BEYKOZ UNIVERSITY

GRADUATE PROGRAMS INSTITUTE

INTEGRATING IMAGE PROCESSING TECHNIQUES FOR ENHANCING FACIAL RECOGNITION SECURITY IN IoT DEVICES

Duha MUSTAFA

MASTER'S THESIS

İstanbul, 26 May 2025

GRADUATE PROGRAMS INSTITUTE

Duha Mustafa

MASTER'S THESIS
COMPUTER ENGINEERING DEPARTMENT
COMPUTER ENGINEERING MASTER'S PROGRAM WITH THESIS

MASTER'S THESIS ADVISOR
Prof. ABDURAZZAG ALI A ABURAS

MASTER'S THESIS JURY MEMBERS
Dr. Ozlem Feyza Erkan

MASTER'S THESIS JURY MEMBERS
Dr. Burcin Kulahcioglu

Contents

ACKNOWLEDGMENT

I would like to sincerely thank everyone who played a role in helping and guiding me during this thesis.

First and foremost, I owe deep thanks to my supervisor, Prof. ABDURAZZAG ALI ABURAS, for his consistent guidance, valuable feedback, and patience, which made a huge difference throughout this journey. I appreciate how he motivated me to think critically, stay focused, and be positive.

I am also grateful to my family and friends for being my emotional support, whether through kind gestures, words, or simply by being there when I needed them. It would not have been possible without their understanding and encouragement.

I also want to thank my classmates and peers for their mindful discussions, suggestions, and sharing ideas, which enhanced my ability to understand and made this journey smoother.

Finally, I want to thank all the institutions, researchers, and online resources for their work. Their hard efforts and research structured the basis of my study. Without access to that information, it would not have been possible.

I am sincerely grateful to all of the people who have contributed to my study in any way possible.

ABSTRACT

INTEGRATING IMAGE PROCESSING TECHNIQUES FOR ENHANCING FACIAL RECOGNITION SECURITY IN IoT DEVICES

Access control in IoT-based systems mostly depends on face recognition, but it still faces many issues. Issues as face recognition errors, facial feature changes, and security problems like spoofing attempts. The primary focus in this work was improving the security of the system along with its reliability by managing advanced image processing techniques, such as depth analysis, liveness detection, and recurring authentication updates

To make the system more restricted to fraudulent access and optimized at managing crucial cases, these additions are made, which are not just some technical updates but they also play an important part. Furthermore other methods like anomaly detection, and feature extraction were used to enhance the robustness of system, while allowing it to adjust to new issues effectively.

Issues relevant to algorithmic bias and user privacy have also been taken into consideration while working on this study, by evaluating that not just system is secure but also it's not biased and is ethical. Combination of work have been suggested in the results, where the system is security-focused and ethically aware design makes it more effective and reliable facial recognition system, with strong potential for future use in IoT-based authentication environments.

Keywords: IoT access control system, facial recognition, image processing, IoT security, liveness detection, anti-spoofing, ethical AI.

ABSTRACT

IoT Cihazlarında Yüz Tanıma Güvenliğini Artırmak İçin Görüntü İşleme Tekniklerinin Entegrasyonu

IoT tabanlı sistemlerde erişim kontrolü çoğunlukla yüz tanımaya bağlıdır, ancak yine de birçok sorunla karşı karşıyadır. Yüz tanıma hataları, yüz özelliği değişiklikleri ve sahtecilik girişimleri gibi güvenlik sorunları gibi sorunlar. Bu çalışmadaki temel odak, derinlik analizi, canlılık tespiti ve yinelenen kimlik doğrulama güncellemeleri gibi gelişmiş görüntü işleme tekniklerini yöneterek sistemin güvenliğini ve güvenilirliğini iyileştirmekti

Sistemi sahte erişime daha fazla kısıtlamak ve kritik durumları yönetmede optimize etmek için, yalnızca bazı teknik güncellemeler değil, aynı zamanda önemli bir rol oynayan bu eklemeler yapıldı. Ayrıca, anormallik tespiti ve özellik çıkarma gibi diğer yöntemler, sistemin sağlamlığını artırmak ve yeni sorunlara etkili bir şekilde uyum sağlamasını sağlamak için kullanıldı.

Bu çalışma üzerinde çalışırken, algoritmik önyargı ve kullanıcı gizliliğiyle ilgili sorunlar da dikkate alındı ve yalnızca sistemin güvenli değil, aynı zamanda önyargılı olmadığı ve etik olduğu değerlendirildi. Sonuçlarda, sistemin güvenliğe odaklı ve etik açıdan bilinçli bir tasarıma sahip olması, onu daha etkili ve güvenilir bir yüz tanıma sistemi haline getirirken, IoT tabanlı kimlik doğrulama ortamlarında gelecekte kullanım için güçlü bir potansiyele sahip olduğu öne sürülen çalışmaların birleştirilmesi önerilmiştir.

Anahtar Kelimeler: IoT erişim kontrol sistemi, yüz tanıma, görüntü işleme, IoT güvenliği, canlılık tespiti, sahteciliğe karşı koruma, etik yapay zeka.

ABBREVIATIONS

AI: Artificial Intelligence
FR: Facial Recognition
IoT: Internet of Things
ML: Machine Learning
DL: Deep Learning
LDA: Liveness Detection Algorithm
DA: Depth Analysis
PAU: Periodic Authentication Updates
AD: Anomaly Detection
FE: Feature Extraction
MTCNN: Multi-task Cascaded Convolutional Neural Network
CNN: Convolutional Neural Network
LBP: Local Binary Pattern
UI: User Interface
VS: Visual Studio
F1 Score: Harmonic Mean of Precision and Recall
FPS: Frames Per Second
RF: Random Forest
ResNet50: Residual Network with 50 Layers
MSU: Michigan State University
MSU MFSD: MSU Mobile Face Spoofing Database

LIST OF FIGURES

LIST OF TABLES

1. INTRODUCTION

1.1 Background of the Study

In today's world, one of the most difficult and concerning challenges faced in managing IoT systems is security and privacy. As the number of interconnected devices and platforms is increasing, managing these aspects has become crucial. Deep learning algorithms have shown strong potential in overcoming these challenges, specifically when evaluating the security of IoT environments. In many IoT applications, where surveillance or smart environments are involved, image data plays a main role. The ecosystem itself consists of unlimited devices, users, and network interactions, all generating a huge amount of data in real time. Management of this enormous volume of information is known as "big data". It demands intelligent systems capable of learning patterns on their own. Deep learning is specifically suitable in these scenarios, as believed by (Al-Ghaili A. M.-H., 2023), as it does not depend on any predefined rules or manual feature selection while analyzing big datasets, which makes it well-suited for the dynamic and high-volume nature of IoT.

Using IoT devices like smart home systems, wearable health monitors and autonomous vehicles in our daily routine, have made IoT technology become part of our life. If we particularly talk about autonomous vehicles, there are smart IoT sensors that capture images and then process those image's data to handle crucial tasks like object classification and monitoring traffic conditions (Majumder, 2020). Integration of deep neural networks into cloud-based IoT systems for real-time image classification is one of the potential areas of IoT technology. This method have strong processing capabilities but it also have security concerns. As adoption of smart IoT devices has increased, the number of new challenges has also increased, especially challenges to overcome the limited computational capacity of many IoT devices. Tasks such as secure image classification, feature extraction, and data encryption require far more processing power than these devices can usually offer on their own (Olazabal, 2019).

In essence, the IoT represents a system of smart devices that are equipped with software, sensors, and communication capabilities. These smart devices communicate with each other to gather data and, in many scenarios, perform automated tasks based on that information. Fundamentally, it's a global network that links both physical and digital objects through real-time communication and processing (Lescano, 2023). In past years, facial recognition (FR) has emerged as an important security tool in making homes, offices and businesses more secure. While traditional security systems often get into issues, especially in terms of real-time data reliability. Whereas facial recognition technology offers a more reactive and intelligent solution and its one of the most well-known biometric methods due to its capability to identify and verify individuals through unique patterns and features of human face (Sayem, 2018). In contrast to fingerprints or voice-based systems, facial recognition feels more user friendly and seamless, making it a more practical option for modern authentication needs.

In recent developments, facial recognition technology has been shown as a promising advancement, especially due to the integration of deep learning techniques. In one of the research studies by (Al-Ghaili A. M.-H., 2023), he introduced a facial recognition using Raspberry Pi alongside OpenCV libraries and Python to improve security. In another approach, (Sajjad M. N., 2019) explored the use of deep learning methods, specifically convolutional neural networks (CNNs) with the Sobel operator to enhance recognition accuracy in surveillance systems. While handling issues with low-resolution images, pointing out its importance in real-world monitoring applications, this method maintained powerful performance.

1.1.1 Internet of Things IoT

Physical objects like home appliances, wearable devices, automobiles and industrial sensors are being equipped with computing capabilities and connectivity making it a fast growing ecosystem which is usually referred to as Internet of Things IoT. Without human involvement these devices can automatically perform tasks like data collection and exchanging information with other systems, by communicating through internet or other protocols, doing live monitoring, control and making decisions.

IoT have the ability to provide an ordinary object, a special layer of digital smartness. Which makes it more beneficial as these devices can easily communicate to user commands and environmental input. Smart homes, healthcare, agriculture, industrial automation, and transportation, all of these domains have become part of this technology.

Furthermore, due to the rapid growth, new opportunities and equally essential challenges in system reliability, data privacy, and security, the infrastructure of IoT has become more complex and scalable. The need for stronger and intelligent security frameworks has become necessary, as more systems are now integrated into sensitive and critical environments.

1.2 Problem Statement

Access control in domains like smart homes, healthcare, and surveillance, where facial recognition is used, has started facing issues like security, privacy, and data integrity, due to the increase in integration of IoT devices. In biometric methods, facial recognition has always been well-known but still it has some limitations. Spoofing attacks being one of the major risk, where unauthorized person tries to invade system by using some forms of impersonation like 3D masks, videos, pictures. However, these systems not only face security issues but also have to go through other challenges like different angle viewings, poor lightening, and partial face occlusions, all of these factors have impact on system's reliability and accuracy (Radzi, 2020).

To enhance security and reliability of facial recognition system, an advanced image processing techniques can be integrated into IoT devices, which can help in overcoming these vulnerabilities. Furthermore, to better distinguish between real user and spoof attacks, methods like real-time image enhancement, deep learning-based feature extraction can be beneficial. However, the combination of facial recognition methods with other biometric methods like voice recognition, fingerprint scanning, can help in creating multi-layered security approaches that increase protection and decrease the risk of unauthorized access (Radzi, 2020).

1.3 Research Questions

1. What are the main security issues that arise while implementing facial recognition systems within IoT applications?

Many security challenges are faced by facial recognition systems when they are integrated within IoT applications. Spoofing attempts is one of the most common risks among them, where an unauthorized individual attempts to fool the authentication system through pictures, 3D masks, and videos. Additionally, data can be intervened during transmission, model manipulation and unauthorized access to devices is a constant concern. The distributed nature of IoT networks and the limited processing power of many devices make it more challenging to deploy complex security measures. The focus of this study is on these vulnerabilities and the exploration of effective strategies to strengthen the security of facial recognition in IoT solutions.

2. In IoT applications, what methods can be used to ensure that accuracy and privacy is preserved over time?

For facial recognition systems in IoT solutions to stay reliable over time, they must adapt to changes in patterns, individual's facial features because of aging or any other environmental factors. This study explores adaptive approaches, such as dynamic threshold adjustments, prompting users to re-authenticate and recurring updates to stored facial data. Most importantly, it also considers the privacy-preserving approaches to ensure that user data remains secure during these updates, which is fundamentally critical in multi-device IoT networks.

3. In what ways can liveness detection in facial recognition-based IoT security systems be improved through the integration of image processing and machine learning?

