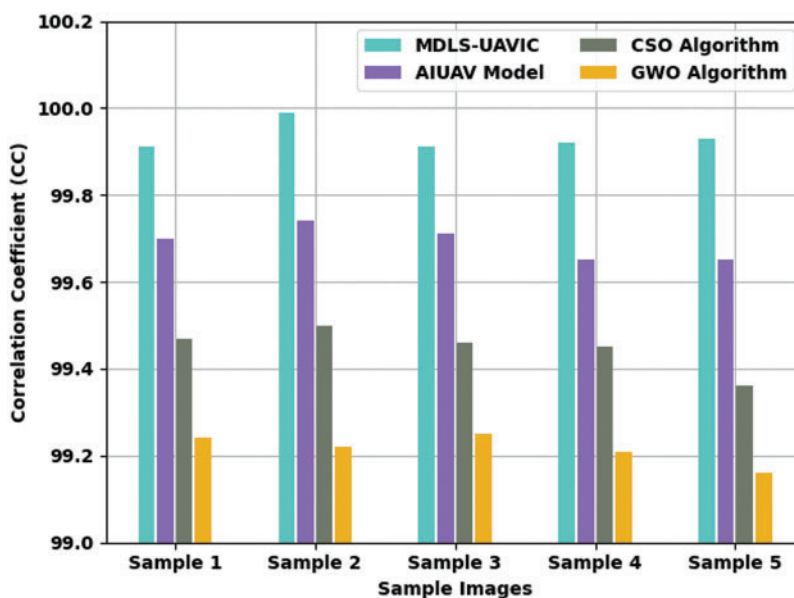


Figure 5: CC analysis of MDLS-UAVIC technique with distinct sample images

Table 4 and Fig. 6 define a comparative CT assessment of the MDLS-UAVIC approach with recent models under distinct images. The figure depicted that the MDLS-UAVIC process has gained enhanced performance with lower values of CT. With sample image 1, the MDLS-UAVIC technique has provided minimal CT of 1.154 s, whereas the AIUAV, CSO, and GWO algorithms have obtained increased CT of 1.449, 2.056, and 2.379 s, correspondingly. Likewise, with sample image 3, the MDLS-UAVIC technique has provided the least CT of 1.411 s, whereas the AIUAV, CSO, and GWO algorithms have obtained maximum CT of 1.802, 2.160 and 2.213 s, respectively. Additionally, with sample image 5, the MDLS-UAVIC model has provided minimal CT of 1.166 s, whereas the AIUAV, CSO, and GWO algorithms have obtained higher CT of 1.682, 1.873, and 2.125 s, correspondingly.

Table 4: Computation time analysis of MDLS-UAVIC technique with various sample images

Sample images	MDLS-UAVIC	AIUAV model	CSO algorithm	GWO algorithm
Sample 1	1.154	1.449	2.056	2.379
Sample 2	1.126	1.578	1.642	2.063
Sample 3	1.411	1.802	2.160	2.213
Sample 4	0.995	1.471	2.226	2.387
Sample 5	1.166	1.682	1.873	2.125

