



Facial Recognition Reinvented: Deep Learning Based Security Alert System

T Sridhar Reddy^{1*}, Dr.B Sujatha², V G V Prasanna Kumar³, P Srihari⁴,
M Devi Harshitha⁵, B Murali Manohar⁶

^{1,2,3,4,5,6}Computer Science & Engineering
Godavari Institute of Engineering & Technology(A), Rajamahendravaram, A.P.India

reddysridhar27@giet.ac.in^{1*}, birudusujatha@gmail.com²,
kumarnani738@gmail.com³, sriharipayyavula66@gmail.com⁴,
harshithavarma228@gmail.com⁵, manoharmanu6634@gmail.com⁶

Abstract. The study focuses on unauthorized access, which signifies attack into a device or residence without the owner's consent. This research aims to address access issues through the enhancement of established devices. In the existing system, a combination of Convolutional Neural Network (CNN) was utilized, resulting in reduced efficiency and increased complexity. To improve this, the proposed system incorporates Harr Cascade and Local Binary Pattern (LBP) algorithms alongside CNN to boost efficiency and streamline complexity. The system takes a person's facial recognition through a camera as input, generating two outcomes. Type 1 indicates unauthorized access, triggering alarm notifications and sending an email alert to the owner. Type 2 signifies authorized access, displaying an authorized message alert without any further action. The model's primary objective is to identify unauthorized individuals and send alerts when an unknown person attempts to enter the premises.

Keywords: CNN, Harr Cascade, LBP, Alert, Authorization.

1. Introduction

In the digital domain, unauthorized access presents a notable security risk, spanning database breaches and network hacks. Physical breaches, like trespassing and break-ins, pose challenges to traditional security measures, compromising personal privacy through identity theft and financial losses. The existing facial recognition system, relying on Convolutional Neural Networks (CNN), has limitations. This study seeks to improve security capabilities through advanced tools such as deep learning and facial recognition. In our dynamic world, technology offers inventive solutions to address the growing need for efficient security measures. Face recognition in AI aims to authenticate individuals by identifying distinctive facial features, a computer vision subfield [5]. Face recognition technology has advanced significantly thanks to deep learning, a kind of machine learning [15]. Convolutional neural networks (CNNs), in particular, have exhibited extraordinary ability in identifying and discriminating faces in pictures and video [12]. Precise face recognition holds paramount importance in security applications [7]. The "Opti Fuzz" system enhances access control security [3] by accurately identifying authorized individuals and preventing unauthorized access [9-10]. Research related to areas such as facial recognition, biometrics, access control, surveillance, and security.

© The Author(s) 2024

K. R. Madhavi et al. (eds.), *Proceedings of the International Conference on Computational Innovations and Emerging Trends (ICCIET 2024)*, Advances in Computer Science Research 112,

https://doi.org/10.2991/978-94-6463-471-6_117

2. EXISTING MODEL

To fully understand just how powerful devices which will detect recognized devices are very less. In the existing model several algorithms were used like PCA (Principal Component Analysis [12], SVM (Support Vector Machine), LDA (Linear Discriminant Analysis) [5] for the extraction of facial features. Although using these algorithms the model was lagged in recognizing the faces in the dark and light illuminations [11].

In the existed system faces the problem of recognizing the authorized people faces accurately and proving less security in restricted areas.

Disadvantages: Low efficiency, High complexity.

3. PROPOSED MODEL

The proposed system employs a webcam to capture streaming video [14], utilizing the Haar cascade for face detection and feature extraction. Following this, the Local Binary Pattern (LBP) identifies highlighted pixel regions, converting them into binary for pattern extraction. These features are compared to a pre-trained CNN model with authorized persons, ensuring accurate face identification in challenging conditions like dark shadows. CNN model training involves converting captured images into layers of face recognition, using Haar cascade for face detection, and transforming detected faces into Local Binary Pattern. This approach integrates Haar cascade, LBP, and CNN techniques for robust face recognition.

Advantages: High efficiency, Time Saving, Low complexity.

