Journal of Data Acquisition and Processing
ISSN: 1004-9037
https://sjcjycl.cn/
DOI: 10.5281/zenodo.7691575

IMPROVING SMART HOME SAFETY WITH FACE RECOGNITION USING MACHINE LEARNING

Shalini KC
Asst. Professor, New Horizon College, Outer Ring Road, Marathahalli, Bengaluru-560103

Siddaraju K
Asst. Professor, Government First Grade College, Kolar-563101

ABSTRACT:

Smart home devices can be programmed to optimize energy usage and reduce waste, leading to lower energy bills. IoT devices allow for remote control and automation of home systems such as lighting, temperature, and security, making daily life more convenient. IoT devices can provide real-time insights into household usage and patterns, allowing for improved awareness and decision making. IoT devices such as smart locks and security cameras can provide real-time monitoring and alerts, improving home security. Now a days user faces many inconvenience in usage of electronic fingerprint door locks such as False rejections, Limited user capacity, vulnerability to environmental factors such as moisture, dirt, and oil, leading to decreased accuracy, cost and maintenance. As there are many drawbacks found in existing methods in alteration to that, we use face recognition technology in smart homes, where it has the potential to greatly improve safety and security. By using machine learning algorithms, smart home devices equipped with cameras and facial recognition software can identify and authenticate authorized users, reducing the risk of unauthorized access. The technology can also alert homeowners of potential intruders and provide real-time monitoring of the home. With its ability to learn and adapt to new faces, face recognition technology has the potential to provide a high level of accuracy and security for smart homes. This technology can be integrated into security monitors, door locks, and other home automation technologies, and access control systems. The implementation of face recognition technology in smart homes can not only enhance safety but also provide a more convenient and personalized user experience. In this research work we use an hybrid machine learning algorithm for face recognition in a home automation system could be with the help of SVMs and CNNs working together (SVM).The CNN can be used for feature extraction from face images, while the SVM can be used for classification and identification of individual faces. This hybrid approach can take advantage of the strengths of both algorithms, providing robust and accurate face recognition performance. Additionally, this hybrid approach can be easily trained on large datasets and can handle variations in lighting, facial expressions, and angles, making it suitable for real-world face recognition applications in home automation systems.

Keywords: Smart Home, Face Recognition, Authorised access, Convolutional Neural Network and Support Vector Machine.

1.INTRODUCTION:

The term "smart" has emerged as a catch all for cutting-edge devices that incorporate some form of AI. Smart technologies are distinguished by their ability to sense and respond to their surroundings [1, 2]. The "smart home" is an emerging idea that relies heavily on smart technology since its ultimate goal is to improve people's quality of life [3–6]. A smart home system typically consists of a central control unit, such as a smartphone app or a smart speaker, that allows homeowners to manage various connected devices in their home, such as lights, appliances, heating/cooling systems, security systems, and entertainment systems. These devices communicate with the central control unit through Wi-Fi or other wireless protocols and can be controlled remotely or through voice commands. Transforming products and services on a large scale has ushered in an era of increased device interoperability, which in turn has fueled the worldwide boom in smart home technology sales [7]. Smart technology's advantages have piqued the curiosity of researchers and industry professionals alike. Smart technology has received a lot of focus recently because of its widespread practical use in home appliances [2, 8]. A "smart home" is a house where electronic devices are networked and managed electronically. A user may manage and automate these devices with the use of software installed on a computer or mobile device. The "smartness" of controlled appliances is determined by their ability to be programmed to learn and adapt their behaviour [9]. In addition, the Wifi connection offered by the home gateway enables management of these devices via smart home hubs like ThinkSpeak, Blynk, and Google Home.

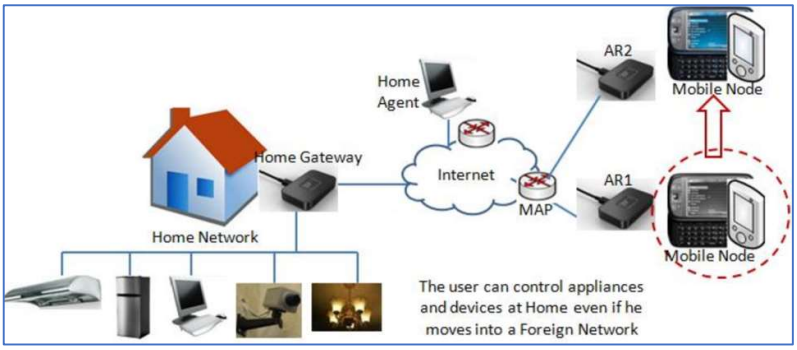

Figure 1.1: Smart Home Architecture

Fingerprint locks for doors are a type of biometric security system is the existing system as shown in the figure 1.2 which is used in homes for security purposes which uses an individual's unique fingerprint as the key to unlock a door. Some common disadvantages of existing fingerprint locks for doors include:

