iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** IV **Month of publication:** April 2023

DOI: https://doi.org/10.22214/ijraset.2023.50243

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue IV Apr 2023- Available at www.ijraset.com

Enhancing Smart Home Security with Face Recognition using Deep Learning

Asif Rahim[1], Yanru Zhong[2], Tariq Ahmad[3]
[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, PR China*
[3]*School of Information and Communication Engineering, Guilin University of Electronic Technology, Guilin, China*

Abstract: ***Recently, security has been a growing concern for human life, and the cost is a significant concern. The research recommends implementing a real-time recognition system to rapidly handle photographs to reduce monitoring expenses and ensure safety in homes and offices by identifying people. The main goal of this study was to create an intelligent face recognition approach using deep learning for intelligent homes. To illustrate the study's effectiveness, the suggested model is contrasted with other cutting-edge techniques. The research introduces a tree-based deep model for facial recognition in the Cloud, which requires fewer computing resources but maintains accuracy. The input volume of the model is partitioned into multiple volumes, and trees are created for each volume according to their height and number of branches. A residual function, constructed from a convolutional layer and two non-linear functions, represents each branch. The proposed model is assessed on various publicly accessible databases and compared with the industry's best deep models for facial recognition.***

Keywords: Smart Home, Face recognition, Convolution Neural Network (CNN), Support Vector Machine (SVM)), Deep Learning

I. INTRODUCTION

Information and communication technology development has produced multiple innovative systems that employ different machine-learning algorithms. The IoT offers a perfect foundation for executing innovative tasks and putting forward inventive concepts in the quickly developing realm of innovation.

The suggested method for this project is typically known as an asset intelligence system, as it presents a secure and improved solution to users.

The IoT comprises many interconnected devices that can create various innovative and practical systems, such as smart cities, smart homes, and facial recognition systems. In 2021, the home automation team carried out research to collect data on intelligent homes, attendance systems, and IoT solutions for intelligent environments. The survey outcomes revealed that respondents had apprehensions about the benefits, drawbacks, prospects, and dangers of potential IoT technologies. These concerns prompted the selection of this subject for the project.

In today's environment, the risk of unfortunate events occurring to homes and their contents is significantly increased if they are not adequately protected.

To simplify, streamline, and eliminate errors in the supply of intelligent home systems, one option is to utilize the fast-evolving technology of the Internet of Things (IoT) in conjunction with face recognition. The IoT is a renowned technology in various fields, such as intelligent homes and urban areas, education, health care, transportation, autonomous, connected vehicles, agriculture, and smart shopping.

However, businesses need help to implement the IoT concept due to concerns over security, privacy, cost, and regulatory issues. Despite this, a poll showed that over half of those surveyed believe that integrating the IoT idea can considerably influence their organization, and 79 percent reported achieving positive results in areas of work that were impossible without the IoT concept.

In order to ensure security and detect potential security breaches, as stated in [2], it is crucial to classify IoT devices. An illustration of an intelligent smart home equipped with several IoT-connected resources is presented in Figure 1. By connecting devices and appliances in a home through the internet, users can oversee and control them from a distance. The popularity of innovative home solutions has recently increased [3].

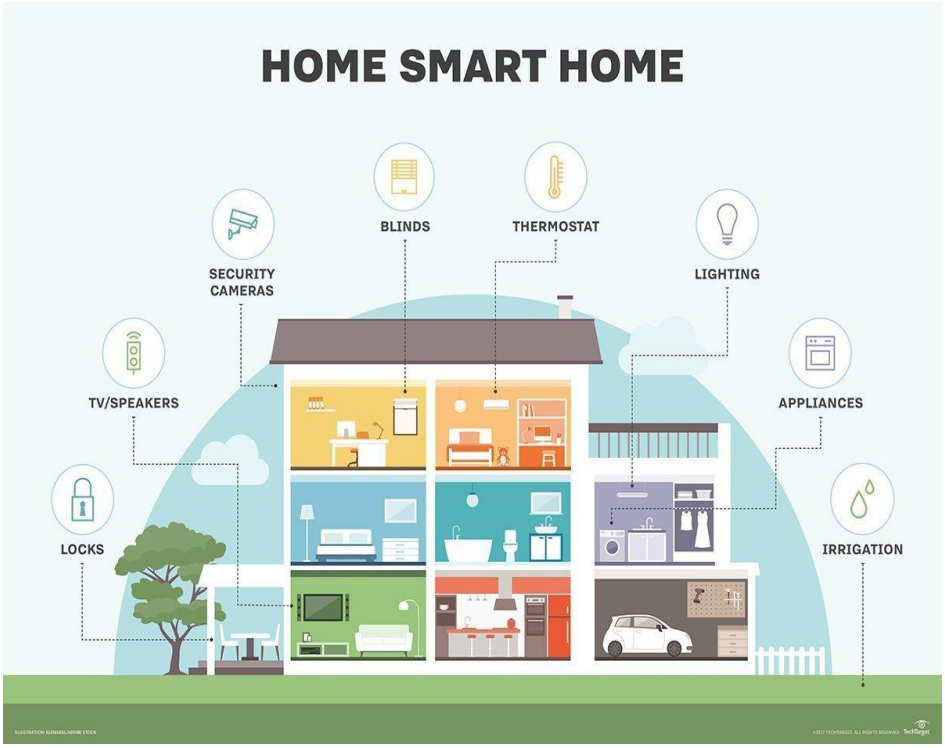


Fig.1 Intelligent Home with various IoT gadgets linked

Various gadgets, such as mobile phones and home automation systems, can be controlled using personal computers, computing devices, wearables, and virtual assistants. These systems offer various advantages, such as the benefits of innovative home solutions include enhanced security through surveillance cameras and automatic door locks, heightened awareness, increased comfort, time efficiency, energy management, and reduced costs. As shown in Figure 2, the delivery of home automation components based on IoT has significantly surged in recent years.

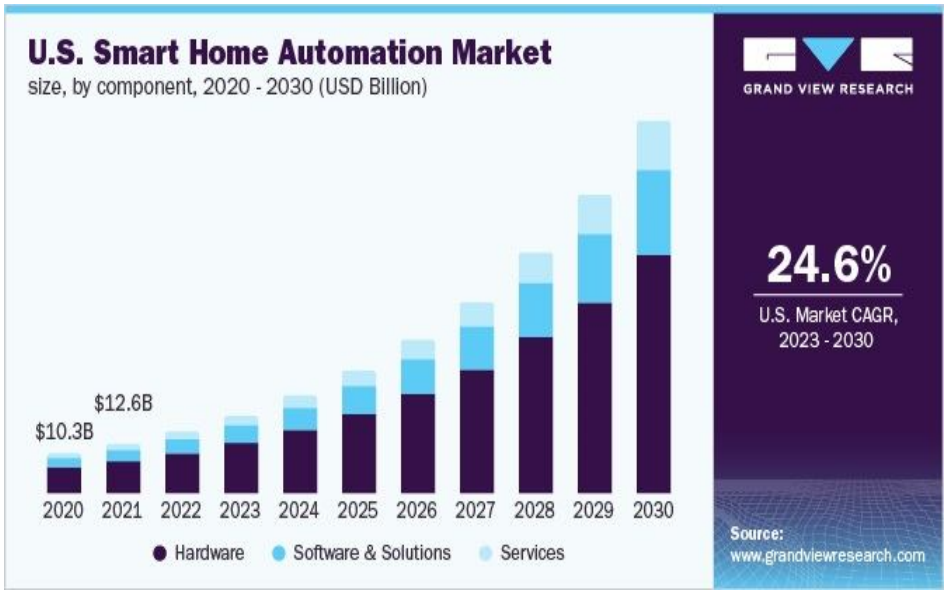


Fig.2 Sales of the IoT-based Intelligent home automation industry.