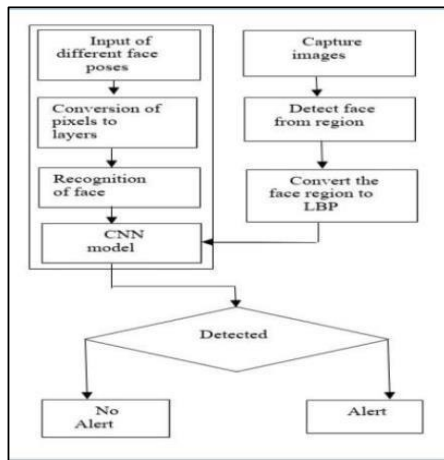


Fig. 1. System Architecture

4. IMPLEMENTATION

Training the model

CNN model underwent training using datasets containing information about authorized persons. Different poses of the face were captured, and facial features, including textures and edges, were extracted for the purpose of training.

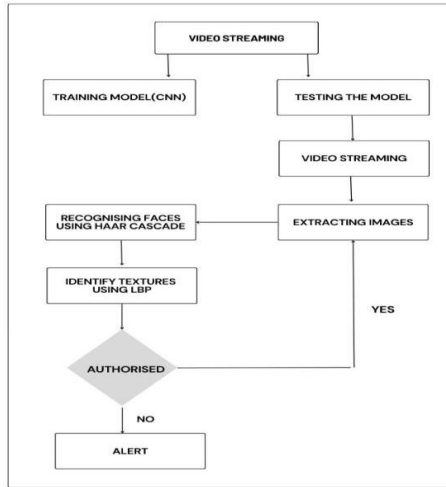


Fig. 2. Block Diagram of Proposed system

Capture Images

Images are captured from the real time video through webcam whenever any person came into the frame at particular distance.

Feature extraction

After the detection of faces, the LBP features are extracted from these regions. Which will capture the unique texture patterns from each detected face.

Evaluation of faces

The detected faces are evaluated with the training model of known faces to know whether the person is authorized or unauthorized.

Alert the user

If the face is authorized one then no alert will be sent just displays an authorized person and the other case if the face is unauthorized the system will make an alarm sound.

5. EVALUATION METRICS:

Assessing an Unauthorized Access detection system centers on metrics like precision, recall. Enhancements include experimenting with Haar Cascade, LBP, and CNNs. A diverse facial image dataset is standardized. Training and evaluating a baseline CNN model precede the integration of Haar Cascade and LBP, resulting in improved metrics. Diversifying the dataset ensures efficiency in real-world scenarios.

6. ALGORITHMS

Haar cascade:

It is particularly well-suited for face detection. It works by identifying specific patterns and features in images or video frames that correspond to faces. Here's a step-by-step explanation of how Haar Cascade is used in face detection.

Feature Selection:

Haar-like features are selected from the positive and negative sample datasets. These features represent variations in pixel values within rectangular regions of the images.

Sliding Window Approach:

To detect faces in an image or video stream, a sliding window approach is used. A small window is moved across the image, and the trained cascade classifier is applied to each window.

Training the cascade:

To ensure diversity and relevance to the target object, positive and negative samples must be gathered before training a cascade classifier. While negative samples lack the object of interest, positive samples do. In order to extract discriminative information from the samples, feature extraction methods. The classifier iteratively learns to discriminate between positive and negative samples using boosting methods. There are several phases in the cascade structure, and each one has a group of poor classifiers. Each stage of classification effectively filters out non-object regions in the input image. Performance is maximized by fine-tuning parameters, such as the number of stages and weak classifiers per stage.

Local Binary Pattern:

This algorithm is a texture analysis technique for facial recognition, other computer vision tasks. LBP works by capturing the local patterns and textures in an image, making it particularly useful for facial feature extraction and discrimination.

Image Pre-processing:

The first step in LBP-based facial recognition is to pre-process the input facial images.

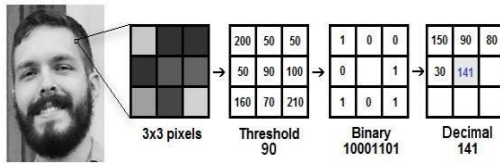


Fig. 3. Conversion to Binary

Pattern Generation:

This is accomplished by contrasting the core pixel's intensity value with the neighboring pixels' intensity values. A neighbor receives a value of 1 if its intensity \geq center pixel, and 0 otherwise.