Figure 1.2: Fingerprint based Door lock system

Fingerprint locks can sometimes fail to recognize a legitimate user's fingerprint, or worse, recognize an unauthorized user's fingerprint, leading to security breaches. Many existing fingerprint locks have limited user capacity, meaning that only a limited number of fingerprints can be stored and recognized. This can be a disadvantage for households with multiple residents or in commercial settings with multiple employees. Fingerprint locks can be impacted by environmental factors such as moisture, dirt, and oil, leading to decreased accuracy and reliability. Fingerprint locks can be more expensive than traditional keyed locks or smart locks that use a code or card. Fingerprint locks require regular cleaning and maintenance to ensure accurate and reliable performance.

There has been an alarming increase in the number of crimes committed with the specific intent of causing harm to elderly or young people who live alone. Children, women, and the elderly, who are often left alone at home due to shifting family structures, are especially at risk. The majority of these incidents could have been avoided as tragedies if assistance had been given in a timely manner.Keeping people safe is crucial in the present day. With the current state of affairs, system security and safety are necessities. The increasing sophistication of modern threats has elevated the importance of security to a critical level. The definition of a contemporary home is one that requires minimal maintenance and provides optimum safety. The rise of wireless technology and automation, when combined, usher in a smarter, more efficient security system. With the use of cameras, an automated home security system may be created for the purpose of keeping an eye on and safeguarding the home's equipment and loved ones.

Recent innovations in communication and information technology have sped up the development of IoT applications and, by extension, smart home technologies. The security systems in smart homes are designed to provide customers with a higher level of comfort and convenience while also lowering operational expenses Improvements in home security have come a long way in the past several decades and will only accelerate in the years to come. When it comes to protecting your house, a smart security system may provide much more than just an alarm that goes off in the event of a break-in that falsely alerts you that someone is in your home.

Convolutional Neural Networks (CNNs) and Support Vector Machines (SVMs) are two types of artificial neural networks that are explored in this study (SVM)based smart home face recognition system is a type of biometric security system that uses an individual's unique facial

features for authentication and access control. The system uses a CNN to extract features from face images and an SVM for classification and identification. This hybrid approach takes advantage of the strengths of both algorithms, providing robust and accurate face recognition performance.

The system can be integrated into smart house technologies include electronic locks, cameras, and other safety features. and access control systems, providing an additional layer of security and convenience. With the ability to learn and adapt to new faces, the system can provide a high level of accuracy and security, while also being easy to use. This type of smart home face recognition system offers a new level of protection and ease for homeowners.

2. RELATED STUDY:

In a time when more and more of us are trying to reduce our impact on the planet, home automation is a viable option for doing our part to preserve precious natural resources. Reduce your home's energy costs by installing a home automation system that turns off lights and electronics when they're not in use. Home automation allows for the automation or simplification of several mundane household duties. An individual using a workplace with a computer must, As an example, you can disable the fan and the lights. every time he leaves the desk and turn them back on again when he returns. This is a mundane yet necessary duty that should not be neglected lest one throw away precious resources. This study presents a facial recognition-based security and energy-saving system to track when an authorised user is present or absent and adjust the ventilation and illumination accordingly. First, a face profile for each verified user was built by extracting LBPH (local binary pattern histogram) elements from their verified photos and modelling them with SVM. In order to distinguish facial objects from the backdrop, the camera takes a picture of the user in front of the computer. Python was used to implement the facial recognition algorithms, and a connection was made to Adafruit's environment so that the desk's lights and fan could be turned on and off automatically. Using the MQTT Protocol, Ada Fruit Cloud updates the relay status on an Arduino Esp8266. With this gadget, when an unknown person is discovered on a camera, the cloud-stored data is automatically updated to reflect an "off" state, turning off the lights and the fan. Even though passive infrared sensors (PIR) are often employed in home automation systems, their sensitivity decreases when the environment they are monitoring is already too hot. As a result, PIR sensors can't see people in the heat in nations like India. Rather than using the more typical PIR sensors for home automation, this setup offers an option. [10]