Facial recognition can benefit greatly from machine learning, a subdivision of artificial intelligence. This assistance can lead to developing new fields or enhancing the efficiency of existing ones. Humans find it difficult to recall faces, but computers can easily store many images in facial databases.

Facial recognition is a cutting-edge technology that utilizes the fundamental of artificial intelligence to address the previously mentioned concerns. It is applied in different settings, such as airport monitoring, personal security, and security measure applications. The primary objectives of this research are:

This study aims to suggest a deep learning-based innovative facial authentication method for smart homes and to assess and contrast this model with other advanced methods to showcase its efficacy. The paper is structured into five sections:

1) The first section presents an introduction to the research.
2) The 2nd section discusses related studies.
3) The 3rd section discusses this study's methodology and innovative framework.
4) The 4th section outlines the findings of the research and compares them to those of prior research
5) Ultimately, the 5th and final section summarizes the paper and elaborates on the outcomes.

II. LITERATURE REVIEW

Salim et al. [4] investigated the topic of facial authentication. The study employed DCT/DL and Deep Learning methodologies. The research resulted in the development of a system that can recognize and classify human faces with 100% accuracy while removing skewed or watermarked images from the database. However, the CNN and deep learning algorithms could not recognize images with watermarks. The system uses Convolutional Neural Networks to detect human faces and draw a yellow box around them. The system has certain restrictions, such as the face cannot be tilted or rotated beyond an angle of 5 to 10 degrees, hidden by objects, or computer-generated. The system can distinguish human and non-human faces and has an 85% resolution rate. The authors reduced their work time by half using this system. The study's methodology and results are discussed in detail in [4].

This dissertation aims to create a facial recognition model based on artificial intelligence, utilizing Deep Learning algorithms, that runs within a Docker container on an Internet of Things (IoT) platform. The model will determine whether to lock or unlock the door system. This research will leverage edge computing and AI by employing a low-power IoT device and containerization paradigm. The containerization process is comparable to virtualization, and low-power IoT devices, such as the Firefly rk-3399, can quickly run Docker. The author's research centers on developing AI models that are containerized with inspiration from Lin et al.'s [5] use of The author's research involves using CSI connector to link the camera and train the AI model to recognize faces through Deep Learning techniques. The system first identifies faces and then converts the image into a set of gradients. The next step involves training the system to recognize authorized users using a Support Vector Machine (SVM) classifier. The authors have created a method for constructing an AI model in a container and deploying it on a Raspberry Pi, an IoT device. Containerized programs are adaptable, versatile, and can operate across multiple platforms, and the containerized program is compatible with various architectures, including ARM, x86, and amd64.

Integrating face recognition technology with IoT platforms in senior care can improve authentication and monitoring. Nevertheless, some challenges must be addressed to ensure the effectiveness and efficiency of such integration; storing biometric data securely and managing the wide range of interface devices are challenges in integrating face recognition technology into Internet of Things platforms for senior care. Elordi et al. [6] have used lightweight deep neural networks to enable secure recognition and interaction guidance. The edge device's characteristics are considered to automatically select inference engines, model configurations, and batch sizes. Homomorphic encryption is employed to protect biometric data privacy. Its potential can be realized by comparing it with the latest available alternatives.

Ouanan et al. [7] aimed to develop a deep learning-based facial recognition system that is being developed which can operate effectively in unconstrained environments, where variables such as lighting, image quality, and background interference cannot be regulated. The researchers utilized Keras, an open-source platform for deep learning, to develop a Convolutional Neural Network (CNN) model based on the VGG16 architecture. The study's performance was assessed using the Labeled Faces in Wild benchmark dataset, and the results indicate that the proposed approach performs better than existing techniques. Nevertheless, face recognition in unconstrained settings still requires significant advancements.

IoT devices are becoming increasingly common in various industries, generating vast amounts of data. The healthcare industry is one area where IoT devices are widely used, generating large volumes of data. The implementation of face recognition technology can play a significant role in protecting healthcare facilities, detecting fraudulent activities related to patients, and monitoring the flow of traffic in hospitals. However, in uncontrolled situations, the accuracy of face identification algorithms can be reduced, and real-time systems are often necessary for various applications, such as intelligent health technologies. Masud et al. [8] suggested a deep learning model based on trees for facial recognition that can be implemented on cloud-based systems.

That achieved 100% accuracy. This model divides an input volume into several volumes, each with a unique tree. The model creates multiple trees based on each volume's branching pattern and height. The proposed approach was tested on publicly available databases and compared to other deep models for facial recognition. The experiment outcomes indicated that the model proposed by the researchers attained an accuracy rate of 98.65%, 99.19%, and 95.84% on the FEI, ORL, and LFW databases.

Face recognition systems have been improved by recent algorithmic advancements, despite the evaluations mentioned above not considering human operators' impact. As a result, the performance of facial recognition systems in real-world settings can differ from evaluation tests. White and colleagues [9] utilized facial recognition technology to address this issue and detect fraudulent passport application identities. The researchers conducted Experiment 1 to test the "candidate lists" generated by the algorithm using passport images from an extensive database. They found that participants' accuracy was significantly lower when matching adult target photographs than children's. Experiment 2, conducted by the researchers, involved comparing the efficiency of trained passport officers who regularly use the system in their jobs to that of student volunteers. The expert "facial examiners" outperformed the others by 20%. The study aimed to evaluate the accuracy of the algorithm-generated "candidate lists" using passport images from an extensive database. Despite the limitations of human error, facial recognition systems can be improved by human operators with appropriate training and mentorship.

Recent technological advancements in embedded systems and technological advancements, particularly the Internet of Things (IoT), have contributed to the increasing popularity of smart homes. The use of deep learning has also resulted in many innovative discoveries. Chen et al. [10] employ a deep learning approach, specifically a convolution neural network model, in facial identification in natural settings. This method involves gathering and analyzing image-based with embedded devices before sending them to the server. Utilizing a lower complexity VGG network model has enhanced face recognition matches' performance on the server, leading to improved efficiency. This intelligent home system can use embedded devices by decreasing their computational demands and improving their recognition accuracy. The technique has successfully tested face recognition in surveillance video in various scenarios. Enhancing face recognition can improve the user's practical skills and protection in an innovative home system.

