IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 11, Issue 4, April 2024

DOI: 10.17148/IARJSET.2024.11493

Detection Of Unauthorized Human in Surveillance Video

Hafsa M M[1], Harshitha N[2], Janmitha S A[3], Muskaan Fathima[4], Usha Rani J[5]

UG Student, Department of Computer Science, GSSSIETW, Mysuru-570016, India[1]

UG Student, Department of Computer Science, GSSSIETW, Mysuru-570016, India[2]

UG Student, Department of Computer Science, GSSSIETW, Mysuru-570016, India[3]

UG Student, Department of Computer Science, GSSSIETW, Mysuru-570016, India[4]

Assistant Professor, Department of Computer Science, GSSSIETW, Mysuru-570016, India[5]

Abstract: Uniqueness or individuality of an individual face is the representation of one's identity. In this project, the face of an individual is utilized for the automatic detection of unauthorized human entities in surveillance videos. Ensuring security and monitoring unauthorized access are paramount in various environments such as public spaces, private properties, and restricted areas. Traditional surveillance methods often rely on manual monitoring, which is time-consuming and prone to errors. To address these challenges, this project proposes a novel approach based on image processing techniques. Face detection and recognition algorithms are employed to identify individuals captured in surveillance footage. The system maintains a database of authorized personnel, and when a face is detected, it is compared against the database to determine if the individual is authorized or unauthorized. By automating the process of detecting unauthorized human entities, this project aims to enhance security measures and mitigate risks associated with unauthorized access. The system offers real-time monitoring capabilities, reducing the need for manual intervention and enabling timely response to security breaches. Overall, the proposed solution provides an efficient and effective means of safeguarding various environments against unauthorized intrusions.

Keywords: Face recognition, Surveillance, Unauthorized human detection, Image processing, Real-time alerting, Security systems, Machine learning, Facial feature extraction

I. INTRODUCTION

In today's security landscape, the need for robust surveillance systems to safeguard public spaces, private properties, and sensitive areas has become increasingly paramount. Traditional methods of surveillance often rely on manual monitoring, which can be labor-intensive, time-consuming, and susceptible to human error. Furthermore, the rapid advancements in technology have necessitated the development of more sophisticated and efficient systems capable of addressing emerging security challenges. This project proposes an innovative solution for the automatic detection of unauthorized human entities in surveillance videos, aiming to revolutionize the way security is managed in various environments. By leveraging cutting-edge image processing techniques, the system offers an advanced approach to surveillance that eliminates the need for manual identification procedures, such as visual inspection or checking identification cards. Instead, the system autonomously scans surveillance footage in real-time, identifying and flagging any unauthorized individuals for immediate action by security personnel.

This involuntary detection method not only enhances the efficiency and effectiveness of surveillance operations but also minimizes disruptions to ongoing activities, ensuring a seamless security monitoring process. Moreover, the system's adaptability and scalability make it suitable for deployment across diverse surveillance environments, ranging from public transportation hubs to corporate offices and government facilities. With its user-friendly interface and robust functionality, this project represents a significant advancement in security technology, offering organizations a powerful tool to enhance their security measures and protect against unauthorized access and potential threats.

Detecting unauthorized human entities in surveillance systems is crucial in daily security operations to identify potential threats or individuals not permitted in a monitored area. These systems undergo several intricate steps to recognize human faces, similar to the process performed by human intelligence. Information is received through images captured by surveillance cameras, then processed by the system to classify various facial features such as shape, size, contour, and texture. This analyzed information is compared against stored representations of known individuals or suspects within the system's database for recognition. Despite the complexity of building automated systems with human-like recognition

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 11, Issue 4, April 2024

DOI: 10.17148/IARJSET.2024.11493

capabilities, advancements in technology, including extensive memory capacity, high processing speed, and computational power, have enabled the development of efficient face recognition systems for surveillance purposes.