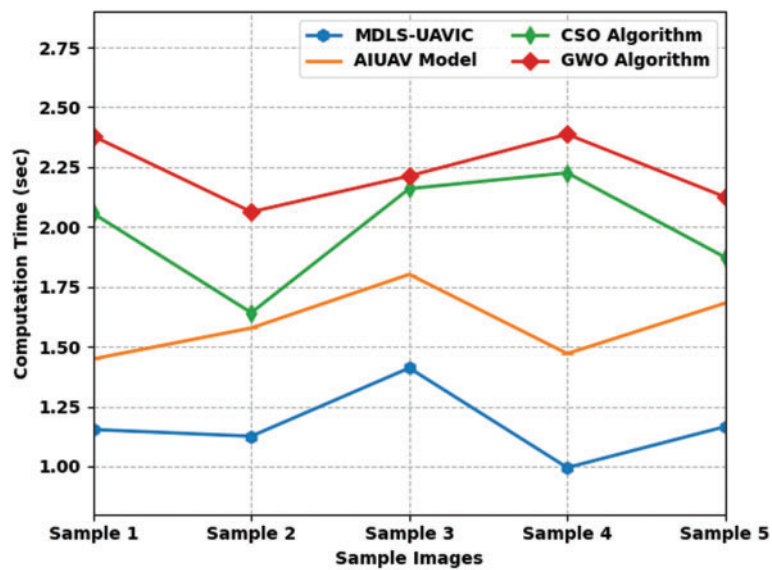


Figure 6: CT analysis of MDLS-UAVIC technique with distinct sample images

Table 5 provides detailed classification results of the MDLS-UAVIC model on the UCM multi-label dataset [23]. Fig. 7 provides a brief $prec_n$ and $reca_t$ examination of the MDLS-UAVIC model with existing models on the test UCM multi-label dataset. The figure indicated that the Conv. NN, CNN-ANN, and CNN-Bil.STM models have provided worse performance with lower values of $prec_n$ and $reca_t$. Besides, the CNN-RNN, GNN-SGAT, and GNN-MLIGAT models have reached slightly increased values of $prec_n$ and $reca_t$. Though the optimal SqueezeNet model has resulted in reasonable $prec_n$ and $reca_t$ of 91.72% and 92.92%, the MDLS-UAVIC model has accomplished maximum $prec_n$ and $reca_t$ values of 92.81% and 94.28%, respectively.

Table 5: Comparative analysis of MDLS-UAVIC technique with recent algorithms on UCM multi-label dataset

Methods	Precision	Recall	F1-Score	F2-Score
Conv. NN	79.91	83.20	80.56	79.36
CNN-ANN	77.90	83.97	80.30	80.69

(Continued)

Table 5 (continued)

Methods	Precision	Recall	F1-Score	F2-Score
CNN-Bil.STM	79.87	84.13	80.52	81.18
CNN-RNN	87.79	86.32	84.99	86.96
GNN-SGAT	87.04	87.56	87.44	86.16
GNN-MLIGAT	87.36	89.75	85.88	88.13
Optimal SqueezeNet	91.72	92.92	94.60	93.41
MDLS-UAVIC	92.81	94.28	95.93	94.32

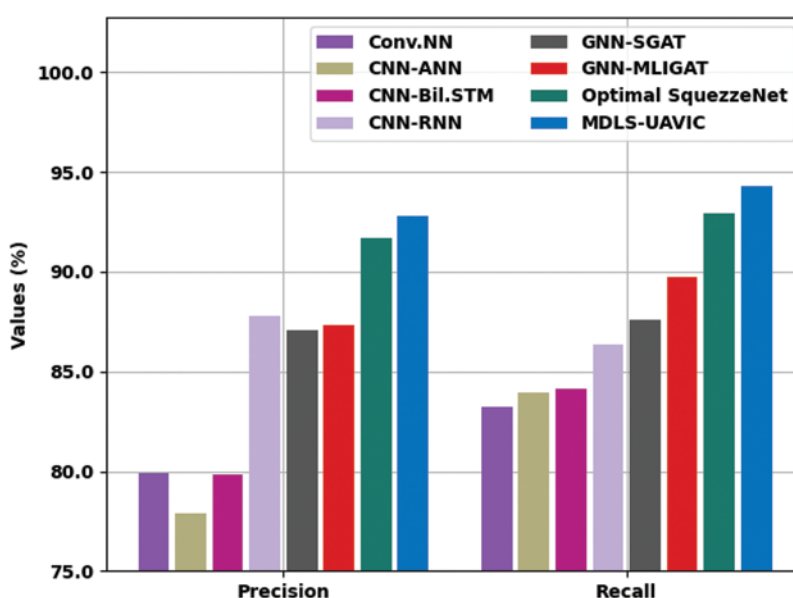
**Figure 7:** $prec_n$ and $reca_l$ analysis of MDLS-UAVIC technique on UCM multi-label dataset

Fig. 8 demonstrates a brief $F1_{score}$ and $F2_{score}$ analysis of the MDLS-UAVIC approach with existing models on the test UCM multi-label dataset. The figure indicated that the Conv. NN, CNN-ANN, and CNN-Bil.STM models have provided worse performance with lower values of $F1_{score}$ and $F2_{score}$. In addition, the CNN-RNN, GNN-SGAT, and GNN-MLIGAT models have attained somewhat increased values of $F1_{score}$ and $F2_{score}$. But, the optimal SqueezeNet model has resulted in reasonable $F1_{score}$ and $F2_{score}$ of 94.60% and 93.41%, the MDLS-UAVIC model has accomplished maximal $F1_{score}$ and $F2_{score}$ values of 95.93% and 94.32%, correspondingly.