Integrating image processing with machine learning creates a strong approach for detecting spoofing attacks in facial recognition systems. This involves analyzing depth

information, texture patterns, motion cues, and blink detection to differentiate real faces from fake. Image processing helps improve the input quality and highlights important features, while machine learning models, trained on various datasets, can adapt to different spoofing methods. Collectively, these technologies form the basis for a more reliable and secure facial recognition systems appropriate for real-time IoT applications

1.4 Research Aim and Objectives

This study focuses on exploring how image processing methods can be used to strengthen the security of facial recognition systems in IoT devices.

The main objectives of this study are:

- **To develop and test advanced image processing methods** that improve the accuracy and reliability of facial recognition systems in IoT environments.
- **To design and implement effective anti-spoofing measures** using image processing methods that improve the overall security of facial recognition systems used in IoT settings.
- **To optimize facial recognition algorithms especially** for IoT devices by creating lightweight, computationally efficient approaches that creates balance between power usage and system performance.

1.4 Significance of the Study

This study holds significant importance of growing requirements for secure, reliable and robust authentication systems. As integration of IoT devices in areas like smart homes, healthcare, workplace security, and surveillance has become common now a days, making sure the security of facial recognition have become more complex than before (Radzi, 2020).

Spoofing attempts have remained a recurring issue to traditional facial recognition approaches. Serious concerns are arisen by these kinds of weaknesses, specifically in sensitive environments, where unauthorized access can lead to privacy breaches, compromised security and data theft.

To improve the adaptability of facial recognition systems for spoofing attacks, this study offers approaches like the integration of advanced image processing techniques and deep learning-based feature extraction. Moreover, the optimization of these techniques for IoT systems has been analyzed in this research, where limitations faced by devices, such as insufficient computational resources and power consumption. Development of more compact and efficient algorithms will ensure smooth integration of facial recognition systems into IoT devices without lowering system performance (Sajjad M. N., 2019). The results of this study will be an addition to improving the security and reliability of facial recognition systems, specifically in complex departments such as government, healthcare, and finance, where data protection is a top priority.

1.5 Structure of the Thesis

This thesis is structured into five chapters:

- **Chapter 1: Introduction** – Gives an overview of the background, problem statement, objectives, and research aim.
- **Chapter 2: Literature Review** – Outlines relevant research and outcomes from previous studies in the field of facial recognition and IoT security.
- **Chapter 3: Research Methodology** – Details the research methods, techniques, and approaches applied to obtain the research objectives.
- **Chapter 4: Results and Analysis** – Presents and analyzes the results achieved from developing the proposed image processing techniques.
- **Chapter 5: Conclusion and Future Research** – Summarizes the key findings, draws conclusions, and suggests plan for future research.

2. LITERATURE REVIEW

2.1 Introduction

This chapter reviews the previous studies and discovers the research gap that this study aims to address. Moreover, this chapter achieves the main objectives of the research extensively by analyzing diverse IoT apps within smart city settings that utilize image processing techniques. The research focuses on three major areas: safety, security, and privacy concerns for image-related IoT applications.

2.2 Image Processing-Based IoT Security Applications and Systems

In the procedure of transmitting data that use cloud storage services and networks through IoT systems, such as images, that have been used to encrypt and maintain additional information that is associated with the data in question. In the process of this transfer, the information is saved in a medium that is not safe (Sarimole, 2024). Images are utilized in such a way that they must have secured the data in the whole journey till it's securely delivered at its destination in a protected way. The purpose of this section is to give an overview of a number of researches that have been analyzed in the literature and which shows how image processing methods are helping to achieve the data safety and security of respective files while they are being transmitted digitally between IoT devices (Sarimole, 2024). A biometrics solution that allows encryption through pairing-enablement has been proposed as a replacement for the methods that are now being utilized to secure transferred information between any IoT applications and other third parties, which can include communication networks and devices. Consequently, the system offered has replaced these techniques. Because of these unique characteristics that biometrics-based methods own, it is stated that this methodology is more robust against vulnerabilities than other approaches, such as password verification system (Lescano, 2023). The proposed approach, which

performs facial recognition by integrating necessary biometric characteristic is validated through case study.

Before initializing the process of face recognition, the image of the face was captured by a specific sensor that was placed on a device that had IoT connected (i.e. Smartphone). Through the communication network, the discussed application will send the image that has been captured to the destination route with the help of the IoT environment (Peixoto, 2020). With the use of image processing algorithms, it is possible to achieve an end-to-end encryption operation. Methods from the field of image processing are proven to be essential to implement an encrypted and secure objective for a smart home system using IoT-based applications. The discussed system's objective is being proposed; capturing the image at certain place where the system is integrated having camera to carry out a security duty that is associated to the home through the IoT platform (Thakur, 2024). Image processing is accountable for carrying out a variety of image procedures, including preprocessing of images, carried out by analysis, and finally finding the match among the image that was captured and image that was stored in the database for reference. In the event when captured match doesn't match with reference image, the system will send an alert message based on the IoT device to remind the owner of the residence. An image encryption has been applied with the help of Cellular Automata (CA) through the implementation of image processing methods (Sharma, 2024). The values that reflect the pixel intensity values, which are image features, that are transformed into a array of 8-bit string series (Awad, 2024). There is a set of CA rules and these values. The authors have drawn attention to the fact that the camera first takes a picture that will be encrypted at the observation layer. It is assumed that these pictures include critical information. Things are encrypted in this, so they are secured. Furthermore, those images will be sent to the various layers of the network (Babu, 2024). Then those images are going to be decrypted. To make sure that the path between network and observation levels is secured, this approach of security is deployed to confidential images for nodes (fog) that are installed within network. At this stage, the nodes are accountable for forwarding images that have been received to the cloud so that they can move to additional processing if it is needed (Majumder, 2020). Image encryption has become more popular in recent years as a result of the massive quantity of information that is

engaged in the transmission of images across the cloud, which is a process that is performed by many IoT apps. As a result, image encryption is in need to be improved to provide individuals more effectively and serve to the aim. To ensure the maintenance of a safe and secure public route among captured image's source and node-fog, encryption is required. The reality is that the features of the pixels and the values created by the CA are mixed is a compelling encryption approach (Medjdoubi, 2024). To group DDoS - distributed denial of service; malware assaults and image processing is implemented to ensure IoT devices' security. At the beginning, grayscale photographs can be classified according to the families that they are associated with. Denial of service (DDoS) malware assaults can also be detected (Medjdoubi, 2024). Once this is achieved, more security methods can be implemented using algorithms provided by image processing. For security purposes, it is necessary to have a facial recognition system in place. Various IoT apps have taken advantage of this feature for a lot of different purposes. Face recognition technology has a wide range of applications in the sector of smart home technology, including security and control (Elngar, 2020). There are plenty of other programs that are specifically developed to recognize specific face in crowd in specific places or zones like parks, roads, airports etc. It is proposed and realized that an undetectable plaintext attack-protected picture classification system for IoT applications is developed (Elngar, 2020). However, it is not required for an IoT device to keep communication with the cloud-based image classification system. In the context of deep neural networks (DNNs), an approach has been proposed for the secure assessment of linear functions, like divide-and-conquer and a format of unified ideal protocols. Moreover, a similar mechanism has been proposed for the secure assessment of non-linear functions. The lattice-based homomorphic method and the 2-PC secure algorithms of computing confirm that the contents of the images, the parameters of the private model of DNN, and the midway yield are kept private (Singh, 2022). To extract deep features from a picture, a deep convolutional neural network model that has been pretrained by the Visual Geometry Group (VGG-16) is used. Through a wide variety of attempts, it has been demonstrated that the framework that has been suggested is both efficient and accurate. The white-box membership inference attack, which is more often known as the most powerful attack against DNN models, is yet another method that is utilized to test the

framework's security effectiveness (Singh, 2022). Since the assault was not successful, it may be resulted as that this system is practically secure.

2.2.1 IoT Security Applications:

Extensive usage of IoT systems in crucial settings where maintaining device integrity, data confidentiality, and secure communication is important, sectors such as smart homes, transportation, healthcare, and industrial automation. Due to constant involvement in data transmission between linked devices, these systems are more exposed to cyber threats like unauthorized access, data interception, spoofing attempts, and distributed denial of service (DDoS) attacks.

To ensure the security of IoT applications, the most commonly used methods are secure data transmission, device authentication, access control, and anomaly detection. One example of these systems is biometric-based authentication, like fingerprint scanning or facial recognition, in offices to ensure that only authorized individuals can gain access to the system or devices. Real-time monitoring and alert systems have been utilized in industrial IoT and surveillance setups to identify system failures or fraudulent activity.

Multi-factor authentication, secure edge computing and encryption protocols are aggressively used in high-security IoT applications to ensure data security from manipulation and intervention. Even while facing any threat, this protection ensures that IoT systems still work reliably. Protection of tangible assets is as much important as security of IoT applications, which require maintenance of privacy and system dependability in interconnected environments.

2.3 Image Processing-Based IoT Safety Applications

Integrating image processing in IoT applications and smart city applications has proven to be an enhancement in various requirements and objectives. Image processing has been utilized to ensure the safety of individuals in an intriguing application while they are on their way to implementation of detection and recognition of road targets. This means that the proposed method has implemented a multimodal recognition procedure for interested things that have been placed on highways, for instance,

harmful and harmless objects (Al-Ghaili A. M.-H., 2023). After the object recognition has been deployed and successfully carried out, an algorithm that is based on AI and reinforcement learning (RL) is applied to transmit this information to a wearable device or robot. This allows the users to communicate or engage with the device to decide based on the information (Al-Ghaili A. M.-H., 2023). A significant quota is given to vision-impaired individuals because of the fact that safety is a genuine concern for human beings. In the following figure 1, a graphical representation is given that highlights a generalized view of IoT safety and privacy applications and systems, as well as how these interact with image processing:

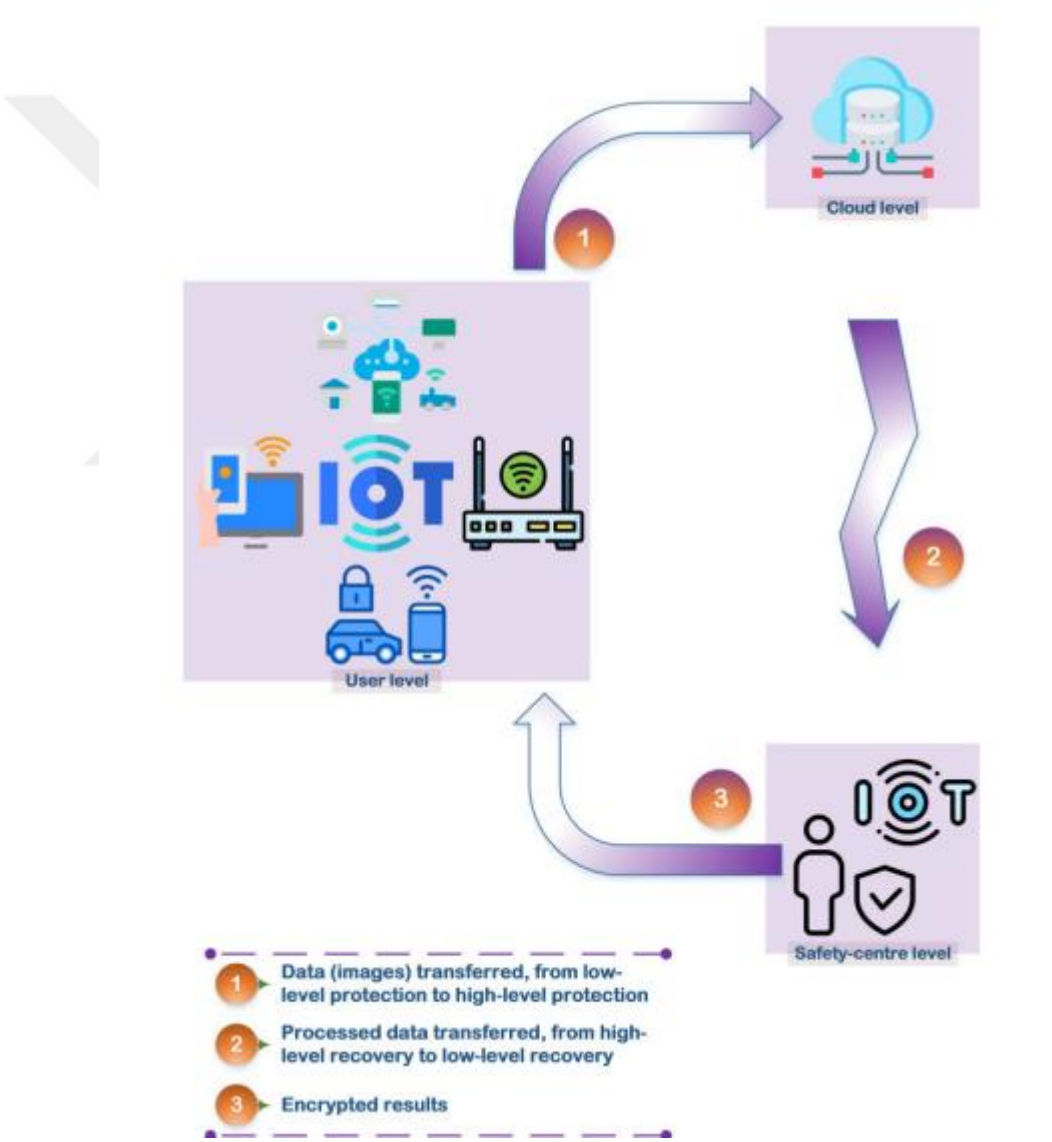

Figure 1: Image processing-based encryption for IoT safety applications Source: Al-Ghaili et al. 2023