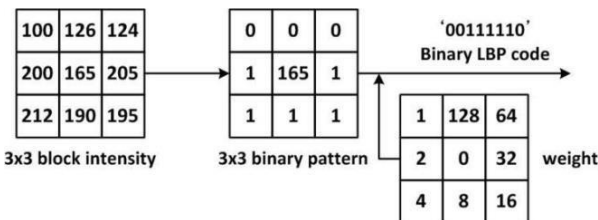


Fig. 4. Converting decimal to binary

Histogram Formation:

After computing LBP codes for image pixels, a histogram portrays their distribution. Each distinct LBP code constitutes a histogram bin. For a succinct feature representation, either normalize the histogram or dimensionality reduction techniques. During recognition, match LBP-based feature vectors with known individuals in a database using classification algorithms.

Convolutional Neural Network:

These are made for image processing tasks.

Convolutional Layers:

CNNs begin use a convolutional layer or layers. These layers provide the input image with a series of learnable filters. It scans across the image to detect specific features. To add non-linearity, an activation function is used following each convolution step.

Pooling Layers:

By identifying the most crucial data, it reduces the sample size of the feature maps. A popular method called "max pooling" uses the maximum value within a narrow window is retained, reducing the spatial dimensions of the feature maps [4].

Pooling lessens the computational effort and increases the network's resistance to slight input distortions and translations.

7. FEATURE EXTRACTION FROM DATASET:

Dataset Description:

For effective monitoring of unauthorized access using facial recognition and machine learning, a dataset containing images of individuals, both authorized and unauthorized, along with corresponding labels, is essential. This dataset will be instrumental in training and evaluating for unauthorized access detection.

Data Collection:

Collect a diverse range of images representing authorized users and potential unauthorized intruders. These images should encompass various lighting conditions, angles, and facial expressions. Capture images using cameras or obtain them from publicly available facial datasets.

Data Annotation:

Create a balanced dataset for facial recognition, labeling images as "authorized" or "unauthorized." Utilize Haar Cascade and LBP algorithms for face detection during testing. Refine the dataset by removing duplicates, incorrect labels, and low-quality images. Augment data through horizontal and vertical flipping and rotation of facial images.

Train CNN to identify unauthorized access based on facial features. Integrate the model into the security system for swift alerts, ensuring computational efficiency and data accuracy in recognizing and responding to unauthorized individuals.

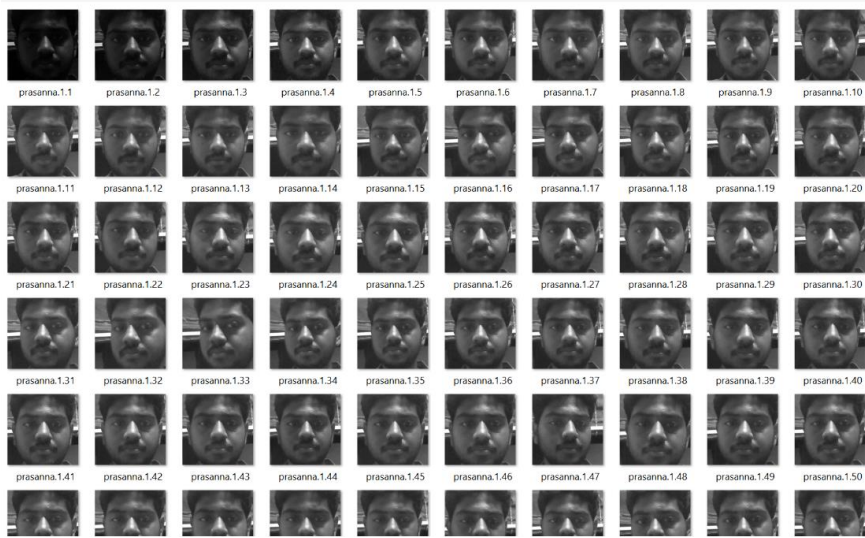


Fig. 5. Dataset of Authorized Person

8. RESULTS

When someone known tries to enter your home or workplace, you can choose to grant or deny access through vigilant monitoring. The software checks images against the database: authorized individuals gain access, while unauthorized ones trigger an alert via email, notifying you of the intrusion. This alert system keeps you informed even when you're away from CCTV monitoring, enabling swift identification of unknown individuals attempting entry into your premises.