The popularity of IoT-based smart home systems continues to rise. The ability to securely lock and open the front door, garage, and other entrances is a crucial feature of the smart home system. This study proposes a Raspberry Pi-based facial recognition security system that can communicate with existing smart-home infrastructure. To implement this, we will utilise a Using a Raspberry Pi, a camera, the Blynk programme, and an SD card. The door's magnetic lock is coupled to a relay circuit, and its status is determined by the facial recognition algorithm's output. Using our suggested approach, we were able to achieve an accuracy of almost 90% in facial recognition, proving its efficacy. To save the necessary training or testing

time while simultaneously increasing recognition precision, we have presented a hierarchical image processing strategy.[11]

The rise in technological sophistication over the past decade has coincided with a corresponding rise in the number of attempted break-ins, making home security and automation systems increasingly popular. Based on the two separate and developing technologies of facial recognition for safety and speech recognition for automation, this article imagines a smart house. In addition, the most recent developments in the field are briefly reviewed, along with the reasons why an offline system was necessary to fill the void left by the new technological protocols presented in this area. In order to guarantee the smooth operation of the smart house, a security system is installed, which uses a Raspberry Pi microcontroller and OpenCV to capture an image when the bell rings and compare it with a database of owners. With only one voice command through the microphone linked to the Arduino V3 module, a disabled, elderly, or paralysed person in a rural area without internet connection may operate the entire home.[12]

There is a new technology on the horizon called the Internet of Things (IoT). allows computers and sensors to work together via a network to solve issues and provide new kinds of services. For example, the IoT is an essential part of today's smart houses. Many conveniences, like climate control, smoke alarms, automated lighting, keyless entry, and more, are available to homeowners thanks to Intelligent home systems. In any case, it also introduces new threats to security and privacy, including unauthorised access to users' private data through methods such as the manipulation of surveillance equipment or the activation of bogus fire alarms, among others. Smart homes are vulnerable to a wide range of security threats as a result of these concerns, and as a result, consumers are hesitant to use this technology. In this overview paper, we shed some light on the Internet of Things (IoT), its the exponential development, objects, and standards, the complex architecture of the Internet of Things (IoT), and the numerous security concerns that arise in a connected dwelling. Not only does this report cover the security measures used, problems that might arise home automation based on the Internet of Things, but it is also suggests a few potential ways forward.[13]

The purpose of the work is to develop methods for automatic face detection, either from a still image or from a video's worth of monitored faces. The availability of very large training datasets and complete task-specific training with a convolutional neural network (CNN) have both contributed to recent advancements in this domain. Despite the complexity of deep network training and face recognition, we show how a large-scale dataset (2.6 million images, over 2.6 thousand people) can be assembled with a mix of automation and humans in the loop and discuss the trade-off between data purity and time. [14]

The author discusses the efficacy of several facial recognition techniques such as Support Vector Machines, Convolutional Neural Networks, and Artificial Neural Networks, all trained on datasets such as Bag of Words, Histograms of Oriented Gradients, and Image Pixels (IPs). Support vector machines (SVM), convolutional neural networks (CNN), and artificial neural networks (ANN) are three examples of machine learning approaches (ANN)have all found applications in pattern identification, most notably in facial recognition

software. To extract features from images, people use BoW, HOG, and IP. AT&T's public face database has been used for testing. Each person is represented by a set of 10 photographs, each of which features a unique facial expression and lighting situation but shares the same standard size and PGM file format (92 by 112 pixels). The recognition accuracy of SVM was 97.00% with BoW, 96.00% with HOG, and 98.00% with IP. When CNN was trained on BoW, HOG, and IP, it improved its recognition accuracy to 94.00%, 99.00%, and 99.50%. ANN was able to achieve recognition accuracies of 96.00%, 99.00%, and 99.50% when evaluated with BoW, HOG, and IP, respectively. As shown by the experiments, the IP with the ANN method outperformed the others by a wide margin.[15]

3. METHODOLOGY:

The proposed method is based on face recognition based access control system using door's camera which clicks an image and compare the captured face with trained image and allows the owner to enter. These process are carried with an hybrid algorithm which is a combination of Deep Learning and SVM.