Table 6 provides detailed classification results of the MDLS-UAVIC system on the AID multi-label dataset. The results indicated that the Conv. NN, CNN-ANN, and CNN-Bil.STM models have provided worse performance with lower values of $prec_n$ and $reca_l$. Also, the CNN-RNN, GNN-SGAT, and GNN-MLIGAT models have reached slightly increased values of $prec_n$ and $reca_l$. The optimal SqueezeNet model has resulted in reasonable $prec_n$ and $reca_l$ of 93.10% and 94.63%, the MDLS-UAVIC model has accomplished maximum $prec_n$ and $reca_l$ values of 94.46% and 95.82%, respectively. Next, the optimal SqueezeNet model has resulted in reasonable $F1_{score}$ and $F2_{score}$ of 92.14% and 93.24%, and

the MDLS-UAVIC model has accomplished maximum $F1_{score}$ and $F2_{score}$ values of 93.66% and 94.32%, respectively.

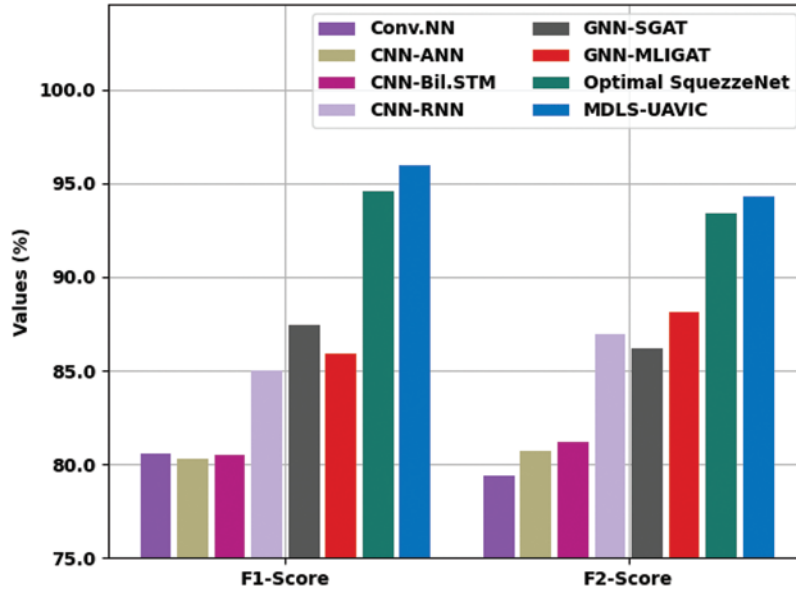


Figure 8: $F1_{score}$ and $F2_{score}$ analysis of MDLS-UAVIC technique on UCM multi-label dataset

Table 6: Comparative analysis of MDLS-UAVIC technique with recent algorithms on AID multi-label dataset

Methods	Precision	Recall	F1-Score	F2-Score
Conv. NN	87.20	87.38	86.63	85.30
CNN-ANN	85.58	88.36	84.75	86.86
CNN-Bil.STM	87.78	88.10	85.83	87.53
CNN-RNN	89.73	90.15	88.83	89.60
GNN-SGAT	89.94	90.64	88.00	89.44
GNN-MLIGAT	90.97	90.31	87.92	88.83
Optimal SqueezeNet	93.10	94.63	92.14	93.24
MDLS-UAVIC	94.46	95.82	93.66	94.32

After detecting the results and discussion, it has been concluded that the MDLS-UAVIC approach has accomplished maximum classification performance over the other models.

5 Conclusion

In this study, a novel MDLS-UAVIC approach was established to securely encrypt the images and classify them into distinct class labels in the smart city environment. The proposed MDLS-UAVIC model follows a two-stage process: encryption and image classification. For image encryption, the signcryption technique effectively encrypts the UAV images. Next, the image classification process involves an Xception-based deep convolutional neural network for the feature extraction process.