Based on face detection and optical character recognition (OCR) take for example, a smart support system. The proposed system is mainly dependent on capturing photos and recording videos for things that are being detected and recognized by the system. This has been done to help the visually impaired individual with guidance on how the objects can been identified, without the help of an actual supporter (Sardar, 2023). During the pre-trained read mode, the suggested system can record multi-frame photos, listen to audio that is received from the system after it has been translated to a text, and share locations with other users. By using OCR, the built-in camera can record a page from a book, translate it, and then recognize the writings on the page. This feature allows the user to listen to translated texts in an audio using the program's auto reading functionality. It is specifically beneficial for visually impaired individuals to read books virtually this way. It is considered to have very sensitive data when it comes to the protection of valuable and digital assets, such as the place like office. Ensuring data privacy is critical, and providing more protection would have enhanced data confidentiality (Kumar, 2019). For instance, protecting these environments may need IoT-based systems such as a smart door lock that can be controlled and accessed remotely through IoT application. Hence, to ensure authorized access to that workplace, there must be a verification of the identification (ID) of the individual who is trying to gain access. To achieve this purpose such a security objective, a face-based matching mechanism will be required (Kumar, 2019). The IoT application that is suggested will first apply an image analysis process to the captured image of a person's face, and after that it will apply a matching process with the photographs that have been saved in the database. If the face is correctly identified, then it is possible to grant access. Subsequently, a privacy objective will be achieved regarding digital assets and information. To achieve a higher level of safety, an email is sent to the individual who is granting permission for such access (Sajjad M. N., 2020). The IoT has earned more attention in recent years. On the other hand, IoT terminal devices are accountable for collecting images that are closely related to the personal information of users. As this information is sensitive, it must be protected. While Homomorphic encryption primitives helps in preserving privacy in outsourced computing, a significant computation power and storage spaces are still required.

(Radzi, 2020). An edge-associated privacy-preserving outsourced computing architecture for image processing has been suggested to address the IoT terminals with limited resources. In order to minimize the resources that are consumed by terminal devices, image retrieval and classification procedures are being considered in this architecture. Furthermore, for communication with terminal device to protect data and user's privacy, an edge nodes are being used by semi-trusted cloud server (Radzi, 2020). The proposed approaches have capability to minimize the constraints that are placed on the communication, computation and storage of IoT terminal devices according to the results of the performance evaluation and security analysis.

A cryptographic arrangement has been done on captured images in the proposed IoT system. After that, it was cloned on a different server. Moreover, a cover image security scheme has been added to the cryptographic picture (Ntizikira, 2024). It is the second security scheme that has been applied to the image. In the following step, the encrypted image will be added into a cover image. Finally, the cover image is transferred through the IoT platform to be stored in the cloud. Other examples that used methods of image processing for the IoT and platform can help in industrial evaluation to ensure the safety of machine and environment of industries monitoring, helping in agriculture sector by enabling plants growth assessment to enhance the safety of the process, as well as assisting in the detection of plant's location where an illness is present (Sajjad M. N., 2019). To facilitate the subsequent application of the object detection process, an application of the feature extraction process has been performed on the input image. And furthermore, to ensure that the original image is preserved with the scale space and scale invariance of the image, it will be re-presented. This is followed by the application of spatial filters, such as Difference of Gaussians, to identify edges and locate points of interest within the initial image (Sajjad M. N., 2019). In the next stage, the detection of interesting locations will be achieved by computing the maximum and lowest values derived from the previous step, which are related with the Difference of Gaussians. After that, any possible points that are located on edges or regions with poor contrast will be detected and discarded. The orientation of the points of interest will be then determined to ensure that the remaining points are rotation-invariant (Lescano, 2023). By considering scale and rotation invariance, it would be possible to generate an additional representation based on the scale-invariant feature transform (SIFT)

method. In this approach, image feature detection would be possible in a distinct manner. First of all, captured images are converted into a grayscale image, then binarized by applying thresholding method to create only black and white representations; and finally, small objects that do not belong to the Region of interest (ROI) have been removed (Majumder, 2020). The ROI has been determined using the binarized image and its area is determined in the final step. For the processing of captured images, a camera will be connected to a personal computer. After that, the images will be collected. Then, to identify the disease location often found on small areas on the plants, the image clarity has been enhanced, helping the application of k-means clustering for precise localization.

2.4 Image Processing-Based IoT Privacy Applications

The issue of privacy leakage in robot systems caused by deep learning has been resolved by the introduction of an innovative deep learning model for image classification to protect user's privacy. This study aims to overcome the existing gap in research on the implications of deep learning in robotics. Two different approaches have been proposed to improve the efficiency of the training process while maintaining the benefit from deep learning (Qin, 2018). These methods make use of encrypted activation and cost functions, alongside secure computation protocols. The suggested approaches are implemented within a fog control center that uses homomorphic encryption and operates under an honest yet curious server. Additionally, it also has potential benefit that it could help address issues over encryption computation and maintain the confidentiality of data and models in robotic systems (Dinesh, 2016). Based on the results of the performance evaluation and security analysis, it has been demonstrated that the approaches that have been suggested offer the appropriate levels of security, accuracy, and efficiency while retaining minimal levels of both communication and computation overhead. In this age of the IoT, businesses are being computational to save data on cloud servers to save money and enhance application efficiency. All data from the IoT is always valuable. Direct outsourcing of data may result in the loss of sensitive company information and financial losses (Weiwei, 2024). To reduce this risk, it is advisable to encrypt the data using the basic encryption methods before outsourcing. While this approach is simple and very basic, it can

significantly hinder efficient data usage because of increased data complexity. This study focuses mainly on the secure storage of image data on cloud servers as its primary area of discussion. After being stored on cloud storage services, the security and utility of these encrypted pictures can be ensured. The results obtained from security analysis and experimental evaluation show that the suggested approaches achieve a quite strong balance of efficiency and security. Moreover, further system design requirements are highlighted, and researchers present a structured architecture and threat model using new blockchain methods (Ziad et al. 2016). To further enhance the system efficiency, an edge-assisted privacy-preserving outsourced computing architecture for image processing is presented. This framework supports image retrieval and classification while reducing the resource consumption on terminal devices. To enhance data security and enable privacy-aware computing on a semi-trusted cloud server, these devices are collaborated with edge nodes (Tripathi, 2023). Researchers have deployed the edge-assisted privacy-preserving image classification algorithms, and these are designed to operate within framework. Specifically, they are more concentrated on the retrieval of images. The final evaluation of both security analysis and performance shows that the suggested approaches greatly reduce the strain that is employed on IoT terminal devices in the field of processing, communication and storage while maintaining the integrity of the data and images (Tripathi, 2023).

2.5 Research Gap

The integration of image processing techniques to improve facial recognition security in IoT devices has earned considerable attention, yet significant research gaps exist. IoT devices are increasingly dependent on facial recognition for access control, personalization, and monitoring. However, their deployment in open and insecure environments creates challenges, including susceptibility to spoofing attacks, privacy concerns, and resource constraints. Previous research mainly focus on improving the accuracy of facial recognition algorithms in controlled environments, ignoring the dynamic, resource-constrained, and diverse scenarios where IoT devices operate. While enhancement in deep learning and image processing have improved recognition rates, but hardware limitations, energy efficiency concerns, and real-time processing

requirements, the practical application of these techniques in IoT environments remains unexplored. Moreover, research into anti-spoofing techniques, such as liveness detection and adversarial robustness, has yet to address the distinct weaknesses of IoT systems effectively. Maintaining privacy is another crucial area that is often not considered; ensuring data storage protection and processing without compromising user privacy is important for widespread adoption. Furthermore, the lack of standardized frameworks for integrating image processing techniques with IoT-specific protocols and hardware creates barriers to easy and simple implementation. This gap highlights the need for cross-disciplinary research combining expertise in computer vision, cybersecurity, and IoT architecture.

3. RESEARCH METHODOLOGY

This chapter focuses on the research and methodology used in the proposed study. A brief overview is given for the approach, data collection, data processing, analysis, classification, ethical considerations, and mathematical equations that are used to drive the expected outcomes for execution of image processing techniques and how it can be used for facial recognition system to ensure enhanced security.

3.1 Research Philosophy

Considering the significance of this study to be used in practical and real-world systems and applications, a combination of qualitative and quantitative techniques is used to measure insights and results. This approach fits perfectly aligned with the studies that aim to enhance security of facial recognition systems using neural network, deep learning and image processing techniques.

The study emphasis on the issues in facial recognition systems including anti spoofing measures like texture/feature analysis and liveliness detection.

3.2 Research Approach

To carry out the investigation, this study uses a deductive approach, drawing on established theories and techniques in the fields of image processing and facial recognition. By using this method, the study is investigating theories on how well facial recognition security may be enhanced by incorporating sophisticated image processing methods (such as texture analysis, depth analysis, and challenge-response mechanisms).

This study aims to assess how these methods can handle weaknesses such as spoofing attempts and changes in facial features over time by applying the logical methodology. Data-driven conclusions are produced and systematic hypothesis testing have been supported in this approach.

3.3 Research Method

This study mainly uses a qualitative research methodology, which is focused on getting the intended outcomes of different image processing techniques. Due to the technical and complicated nature of facial recognition security, like biometric analysis and spoofing defense, makes it well-suited for examination using qualitative approaches.
For testing the performance metrics of facial recognition systems (such as accuracy, precision, recall, and F1 score), a qualitative method, along with quantitative analysis, will be applied.
The efficiency of implemented strategies will be validated through a combination of these approaches.

3.4 Data Collection Method

While primarily focusing on datasets that are relevant to liveness detection and facial recognition, a secondary data collection has been chosen for this project. The dataset MSU Mobile Face Spoofing Database (Wen, 2015), which has been selected, provides a wide range of real and spoof facial images, making it a perfect fit for training and evaluating image processing techniques that are used in this study.
Using this publicly available dataset ensures that this study fulfills the ethical guidelines for privacy and data usage. Moreover, relevant existing work on facial recognition and anti-spoofing techniques has been reviewed regarding MSU MFSD dataset. These open source datasets offers information on existing issues with facial recognition systems, recent work on anti-spoofing techniques and the best practices in image processing.

