Impact Factor 6.1

Journal of Cyber Security

ISSN:2096-1146

Scopus

DOI

Google Scholar

More Information
www.journalcybersecurity.com

Crossref doi Google Scholar scopus

Face Recognition-Based Video Surveillance and Tracking System

Ramakrishna Hegde[1] and Soumyasri S M[2]

1. Professor, Dept. of CSE, JSS Science and Technology University, Mysore
2. Associate Professor, Dept. of MCA, Vidya Vikas Institute of Engineering and Technology, Mysore

Abstract **- This abstract explores the innovative landscape of video-surveillance-and-tracking systems employing facial recognition technology, delving into their background, social benefits, and implications. These systems represent a pivotal advancement in security and data analysis, leveraging artificial intelligence and computer vision to redefine surveillance capabilities. The background of innovation stems from the pressing need for enhanced security measures in various sectors, including public safety and transportation. By addressing limitations in traditional surveillance methods, facial recognition- enabled systems offer real-time identification and tracking of individuals with unprecedented accuracy. Furthermore, these systems align with societal demands for improved safety protocols, aiding in deterring criminal activities and optimizing resource allocation for security personnel. However, their deployment also raises ethical and privacy concerns, necessitating robust safeguards and transparent governance frameworks. Ultimately, video surveillance and tracking systems using facial recognition technology hold the potential to enhance public safety while navigating complex ethical considerations. The proposed system offers a powerful solution for live location tracking and access management through the integration of CCTV cameras, facial recognition, Python-based computer vision, and machine learning techniques. By addressing the limitations of traditional methods and leveraging advanced technologies, this project contributes to enhancing security, efficiency, and convenience in premises management.**

Keywords: Video Surveillance, facial Recognition, machine Learning, artificial intelligence.

I. INTRODUCTION

In an era marked by increasing security concerns and the ever- growing need for advanced surveillance technologies, the convergence of video surveillance and facial recognition has emerged as a game-changing solution. This integration combines the power of video cameras and facial recognition algorithms to create a comprehensive system that significantly enhances security, monitoring, and access control in a wide range of environments.

Video surveillance, a staple of security infrastructure for decades, has evolved from analogue closed-circuit television (CCTV) systems to high-definition digital networks. These systems have been instrumental in deterring and documenting security breaches, but their effectiveness often depends on human monitoring and manual review of extensive video footage [4]. Facial recognition, once a realm of science fiction, has evolved into a sophisticated tool with the potential to revolutionize how we monitor and secure our surroundings [3]. This technology leverages the unique characteristics of an individual's face to accurately identify and track them within a network of cameras. What was once a futuristic concept is now a tangible reality, finding applications across diverse sectors such as law enforcement, commercial enterprises, transportation hubs, and public spaces.

The value of facial recognition rests not only in its ability to match faces with known individuals or identified persons of interest quickly and correctly but also in its real-time tracking capabilities [1]. It enables surveillance systems to track persons as they move across monitored regions, providing previously impossible levels of situational awareness.

Despite the promise of enhanced security and efficiency, face recognition technology has sparked issues about ethics, privacy, and information about ethics usage. Concerns about algorithm bias, data privacy violations, and the need for legal frameworks have made it critical to traverse this technological world with precaution and responsibility [4].

This exploration delves into the realm of tracking and video surveillance using facial recognition technology, examining its underlying principles, applications, benefits, and the ethical dilemmas it poses. One promising use of convolutional neural networks (CNNs) is the improvement of surveillance techniques through real-time object detection[8].

II. RELATED WORK

Real-world applications of Face Recognition are currently being used to make the world safer, smarter, and more convenient.Some of its most common use cases include finding missing persons, solving retail crime, security identification, identifying accounts on social media, school attendance systems, and recognizing drivers in cars [4]. There are several methods to perform facial recognition depending on the performance and complexity.

Tradition Face Recognition Algorithms

In the 1990s, all methods of facial recognition were used. In the early 1990s, hand-drawn illustrations became popular, and then local learning techniques became popular in the late 2000s. Currently, face recognition and face recognition algorithms are widely used in OpenCV. are as follows:

- Eigenfaces (1991)
- Local Binary Patterns Histograms (LBPH) (1996)
- Fisherfaces (1997)
- Speed Up Robust Features (SURF) (2006)

Each technique takes a different approach to extracting the image information and preparing it for the input image. Fischer-faces and Eigenfaces have the same techniques as SURF and SIFT [5].
LBPH is a simple yet very efficient method but is slow compared to modern face recognizers.