Finally, SSO with a recurrent neural network (RNN) model is exploited for UAV image classification. The experimental validation of the MDLS-UAVIC approach was tested utilizing a benchmark dataset, and the outcomes are examined in various measures. The comparative analysis ensured the effective performance of the MDLS-UAVIC approach on recent methodologies. In the future, an ensemble of DL-based classification methods can be designed to accomplish maximum performance.

Some limitations that can be associated with the use of computational intelligence techniques for secure unmanned aerial vehicle (UAV) image classification in a smart city environment:

- Dependence on training data: Computational intelligence techniques, such as deep learning algorithms, require a large amount of labeled training data to achieve high accuracy in image classification. However, collecting and labeling such data can be time-consuming and expensive, especially for a specific smart city environment.
- Sensitivity to environmental factors: UAV image classification can be affected by various environmental factors, such as lighting conditions, weather, and camera quality. These factors can impact the quality of the captured images, which in turn affects the accuracy of the classification results.
- Security concerns: The use of UAVs in a smart city environment raises security concerns, as these vehicles can be vulnerable to cyberattacks and can potentially be used for malicious purposes. While the paper may address security concerns, it is important to consider the potential limitations of the proposed approach in mitigating such risks.
- Integration with existing systems: In a smart city environment, UAV image classification systems need to be integrated with other existing systems, such as surveillance cameras and emergency response systems. The integration process can be challenging, as different systems may have different data formats and communication protocols.
- Regulatory and ethical considerations: The use of UAVs in a smart city environment may be subject to regulatory and ethical considerations, such as privacy concerns and compliance with local laws and regulations. These considerations need to be taken into account when implementing a UAV image classification system.

Acknowledgement: The authors would like to acknowledge the appreciation to the Deputyship for Research & Innovation, Ministry of Education in Saudi Arabia for funding this research work.

Funding Statement: The authors extend their appreciation to the Deputyship for Research & Innovation, Ministry of Education in Saudi Arabia for funding this research work through the Project Number RI-44-0446.

Author Contributions: The authors confirm contribution to the paper as follows: study conception and design: Firas Abedi, Hayder M. A. Ghanimi; data collection: Abeer D. Algarni, Naglaa F. Soliman; analysis and interpretation of results: Walid El-Shafai, Ali Hashim Abbas, Zahraa H. Kareem; draft manuscript preparation: Hussein Muhi Hariz and Ahmed Alkhayat. All authors reviewed the results and approved the final version of the manuscript.

Availability of Data and Materials: Not applicable.