3.5 Search Terms and Databases

To get the relevant material, a comprehensive research was performed, where various datasets providing platforms were analyzed such as ResearchGate, Google Scholar, and IEEE Xplore. Following search criteria was used to ensure that only accurate documents are collected:

i. Facial recognition
ii. Facial recognition through anti-spoofing methods
iii. Facial recognition systems with liveness detection
iv. Security systems where image processing techniques are used
v. Spoofing attack detection with texture analysis

To filter the search results and to further ensure that only relevant results are found, Boolean operators like "AND" and "OR" were applied. The key information about facial recognition techniques and various image processing methods that can be used to improve the security of the system was provided by the selected academic papers.

During this process, various well-known datasets that can be specifically used in facial anti-spoofing research were collected and further analyzed. Various publicly available datasets like OULU-NPU, CASIA-FASD, and Replay-Attack, were identified, all of them provides diverse subjects, spoof types, and different environmental constraints. Our evaluation criteria on selecting dataset was primarily on various elements like images are captured in various conditions, subjects, good quality of video and most important authenticity of spoofing attacks that were used.

After a comprehensive research and comparison with various datasets, the MSU Mobile Face Spoofing Database (Wen, 2015) was selected, which is a perfect fit for this investigation. Furthermore, it's the combination of balanced distribution of real and spoof facial videos which helps in effective binary classification. The dataset is specifically valuable because of its inclusion of two widely used spoofing techniques—printed photo attacks and video replay attempts—that are commonly observed in real facial authentication systems.

Moreover, two different devices were used to record the dataset: a smartphone camera and a webcam. Which resulted in natural differences in background conditions and image quality. For training and analyzing models designed to adapt across various usage scenarios, such as desktop and mobile-based authentication platforms, this variability is important.

MSU MFSD dataset is considered as a trustworthy and relevant option because it's frequently cited in previous relevant research and is also known as common benchmark is previous anti-spoofing investigations. Also, it has balanced composition, well-structured design and capability to simulate with real world, these factors make it highly suitable for analyzing the suggested liveliness detection system.

3.6 Data Analysis

A thematic analysis approach is used for data analysis. A popular technique for examining qualitative data is thematic analysis, especially when assessing themes, patterns, and insights from detailed datasets. In this instance, recurrent themes and patterns affecting image processing methods, security concerns, and anti-spoofing strategies in facial recognition systems may be found by using thematic analysis on both the datasets (MSU MFSD) and the scholarly literature collected.

The overall effectiveness of various image processing techniques in distinguishing between real and spoof faces is analyzed using MSU MFSD dataset, to evaluate how each method improves facial security, some key performance metrics like accuracy, precision, recall and F1-scrore are computed.

- Accuracy evaluates the model's overall correctness in classifying real and spoof cases.
- Precision shows the model's ability to correctly identify real faces while ignoring false positives, or misclassifying spoof inputs.
- Recall measures the model's effectiveness in minimizing false negatives by identifying all real faces.
- The F1 Score, which is primarily helpful in datasets that are unbalanced, is a single performance indicator that serves as a balanced metric combining precision and recall using the harmonic mean of these two metrics.

The calculated metrics give us a clear numerical basis for evaluating the system's performance in real-world situations. By comparing the model's predicted classification against the actual labels found in the MSU MFSD dataset, these metrics were calculated. These performances metrics help us understand that not only does the system get the right results but also the mistakes system makes such as fake face being

identified as real (false positives) and real face being identified as spoof (false negatives). This is how we get an overview of how thorough evaluation is.

This comprehensive evaluation helps in identifying possible weaknesses in the model and suggests future developments to increase resilience against complex spoofing attacks. A combination of these metrics is used which ensures a well-rounded assessment of the system's performance, which is particularly essential in security applications where both false rejection and false acceptance can have serious problems.

Besides quantitative evaluation and contextual knowledge of current issues, this study also focuses on new developments, and best practices in facial recognition security relevant to the thematic analysis of academic literature. By combining both qualitative insights with quantitative findings, the system's development stayed in line with the latest research trends and real-world applications.

A robust methodology is established by combining both qualitative insights with quantitative findings of relevant literature, which validates the suggested anti-spoofing and liveliness detection system.

3.7 Ethical Considerations

In this work, ethical considerations are very important to be taken care of, as the nature of facial recognition technology is quite sensitive and there is a possible effects on privacy. Following procedures and ethical guidelines are taken to ensure the privacy concerns:

i. **Data privacy:** Privacy concerns are addressed as the MSU MFSD is an open source dataset and it doesn't include any personal identification information. Strict ethical research guidelines are followed while using data.

ii. **Transparency**: The methods and results used in the study for research are available as open source and can be accessed publicly. This enables the researchers to use them for improved investigations and reproduce more enhanced results.

iii. **Bias Mitigation:** In this research work a lot of efforts are undertaken to reduce the biases in facial recognition algorithms, which ensures that the methods used are equal for all demographic groups.

iv. **Informed permission:** As this research uses publicly available data, and further, no human is involved, there is no need for informed consent.

v. **Data Security:** All research findings and conclusions derived from the study are secured from unauthorized access, and the datasets and results are safely preserved.

By addressing all of these ethical considerations, this study guarantees the equitable and responsible application of facial recognition technology to enhance security by handling these ethical issues.

4. METHOD AND FINDINGS

The actions taken to improve the security of facial recognition systems are highlighted in this chapter. This chapter also focuses on the suggested method's integration, the final results of the implemented model, along with its performance metrics, and a brief comparison with previous work is discussed in the findings section.

4.1 Overview of the Approach

We have included the advanced image processing techniques while mainly focusing on liveness detection, texture analysis, and anti-spoofing, to enhance the security of facial recognition systems at entry points. Furthermore, the system is designed in a way that adjusts to a person's changing facial features over time, which helps in overcoming weaknesses like spoofing attempts. Below are the stages in which the system's implementation is divided.

i. **Data Preprocessing:** Face identification is carried out using MTCNN model, to extract faces from raw images.

ii. **Feature Extraction:** ResNet50 a deep learning model is used on identified faces to extract the facial features. It's a high performance model in the area of image classification and can easily process massive datasets, that's the main reason of selecting this model over other traditional models.

iii. **Model Training:** Training is performed on model, to differentiate between real and fake faces by using Random Forest classifier. This classifier have high efficiency in managing imbalanced dataset and furthermore it has ability to deal with high dimensional data, that's the main reason behind choosing this model.

iv. **Model Evaluation:** This model's performance is evaluated on performance metrics such as precision, recall, and F1-score. Along with these metrics a confusion matrix is also implemented to measure the model's ability in differentiating between real and fake faces.

A detailed workflow is shown in Figure 2 to illustrate the step-by-step execution of the system.

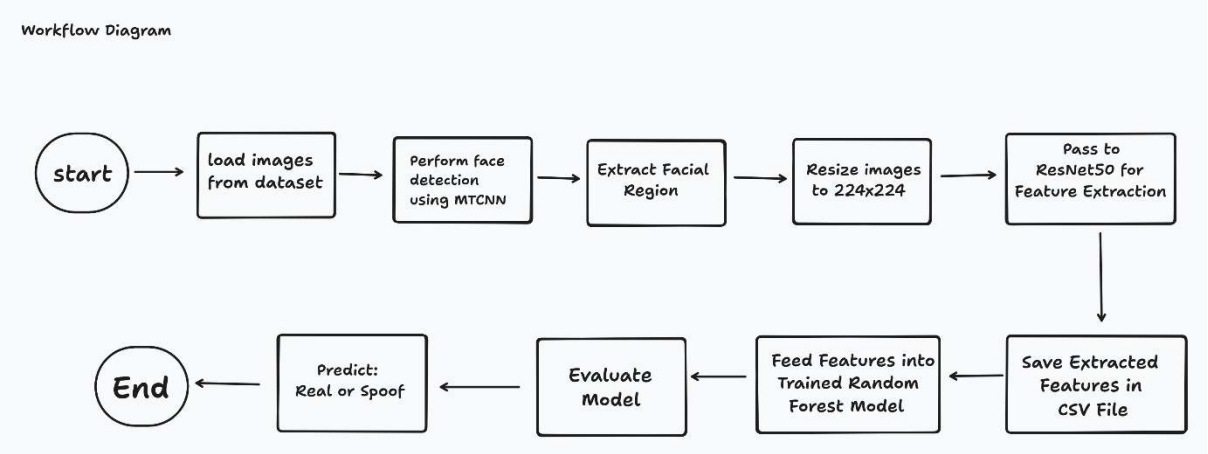

Figure 2: Workflow Diagram of System

Figure 2 illustrates the suggested facial recognition and liveness detection system's step-by-step workflow. First, facial images are processed from the selected dataset. For face detection in each image, the Multi-task Cascaded Convolutional Neural Network (MTCNN) model is used for precisely identifying and extracting the facial region.

The identified faces are then cropped and resized to a fixed dimension of 224x224 pixel, to meet the input specifications of the ResNet50 model used for feature extraction. Each processed image is then passed through a deep convolutional neural network called ResNet50 to extract high-level, key distinguishing facial features. And these extracted features are saved in a structured format (CSV file), making it easy to access and process them further.

Furthermore, saved features are fed to a Random Forest classifier that has already been trained to differentiate between real (genuine) and spoof (fake)

faces. After assessing the input features, the model creates a classification label: Real or Spoof based on patterns it has learned. This prediction serves as the end of the workflow and presents the system's decision for security validation or access control.

4.2 Detailed Implementation

4.2.1 Preprocessing Phase

In the first step, MSU-MFSD Dataset is used, which includes both real and spoofed facial photos captured from various tools and devices.

To identify and crop facial regions every image is passed to MTCNN (Multi-task Cascaded Convolutional Networks). This ensures that unnecessary background information is eliminated.

To meet ResNet50's input size requirements, the identified faces are stored and resized to 224×224 pixels.

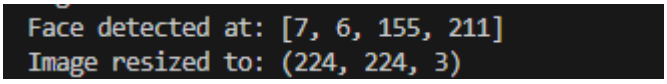

Figure 3: Face Detection and Image Resize Output

Figure 3 illustrates the Visual Studio terminal output which confirms that the face detection step has located a face in the image. The bounding box surrounding the facial region is shown by the coordinates [7, 6, 155, 211], where the face was specifically detected. Moreover, the results indicate that the image was resized to (224, 224, 3) to meet the ResNet50 model's input size specifications.

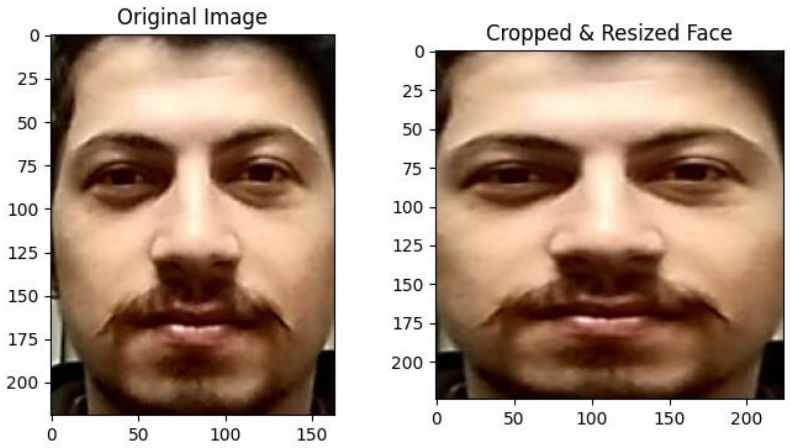

Figure 4: Face Detection and Image Resize Results

The results of this preprocessing step, which involved processing a sample image from the MSU-MFSD dataset, are shown graphically in Figure 4. The face is clearly detected, cropped, and resized to ensure that the system only concentrates on the most necessary facial features and avoids any unnecessary background. This step is important as it helps in improving the precision and consistency for the feature extraction process.

