Pakistan Journal of Engineering Technology and Science (PJETS)
Volume 13. Issue.1, PP. 103-112, JUNE 2025
https://doi.org/10.22555/pjets.v13I1.1349
E-ISSN 2224-2333
P-ISSN 2222-9930

AI-Powered UAV-Patrolling Drone For Real-Time Unauthorized Person Detection

Khurram Iqbal[1*], Muhammad Saad Bin Ehtisham[2], Muzammil Ahmad Khan[3], Adnan Chohan[1], Perfshan Erum[4], Khalil ur Rahman[5]

[1]*Hamdard University, Department of Computing, Faculty of Engineering Science and Technology, Karachi, Pakistan*

[2]*National University of Modern Languages, Department of Computer Science, Faculty of Engineering and Computing, Karachi, Pakistan*

[3]*Sir Syed University of Engineering and Technology, Computer Engineering Department, Karachi, Sindh, Pakistan*

[4]*NED University of Engineering and Technology, Department of Mathematics, Karachi, Sindh, Pakistan*

[5]*Nazeer Hussain University, Department of Electrical Engineering, Karachi, Sindh, Pakistan*

[*]*Corresponding Author: khurramiqbal.nust@gmail.com*

ABSTRACT:

In the modern era, the integrity and safety of secure environments have become critically important. To address these challenges, an AI-powered UAV-patrolling drone system for real-time unauthorized person detection has been proposed. This drone executes pre-determined flight paths, strategically covering surveillance gaps left by static CCTV cameras or human guards. The system integrates multiple state-of-the-art technologies, incorporating advanced facial recognition using Dlib-HOG, CNN, VGG-Face, Google FaceNet, and OpenFace, along with comprehensive facial analysis providing real-time analysis of race, age, gender, and facial expressions. This technology is especially valuable for securing large venues, critical infrastructure, and high-profile events where unauthorized access poses significant risks. The system's hybrid architecture allows for optimal performance across different lighting conditions, angles, and crowd densities, setting a new standard for intelligent surveillance systems.

Keywords: *Drone surveillance, Unconstrained Environment, Un-authorized Person Detection, Surveillance Videos, Face Recognition, Facial expression Analysis & Prediction.*

I. INTRODUCTION

This article investigates the integration of face recognition technology with unmanned aerial vehicles (UAVs) for various applications [1-5]. The main aim is to equip drones with the ability to identify individuals on the ground for applications like surveillance, patrolling, and remote monitoring. Advanced face recognition relies on deep learning, systems encouraged by the functionality of the human brain, and strives to emulate human-like intelligence through artificial systems [6-8]. Deep learning contains convolutional neural networks (CNNs) and generative neural networks. Among these, convolutional neural networks have proven highly effective in addressing computer vision challenges and are extensively utilized in face recognition tasks [9-10].

During public events, such as concerts and large gatherings, there have been numerous cases of unauthorized person entry violations that are difficult to detect manually by a security guard or a random CCTV camera because their field of view is too limited. It is essential to develop AI-driven autonomous drones alongside diverse cutting-edge face recognition and expression analysis models, depending upon the situation, in order to increase accuracy, especially when distance and resolution are key parameters [11-15].

1.1 Comments on the Literature Review

To create the proposed system, the literature review discusses relevant previous studies to express a particular area of research. For this purpose, the articles cited above were considered for implementing and constructing the required system. The existing study integrated a Dlib-HOG, CNN, VGG-Face, Google FaceNet, and OpenFace model to detect race, age, gender, and facial expressions accurately. Face recognition using drones equipped with high-resolution cameras for face recognition has been documented in existing literature (Table 1). However, the main objective of our artical is to detect any un-authorized person in our desired envionent and provide face recognition, facial analysis & expression predictions of that Un-Authorized Person's face with an accuracy up to 99.85% on high resolution and at least up to 60% on low resolution using a hybrid model, which is useful for security guards and security teams by leveraging UAV-patrolling drones paired with intelligent cameras [16-21]. The existing systems' comparative analysis is performed in the following Table 1.