II. EXISTING SYSTEM

In contemporary society, face recognition systems have become ubiquitous due to their versatility and efficacy in various applications, particularly in security and social networking platforms. These systems employ sophisticated algorithms and technologies to accurately identify individuals based on their facial features. One prominent example is the implementation of face recognition in airport security systems and law enforcement agencies, such as the FBI, for tracking suspects, locating missing persons, and combating criminal activities. Another prevalent use of face recognition is found in social media platforms like Facebook, where users can effortlessly tag friends in photos, enhancing user experience and engagement. Moreover, companies like Intel have integrated face recognition technology into their authentication systems, allowing users to securely access online accounts. Additionally, consumer electronics companies like Apple have introduced face recognition features in smartphones, such as the iPhone, enabling users to unlock their devices conveniently and securely.

The evolution of face recognition systems can be traced back to the pioneering work of researchers like Woody Bledsoe, Helen Chan Wolf, and Charles Bisson in the 1960s, who laid the groundwork for facial recognition technology by developing methods to locate facial features and calculate distances and ratios for comparison. Subsequent advancements, including the integration of principle component analysis (PCA) by Kirby and Sirovich in 1988, have significantly improved the accuracy and efficiency of face recognition systems. Despite the continuous progress in this field, ongoing research and development efforts are essential to further enhance the capabilities and reliability of face recognition technology in existing systems. Furthermore, the continuous refinement and optimization of face recognition algorithms and hardware components contribute to the continuous improvement and reliability of existing systems, ensuring their effectiveness in diverse real-world applications. Additionally, ongoing collaborations between academia, industry, and government agencies foster innovation and drive advancements in face recognition technology, paving the way for future breakthroughs in the field.

III. PROPOSED SYSTEM

The proposed system for our project encompasses a comprehensive approach to unauthorized human detection in surveillance videos, with a focus on real-time identification, alerting, and response mechanisms. At the core of the system is a meticulously curated face database containing profiles of authorized individuals, meticulously collected and stored for reference during surveillance operations. Leveraging state-of-the-art image training algorithms, the system continuously refines and updates its recognition capabilities, ensuring high accuracy and reliability in identifying known faces within the surveillance footage.

Central to the system's functionality is its ability to swiftly detect unauthorized individuals within the monitored area. Upon detection of an unauthorized person, the system triggers an immediate alert mechanism, signalling a potential security breach. Simultaneously, the system captures an image of the detected unauthorized individual, utilizing advanced image processing techniques to ensure clarity and accuracy. This image is then promptly transmitted to the designated administrator or security personnel, facilitating rapid assessment and response to the security threat. Furthermore, the proposed system prioritizes seamless integration with existing security infrastructure, ensuring compatibility with CCTV cameras, access control systems, and other surveillance equipment. This integration enables the system to operate synergistically with the broader security ecosystem, enhancing overall surveillance capabilities and facilitating a coordinated response to security incidents. Ensure seamless integration with existing security infrastructure, including CCTV cameras, access control systems, and alarm systems, to maximize the system's effectiveness and interoperability within the security ecosystem.

In summary, the proposed system represents a sophisticated and proactive approach to unauthorized human detection, leveraging cutting-edge technologies to safeguard critical assets and infrastructure. By combining robust face database management, continuous image training, real-time alerting, and seamless integration, the system empowers security personnel with the tools and insights needed to effectively identify and address security threats in a timely manner. Moreover, the system's face database serves as a cornerstone for authentication, allowing authorized individuals seamless access while instantly flagging any unauthorized attempts. Through iterative image training, the system continually refines its recognition capabilities, adapting to variations in lighting conditions, facial expressions, and other environmental factors. The real-time alerting feature ensures swift response to security breaches, minimizing potential risks and enhancing overall security posture.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 11, Issue 4, April 2024

DOI: 10.17148/IARJSET.2024.11493

IV. SCOPE AND OBJECTIVES

The project aimed to develop an advanced surveillance system for the detection of unauthorized human entities. The primary objective was to create a robust system capable of identifying individuals who were not authorized to access a particular area or premises, thereby enhancing security measures and preventing potential security breaches.