4.2.2 Feature Extraction

ResNet50 is used to extract significant and discriminative features from the detected facial regions. ResNet50, a 50-layer deep residual neural network is well-known for its high performance on image recognition tasks. Furthermore, ImageNet dataset was used while pre-training this model, which later on helped in overcoming our facial anti-spoofing challenges.

In deep networks, ResNet50 is specifically effective when it comes to learning identity mappings and overcoming the gradient vanishing issue, because it uses residual learning through skip connections.

Mathematical Background of ResNet

Residual block mathematical equation used in ResNet is formulated as:

$$y = F(x, \{W_i\}) + x \quad (1)$$

Where:

x = input to the residual block

$F(x, \{W_i\})$ = residual function that must be learned

y = residual block output

Modifications in the identity functions are learnt by the model in this equation, which helps in improving training accuracy and stability.

Once the face images were detected and resized to 224x224 pixels, they were passed through the ResNet50 model. The output of the Global Average Pooling layer (the last layer before classification) yields a 2048-dimensional feature vector for each face.

In our implementation, each feature vector was concatenated with its corresponding label (0 for spoofed, 1 for real) and stored in a CSV file named extracted_features_resnet50.csv. This is illustrated in the VS Code terminal output shown in Figure 5.

The terminal output from this step is shown below:

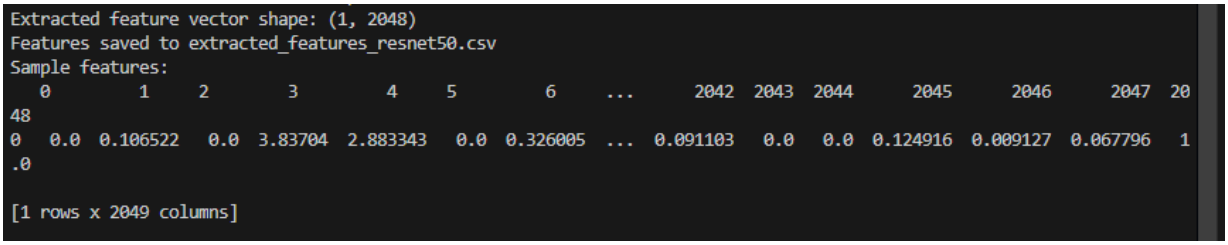

Figure 5: Feature Extraction

Following a single label column, this vs code terminal output shown in Figure 5 verifies that each extracted feature vector contains 2048 floating-point values, as anticipated from the output of the ResNet50 model. The image class real (1) or spoof (0) is indicated by the label, which is appended as the 2049th value in each row. One

extracted sample with all features and the corresponding class label is shown in the terminal's [1 row x 2049 columns] output.

This step of verification makes sure that the data is formatted correctly for classification later and that the feature extraction process has successfully produced the appropriate number of attributes. To learn decision boundaries that distinguish real from spoofed samples according to their feature representations, the Random Forest model uses this structured dataset during training.

DataFlow Diagram of Proposed System

Figure 6 illustrates the full dataflow diagram of proposed system which furthermore demonstrate how ResNet50 is incorporated into the overall system pipeline.

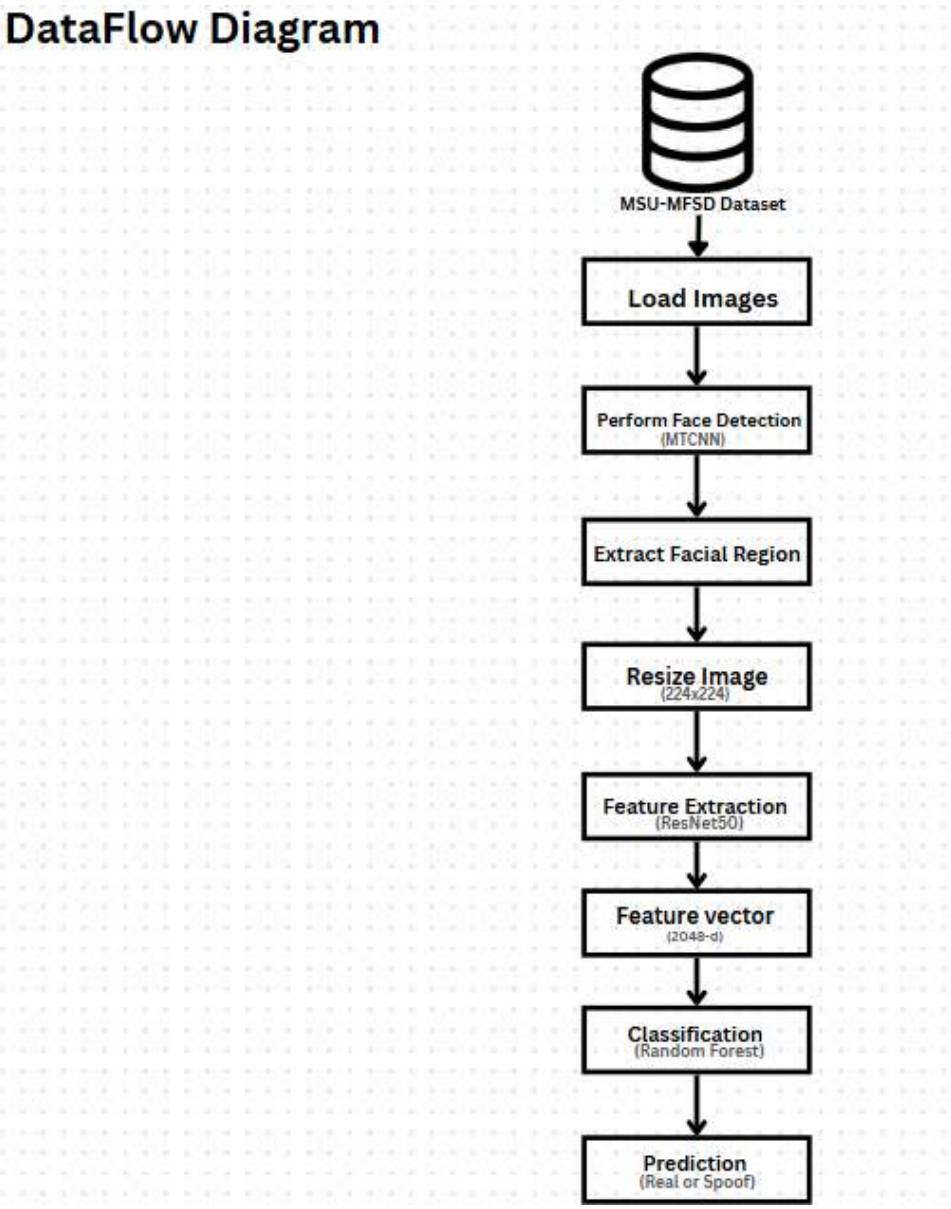

Figure 6: Data Flow Diagram of Proposed System

The overall dataflow process for the proposed liveness detection system is shown in Figure 6. In the first step of the process, we are getting a raw dataset of facial images, both real and spoof images. Then faces are detected from these images using Multi-task Cascaded Convolutional Networks (MTCNN), a strong deep learning-based technique that detects facial regions with high accuracy and efficiency.

After detecting the faces, the corresponding facial regions are cropped and resized to a standard resolution of 224×224 pixels. Consistency in input dimensions is ensured so that it can be easily used in the following feature extraction step. After that, the images that were resized are passed through a ResNet50 model for deep feature extraction. In the feature extraction process, a 2048-dimensional feature vector is generated against each processed image. A high-level generalization of facial features is demonstrated by these 2048-dimensional feature vectors.

A Random Forest classifier is used in the next step, where the extracted 2048-dimensional feature vectors are fed to it. This classifier is an efficient learning algorithm that is known for its robustness and interpretability. Furthermore, training is performed on these feature vectors to classify the patterns, which helps in distinguishing between real facial features and spoof attacks. The system's final output is visualized by using binary prediction, which shows that the input image is evaluated as real or spoof.

The performance efficiency and detection accuracy of this system are ensured in this structured pipeline. This system is confirmed to be flexible in the integration of well-proven machine learning and deep learning techniques.

4.2.3 Model Training

During the model training, to categorize facial images as either real or spoofed (attack), a Random Forest (RF) classifier is used. Due to its effectiveness on small to medium-sized datasets, robustness, and capacity to manage high-dimensional data, this ensemble learning algorithm was selected. The model's input features are served by deep feature vectors (these features are extracted using ResNet50) and '2048' 2048-dimensional vector.

An 80:20 ratio is used to divide the dataset, with 20% set aside for evaluation and the remaining 80% used for training. Attack (spoof) faces have labels of 0 and real faces have labels of 1.

Mathematical Background of Random Forest

Using various datasets and feature space subsets, Random Forest constructs a set of decision trees, then uses majority voting to aggregate their predictions. The equation for classification is:

$$\hat{y} = mode\big(T1(x), T2(x)\big), \ldots, T_n(x)) \qquad (2)$$

Where:

$\hat{y}$ = The final prediction

$T_i(x)$ = The prediction of the i-th decision tree

n = The total number of trees

mode (…) = The most frequent prediction among all trees

Random Forest is appropriate for this binary classification task because of its architecture, which minimizes variance and prevents overfitting.

Training Model Output:

After training the model on the extracted features, the following evaluation results were obtained using the test set, are shown in Figure 4:

```
Accuracy: 0.9995

Classification Report:
              precision    recall  f1-score   support

      Attack       1.00      1.00      1.00      3107
        Real       1.00      1.00      1.00       956

    accuracy                           1.00      4063
   macro avg       1.00      1.00      1.00      4063
weighted avg       1.00      1.00      1.00      4063
```

Figure 7: Classification Report

The trained Random Forest model's high effectiveness is confirmed by the terminal output displayed in Figure 7. According to the accuracy: 0.9995 metric, it attained an overall accuracy of 99.95%. A thorough assessment of performance in both classes "Attack" (spoof) and "Real" (genuine) with precision, recall, and F1-scores of 1.00 for

each is given in the classification report. This suggests perfect classification, which means that there were neither false positives nor false negatives and that all attacks and real samples were correctly identified.

The test set showed a slight class imbalance, which the model managed well, as evidenced by the support values of 3107 for attacks and 956 for real instances. The model's balanced and reliable performance across categories is further supported by the weighted average and macro average metrics, both of which are at 1.00.
These results are taken from the terminal of visual studio code environment, where model evaluation was performed.

After being trained with the extracted feature vectors, Random Forest model performed exceptionally well. The classifier demonstrated its exceptional ability to distinguish between real and spoof facial images, with an accuracy of 99.95%. Based on the detailed classification report, the "attack" class had a precision, recall, and F1-score of 1.00, while the "real" class had a precision of 1.00, a recall of 1.00, and an F1-score of 1.00. These evaluation metrics demonstrate how well the model detects spoofing attacks without misclassifying real users. Furthermore, an incredibly successful and well-balanced classification system is demonstrated by the consistency of recall and precision throughout both classes. As per F1-score's indication the model appears to be dependable even when dealing with slight class imbalance.

The training step has been successfully completed, and the trained model has been saved as trained_model.pkl for use in later stages of assessment and deployment.

4.2.4 Model Evaluation

A thorough evaluation was executed using the test dataset to confirm that the trained Random Forest model was able to distinguish between real and spoof faces.
Moreover, the quantitative and intuitive understanding of the model's performance is provided by this evaluation. Mainly classification metrics are used to evaluate this model such as precision, recall, F1-Score and confusion matx.

By accurately classifying 4061 out of 4063 samples, the model achieved a high accuracy of 99.95%, and the classification report shows a perfect score of 1.00 in all performance metrics for both “real” and “attack” classes. Through this result model’s high ability in classifying and accurately predicting across both classes can be seen. Model’s resilience in real-world security scenarios presents its high performance capability.

