Enabling Unmanned Aerial Vehicle Borne Secure Communication With Classification Framework for Industry 5.0

Deepak Kumar Jain, *Senior Member, IEEE*, Yongfu Li, Meng Joo Er, *Senior Member, IEEE*, Qin Xin, Deepak Gupta, and K. Shankar, *Senior Member, IEEE*

***Abstract*—The fifth industrial revolution (Industry 5.0) integrates humans and machines to satisfy the increasing customization demands of the manufacturing complexity using an optimized robotized manufacturing process. Industry 5.0 make use of collaborative robots (cobots) for optimizing productivity and ensuring safety. At the same time, unmanned aerial vehicles (UAVs) are predicted to be the main part of industry 5.0 in the forthcoming days. Regardless of high mobility and energy-limited UAVs for wireless communication as significant advantages, different issues are also existing in the UAV networks, such as security, reliability, etc. Several research works have focused on resolving security issues in UAV communication to support safety-critical applications. With this motivation, this article presents an artificial intelligence-based UAV-borne secure communication with classification (AIUAV-SCC) framework for industry 5.0 environment. The proposed AIUAV-SCC model involves two major phases namely image steganography-based secure communication and deep learning (DL)-based classification. At the initial stage, a new image steganography technique with multilevel discrete wavelet transformation, quantum bacterial colony optimization based optimal pixel selection, and encryption processes take place. Next, in the second stage, the Bayesian optimization (BO)-based SqueezeNet model is applied for the classification of securely received UAV images where the parameters in the SqueezeNet method are optimally tuned by the utilize of the BO technique. To validate the performance of the presented model, extensive simulations are applied using the UC Merced dataset (UCM) aerial dataset and the outcomes are investigated under several dimensions. The outcomes make sure the goodness of the presented model on test UCM aerial dataset over the compared methods.**

***Index Terms*—Artificial intelligence, encryption, image steganography, Industry 5.0, secure communication, unmanned aerial vehicles (UAVs).**

I. Introduction

TRACED back to 1780s, the Industry 1.0 has begun with the generation of mechanical power from water, steam, and fossil fuel. In Industry 2.0, electrical energy was favored by manufacturing companies with assembly lines and mass production in the 1870s [1]. By the usage of electronics and information technologies (IT), Industry 3.0 has adapted with the production industries with the concept of automation in the 1970s. Then, Industry 4.0 uses Internet of Things (IoT) and cloud computing (CC) to offer a real-time interface amongst the virtual as well as the physical environment. Though Industry 4.0 is still yet to be explored, several manufacturers have started to concentrate on Industry 5.0, which integrates autonomous manufacturing with human intelligence as shown in Fig. 1 [2]. With the utilization of robots in production along with human intelligence, Industry 5.0 introduces the concept of collaborative robots (cobots), which is employed for the optimization of productivity and reliability. Industry 5.0 is intended for enabling limitless, reliable, secure, and intelligent connectivity in manufacturing processes [3]. It is predictable that Industry 5.0 would bring a full-fledged architecture for linked and automated systems from independent cars to unmanned aerial vehicles (UAV) with diverse and stringent needs based on latency, data rate, energy efficiency, and reliability. It is so called drones, act as a major part in extensive scenarios that could exceed 5G and 6G [4], [5]. Because of the exclusive feature of UAVs such as flexibility, mobility, and independent function, they are widely utilized in several applications in the following years. For instance, a few applications of UAVs include remote construction, media production, package delivery, and real-time surveillance. Furthermore, the UAVs are deliberated as the major operators on IoT and smart city environment. The placement of UAVs

Manuscript received May 26, 2021; revised August 19, 2021 and October 8, 2021; accepted October 18, 2021. Date of publication November 8, 2021; date of current version May 6, 2022. This work was supported by the National Natural Science Foundation of China under Grant U1964202. Paper no. TII-21-2189. *(Corresponding author: Qin Xin.)*

Deepak Kumar Jain and Yongfu Li are with the Key Laboratory of Intelligent Air-Ground Cooperative Control for Universities in Chongqing, College of Automation, Chongqing University of Posts and Telecommunications, Chongqing 400065, China (e-mail: deepak@cqupt.edu.cn; liyongfu@cqupt.edu.cn).

Meng Joo Er is with the Institute of Artificial Intelligence and Marine Robotics, College of Marine Electrical Engineering, Dalian Maritime University, Dalian 116026, China (e-mail: mjer@dlmu.edu.cn).

Qin Xin is with the Faculty of Science and Technology, University of the Faroe Islands, 100 Torshavn, Faroe Islands (Denmark) (e-mail: qinx@setur.fo).

Deepak Gupta is with the Department of Computer Science and Engineering, Maharaja Agrasen Institute of Technology, Delhi 110086, India (e-mail: deepakgupta@mait.ac.in).

K. Shankar is with the Federal University of Piauí, Teresina 64049-550, Brazil (e-mail: drkshankar@ieee.org).

Color versions of one or more figures in this article are available at https://doi.org/10.1109/TII.2021.3125732.

Digital Object Identifier 10.1109/TII.2021.3125732

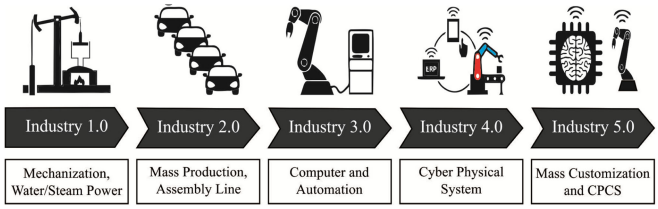

Fig. 1. Pipeline of Industry 5.0.

is becoming greater, and the Federal Aviation Administration estimated that the amount of commercial UAVs fleet could be attained to 1.6 million by 2024.

In spite of containing higher mobility and energy-limited UAVs for wireless transmission as significant advantages, several experiments [6] are presented using UAV transmission networks. To assist security crucial tasks like crash, collision evasion, high delay latency, security, and real-world control are essential in UAV schemes than usual transmission connection present in global transmissions systems. The security vulnerability in UAV transmission is examined by the researcher as drones are linked straight to the Internet and interact wirelessly, therefore, causes a serious threat to the secrecy of the UAV network [7]. The cellular user device could endure interference because of line of sight (LOS) relations in UAV that are affected by the hackers. Henceforth, it is essential for addressing the safety of UAV transmission network.