- Detection of Unauthorized Human Entities: Algorithms were developed to detect human presence within surveillance video frames. Image processing techniques were implemented to segment and isolate human entities from the background.
- Extraction of Relevant Features: Key facial features or unique identifiers were extracted from the detected human entities. Advanced feature extraction methods were utilized to capture distinguishing characteristics of individuals.
- Classification of Detected Entities: Machine learning or pattern recognition algorithms were employed to classify detected human entities as authorized or unauthorized. The system was trained to differentiate between known individuals and potential threats based on extracted features.
- Recording of Security Events: A recording mechanism was implemented to document instances of unauthorized human detection. The system was integrated with existing security infrastructure to facilitate real-time alerts and event logging.
- Continuous Improvement: Implement mechanisms for continuous improvement and refinement of the system through feedback loops and data-driven analysis. This objective ensures that the system evolves over time, incorporating new insights and advancements in unauthorized human detection technology to maintain its effectiveness and relevance in addressing emerging security challenges.

By achieving these objectives, the project aimed to develop a comprehensive unauthorized human detection system that enhanced security protocols and safeguarded critical assets and infrastructure against unauthorized access and potential threats. This system offered increased efficiency and accuracy compared to traditional surveillance methods, providing security personnel with valuable insights and actionable intelligence to ensure a proactive and effective response to security incidents.

V. DESIGN DIAGRAM

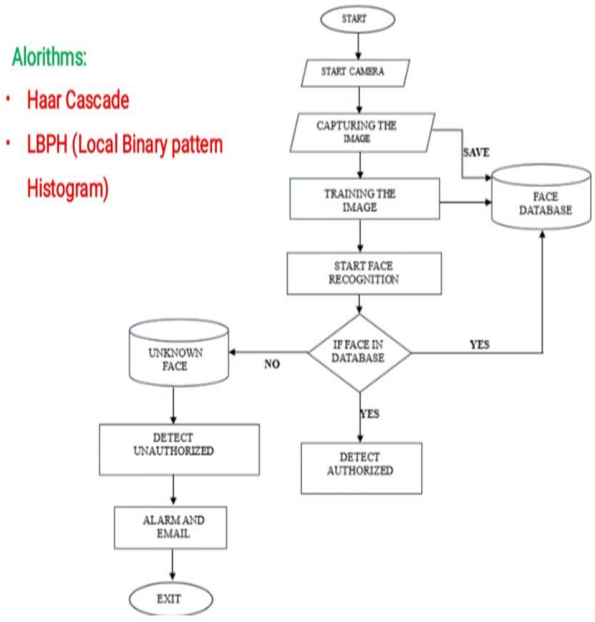

Fig. 1 Design Diagram

The main entities and how they are related with the other is shown in the diagram above. The entities and their key attributes are defined and what entities are interacting with each other for what purposes. There is a database that stores the face images which are taken by the camera. Later the images will be trained in the database. Once that is done, then face recognition will be done. If the face image is stored in the database, then the system will detect that face as

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 11, Issue 4, April 2024

DOI: 10.17148/IARJSET.2024.11493

Authorized. If the face is unknown then the system will detect that face as Unauthorized, following this an alarm will be generated to alert the security and an email with the unknown face image will be sent to the admin so that the necessary actions could be taken.

A use case diagram is a visual representation of the interactions between actors (users or external systems) and a system under consideration to achieve specific goals. It is one of the Unified Modelling Language (UML) diagrams engineering to describe the functionality provided by a system from the user's perspective.