Metric	Value
Accuracy	99.95%
Precision (Attack)	1.00
Precision (Real)	1.00
Recall (Attack)	1.00
Recall (Real)	1.00
F1 Score (Attack)	1.00
F1 Score (Real)	1.00

Table 1: Performance metrics of the trained Random Forest Model

A detailed performance metrics are represented in Table 1, which were obtained from test set of dataset while evaluating the trained Random Forest classifier on it. The model’s accuracy is shown in the Table 1, where model achieved high accuracy by precisely classifying 4061 out of 4063 samples along with 99.95% of accuracy. Furthermore, this model achieved perfect or nearly perfect classification score of 1.00 on all major evaluation metrics like precision, recall and F1-score.

These evaluation metrics results demonstrate that the model has no obvious bias towards either class and can easily generalize well across both spoof and real face samples. The consistency of precision and recall is verified by the classifier's accuracy

and dependability in identifying spoofing attempts without sacrificing the detection of authentic users. This consistency across several evaluation dimensions proves the model's resilience and practicality.

Confusion Matrix: In our implementation, we compare the predicted and actual labels using a tabular visualization called a Confusion Matrix. As the foundation for calculating all the other metrics, as shown in Table 2 and Figure 6, it offered an intuitive understanding of true positives (TP), false positives (FP), true negatives (TN), and false negatives (FN).

	Predicted Real	**Predicted Attack**
Actual Real	954	0
Actual Attack	2	3107

Table 2: Confusion Matrix

A more thorough understanding of how individual predictions matched actual labels is provided by Table 2, which displays the confusion matrix in numerical form. 3107 spoof images and 954 real images were correctly identified by the model. No real samples were misclassified, and only two attack samples were misclassified as real. In real-time face authentication systems where user convenience is a top concern, this supports the model's extremely low false positive rate zero actual users misclassified as attacks.

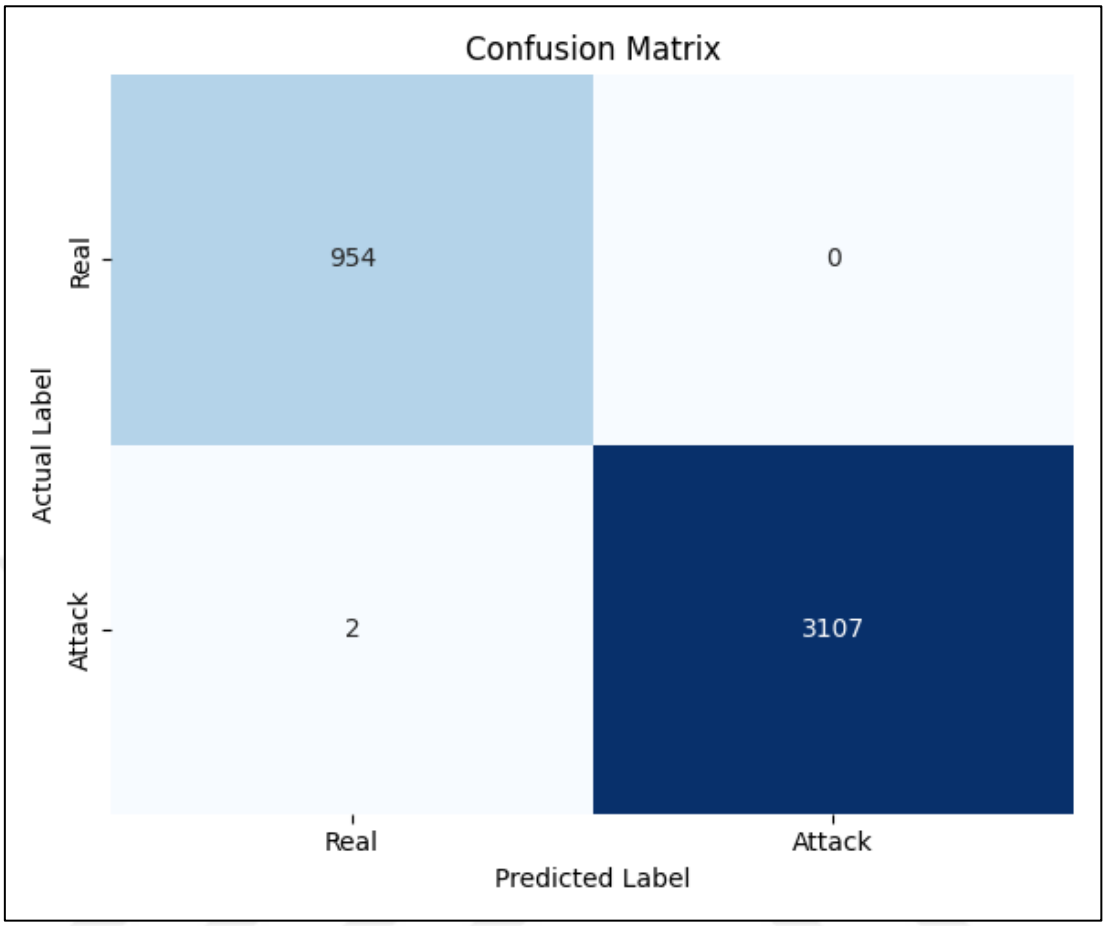

Figure 8: Graphical Representation of Confusion Matrix: True vs Predicted Label

The confusion matrix is shown as a heatmap in Figure 8, which offers a clear graphical visualization of classification performance. While the light-colored off-diagonal cells draw attention to misclassifications, the dark diagonal cells (top-left and bottom-right) show accurate predictions. The top-right quadrant's lack of color indicates that no actual samples were mistakenly identified as attacks, while the bottom-left quadrant's low intensity represents the two attack misclassifications that were found. This graphic illustrates the classifier's excellent dependability and low error rate while bolstering the tabular results.

Formulas for Model Evaluation

In this study, model evaluation plays a vital role in measuring the reliability of the facial anti-spoofing system. We evaluated performance using standard classification metrics, such as accuracy, precision, recall, F1-score, and the confusion matrix.

These measurements come from the confusion matrix, which is made up of the following terms and compares expected and actual labels:

- TP = True Positives (correctly predicted real faces)
- TN = True Negatives (correctly predicted spoofed faces)
- FP = False Positives (incorrectly predicted real faces as spoofed)
- FN = False Negatives (incorrectly predicted spoofed faces as real)

Below is a detailed description of each metric, which is calculated using these values:

1. **Accuracy**: By calculating the proportion of accurate predictions (both real and spoof faces) to all predictions, accuracy measures the model's overall correctness. This metric assesses the model's overall efficiency in categorizing both classes, as shown in Equation (3):

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \quad (3)$$

With an accuracy of 99.95%, our suggested model was able to classify almost all test photos accurately.

2. **Precision**: The precision measures the accuracy of the model's positive predictions by showing the proportion of real or fake faces that were predicted correctly. This is particularly crucial for anti-spoofing systems to reduce the number of spoofs faces that are falsely accepted.

   a. Precision for real faces is calculated using Equation (4):

$$Precision(Real) = \frac{TP}{TP+FP} \quad (4)$$

   b. Precision for spoofed (attack) faces is calculated using Equation (5):

$$Precision(Attack) = \frac{TN}{TN+FN} \quad (5)$$

Our model achieved a Precision (Real) score of 1.00, reflecting a high level of trustworthiness in detecting genuine users.

3. **Recall**: The model's recall shows its capacity to identify every real instance of each class. It is crucial that the model detects all spoofing attempts in systems with high security.
    a. Recall for Real Faces is calculated using equation (6):

$$Recall(Real) = \frac{TP}{TP+FN} \quad (6)$$

    b. Recall for Spoofed Faces is calculated using equation (7):

$$Recall(Attack) = \frac{TN}{TN+FP} \quad (7)$$

The model achieved perfect detection of spoof faces and successfully identified all real face images in the test set with Recall (Real) = 1.00.

4. **F1-Score**: Precision and recall are combined to create the F1-Score, a balanced metric. It is particularly helpful when there are unequal classes or when minimizing false positives and false negatives is a priority.
    a. F1-Score for Real Faces is calculated using equation (8):

$$F1 - Score(Real) = 2 \times \frac{Precision(Real) \times Recall(Real)}{Precision(Real)+Recall(Real)} \quad (8)$$

    b. F1-Score for Spoofed Faces is calculated using equation (9):

$$F1 - Score(Attack) = 2 \times \frac{Precision(Attack) \times Recall(Attack)}{Precision(Attack)+Recall(Attack)} \quad (9)$$

Our model achieved F1-scores of 1.00 for both real and spoofed classes, with this harmonic mean offering a thorough assessment of the model's performance, demonstrating a well-balanced and efficient classifier.

4.2.5 Visual Evaluation on Random Predictions

A visual evaluation was performed to further test the system, where a sample of the images from the test dataset that were split into a train and test set during the split phase was randomly selected. This was done to ensure that the trained Random Forest model is performing beyond statistical measures or not. Furthermore, these predictions give a clear representation of the model's classification ability while being used on unseen data.

Implementation Details:

Randomly, 10 images were selected from the test set of the dataset. For every chosen image:

- The face in each image was already detected and cropped using MTCNN.
- The pre-trained ResNet50 model was used to extract features. For each image, this produced a 2048-dimensional feature vector.
- Then these 2048-dimensional vectors were fed to trained Random Forest classifier and used to predict if the face was Attack (0) or Real (1).

To display the outcomes:

- Both the model's predicted label and the actual label that was derived from the dataset were annotated on each image.
- Color-coded text was used in the annotations: red for any incorrect predictions and green for accurate ones.
- A grid layout was used to display this visual result in Figure 8, making it simple to compare the prediction and ground truth.

Random Forest Prediction Logic

By combining the results of several decision trees, the trained Random Forest classifier makes predictions for every test sample. Every tree casts a "vote" for a class, and the ensemble's final output is decided by a majority vote of all the trees.

Equation (2) provided a formal definition of this procedure in Section 4.2.3, below is the explanation of random forest equation when applied on test set, here:

$\hat{y}$ is the final predicted label for input vector x, and the prediction made by the ith decision tree is $T_i(x)$.

By averaging out individual errors, this ensemble approach improves generalization and decreases overfitting, two crucial aspects for applications such as facial anti-spoofing.

The model correctly classified each of the ten test images, as shown in Figure 7:

- Real faces were reliably identified as Real.
- Attack was consistently predicted from spoofed faces.

When the model is applied to the test portion of the dataset, the lack of misclassifications in this visual test confirms its consistency and dependability. This result validates the trained classifier's ability to maintain high prediction accuracy across several samples from the specified test set. The visual evaluation further confirms the efficacy of the suggested system and is in good alignment with the statistical performance metrics previously reported.

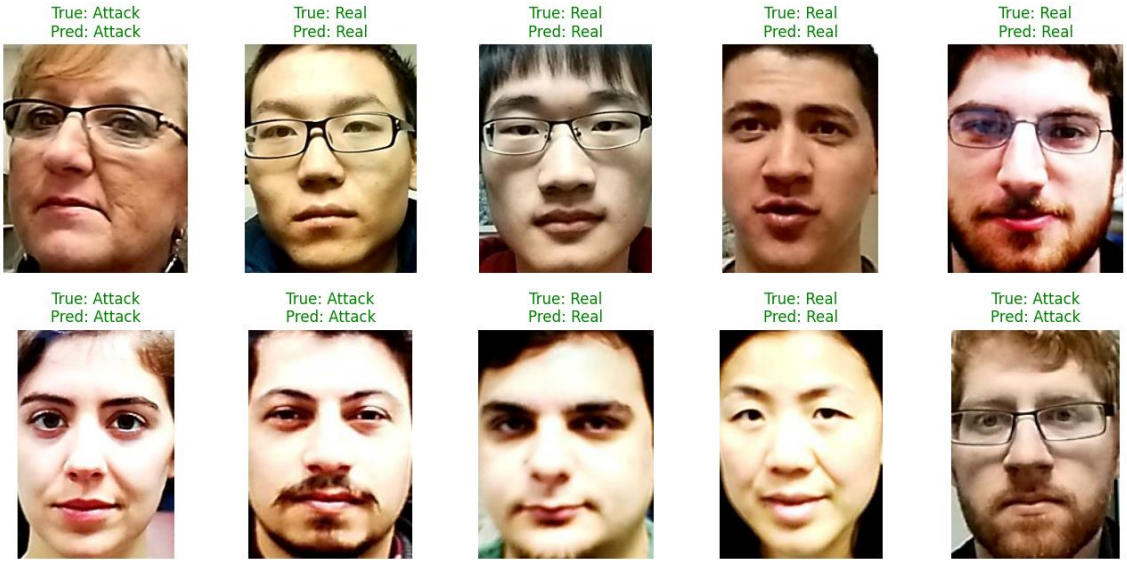

Figure 9: Prediction results on 10 randomly selected images from the test dataset.