Several robust and high secured data maintaining methods have existed in the literature for ensuring robustness and security of the method regarding its efficiency. Image steganography has made an extensive application in the area of mobile computing, transmission, privacy of medicinal, customized secure image retrieval content, surveillance, and record online voting systems. Data encryption represents cryptography which leads to reordering the secret data, thus, it is not noticeable by eavesdroppers. Nowadays, security is the main objective for hiding sensitive information from hackers and intruders which turns into a complex process [8], [9]. Then, a few methods should be utilized as alterations for a lesser number of pixels or convert coefficients, using an encrypted form of secret message to be embedded.

Various researches are needed to select appropriate tradeoff among efficiency calculation processes like payload capacity, security, and imperceptibility. Presently, secured data is used for the transmission of audio files, videos, text messages, and images. In this method, the confidential message in the file is transmitted to the client at another end in such a way that the message is unhidden. Therefore, this article aims to hide the embedded data with the carriers and share the data in an unnoticeable way for UAVs along with the image classification in industry 5.0 environment.

This article develops an artificial intelligence-based UAV-borne secure communication with classification (AIUAV-SCC) framework for industry 5.0 environment. The proposed AIUAV-SCC model involves two major phases namely image steganography-based secure communication and deep learning (DL) based classification. The image steganography technique involves multilevel discrete wavelet transformation (DWT), quantum bacterial colony optimization (QBCO)-based optimal pixel selection, and encryption. Besides, the Bayesian optimization (BO)-based SqueezeNet model is applied for the classification of securely received UAV images. For examining the effectual outcome of the AIUAV-SCC method, a set of experimentations take place on the UC Merced (UCM) dataset aerial dataset and the results are investigated under several dimensions. In short, the key contributions of the article are summarized in the following.

- Propose a new AIUAV-SCC framework to accomplish secure communication and classification in Industry 5.0 environment.
- Employs two phases image steganography based secure communication and DL-based classification.
- Apply multilevel DWT to generate a set of vector coefficients.
- Derive a QBCO algorithm by integrating quantum computing (QC) concepts into the traditional BCO algorithm to improve the convergence rate.
- Employ signcryption, ElGamal public key cryptosystem (EPKC), and Kernel homomorphic encryption (KHE) techniques to encrypt R, G, and B channels.
- Design BO-based SqueezeNet model for UAV image classification in industry 5.0 environment.
- Validate the effectiveness of the AIUAV-SCC framework on the UCM aerial dataset and examine the outcomes in terms of distinct measures.

The remaining portions of the study are arranged as follows. Section II offers the existing works interrelated to the study and Section III elaborates the proposed AIUAV-SCC model. Next, Section IV validates the performance of the AIUAV-SCC model, and Section V concludes the study.

II. Related Works

This section reviews the recent state-of-the-art security-based solutions developed for UAV communication networks. In [7], a secure fog-enabled IIoT model is presented by appropriately plugging several security features into it and offloading a few tasks judiciously to fog nodes. Sharma *et al.* [10] presented new functional encryption for UAV-aided HetNet module for securing data. In this module, UAV performs as a relay node in which the user terminal is in non-LOS transmission with the mobile base station. In Lei *et al.* [11], an improved lightweight identity security authentication protocol, ODIAP is presented to UAV networks. At the same time, this study entirely deliberates the computation load and offers identity data verification with generation technique depending upon the Chinese residual proposal.

Khoei *et al.* [12] proposed the ECDH technique to exchange keys. When the keys are safely allocated among the clients using this technique and accurate arbitrariness of keys are attained, later OTP contains a quicker and high secure encryption method. He *et al.* [13] proposed a secure communication system for the UAV network. In this method, every drone preserves and handles a region where the official device could attain a transmission key without an online central authority. Using hierarchical identity-based transmission encryption and pseudonym method, each device in this scheme could transmit the encrypted message

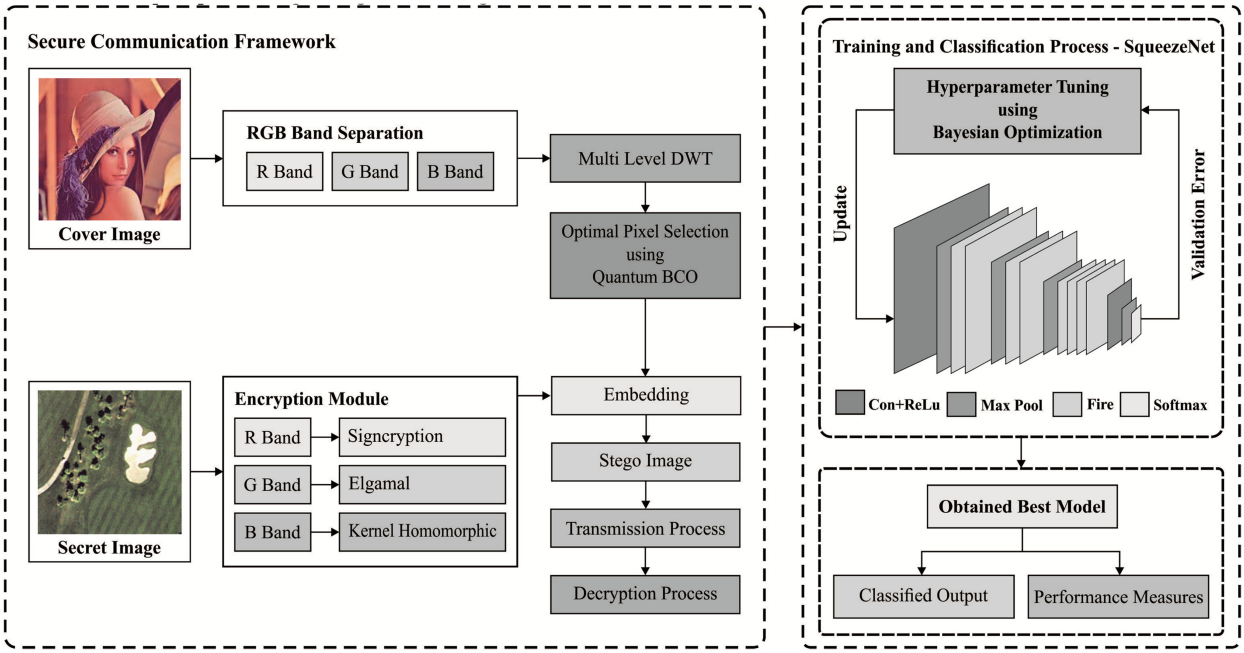

Fig. 2. Overall process of proposed AIUAV-SCC model.