Daescu et al. [11] The goal is to create a facial recognition technology that can aid people with prosopagnosia in recognizing individuals and provide personal information through intelligent glasses in the future. The authors have created a facial recognition system that employs a client-server architecture, distinguishing it from prior systems that were run locally on glasses or mobile devices. The authors designed and created programs for intelligent glasses and smartphones to take pictures of faces and connect to the server for facial recognition. The Deep Convolutional Neural Networks (CNNs) used in the back-end system of the facial recognition system achieved an accuracy of 98.18 percent. This system can adapt to recent identities and changes in appearance without needing to recreate the entire model.

Today's world is constantly advancing with science and technology, making it challenging to keep up. Biometric identification technology is becoming more prevalent as mobile devices continue to proliferate, and it is both more secure and convenient than traditional authentication methods. The integration of artificial intelligence and the Internet of Things has notably impacted several fields, including transportation, commerce, and food, particularly in cities. The article by Liu et al. [12] aims to develop a facial recognition system using deep learning and apply it to intelligent supermarket shopping carts. Traditional shopping carts are equipped with tablet computers that customers can use to log in using face identification technology can enhance security and convenience in the process. The image of the user's face is pre-processed-processed to extract significant features. A matching network learning method is used for facial recognition when there are not enough user samples.

DL is becoming increasingly important in IoT, medical, and healthcare industries for better touchless authentication, particularly concerning infectious diseases like COVID-19. Hussain et al. [13] created a system that intelligently controls smart locks and doors using Raspberry Pi's GPIO pins. An SVM classifier may also be used. If authentication fails, the system sends an email containing facial images and time information from the SQL database to the designated location. This method achieved a high accuracy rate of 99.56%. Home security systems have become essential for households today. However, traditional access control methods, like keys or passwords, have weaknesses that can lead to severe issues like theft or identity theft. Syafeeza et al. [14] utilized Raspberry Pi, a compact and customizable computer board, to manage face identification, protection, and lock systems. A camera captures images of individuals standing in front of the door, and the Internet of Things (IoT) system permits users to regulate access to the door.

Nowadays, security has become an essential aspect of human life. However, the cost of implementing security measures should be lowered. In this regard, Othman et al. [15] suggested a system for image recognition that can quickly process images. The primary objective of their study is to identify individuals to ensure safety in their homes and workplaces. The proposed system utilizes a PIR sensor to identify motion in a designated area.

Then the Raspberry Pi captures images of the detected motion, which are scanned for faces and recognized by the system. The last step involves sending photos and notifications to a smartphone based on the IoT system using Telegram. This technology is characterized by low computational cost, real-time processing, and high speed.

Facial recognition involves recognizing a specific individual from a crowd, whether solitary or in a massive group. Farayola et al.'s [16] research has contributed significantly to developing a proposed Convolutional Neural Network (CNN) for face recognition, which can accurately identify 97 percent of faces captured in videos or images using a pre-trained VGG Face model. Applying metric learning on datasets to extract unique features is an essential preliminary measure.

Current systems for facial identification use an amalgamation of deep learning techniques (DBNs) and local binary patterns (LBP). However, both approaches have challenges when dealing with many face photographs and regional facial features. To address this, a new approach called the Curvelet–Fractal is proposed, which combines the Curvelet and Fractal dimensions to extract the local multimodal features of a face. Waisy et al. [17] The results demonstrate that the proposed MDFR representations work well with the Curvelet-Fractal technique. The authors have evaluated the proposed methods on four large-scale face datasets and compared them with existing approaches like LBP, DBN, and WPCA. The results show that the proposed methods outperform these existing approaches and produce better results.

The research by Ghazi et al. [18] focuses on evaluating the effects of misalignment caused by inaccurate localization of facial features. They use VGG-Face and Lightened CNN deep learning models to retrieve facial characteristics. Even though deep learning is a potent tool for face recognition, it can still be improved by pre-processing-processing techniques like normalizing illumination and positioning, notably if the training dataset lacks variations.

Researchers are focusing on enhancing the reliability of face identification technology for real-time use in intelligent urban areas as biometric technologies are increasingly being integrated into such cities. AbdELminaam et al.'s [19] study utilize transfer learning in fog and cloud computing to create a robust face identification system. The system utilizes deep convolutional neural networks (DCNN) to retrieve facial characteristics for comparing different faces despite conclusions, expressions, lighting, and positions affecting FR performance. The proposed method is evaluated using three machine learning techniques and three face image datasets, with accuracy, precision, sensitivity, and specificity performance metrics.

Facial recognition systems that use deep learning techniques have demonstrated impressive performance when trained on a vast quantity of annotated data. Data augmentation is used to expand the number of samples in small-sample learning to improve accuracy. Pei et al.'s [20] study employs geometric alterations, modifications in image brightness, and different filter techniques to address this problem. By performing orthogonal tests, the researchers conducted experiments to identify the best data augmentation method. Moreover, the accuracy increases to 98.1% as more data is acquired, reaching a high of 98.1%. The authors tested their attendance method in an actual classroom environment.

The emergence of new threats like widespread scams has resulted in a significant rise in the creation and dissemination of pertinent algorithms. Alzu’bi et al.'s [21] the study employs deep learning techniques to gather and analyze the most recent MFR research, presenting valuable insights and thorough discussions on the development process of MFR systems. This comprehensive research investigates various current methods and accomplishments in MFR, intending to provide a worldwide view of the topic.

Face identification has become a significant area of interest in computer vision and image analysis, mainly due to its diverse applications across different industries. The study by Chihaoui et al. [22] The article provides a summary of the most in-demand face identification techniques in each category, along with their advantages and disadvantages. The study also includes information about the benefits and challenges of facial recognition technology, its applications, and the limitations of existing systems. Additionally, the paper discusses the face recognition technique, aiming to provide an up-to-date overview of the current status of this technology.

We live in a technological age where the Internet of Things (IoT) is becoming integral to our daily lives. Face recognition, using picture analysis and computer vision algorithms, provides numerous possibilities for this technology. Security is a fundamental human right supported by many studies and investigations worldwide. There have been various developments in IoT-based home security, and Qureshi et al. [23] are working on a project focusing on facial recognition. This process involves capturing images of a person's face, comparing them to a database image, and opening the gate if there is a match. A notification will be triggered if there is no match when a facial recognition algorithm, developed based on the OpenCV library, identifies a face.

Facial recognition has become a crucial aspect of security, with the ability to accurately identify a person's identity, expressions, and emotions through their face.

Histogram-based facial recognition is a method used by [24] to improve the accuracy of facial recognition systems. In this method, the face is partitioned into various regions, and histogram values are retrieved for each region. These histogram values are then merged into a single vector. This vector compares facial photographs and identifies the most efficient result.