3.1 Hardwares Used:

Here are some hardware used to implement out proposed method, the whole idea of implementation cannot be done without the components.

3.1.1 Raspberry Pi 4 Model B:

Raspberry Pi is a popular and affordable single-board computer that can be used to implement machine learning (ML) projects. Here are some ways to implement Raspberry Pi in ML projects. Raspberry Pi can be used to build image processing projects using ML algorithms such as object detection and image classification. This can be done using libraries such as OpenCV and TensorFlow.

3.1: Raspberry Pi 4 B

3.1.2: Raspberry Pi Camera:

The high-definition 5MP camera is great for drones or a CCTV project since it takes stunning still images and video. Due to its compact size, the camera module may serve several purposes, including as a covert spy device or the imaging component of a Pi-phone.

Figure 3.2 : Raspberry Pi Camera with 5Mega Pixel

3.1.3: Solenoid Door Lock:

A solenoid door lock is a type of electrical lock that uses a solenoid, which is an electromagnet, to lock or unlock a door. When the solenoid is energized, it creates a magnetic field that pulls a metal armature into the core of the solenoid, which in turn, locks the door. When the solenoid is de-energized, the magnetic field disappears and the armature is released, unlocking the door. This door lock is connected with board and once the exact face is detected the door automatically opens.

Figure 3.3 : Solenoid door lock

3.2: Data Pre -Processing:

The first step in the machine learning process is called "data pre-processing," and it entails cleaning, converting, and otherwise preparing data for further analysis and modelling. It's a crucial stage in the machine learning process since it affects how well and how accurately the final models operate.The goal of data pre-processing is to prepare data in a way that allows machine learning algorithms to make accurate predictions and avoid common pitfalls, such as overfitting and underfitting. A webcam or locally stored image can supply the system with its input real-time visual. Low-contrast real-time photos can have their original contrast restored with an image enhancer and filter that uses tone mapping.

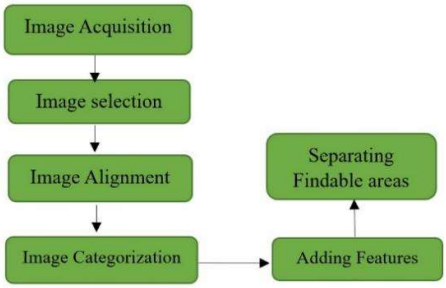

Figure 3.4: Data Pre-Processing

The images are captured in real time by the camera, and then stacked for later use. By sifting through a collection of images, one may pick the top candidates to include in a final composition.

3.3 Proposed System Architecture:

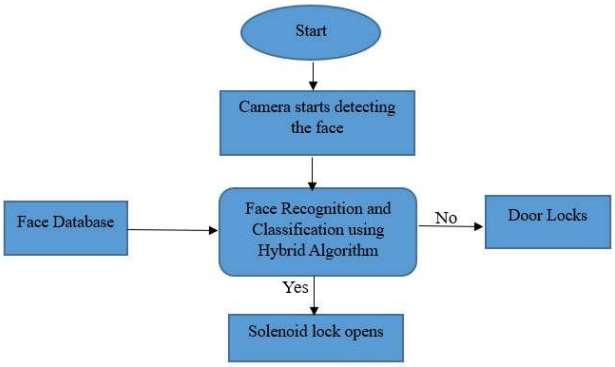

Figure 3.5 : Flow Diagram

We simply require the scale-normalized front faces from the input photos for our algorithm. Facial detection and extraction can help cut down on processing time needed for feature extraction. Convolutional neural networks for face recognition. Convolutional Neural Network (CNN) and Support Vector Machine (SVM)-based facial recognition system. is a type of biometric security system that uses an individual's unique facial features for authentication and access control.CNNs are used in deep learning-based face detection techniques. Convolution operations are performed on the input image to extract features and classify regions of the image as faces or non-faces. The equation used in a CNN is as follows:

$$f(y) = X * y + c \quad -(1)$$

where f(x) is the output of the convolutional layer, W is the weight matrix, x is the input to the layer, and b is the bias term.

