International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-67992147-6799 www.ijisae.org Original Research Paper

Artificial Intelligence Based Intruder Detection Home Security System

M. Jahir Pasha[1], Dr. B. Maruthi Shankar[2], Dr. S. A. Sivakumar[3], S. Aswin[4], A. Bragadeesh[5], S. Deepak[6]

Submitted: 12/09/2023 **Revised**: 25/10/2023 **Accepted**: 10/11/2023

Abstract: An effective face detection and identification algorithm is required to design a highly effective intruder detecting surveillance system. When a person is captured on camera, CNN, an artificial intelligence programme that detects objects, and Grassmann's algorithm are utilised to determine whether or not the individual is an invader. The research's objective is to identify the quickest method for homeowners to be notified if a burglar or intruder breaks into their house utilising a proactive surveillance system. This device's programming was based on several recognition algorithms and a framework for evaluating factors that might distinguish between intruders and burglars. Developmental research was employed in the design to address the research topic. The outcome demonstrates that the system is capable of spotting and identifying burglars and can inform the homeowners in advance via email and emergency alarms. The technology can identify intruders, alert the family members in advance, and activate the home's alarm system, it is determined

***Keywords**: Artificial Intelligence, face detection, Grassmann's algorithm, Intruders and burglars*

1. Introduction

As society increasingly relies on video monitoring to increase security and safety, video surveillance is becoming more and more important [1-4]. Such devices are typically implemented for security in places like banks and parking lots where crimes can happen. The systems are implemented for safety in places where accidents could happen, like on roads or motorways and at building sites. The fundamental advantage of surveillance video data as a proactive real-time warning system is now lost because it is mostly employed as a forensic tool. The main issue is that while adding more video cameras is reasonably inexpensive, hiring and paying for human observers of the video feeds is quite expensive [5-6]. Additionally, human operators for surveillance monitoring quickly grow weary and complacent due to individual faces and issue a warning in order to avert an undesirable event or limit the impact. From a different angle, intelligent cameras eliminate the need for human operators to continuously monitor all the video feeds in order to spot the behaviours that are of interest, which lowers operating costs and improves efficacy [7-9].

[1]*Associate Professor, Department of Computer Science and Engineering, G.Pulllaiah College of Engineering and Technology, Kurnool, India; jahir4444@gmail.com*
[2]*Associate Professor-ECE, Sri Krishna College of Engineering and Technology, Coimbatore, India; drmaruthishankar@gmail.com*
[*3]*Associate Professor-ECE, Dr.N.G.P. Institute of Technology, Coimbatore, India ; drsasivakumar@gmail.com**
[4,5,6]*UG Scholar-ECE, Sri Krishna College of Engineering and Technology, Coimbatore, India; aswinselvaraj22@gmail.com, bragadeesh19@gmail.com, deepak.888.3d@gmail.com*
*****Correspondence: drsasivakumar@gmail.com*

Person identification is the task of matching individuals across different cameras in a multi-camera surveillance system. It is a difficult problem due to the large variety in appearance caused by factors such as pose, illumination, occlusion, and camera viewpoint. The goal of person identification is to associate the same human's identity across different cameras, which can be used for various implementations such as video surveillance, crowd analytics, and keeping a track of individuals in public spaces. Recent advances in deep learning and computer vision have led to significant progress in person re-identification, making it a promising area of research for real-world applications [10-14].

Holistic and feature-based methods are the two basic methods for recognising faces. To compare an image against a database of recognised faces, feature-based methods require extracting particular features from an image, such as the eyes, nose, and mouth. Comparatively, holistic methods use cutting-edge technologies like deep learning to match against a database while analysing the full face as a single unit [15-17].

The AI algorithms used in the system can continually improve their accuracy through machine learning. Regular updates and improvements to the AI models are essential to keep the system up-to-date with the latest security threats. The combination of these AI-powered features enhances the overall efficiency and effectiveness of a home security system, providing homeowners with peace of mind and an increased level of protection against potential intruders or security breaches [18-21].

Fig 1. Insight on Intruder Detecting Home Security System

2. Related Works

Convolutional neural networks (CNNs) and deep learning have recently made considerable strides, improving facial recognition accuracy. These techniques are able to handle changes in lighting, position, and emotion as well as learn effective representations of faces. The variances in age, ethnicity, and changes in look brought on by plastic surgery or ageing, however, continue to pose problems for face identification. This phase is crucial since it applies the feature extraction algorithm to extract the features. The steps involve information compression, removing noise from the data, and reducing features that are unnecessary. The facial region is then transformed into a vector with a specified dimension in which the locations of the facial characteristics coincide. Following the completion of the prior stage, the features are analysed, and after that, the recognition component is utilised to learn each person's face and then save it in the database. The model is tested against a particular input image once it has been trained. Every preceding step, including preprocessing and others, is repeated.If everything goes according to plan, the model will be able to identify a person without the person's knowledge or permission. The model's evaluation must be able to establish whether or not the assumption is accurate.