These algorithms are not faster compared to modern-day face- recognition algorithms. Traditional algorithms can't be trained only by taking a single picture of a person.

Deep Learning for Face Recognition

Some of the widely used Deep Learning-based face recognition systems are:

- DeepFace
- DeepID series of systems
- VGGFace
- FaceNet

Face recognizers generally take face images and find the important points such as the corner of the mouth, an eyebrow, eyes, nose, lips, etc. The coordinates of these points are called facial feature points. There are 66 such points. In this way, a different technique for finding feature points gives different results [5, 1].

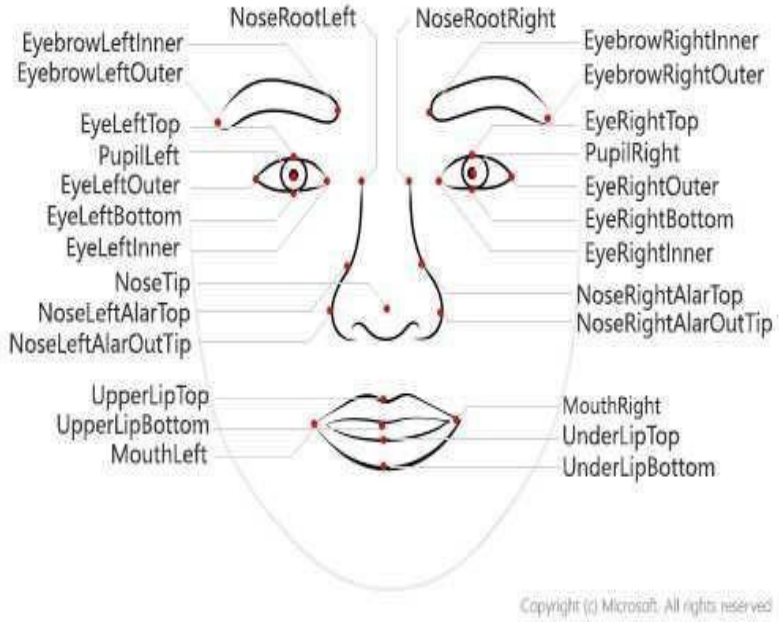


Fig. 1: Traditional Face Recognition Model. (Source: Microsoft)

Fig. 1 shows the traditional face recognition model and can be used in our application also.

How Does a Traditional Face Recognition Model Work?

- Face Detection: Face detector algorithms locate faces draw bounding boxes around faces and keep the coordinates of bounding boxes.
- Face Alignments: Normalize the faces to be consistent with the training database.
- Feature Extraction: Extract features of faces that will be used for training and recognition tasks.
- Face Recognition: Matching the face against one or more known faces in a prepared database. In the traditional method of face recognition, we had separate modules to perform these 4 steps, which was painful. -In this article, you will see a library that combines all these 4 steps in a single step [6]. The visual surveillance system needs reliable and quick ways to identify and follow moving objects. In this study,it looked into ways to use UAVs to track and detect objects[9]

III. METHODOLOGY

The "Video Surveillance and Tracking System Using Facial Recognition" relies on the face recognition library, a convenient wrapper for dlib's facial recognition functionalities. The system begins by uploading a clear image of the target individual, which is processed by the face recognition library in its default BGR format, requiring subsequent conversion to RGB for further analysis. The extracted facial encodings are then stored in an array, facilitating subsequent recognition. [1].