secretly and decrypt the authorized ciphertext. García-Magariño *et al.* [14] utilized secure asymmetric encryption using a pre-shared existing authorized UAV. By this method, incorrect data could be identified if an authorized UAV is physically stolen. The new agent-based simulator security UAV is utilized for validating the presented technique. The advancement of this study [15] is to suggest an encryption communication system on the basis of SM4 technique and enhance the stream encryption mode (CTR) of the SM4 method. Related to the conventional SM4 CTR method, the decryption and encryption speediness is enhanced by 7.7%, and ChaCha20 flow Encryption approach is highly persistent of packet loss.

In Chen *et al.* [16], a traceable and privacy-preserving authentication is presented for integrating the hash function, digital signature, ECC, and another cryptography method to UAV applications. To sensitive regions, players should attain flight authorization from the control station beforehand they could handle UAV in the regions. The conventional cryptography facilities such as availability, nonrepudiation, integrity, anonymity, confidentiality, defence, privacy towards DoS, and spoofing attacks could be guaranteed. In Duan *et al.* [17], a novel Stegno-CNN module is presented which resolves the challenge of two images embedding in a carrier image and could efficiently rebuild two secret images. It contains encoding as well as decoding networks, where the decoding network comprises two extraction networks. Haque and Chowdhury [18] proposed a new robust and lightweight framework which simultaneously does not compromise pragmatic and security in the influence of energy effective atmosphere. Likewise, it proposed a selective encryption method for reducing overhead and data hiding techniques to raise the privacy of the communication. Though several secure communication and classification techniques have existed in the literature, very few researchers have focused on the Industry 5.0 environment. Therefore, it is still needed to improve security and classification performance for the UAVs in Industry 5.0.

III. Proposed Model

The overall working procedure involved in the presented AIUAV-SCC technique is showcased in Fig. 2. The presented model involves two major stages namely secure communication and image classification. During the secure communication process, different operations are involved such as channel extraction, decomposition, optimal pixel selection, encryption, and embedding process. Besides, the presented method uses multilevel DWT for the generation of a collection of vector coefficients. In addition, the optimal pixel selection process is carried out using the QBCO algorithm over the R, G, and B channels. On the other hand, the channel separation and encryption of the three channels of the secret image also take place. Moreover, the encryption of the R, G, and B channels of the secret image takes place using three encryption techniques such as signcryption, EPKC, and KHE. At the receiver side, the decryption and extraction processes are carried out to reconstruct the secret image. Finally, the SqueezeNet model with BO-based parameter optimization process gets executed to classify the UAV images.

A. Multilevel DWT-Based Decomposition Process

The RGB cover image is divided on the basis of HH, LH, LL, and HL bands for finding pixel position. The 2D-DWT is the most significant spatial to frequency domain conversion method. The partition is made with two processes namely, vertical and horizontal processes. The horizontal function decomposes an image to High (H) and Low (L) frequency bands. Later, the vertical function decomposes an image to LL_1, LH_1, HL_1, and

HH_1 frequency bands. For the next decompositions, LL_1 band decompose to LL_2, LH_2, HL_2, and HH_2, where the image size represents 'M∗N'. Initially, to downsample and filter the image, the horizontal decomposition decreases the image to $M \times \frac{N}{2}$ size.

The vertical one decrease downsample the images to $\frac{M}{2} \times \frac{N}{2}$. The single-level decomposition outcome is done using

$$[C_1 C_2 C_3 C_4] \;=\; \mathrm{DWT}\,(C) \tag{1}$$

where "C_1", "C_2", "C_3," and "C_4" denotes coefficient values of the decomposing frequency band. "C_1" denotes low-level frequency band that is additionally decomposed for extracting sub-bands as

$$\left[C_1^{\mathrm{LL1}} C_1^{\mathrm{LH1}} C_1^{\mathrm{HL1}} C_1^{\mathrm{HH1}}\right] \;=\; \mathrm{DWT}\,(C_1)\,. \tag{2}$$

The coefficient in low-frequency band C_1^{LL1} is over decomposed, since it produces the edge and texture-related details of an image. The following decomposition is executed on low band LL_1. The decomposition formation of frequency band is presented by

$$\left[C_1^{\mathrm{LL2}} C_1^{\mathrm{LH2}} C_1^{\mathrm{HL2}} C_1^{\mathrm{HH2}}\right] = \mathrm{DWT}\,(\mathrm{LL}_1) \tag{3}$$

where C_1^{LL2} denotes low-level frequency band of second-level decomposition.

B. QBCO-Based Optimal Pixel Selection Process

The multilevel DWT transformation process results in the generation of vector coefficients for the applied cover image. Amongst the distinct vector coefficients, the optimum pixels are chosen by the use of QBCO algorithm. BCO algorithm is developed by Niu *et al.* [20] and it involves simplified optimization process, several exchange topology structures, high convergence, and simple design. The chemotaxis procedure is a significant process in the BCO algorithm. It encompasses two major processes as running and tumbling. Particularly, the aim of the running process is to produce a new position $(\theta_{\mathrm{i}}(T))$ related to the earlier position $(\theta_{\mathrm{i}}(T-\mathrm{l}))$, adaptive neighborhood oriented study (or arbitrary oriented study) $(P\mathrm{best}_i)$, and group-oriented study $(G\mathrm{best})$. For enhancing the diversity and convergence, the tumbling process gets executed if the running process is considered invalid at certain level. During the tumbling process, extra arbitrariness (tur_i) element is applied for obtaining optimum positions for nutrients. Besides, the running and tumbling strategies are defined as

$$\theta_i\;(T) = \theta_i\;(T-1) + R_i * (G\mathrm{best} - \theta_i\,(T-1)) + (1-R_i) * (P\mathrm{best}_i - \theta_i\,(T-1)\;) \tag{4}$$

$$\theta_i\;(T) = \theta_i\;(T-1) + \mathrm{R_i} * (G\mathrm{best} - \theta_i\,(T-1)) + (1-R_i) * (P\mathrm{best}_i - \theta_i\,(T-1)) + C\,(\mathrm{i}) * tur_i \tag{5}$$

where C indicates chemotaxis step size [21]. The arbitrariness variable is provided as $tu\,r_{\mathrm{i}} = \Delta(i)/\sqrt{\Delta^{\mathrm{T}}(i)\Delta(i)}$, where $\Delta(i)$ implies the direction angle of ith bacterium in which the components exist in the range of [-l, 1]. The variables R_1 and R_2 are two arbitrarily created constants and the values exist in the interval of [0, 1]. For improving the convergence rate of the BCO technique, QC concept is incorporated and derived from the QBCO algorithm.