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

References

- [1] T. Caramés, O. Novoa, M. Albela and P. Lamas, “A UAV and blockchain-based system for industry 4.0 inventory and traceability applications,” *Sensors and Applications*, vol. 4, no. 1, pp. 1–7, 2018.
- [2] T. Caramés, O. Novoa, I. Míguez and P. Lamas, “Towards an autonomous industry 4.0 warehouse: A UAV and blockchain-based system for inventory and traceability applications in big data-driven supply chain management,” *Sensors*, vol. 19, no. 10, pp. 23–94, 2019.
- [3] G. Lee, W. Saad and M. Bennis, “Online optimization for UAV-assisted distributed fog computing in smart factories of Industry 4.0,” in *Proc. of IEEE Global Communications Conf. (GLOBECOM)*, Abu Dhabi, United Arab Emirates, pp. 1–6, 2018.
- [4] S. Aggarwal, N. Kumar, M. Alhussein and G. Muhammad, “Blockchain-based UAV path planning for Healthcare 4.0: Current challenges and the way ahead,” *IEEE Network*, vol. 35, no. 1, pp. 20–29, 2021.
- [5] R. Barenji and B. Nejad, “Blockchain applications in UAV-towards Aviation 4.0,” *Intelligent and Fuzzy Techniques*, vol. 37, no. 2, pp. 411–430, 2022.
- [6] E. Petritoli and F. Leccese, “Precise takagi-sugeno fuzzy logic system for UAV longitudinal stability: An Industry 4.0 case study for aerospace,” *ACTA IMEKO*, vol. 9, no. 4, pp. 10–46, 2020.
- [7] V. Aliksieiev and B. Markovych, “Implementation of UAV for environment monitoring of a smart city with an airspace regulation by AIXM-format data streaming,” *Industry*, vol. 5, no. 2, pp. 90–93, 2020.
- [8] S. Aggarwal, N. Kumar and S. Tanwar, “Blockchain-envisioned UAV communication using 6G networks: Open issues, use cases, and future directions,” *IEEE Internet of Things Journal*, vol. 8, no. 7, pp. 5416–5441, 2021.
- [9] L. Das, “Human target search and detection using autonomous UAV and deep learning,” in *Proc. of IEEE Int. Conf. on Industry 4.0, Artificial Intelligence, and Communications Technology (IAICT)*, Bali, Indonesia, pp. 55–61, 2020.
- [10] F. Long, F. Sun and Z. Yang, “A novel routing algorithm based on multi-objective optimization for satellite networks,” *Journal of Networks*, vol. 6, no. 2, pp. 238–246, 2011.
- [11] J. Raj, “Security enhanced blockchain based unmanned aerial vehicle health monitoring system,” *Journal of ISMAC*, vol. 2, no. 2, pp. 121–131, 2021.
- [12] M. Shibli, P. Marques and E. Spiridon, “Artificial intelligent drone-based encrypted machine learning of image extraction using pretrained convolutional neural network (CNN),” in *Proc. of Int. Conf. on Artificial Intelligence and Virtual Reality*, Nagoya, Japan, pp. 72–82, 2018.
- [13] M. Minu and R. Canessane, “Secure image transmission scheme in unmanned aerial vehicles using multiple share creation with optimal elliptic curve cryptography,” *Indian Journal of Computer Science and Engineering*, vol. 12, no. 1, pp. 129–134, 2021.
- [14] R. Mardiyanto, H. Suryoatmojo, F. Setiawan and A. Irfansyah, “Low cost analog video transmission security of unmanned aerial vehicle (UAV) based on linear feedback shift register (LFSR),” in *Proc. of Int. Seminar on Intelligent Technology and Its Applications (ISITIA)*, Surabaya, Indonesia, pp. 414–419, 2021.
- [15] E. Abualsauod, “A hybrid blockchain method in Internet of Things for privacy and security in unmanned aerial vehicles network,” *Computers and Electrical Engineering*, vol. 99, no. 3, pp. 107–127, 2022.
- [16] I. Punithavathi, S. Dhanasekaran, P. Duraipandy, E. Lydia, M. Sivaram *et al.*, “Optimal dense convolutional network model for image classification in unmanned aerial vehicles based ad hoc networks,” *International Journal of Ad Hoc and Ubiquitous Computing*, vol. 39, no. 1, pp. 46–60, 2022.
- [17] R. Kumar, P. Kumar, R. Tripathi, G. Gupta, T. Gadekallu *et al.*, “SP2F: A secured privacy-preserving framework for smart agricultural unmanned aerial vehicles,” *Computer Networks*, vol. 18, no. 7, pp. 107–119, 2021.
- [18] M. Elhoseny and K. Shankar, “Reliable data transmission model for mobile ad hoc network using signcryption technique,” *IEEE Transactions on Reliability*, vol. 69, no. 3, pp. 1077–1086, 2020.
- [19] F. Chollet, “Xception: Deep learning with depthwise separable convolutions,” in *Proc. of the IEEE Conf. on Computer Vision and Pattern Recognition*, Honolulu, HI, USA, pp. 1251–1258, 2017.

- [20] R. Hang, Q. Liu, D. Hong and P. Ghamisi, "Cascaded recurrent neural networks for hyperspectral image classification," *IEEE Transactions on Geoscience and Remote Sensing*, vol. 57, no. 8, pp. 5384–5394, 2019.
- [21] A. Kaveh and A. Zaerreza, "Shuffled shepherd optimization method: A new meta-heuristic algorithm," *Engineering Computations*, vol. 37, no. 7, pp. 2357–2389, 2020.
- [22] R. Ambika, L. Biradar and V. Burkpalli, "Encryption-based steganography of images by multiobjective whale optimal pixel selection," *International Journal of Computers and Applications*, vol. 2, no. 6, pp. 1–10, 2019.
- [23] Y. Li, R. Chen, Y. Zhang, M. Zhang and L. Chen, "Multi-label remote sensing image scene classification by combining a convolutional neural network and a graph neural network," *Remote Sensing*, vol. 12, no. 23, pp. 40–63, 2020.