

A Deep Learning-Based Intelligent Face Recognition Method in the Internet of Home Things for Security Applications

Asif Rahim¹, Yanru Zhong^{2*}, Tariq Ahmad³

¹ School of Computer and Information Security, Guilin university of Electronic Technology, Guilin, China

² Guangxi Key Laboratory of Intelligent Processing of Computer Images and Graphics, Guilin University of Electronic Technology, Guilin, China

³ School of Information and Communication Engineering, Guilin University of Electronic Technology, Guilin, China

Abstract: At the beginning of the 21st century, human life has become increasingly dependent on security. At this point, the cost is the essential consideration. This approach can reduce monitoring costs. This research proposes a real-time recognition system to deal with photos as soon as possible. We hope that by identifying people, we can keep our homes and offices safe. One of the primary goals of this research was to develop a method of intelligent face recognition for smart homes based on deep learning. To demonstrate the usefulness of our study, we also examine and contrast this model with other methodologies deemed contemporary. This research proposes a tree-based deep model for cloud-based face recognition. The proposed deep model is less computationally demanding without affecting accuracy. Trees for each volume are built in the model's input volume, split into many ones. The number of branches and their height characterizes trees. Residual functions are used to represent each branch, and they are built from a convolutional layer and two non-linear functions. In various openly accessible databases, the proposed model is put to the test. It also compares to the best deep facial recognition models in the industry today.

Keywords: smart home, face recognition, deep learning.

一種基於深度學習的物聯網智能人臉識別方法在安防應用中的應用

摘要：21 世紀初，人類的生活越來越依賴於安全。在這一點上，成本是必不可少的考慮因素。這種方法可以降低監控成本。本研究提出了一種實時識別系統來盡快處理照片。我們希望通過識別人員身份，我們可以保護我們的家庭和辦公室安全。本研究的主要目標之一是開發一種基於深度學習的智能家居智能人臉識別方法。為了證明我們研究的有用性，我們還檢查了該模型並將其與其他被認為是當代的方法進行了對比。本研究提出了一種基於樹的深度模型，用於基於雲的人臉識別。所提出的深度模型在不影響準確性的情況下對計算要求較低。每個卷的樹都構建在模型的輸入卷中，分成許多樹。樹枝的數量和高度是樹木的特徵。殘差函數用於表示每個分支，它們由一個卷積層和兩個非線性函數構成。在各種可公開訪問的數據庫中，對所提出的模型進行了測試。它還與當今業界最好的深度面部識別模型進行了比較。

关键词：智能家居，人脸识别，深度学习。

Received: July 7, 2022 / Revised: August 3, 2022 / Accepted: September 9, 2022 / Published: October 30, 2022

Fund Project: The National Natural Science Foundation of China (No. 62166011); The Innovation Key Project of Guangxi Province (No. 222068071); Guangxi Key Laboratory of Intelligent Processing of Computer Images and Graphics

About the authors: Asif Rahim, School of Computer and Information Security, Guilin University of Electronic Technology, Guilin, China; Yanru Zhong, Guangxi Key Laboratory of Intelligent Processing of Computer Images and Graphics, Guilin University of Electronic Technology, Guilin, China; Tariq Ahmad, School of Information and Communication Engineering, Guilin University of Electronic Technology, Guilin, China

Corresponding author Yanru Zhong, rosezhong@guet.edu.cn

1. Introduction

The rapid growth of information and communications technology has led to the implementation of a great number of intelligent systems that use various machine learning algorithm methodologies. The Internet of Things (IoT) is the greatest choice for performing intelligent work and putting innovative ideas into action in the rapidly developing field of invention. The approach suggested for usage during this project is frequently referred to as an asset smartness system. This is because it will offer an improved solution to the user safely.

IoT is made up of a growing number of devices that can make numerous intelligent and useful systems, such as smart cities, smart homes, and face recognizers. 2021 was the year that the Home automation group carried out the study to get information regarding smart homes, smart attendance systems, and responses to IoT solutions for smart environments. Additionally, the results of the survey showed that respondents clearly articulated their worries over the strengths, weaknesses, opportunities, and threats posed by prospective IoT technologies. These worries served as the impetus for selecting this topic for the project.

If a home and its contents are not adequately protected in today's environment, there is a significant increased risk of experiencing various unfortunate events. We frequently employ IOT, which is a rapidly developing technology, in conjunction with face recognition to make the process of supplying smart home systems easier, more straightforward, and error-proof. Devices connected to IoT are well-known for their use in various domains including smart homes and cities, as well as in fields such as education and health care. Besides that, there will be advancements in areas such as transportation and autonomous connected vehicles, agriculture of IoT devices that are used in these environments.

According to [1], businesses think that the IoT concept is the most difficult to put into practice, which makes it hard for them to do. Security, privacy, cost, and regulatory issues are some to pay attention. Over half of those polled said that implementing the IoT concept can have a big impact on the company. 79% of those polled said that the IoT concept has helped them achieve positive results in many areas of work that they couldn't have done without the IoT concept.

It is necessary to categorize IoT devices for various reasons, as explained in [2] an IoT device that fails to operate as expected or unexpectedly may indicate that a security event has occurred within the system. Fig. 1 presents an example of an intelligent smart home with several IoT-connected utilities. The ability to link objects and equipment through Internet in a home allows users to monitor and manage them remotely. Recently [3], smart home solutions have grown.

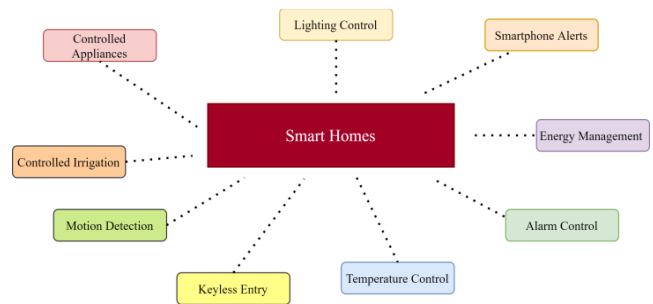


Fig. 1 Intelligent Smart with different IoT devices connected

Mobile devices, laptops, desktops, tablets, smart watches, and even voice assistants can all be used to control home automation systems. Security cameras, automated door locks, increased awareness, more comfort, time savings, energy regulation and cost savings are just a few perks that come with home automation systems, which offer many features to their users. Recently IoT-based home automation components shipments have been increased to a wide number of ranges, as shown in Fig. 2.

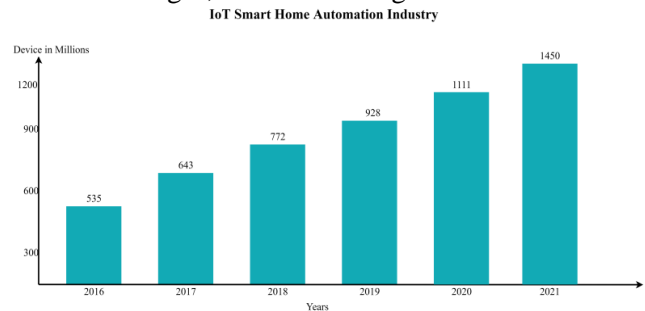


Fig. 2 Selling the smart home automation industry based on IoT

A growing field known as machine learning, which is a subset of artificial intelligence, can be of great assistance in the process of facial recognition. This assistance, in turn, could be used to either explore new fields or even improve the effectiveness of fields that are already in existence. It is quite difficult for humans to recall the faces of other people, but the computer does not have this problem, and it may be used in situations when there is a requirement to retain a greater number of photographs in databases of facial records. The face recognition system is an innovative piece of technology that uses the principles of artificial intelligence to offer a superior answer to the issues listed above. The same kinds of applications are used for airport surveillance, private security, and other kinds of security, among other places. The main objectives of this study are

- To propose deep learning based intelligent face recognition method for smart homes.
- To evaluate and compare this model with other methods to show the effectiveness of this study.

This paper is divided into five sections. Section 1 shows the introduction of this study. Section 2 shows the related studies and Section 3 shows the

methodology and novel framework of this research. Section 4 shows the results of the current study, a comparative analysis with previous studies, and discussion of the results. Section 5 is the conclusion; section 6 is about limitations and further study.

2. Literature Review

Face recognition in [4] is modeled and simulated using DCT/DL and Deep Learning techniques. This study produced 100% accurate human face detection and identification system. The system will remove watermarked or skewed images from the database. Face tracking results with watermarks." Because of the ambiguity of the first image, Convolutional Neural Networks (CNNs) and deep learning appear unable to correctly identify it. Thus, CNN and deep learning algorithms have a cap. The watermark image is protected and hence, cannot be recognized. An image of a human face can be detected using CNN. If the image has human traits, a yellow tracking box indicates the designated face. A yellowish box will be drawn around the chosen face or image. The following distinguishing aspects of the human face are used to trace, scan, and detect it using CNN and deep learning approaches: Human faces are not slanted or angled beyond 5 to 10 degrees. The face may not be hidden by another object or placed on another one. No computer-generated images of people's faces. The CNN/DL will not recognize the facial image if it has a watermark. To work, the deep learning algorithm must examine photos, identify faces, and store them in a database. A folder named Image Folder will let MATLAB distinguish between images with and without human faces. Face detection systems have great resolution around 85% of the time. The program may distinguish human and non-human faces. As a result, authors cut their work time in half.

An AI-based facial recognition model using Docker containers is the purpose of this thesis. This study develops an AI-based facial recognition model using Deep Learning. In a Docker Container on an IoT platform, the model will decide whether to lock or unlock the door system. This study will use a low-power IoT device containerization paradigm to implement edge computing and AI. Containerization is like virtualization. IoT devices can easily run the Docker (Firefly-RK3399). Docker manages the dependences and modules for containerized programs. The author's research focuses on building containerized AI models. [5] used a CSI connector to connect the camera and train the system to recognize faces. The algorithm uses deep learning, a sub-type of Artificial Intelligence. After a deep learning algorithm has identified the faces, the image is converted into a set of gradients. SVM classifier can be used to train an image recognition system using modified gradients. Finally, the authorized user may be found. The authors

devised a way for constructing a containerized AI model and installing it on a Raspberry Pi (an IoT device). Containerized programs are efficient, portable, and cross-platform. The containerized program is also architecture-neutral (ARM, x86, amd64).

With the use of face recognition technology in IoT platforms for senior care, authentication and monitoring can be improved. However, due to the possibility of restricted engagement capabilities on the part of users, the broad variety of interface devices, and the requirement to securely store biometric data, its inclusion may prove difficult. Deep neural networks are used for secure recognition and interaction guiding [6], and they are lightweight. In an automated method, the inference engines, model configurations, and batch sizes are chosen based on the characteristics of the edge device being used. Biometric data are encrypted homomorphically to maintain privacy. Its potential can be recognized by contrasting it with the most recent alternatives that are available.

Deep learning-based facial recognition systems have made significant strides recently, and they will continue to do so. In unconstrained situations, where factors such as illumination, image resolution, and background clutter cannot be controlled, a considerable deal of work remains to be done in the field of face identification. The goal of [7] was to identify a person of interest in these unrestricted circumstances. As a result, here are the contributions we've made: Using Keras, a fast open platform for deep learning, the Convolution Neural Network model (CNN) based on the VGG16 architecture was created and tested. It was necessary to conduct a series of experiments using the labeled faces in Wild benchmark dataset to demonstrate that the proposed approach is state-of-the-art (LFW).

IoT devices are rapidly being used in many industries. The extensive use and growth of IoT in many areas have generated a huge amount of data. The use of IoT devices for medical surveillance generates massive volumes of data. Face recognition is an important tool for securing medical facilities, detecting patient fraud, and tracking hospital traffic. Face-recognition algorithms are less accurate in an uncontrolled environment. Also, many applications, like smart healthcare, require real-time systems. A tree-based deep model can accomplish cloud-based facial recognition. The proposed deep model in [8] is 100% accurate. The model splits one input volume into multiple volumes, each with its own tree. A tree's branching pattern and total height define it. A residual function composed of a convolutional layer and two non-linear functions represents each branch. The proposed approach was tested in public databases. The performance was also compared with the latest deep models for facial recognition. Using the FEI, ORL, and LFW databases, the suggested model has 98.65% 99.19%, and 95.84% accuracy.

Recent algorithmic improvements have coincided with increased use of automatic facial recognition systems. However, benchmarking evaluations do not take human operators into account. As a result, the system's performance differs from the findings of evaluation tests. To combat this, [9] used facial recognition technology to check passport applications for identity fraud. Experiment 1 used passport images from a large database to test algorithm-generated "candidate lists." Researchers discovered that participants' accuracy was substantially worse when matching photographs of adult targets than when matching photographs of children. Using Experiment 2, researchers compared student participants' performance to that of professional passport officers, who use the system regularly in their professions. Fortunately, a team of expert "facial examiners" outperformed the others by 20%. In real-world circumstances, human error can limit facial recognition system accuracy by up to 50%. Proper training and mentorship may improve face human operators of recognition systems, although practice alone does not remove these limitations.

Because of technological breakthroughs in embedded systems and IoT, the concept of the "smart home" has gained popularity recently. Deep learning, on the other hand, has resulted in several ground-breaking findings. Deep learning can enhance the user experience and security of a smart home system. In [10], the convolution neural network model is employed in the field of face identification in natural situations as part of the deep learning approach, which is part of the deep learning method. Photographic images are gathered and analyzed by embedded devices before being transmitted to the server. Face recognition matches on the server have been improved using a lighter VGG network model, which is more efficient. Embedded devices can benefit from this smart home system by reducing their calculation requirements and increasing identification accuracy. Face recognition in surveillance video was successfully tested with this technique in several scenarios.

People who suffer from prosopagnosia have difficulty telling the difference between different people based on their facial traits. Authors intend to develop a facial recognition system that can identify people and provide them with personal information by using wearing glasses in the future. [11] provided a facial identification system built on a client-server architecture, as opposed to previous systems that ran locally on glasses or cellphones. To capture photographs and establish a connection with the server, authors designed and created programs for both smart glasses and smartphones. Deep CNNs were used in the back-end system to achieve 98.18 percent accuracy in facial recognition. This was achieved using deep CNNs. The system is capable of accommodating new identities and looks without the need to recreate the model from scratch.

Science and technology abound in the world we live in today, and it is impossible to keep up. The development of biometric identification applications and requirements is occurring at a rapid rate in line with the increasing proliferation of mobile devices. In comparison to previous identity authentication methods, biometric identification technology is both more secure and more convenient, making it a step in the right direction. Recently, cities have had a significant impact from the confluence of artificial intelligence and the IoT, which has had a significant impact on retail, transportation, and even cuisine. A deep learning-based facial recognition system for the smart shopping cart is the objective of [12], and it will be built and implemented in this article. In supermarkets, tablet computers are used in conjunction with the traditional shopping trolleys that are commonly present. Customers may log in using a tablet and facial recognition technology, which increases the security and simplicity of the process. The tablet collects face samples from the user, and the image is then preprocessed to extract important features from the sample. When there are not enough user samples available, the matching network learning method with a short training set is used for facial recognition.

Deep learning (DL) is becoming increasingly significant in IoT, as well as in the medical and healthcare industries. This field can benefit from better touchless authentication, especially regarding infectious disorders like coronavirus sickness 2019. Security solutions such as biometric touch authentication and lost keys and passwords all have weaknesses. To overcome these challenges, IoT-based intelligent control medical authentication systems using DL models have been created. In this project, IoT and DL models are employed to authenticate human faces. [13] chose the Raspberry Pi due to its inexpensive cost and major controller role (RPI). The RPI's GPIO pins were used to develop a smart control system for smart locks and doors. To get access to the system, a camera module takes a picture of the user's face and compares it to database photos. Face detection is performed using Haar cascade techniques, whereas face recognition is performed using the following processes. In the first step, pre-trained CNN models (ResNet-50 and VGG-16) and the LBPH approach extract facial features. In the second step, SVM classifier might be used. Otherwise, the door locks and an email with the face photographs and time information from the SQL database are sent to the home/medical place. Compared with other related strategies, this strategy achieved 99.56 percent accuracy.

Every household today requires the installation of a home security system. The traditional method for opening a door was with the use of a key, a security card, a password, or some other form of identification. Having your keys stolen or misplaced, on the other hand, might lead to much more serious problems, such

as robbery and identity theft. This has developed into a significant issue. Deep learning facial recognition in conjunction with IoT can be used to construct a more effective access control system for doors, which could be a solution to this problem. According to [14], Raspberry Pi, a small programmable computer board, is in charge of controlling face recognition, youth systems, and locking systems, among other things. A camera is used to capture images of the person who is standing in front of the door. The IoT system allows the user to control the door access.

Recently, human life has become increasingly reliant on the availability of security. For the time being, the most significant aspect is the price. The cost of keeping an eye on devices from the outside is prohibitive,; so this option comes in handy. An image recognition system that can process images at a breakneck pace is proposed in [15], as discussed in detail in the following sections. is the major purpose of this study is to identify individuals to protect one's home and workplace. The PIR sensor is used to accomplish this by detecting movement in a limited area. Finally, the Raspberry Pi is responsible for taking the photographs. The photograph will be scanned for faces and recognized when it has been acquired. The final step will be to use the Telegram to send photographs and notifications to a smartphone-based IoT. A low computing cost is associated with this technology, and the systems are real-time and fast. The system proposed in this study can provide real-time facial recognition capabilities.

Face recognition is the ability to recognize an individual in a group of individuals, whether they are alone or in a big gathering of people. Deep learning has emerged as the most effective method for dealing with face recognition difficulties using CNNs, and it has been increasingly popular recently due to its outstanding performance. Challenges in computer vision such as modeling and saliency detection, semantic segmentation, handwriting recognition in digital form, and emotion identification all use this extremely strong technology to some extent. New datasets have had a significant impact on the development of CNN models that employ well-known CNN architectures as Alex Net and VGG. [16] made a substantial contribution to the implementation of a suggested CNN for face identification, which can properly identify 97 percent of the faces tracked in video or image capture using a VGG Face that has been previously trained. Implementing metric learning to generate distinguishable features from our data sets is also a vital first step.

A combination of local binary patterns (LBP) and deep learning techniques (DBNs) has been used in recent face recognition systems (DBN). Both suffer from an abundance of face photographs, but the latter overlooks the value of regional facial features. Local

handmade feature descriptors combined with the DBN can be used to tackle unconstrained face recognition. The Curvelet–Fractal approach to multimodal local feature extraction was first proposed. It combines the Curvelet and Fractal dimensions. The Curvelet transform may readily convey the essential structure of the face (e.g., edges and curves), whereas the fractal dimension is one of the most powerful texture descriptors for images of faces. This is the method's main inspiration. The MDFR framework uses a DBN on top of local feature representations rather than pixel intensity representations for add additional feature representations. [17] showed that the MDFR representations complement the Curvelet–Fractal technique. Finally, the suggested strategies were tested on four large-scale face datasets (SDUMLA-HMT, FERET, CAS-PEAL-R1, and LFW). On all datasets, the proposed approaches outperform existing approaches (e.g. LBP, DBN, and WPCA) in terms of producing innovative results.

Deep learning-based algorithms have dominated face recognition due to their superior performance on tough wild datasets. The authors tested these strategies on datasets including Labeled Faces in the Wild and YouTube Faces. This system's ability to deal with variations in individual appearance caused by variables like head attitude, lighting, occlusion and misalignment was not fully evaluated. However, misalignment owing to erroneous facial feature localization was evaluated by in [18]. The deep learning models VGG-Face and Lightened CNN were used to extract face representations. But even while deep learning provides a powerful representation for face recognition, it can benefit from preprocessing such as position and illumination normalization. This is especially relevant if the dataset used to train a deep learning model excludes variances. Experiments have shown that deep learning-based representation can withstand misalignment and facial feature localization errors up to 10% of the intraocular distance.

Many smart cities are incorporating face recognition (FR) and other biometric technologies. Researchers and engineers from all around the world have been working hard to improve the reliability of these systems and their everyday uses. FR is developing new technology for use in real-time situations. The project [19] uses transfer learning in fog and cloud computing to develop a comprehensive FR system. Occlusions, expressions, lighting, and positions can all affect FR performance, which is why deep convolutional neural networks (DCNNs) were developed. DCNN extracts relevant facial features. These features allow us to easily compare two faces. Online learning can be performed by adding new users to the system and revising existing projections. The proposed method was evaluated using three common machine learning techniques: Decision Tree, K Nearest Neighbor, and Support Vector

Machine. The suggested system was evaluated using three face image datasets (SDUMLA-HMT, 113, and CASIA) and performance parameters of accuracy, precision, sensitivity, and specificity. The proposed technique outperforms all other algorithms in all metrics. Compared with the comparison algorithms, the suggested method has 99.06% accuracy, 99.12% precision, 99.07% recall, and 99.10% specificity.

Recently, various deep learning-based facial recognition systems have demonstrated outstanding performance when trained on massive amounts of labeled data. In part due to the difficulties in obtaining data, a convolutional neural network (CNNs) for daily attendance taking facial identification is a tough area to research and develop. In small sample learning, data augmentation has been used to expand the number of samples to improve accuracy. To overcome this issue, [20] employs geometric transformations, image brightness adjustments, and various filter operations in this research. Additionally, authors determine the most effective data augmentation strategy based on orthogonal tests and experiments. Authors finally get to put the author's attendance strategy to the test in a real classroom setting. The author's proposed technique, which uses a VGG-16 network and data augmentation, is 86.3 percent more accurate than PCA and LBPH, respectively. As additional data are acquired, the accuracy increases to 98.1%, reaching 98.1%.

It has recently been demonstrated that masked face recognition (MFR) can be used in various applications, including masked face tracking for the safety of people and the secure identification of individuals. The design and dissemination of relevant algorithms have increased dramatically because of new dangers, such as pandemics and fraud. Research on how to identify and authenticate people wearing masks is expected to continue for a long time, and more efficient ways for real-time MFR are needed. Using machine learning, it is now possible to identify and authenticate people whose faces are obscured by masks or other forms of concealment. Using deep learning techniques, [21] compiles and reviews the most recent MFR studies, providing insights and extensive discussion on the development pipeline of MFR systems. Deep network topologies and deep feature extraction methodologies are used as the basis for the introduction of cutting-edge approaches. Data sets and metrics used for MFR benchmarking and evaluation are also covered here. An extensive list of problems and potential solutions is provided. A wide range of contemporary approaches and achievements are examined in this thorough study, which provides a worldwide perspective on MFR.

Although face recognition is a tough topic in image analysis and computer vision, it has received a great deal of attention recently due to the numerous applications it has in various industries. Face recognition systems can be divided into three major categories based on how the face data are collected:

those that work with intensified photos, those that work with video sequences, and those that require additional sensory data, such as 3D information or infrared photography, to name a few examples. [22] presents an overview of some of the most popular techniques in each of these areas, as well as some of the advantages and disadvantages of the many systems discussed. This document also includes information on the advantages of facial recognition technology, the applications of this technology, and some difficulties that existing systems have in performing this function. The technique of face recognition is also discussed in this document, which provides an overview of this status of the technology.

We live in the age of technology, and we own it. IoT will soon be like a new member of our family, capable of being integrated into various areas of our daily lives to produce results that are both precise and desirable. Regarding the use of picture analysis and the algorithmic understanding known as computer vision, face recognition offers an ocean of possibilities. Security is a fundamental human right that no one can reject, and to support this right, there are numerous studies and investigations occurring around the globe. Various breakthroughs in IoT-based home security have been made recently. The authors of [23] are working on a project called Face Recognition. Facial recognition is the process of identifying a person based on their appearance. The system uses a method for capturing images. The camera takes a snapshot of the face and compares it to the database image. The gate will open if the picture matches the database, or a notification will be sent if it doesn't. The OpenCV library will be used for the recognition algorithms.

A person's face can reveal more about their identity, expression, and feelings than any other part of their body. Every person in today's culture wants to be more protected from unauthorized authentication in today's environment. With the goal of increasing security, "Facial Recognition" has come into play and taken on the most challenging duty of accurately and reliably tracking down a person's face. [24] used histogram-based facial recognition to improve face recognition accuracy by separating a face into many regions and extracting histogram values, which are then combined into a single vector. The facial photographs are compared using this vector and the most efficient result is found. Histograms are employed in face-recognition software. To aid in object detection, computer vision and image processing use the histogram of oriented gradients (HOG). Localized areas of an image are counted for instances of gradient orientation. A dense grid of equally spaced cells is used to compute edge orientation histograms, scale-invariant feature transform descriptors, and shape contexts; however this method varies in that it uses overlapping local contrast normalization for enhanced accuracy.

Face recognition (FR) is used in various applications, including biometrics, security records, access control,

law enforcement, smart cards, and reconnaissance devices. It is a means of distinguishing people based on their facial images. Convolutional Neural Systems, a framework of profound systems, have been proven to be effective in achieving success for FR. Several pre-processing operations, such as testing, must be completed before the application of Convolutional Neural Systems in real-time structures. The Convolutional Neural Systems perform all of the processing (including selection, highlight extraction, and instruction) because of the arrangement, which uses all the images (and their pixel values) as input. The field of encounter acknowledgment has seen particularly promising results from CNNs, which have demonstrated promising results. How to build a "excellent" supplementary format for CNNs while simultaneously explaining why they operate so well remains an unaddressed question to date. Recent questions have tended to be more knowledgeable about the specifics of CNN's model design according to [25].

Individuals are increasingly desirous to being able to use all of their electronic devices at any time and from any location, which involves the usage of a network and an Internet connection. This is despite the fact that it raises many significant security risks. It was decided to employ the IoT and Artificial Intelligence (AI) in [26] to develop a home automation security system that could be accessed remotely using an Android application. To control door entrance in a highly efficient security system, face recognition technology is employed. It is possible to set up security PINs in the event of technical failure, but these PINs are only available to the owner. Although home automation systems can be used for a range of tasks, the cost may be prohibitive for many customers. It is the author's aim that, by leveraging multi-modal security, authors will be able to create a solution that is both cost-effective and simple to use for end users. Using the Haar Cascade and LBPH, the system was 92.86 percent accurate in detecting real world faces.

IoT refers to remotely connecting and monitoring real-world entities. Making our homes and workplaces smarter [27], safer, and more automated is possible. This project uses wireless technology to create an intelligent security system that can send alerts to the owner and raise an alarm if necessary. Many security solutions on the market are out of the reach of the common individual. [28] informs the user about OpenCV2, LBPH, and SMTP. Local implementation focuses on the home, college, and workplace. Once the camera is activated, the system produces real-time facial recognition. The taken image is compared to the database photos and if they match, the door opens and the user is permitted in. If the photograph does not match any photographs in the database, it is sent to the owner's email. The system will wait for the owner to respond before taking action. It will provide or restrict

access based on the owner's information. The project's main goal is to develop a real-time, low-cost facial recognition system.

Nowadays, we use modern locking system programs to lock and unlock our autos. We can unlock our automobile from the outside, or use a keyless entry remote control to access the doors. These locking methods are convenient, but they can be difficult to operate when the hands of someone are full and they don't have their keys with them, or when they lose their keys. Face recognition can be used to unlock the vehicle. Face recognition is be a vital component of future intelligent vehicle applications in the next generation of autonomous vehicles. [29] proposes a locking mechanism for AV using deep learning and facial recognition technologies. This paper's purpose is to use a photo dataset with training, validation, and test folder. The Convolution Neural Network (CNN) in this study was programmed in Python using Google Colab. The authors created two folders to test two approaches of recognizing faces. Finally, after training the dataset, a test was run, with positive results. The models can properly predict the ultimate outcome and produce notable outcomes. The data gathering includes the front, right (30–45 degrees), and left facial angles (30–45 degrees).

Deep learning is beneficial in various fields, including natural language processing, computer vision, image processing, and machine vision [30]. Using a technique known as deep learning, it is feasible to construct an image of a human being that is indistinguishable from the real thing, making it hard for humans to distinguish between the two. Deep fakes, which are produced by generative adversarial neural networks and can pose a threat to the public, have been discovered (GAN). It is vital to identify and stop the distribution of deep-fake image content. Several studies have been conducted on deep fakes in the field of picture manipulation. The main disadvantages of the current approaches are their inaccuracy and long processing durations. Local Binary Pattern Histogram (LBP Histogram) of Fisherface's Local Binary Pattern (Fischerface's LBP Histogram) is used to detect deep fake face photo analysis (FF-LBPH). Fisherface is a face recognition technology that uses LBPH shrink the size of the face space. Create a deep fake detection classifier by combining the DBN and RBM techniques. The publicly available datasets used in this study are FFHQ, 100K-Faces DFFD, and CASIA-WebFace, among others.

A significant amount of work is being done in the field of home security, where IoT is poised to be a game changer in terms of ensuring the safety of our everyday lives. Door lock security is one of the most important aspects to keep an eye out for your home, as many times the door lock does not provide the amount of safety that is required by the law. A well-established approach, known as facial recognition, is used to

recognize and identify the face of an image. As part of the author's smart door proof of concept, [32] will use a front-facing HD camera connected to a monitor to display the identity of the person standing in front of it. Additionally, we'll be using the Raspberry Pi's ARM processor to process text inputs and display the results on the computer's screen. The Local Binary Pattern Histogram (LBPH) is used to determine the popularity of various facial expressions.

In today's society, home security is paramount. If we safeguard our homes with old-fashioned methods, thieves are more likely to break in. A costly security system must protect the author's home. To address this issue, authors created an IoT platform that allows us to set up a smart home security system. [33] suggests using face recognition technology to construct an automatic door lock and unlock system. In case of an emergency, authors can be notified remotely. The Raspberry Pi will have PIR and other sensors attached to it, as well as a camera. When a camera captures an image of a person in front of the door, it uses a local binary pattern (LBP). The door unlocks if the person's image matches a family member or other recognized individuals. An email containing a photo of the intruder will be sent to the owner's Gmail account. The suggested method warns the home's owner anytime about unknown individual approaches the front door. This knowledge will help the user.

The most defining characteristic of a person is his face. Every individual, including identical twins, has a unique facial expression. Facial recognition and identification system is required in order for people to be distinguished from one another. A face-recognition system is a type of identification system that uses biometrics, such as facial recognition, to identify its users. Face recognition technology is currently being used in various applications, including unlocking a phone and identifying thieves or intruders. This technology is more secure because it is based solely on a facial image and does not rely on any additional dependencies, such as a key or a card, to function properly. Face detection and face identification are the two most important elements in the development of a human identification system. In deep learning is used in this study to construct a face recognition system using OpenCV in Python.

The authors of [34] discuss how to do so. Because of its high accuracy, deep learning for face identification appears to be a good method for face identification. The accuracy of the suggested facial recognition system is demonstrated in an experimental setting. Due to the enormous domain difference and lack of paired images in multiple modalities during training, heterogeneous face matching is a significant barrier in face recognition. An approach to face matching based on deep learning (CDL) is presented in [35]. CDL seeks a shared feature space to approximate a homogeneous face matching problem for the

heterogeneous face matching problem. For the most part, CDL's objective function is divided into two components. For example, a trace norm and a block-diagonal prior are used in the early portion of the algorithm to ensure that unpaired images from many modalities are grouped and correlated.

Optimizing low-rank constraints directly is challenging, hence an approximation variation approach is introduced. For a short training set, the second component uses a cross modal ranking among triplet domain specific images to maximize the margin of various identities and boost data. Additionally, the CDL parameters are iteratively updated using an alternate minimization method. Experimental findings reveal that CDL outperforms state-of-the-art heterogeneous face recognition algorithms on the tough CASIA NIR-VIS 2.0 database, IIIT-D Sketch database, CUHK Face Sketch (CUFS), and the CUHK Face Sketch FERET. Table 1 shows the comparative analysis of previous state of the art studies with the outcome of security attack detection for face spoofing in smart homes.

Table 1 Comparative analysis

Source	Dataset	Techniques	Accuracy
[36]	IoT based dataset stored on Cloud	Deep Learning	89.5%
[37]	IoT based dataset stored on Cloud	CNN	88.78%
[38]	Face recognition dataset	LSTM-CNN	90.85%
[15]	Physiological dataset	CNN3D	91.26%
[14]	Face recognition dataset	Inception	92.05%
[13]	Physiological dataset	CNN	85.5%
[33]	Face recognition dataset	Xception	83.4%
[10]	Physiological dataset	CNN	86.5%
[34]	IoT based dataset stored on Cloud	CNN-LSTM	91.5%

3. Methodology

In this research, we are using IoT based face recognition system for smart homes, gathering data from Raspberry Pi based vision system. Fig. 3 shows the flowchart of current study. In the first step we will capture the image from Raspberry Pi based vision system. This image will be sent to cloud storage for matching. In the next step we will compare the face with the smart home individuals; deep learning based novel architecture will extract features from face and compare it with database. If the face matches and recognized by trained algorithm, the smart gate will be unlocked otherwise it remains closed.

3.1. Dataset Description

The dataset has been collected from raspberry pi based camera module. Dataset contains only few

members which are directly correlated to the individuals of family members of a smart home. Dataset contains the following features:

Table 2 Dataset description

Feature	Description	Value	Variable Type
Images	Camera Captures Image	Image in Pixels RGB	Input
Ground Truth	Image captured with camera, matched with the local database	Recognized Image	Input
User ID	Integer number related to camera image	Any integer or random number	Input
Security Check	Matched 1 Unmatched 0	0 or 1	Output

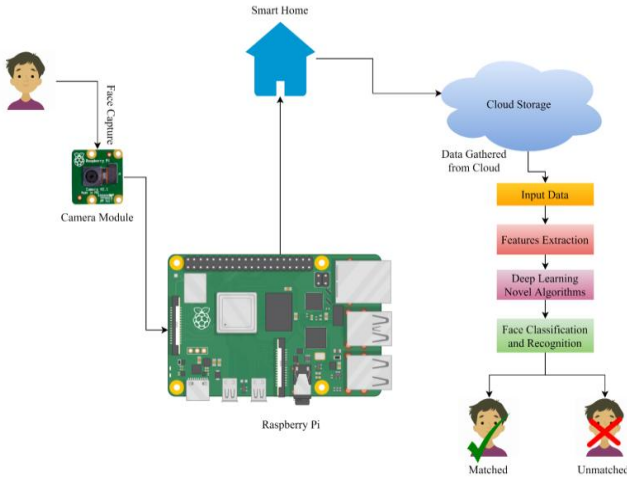


Fig. 3 Flowchart of the current study

3.2. Model Architecture

In this study, we are developing a model consists of CNN and merging it with SVM-Boosted algorithm. Reason behind merging these two algorithms is to make the architecture more suitable for classification. The input image taken from local database will be added to Convolutional Layer, features will be extracted at max pooling layer. Textures of each face will be identified and matched with the ground truth, and then the values will be extracted to CSV file to make the system more robust. When we extract the CSV file, containing features (see Table 2), we apply SVM-Boosted algorithm to classify the correct face. Fig. 4 shows the architectural diagram of proposed CNN-SVM Boosted Face Recognition algorithm. Mathematically, the proposed architecture has been proved in following equations:

$$G(m, n) = (f * h)[m, n] = \sum_j \sum_k h[j, k] f[m - j, n - k] \dots$$

(1) While kernel convolution is an integral part of CNNs, it is also employed in a wide variety of other computer vision algorithms. On achieve this effect, we apply a small numeric matrix (the kernel or filter) to our image and then evaluate the resulting transformation. When we have an input image (denoted

f) and a kernel (denoted h), we can use this information to determine the values of the feature maps. M and N denote the row and column indexes of the final matrix.

This model has been developed by ensembling the Support Vector Classifier model into XGBoost Classifier to improve both models' accuracy. Mathematical model of SVM-XGBC Classification model is as follows:

$$y = y^i = y^i + G(m, n) * \frac{\partial \sum (y_i - y_i^p)^2}{\partial y_i^p} \dots \quad (a)$$

Then we will calculate the support vectors to classify FDI attacks in dataset as:

$$w \cdot y + b = 1 \dots (\text{Vector 1})$$

$$w \cdot y + b = -1 \dots (\text{Vector 2})$$

Here P is the probability function of Support Vector Classifier and y^i is the output of XGBC classification model. Expression $\frac{\partial \sum (y_i - y_i^p)^2}{\partial y_i^p}$ shows the sum of residual in trees, α is the learning rate of XGBC. When XGBC takes the output of y, it will be sent to probability function of Support Vector Classifier for classification.

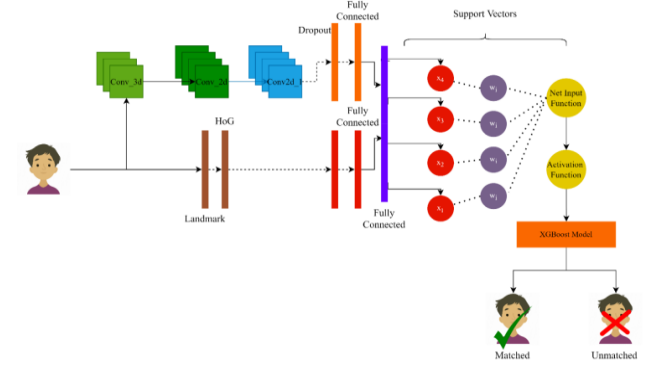


Fig. 4 Proposed model architecture

3.2.1. Texture Classification

Distinguishing between different textures is a long-standing issue in pattern recognition known as "Texture Classification." The main problem here is to generate useful features to extract from a given textured image since many extremely complex classifiers exist. We can perceive optical texture by looking at it, but only tactile texture can be felt by putting our hands on it. Optical or visual texture is a term used to describe the image's form and content.

3.2.2. Feature Engineering

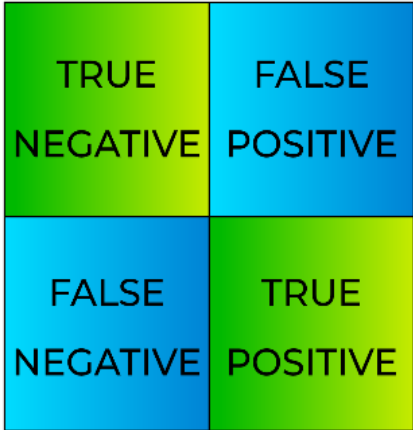
These are functions that can be employed by learning machines by analyzing data from a certain domain. Raw data must be transformed into machine-learning representations and such a transformation must be done manually. This study uses a correlation matrix to determine the degree of correlation between the various variables. Correlation matrices are just covariance matrices. The correlation is a summary metric for measuring the linear strength of association. The frequency and direction of a straight-line connection between two quantitative variables are

summarized by the concept of correlation. This correlation accepts values ranging from -1 to +1; these values are represented by r.

3.2.3. Performance Evaluation

F1 Score and accuracy measures have been used to evaluate the system's accuracy. While the confusion matrix has indicated that the classified and misclassified clauses have been classified and misclassified. The metrics utilized in this investigation are shown in the Table 3.

Table 3 Description of metrics

Metric	Description
Accuracy	$\text{Accuracy} = \frac{\text{TP}}{(\text{TP} + \text{TN}) * 100}$ <p>True-Positive (TP): the feature result is 1 and sample is present in this data file. True-Negative (TN): the feature result is 0 and sample is absent in data file.</p>
Confusion Matrix	

4. Results and Discussions







For a range of classification problems, the deep neural network is one of the most promising new machine learning techniques. It has been shown that CNNs outperform its convolutional counterparts on a number of image categorization problems. In this branch of machine learning, deep learning techniques can be used to develop an end-to-end model to categorize medical images from their raw pixels. In this research we have proposed two new modified models of CNN to predict the correct face for home security.

Correct face is determined by analyzing texture of image and matched with ground truth. Table 4 shows the correctly identified face as labeled in dataset as 0 or 1.

Table 4 Face recognition

Face	Ground truth	Label
		Matched Security lock Opened

Continuation of Table 4

		Matched Security lock Opened
		Matched Security lock Opened
		Miss Matched Security lock not Opened

4.1. Hybrid Model Performance

In the Fig. 5 below, the model has been created by combining the CNN-SVM with the XGBoost Classifier to improve both models' accuracy simultaneously. When XGB receives the output of y, it will be forwarded to the probability function of SVM to determine whether a class has changed, whether it is from Class A (Matched Faces) or Class B (Unmatched faces). The hybrid Model Performance is depicted in Fig. 5.

Table 5 Statistical results from the model

Epoch	Loss	Accuracy	Validation Loss	Validation Accuracy
1	3.979	71.067	5.83166	71.454
2	3.523	72.333	3.89523	78.724
3	2.213	88.200	2.90186	87.078
19	0.09	99.4	0.133	90.586

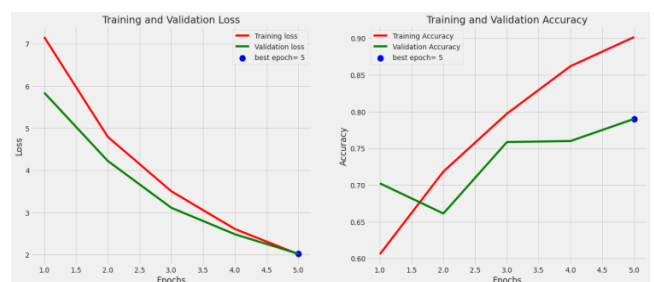


Fig. 5 Performance of the proposed model

Fig. 5 shows that the best epoch that model has gained so far, was 19 with 99.4% accuracy and 0.133 validation loss.

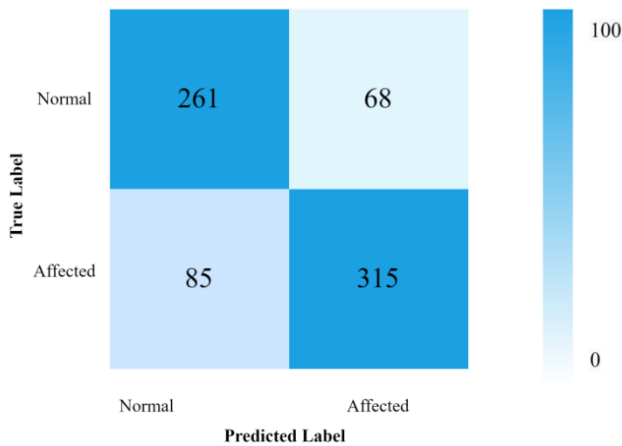


Fig. 6 Confusion matrix of the model

The confusion matrix of the model can be seen in Fig. 6. 315 true positive values show that the model performs well. It can be seen that 85 false positive values and 68 false negative values were the reason for the less accuracy which can be improved using optimization techniques.

5. Conclusion

Security has grown increasingly important to human life since the turn of the 21st century. In this moment, we are mostly concerned with financial factors. The use of this method results in lower monitoring costs. This study suggests a real-time recognition system for expediently handling photographic material. The primary purposes of this research were to develop a Deep Learning-based intelligent face recognition method for use in smart homes. In order to demonstrate the usefulness of this study, we also examine and contrast this model with other cutting-edge or state-of-the-art methodologies. Through proper identification, we anticipate increased security for our communities. In this study, we present a deep model based on trees that can be used for facial recognition in the cloud. The suggested deep model requires fewer computer resources to run yet maintains high accuracy. In the model's input volume, which has been partitioned into several volumes, trees are constructed for each individual volume. We have high hopes that by identifying people, we will be able to maintain the safety of our homes and offices. This research was conducted with the intention of developing, as one of its key goals, a method of intelligent face recognition for use in smart homes that was based on deep learning. In order to show that the findings of our research are applicable, we compare and contrast our model with other research approaches that are currently considered to be the most cutting-edge in the field. A tree-based deep model is proposed here for cloud-based facial recognition based on this research. The deep model that has been proposed requires less computing power but maintains the same level of accuracy. In the model's input volume, which has been partitioned into

several volumes, trees are constructed for each individual volume. The number of branches and the height of a tree are two characteristics that define it. Each branch is represented by a set of residual functions, each of which is constructed from a convolutional layer and two non-linear functions. Residual functions are employed. The suggested approach is validated across a selection of databases that are freely available to the public. In addition to this, it is compared to the most advanced deep models currently available in the market for facial recognition. The size and shape of a tree can be determined by its height and its number of branches. Residual functions, constructed from a convolutional layer and two non-linear functions are utilized to represent each individual branch. The proposed approach is tested in a number of public datasets. In addition, it is compared against state-of-the-art deep models for facial recognition. Current model of CNN-SVM-Boosted classifier performs well with 99.4% of correctly classifying the correct person from home.

6. Limitations and Further Study

Limitation of current study is that we have not implemented it on real-time. Further perspective of research is to make a real time model on real time dataset to improve security of smart homes.

Acknowledgment

This work is supported by the National Natural Science Foundation of China (No. 62166011) and the Innovation Key Project of Guangxi Province (No. 222068071), Guangxi Key Laboratory of Intelligent Processing of Computer Images and Graphics.

References

- [1] KHARE S., and TOTARO M. Ensemble Learning for Detecting Attacks and Anomalies in IoT Smart Home. In: *3rd International Conference on Data Intelligence and Security, South Padre Island, TX, USA, June 24-26, 2020*, 2020: 56-63. DOI: 10.1109/ICDIS50059.2020.00014.
- [2] SIVANATHAN A., GHARAKHEILI H.H., LOI F., RADFORD A., WIJENAYAKE C., VISHWANATH A., and SIVARAMAN V. Classifying IoT Devices in Smart Environments Using Network Traffic Characteristics. *IEEE Transactions on Mobile Computing*, 2019, 18(8): 1745-1759. DOI: 10.1109/TMC.2018.2866249.
- [3] RATHORE A.S., XU C., ZHU W., DAIYAN A., WANG K., LIN F., REN K., and XU W. Scanning the Voice of Your Fingerprint with Everyday Surfaces. *IEEE Transactions on Mobile Computing*, 2021, 1233(c): 1-18. DOI: 10.1109/TMC.2021.3049217.
- [4] AMERSHI S., BEGEL A., BIRD C., DELINE R., GALL H., KAMAR E., NAGAPPAN N., NUSHI B., and ZIMMERMANN T. Software Engineering for Machine Learning: A Case Study. In: *2019 41st International Conference on Software Engineering: Software Engineering in Practice*, 2019: 291-300. DOI: 10.1109/ICSE-SEIP.2019.00042.

- [5] LIN W., and HU S. Design and implementation of an offline face recognition locker. *Journal of Physics: Conference Series*, 2020, 1634(1): 1-66. DOI: 10.1088/1742-6596/1634/1/012131.
- [6] ELORDI U., BERTELSEN A., UNZUETA L., ARANJUELO N., GOENETXEA J., and ARGANDA-CARRERAS I. Optimal deployment of face recognition solutions in a heterogeneous IoT platform for secure elderly care applications. *Procedia Computer Science*, 2021, 192: 3204-3213. DOI: 10.1016/j.procs.2021.09.093.
- [7] OUANAN H., GAGA A., DIOURI O., OUANAN M., and AKSASSE B. Development of Deep Learning-Based Facial Recognition System. *Advances in Intelligent Systems and Computing*, 2020, 1106(February): 45-52. DOI: 10.1007/978-3-030-36677-3_6.
- [8] MASUD M., MUHAMMAD G., ALHUMYANI H., ALSHAMRANI S.S., CHEIKHROUHO O., IBRAHIM S., and HOSSAINE S. Deep learning-based intelligent face recognition in IoT-cloud environment. *Computer Communications*, 2020, 152(February): 215-222. DOI: 10.1016/j.comcom.2020.01.050.
- [9] WHITE D., DUNN J.D., SCHMID A.C., and KEMP R.I. Error rates in users of automatic face recognition software. *PLoS One*, 2015, 10(10): 1-14. DOI: 10.1371/journal.pone.0139827.
- [10] CHEN S., DING S., FU H., XIAN Y., LIU X., and ZHANG C. Deep Learning Applied to Smart Home Face Recognition Access Control System. In: *Proceedings of the 2018 2nd International Conference on Artificial Intelligence: Technologies and Applications*, 2018, 146: 13-15. DOI: 10.2991/icaia-18.2018.4.
- [11] DAESCU O., HUANG H., and WEINZIERL M. Deep learning based face recognition system with smart glasses. *ACM International Conference Proceeding Series*, 2019: 218-226. DOI: 10.1145/3316782.3316795.
- [12] LIU C.-Y., and CHEN Y.-J. The Design of Deep-Learning-Based Facial Recognition System for Smart Shopping Cart. [Online] Available from: file:///C:/Users/%D0%90%D0%B4%D0%BC%D0%B8%D0%BD/Downloads/4131_1042.pdf
- [13] HUSSAIN T., HUSSAIN D., HUSSAIN I., AL-SALMAN H., HUSSAIN S., ULLAH S.S., and AL-HADHRAMI S. Internet of Things with Deep Learning-Based Face Recognition Approach for Authentication in Control Medical Systems. *Computational and Mathematical Methods in Medicine*, 2022: Article ID 5137513. DOI: 10.1155/2022/5137513.
- [14] SYAFEEZA A.R., MOHD M.K., ALIF F., ATHIRAH Y.N., JAAFAR A.S., NORIHAN A.H., and SALEHA M.S. IoT based facial recognition door access control home security system using raspberry pi. *International Journal of Power Electronics and Drive Systems*, 2020, 11(1): 417-424. DOI: 10.11591/ijpeds.v11.i1.pp417-424.
- [15] OTHMAN N.A., and AYDIN I. A face recognition method in the Internet of Things for security applications in smart homes and cities. In: *6th International Istanbul Smart Grids and Cities Congress and Fair, 25-26 April, 2018, Istanbul*. 2018: 20-24. DOI: 10.1109/SGCF.2018.8408934.
- [16] FARAYOLA M., and DUREJA A. A Proposed Framework: Face Recognition With Deep Learning. *International Journal of Science and Technology Research*, 2020, 9(7).
- [17] AL-WAISY A.S., QAHWAI R., IPSON S., and AL-FAHDAWI S. A multimodal deep learning framework using local feature representations for face recognition. *Machine Vision and Applications*, 2018, 29: 35-54. DOI: 10.1007/s00138-017-0870-2.
- [18] GHAZI M.M., and EKENEL H.K. A Comprehensive Analysis of Deep Learning Based Representation for Face Recognition. In: *Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition*, 2016: 102-109. DOI: 10.1109/CVPRW.2016.20.
- [19] ABDELMINAAM D.S., ALMANSORI A.M., TAHA M., and BADR E. A deep facial recognition system using computational intelligent algorithms. *PLoS One*, 2020, 15(12): 1-27. DOI: 10.1371/journal.pone.0242269.
- [20] PEI Z., XU H., ZHANG Y., GUO M., and YEE-HONG Y. Face recognition via deep learning using data augmentation based on orthogonal experiments. *Electronics*, 2019, 8(10): 1-16. DOI: 10.3390/electronics8101088.
- [21] ALZU'BI A., ALBALAS F., AL-HADHRAMI T., YOUNIS L.B., and BASHAYREH A. Masked face recognition using deep learning: A review. *Electronics*, 2021, 10(21). DOI: 10.3390/electronics10212666.
- [22] CHIAOUI M., ELKEFI A., BELLIL W., and BEN AMAR C. A survey of 2D face recognition techniques. *Computers*, 2016, 5(4): 41-68. DOI: 10.3390/computers5040021.
- [23] QURESHI S. Face Recognition (Image Processing) based Door Lock using OpenCV, Python and Arduino. *International Journal for Research in Applied Science and Engineering Technology*, 2020, 8(6): 1208-1214. DOI: 10.22214/ijraset.2020.6197.
- [24] FANG Y., HU J., and DENG W. Identity-Aware CycleGAN for Face Photo-Sketch Synthesis and Recognition. *Pattern Recognition*, 2020, 102: 107249.
- [25] SABHARWAL H., and TAYAL A. Human Face Recognition. *International Journal of Computer Applications*, 2014, 104(11): 1-3. DOI: 10.5120/18243-9173.
- [26] UDDIN K.M.M., SHAHELA S.A., RAHMAN N., MOSTAFIZ R., and RAHMAN M.M. Smart Home Security Using Authentication and Mobile Application. *International Journal of Wireless and Microwave Technologies*, 2022, 12(2): 40-50. DOI: 10.5815/ijwmt.2022.02.04.
- [27] RAHIM A. An Intelligent Approach for Preserving the Privacy and Security of a Smart Home Based on IoT Using LogitBoost Techniques. *Journal of Human University Natural Sciences*, 2022, 49(4): 372-388, DOI: 10.55463/issn.1674-2974.49.4.39
- [28] REDDY K.T. Intelligent Door Lock System with Face Recognition. *International Journal for Research in Applied Science & Engineering Technology*, 2020, 8(5): 364-371. DOI: 10.22214/ijraset.2020.5060.
- [29] ZALEHA S., ITHNIN H.N., WAHAB N.H.A., and SUNAR N. Intelligent Locking System using Deep Learning for Autonomous Vehicle in Internet of Things. *International Journal of Advanced Computer Science and Applications*, 2021, 12(10): 565-578. DOI: 10.14569/IJACSA.2021.0121063.
- [30] AHMAD T., WU J., KHAN I., RAHIM A., and KHAN A. Human Action Recognition in Video Sequence using Logistic Regression by Features Fusion Approach based on CNN Features. *International Journal of Advanced Computer Science and Applications*, 2021, 12(11): 18-25. DOI.org/10.14569/IJACSA.2021.0121103
- [31] SUGANTHI S.T., UVAZE M., AYOUBKHAN A., KUMAR K.V., BACANIN N., VENKATACHALAM K., HUBÁLOVSKÝ Š., and TROJOVSKÝ P. Deep learning

model for deep fake face recognition and detection. *PeerJ Computer Science*, 2022, 8: 1-20. DOI: 10.7717/PEERJ-CS.881.

[32] AKSHAY H.A., SHARMA L., DEEP M., NUTHAN G.S., and ASHA P.N. Smart Home Security using Facial Recognition and Unusual Event Detection. *International Journal for Research in Applied Science & Engineering Technology*, 2020, 8(6): 1462-1468. DOI: 10.22214/ijraset.2020.6239.

[33] DHOBAL M.R., BIRADAR R.Y., PAWAR R.R., and AWATADE S.A. Smart Home Security System Using IoT, Face Recognition and Raspberry Pi. *International Journal of Computer Applications*, 2020, 176(13): 45-47. DOI: 10.5120/ijca2020920105.

[34] TEOH K.H., ISMAIL R.C., NAZIRI S.Z.M., HUSSIN R., ISA M.N.M., and BASIR M.S.S.M. Face Recognition and Identification using Deep Learning Approach. *Journal of Physics: Conference Series*, 2021, 1755(1). DOI: 10.1088/1742-6596/1755/1/012006.

[35] WU X., SONG L., HE R., and TAN T. Coupled deep learning for heterogeneous face recognition. In: *The Thirty-Second AAAI Conference on Artificial Intelligence*, 2018: 1679-1686.

[36] PRAVEEN K.V., PRATHAP P.M.J., DHANASEKARAN S., PUNITHAVATHI I.S.H., DURAI PANDY P., PUSTOKHINA I.V., and PUSTOKHIN D.A. Deep learning based intelligent and sustainable smart healthcare application in cloud-centric IoT. *Computers, Materials & Continua*, 2021, 66(2): 1987-2003. DOI: 10.32604/cmc.2020.012398.

[37] QUY V.K., VAN HAU N., VAN ANH D., and NGOC L.A. Smart healthcare IoT applications based on fog computing: architecture, applications and challenges. *Complex & Intelligent Systems*, 2022, 8: 3805-3815. DOI: 10.1007/s40747-021-00582-9.

[38] PANDIMURUGAN V., JAIN A., and SINHA Y. IoT based face recognition for smart applications using machine learning. In: *2020 3rd International Conference on Intelligent Sustainable Systems*, 2020: 1263-1266. DOI: 10.1109/ICISS49785.2020.9316089.

參考文:

[1] KHARE S. 和 TOTARO M. 用於檢測物聯網智能家居中的攻擊和異常的集成學習。在：第三屆數據智能與安全國際會議，美國德克薩斯州南帕德里島，2020年6月24-26日，2020：56-63。DOI：10.1109/ICDIS50059.2020.00014。

[2] SIVANATHAN A., GHARAKHEILI H.H., LOI F., RADFORD A., WIJENAYAKE C., VISHWANATH A. 和 SIVARAMAN V. 使用網絡流量特徵對智能環境中的物聯網設備進行分類。電氣和電子工程師協會移動計算彙刊，2019，18(8)：1745-1759。DOI：10.1109/TMC.2018.2866249。

[3] RATHORE A.S., XU C., ZHU W., DAIYAN A., WANG K., LIN F., REN K. 和 XU W. 用日常表面掃描指紋的聲音。電氣和電子工程師協會移動計算彙刊，2021年，1233(c)：1-18。DOI：10.1109/TMC.2021.3049217。

[4] AMERSHI S., BEGEL A., BIRD C., DELINE R.,

GALL H., KAMAR E., NAGAPPAN N., NUSHI B. 和 ZIMMERMANN T. 機器學習軟件工程：案例研究。在：2019年第41屆軟件工程國際會議：實踐中的軟件工程，2019：291-300。DOI：10.1109/ICSE-SEIP.2019.00042。

[5] LIN W. 和 HU S. 離線人臉識別儲物櫃的設計與實現。物理學雜誌：系列會議，2020年，1634(1)：1-66。DOI：10.1088/1742-6596/1634/1/012131。

[6] ELORDI U., BERTELSEN A., UNZUETA L., ARANJUELO N., GOENETXEA J. 和 ARGANDA-CARRERAS I. 人臉識別解決方案在異構物聯網平台中的最佳部署，用於安全的老年護理應用。程序員計算機科學，2021，192：3204-3213。DOI：10.1016/j.procs.2021.09.093。

[7] OUANAN H., GAGA A., DIOURI O., OUANAN M. 和 AKSASSE B. 基於深度學習的面部識別系統的開發。智能係統與計算進展，2020，1106(二月)：45-52。DOI：10.1007/978-3-030-36677-3_6。

[8] MASUD M., MUHAMMAD G., ALHUMYANI H., ALSHAMRANI S.S., CHEIKHROUHO O., IBRAHIM S. 和 HOSSAINE S. 物聯網雲環境中基於深度學習的智能人臉識別。計算機通信，2020，152(二月)：215-222。DOI：10.1016/j.comcom.2020.01.050。

[9] WHITE D., DUNN J.D., SCHMID A.C. 和 KEMP R.I. 自動人臉識別軟件用戶的錯誤率。公共科學圖書館一號，2015年，10(10)：1-14。DOI：10.1371/journal.pone.0139827。

[10] CHEN S., DING S., FU H., XIAN Y., LIU X. 和 ZHANG C. 深度學習應用於智能家居人臉識別訪問控制系統。見：2018年第二屆人工智能國際會議論文集：技術與應用，2018，146：13-15。DOI：10.2991/icaite-18.2018.4。

[11] DAESCU O., HUANG H. 和 WEINZIERL M. 基於深度學習的智能眼鏡人臉識別系統。美國計算機學會國際會議論文集，2019：218-226。DOI：10.1145/3316782.3316795。

[12] LIU C.-Y. 和 CHEN Y.-J. 基於深度學習的智能購物車人臉識別系統設計。[在線]可從：file:///C:/Users/%D0%90%D0%B4%D0%BC%D0%B8%D0%BD/Downloads/4131_1042.pdf

[13] HUSSAIN T., HUSSAIN D., HUSSAIN I., AL-SALMAN H., HUSSAIN S., ULLAH S.S. 和 AL-HADHRAMI S. 基於深度學習的物聯網人臉識別方法在控制醫療中的身份驗證系統。醫學計算和數學方法，2022：文章ID 5137513。DOI：10.1155/2022/5137513。

[14] SYAFEEZA A.R., MOHD M.K., ALIF F., ATHIRAH Y.N., JAAFAR A.S., NORIHAN A.H. 和 SALEHA M.S. 使用樹莓派的基於物聯網的面部識別門禁控制家庭安全系統。國際電力電子與驅動系統雜誌，2020，11(1)：417-424。DOI：10.11591/ijpeds.v11.i1.pp417-424。

[15] OTHMAN N.A. 和 AYDIN I. 物聯網中用於智能家居和城市安全應用的人臉識別方法。在：第六屆國際伊斯坦布爾智能電網和城市大會暨博覽會，2018年4月25日至26日，伊斯坦布爾。2018：20-24。DOI：

10.1109/SGCF.2018.8408934。

[16] FARAYOLA M. 和 DUREJA A. 提議的框架：深度學習的人臉識別。國際科學技術研究雜誌, 2020, 9(7).

[17] AL-WAISY A.S., QAHWAJI R., IPSON S. 和 AL-FAHDAWI S. 一種使用局部特徵表示進行人臉識別的多模式深度學習框架。機器視覺與應用, 2018, 29: 35-54. DOI : 10.1007/s00138-017-0870-2。

[18] GHAZI M.M. 和 EKENEL H.K. 基於深度學習的人臉識別表示綜合分析。在：電氣和電子工程師協會 計算機協會計算機視覺和模式識別會議論文集, 2016 年：102-109. DOI : 10.1109/CVPRW.2016.20。

[19] ABDELMINAAM D.S., ALMANSORI A.M., TAHA M. 和 BADR E. 使用計算智能算法的深度面部識別系統。公共科學圖書館一號, 2020 年, 15(12) : 1-27. DOI : 10.1371/journal.pone.0242269。

[20] PEI Z., XU H., ZHANG Y., GUO M. 和 YEE-HONG Y. 基於正交實驗使用數據增強通過深度學習進行人臉識別。電子學, 2019, 8(10): 1-16. DOI : 10.3390/electronics8101088。

[21] ALZU'BI A., ALBALAS F., AL-HADHRAMI T., YOUNIS L.B. 和 BASHAYREH A. 使用深度學習進行蒙面人臉識別：綜述。電子, 2021, 10(21). DOI : 10.3390/電子產品 10212666。

[22] CHHAOUI M., ELKEFI A., BELLIL W. 和 BEN AMAR C. 二維人臉識別技術調查。計算機, 2016, 5(4): 41-68. DOI : 10.3390/計算機 5040021。

[23] QURESHI S. 基於人臉識別（圖像處理）的門鎖，使用打開簡歷、Python 和阿杜諾。國際應用科學與工程技術研究雜誌, 2020, 8(6): 1208-1214. DOI : 10.22214/ijraset.2020.6197。

[24] FANG Y., HU J. 和 DENG W. 用於人臉素描合成和識別的身份識別循環一致性生成對抗網絡。模式識別, 2020, 102: 107249。

[25] SABHARWAL H. 和 TAYAL A. 人臉識別。國際計算機應用雜誌, 2014, 104(11): 1-3. DOI : 10.5120/18243-9173。

[26] UDDIN K.M.M., SHAHELA S.A., RAHMAN N., MOSTAFIZ R. 和 RAHMAN M.M. 使用身份驗證和移動應用程序智能家居安全。國際無線與微波技術雜誌, 2022, 12 (2): 40-50. DOI : 10.5815/ijwmt.2022.02.04。

[27] RAHIM A. 一種使用邏輯提升技術保護基於物聯網的智能家居隱私和安全的智能方法。湖南大學自然科學學報, 2022, 49(4): 372-388, DOI: 10.55463/issn.1674-2974.49.4.39

[28] REDDY K.T.人臉識別智能門鎖系統。國際應用科學與工程技術研究雜誌, 2020, 8(5): 364-371. DOI :

10.22214/ijraset.2020.5060。

[29] ZALEHA S., ITHNIN H.N., WAHAB N.H.A. 和 SUNAR N. 物聯網中使用深度學習的自動駕駛汽車智能鎖定系統。國際高級計算機科學與應用雜誌, 2021, 12(10): 565-578. DOI : 10.14569/IJACSA.2021.0121063。

[30] AHMAD T., WU J., KHAN I., RAHIM A. 和 KHAN A. 使用基於美國有線電視新聞網特徵的特徵融合方法進行邏輯回歸的視頻序列中的人類行為識別。國際高級計算機科學與應用雜誌, 2021, 12(11): 18-25. DOI.org/10.14569/IJACSA.2021.0121103

[31] SUGANTHI S.T., UVAZE M., AYOOBKHAN A., KUMAR K.V., BACANIN N., VENKATACHALAM K., HUBÁLOVSKÝ Š. 和 TROJOVSKÝ P. 用於深度人臉識別和檢測的深度學習模型。同行 J 計算機科學, 2022, 8 : 1-20. DOI : 10.7717/PEERJ-CS.881。

[32] AKSHAY H.A., SHARMA L., DEEP M., NUTHAN G.S. 和 ASHA P.N. 使用面部識別和異常事件檢測的智能家居安全。國際應用科學與工程技術研究雜誌, 2020, 8(6): 1462-1468. DOI : 10.22214/ijraset.2020.6239。

[33] DHOBAL M.R., BIRADAR R.Y., PAWAR R.R. 和 AWATADE S.A. 使用物聯網、人臉識別和樹莓派的智能家居安全系統。國際計算機應用雜誌, 2020, 176(13): 45-47. DOI : 10.5120/ijca2020920105。

[34] TEOH K.H., ISMAIL R.C., NAZIRI S.Z.M., HUSSIN R., ISA M.N.M. 和 BASIR M.S.S.M. 使用深度學習方法進行人臉識別和識別。物理學雜誌：系列會議, 2021 年, 1755(1) 。 DOI : 10.1088/1742-6596/1755/1/012006。

[35] WU X., SONG L., HER R. 和 TAN T. 用於異構人臉識別的耦合深度學習。在：第三十屆人工智能會議, 2018 : 1679-1686。

[36] PRAVEEN K.V., PRATHAP P.M.J., DHANASEKARAN S., PUNITHAVATHI I.S.H., DURAI PANDY P., PUSTOKHINA I.V. 和 PUSTOKHIN D.A. 以雲為中心的物聯網中基於深度學習的智能和可持續智能醫療保健應用。計算機、材料和康體佳, 2021, 66(2) : 1987-2003. DOI : 10.32604/cmc.2020.012398。

[37] QUY V.K., VAN HAU N., VAN ANH D. 和 NGOC L.A. 基於霧計算的智能醫療物聯網應用：架構、應用和挑戰。複雜與智能系統, 2022 年, 8 : 3805-3815. DOI : 10.1007/s40747-021-00582-9。

[38] PANDIMURUGAN V., JAIN A. 和 SINHA Y. 基於物聯網的人臉識別，用於使用機器學習的智能應用。在：2020 年第三屆智能可持續系統國際會議, 2020 : 1263-1266. DOI : 10.1109/ICISS49785.2020.9316089。