In the fields of computer vision and artificial intelligence, emotion detection and recognition have made significant strides. In order to extract Haar-like features for face detection and to use neural networks to confirm and categorise human emotion, the article suggests utilising the Viola Jones method. In the paper, a system that extracts facial cues to identify human mood is proposed. To identify human emotions, a wide range of approaches have been applied. Ihor Paily published one of the ground-breaking works in face recognition. In this study, face detection is demonstrated by removing Haar-like features and categorising them using neural networks [2]. Due to the difficulties presented by a picture's 2dimensionality, researchers in another study took an intriguing approach to the problem of mapping facial emotions by attempting to do a digital image analysis using the region of interest. Here, academics have used the characteristics of the lips and analysed them in light of the expressions they create [4]. A system to recognise and predict facial emotions has been implemented in another study on facial expression identification using the statistical unsupervised technique known as ICA (independent component analysis) and the feature-optimizing techniques known as genetic algorithms [3]. Additionally, Kharat and Dudul's research [5] shows that facial expressions made during social encounters account for roughly 55% of the overall emotion display.

Convolutional Neural Networks (CNNs) have been at the forefront of AI-based face detection. Models like "Single Shot Multibox Detector" (SSD), "You Only Look Once" (YOLO), and "Faster R-CNN" have shown significant improvements in accuracy and speed. Researchers have focused on developing real-time face detection algorithms to enable applications like video surveillance, human-computer interaction, and facial recognition systems. AI models have been refined to achieve higher accuracy and robustness against variations in lighting conditions, facial expressions, pose, and occlusion.

The availability of large-scale face datasets, such as MS-Celeb-1M, MegaFace, and WIDER Face, has contributed to training more accurate and generalizable face detection models. Researchers have also explored ways to address privacy and ethical concerns related to face detection, particularly in surveillance and public spaces. Advancements in edge computing and model optimization have made it possible to deploy face detection algorithms on resource-constrained devices like smartphones and IoT devices.

Some research has focused on domain-specific face detection, such as detecting faces in thermal images or underwater environments. Researchers have explored multi-task learning approaches to simultaneously perform face detection along with other related tasks like facial landmark localization and gender recognition. Adversarial attacks, where imperceptible perturbations are added to an image to deceive the face detection system, have also been studied to improve the robustness of models. Efficient face detection architectures have been proposed to achieve a balance between accuracy and computational efficiency, making them suitable for real-world applications. It's important to note that the field of AI is rapidly evolving, and there may have been further advancements and breakthroughs in AI-based face detection beyond my last update. To stay up-to-date with the latest research and developments, I recommend exploring academic databases, conference proceedings, and research publications in the field of computer vision and AI.

3. Proposed System

A face recognition system's face detection phase is its initial operation. There has been a lot of study in this field, but the most of it is efficient and effective for still photos only and cannot be immediately adapted to video sequences. Since many years ago, face identification in group of frames has been a hot topic in the fields of image processing, computer vision, and biometrics. Videos have more information than a single image when compared to still face recognition, and videos also have spatiotemporal information. By combining information from several frames, temporal data, and multiple positions of faces in movies, it is feasible to investigate the shape information of faces and increase the reliability of face recognition in videos.

Video has spatio-temporal information, which is more comprehensive than a single image. By combining data from multiple frames, temporal data, and multiple postures of faces in videos, it is possible to extract face shape data and incorporate it into the face recognition framework, improving face recognition accuracy and resulting in more robust and stable recognition.