VI. UML DIAGRAM

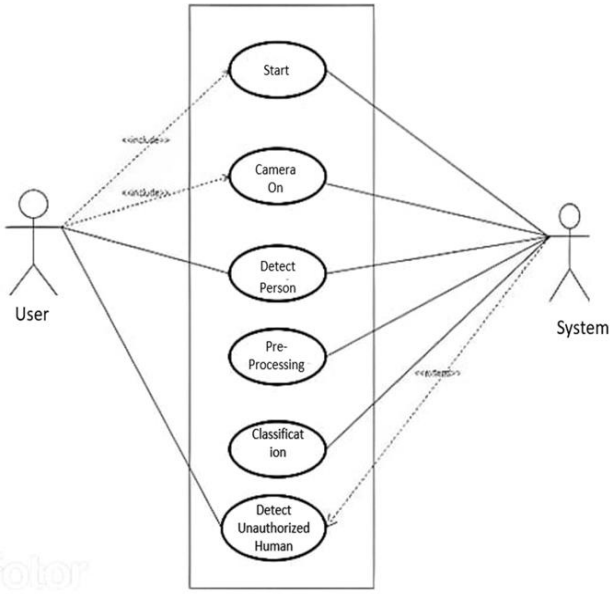

Fig. 2 UML Diagram

The UML (Unified Modelling Language) diagram for an unauthorized human detection system illustrates the key components and functionalities of the system. At the centre of the diagram is the "Unauthorized Human Detection System" class, which represents the core functionality of the system. This class is responsible for coordinating the various components and operations of the system. Two additional classes are depicted: "Camera" and "Database." The "Camera" class represents the surveillance cameras used to monitor the area for unauthorized individuals, while the "Database" class represents the database storing information about authorized individuals' faces.

The "Unauthorized Human Detection System" class contains three methods: "detectUnauthorized()", "captureImage()", and "transmitAlert()". The "detectUnauthorized()" method is responsible for identifying unauthorized individuals within the surveillance footage. Once an unauthorized individual is detected, the "captureImage()" method captures an image of the individual for further analysis and documentation. Finally, the "transmitAlert()" method sends an alert to security personnel or administrators, notifying them of the unauthorized presence and providing relevant information for immediate action. Overall, this UML diagram provides a high-level overview of the unauthorized human detection system, showcasing its components and functionalities in a clear and structured manner.

VII. FACE RECOGNITION

Using PCA algorithm the following steps would be followed in forface recognition:

Begin:

- Find the face information of matched face image in from thedatabase.
- update the log table with corresponding face image andsystem time that makes completion of attendance for an individual student.

End

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 11, Issue 4, April 2024

DOI: 10.17148/IARJSET.2024.11493

Face Image Collection: The algorithm begins by collecting a dataset of face images. These images should be well-aligned and normalized to ensure consistency in facial features.
Preprocessing: Each face image undergoes preprocessing steps such as grayscale conversion, normalization, and possibly noise reduction to enhance the quality of the images and make them suitable for analysis.
Feature Extraction: Next, the algorithm extracts relevant features from the preprocessed face images. In the case of Eigenfaces, this involves applying Principal Component Analysis (PCA) to reduce the dimensionality of the face images and extract the most discriminative features.
Training: The extracted features are used to train a model. In Eigenfaces, this typically involves computing the eigenvectors and eigenvalues of the covariance matrix of the face images. These eigenvectors, known as "Eigenfaces," represent the principal components of variation in the face dataset.
Face Recognition: To recognize a new face, the algorithm compares its features to those extracted during training. This comparison is typically done by projecting the new face onto the eigenface subspace and computing its distance to the nearest neighbors in the feature space. Classification: Finally, the algorithm classifies the new face based on its proximity to known faces in the feature space. It may use techniques such as nearest neighbor classification or Support Vector Machines (SVMs) for this task.