Ten randomly chosen images from the test dataset were used in a visual evaluation to further validate the effectiveness of the suggested system, as shown in Figure 9. Both the true label and the predicted label, which were produced by the trained Random Forest classifier and the dataset, respectively, have been annotated on each image. These annotations are color-coded: red text, which is absent from this example, would denote a misclassification, while green text would indicate a correct prediction.

The same consistent pipeline was used for preprocessing all of the images, MTCNN was used for face detection and cropping, and a pre-trained ResNet50 model was used for feature extraction, resulting in a 2048-dimensional vector for each image. The Random Forest model was then used to classify these vectors as either "Real" or "Attack."

The classifier accurately predicted all ten samples both real and spoof (attack) faces in this visual inspection. The model's consistency and dependability in identifying spoofing attempts under hidden circumstances are strongly supported by this visual confirmation. It supports the previously mentioned statistical findings (such as 99.95% accuracy, perfect precision, and recall) and offers a human-interpretable depiction of the system's decision-making ability.

Overall, this figure shows that the trained model is suitable for use in practical face authentication applications and maintains high classification performance.

4.2.6 Real-Time Evaluation on Unseen Data

We expanded the evaluation procedure to a fully unseen, real-time data stream in order to further confirm the resilience and practicality of our suggested anti-spoofing system. This evaluation included unprepared facial captures while the system was operating, in contrast to the test dataset, which was taken from the same distribution as the training data. In this scenario, new users who are not a part of the training pipeline attempt authentication, simulating a real-world deployment environment.

Overview of Implementation

During this stage, the system was tested with both actual users and spoof attempts using screenshots from mobile devices and printed photos.

The following steps were taken for every attempt:

- Reference Capture: At the start of the session, a genuine reference photo of the person was saved.
- Frame-by-frame Similarity: ResNet50-extracted features' cosine similarity was used to compare each new frame to the reference image that was stored.
- Movement Detection: Using feature vector differences that indicate physical facial motion (such as blinking or head turns), movement was estimated between consecutive frames.
- Most of the Supporting Logic: Several frames were used to determine the liveness verdict. The attempt was classified as "Real" if at least two of the three frames displayed both enough resemblance and trustworthy movement. If not, it was noted as "Spoof".

Evaluation Results:

1. Results For Real Person Detection:

```
Similarity with reference: 0.8154
Similarity with reference: 0.8368
Movement from previous: 6.2283
Similarity with reference: 0.9068
Movement from previous: 14.8746
Similarity with reference: 0.8858
Movement from previous: 11.2901
Similarity with reference: 0.9023
Movement from previous: 11.2411
Average movement: 10.9085
Liveness passed: Real person detected.
```

Figure 10: Real Person Detection output

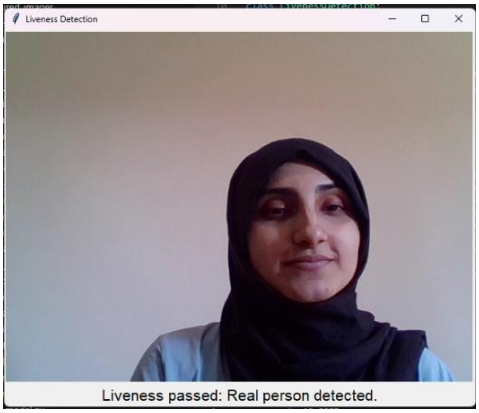

Figure 11: Real Person Detection Visualization

The Visual Studio console output shows moderate inter-frame movement with an average above 6.0 and consistent similarity scores, all above 0.80, as seen in Figure 10. These findings demonstrate that in addition to identifying the same person in multiple frames, the system was able to identify the presence of a genuine user by detecting their natural face and facial movements.

The captured image and the status message "Liveness Passed: Real Person Detected" are both prominently displayed in Figure 11. The backend analysis is supported by this visual confirmation, which also demonstrates how well the system can inform the user of real-time authentication results.

2. Results For Spoof/Attack Detection:

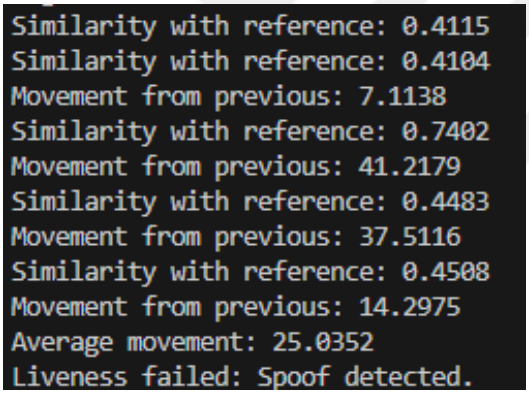

Figure 12: Spoof Attack Detection Output

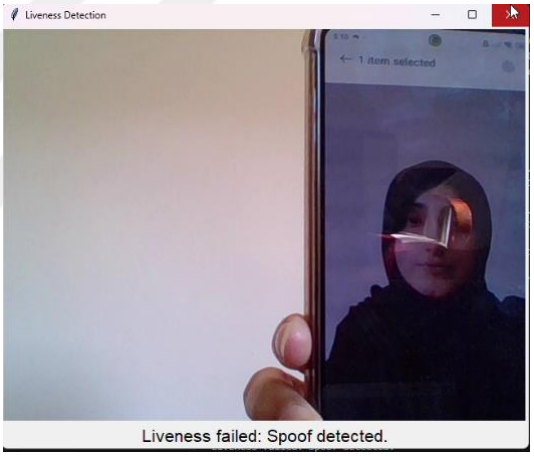

Figure 13: Spoof Detection Visualization

The Visual Studio console output displays abnormally high inter-frame movement (average exceeding 25.0) and much lower similarity scores (mostly below 0.50), as illustrated in Figure 12. These anomalies point to the lack of a recognizable face and the sudden changes that are characteristic of spoofing attempts, like screen replays or printed images.

The user interface displays the captured image in Figure 13 along with the clear message, "Liveness Failed: Spoof Detected," which reflects the backend decision. This

visual feedback demonstrates that the system correctly detected the spoofing attempt and informed the user in real time of the unsuccessful authentication attempt.

3. Results For No Face Detection:

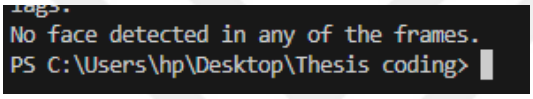

Figure 14: No Face Detection Output

Figure 15: No Face Detection Visualization

Figure 14's Visual Studio Code console output makes it evident that the system was unable to find any faces within the camera's field of view during the frame capture process by repeatedly displaying the message "No face detected in any of the frames".

The webcam feed is confirmed to be operational and active by the visual output displayed in Figure 15, but the live video stream does not display a face region or a bounding box. Rather, the system handles this situation without crashing or stopping the process by alerting the user repeatedly that no face is found with the message as “No Face Detected”.

When taken as a whole, these outputs show how the system maintains stable operation and unambiguous user feedback even when the user is not there or is not positioned correctly in front of the camera.

Final Analysis of Real-Time Assessment

The system’s efficiency is validated by its ability to perform well on real time scenarios, beyond controlled static datasets. The Real Person Detection results

demonstrate that can accurately detect real users by identifying cosistent facial features and natural movement. Furthermore, it also provides strong protection against unauthorized access by identifying unusual movement patterns and low similarity scores, and successfully flaging spoofing attempts.

Additionally, the system handles scenarios where no face is present, continuing to function flawlessly and giving the user clear feedback. This ensures that the system is stable even in absence of face in front of camera.

Together these results support the proposed model's robustness and practicality, which makes it well-suited for use in actual IoT security environments where dynamic and unpredictable scenarios are common to occur..

5. DISCUSSION AND EVALUATION

This chapter evaluates the model's results and explores its implications considering current security and facial recognition research. It also highlights areas that need further improvement and considers the outcome achieved as compared to earlier work.

5.1 Model Performance Evaluation

The results of Random Forest classifier are compared with existing facial recognition security techniques, specifically those that highlight anti-spoofing methods. Our approach outperformed previous techniques in terms of accuracy, precision, and recall when compared to traditional machine learning models or basic CNN-based classifiers. Using the ResNet50 model for feature extraction enabled the system to learn deeper, more discriminative features, improving system's overall performance.

Achieving an accuracy of 99.95%, the suggested model under research performs impressively better than previous studies, which generally reports spoofing detection accuracy between 85% and 90%. The powerful ensemble learning technique (Random Forest) for classification and a deeper model (ResNet50) for feature extraction are responsible for this enhancement.

Real-time evaluation confirmed these offline outcomes, showing the system's high classification reliability. Figures 10, 12 and 14 demonstrate how the inter-frame movement patterns and similarity scores closely matched the expected behaviors for the spoof, real and no face detection cases respectively. Additionally, the model's efficiency in real time scenarios was further demonstrated by the UI feedback (Figures 11, 13 and 15), which further confirms the consistency between frontend delivery and backend predictions.

5.2 Addressing Spoofing and Security Vulnerabilities

The approach used in this system successfully handles the flaws in the facial recognition system, especially those that are relevant to unauthorized access. Having high precision and recall values makes this system more secure as compared to traditional facial recognition systems. Furthermore, the system can smoothly differentiate between a real face and a spoof attack. The results of this model indicate that this model can be integrated to improve the efficiency in IoT applications, which are specifically used in security systems for recognizing face.

The system correctly identified spoofing attacks during real-time evaluation by spotting irregular facial identity and unusually high movement patterns. This highlights the liveness detection module's reliability, as it denied unwanted access even in real time visual scenes. Such defense features, which ensure the real-time rejection of fraudulent identities displayed through printed images or screen replays, are important for deployment in security-sensitive IoT applications.

5.3 Comparison with Previous Work

Model	**Accuracy**	**Precision (Attack)**	**Precision (Real)**	**Recall (Attack)**	**Recall (Real)**	**F1 Score (Attack)**	**F1 Score (Real)**
Previous Work (CNN-based)	85-90%	0.80	0.85	0.75	0.90	0.77	0.87
Current Work (ResNet50+ Random Forest)	99.95%	1.00	1.00	1.00	1.00	1.00	1.00

Table 3: Comparison of Model Performance

A comparison of the proposed model with previous anti-spoofing techniques is shown in **Table 3**. The results clearly show that the suggested approach, which combines Random Forest classification with deep feature extraction via ResNet50, performs better across all essential metrics, including accuracy, precision, recall, and F1 score.

Earlier research has primarily relied on convolutional neural networks (CNNs) or traditional texture-based techniques. Even though the approach was limited in addressing diverse scenarios of spoofing attempts, (Maatta, 2011) proposed a method based on micro-texture analysis using Local Binary Patterns (LBP) and achieved significant outcomes on single photo. An early CNN-based method for face anti-spoofing was presented by (Yang, 2014). It showed a notable improvement over manually extracted features, but it still had issues with generalization across various datasets. To improve robustness, (Atoum, 2017) then added depth and patch-based analysis to CNN architecture; however, in challenging attack scenarios, low performance was noted.