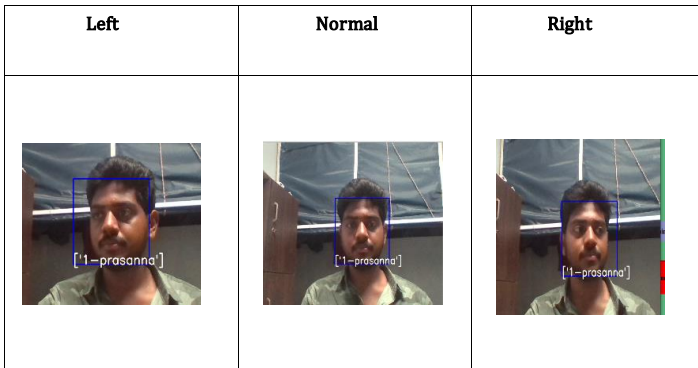


Fig.6. Poses in different angles

Table 1. Poses in different conditions


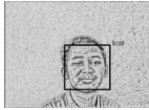

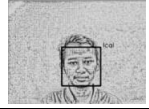

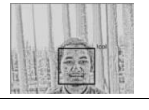

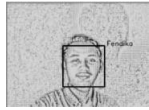
Less light		
Normal light		
Background light		
Flash lighting		

Table 2. Results of persons in different poses

S. No	Face pose		
	Right	Normal	Left
#1	2	3	1
#3	2	3	1
#4	3	3	2
#5	3	3	1
#6	3	3	3
#7	3	3	3
#8	3	3	3
Total recognized	19/21	21/21	14/21
% recognized	90.48	100.00	60.62
Cumulative % recognized	83.7		

9. COMPARATIVE STUDY

Facial recognition serves as a pivotal element in biometrics, surveillance, security, and authentication. This paper introduces an advanced security system tailored for restricted areas, permitting entry exclusively to individuals registered in the training database. Utilizing facial and motion detection, the system enhances security. Upon detecting human motion, it initiates facial recognition for access authorization while simultaneously tracking motion coordinates. In case of facial recognition failure, an anesthetic gun automatically neutralizes intruders. Experimental results highlight the system's efficacy in preventing unauthorized access, a central focus of this study. To augment existing security systems, the model replaces the less efficient and complex.

Convolutional Neural Network (CNN) with a blend of Haar Cascade and Local Binary Pattern (LBP) algorithms. When a camera captures a person's face, the system categorizes the outcome into Type 1 (unauthorized access, triggering alarms and email alerts) or Type 2 (authorized access with a message). Table 9.1 Comparative study of existing and proposed models.

Table 3. Comparison of Existed and Proposed

ASPECT	EXISTED	PROPOSED
Algorithm	SVM	CNN
Technique	Fuzzy Inference System (FIS)	LBP, Haar Cascade
Alert	Identify unauthorized and gives alert	Buzz alert and email
Accuracy	Gives accuracy of 85%	Gives accuracy of 95%

10. CONCLUSION AND FUTURE WORK

The experiments aimed to boost Unauthorized Access detection, yielding significant insights and security enhancements. Combining Haar Cascade, Local Binary Pattern (LBP), and Convolutional Neural Networks (CNNs) birthed a sophisticated security alert system. There were notable boosts in accuracy. Haar Cascade and LBP integration fortified the CNN model, streamlining efficiency and reducing complexity. Data augmentation techniques fortified the model's resilience. Real-time camera feed trials underscored practicality, stressing user-friendliness and usability. Refinement of threshold values and hyper parameter optimization honed accuracy and response time. In conclusion, these experiments birthed a highly effective Unauthorized Access detection system, swiftly flagging unauthorized individuals while minimizing false alarms. The system has potential for securing sensitive premises, particularly when amalgamated with security cameras and smart sensors, limiting access to authorized person and sounding alarms for unauthorized attempts.