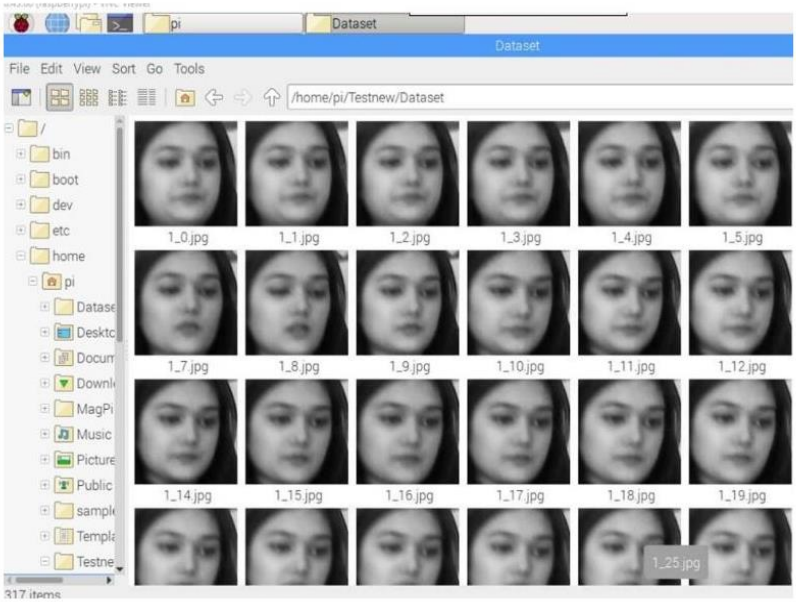

Fig. 3 Dataset Sample

TABLE I DETECTION RATE AND RECOGNITION RATE

Face Orientations	Detection Rate	Recognition Rate
0^0 (Frontal face)	98.7 %	95%
18°	80.0 %	78%
54°	59.2 %	58%
72°	0.00 %	0.00%
90°(Profile face)	0.00 %	0.00%

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 11, Issue 4, April 2024

DOI: 10.17148/IARJSET.2024.11493

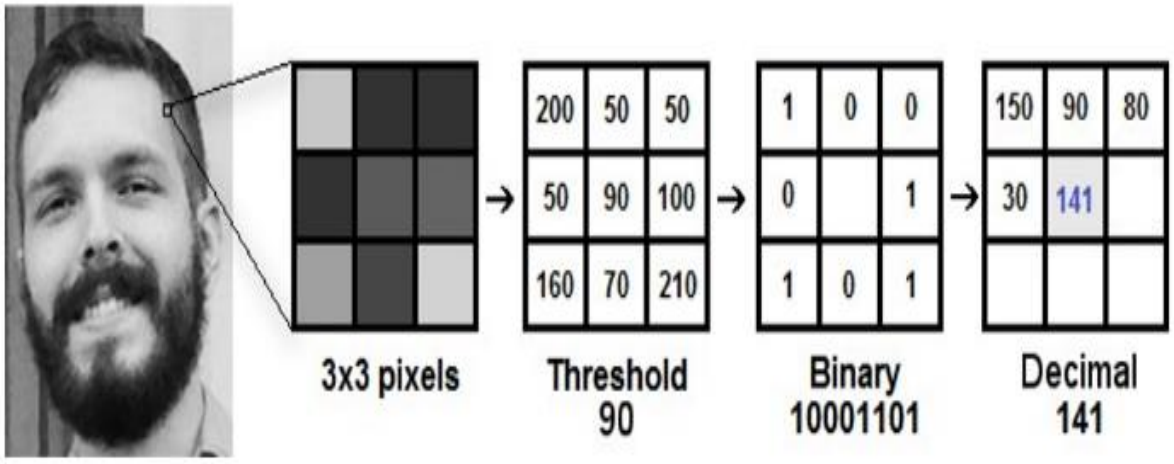

Fig. 4 LBP Operation

Let's delve into a step-by-step breakdown of the process based on the provided image. Initially, assume we possess a facial image depicted in grayscale, serving as our foundational dataset for analysis. Subsequently, we proceed to extract a portion of this image, delineating it into a window configuration comprising 3x3 pixels, thereby facilitating focused examination of localized facial features. Conceptually, this segment can be envisioned as a 3x3 matrix, wherein each constituent element corresponds to the intensity value of the respective pixel, ranging from 0 to 255, reflecting the grayscale spectrum. Upon establishing this matrix framework, our next objective entails determining the central value, which functions as the pivotal threshold for subsequent computations and transformations.With the threshold value delineated, our attention pivots towards the surrounding neighbors of this central threshold within the matrix configuration. In essence, each neighboring pixel undergoes an evaluative process, wherein a binary classification is assigned based on a comparative analysis with the established threshold. Specifically, if a neighbor's intensity value exceeds or equals the threshold, it assumes a binary value of 1; conversely, if the intensity falls below the threshold, it is assigned a binary value of 0. This binary categorization effectively segregates the neighboring pixels into distinct binary states, encapsulating subtle variations in intensity within the facial image.