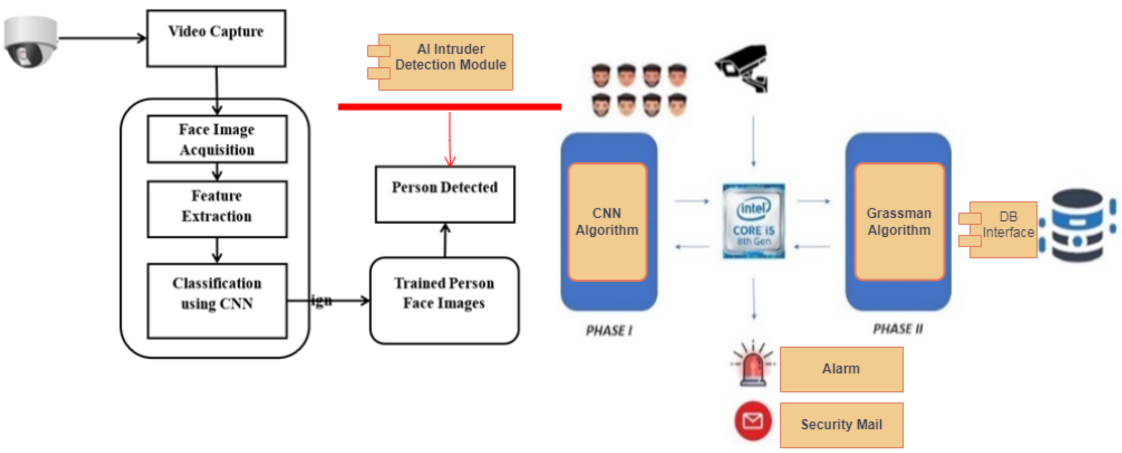

Fig 2. Proposed Architecture

Compared to image-based recognition, video-based recognition offers additional benefits. First, the task of face recognition can be facilitated by using the temporal information of faces. Second, better representations can be extracted from the video stream and used to enhance recognition outcomes, such as face models or super-resolution images. Last but not least, video-based recognition helps updating or learning the subject model over time.

High-definition security cameras with built-in AI capabilities are essential components of the system. These cameras can analyze video feeds in real-time using AI algorithms to detect and identify people, objects, and unusual activities. The AI system can differentiate between ordinary movements (e.g., pets or swaying trees) and potential intruders. It can analyze motion patterns to identify suspicious activities. Advanced facial recognition algorithms enable the system to recognize known individuals (e.g., family members) and identify unfamiliar faces, raising alerts if necessary. The AI system can identify specific objects such as bags, packages, or weapons left behind by intruders or visitors. The AI system can learn the typical behavior of residents and recognize abnormal patterns, helping to identify potential threats. When the system detects something unusual or a potential intruder, it sends real-time alerts to homeowners or a professional monitoring service through a mobile app or other communication channels. The security system can integrate with other smart home devices, such as smart locks, smart lights, and smart alarms, to respond effectively to potential threats. For example, if an intruder is detected, the system can automatically lock doors and turn on lights to deter them. Cloud-based AI platforms can process and analyze data from multiple homes, allowing the system to learn from a larger dataset and improve its accuracy over time. As AI-based security systems collect sensitive data, it's crucial to ensure robust privacy and data security measures to protect homeowners' information

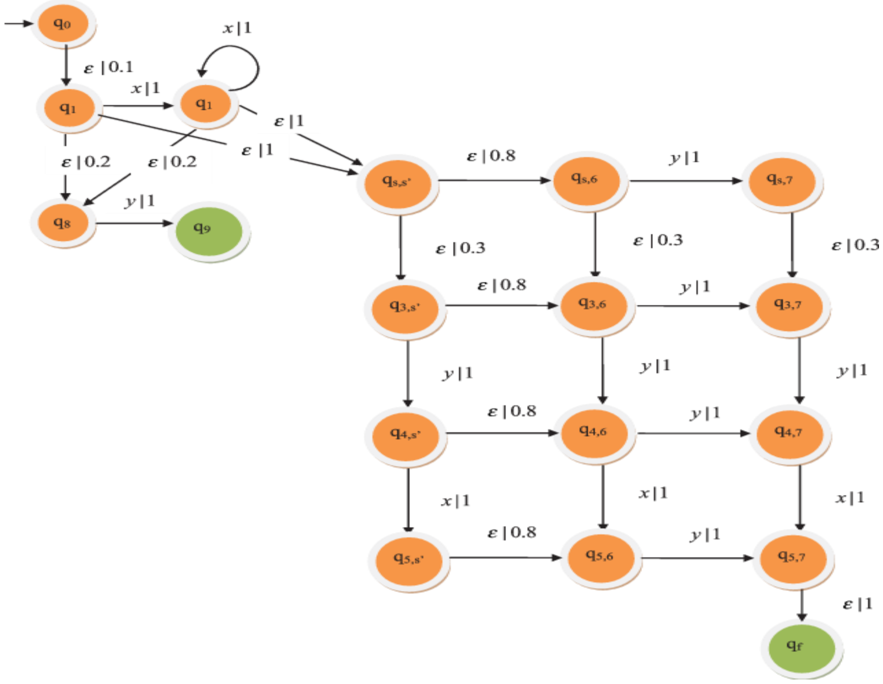

Fig 3. SDL Diagram of proposed architecture.