Convolutional Neural Networks (CNNs) have shown great success in FR due to their ability to perform processing, including selection, highlight extraction, and instruction, using all input images and their pixel values. Before applying CNNs in real-time systems, several pre-processing-processing operations must be completed. Although Convolutional neural networks (CNNs) have demonstrated favorable outcomes in facial recognition, the effectiveness of CNNs in face recognition has been established. However, there is still a need to develop alternative structures that enhance their performance and better understand the reasons behind their success. Recent studies have focused on improving the details of CNN model design, as noted by Sabharwal et al. [25].

A need for accessing electronic devices remotely at any time and place has resulted in the utilization of networks and internet connections, even though it poses significant security risks. In order to address this issue, Mohammad et al. [26] utilized the Internet of Things (IoT) and Artificial Intelligence (AI) to create a protection system for home automation. This system can be controlled and accessed remotely using an Android application. The system utilizes face recognition technology for efficient door entrance control, and security PINs can be set up as a backup. The authors plan to use multiple security modes to create an affordable, user-friendly solution for consumers. The algorithm successfully retrieved faces in actual scenarios with an accuracy rate of 92.86% using Haar Cascade and LBPH. While home automation systems can be expensive, the authors hope their solution will make it accessible to more users.

Many existing security solutions can be expensive and unaffordable for many people. Reddy et al.'s [27] study aim to introduce OpenCV2, LBPH, and SMTP to users and focus on local implementation in homes, colleges, and workplaces. It employs existing facial identification technology, where the camera captures photograph and compares it to database photos. If there is a match, the door will open, and the user will be allowed access. If there is no match, Once the system detects a face, it will send the captured image to the user's email address for verification. The system will pause until it receives a response from the owner before granting or denying access. The primary goal of this endeavor is to produce an inexpensive facial identification system that operates in the physical world.

We now have advanced programs for blocking systems that can secure and unsecured our vehicles. We can use keyless entry remote controls to unlock our cars or unlock them from the outside. Although these techniques are user-friendly, they can be difficult if someone carries multiple items or misplaced keys. In the next generation of autonomous vehicles, facial recognition will be crucial to future intelligent vehicle applications. Zaleha et al. [28] propose a locking mechanism for autonomous vehicles using deep learning and facial identification technology. This study uses a photo dataset with a training, validation, and test folder. The authors devised two directories to evaluate two different methods of detecting faces. Finally, a test was conducted after training the dataset, which produced positive results. The models could predict the outcome accurately and produce remarkable results. The data collection involved capturing images of the front, right (30-45 degrees), and left side (30-45 degrees) angles.

Deep learning is a versatile technology that can be applied in various domains, such as natural language analysis, image analysis, and machine learning [29]. One of the most significant issues arising from deep learning is the emergence of deep fakes, which are computer-generated images that can be indistinguishable from natural images. These deep fakes can pose a risk to public safety, and many studies have been conducted to detect them. However, current methods need shorter processing times and higher accuracy. Suganthi et al. [30] proposed a deep fake detection method using the Local Binary Pattern Histogram of Fischerface's Local Binary Pattern (FF-LBPH). The proposed method combines the DBN and RBM techniques to create a deep fake detection classifier. The study used several publicly available datasets, including FFHQ, 100K-Faces DFFD, and CASIA-WebFace.

In-home security, the Internet of Things (IoT), significantly ensures our safety. One concern is the security of our door locks, as they may only sometimes provide the required level of safety. Facial recognition is a well-known technique that can be used to recognize and identify individuals from an image. In their proof of concept for a bright door, Akshay et al. [31], the system will utilize a high-resolution camera positioned towards the front door, connected to show the individual's identity who is standing in front of the door. Additionally, the ARM processor of Raspberry Pi will be utilized to handle text inputs and showcase outcomes on display to detect various facial expressions, and the Local Binary Pattern Histogram (LBPH) will be used.

Home security is significant in the current era, and conventional security measures may only sometimes be adequate to deter thefts. To address this issue, Manoj et al. [32] the authors suggest a method for creating an intelligent home-protecting system using face identification technology utilizing an IoT platform. The system involves a Raspberry Pi with an attached PIR, other sensors, and a camera. When the camera takes a picture of an individual at the front door, the system uses a local binary pattern (LBP) to match the person's image with those of recognized family members or other individuals.

If a match is found, the door unlocks, and if not, The system will send an email to the owner's gmail account with an image of the robber when detected by the camera. This method alerts the owner whenever an unknown individual approaches the front door, helping enhance home security.

The human face is the unique feature of an individual, which can be used for identification purposes through facial recognition systems. This technology is currently used in various applications, such as unlocking smartphones and detecting intruders—facial recognition is solely based on the facial image of an individual, making it a more secure option. Face detection and identification are the two primary components of the human identification system, which can be developed using deep learning techniques in Python using OpenCV. Teoh and his colleagues [33] have discussed constructing a facial recognition system using deep learning, which is highly accurate in experimental settings.

The main issue in face recognition is the difficulty of matching faces in multiple modalities due to the need for paired images and a significant domain difference. Wu et al. [34] proposed a deep learning approach called CDL for face matching to create a shared feature space approximating a homogeneous face-matching problem. The CDL objective function has two components, where the first component uses a trace norm and a block-diagonal prior to the group and correlates unpaired images from various modalities. As optimizing low-rank constraints is challenging, an approximation variation approach is introduced. The CDL parameters are updated iteratively using an alternate minimization method. Blow table presents a comparison of the past study.

TABLE I
COMPARATIVE ANALYSIS

Reference	Dataset	Outcome	Techniques	Accuracy
Praveen et al. [35]	IoT-based dataset stored on Cloud	Security assault discovery for confronting spoofing	Deep Learning	89.5%
Quy et al. [36]	IoT-based dataset stored on Cloud	Security assault discovery for confronting spoofing	CNN	88.78%
Pandimuruga n et al. [37]	Face recognition dataset	Security assault discovery for confronting spoofing	LSTM-CNN	90.85%
Othman et al. [15]	Physiological dataset	Security assault discovery for confronting spoofing	CNN3D	91.26%
Syafeeza et al. [14]	Face recognition dataset	Security assault discovery for confronting spoofing	Inception	92.05%
Hussain et al. [13]	Physiological dataset	Security assault discovery for confronting spoofing	CNN	85.5%
R. et al. [32]	Face recognition dataset	Security assault discovery for confronting spoofing	Xception	83.4%
Chen et al. [10]	Physiological dataset	Security assault discovery for confronting spoofing	CNN	86.5%
Teoh et al. [33]	IoT-based dataset stored on Cloud	Security assault discovery for confronting spoofing	CNN-LSTM	91.5%

III.METHODOLOGY

This study aims to create a system for intelligent homes that uses face identification and is based on the Internet of Things (IoT), utilizing a Raspberry Pi-based vision framework to accumulate information. Figure 3 illustrates the flowchart of the current study, which involves several steps. Firstly, an image is captured from the Raspberry Pi-based vision system, and then transmitted to the cloud storage for matching. Next, a profound learning-based novel engineering is utilized to extricate highlights from the confront and compare it with the database of known people authorized to reach the savvy homes. If the face detected by the algorithm matches the faces in the database of known individuals, the smart gate will unlock and allow access to the authorized person. However, If the recognized face does not match any authorized individuals in the system, the smart gate will remain locked, and access will not be granted.