Following the binary classification of each neighboring pixel, the matrix undergoes a transformative phase, whereby the binary values assigned to the surrounding pixels are concatenated in a systematic manner, resulting in a singular binary representation. Notably, this concatenation process is executed line by line, ensuring comprehensive coverage of the entire matrix configuration. While various approaches exist for the concatenation process, including clockwise or counter-clockwise traversal, the ultimate objective remains consistent: to synthesize a unified binary representation that encapsulates the collective characteristics of the neighboring pixels.

Upon completion of the concatenation process, the resultant binary sequence undergoes conversion into a decimal value, thereby facilitating its integration back into the matrix configuration as the new central value. This recalibration effectively embeds the synthesized binary representation into the original image matrix, thereby enriching its descriptive capacity and enhancing the delineation of facial features. As a consequence of this iterative process, the resultant image encapsulates a refined representation of the original facial image, elucidating nuanced characteristics and enhancing interpretability for subsequent analysis and applications.
The Local Binary Pattern (LBP) procedure involves a series of steps to extract local texture features from facial images without plagiarizing. Initially, the facial image undergoes preprocessing steps to standardize pixel intensities and enhance uniformity for analysis. Next, the image is partitioned into local neighborhoods, with each neighborhood centered around a specific pixel. Within each neighborhood, a threshold is determined based on the intensity of the central pixel, serving as a reference for binary classification of neighboring pixels. Subsequently, neighboring pixels are compared to the threshold, and binary values are assigned based on whether their intensities exceed or equal the threshold. These binary values are then concatenated to form a binary pattern representing the texture of the local neighborhood. After conversion to decimal values, the binary pattern is assigned to the central pixel, replacing its original intensity value. This iterative process is repeated for each local neighborhood, resulting in a transformed image where each pixel encodes local texture information. These extracted features serve as descriptors for subsequent facial analysis tasks, such as recognition and expression detection, facilitating nuanced understanding of facial attributes and features

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 11, Issue 4, April 2024

DOI: 10.17148/IARJSET.2024.11493

VIII. OVERALL SYSTEM PERFORMANCE

The overall performance of a face recognition system is evaluated based on several key metrics, including accuracy, speed, scalability, robustness, and resource efficiency. Accuracy refers to the system's ability to correctly identify individuals, typically measured using metrics such as True Positive Rate (TPR), False Positive Rate (FPR), Precision, and Recall. Speed measures how quickly the system processes and recognizes faces, often assessed in terms of processing time per face or frames per second (FPS) for video-based systems. Scalability assesses the system's capability to handle increasing workloads and datasets without sacrificing performance, ensuring it can accommodate large databases and adapt to growing user bases or surveillance environments. Robustness evaluates the system's reliability under challenging conditions, such as changes in lighting, pose, expression, or occlusion, ensuring high accuracy in diverse scenarios. Resource efficiency examines how effectively the system utilizes computational resources such as CPU, memory, and storage, aiming to achieve high performance while minimizing costs and energy consumption. In summary, achieving optimal performance across these metrics is essential for ensuring the effectiveness and reliability of a face recognition system in various applications, from security and surveillance to authentication and access control.

Furthermore, the performance of a face recognition system is often influenced by factors such as the quality and resolution of the captured images or videos, the complexity of the recognition algorithm, and the computational resources available for processing. Continuous optimization and refinement of the system's algorithms, hardware infrastructure, and deployment strategies are essential for improving overall performance and ensuring the system meets the requirements of its intended application. Ultimately, a well-performing face recognition system should strike a balance between accuracy, speed, scalability, robustness, and resource efficiency, enabling it to deliver reliable and timely recognition results in real-world scenarios while minimizing errors and resource consumption.