Respondents were split into two categories based on their familiarity with facial recognition software. Five respondents with prior exposure to face recognition technologies made up one group. Another six participants had never used a face recognition system and made up the "naive" group.

$$\text{Total Score} = \sum_{j=1}^{6} M_j \times T_j \text{ - (2)}$$

The system works by first extracting features from a face image using a CNN. The CNN is trained on a large dataset of face images to learn to identify and extract the most important features of a face. These features are then used as input to an SVM classifier, which performs the actual face recognition and identification. The SVM uses a boundary, known as a hyperplane, to separate faces into different classes based on their features. When a new face is presented, the system predicts which class it belongs to by measuring the distance from the hyperplane. This hybrid approach of using both CNN and SVM algorithms offers several benefits. The CNN provides robust and accurate feature extraction, while the SVM provides efficient and effective classification and recognition. The system can be trained on large datasets to achieve high accuracy, and can be adapted to new faces and changing conditions. This type of face recognition system can be used for various applications, including security, access control, and personal identification.

4. RESULTS AND DISCUSSIONS:

A computer can detect, categorise, and align facial photos with the use of machine learning and neural networks; given a 2D image, the machine can produce an aligned 3D version of the same face. Facial recognition is achieved in this method by first classifying and then aligning a 2D picture of a person's face. A person's identity can be represented by a vector representation of their distinctive traits. Without any help from a human, the system can determine who is in a photo or video and assign them a unique identifier. A ground-breaking and ground-breaking algorithmic notion is face identification in ordinary photographs captured under natural circumstances. Despite the machine's best efforts to mimic the human mind and vision, its facial recognition accuracy is still rather low. There is always room for improvement, even though much progress has been made in recent decades, when it comes to detecting two-dimensional photos of faces taken in entirely controlled and confined settings. Methods like intelligent biometric identification and sketch control are used. However, the system's capabilities are severely constrained in a real-world setting, where factors like lighting, facial expressions, and age play a role. As a rule, system performance degrades noticeably under uncontrolled and unexpected situations that were not factored into the design of the system.

A database of photos may be searched to find a match for a 2D image of a face. Face photos are saved in a face database, where there are sets of photographs and each set corresponds to a face. The facial ID consists of a collection of characteristics. When a convolutional neural network (CNN) is executed, the face IDs that are generated from the 2D images are sorted based on the values that are assigned to them in each of the layers immediately next to the layer

being processed. After comparing the identifiers to the identification of the person portrayed in the image, the faces are divided based on the categorization.

Table 1: Comparison of Proposed method with existing methods for Face Recognition

S.No	Method used to Implement	Accuracy in %
1.	Novel Multi-face ORL	98.35
2.	CNNs, FERET, LFW and YTF	94.23
3.	LBP	98.28
4.	LBP and SVM	96.83
5.	**Proposed Method**	**99.25**

In the first work taken for compression the facial recognition programmes have made extensive use of PCA in conjunction with other algorithms for decades. kings. [16] In addition to the ABAS algorithm, LBP and PCA were also employed for facial recognition. Multiple methods for face recognition have been developed by combining LBP and PCA as feature extraction techniques with the ABAS algorithm to optimise the Neural Network, in this case employing the SoftMax function. Time spent identifying faces has been reduced. Followed by the another work which is used CNN, FERET, LFW and YTF are the algorithms gave the accuracy of 94.23%.And hereby another work also been processed by LBP algorithm which returns the accuracy of 98.28%.And as per the reference there was an research taken by researcher where they used both LBP and SVM which returns 96.83% of accuracy in recognising faces. In connection with that our proposed methodology which has the combination of CNN and SVM returns 99.25% of accuracy.

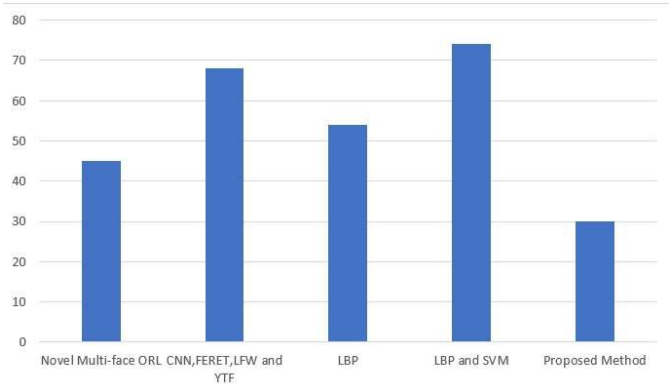

Figure 4.1: Computation results compression between Algorithms

The computational time for different algorithms varies greatly and depends on several factors, including the size of the input data, the complexity of the algorithm, the computational resources available, and the efficiency of the implementation. Some algorithms are designed to be fast and computationally efficient, while others are designed to be more accurate and may require more computational resources. With reference to the existing work used for the face recognition some algorithms takes more time to compute the process. In that way

CNN,FERET,LFW and YTF algorithm took 67% for computing. And the researcher used LBP algorithm used 55% of computation time. Hereby the LBP and SVM algorithm takes 75% of time for computation and our Proposed Method takes around 30% for computation.

5. CONCLUSION:

In conclusion, the integration of facial recognition technology into smart home systems has enormous promise for improving safety and convenience in the home. Real-time face detection and recognition is made possible by smart home systems thanks to algorithms like Convolutional Neural Networks (CNNs) and Support Vector Machines (SVMs), which allow for features like automated door opening, temperature regulation, and lighting customization. However, there are still challenges that need to be addressed, such as improving the accuracy of face recognition systems, particularly in low-light conditions, and protect the confidentiality of sensitive data. Additionally, further research is needed to explore combination of facial recognition software with other smart home systems and devices. Overall, the implementation of facial recognition software in smart home systems is an exciting development that has opportunity to dramatically enhance standard of living for homeowners.

REFERENCES:

1. Chan, M., et al., A review of smart homes—Present state and future challenges. Computer Methods and Programs in Biomedicine, 2008. 91(1): p. 55-81.

2. Balta-Ozkan, N., O. Amerighi, and B. Boteler, A comparison of consumer perceptions towards smart homes in the UK, Germany and Italy: reflections for policy and future research. Technology Analysis & Strategic Management, 2014. 26(10): p. 1176-1195.

3. Alam, M.R., M.B.I. Reaz, and M.A.M. Ah, Statistical modeling of the resident's activity interval in smart homes. Journal of Applied Sciences, 2011. 11(16): p. 3058-3061.

4. Arunvivek, J., S. Srinath, and M.S. Balamurugan, Framework development in home automation to provide control and security for home automated devices. Indian Journal of Science and Technology, 2015. 8(19).

5. Dawid, H., et al., Management science in the era of smart consumer products: challenges and research perspectives. Central European Journal of Operations Research, 2017. 25(1): p. 203- 230.

6. Hong, J., J. Shin, and D. Lee, Strategic management of next-generation connected life: Focusing on smart key and car-home connectivity. Technological Forecasting and Social Change, 2016. 103: p. 11-20.

7. Khedekar, D.C., et al., Home Automation—A Fast - Expanding Market. Thunderbird International Business Review, 2017. 59(1): p. 79-91.

8. Coughlan, T., et al., Current issues and future directions in methods for studying technology in the home. PsychNology Journal, 2013. 11(2): p. 159-184.

9. E. K. Choe, S. Consolvo, J. Jung, B. L. Harrison, and J. A. Kientz,"Living in a glass house: a survey of private moments in the home," in UbiComp 2011. ACM, 2011, pp. 41–44.

10. Karthikeyan, M. et al. "Real Time Face Recognition based Smart Lab for Energy Conservation." Webology (2021): n. pag.

11. Abdullah, Sarah. "Development of Face Recognition Based Smart Door Lock." International Journal of Advances in Scientific Research and Engineering (2021): n. pag.

12. Munir, Al-Kaber et al. "Face and Speech Recognition Based Smart Home." 2019 International Conference on Engineering and Emerging Technologies (ICEET) (2019): 1-5.

13. Touqeer, Haseeb et al. "Smart home security: challenges, issues and solutions at different IoT layers." The Journal of Supercomputing 77 (2021): 14053 - 14089.

14. Parkhi, Omkar M. et al. "Deep Face Recognition." British Machine Vision Conference (2015).

15. Islam, Kh Tohidul et al. "Performance of SVM, CNN, and ANN with BoW, HOG, and Image Pixels in Face Recognition." 2017 2nd International Conference on Electrical & Electronic Engineering (ICEEE) (2017): 1-4.

16. F. Wang, F. Xie, S. Shen, L. Huang, R. Sun and J. Le Yang, "A Novel Multiface Recognition Method With Short Training Time and Lightweight Based on ABASNet and H Softmax," in IEEE Access, vol. 8, pp. 175370-175384, 2020, doi: 10.1109/ACCESS.2020.3026421