Table 1: Review of Existing Research Literature

Sr. No.	Research Article	Year	Methodology	Drone Surveillance
1	Open Source Face Recognition	2022	Hybrid Framework Review	No
2	Real-Time Face Detection and Face Recognition	2022	OpenCV & Python	No
3	Drone-Based Face Recognition Using Deep Learning	2021	VGG16	Yes
4	Convolutional neural networks for image classification	2020	CNN	No
5	Emotion Recognition Using Image Processing	2020	GAN (Generative Adversarial Network)	No

II. MATERIALS AND METHODS

2.1 Convolution Operation

Figure 1 shows a 2D image of *f* and *g*. The convolutional operation can be defined as:

$$(f * g)(x, y) = \sum_{i=-k}^{k} \sum_{j=-k}^{k} g(i, j).f(x + i, y + j) \quad (1)$$

Where $f(x, y)$ is inpuimage, $g(i, j)$ is the filter, and k is the size of the filter

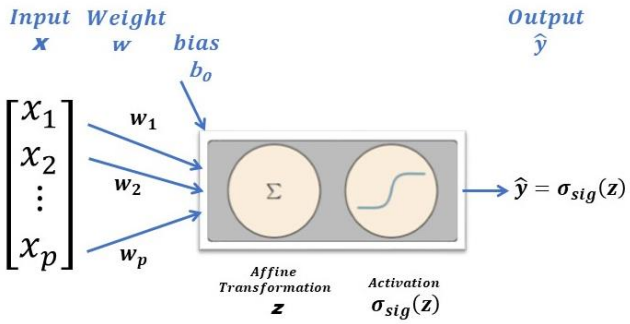

Figure 1: The sigmoid model represented with neural network terminology as a shallow neural network.

Mathematical modelling is essential in Convolutional Neural Networks as they present non linear functions, allowing the setup to detect difficult arrangements inside the data available.The Convolutional Neural Networks helping the network develop more expressive representations. Without activation functions, the network would be restricted to linear transformations, significantly limiting its ability to model complex relationships within the data [22-26].

$$\sigma_{sig}(z) = \frac{1}{1 + e^{-z}} \tag{2}$$

Where x is input vector and b_0 is bias term

2.2 ReLU Activation Function

$$ReLU(z) = max(0, z) \tag{3}$$

2.3 Pooling Operation

$$P(x, y) = max_{(i,j)\epsilon R} f(x + i, y + j) \tag{4}$$

2.4 Fully Connected Layer

It is described as

$$z = b_0 + \sum_{i=1}^{p} w_i x_i \tag{5}$$

2.5 Convolutional layer of a Convolutional Neural Network

The convolutional relation between the Input and Filter provides an output. [28]:

$$\frac{\partial L}{\partial F} = Convolution(Input\ X, Loss\ gradient\ \frac{\partial L}{\partial O})$$

$$\frac{\partial L}{\partial F} = \frac{\partial L}{\partial O} * \frac{\partial O}{\partial F} \tag{6}$$

For every element of x_i

$$\partial L/\partial x_i = \sum_{j=1}^{m} \partial L/\partial O_j * \partial O_j/\partial x_i \tag{7}$$

Where $\frac{\partial L}{\partial F}$ is gradient to updated filter F, $\frac{\partial L}{\partial O}$ is loss gradient from earlier layer and $\frac{\partial O}{\partial F}$ is local gradients, O and F are matrices

2.6 F1-score

$$Precision = \frac{TP}{TP + FP} \tag{8}$$

$$Recall = \frac{TP}{TP + FN} \tag{9}$$

Where

This system includes True positive and false positive and true negative and false negative values.

The F1-score, which is a harmonic mean of precision and recall, can be calculated [29, 30]:

$$F1 = 2 \times \frac{Precision \times Recall}{Precision + Recall} \tag{10}$$

III. RESULTS AND DISCUSSION

Face recognition using drone cameras has been reported by researchers in the literature [1-3, 26, 27], but this project implements a real-time Detection of Unauthorized Persons using a Face Recognition Hybrid Model, which allows you to switch between the various face recognition models. In real-time systems, computational time is a very big parameter, and it affects the efficiency of the system, especially where distance and resolution are important. The user can select from up to 10 state-of-the-art Face Recognition Frameworks on a UAV-Autonomous Drone surveillance to detect Unauthorized Persons with high accuracy, from 99.85%. As shown in Figures 2,3, and 4.