4.Implementation & Simulation Results

Home Page of the proposed system designed using HTML and CSS. Admin Login Page depicts that the house owner or security can access the system's admin portal to add new users and view the activity recorded. User Information Page depicts that the user can view the name and other additional details of the users whose faces have already been registered in the database and can edit the details if needed. During the surveillance mode, if any unknown face is detected, immediately the frame is captured and sent to the owner via mail and buzzer beeps. When "Verify" is clicked in home page, surveillance mode is turned on and if an registered user appears, his/her name will be displayed and their entry information will be noted

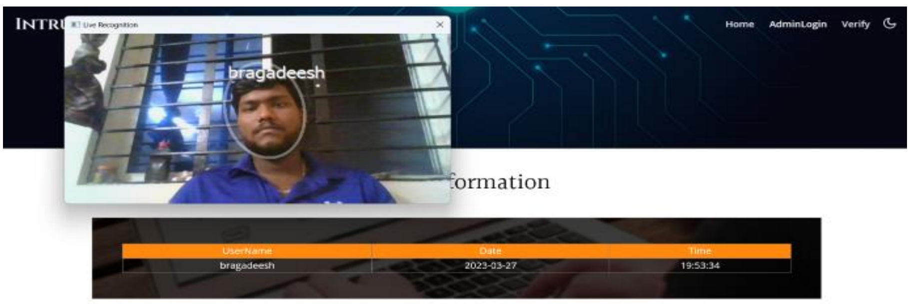

Fig 4. Home Page Design

The proof that a mail is sent to the owner immediately after the entry information of the appeared user is noted. During the survelliance mode, if any unknown face is detected, immediately the frame is captured and sent to the owner via mail and buzzer beeps

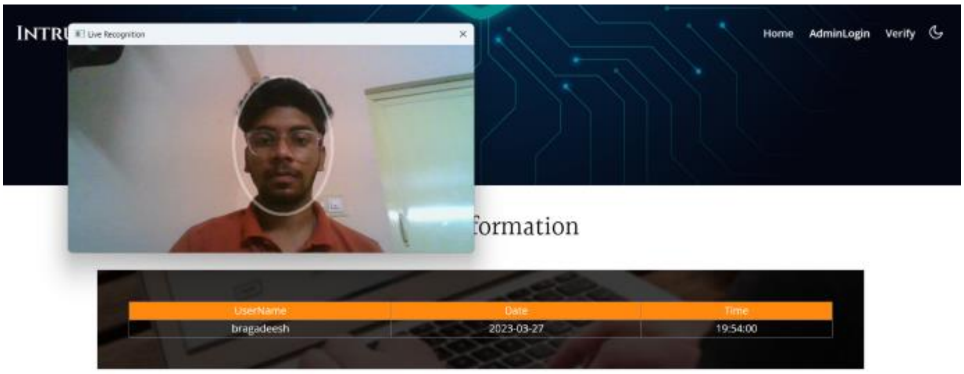

Fig 5. Intruder detection using proposed system

The proof that, When buzzer beeps, a mail is immediately triggered to the owner's mail saying "Intruder Detected" with the Image of the intruder.

Fig 6. Mail Alert sent after Intruder detection using proposed system

5.Conclusion

We examined facial recognition techniques in this work for both still images and moving pictures. The majority of these techniques in use today only conduct video-to-video matching or frozen image face recognition and they call for perfectly aligned face images. They are unsuitable for face recognition in surveillance scenarios due to the factors such as: a restriction on the number of face images that can be extracted from each video (roughly ten); significant pose and lighting variations; a lack of assurance regarding the face image alignment; and resource constraints influenced by real-time processing. Then, we present a face feature-based solution for face detection in surveillance-related still photos and videos. The generality of this architecture allows for still-to-still, real-time matching of still and moving pictures in movies. The training process use static graphics while the recognition job is conducted over video clips. It can be concluded from our results that using video sequences results in higher recognition rates even if static images and video sequence use the same methods to handle the same problems. This method is assessed for face detection based on still photos and films using real-time picture datasets

References

[1] Agustina J. R. and Clavell G (2019) "The Impact of CCTV on Fundamental Rights and Crime Prevention Strategies: The Case of the Catalan Control Commission of Video Surveillance Devices," Computer Law and Security Review, pp. 168-174, doi:10.1016/j.clsr.2020.01.006.

[2] Banuchitra S and Kungumaraj K (2019) "A comprehensive survey of content-based image retrieval techniques," International Journal of Engineering and Computer Science, vol.5, no.8, pp.17577-17584, doi:10.18535/ijecs/v5i8.26.