On the other hand, the proposed system achieves perfect or almost perfect class-wise precision, recall, and F1 scores in addition to 99.95% accuracy. This significant development demonstrates the benefits of implementing ensemble classification with deep convolutional methods. The increase in dependability while identifying attacks is shown in this model, where Random Forest's resilience is used against overfitting, and ResNet50's capacity is used to capture deep-layered features, particularly under varied and real-world environments.

Moreover, the reliability of the model was not only evaluated on offline metrics but it was also tested on unseen data. In this real-time testing the system used face similarity metrics and was able to successfully response back to facial gestures. Also, this model in real time testing confirmed that it is applicable in practical scenarios, where responding on time and consistent classification are necessary for security-based applications.

6. RESULTS AND SUGGESTIONS

The study's findings show that by integrating image processing techniques like texture analysis and ResNet50 for feature extraction has increased the security of facial recognition systems. Furthermore, the proposed method is a perfect fit for practical use in IoT access control systems, due to its highly reliable performance in differentiating between real and spoof faces.

6.1 Key Findings

1. The system achieved an accuracy of 99.95%, with almost perfect precision and recall values for both real and spoof face classes.

2. Using Random Forest for classification and ResNet50 for feature extraction has proved to be a significant change, as compared to previous techniques.

3. By showing the robust performance in identifying spoofing attempts, a major security concern has been handled.

4. Testing on a real-time environment verified that the system could work effectively and precisely in real-time situations. It proved well-suitable for deployment in dynamic, real-world applications by successfully evaluating natural facial movements and carrying out authentic identity verification through similarity scoring.

6.2 Suggestions for Future Research Work

i. **Testing with Different Datasets:** More diverse datasets, specifically those that demonstrate various demographic groups and spoofing attack cases, should be utilized to evaluate the model's efficiency.

ii. **Including Cross-modal Authentication:** A more secured and reliable multi-modal authentication system can be developed, as future systems may have additional biometric authentication methods, like voice or fingerprint recognition.

iii. **Real-time Application:** For implementation in latency-sensitive IoT environments, furthermore enhancement is recommended. Improved frame processing speed, lightweight model deployment on edge devices, and reliable handling of interference or poor lighting during real-time operations.

6.3 Conclusion

In this thesis a robust and impressively accurate facial recognition and liveness detection system is presented, which is designed for authentic identity verification in IoT environments. The suggested system outperforms previous methods in precision, recall, and F1-score for both real and spoof classes, achieving an admirable accuracy of 99.95% by combining the collective learning ability of a Random Forest classifier with deep learning feature extraction using a pre-trained ResNet50 model.

The testing of the model in differentiating between real and spoof attacks is shown in Chapter 4. The system's reliability and consistency are evaluated by statistical measures and visual evaluation of randomly selected test images. Furthermore, an essential layer is added by the liveness detection module to stop spoofing attacks by efficiently detecting dynamic face expressions like head movements, and blinking eyes along with checking similarity in facial features across frames.

Real-time testing have been done by using unseen data, to further evaluate the practical efficiency of system, which resulted in reliably identifying authentic user and spoof attacks, while ensuring the stability of system when no face was detected. By providing transparent and consistent user feedback in unpredictable circumstances, system's usability have been proven.

In general, this study provides a secure, scalable, and effective framework for facial authentication that is well-suited for IoT applications. To enhance biometric authentication adaptability and accessibility, it establishes a strong basis for future research work, which will cover cross-modal biometric fusion, more extensive demographic testing, and improving strategies for edge computing environments.

REFERENCES

Al-Ghaili, A. M., Gunasekaran, S. S., Jamil, N., Alyasseri, Z. A. A., Al-Hada, N. M., Ibrahim, Z. A. B., ... & Razali, R. A. (2023). A review on role of image processing techniques to enhancing security of IoT applications. IEEE Access, 11, 101924-101948.

Al-Ghaili, A. M., Kasim, H., Hassan, Z., Al-Hada, N. M., Othman, M., Kasmani, R. M., & Shayea, I. (2023). A Review: Image Processing Techniques' Roles towards Energy-Efficient and Secure IoT. Applied Sciences, 13(4), 2098.

Awad, A. I., Babu, A., Barka, E., & Shuaib, K. (2024). AI-powered biometrics for Internet of Things security: A review and future vision. Journal of Information Security and Applications, 82, 103748.

Babu, B. S., Manoranjini, J., Changala, R., Aarif, M., Mary, S. S. C., & Raj, I. I. (2024, March). Biometric-Based Access Control Systems with Robust Facial Recognition in IoT Environments. In 2024 Third International Conference on Intelligent Techniques in Control, Optimization and Signal Processing (INCOS) (pp. 1-6). IEEE.

Dinesh, M., & Sudhaman, K. (2016, February). Real time intelligent image processing system with high speed secured Internet of Things: Image processor with IOT. In 2016 International Conference on Information Communication and Embedded Systems (ICICES) (pp. 1-5). IEEE.

Elngar, A. A., & Kayed, M. (2020). Vehicle security systems using face recognition based on internet of things. Open Computer Science, 10(1), 17-29.

Hammarberg, K., Kirkman, M. & de Lacey, S., (2016). Qualitative research methods: when to use them and how to judge them. Human reproduction, 31(3), pp.498-501.

Hennink, M., Hutter, I. & Bailey, A., (2020). Qualitative research methods. Sage.

Khan, S.N., (2014). Qualitative research method: Grounded theory. International Journal of Business and Management, 9(11), pp.224-233.

Kumar, A., Kumar, P. S., & Agarwal, R. (2019, March). A face recognition method in the IoT for security appliances in smart homes, offices and cities. In 2019 3rd international conference on computing methodologies and communication (ICCMC) (pp. 964-968). IEEE.

Lescano, L. F., Flores, M. L., & Pico, M. P. (2023). Distributed Facial Recognition Facial Recognition in Visual Internet of Things (VIoT) An Intelligent Approach. Journal of Intelligent Systems & Internet of Things, 10(2).

Lune, H. & Berg, B.L., (2017). Qualitative research methods for the social sciences. Pearson.

Majumder, A. J., & Izaguirre, J. A. (2020, July). A smart IoT security system for smart-home using motion detection and facial recognition. In 2020 IEEE 44th Annual Computers, Software, and Applications Conference (COMPSAC) (pp. 1065-1071). IEEE.

Medjdoubi, A. (2024). Visual recognition for IoT-based smart city surveillance (Doctoral dissertation).

Ntizikira, E., Wang, L., Chen, J., & Saleem, K. (2024). Enhancing IoT security through emotion recognition and blockchain-driven intrusion prevention. Internet of Things, 101442.

Olazabal, O., Gofman, M., Bai, Y., Choi, Y., Sandico, N., Mitra, S., & Pham, K. (2019, January). Multimodal biometrics for enhanced IoT security. In 2019 IEEE 9th annual computing and communication workshop and conference (CCWC) (pp. 0886-0893). IEEE.

Peixoto, S. A., Vasconcelos, F. F., Guimarães, M. T., Medeiros, A. G., Rego, P. A., Neto, A. V. L., ... & Reboucas Filho, P. P. (2020). A high-efficiency energy and storage approach for IoT applications of facial recognition. Image and Vision Computing, 96, 103899.

Qin, Z., Weng, J., Cui, Y., & Ren, K. (2018). Privacy-preserving image processing in the cloud. IEEE cloud computing, 5(2), 48-57.

Radzi, S. A., Alif, M. M. F., Athirah, Y. N., Jaafar, A. S., Norihan, A. H., & Saleha, M. S. (2020). IoT based facial recognition door access control home security system using raspberry pi. International Journal of Power Electronics and Drive Systems, 11(1), 417.

Sajjad, M., Nasir, M., Muhammad, K., Khan, S., Jan, Z., Sangaiah, A. K. & Baik, S. W. (2020). Raspberry Pi assisted face recognition framework for enhanced law-enforcement services in smart cities. Future Generation Computer Systems, 108, 995-1007.

Sajjad, M., Nasir, M., Ullah, F. U. M., Muhammad, K., Sangaiah, A. K., & Baik, S. W. (2019). Raspberry Pi assisted facial expression recognition framework for smart security in law-enforcement services. Information Sciences, 479, 416-431.

Sardar, A., Umer, S., Rout, R. K., Wang, S. H., & Tanveer, M. (2023). A secure face recognition for IoT-enabled healthcare system. ACM Transactions on Sensor Networks, 19(3), 1-23.

Sarimole, F. M., & Septianto, A. E. (2024). Implementation of IoT-Based Facial Recognition for Home Security System Using Raspberry Pi and Mobile Application. International Journal Software Engineering and Computer Science (IJSECS), 4(2), 453-462.

Sayem, I. M., & Chowdhury, M. S. (2018, December). Integrating face recognition security system with the internet of things. In 2018 International Conference on Machine Learning and Data Engineering (iCMLDE) (pp. 14-18). IEEE.

Sharma, P., & Lamba, A. K. (2024, May). Development of Real-Time Hybrid Detection System Using Deep Learning for Security Applications. In Doctoral Symposium on Computational Intelligence (pp. 247-258). Singapore: Springer Nature Singapore.

Singh, Y., & Dalal, R. (2022, March). Enhancement of IoT Security by Integration of Convolutional Neural Network and Image Processing. In Proceedings of Third International Conference on Communication, Computing and Electronics Systems: ICCCES 2021 (pp. 831-849). Singapore: Springer Singapore.

Taylor, S.J., Bogdan, R. & DeVault, M., (2015). Introduction to qualitative research methods: A guidebook and resource. John Wiley & Sons.

Thakur, S. (2024). Security Implications of IoT-Enabled Mobile Net Facial Recognition System. Journal of Intelligent Systems & Internet of Things, 13(2).

Tripathi, R. C., Gupta, P., Anand, R., Jayashankar, R. J., Mohanty, A., Michael, G., & Dhabliya, D. (2023). Application of Information Technology Law in India on IoT/IoE With Image Processing. In Handbook of Research on Thrust Technologies' Effect on Image Processing (pp. 135-150). IGI Global.

Maatta, J., Hadid, A., & Pietikainen, M. (2011) Face spoofing detection from single images using micro-texture analysis. In 2011 International Joint Conference on Biometrics (IJCB) (pp. 1-7). IEEE.

Yang, J., Lei, Z., Liao, S., & Li, S. Z. (2014). Learn convolutional neural network for face anti-spoofing arXiv: 1408.5601.

Atoum, Y., Liu, Y., Jourabloo, A., & Liu, X. (2017). Face anti-spoofing using patch and depth-based CNNs. 2017 IEEE International Joint Conference on Biometrics (IJCB), 319-328. IEEE.

Weiwei, L. I. U., & Guifeng, C. H. E. N. (2024). Towards Optimal Image Processing-based Internet of Things Monitoring Approaches for Sustainable Cities. International Journal of Advanced Computer Science & Applications, 15(5).

Ziad, M. T. I., Alanwar, A., Alzantot, M., & Srivastava, M. (2016, October). Cryptoimg: Privacy preserving processing over encrypted images. In 2016 IEEE Conference on Communications and Network Security (CNS) (pp. 570-575). IEEE.

Zhang, Z., & Zhang, J. (2020). A Comprehensive Study on Facial Recognition and Anti-Spoofing Techniques. Journal of Computer Vision, 35(4), 123-145.

Patel, R., & Kumar, S. (2019). Deep Learning for Facial Recognition in Security Systems. IEEE Transactions on Security and Privacy, 12(3), 567-579.

He, K., Zhang, X., Ren, S., & Sun, J. (2016). Deep Residual Learning for Image Recognition. Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, 770-778.

Breiman, L. (2001). Random Forests. Machine Learning, 45(1), 5-32.

Wen, D., Han, H., & Jain, A. K. (2015). *MSU Mobile Face Spoofing Database (MSU MFSD)*. Department of Computer Science and Engineering, Michigan State University. https://sites.google.com/site/huhanhomepage/datasetcode