Algorithm 1: Pseudocode of BCO Algorithm.

```
Begin
For (Every iteration)
    For (Every run)
    Chemotaxis and Communication:
      Tumbling (Chemotaxis and Communication)
        While (higher swimming processes are unsatisfied)
          Swimming (Chemotaxis and Communication)
        End while
      Interactive Exchange:
        Individual and group exchanging process
      If (Reproduction and elimination criteria is
      unsatisfied)
        Reproduction and elimination
      End If
      If Migration condition is satisfied
        Migration
      End If
    End For
  End For
End
```

QC is a novel type of processing module that accepts the idea relevant to quantum models as state superposition, quantum entanglement, and measurements. The fundamental component of QC is a qubit. The two fundamental conditions $|0\rangle$ and $|1\rangle$ create a qubit that is stated by linear integration as given by

$$|Q\rangle \;=\; \alpha\,|0\rangle + \beta\,|1\rangle\,. \tag{6}$$

$|\alpha|^2$ represents the likelihood of observing condition $|0\rangle$, $|\beta|^2$ and $|1\rangle$, where $|\alpha|^2 + \;|\beta|^2 = \;1$. A quantum is comprised of n qubits. According to the quantum superposition nature, every quantum has 2^n probable values [22]. An n qubits quantum is represented by

$$\Psi \;= \sum_{x=0}^{2^n-1} C_x\;|x\rangle\,, \sum_{x\,=\,0}^{2^n-1} |C_x\;|^2 = \;1. \tag{7}$$

Quantum gates could alter the qubit states such as Hadamard gate, rotation gate, NOT gate, and so on. The rotation gate has been defined by mutation function for generating quanta method an optimum solution, and lastly, detect global optimum solutions. The rotation gate is determined by

$$\begin{bmatrix}\alpha^d\,(t+1)\\ \beta^d\,(t+1)\end{bmatrix} = \begin{bmatrix}\cos\left(\Delta\theta^d\right) & -\sin\left(\Delta\theta^d\right)\\ \sin\left(\Delta\theta^d\right) & \cos\left(\Delta\theta^d\right)\end{bmatrix}\begin{bmatrix}\alpha^d\,(t)\\ \beta^d\,(t)\end{bmatrix} \text{ for } d = 12,\ldots,n. \tag{8}$$

$\Delta\theta^d = \Delta \times S\;(\alpha^d,\;\beta^d)$, $\Delta\theta^d$ denotes the rotation angle of qubit, when Δ and $S(\alpha^d,\;\beta^d)$ represent direction and size of rotations, correspondingly.

C. Encryption Process

During the encryption process, the channel extraction of the secret images takes place. Then, the individual R, G, and B bands

are encrypted using signcryption, EPKC, and KHE techniques. The encryption of the RGB elements in an individual way offers improved security of the embedding process. Afterward, the encrypted RGB elements are embedded to the effectively chosen pixel points in the cover images. It guarantees the secrecy of the stego images owing to the processes of encrypting and embedded the confidential image.

1) R Channel Encryption Using Signcryption Technique: At this stage, the R channels of the secret image get encrypted using signcryption technique. The presented security technique is a public key encryption module with a digital signature that could enhance integrity, nonrepudiation, authenticity, availability, and confidentiality. The encryption is associated rather than simple encryption, and an individual session key is reutilized for some encryptions to achieve improved effectiveness. Basically, this signcryption approach has three phases: key generation, signcryption, and designcryption. Since encryption provides confidentiality and signature offers authenticity, signcryption consecutively executes the processes of encryption and signature in one logical step, when the expenses of estimation and transmission are not the same as the series of signatures [23]. It contains subsequent phases such as key generation, parameter initialization, signcryption, and designcryption.

During the parameter initialization process, the signature-based security analyses primarily share a few variables such as large prime numbers to hash values, key generation, and receiver and sender keys. In the signcryption security module, the keys are created by cryptographic process; the function of the elliptic curve-based method generates prime numbers and factors of this number. The initiated variables contain r_1, Su_1, Rr_2, and Ru_1. For maximizing the secure communication of the UAV communication, these keys are utilized. This encryption procedure needs to transmit the data/information to the receiver afterward security analyses. Now, the hash and one keyed hash value-based encrypted information together with movement vectors have been deliberated.

2) G Channel Encryption Using EPKC Technique: During the G channel encryption, the EPKC technique is applied to encrypt it. Conventionally, the EPKC technique is developed in 1985 by discrete logarithm problem complexity for several areas (partial homomorphic encryption module). It comprises three main operations such as encryption, decryption, and key generation [24]. Commonly, this module includes a private key (i.e., arbitrary number) $xi \in Zi_{qi'}$ with its corresponding public key $yi \equiv (gi')^{xi}$ *mod qi*, where gi' states generator to Gi_1 with primary arrangements qi'. A novel involvement of this study's aim is for enhancing the equivalent private key with a novel hybrid technique. The full explanation regarding the presented technique is provided in the following segment. Furthermore, the encrypted image $mi \in Gi_1$ and public key yi is defined by pair $\mathrm{i}_1 \equiv (gi')^{ri} modqi; ci_2 \equiv yi^{ri}\mathrm{mi}\ mod\ qi$, where ri denotes random number. Additionally, the decrypted cipher text $\{ci_1, ci_2\}$ and private key xi is defined by $mi \equiv \mathrm{ci}_2(\mathrm{ci}_1^{xi})^{-1}$ *mod qi*.

This module possesses similar cipher images using selected plain image attacks for each probabilistic polynomial time adversary Ai. To understand better, the EPKC technique is determined as a game module with a challenger Ci and adversary *Ai*.

- Primarily, Ai selects different images $mi_0, mi_1 \in Gi_1$ and send to Ci'.
- Later, the module calculates Ci' chooses $ai \in \{01\}$ and $ri_1,\ xi \in Zi_{qi'}$ randomly and places $yi \equiv (gi')^{xi}$ *mod qi*, $ci_1 \equiv (gi')^{ri}$ *mod qi* and $ci_2 \equiv (gi')^{rixi}\mathrm{mi}_{ai}$ *mod qi*. Additionally, Ci' provides *Ai* as gi', yi, ci_1, and ci_2.
- Calculate challenge as Ci' requests Ai regarding ai.
- Calculate guess Ai gives ai' and send it returns to Ci'. At this time, Ai attains if $a\,i' = ai$ fails.

Assume *Ai* wjere gi', $(gi')^{xi}$, $(gi')^{ri}$, and $(gi')^{xiri}mi_{ai}$ yet, Ai could not develop the right to access *xi* and *ri*'. At this point, the success potential of probabilistic polynomial time adversary *Ai* to attain ai accurately is slightly improved compared to random guess as

$$Pi\ \ [a\,i' = ai] = \frac{1}{2} + negl \tag{9}$$

where Pi states success likelihood and $negl$ denotes slight development.

3) B Channel Encryption Using KHE Technique: Finally, the R channels of the secret image get encrypted using signcryption technique. This presented KHE system is depending comprises four polynomial time methods such as kernel homomorphic evaluation, kernel homomorphic decryption, KHE, and kernel homomorphic key generation. The group representation and operations must be effective on 3X2 vector space. In this study, a homomorphism is determined as follows ∂: $Eec(r)mod(n) \rightarrow Dec(c)mod(n)$ and the ideal group of kernel homomorphism for decryption and encryption "∂" is determined by $\Delta = \{r' \in Enc(r) : \partial(r') = c\}$ and $\Delta - 1 = \{c' \in Dec(c) :\ \partial^{-1}(c') = r\}$ the common formula of kernel homomorphism is provided in the applied kernel as (10). In (11) and (12), they obtain actual message r when decrypting ciphertexts [25]. If they encrypt two parts of message r such as r_1 and r_2 , they would attain resultant cipher texts (c_1 and c_2), from (12) and (17) and in decryption they attain plaintexts from (16) and

$$r_1 = \partial^{-1}\ \left(e_{\mathrm{Dec}(c_1)\mathrm{mod}(n)}\right) \tag{10}$$

where $e \subseteq \mathrm{Dec}(c_1)\mathrm{mod}(n)$

$$r_2 = \partial^{-1}\ \left(e_{\mathrm{Dec}(c_2)\mathrm{mod}(n)}\right) \tag{11}$$

$$c = \begin{cases} ker.\,(r_1 \oplus r_2) = ker.\,(r_1) \oplus ker.\,(r_2)\,. \\ ker.\ (r_1 * r_2) = |\ ker.\ (r_1) *|\ ker.\ (r_2)\,. \end{cases} \tag{12}$$

$$c_1 = \partial\left(\mathrm{Enc}\,(r_1)\,\mathrm{mod}\,(n)\right) \tag{13}$$

where $\partial(r_1 \in \mathrm{Enc}(r)\mathrm{mod}(n))$

$$c_2 = \partial\left(\mathrm{Enc}\,(r_2)\,\mathrm{mod}\,(n)\right) \tag{14}$$

where $\partial(r_2 \in \mathrm{Enc}(r)\mathrm{mod}(n))$

$$c = \partial\left(\mathrm{Enc}\,(r_1)\,\mathrm{mod}\,(n)\right) \oplus \partial\left(\mathrm{Enc}\,(r_2)\,\mathrm{mod}\,(n)\right). \tag{15}$$

By ∂^{-1} as homomorphism in (10) and (11) to decryption. While $c_1,\ c_2 \in \mathrm{Dec}(c)\mathrm{mod}(n)$, thus $\partial^{-1}\,c_1 = r_1\,,\ \partial^{-1}\,c_2 = r_2$ and $r_1 \oplus\ r_2 =\ r$, and $r_1 *\ r_2 =\ r$

$$r = \begin{cases} \partial^{-1} \cdot (c_1 \oplus c_2) = \partial^{-1}\,(c_1) \oplus \partial^{-1}\,(c_2) \\ \partial^{-1} \cdot (c_1 * c_2) = \partial^{-1}\,(c_1) * \partial^{-1}\,(c_2) \end{cases}. \tag{16}$$

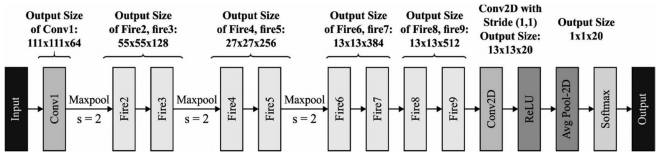

Fig. 3. Structure of SqueezeNet.

Equations (13) and (14) are given as

$$c = c_1 \oplus c_2 \; OR \; c = c_1 * c_2. \tag{17}$$

Equations (10) and (11) are given by

$$r = r_1 \oplus r_2 \; OR \; r = r_1 * r_2. \tag{18}$$

When they proceed $\oplus$ of r_1 with r_2 and c_1 with c_2, etc., without kernel, it would be deliberated as noise.