3.1.1 Face Recognition Framework

Figure 2: Loading image in Face-Recognition, Source: face-recognition documentation [28]

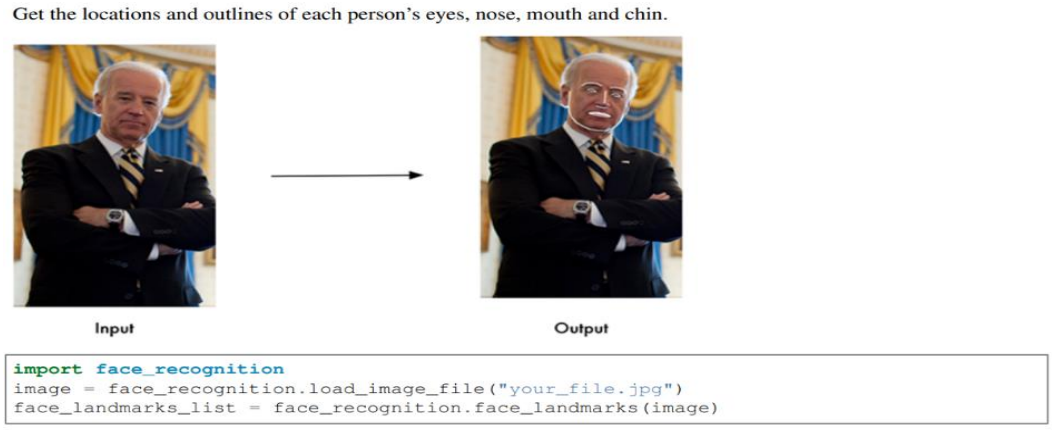

Figure 3: Face Landmarks Detection, Source: face-recognition documentation [28]

```
import face_recognition
known_image = face_recognition.load_image_file("biden.jpg")
unknown_image = face_recognition.load_image_file("unknown.jpg")

biden_encoding = face_recognition.face_encodings(known_image)[0]
unknown_encoding = face_recognition.face_encodings(unknown_image)[0]

results = face_recognition.compare_faces([biden_encoding], unknown_encoding)
```

Figure 4: Face Recognition Method, Source: face-recognition documentation

3.1.2 Speeding Up the Recognition

Face recognition can be performed efficiently by utilizing multiple CPU cores on a computer. For instance, if your computer has 4 CPU cores, the processing speed can be increased by a factor of 4 by utilizing all the cores simultaneously (Figure 5). If you are utilizing Python version 3.4 or above, you can specify the number of cores to be used by passing the '**–cpus'** parameter.

```
$ face_recognition --cpus 4 ./pictures_of_people_i_know/ ./unknown_pictures/
```

Figure 5: Speeding Up the Recognition

3.1.3 DeepFace Hybrid Framework

Figures 6-8 show the DeepFace framework, facial attributes analysis, and framework accuracy analysis, respectively.

```
models = ["VGG-Face", "Facenet", "Facenet512", "OpenFace", "DeepFace", "DeepID", "ArcFace", "Dlib", "SFace"]

#face verification

result = DeepFace.verify(img1_path = "img1.jpg", img2_path = "img2.jpg", model_name = models[1])

#face recognition

df = DeepFace.find(img_path = "img1.jpg", db_path = "C:/workspace/my_db", model_name = models[1]
```

Figure 6: DeepFace framework

```
obj = DeepFace.analyze(img_path = "img.jpg", actions = ['age', 'gender', 'race', 'emotion'])
```