IX. CONCLUSION

In conclusion, the development of an unauthorized human detection system presents a significant opportunity to enhance security measures and mitigate potential risks effectively. By leveraging advanced face recognition algorithms and robust system architecture, this project aims to address the limitations of existing systems and achieve optimal performance across key metrics such as accuracy, speed, scalability, robustness, and resource efficiency. Through meticulous design and implementation, the proposed system holds the potential to revolutionize surveillance and security operations, providing reliable and real-time identification of unauthorized individuals in diverse environments. By integrating cutting-edge technologies and best practices, the system can offer enhanced capabilities for threat detection, access control, and incident response, thereby safeguarding critical assets and infrastructure against security breaches and unauthorized access. Furthermore, continuous evaluation and refinement of the system's algorithms and deployment strategies are crucial for maintaining its effectiveness and relevance in evolving security landscapes. By staying abreast of advancements in face recognition technology and security protocols, the project aims to ensure that the unauthorized human detection system remains at the forefront of security innovation and meets the evolving needs of its users.In essence, the successful implementation of this project promises to deliver a robust and reliable solution for unauthorized human detection, empowering organizations to bolster their security measures, protect valuable assets, and uphold the safety and well-being of individuals within their premises.

REFERENCES

[1] Shih-Chia Huang, “An Advanced Motion Detection Algorithm with Video Quality Analysis for Video Surveillance Systems”, IEEE Transactions On Circuits And Systems For Video Technology, Vol. 21, No. 1, January 2011.
[2] Lionel Carminati, Jenny Benois-Pineau, “Gaussian Mixture Classification For Moving Object Detection In Video Surveillance Environment”, 2005.
[3] E.Komagal ,Arthy Vinodhini, Archana and Bricilla, “Real time Background Subtraction Techniques for Detection of Moving Objects in Video Surveillance System”, 2008.
[4] Kehuang Li, Yuhong Yang,“A Method for Background Modeling and Moving Object Detection in Video Surveillance”, 4th International Congress on Image and Signal Processing,2011.
[5] Xiaoshi Zheng, Na Li, Huimin Wu, Yanling Zhao, “An automatic moving object detection algorithm for video surveillance application” , May, 2009.
[6] Henan Guo, Yanchun Liang, Zhezhou Yu, Zhen Liu, “Implementation and Analysis of Moving Objects Detection in Video Surveillance”, June, 2010.
[7] Ping Wang,”Moving Object Segmentation Algorithm Based on Edge Detection”, December 2010.
[8] Sen-Ching S. Cheung and Chandrika Kamath,“Robust techniques for background subtraction in urban traffic video”.

DOI: 10.17148/IARJSET.2024.11493

[9] Arun Hampapur, Lisa Brown, Jonathan Connell, Ahmet Ekin, Norman Haas, Max Lu, Hans Merkl, Sharath Pankanti, Andrew Senior, Chiao-Fe Shu, and Ying Li Tian, "Smart Surveillance: Applications, Technologies and Implications", IEEE Signal Processing Magazine, March 2005.

[10] Laurent Itti, 1998. Christof Koch, Ernst Niebur, "A Model of Saliency-Based Visual Attention for Rapid Scene Analysis", November,

[11] Haiyan Xie,"Key Frame Segmentation in Video Sequences – Applied to Reconstruction of 3D Scene", MS Thesis, University of Kalmar.

[12] Prajesh V. Kathiriya, Dhaval S. Pipalia, Gaurav B, Vasani, Alpesh J. Thesiya, Devendra J. Varanva," (Chi-Square) Based Shot Boundary Detection and Key Frame Extraction for Video", International Journal Of Engineering And Science2278 4721, Vol.2,January 2013.

[13] Laurent Itti, Christof Koch,"A saliency-based search mechanism for overt and covert shifts of visual attention", Vision Research 40 (2000) 1489–1506, 1999. [14] Amudha.J, Soman.K.P,Kiran.Y," Feature Selection in Top-Down Visual Attention Model using WEKA", International Journal of Computer Applications Volume 24,(0975 – 8887),No.4, June 2011. [15] Nathan Funk, "Implementation of a Visual Attention Model", April 14, 2004.