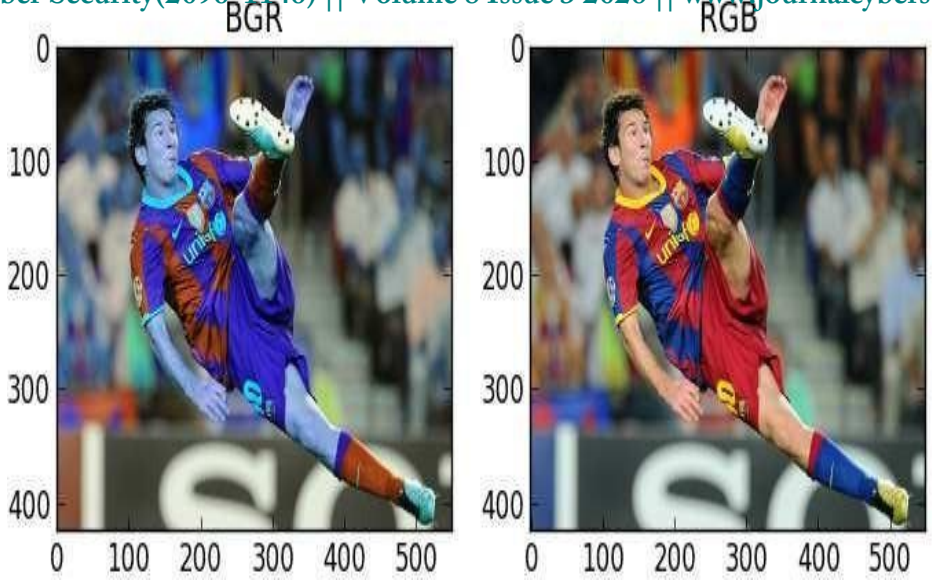
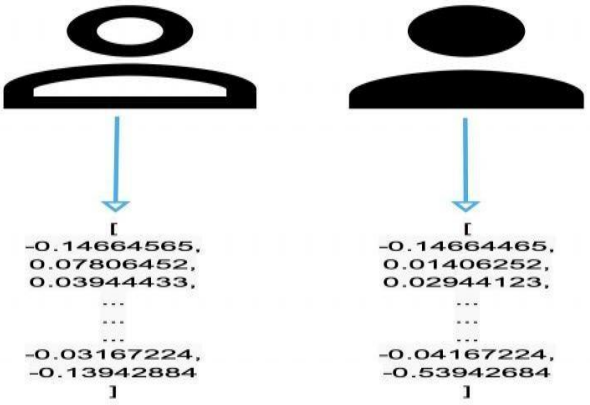


Fig. 2. a) BGR Format b) RGB format Fig. 2 a and b explain the BGR and RGB image formats.

In the operational phase, the system utilises the OpenCV library to access video frames. Each frame undergoes a 1/4 resizing exclusively for recognition purposes, contributing to improved Frames Per Second (FPS). The face recognition. Face locations function is applied to the resized image to detect faces, and the resulting bounding box coordinates are adjusted by a factor of 4 to align accurately with the output frame. For each detected face, the system computes face encodings using face recognition, Face



encodings().

Fig. 3 : Face encoding model

The Fig. 3 depicts the face recognition model. The face distance() function calculates the distance between the test image and all images in the training directory. The index corresponding to the minimum face distance indicates the matching face in the training set. Upon identifying a match, the system proceeds to mark the person. A bounding box is drawn around the recognized face using cv2, and the matching name is displayed on the output frame using cv2. The system captures and records the camera's location, along with the date and time, storing this information in a file. This comprehensive process ensures real-time facial recognition and tracking capabilities within a video surveillance framework. [1].

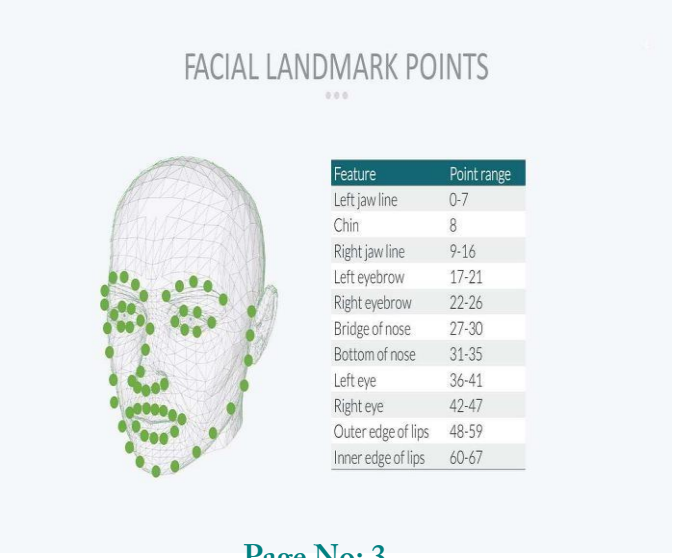


Fig. 4. Facial Landmark Points

Fig. 4 explains the facial landmark points which will be used in our research works. Main landmarks are left jawline, chin, right jawline, left eyebrow, right eyebrow, bridge of nose, bottom of nose, left eye, right eye, outer edges of lips and inner edges of lipps.The entire process can be summarized as follows:

The process begins by uploading a clear image of the target individual. This image is then processed in BGR format using the face recognition library and converted to RGB. Facial encodings are computed for the image and subsequently stored. Video frames are accessed using the OpenCV library, and each frame is resized to 1/4 of its original size to enhance recognition and processing efficiency. Faces are detected within the resized frames using the face_locations() function, with bounding box coordinates adjusted accordingly. Face encodings are then computed for each detected face.

Using the face_distance() function, the distance between the test image and images in the training set is calculated. A match is identified based on the minimum face distance index. Once a match is found, a bounding box is drawn around the recognized face using cv2, and the matching name is displayed on the output frame. Additionally, the camera location, date, and time are captured, and this information is recorded in a file.

Finally, when a person match is located, the SMTP client is triggered to send an email notification to the authorized person

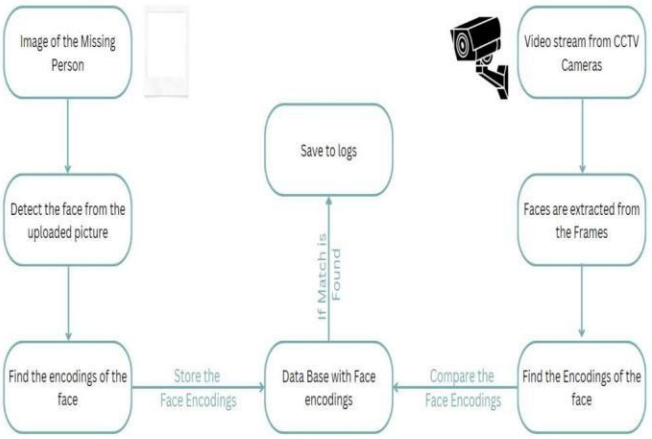


Fig. 5: System Workflow.

Fig. 5 explain the system workflow and it consists of number of phases which includes image of the missing person, detection of the missing person, face encoding, store it in database with face encoding, save to logs, video streams from CCTV cameras, faces are extracted from the frames, fin the encoding of the face and compare it with data base.

IV. RESULT ANALYSIS

A study of the outcomes of a facial recognition video surveillance and monitoring system entails assessing several factors to ascertain the system's efficacy, precision, and moral implications. Here are some important things to think about:

1. **Performance and Accuracy:**

- Face Identification Accuracy: Evaluate how well the system can identify faces and compare them to a database.
- False Positives and Negatives: Look for instances of false positives, which are when a non-matching face is mistakenly identified, and false negatives, which are when a matching face is not found.
- Speed and Efficiency: Assess the system's quickness in identifying and matching faces in situations that occur in real-time or very close to it [3].

2. **Data Security and Privacy:**

- Compliance: Verify that the system conforms to applicable standards, data protection laws, and privacy laws.
- Data Encryption: Assess the security measures implemented to guard against unwanted access to the facial recognition data [4].

3. **Robustness of the System:**

- Handling Variability: Evaluate how well the system adapts to changes in ambient elements such as illumination, posture, and facial expressions.
- Adaptability: Determine whether the system can adjust to how people's faces change over time [6].

4. **Integration with Surveillance and Tracking:**

- Accurate Tracking: Assess the system's ability to follow certain users over several video streams or frames.
- Integration with Other Systems: Evaluate how well the facial recognition technology works in tandem with other

technologies for tracking and surveillance [7].

5. **Alerts and Notifications:**

- Real-time Alerts: Find out if the system can send out alerts in real-time to those who have been identified.
- Accuracy of Notifications: Make sure that alerts are precise and dependable to prevent needless alarm [4]s.

6. **Usability and User Interface:**

- User-Friendliness: Assess how simple it is to use and how well it allows you to configure and administer the system.
- Training Requirements: Determine the degree of training necessary for users to operate and interpret the results effectively [3].