A. Overview of the Dataset

The dataset utilized in this study was collected from a camera module based on Raspberry Pi. The dataset is confined to a slight gathering of people specifically related to the family individuals of a savvy home. The data set contains the subsequent attributes:

TABLE 2
OVERVIEW OF DATASET

Attributes	Interpretation	Value of data	Variable
Pictures	Camera Captures picture in Pixels RGB	Image data	Input
Ground Truth	Camera capture picture matched with the local database	Identified Picture	Input
User number	Integer number related to the camera image	Any integer or random number	Input
Security Check	Result of face recognition: Matched (1) or Unmatched (0)	0 or 1	Output

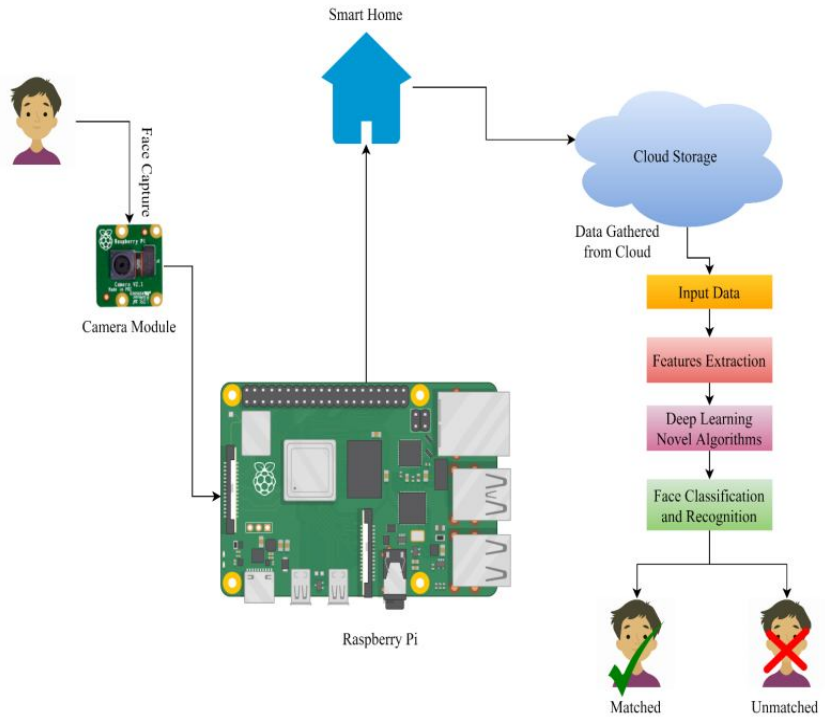


Fig. 3 Flow Diagram of the Present Study

B. Architectural model

The research aims to create an architecture for face recognition that combines Convolutional Neural Network (CNN) with the SVM-Boosted algorithm to improve classification performance. The local database's input image will undergo feature extraction in the convolutional layer, followed by the max pooling layer. This process involves using the extracted features from the Convolutional Layer to analyze the texture of each face and compare it with the reference or expected data (i.e., ground truth) for identification. The extracted values will be stored in a CSV file to enhance the system's robustness. After extricating the csv record, which contains the highlights in Table 2, the SVM-Boosted calculation will classify the right confront. Figure 4 outlines the building chart of the proposed CNN-SVM Boosted Confront Acknowledgment calculation. The proposed engineering has been approved numerically with the taking-after conditions.

$$G(m,n) = (f*h)[m,n]$$
$$= \sum_j \sum_k h[j,k] f[m-j, n-k] \ldots (1)$$

In computer vision, kernel convolution is widely used in convolutional neural networks (CNNs) and other algorithms. Convolutional neural networks apply a small matrix, known as a kernel or filter, to an image and then evaluate the resulting transformation. The feature maps' values can be computed by feeding an input image (f) and a kernel (h) into the network, with M and N denoting the row and column indices of the resulting matrix. In this study, In order to enhance the accuracy, we have devised a classification model which integrates the Support Vector Classifier (SVM) and the XGBoosting Classifier (XGBC). The mathematical expression of the SVM-XGBC model is presented below:

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

We are going to classify FDI assaults within the dataset by calculating the support vectors as takes after:

$$w.y + b = 1 \ldots (\text{vector1})$$
$$w.y + b = -1 \ldots (\text{vector2})$$

In this equation, P is the probability function of SVM, while yi is the outcome of the XGBC classification model. The term $\frac{\partial \sum \left(y_i - y_i^p\right)^2}{\partial y_p^i}$ represents the total residuals in trees, and α is the learning rate of XGBC. After the output y is obtained from XGBC, it is passed into the probability function of SVM for classification.

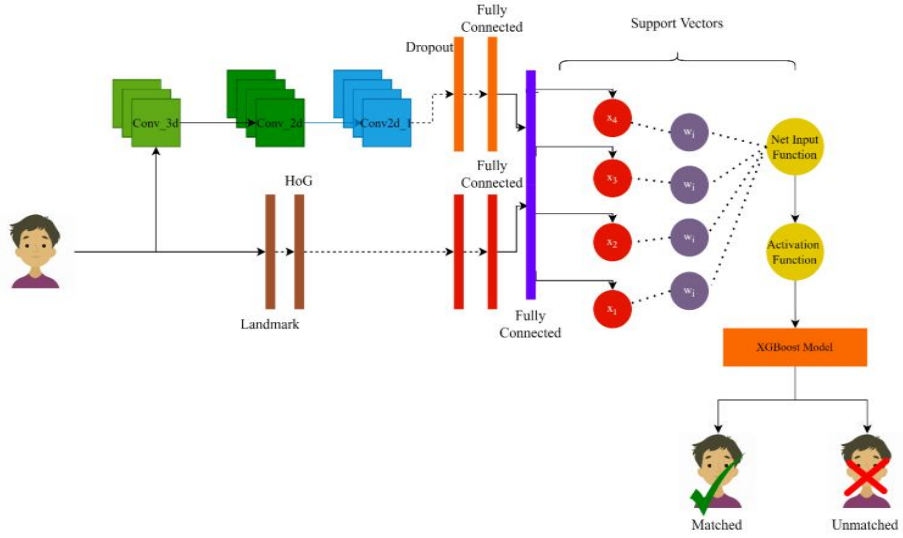
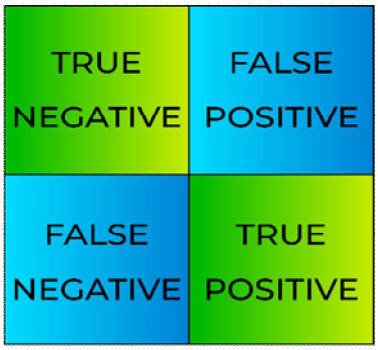