Figure 7: Facial Attributes Analysis, Source: Deep Face Documentation

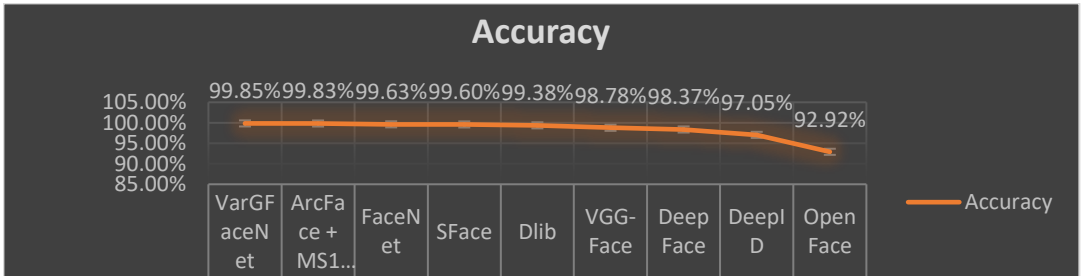

Figure 8: Frameworks Accuracy Analysis

Start Surveillance System: This button will open the Surveillance window, to connect the drone and start surveillance, "Exit Program", to exit the application (Figure 9):

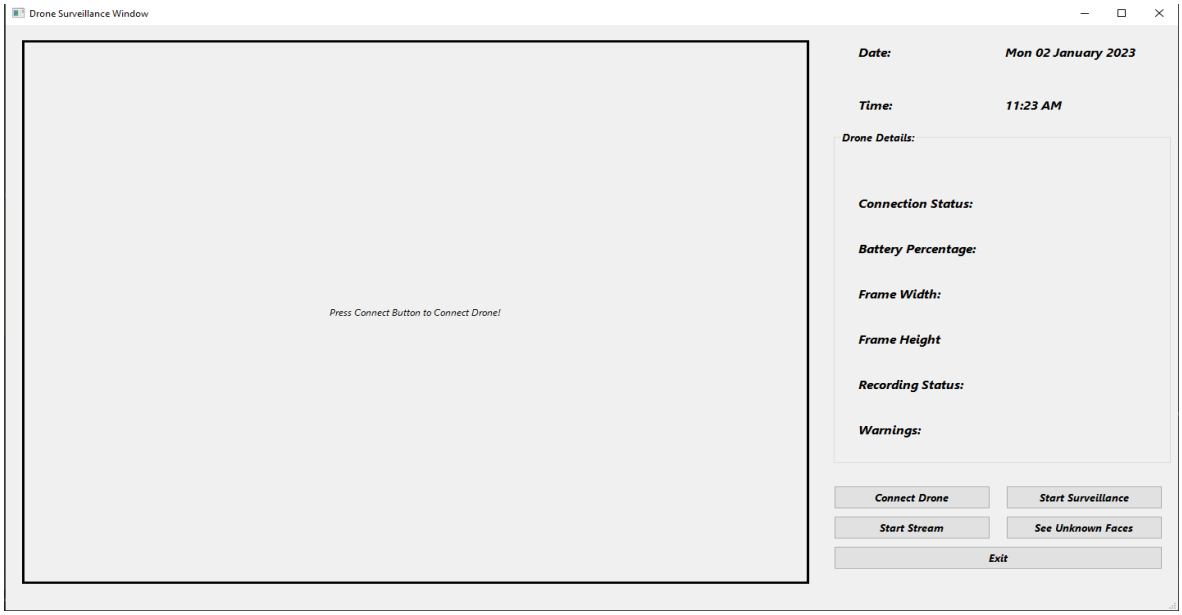

Figure 9: Surveillance System Window

Press the "Connect Drone" Button to connect the drone with the Surveillance System, but before that Tello Drone must be on and connected with Wifi on the Workstation. The "Start Surveillance" button will let the drone take off and fly through the predefined path given.

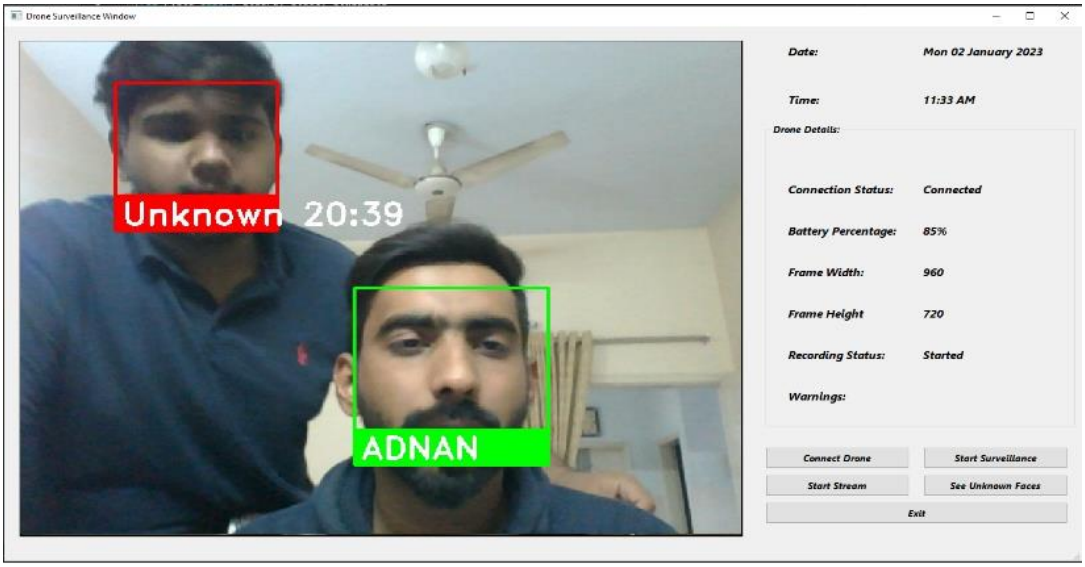

Figure 10: Surveillance Output

Press "Open Camera" to initialize the camera/webcam to take a picture of the authorized person (Figure 10). The "Capture Image" button will take a picture. "Register This Person" Button will take the picture of this authorized person and take out the face encodings that which will store the face encodings in a List and dump it into the database. For Guidance, a Text Box is given that guides step by step on what to do. Face Analysis Output is shown in Figure 11.

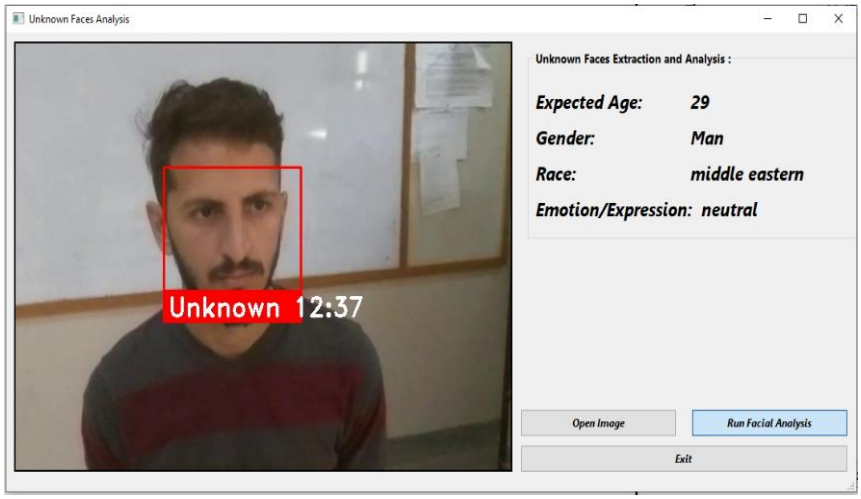

Figure 11: Face Analysis Output

3.2 Application Testing

The tables below show the application testing cases (Table 2-9)

Table 2: Test Case 1

Pre-Conditions	Checking the application execution
Actions	Run the application after installing all the dependencies
Result	Passed
On Failure	The program will not execute/launch or crash after stating
Prepared &Tested By	Adnan Chohan

Table 3: Test Case 2

Pre-Conditions	Checking the working of the Buttons of the Main Page
Actions	Run the application, press all the buttons
Result	Passed
On Failure	The program will crash, or the buttons will not be functional
Prepared &Tested By	Adnan Chohan

Table 4: Test Case 3

Pre-Conditions	Checking all the Windows to see if popping up or not
Actions	Run the application, press the button of the required window to open.
Result	Passed
On Failure	The program will crash, or the buttons will not be functional, and the window will open but not be functional
Prepared &Tested By	Saad Bin Ehtisham

Table 5: Test Case 4

Pre-Conditions	Checking Drone Connectivity with the application
Actions	Run the application, press the "Connect Drone" button, and check the connectivity status
Result	Passed
On Failure	The program will crash, or the buttons will not be functional, and the Drone will not get connected
Prepared &Tested By	Saad Bin Ehtisham

Table 6: Test Case 5

Pre-Conditions	Checking the Face Analysis Function
Actions	Run the application, open the face analysis window from the Surveillance window, and run the analysis
Result	Passed
On Failure	The program will crash, or the buttons are not functional, and analysis will not run, and any execution error
Prepared &Tested By	Saad Bin Ehtisham

Table 7: Test Case 6

Pre-Conditions	Checking the Person Registration
Actions	Run the application, open the Register Person Window, and start registering the persons by capturing Images
Result	Passed
On Failure	The program will crash, or buttons are not functional and pictures are not getting captured, and Person registration is failing
Prepared &Tested By	Saad Bin Ehtisham

Table 8: Test Case 7

Pre-Conditions	Checking Drone Save Take off and Landing
Actions	Run the application, start Drone Surveillance to take off the drone, and check if it is landing safely after patrolling
Result	Passed
On Failure	The program will crash Drone will not take off or land, or crash somewhere
Prepared & Tested By	Saad Bin Ehtisham

Table 9: Test Case 8

Pre-Conditions	Checking the Recordings and Unknown Faces Capturing
Actions	Run the application, start Drone Surveillance to take off the drone, and recording will auto start and will capture unknown faces if detected
Result	Passed
On Failure	The program will crash Drone will not take off or did not land, or will crash somewhere, or the recording will not start or will not recognize faces
Prepared &Tested By	Saad Bin Ehtisham

IV. CONCLUSION

In summary, the current research offers a solid and ingenious approach for bolstering security in immense areas by deploying a drone with a camera for spontaneous monitoring. To overcome the drawbacks of conventional surveillance techniques like stationary CCTV cameras and human patrols, the system enhances facial identification and analysis by combining deep learning and convolutional neural networks (CNNs) with a hybrid model. To make it possible to guarantee a more adaptive and all-encompassing security solution, the unmanned aerial vehicle's ability to patrol predefined routes across under-monitored regions and its comprehensive facial analysis capabilities, which incorporate features like age, gender, race, and expressions, are coupled. This system makes use of state-of-the-art artificial neural network (ANN) approaches to simulate human cognitive procedures by using models such as Dlib-HOG CNN, Google FaceNet, VGG-Face, OpenFace, Facebook DeepFace, DeepID, ArcFace, and SFace for recognition and the DeepFace module for evaluation of facial features. Through this study, we show whether a hybrid system of this kind might revolutionize video surveillance by providing a dependable, adaptable, and versatile way to successfully satisfy today's exigencies for safety.

REFERENCES

[1] D. Wanyonyi and T. Celik, "Open-Source Face Recognition Frameworks: A Review of the Landscape," IEEE Access, vol. 10, pp. 50601-50623, 2022.

[2] G. Amato, F. Falchi, C. Gennaro, F. V. Massoli, and C. Vairo, "Multi-Resolution Face Recognition with Drones," presented at the 2020 3rd International Conference on Sensors, Signal and Image Processing, Prague, Czech Republic, 2020. [Online]. Available: https://doi.org/10.1145/3441233.3441237.

[3] P. Chandrakala, B. Srinivas, and M. A. Kumar, "Real Time Face Detection and Face Recognition using OpenCV and Python," 2022.

[4] R. Th. Hasan and A. Bibo Sallow, "Face Detection and Recognition Using OpenCV," Journal of Soft Computing and Data Mining, vol. 2, no. 2, pp. 86-97, 10/24 2021. [Online]. Available: https://publisher.uthm.edu.my/ojs/index.php/jscdm/article/view/8791.

[5] H. Kikuchi, K. Eto, K. Waki, and T. Mori, "Vulnerability of privacy visor used to disrupt unauthorized face recognition," in 2021 IEEE Conference on Dependable and Secure Computing (DSC), 2021: IEEE, pp. 1-7.

[6] A. Deeb, K. Roy, and K. D. Edoh, "Drone-Based Face Recognition Using Deep Learning," Advanced Machine Learning Technologies and Applications, p. 197, 2021.

[7] A. O. Tarasenko and Y. V. Yakimov, "Convolutional neural networks for image classification," 2020.

[8] M. Rouhsedaghat, Y. Wang, S. Hu, S. You, and C. Kuo, Low-Resolution Face Recognition In Resource-Constrained Environments. 2020.

[9] A. R. Revanda, C. Fatichah, and N. Suciati, "Utilization of Generative Adversarial Networks in Face Image Synthesis for Augmentation of Face Recognition Training Data," in 2020 International Conference on Computer Engineering, Network, and Intelligent Multimedia (CENIM), 2020: IEEE, pp. 396-401.

[10] Q. Frimpong, "Emotion recognition using image processing," 2020.

[11] C. Piciarelli and G. Foresti, Drone patrolling with reinforcement learning. 2019, pp. 1-6.

[12] H.-J. Hsu and K.-T. Chen, Face Recognition on Drones. 2015, pp. 39-44.

[13] Y. Li et al., "Deep Learning for UAV-Based Face Detection: Challenges and Solutions," *Remote Sens.*, vol. 14, no. 3, 2022.

[14] J. Wang and L. Zhang, "Edge-Computing-Driven Face Recognition for Drones," *IEEE IoT J.*, vol. 9, no. 10, 2022.

[15] S. Chen et al., "Real-Time Face Recognition on Embedded Systems Using OpenCV," *J. Real-Time Image Process.*, vol. 18, pp. 1023–1036, 2021.

[16] K. He et al., "Masked Face Recognition: A Comparative Study," *IEEE FG*, 2021.

[17] L. Wei et al., "Privacy-Preserving Face Recognition in Public Spaces," *IEEE Trans. Inf. Forensics Secur.*, vol. 16, 2021.

[18] M. Sandler et al., "MobileFaceNets: Efficient CNNs for Face Recognition on Mobile Devices," *IEEE CVPR*, 2020.

[19] T. Baltrusaitis et al., "OpenFace 2.0: Facial Behavior Analysis Toolkit," *IEEE Trans. Affect. Comput.*, 2020.

[20] A. Geitgey, "Face Recognition with Python and OpenCV," *O'Reilly Media*, 2020.

[21] R. Ranjan et al., "Unconstrained Face Recognition Using Deep Learning," *Int. J. Comput. Vis.*, vol. 127, 2019.

[22] F. Schroff et al., "FaceNet: A Unified Embedding for Face Recognition," *IEEE CVPR*, 2015.

[23] A. Krizhevsky et al., "ImageNet Classification with Deep Convolutional Neural Networks," *NIPS*, 2012.

[24] P. Viola and M. Jones, "Rapid Object Detection Using a Boosted Cascade of Simple Features," *IEEE CVPR*, 2001.

[25] N. Dalal and B. Triggs, "Histograms of Oriented Gradients for Human Detection," *IEEE CVPR*, 2005.

[26] D. King, "Dlib: A Modern C++ Toolkit for Machine Learning," *J. Open Source Softw.*, 2017.

[27] O. M. Parkhi et al., "Deep Face Recognition," *BMVC*, 2015.

[28] Y. Taigman et al., "DeepFace: Closing the Gap to Human-Level Recognition," *IEEE CVPR*, 2014.

[29] I. Goodfellow et al., "Generative Adversarial Networks," *NIPS*, 2014.

[30] C. Szegedy et al., "Going Deeper with Convolutions," *IEEE CVPR*, 2015.