7. **Updating and maintaining the system:**

- Scalability: Take into account the system's capacity to accommodate a growing database of faces [6].
- Frequent Updates: Make sure the system receives updates regularly to fix security flaws and boost efficiency.

Frequent evaluation of these factors will aid in performance optimization and problem-solving for the facial recognition video surveillance and tracking system.

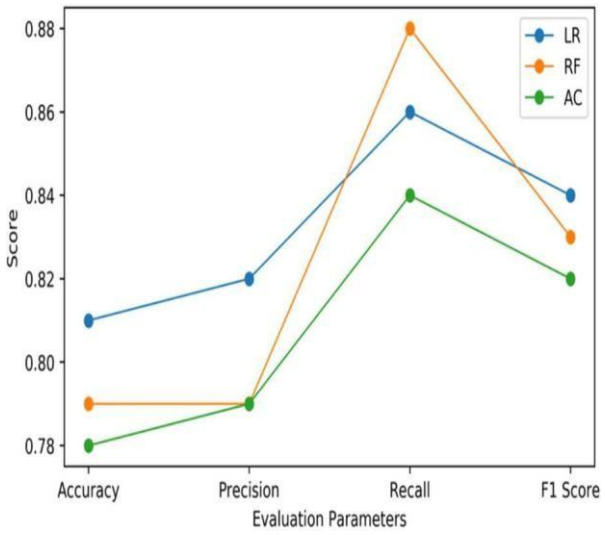


Fig. 6 Evaluation parameters

Fig. 6 shows the evaluation parameters such as accuracy, precision, recall and F1 score and here we note the score deference in LR, RF and AC.

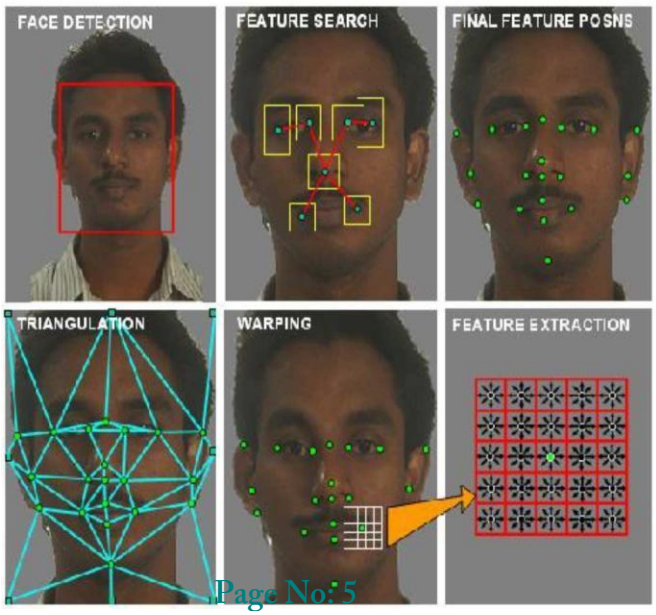
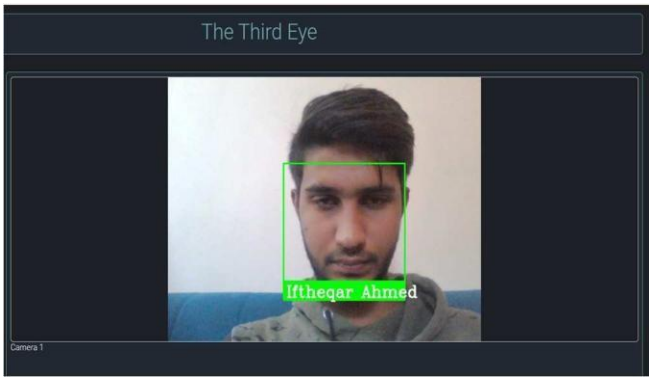


Fig. 7 : Feature Extraction

Fig. 7 illustrate the image feature extraction based on the traditional extraction method.

The series steps are involved to extract the image feature which includes face detection , search for the main features, creating the final features recognition, construct the triangulation, warping the required features and finally features are extracted which is used to compare with the image stored in the database.



(a)

Fig 8 b: Facial recognition video surveillance

Fig. 8 a & b explain the process of facial identification and recognition

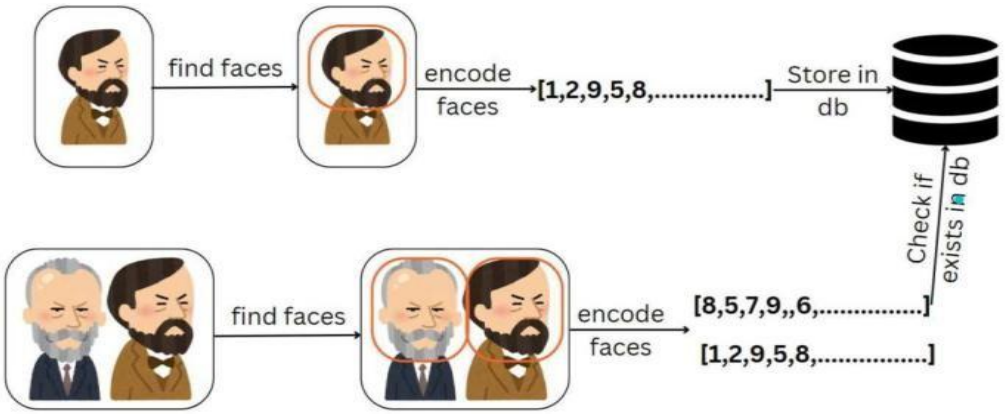


Fig. 9: Face Recognition and Comparison

Fig. 9 explain the face recognition and comparison process which includes finding the faces, encode the faces, store it in data base, check it exist in database.

V. CONCLUSION

In this research, we have built and proposed a system that focuses on video camera face identification and recognition. surveillance systems that play a major role in situational control. These technologies convert video surveillance from a data-gathering instrument to a system for gathering intelligence and information [5, 6]. Surveillance systems can respond to an activity in real time and obtain pertinent information at a much greater resolution by using real-time video analysis.

Innovations in video surveillance and monitoring systems are centered around the integration of facial recognition technology,

artificial intelligence, and computer vision. These systems leverage advanced algorithms to accurately identify and track individuals in real time, enhancing traditional surveillance capabilities. By comparing detected faces with databases of known individuals, these systems improve security measures and streamline access control. Moreover, they provide valuable data for various applications, such as threat detection and behaviour analysis. However, the implementation of such systems raises ethical and privacy concerns, necessitating the development of strong privacy protections and clear management frameworks. Overall, these innovations have the potential to revolutionize security practices while addressing ethical and social implications in a complex and connected world. [4].

REFERENCES

[1] G. Chandan et al, "Real Time Object Detection and Tracking Using D eep Learning and OpenCV," *International Conference on Inventive Research in Computing Applications (ICIRCA),* 2018.

[2] W. Sultani, C. Chen and M. Shah, "Real-World Anomaly Detection in Surveillance Videos," *Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition,* pp. 6479- 6488, 2018.

[3] O. Xu et al, "Background Modelling Methods in Video Analysis: A Review and Comparative Evaluation," *CAAI Transactions on Intelligence Technology,* 2016.

[4] E. Heilmann, "Video surveillance and security policy in France: from regulation to widespread acceptance," *Information Polity 16 (2011),* p. 369–377, 2011.

[5] M. A.R. Ahad, "Computer vision and action recognition: A guide for image processing and computer vision community for action understanding," *Atlantis/Springer,* 2011.

[6] C. Lakshmi Devasena, R. Revathi and M. Hemalatha, "Video Surveillance Systems," *IJCSI International Journal of Computer Science Issues,* vol. 8, no. 4, 2011.

[7] H. Yousefi, Z. Azimifar and A. Nazemi, "Locally anomaly detection in crowded scenes using Locality constrained Linear Coding," *2017 Artificial Intelligence and Signal Processing Conference (AISP),* pp. 205-208, 2017.

[8] Justin Lai and Sydney Maples, Ammunition Detection: Developing a Real-Time Gun Detection Classifier, Stanford University, Feb 2017.

[9] Shreyamsh Kamate, UAV: Application of Object Detection and Tracking Techniques for Unmanned Aerial Vehicles, Texas A University, 2015

[10] Mohana and H.V.R. Aradhya, "Elegant and efficient algorithms for real time object detection counting and classification for video surveillance applications from single fixed camera", *2016 International Conference on Circuits Controls Communications and Computing (14C)*, pp. 1-7, 2016.