Fig.4 Proposed Model Architecture

1) *Texture Classification:* Texture classification is a challenging task in pattern recognition, where the goal is to differentiate between different textures. One of the primary challenges is identifying valuable features that can be extracted from the textured image, as many complex classifiers are available. Textures can be perceived either visually or tactually, whereas optical texture refers to the form and content of the image, while tactile texture can be felt by touching the surface.
2) *Feature Engineering:* Machine learning models can utilize various functions to analyze data within a specific domain. Before using machine learning algorithms, raw data must be converted into a format that the model can process and use, which usually requires manual work. The researchers in this study used a correlation matrix to evaluate the relationship between different variables. A correlation matrix is a matrix that measures the degree of the linear relationship between variables, similar to a covariance matrix. This study employs a correlation matrix to evaluate the relationship between different variables. A correlation matrix is a covariance matrix that summarizes the strength of the linear association between variables. The correlation coefficient, represented by 'r,' is a summary measure that indicates the strength and direction of a linear relationship between two quantitative variables. It ranges from -1 to +1, with -1 representing a perfect negative correlation, 0 representing no correlation, and +1 representing a perfect positive correlation.
3) *Performance Evaluation:* The system's performance was assessed in this research using F1 Score and accuracy measures. Additionally, the confusion matrix was used to determine the number of correctly and incorrectly classified instances. Table 3 provides a summary of the evaluation metrics used in this study.

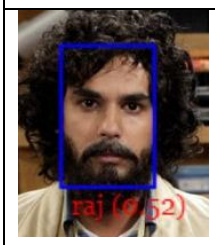
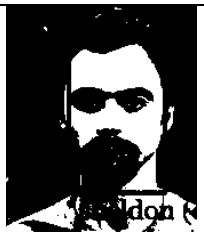
TABLE 3
DESCRIPTION OF MATRICS

Metric	Description
Accuracy	$\text{Accuracy} = \frac{\text{TP}}{(\text{TP}+\text{TN})*100}$ True-Positive (TP): if the output is 1 so it is present in the data file True-Negative (TN):): if the output is 0 so it is not present in the data file
Confusion Matrix	

IV. RESULTS AND DISCUSSIONS

Deep neural networks are a highly effective machine learning technique for classification tasks. Among these, convolutional neural networks are especially adept at image classification tasks. These networks have been shown to perform better than other approaches in tasks such as image categorization. By applying deep learning techniques, it is possible to build an end-to-end model for medical image classification that takes raw pixel data as input. This study has presented two CNN models that are changed to identify the correct face for home protection by analyzing the image's texture and comparing it to the ground truth. The identified face is labeled as 0 or 1 in the dataset, and Table 4 shows the faces that have been correctly recognized.

TABLE 4
FACE RECOGNITION

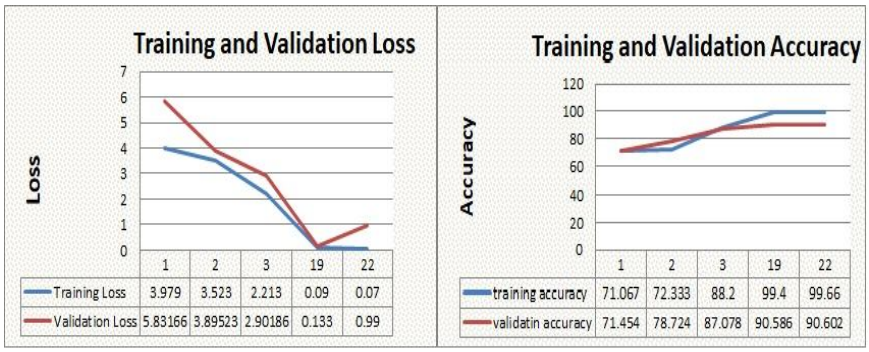
Face	Ground truth	Label	Face	Ground truth	Label
		Matched Security lock Opened			Matched Security lock Opened
		Matched Security lock Opened			Miss Matched Security lock not Opened

A. *Hybrid Model Proficiency*

The diagram illustrates the integration of CNN-SVM and XGBoost Classifier models to enhance their accuracy simultaneously. Once y is produced, XGB will utilize SVM's probability function to assess if there is a change in class, either from Matched Faces (Class A) or Unmatched Faces (Class B). Figure 5 illustrates the performance of the combined model.

TABLE 5
STATISTICAL RESULTS FROM 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
22	0.07	99.66	0.99	90.602



	1	2	3	19	22
Training Loss	3.979	3.523	2.213	0.09	0.07
Validation Loss	5.83166	3.89523	2.90186	0.133	0.99

	1	2	3	19	22
training accuracy	71.067	72.333	88.2	99.4	99.66
validatin accuracy	71.454	78.724	87.078	90.586	90.602

Fig.5 Performance of Proposed Model

The model's most successful epoch is depicted in Figure 5, which occurred at epoch 22, achieving an accuracy of 99.66% and a validation loss of 0.99.

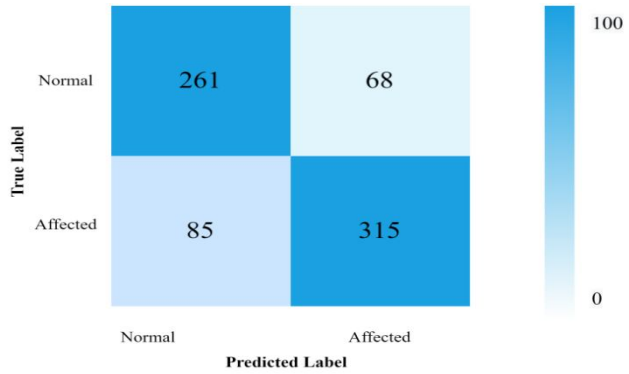


Fig.6 Confusion Matrix

Figure 6 displays the error matrix of the model, indicating a solid performance with 315 true positive values. However, 85 instances of false positives and 68 instances of false negatives affect the model's accuracy. These inaccuracies can be addressed by applying optimization techniques.

V. CONCLUSIONS

Since the start of the 21st century, security has become increasingly crucial in people's lives, particularly financial matters. A real-time recognition system has been proposed to efficiently manage photographic material to reduce monitoring expenses. This research aimed to develop an intelligent face identification approach using Deep Learning to secure smart homes. To showcase this study's efficacy, we compared and analyzed it with other advanced techniques. By accurately recognizing individuals, we can improve privacy in our surroundings. This research presents a tree-based deep model for facial identification in the Cloud. The high accuracy of this deep model is maintained with fewer computer resources. The model's input volume is divided into several sub-volumes, and a tree is created for each. Identifying individuals ensures the safety of our homes and workplaces. This research focuses on developing an intelligent face recognition method using deep learning for smart homes. The proposed model is compared and contrasted with other cutting-edge approaches in the field to demonstrate its applicability. The CNN-SVM-Boosted Classifier model has achieved an accuracy of 99.66% in identifying the correct person in a smart home, demonstrating its high performance. However, the study has yet to be implemented in real-time, and future research endeavors to create a real-time model by using actual time datasets to improve the security of smart homes.