11. REFERENCES

1. A. Ibrahim, T. Horiuchi and S. Tominaga. "Illumination-Invariant Representation for Natural Colour Images and its Application", IEEE Southwest Symposium on Image Analysis and Interpretation, pp.157- 160, 2012.
2. A. Şengur, Z. Akhtar, Y. Akbulut, S. Ekici and U. Budak, "Deep Feature Extraction for Face Liveness Detection," 2018 International Conference on Artificial Intelligence and Data Processing (IDAP), Malatya, Turkey, 2018, pp. 1-4.
3. B.S.B. Dewantara and J. Miura, "Opti fuzz: a robust illumination invariant face recognition system and its implementation", Machine Vision and Applications, Vol. 27, No. 6, pp. 877-891, 2016.
4. F. M. J. Mehedi Shamrat, M. A. Jubair, M. M. Billah, S. Chakraborty, M. Alauddin and R. Ranjan, "A Deep Learning Approach for Face Detection using Max Pooling," 2021 5th International Conference on Trends in Electronics and Informatics (ICOEI), Tirunelveli, India, 2021, pp. 760-764.
5. J. Mazanec, and M. Melisek, "Support vector machines, PCA and LDA in face

6. K. J. Biju, R. Kuriakose, S. Sulaikha, K. J. Sharon and F. A. Rawther, "Intruder Detection System for Video Surveillance Using Machine Learning," 2023 9th International Conference on Smart Computing and Communications (ICSCC), Kochi, Kerala, India, 2023, pp. 365-368.
7. K. Murugan, R. D. Reddy, N. Chandralekha, T. Ravikiran and T. Deepika, "Residential Home Surveillance System," 2023 World Conference on Communication & Computing (WCONF), RAIPUR, India, 2023, pp. 1-6.
8. K.I. Kim, K. Jung, and H.J. Kim, "Face recognition using kernel principal component analysis," IEEE Signal Processing Letters, vol.9, no.2, pp.40-42, February 2002.
9. L.S. Oliveira, D.L. Borges, F.B. Vidal, L. Chang, "A fast eye localization and verification method to improve face matching in surveillance videos," IEEE International NMJK; Conference on Systems, Man, and Cybernetics (SMC), pp.840-845, October 2012.
10. M. Hemalatha, J. S. Priya, J. R. P. S. T. Porselvi and S. S., "An Intelligent Authentication System for Improved Security," 2022 International Conference on Power, Energy, Control and Transmission Systems (ICPECTS), Chennai, India, 2022, pp. 1-5.
11. M. Turk and A. Pentland, "Face recognition Using eigenfaces". Proc. IEEE Conference on Computer Vision and Pattern Recognition. pp.586–591, 1991.
12. M.A. Kashem, M.N. Akhter, S. Ahmed, M.M. Alam, "Face recognition system based on Principal Component Analysis (PCA) with Back Propagation Neural Networks (BPNN)," Canadian Journal of Image Processing and Computer Vision, vol. 2, no. 4, April 2011
13. Kuraparathi, Swaraja, Madhavi K. Reddy, C. N. Sujatha, Himabindu Valiveti, Chaitanya Duggineni, Meenakshi Kollati, and Padmavathi Kora. "Brain Tumor Classification of MRI Images Using Deep Convolutional Neural Network." Traitement du Signal 38, no. 4 (2021).
14. R. Nayak, M. M. Behera, U. C. Pati and S. K. Das, "Video-based Real-time Intrusion Detection System using Deep-Learning for Smart City Applications," 2019 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS), Goa, India, 2019, pp. 1-6.
15. Y.V. Lata, C.K. BTungathurthi, H.R.M. Rao, A. Govardhan, L.P. Reddy, "Facial recognition using eigenfaces by PCA," International Journal of Recent Trends in Engineering, vol.1, no.1, May 2009.

Open Access This chapter is licensed under the terms of the Creative Commons Attribution-NonCommercial 4.0 International License (<http://creativecommons.org/licenses/by-nc/4.0/>), which permits any noncommercial use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.