[3] Çarıkçı M and Özen F (2021) "A face recognition system based on eigenfaces method, "Procedia Technology, vol. 1, pp. 118-123, doi:10.1016/j.protcy.2012.02.023

[4] Chang X , Nie F ,Wang S ,Yang Y, Zhou X, and C. Zhang (2019) "Compound rank-k projections for bilinear analysis," IEEE Transactions on Neural Networks and Learning Systems, vol. 27, no. 7, pp. 1502–1513.

[5] Elfasakhany, Hernández J, García J. C, Reyes M, and Martell F (2020)"Design and development of a house-mobile security system," Engineering, vol.03,no.12,pp.1213-1224,doi:10.4236/eng.2011.312151.

[6] Faux Fand Luthon F (2019) "Theory of evidence for face detection and tracking, "International Journal of Approximate Reasoning, vol. 53, no. 5, pp. 728-746,doi:10.1016/j.ijar.2019.02.002.

[7] Li S (2020) "The application of face recognition based on opencv," Advanced Materials Research, vol.403-408, pp.2350-

[8] Li W ,Zhao R ,Xiao T, and Wang X (2019) "Deepreid: Deep filter pairing neural network for person re-identification," in Proc. CVPR, pp. 152–159.

[9] Liao S, Hu Y, Zhu X, and Li S Z (2018) "Person re-identification by local maximal occurrence representation and metric learning," in Proc. CVPR, pp. 2197–2206.

[10] Ni JandChellappa R (2022)"Evaluationofstate-of-the-artalgorithmsforremoteface recognition," 2010 IEEE International Conference on Image Processing,doi:10.1109/icip.2010.5652608.

[11] Reza Khan S and Sultana Dristy F (2020) "Android based security and HomeAutomationSystem,"TheInternationalJournalof AmbientSystemsandApplications, vol. 3, no. 1, pp. 15-24, doi: 10.5121/ijasa.2014.3102. ISSN:2502-4752IndonesianJElecEng&CompSci,Vol.24,No.2,November2021:843-852852

[12] Richey R C and Klein J D, (2019) "Developmental research methods: Creating knowledge from instructional design and development practice," Journal of Computing in Higher Education, vol.16, no.2,pp.23-38,doi:10.1007/bf02961473.

[13] Viola P and Jones M. J. (2020) "Robust real-time face detection," International Journal of Computer Vision, vol. 57, no. 2, pp. 137-154,doi:10.1023/b:visi.0000013087.49260.fb.

[14] Wang Y.Q (2019) "An analysis of the viola-jones face detection algorithm" Image Processing On Line, vol.4, pp.128-148,doi:10.5201/ipol.2014.104.

[15] Xia R, Pan Y, Lai H, Liu C, and Yan S (2018) "Supervised hashing for image retrieval via image representation learning." in Proc. AAAI , pp. 2156–2162.

[16] Yang M, Li F, Zhang L, and Zhang Z (2018) "Deep learning algorithm withvisual impression," Information Processing Letters, vol. 136, pp. 1-4, doi:10.1016/j.ipl.2018.03.004.

[17] Yang Y ,Nie F, Xu D ,Luo J ,Zhuang Y, and Pan Y (2020) "A multimedia retrieval framework based on semi-supervised ranking and relevance feedback," IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 34, no. 4, pp. 723–742.

[18] Yang Y, Ma Z ,Hauptmann A. G, and Sebe N (2021) "Feature selection for multimedia analysis by sharing information among multiple tasks," IEEE Transactions on Multimedia, vol. 15, no. 3, pp. 661–669.

[19] Zheng L, Bie Z, Sun Y, Wang J, Wang S, Su C, and Tian Q(2022) "Mars: A video benchmark for large-scale person re-identification," in Proc. ECCV, pp. 868–884.

[20] Zheng L, Shen L, Tian L, Wang S, Wang J, and Tian Q (2021) "Scalable person re-identification: A benchmark," in Proc. ICCV, pp. 1116– 1124.

[21] Zheng L, Wang S, Tian L, He F, Liu Z, and Tian Q(2019) "Query-adaptive late fusion for image search and person re-identification," in Proc. CVPR, pp. 1741–1750.

[22] Russo, L., Kamińska, K., Christensen, M., Martínez, L., & Costa, A. Machine Learning for Real-Time Decision Support in Engineering Operations. Kuwait Journal of Machine Learning, 1(2). Retrieved from http://kuwaitjournals.com/index.php/kjml/article/view/117

[23] Anand, R., Ahamad, S., Veeraiah, V., Janardan, S.K., Dhabliya, D., Sindhwani, N., Gupta, A. Optimizing 6G wireless network security for effective communication (2023) Innovative Smart Materials Used in Wireless Communication Technology, pp. 1-20.