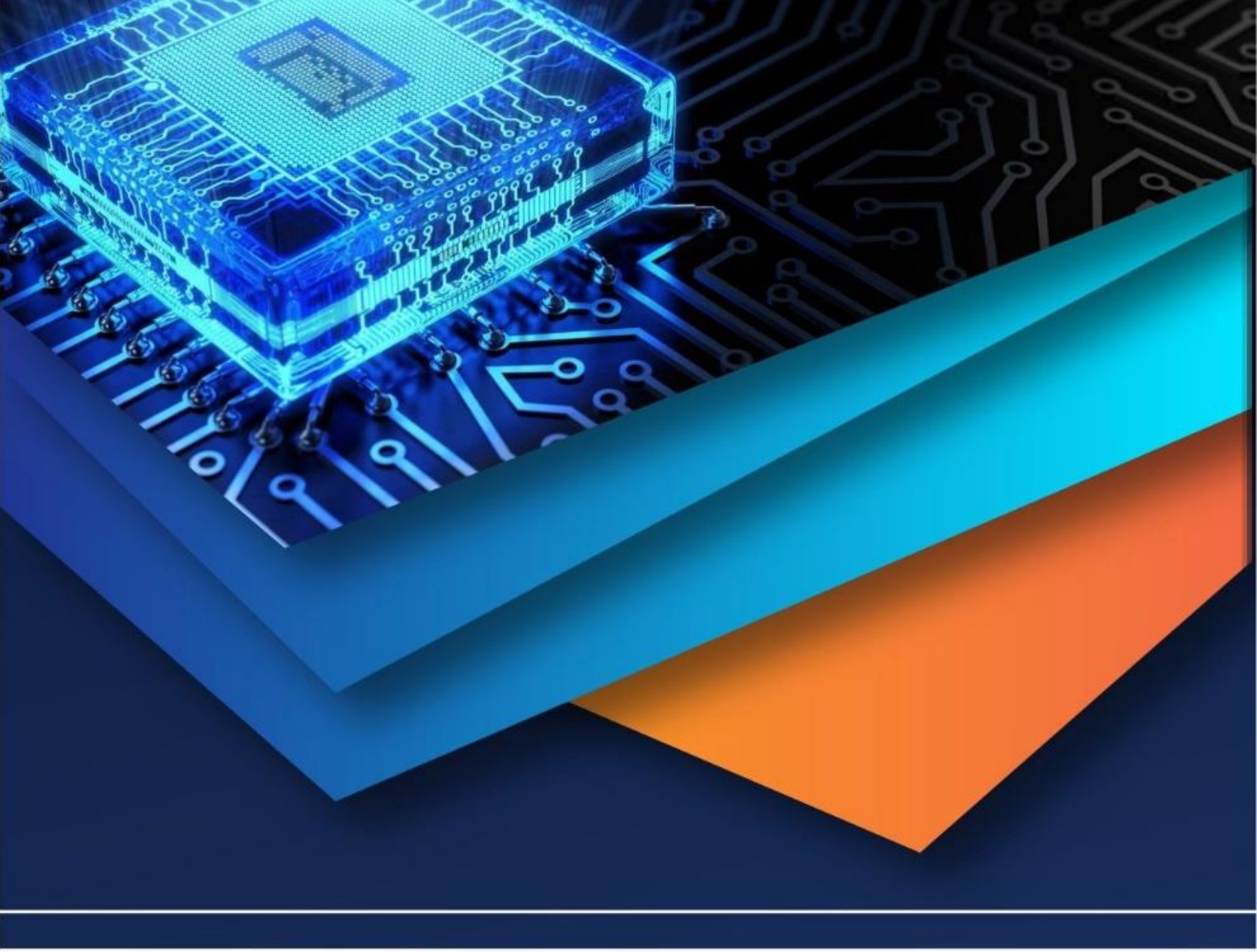
VI. ACKNOWLEDGMENT

The National Natural Sciences Foundation of China (No. 62166011) and the Innovation Key Project of Guangxi Province (No. 222068071) support this research. Additionally, the research is conducted in the Guangxi Key Laboratory of Intelligent Processing of Computer Images and Graphics.