D. BO-SqueezeNet Based Classification Process

After the successful reconstruction of the UAV images, the BO-SqueezeNet model is applied for determining the class labels of the implemented test UAV image. The BO technique is utilized for optimally adjusting the hyperparameters of the SqueezeNet method. The SqueezeNet deep CNN has a compressed framework design and contains relatively small amount of parameters. SqueezeNet is a DL model that contains 15 layers with five distinct layers as 2 convolutional layers, three max pooling layers, 8 fire layers, 1 global average pooling layer, and 1 output softmax layer. The input of the network has 227∗227 dimension with an RGB channel. The convolutional layer will convolute amongst the weight and smaller region in the input volume with 3∗3 kernel. It makes use of the fire layer that incorporates squeeze and expansion stages amongst the convolutional layers. The squeeze stage exploits the filter of size 1∗1, where the expansion utilizes the filter sizes of 1∗1 and 3∗3. Initially, the input tensor H × W × C permits with squeeze and convolutional count is equivalent to C/4 of the input tensor channel count. Next to the initial stage, the data gets passed via the expansion, and data depth is extended to C/2 of the depth of the outcome tensor. The squeeze and expansion stages are linked together by the ReLu units. At last, the expansion outcomes are piled up to the depth dimensions of the input tensor with concatenation function. Fig. 3 illustrates the structure of SqueezeNet.

Next, the hyperparameters in the SqueezeNet are tuned by the utilize of BO concept, which is based on the Bayesian theorem. In the training process, the BO module would trace a function that contains their data in the learned data. In BO technique, the major aim is to attain the interrelated hyperparameter that makes learning outline maximal. In numerical equation, they could assume a global minimization/maximization issue of the black box (unknown) function f

$$x^{\diamondsuit} = \arg\max_{x \in X} f(x). \tag{19}$$

Now, X denotes the searching space of x. Affect by the nature of Bayes' formula, BO estimates the posteriori probability $P(D1L)$ of module D with the support of learned data

Algorithm 2: Bayesian Optimization.

For $i = 1, 2,$ do
  Search x_i by enhancing the acquisition function v,
  $$xi = \underset{x}{\operatorname{argmax}}\, \nu(x|N_{1:i-1})$$
  Calculate objective function: $y_i = f(x_i)$
  Augment data $N_{1:i} = \{N_{1:i-1}, (x_i, y_i)\}$
  Upgrade the module
End For

Fig. 4. Sample UAVs images.

L. Posteriori likelihood is related to the probability $P(L|D)$ of observation L and the product of previous likelihood $P(D)$

$$P(D|L) \propto P(L|D)\, P(D). \tag{20}$$

Equation (20) depicts the major behavior of BO [27]. Briefly, BO search for an optimal module among them. Currently, one could recollect the cross-validation technique. But it is difficult to detect an optimal module in several instances of prelisted hundreds of alternate. Therefore, BO speeds up the process by decreasing the computation cost, and they don't require skill for guessing the output. This technique integrates the previous distribution of $f(x)$ function with instances of the previous knowledge for obtaining posterior. This posterior calculates the value that defines maximized point of the $f(x)$. Here, the condition of maximized procedure is the formula named acquisition function. They present a pseudocode format of BO through a table. In this technique, $N_{1:i-1} = \{x_n, y_n\}_{n=1}^{i-1}$ reflect the trained dataset that comprises $i-1$ observation of f function.

IV. Performance Validation

The performance of the proposed AIUAV-SCC method is experimented against UCM dataset [26]. The proposed technique has been simulated in Python 3.6.5 with additional packages such as tensorflow (GPU-CUDA Enabled), keras, numpy, pickle, matplotlib, sklearn, pillow, and opencv-python. In addition, an extensive experimental analysis takes place to make sure the security level of the AIUAV-SCC model. The parameter setting is provided as follows: mini batch size: 200, dropout: 0.5, hidden layer count: 3, number of hidden units: 1024, and activation

TABLE I
RESULT ANALYSIS OF PROPOSED AIUAV-SCC METHOD WITH EXISTING METHODS WITH RESPECT TO MSE AND PSNR

Test Images	AIUAV-SCC		CSO-MDWT		GWO-MDWT		PSO-MDWT	
	MSE	PSNR	MSE	PSNR	MSE	PSNR	MSE	PSNR
Image 1	0.054	60.807	0.182	55.530	0.282	53.628	1.565	46.186
Image 2	0.075	59.380	0.169	55.852	0.226	54.590	2.063	44.986
Image 3	0.043	61.796	0.200	55.121	0.230	54.514	2.220	44.667
Image 4	0.125	57.162	0.209	54.929	0.256	54.048	2.063	44.986
Image 5	0.128	57.059	0.176	55.676	0.227	54.571	2.542	44.079

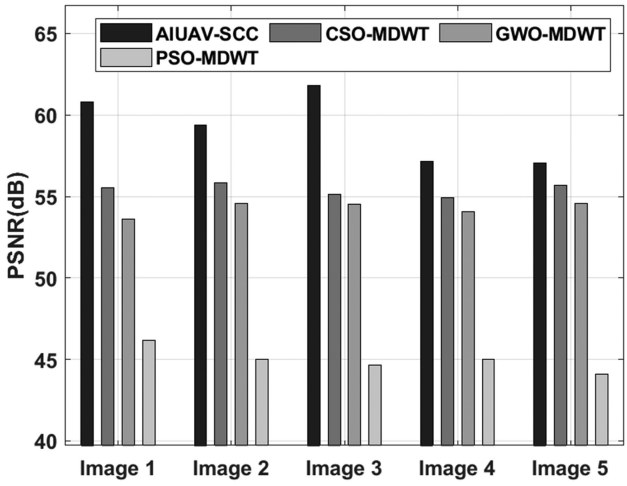

Fig. 5. PSNR analysis of AIUAV-SCC method with recent approaches.

function: softmax. Fig. 4 illustrates the sample test images in the UCM dataset.

A detailed comparative study of the AIUAV-SCC model with recent algorithms takes place in Table I. The results showcase that the PSO-MDWT technique has offered insignificant outcomes with the maximum MSE value. On continuing with, the GWO-MDWT and CSO-MDWT techniques have resulted in moderate MSE values. But the proposed AIUAV-SCC model has accomplished improved results with the lesser MSE values. For instance, on test image 1, the AIUAV-SCC technique has resulted in a lesser MSE of 0.054 whereas the CSO-MDWT, GWO-MDWT, and PSO-MDWT models have demonstrated slightly higher MSE of 0.182, 0.282, and 1.565, respectively. Next to that, on test image 3, the AIUAV-SCC method has resulted in a lower MSE of 0.043 while the CSO-MDWT, GWO-MDWT, and PSO-MDWT approaches have revealed slightly superior MSE of 0.200, 0.230, and 2.220, respectively. Finally, on test image 5, the AIUAV-SCC methodology has resulted in a minimal MSE of 0.128 whereas the CSO-MDWT, GWO-MDWT, and PSO-MDWT models have showcased slightly higher MSE of 0.176, 0.227, and 2.542 correspondingly.

Fig. 5 showcases the PSNR analysis of the AIUAV-SCC model with other models. From the figure, it can be apparent that the AIUAV-SCC system has offered superior outcomes with higher PSNR values. For instance, on test image 1, the AIUAV-SCC technique has attained a maximum PSNR of 60.807 dB whereas the CSO-MDWT, GWO-MDWT, and PSO-MDWT models have obtained a minimum PSNR of 55.530, 53.628, and 46.186 dB, respectively. Simultaneously, on the test image 5, the AIUAV-SCC manner has attained a maximum PSNR of 57.059 dB, whereas the CSO-MDWT, GWO-MDWT, and PSO-MDWT models have obtained a minimum PSNR of 55.676, 54.571, and 44.079 dB correspondingly.

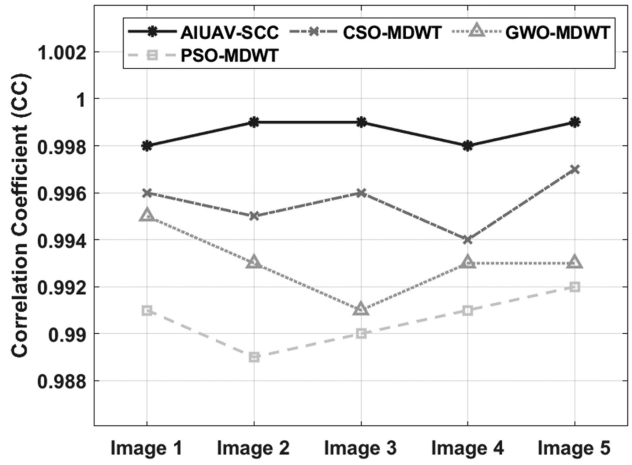

Fig. 6. CC analysis of AIUAV-SCC model with recent approaches.

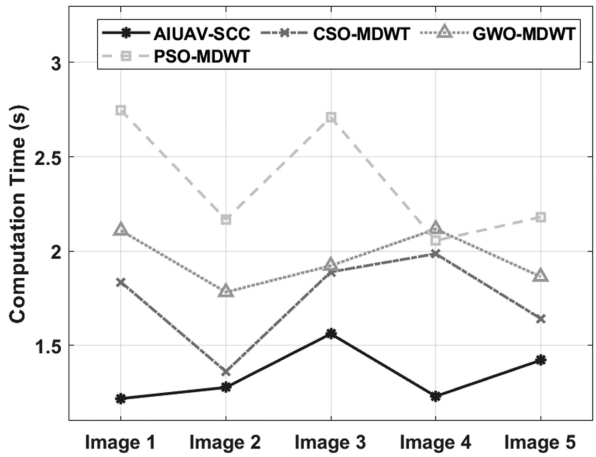

Fig. 7. CT analysis of AIUAV-SCC model with existing techniques.

Fig. 6 showcases the CC analysis of the AIUAV-SCC method with other techniques. From the figure, it is noticed that the AIUAV-SCC technique has offered superior results with higher CC values. For instance, on test image 1, the AIUAV-SCC technique has attained a maximum CC of 0.998 whereas the CSO-MDWT, GWO-MDWT, and PSO-MDWT models have obtained a minimum CC of 0.996, 0.995, and 0.991, respectively. Concurrently, on test image 5, the AIUAV-SCC algorithm has obtained an increased CC of 0.999 whereas the CSO-MDWT, GWO-MDWT, and PSO-MDWT models have obtained a minimum CC of 0.997, 0.993, and 0.992, respectively.

Fig. 7 demonstrates the CT examination of the AIUAV-SCC technique with other techniques [19]. The PSO-MDWT technique has offered insignificant outcomes with the maximum CT value. On continuing with, the GWO-MDWT and CSO-MDWT

TABLE II
PERFORMANCES OF PROPOSED WITH EXISTING MODELS ON THE UCM DATASET

Methods	Precision	Recall	F1-Score	F2-Score
CNN	80.09	81.78	78.99	80.18
CNN -RBFNN	78.18	83.91	78.80	81.14
CA-CNN -BiLSTM	79.33	83.99	79.78	81.69
AL-RN-CNN	87.62	86.41	85.70	85.81
MLRSSC-CNN–GNN-SGAT	86.41	88.17	86.09	87.03
MLRSSC-CNN-GNN-MLI GAT	87.11	88.41	86.39	87.27
BO-SqueezeNet	92.57	93.50	93.12	93.42

techniques have resulted in moderate CT values. But the proposed AIUAV-SCC manner has accomplished increased results with minimum CT values.

Finally, a comprehensive classification results analysis of the BO-SqueezeNet approach with other algorithms [26] on UCM dataset takes place in Table II. By looking into the experimental values, it is obvious that the BO-SqueezeNet technique has outperformed all the other methodologies with the maximal precision of 92.57%, recall of 93.50%, F1-score of 93.12%, and F2-score of 93.42%. From the aforementioned result analysis, it can be apparent that the proposed method is established to be a suitable tool for securely transmitting data and classifying images for the UAV networks in Industry 5.0 environment.

V. CONCLUSION

This article has developed a novel AIUAV-SCC technique for reliable data transmission by UAVs in Industry 5.0 environment. The presented method contains distinct stages of operations like channel extraction, multilevel DWT-based decomposition, QBCO based optimal pixel selection, encryption, and embedding process. The QBCO algorithm is developed by the incorporation of QC concepts into the traditional BCO algorithm to improve the convergence rate. Furthermore, three encryption techniques such as signcryption, EPKC, and KHE are applied for the R, G, and B channels of the secret image. For examining the effective outcome of the AIUAV-SCC model, a set of experimentations take place on UCM dataset aerial dataset and the outcomes are investigated under several dimensions. The experimental outcome ensured the goodness of the presented model on the test UCM aerial dataset over the compared methods. In the future, on-board data compression techniques can be employed to reduce the data being transmitted in the 6G environment.

REFERENCES

[1] H. H. R. Sherazi, L. A. Grieco, M. A. Imran, and G. Boggia, "Energy-efficient LoRaWAN for industry 4.0 applications," *IEEE Trans. Ind. Informat.*, vol. 17, no. 2, pp. 891–902, Feb. 2021.

[2] S. Nahavandi, "Industry 5.0—A human-centric solution," *Sustainability*, vol. 11, no. 16, 2019, Art. no. 4371.

[3] S. Shah *et al.*, "Security measurement in industrial IoT with cloud computing perspective: Taxonomy, issues, and future directions," *Sci. Program.*, 2020, 2020 Art. no. 8871315.

[4] L. W. Qin *et al.*, "Precision measurement for industry 4.0 standards towards solid waste classification through enhanced imaging sensors and deep learning model," *Wireless Commun. Mobile Comput.*, 2021, 2021, Art. no. 9963999.

[5] M. M. Ahsan, I. Ali, M. Imran, M. Y. I. Idris, S. Khan, and A. Khan, "A fog-centric secure cloud storage scheme," *IEEE Trans. Sustain. Comput.*, to be published, doi: 10.1109/TSUSC.2019.2914954.

[6] R. Gupta, A. Nair, S. Tanwar, and N. Kumar, "Blockchain-assisted Secure UAV Communication in 6G Environment: Architecture, Opportunities, and Challenges," *IET Commun.*, vol. 15, pp. 1352–1367, 2021.

[7] J. Sengupta, S. Ruj, and S. D. Bit, "A secure fog-based architecture for industrial internet of things and industry 4.0," *IEEE Trans. Ind. Informat.*, vol. 17, no. 4, pp. 2316–2324, Apr. 2021.

[8] S. K. Lakshmanaprabu *et al.*, "An effect of big data technology with ant colony optimization based routing in vehicular ad hoc networks: Towards smart cities," *J. Cleaner Prod.*, vol. 217, pp. 584–593, 2019.

[9] M. A. Jan *et al.*, "Lightweight mutual authentication and privacy-preservation scheme for intelligent wearable devices in Industrial-CPS," *IEEE Trans. Ind. Informat.*, vol. 17, no. 8, pp. 5829–5839, Aug. 2021.

[10] D. Sharma, S. K. Gupta, A. Rashid, S. Gupta, M. Rashid, and A. Srivastava, "A novel approach for securing data against intrusion attacks in unmanned aerial vehicles integrated heterogeneous network using functional encryption technique," *Trans. Emerg. Telecommun. Technol.*, vol. 32, 2020, Art. no. e4114.

[11] Y. Lei, L. Zeng, Y. X. Li, M. X. Wang, and H. Qin, "A lightweight authentication protocol for UAV networks based on security and computational resource optimization," *IEEE Access*, vol. 9, pp. 53769–53785, 2021.

[12] T. T. Khoei, E. Ghribi, P. Ranganathan, and N. Kaabouch, "A performance comparison of encryption/decryption algorithms for UAV swarm communications," 2021, doi: 10.13140/RG.2.2.17379.48160.

[13] S. He, Q. Wu, J. Liu, W. Hu, B. Qin, and Y. N. Li, "Secure communications in unmanned aerial vehicle network," in *Proc. Int. Conf. Informat. Secur. Pract. Experience*, 2017, pp. 601–620.

[14] I. García-Magariño, R. Lacuesta, M. Rajarajan, and J. Lloret, "Security in networks of unmanned aerial vehicles for surveillance with an agent-based approach inspired by the principles of blockchain," *Ad Hoc Netw.*, vol. 86, pp. 72–82, 2019.

[15] T. Li *et al.*, "Lightweight secure communication mechanism towards UAV networks," in *Proc. IEEE Globecom Workshops*, 2019, pp. 1–6.

[16] C. L. Chen, Y. Y. Deng, W. Weng, C. H. Chen, Y. J. Chiu, and C. M. Wu, "A traceable and privacy-preserving authentication for UAV communication control system," *Electronics*, vol. 9, no. 1, 2020, Art. no. 62.

[17] X. Duan, N. Liu, M. Gou, W. Wang, and C. Qin, "SteganoCNN: Image steganography with generalization ability based on convolutional neural network," *Entropy*, vol. 22, no. 10, 2020, Art. no. 1140.

[18] M. S. Haque and M. U. Chowdhury, "A new cyber security framework towards secure data communication for unmanned aerial vehicle (UAV)," in *Proc. Int. Conf. Secur. Privacy Commun. Syst.*, 2017, pp. 113–122.

[19] Ambika, R. L. Biradar, and V. Burkpalli, "Encryption-based steganography of images by multiobjective whale optimal pixel selection," *Int. J. Comput. Appl.*, pp. 1–10, 2019, doi: 10.1080/1206212X.2019.1692442.

[20] B. Niu and H. Wang, "Bacterial Colony Optimization," *Discrete Dyn. Nature Soc.*, 2012, 2012, Art. no. 698057.

[21] H. Wang, L. Tan, and B. Niu, "Feature selection for classification of microarray gene expression cancers using bacterial colony optimization with multi-dimensional population," *Swarm Evol. Comput.*, vol. 48, pp. 172–181, 2019.

[22] D. Wang, H. Chen, T. Li, J. Wan, and Y. Huang, "A novel quantum grasshopper optimization algorithm for feature selection," *Int. J. Approx. Reasoning*, vol. 127, pp. 33–53, 2020.

[23] M. Elhoseny and K. Shankar, "Reliable data transmission model for mobile ad hoc network using signcryption technique," *IEEE Trans. Rel.*, vol. 69, no. 3, pp. 1077–1086, Sep. 2020.

[24] G. Kalyani and S. Chaudhari, "Data Privacy Preservation in MAC Aware Internet of Things With Optimized Key Generation," *J. King Saud Univ.-Comput. Inf. Sci.*, 2019.

[25] S. Ullah, X. Y. Li, M. T. Hussain, and Z. Lan, "Kernel homomorphic encryption protocol," *J. Inf. Secur. Appl.*, vol. 48, 2019, Art. no. 102366.

[26] Oct. 2010. [Online]. Available: http://weegee.vision.ucmerced.edu/datasets/landuse.html

[27] 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 Sens.*, vol. 12, no. 23, 2020, Art. no. 4003.