REFERENCES

[1] S. Khare and M. Totaro, "Ensemble Learning for Detecting Attacks and Anomalies in IoT Smart Home," Proc. - 2020 3rd Int. Conf. Data Intell. Secure. ICDIS 2020, pp. 56–63, 2020, doi: 10.1109/ICDIS50059.2020.00014.
[2] A. Sivanathan et al., "Classifying IoT Devices in Smart Environments Using Network Traffic Characteristics," IEEE Trans. Mob. Comput., vol. 18, no. 8, pp. 1745–1759, 2019, doi: 10.1109/TMC.2018.2866249.
[3] A. S. Rathore et al., "Scanning the Voice of Your Fingerprint with Everyday Surfaces," IEEE Trans. Mob. Comput., vol. 1233, no. c, pp. 1–18, 2021, doi: 10.1109/TMC.2021.3049217.
[4] S. Amershi et al., "Software Engineering for Machine Learning: A Case Study," Proc. - 2019 IEEE/ACM 41st Int. Conf. Softw. Eng. Softw. Eng. Pract. ICSE-SEIP 2019, pp. 291–300, 2019, doi: 10.1109/ICSE-SEIP.2019.00042.
[5] W. Lin and S. Hu, "Design and implementation of an offline face recognition locker," J. Phys. Conf. Ser., vol. 1634, no. 1, pp. 1–66, 2020, doi: 10.1088/1742-6596/1634/1/012131.
[6] U. Elordi, A. Bertelsen, L. Unzueta, N. Aranjuelo, J. Goenetxea, and I. Arganda-Carreras, "Optimal deployment of face recognition solutions in a heterogeneous IoT platform for secure elderly care applications," Procedia Comput. Sci., vol. 192, pp. 3204–3213, 2021, doi: 10.1016/j.procs.2021.09.093.
[7] H. Ouanan, A. Gaga, O. Diouri, M. Ouanan, and B. Aksasse, "Development of Deep Learning-Based Facial Recognition System," Adv. Intell. Syst. Comput., vol. 1106 AISC, no. February, pp. 45–52, 2020, doi: 10.1007/978-3-030-36677-3_6.
[8] M. Masud et al., "Deep learning-based intelligent face recognition in IoT-cloud environment," Comput. Commun., vol. 152, no. September 2019, pp. 215–222, 2020, doi: 10.1016/j.comcom.2020.01.050.
[9] D. White, J. D. Dunn, A. C. Schmid, and R. I. Kemp, "Error rates in users of automatic face recognition software," PLoS One, vol. 10, no. 10, pp. 1–14, 2015, doi: 10.1371/journal.pone.0139827.
[10] S. Chen, S. Ding, H. Fu, Y. Xian, X. Liu, and C. Zhang, "Deep Learning Applied to Smart Home Face Recognition Access Control System," vol. 146, no. ICAITA, pp. 13–15, 2018, doi: 10.2991/icaita-18.2018.4.
[11] O. Daescu, H. Huang, and M. Weinzierl, "Deep learning based face recognition system with smart glasses," ACM Int. Conf. Proceeding Ser., pp. 218–226, 2019, doi: 10.1145/3316782.3316795.
[12] C. Liu, Y. Chen, and I. Member, "The Design of Deep-Learning-Based Facial Recognition System for Smart Shopping Cart."
[13] T. Hussain et al., "Internet of Things with Deep Learning-Based Face Recognition Approach for Authentication in Control Medical Systems," Comput. Math. Methods Med., vol. 2022, 2022, doi: 10.1155/2022/5137513.
[14] A. R. Syafeeza, M. K. Mohd Fitri Alif, Y. Nursyifaa Athirah, A. S. Jaafar, A. H. Norihan, and M. S. Saleha, "IoT based facial recognition door access control home security system using raspberry pi," Int. J. Power Electron. Drive Syst., vol. 11, no. 1, pp. 417–424, 2020, doi: 10.11591/ijpeds.v11.i1.pp417-424.
[15] N. A. Othman and I. Aydin, "A face recognition method in the Internet of Things for security applications in smart homes and cities," Proc. - 2018 6th Int. Istanbul Smart Grids Cities Congr. Fair, ICSG 2018, no. October, pp. 20–24, 2018, doi: 10.1109/SGCF.2018.8408934.
[16] M. Farayola and A. Dureja, "A Proposed Framework: Face Recognition With Deep Learning," Int. J. Sci. Technol. Res., vol. 9, no. 07, p. 7, 2020.
[17] A. S. Al-Waisy, R. Qahwaji, S. Ipson, and S. Al-Fahdawi, "A multimodal deep learning framework using local feature representations for face recognition," Mach. Vis. Appl., vol. 29, no. 1, pp. 35–54, 2018, doi: 10.1007/s00138-017-0870-2.
[18] M. M. Ghazi and H. K. Ekenel, "A Comprehensive Analysis of Deep Learning Based Representation for Face Recognition," IEEE Comput. Soc. Conf. Comput. Vis. Pattern Recognit. Work., pp. 102–109, 2016, doi: 10.1109/CVPRW.2016.20.
[19] D. S. AbdELminaam, A. M. Almansori, M. Taha, and E. Badr, "A deep facial recognition system using computational intelligent algorithms," PLoS One, vol. 15, no. 12 December, pp. 1–27, 2020, doi: 10.1371/journal.pone.0242269.
[20] Z. Pei, H. Xu, Y. Zhang, M. Guo, and Y. Yee-Hong, "Face recognition via deep learning using data augmentation based on orthogonal experiments," Electron., vol. 8, no. 10, pp. 1–16, 2019, doi: 10.3390/electronics8101088.
[21] A. Alzu'bi, F. Albalas, T. Al-Hadhrami, L. B. Younis, and A. Bashayreh, "Masked face recognition using deep learning: A review," Electron., vol. 10, no. 21, 2021, doi: 10.3390/electronics10212666.
[22] M. Chihaoui, A. Elkefi, W. Bellil, and C. Ben Amar, "A survey of 2D face recognition techniques," Computers, vol. 5, no. 4, pp. 41–68, 2016, doi: 10.3390/computers5040021.
[23] S. Qureshi, "Face Recognition (Image Processing) based Door Lock using OpenCV, Python and Arduino," Int. J. Res. Appl. Sci. Eng. Technol., vol. 8, no. 6, pp. 1208–1214, 2020, doi: 10.22214/ijraset.2020.6197.
[24] Y. Fang, J. Hu, and W. Deng, "Identity-Aware CycleGAN for Face Photo-Sketch Synthesis and Recognition."
[25] H. Sabharwal and A. Tayal, "Human Face Recognition," Int. J. Comput. Appl., vol. 104, no. 11, pp. 1–3, 2014, doi: 10.5120/18243-9173.
[26] I. J. Wireless et al., "Home Security Using Authentication and Mobile Application," no. April, pp. 40–50, 2022, doi: 10.5815/ijwmt.2022.02.04.
[27] K. T. Reddy, "Intelligent Door Lock System with Face Recognition," Int. J. Res. Appl. Sci. Eng. Technol., vol. 8, no. 5, pp. 364–371, 2020, doi: 10.22214/ijraset.2020.5060.
[28] S. Zaleha. H, N. Ithnin, N. H. A. Wahab, and N. Sunar, "Intelligent Locking System using Deep Learning for Autonomous Vehicle in Internet of Things," Int. J. Adv. Comput. Sci. Appl., vol. 12, no. 10, pp. 565–578, 2021, doi: 10.14569/IJACSA.2021.0121063.
[29] T. Ahmad et al., "Human Action Recognition in Video Sequence using Logistic Regression by Features Fusion Approach based on CNN Features," Int. J. Adv.Comput. Sci. Appl., vol. 12, no. 11, pp. 18–25, 2021, doi.org/10.14569/IJACSA.2021.0121103
[30] S. T. Suganthi et al., "Deep learning model for deep fake face recognition and detection," PeerJ Comput. Sci., vol. 8, pp. 1–20, 2022, doi: 10.7717/PEERJ-CS.881.
[31] A. H A, "Smart Home Security using Facial Recognition and Unusual Event Detection," Int. J. Res. Appl. Sci. Eng. Technol., vol. 8, no. 6, pp. 1462–1468, 2020, doi: 10.22214/ijraset.2020.6239.
[32] M. R., R. Y., R. R., and S. A., "Smart Home Security System using Iot, Face Recognition and Raspberry Pi," Int. J. Comput. Appl., vol. 176, no. 13, pp. 45–47, 2020, doi: 10.5120/ijca2020920105.
[33] K. H. Teoh, R. C. Ismail, S. Z. M. Naziri, R. Hussin, M. N. M. Isa, and M. S. S. M. Basir, "Face Recognition and Identification using Deep Learning Approach," J. Phys. Conf. Ser., vol. 1755, no. 1, 2021, doi: 10.1088/1742-6596/1755/1/012006.

[34] X. Wu, L. Song, R. He, and T. Tan, "Coupled deep learning for heterogeneous face recognition," 32nd AAAI Conf. Artif. Intell. AAAI 2018, pp. 1679–1686, 2018.
[35] K. V. Praveen et al., "Deep learning based intelligent and sustainable smart healthcare application in cloud-centric IoT," Comput. Mater. Contin., vol. 66, no. 2, pp. 1987–2003, 2020, doi: 10.32604/cmc.2020.012398.
[36] V. K. Quy, N. Van Hau, D. Van Anh, and L. A. Ngoc, "Smart healthcare IoT applications based on fog computing: architecture, applications and challenges," Complex Intell. Syst., 2021, doi: 10.1007/s40747-021-00582-9.
[37] V. Pandimurugan, A. Jain, and Y. Sinha, "IoT based face recognition for smart applications using machine learning," Proc. 3rd Int. Conf. Intell. Sustain. Syst. ICISS 2020, pp. 1263–1266, 2020, doi: 10.1109/ICISS49785.2020.9316089.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY