IMPLEMENTATION OF A BIMODAL BIOMETRIC-BASED SURVEILLANCE SYSTEM

BY

KARIS OVURU

18CK024253

A PROJECT REPORT SUBMITTED TO THE DEPARTMENT OF ELECTRICAL AND INFORMATION ENGINEERING, IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE AWARD OF THE DEGREE OF BACHELOR OF ENGINEERING IN ELECTRICAL AND ELECTRONICS ENGINEERING.

SUPERVISED BY DR. MOSES OLANIYAN

JUNE 2023

DECLARATION

I hereby declare that I carried out the work reported in this project in the Department of Electrical and Information Engineering, Covenant University, under the supervision of DR. OLANIYAN MOSES I also solemnly declare that to the best of my knowledge, no part of this report has been submitted here or elsewhere in a previous application for the award of a degree. All sources of knowledge used have been duly acknowledged.

…………………………………….

KARIS OVURU

18CK024253

CERTIFICATION

This is to certify that the project titled " CONSTRUCTION OF A BIMODAL BIOMETRIC-BASED SURVEILLANCE SYSTEM" by Karis Ovuru, meets the requirements and regulations governing the award of the Bachelor of Engineering (Electrical and Electronics Engineering) degree of Covenant University and is approved for its contribution to knowledge and literary presentation

Supervisor 1: Sign: ______________________ ______________________

Name: Engr. Dr. Olaniyan Moses Date:

Head of Department Sign: ______________________ ______________________

Name: Prof. Emmanuel Adetiba Date:

Internal Examiner: Sign: ______________________ ______________________

Name: Date:

DEDICATION

ACKNOWLEDGEMENT

TABLE OF CONTENTS

DECLARATION..2

CERTIFICATION..3

CHAPTER ONE..8

CHAPTER TWO..13

CHAPTER THREE..47

CHAPTER FOUR..58

CHAPTER FIVE..59

LIST OF FIGURES

CHAPTER ONE

INTRODUCTION

1.1 BACKGROUND OF STUDY

Surveillance systems are crucial instruments to protect people and property in various settings, such as government buildings, airports, banks, and public spaces. Surveillance systems have increasingly used biometric technology due to their capacity to recognize persons because of their distinguishing traits, either behavioral or physical. [1]. Bimodal biometric systems that use both fingerprint and facial recognition technologies have gained significant interest in recent years due to their potential to enhance the accuracy and reliability of biometric authentication and surveillance systems.

The Gartner hype cycle for 2013 indicates that biometric identification methods are close to reaching their full potential and will boost productivity in the years to come. You typically do not need to remember your identification number or password when using merely biometric authentication (PIN); you simply need to provide a few physiological and/or behavioral traits related to you. [2].

This study proposes to improve bimodal biometric multi-factor authentication. To improve the precision and dependability of the identification process, this project intends to design a bimodal biometric-based surveillance system that includes both facial and fingerprint recognition.

With the help of facial and fingerprint scans, this bimodal biometric technology can identify people more accurately and dependably.

The technology incorporates liveness detection to guard against attempts to circumvent it via spoofing techniques and uses sophisticated algorithms to match and identify people based on their fingerprints and facial scans. The effectiveness of this new technology in precisely identifying people has been tested and analyzed in a controlled environment.

To improve security and access control, the technology is now being used in a variety of locations, including airports, governmental structures, and financial institutions. This system's objective is to offer a strong and trustworthy identification mechanism that can be applied in various circumstances to protect people's and places' safety.

Overall, a bimodal biometric-based surveillance system that uses fingerprint and facial recognition aims to provide an accurate, dependable, and secure identification method that may be applied to a range of situations. Combining facial and fingerprint modalities can be an effective method for increasing security and preventing identity fraud.

1.2 SIGNIFICANCE & MOTIVATION FOR THE STUDY

The importance of this research is in its ability to improve the accuracy and reliability of identification by combining the strengths of both fingerprint and facial recognition. By adding a layer of protection and lowering the possibility of false positives or false negatives, the bimodal biometric system overcomes the drawbacks of conventional uni-modal systems.[3]

The study will offer useful information about the functionality and efficiency of the bimodal system, which can be used to enhance and perfect the system for the next deployments.

The study will also contrast the bimodal system with conventional uni-modal systems to show the benefits of utilizing a bimodal strategy.

The findings of this work will have profound effects on many different fields and applications, including security, access management, and identity management, where precise and trustworthy identification is crucial.

1.3 AIM AND OBJECTIVES

1.3.1 AIM

This undertaking attempts to design and implement a bimodal biometric-based surveillance system to improve the accuracy and reliability of identification by combining the strengths of both fingerprint and facial recognition.

1.3.2 OBJECTIVES

The system's particular goals include:

- To design a system that can capture and store fingerprint and facial data.
- To implement facial and fingerprint recognition algorithms to create a bimodal biometric system.
- To assess the bimodal biometric system's operation's accuracy, dependability, and speed.

1.4 METHODOLOGY

The study employs a quantitative research method to gather and examine numerical data. The research design will be experimental, where the bimodal biometric system will be tested using a sample of individuals. The study will involve the following steps:

- Data collection: The study will collect facial and fingerprint images from a sample of individuals. The images will be stored in a database for use in the bimodal biometric system.
- Algorithm development: The study will develop facial and fingerprint recognition algorithms using machine learning techniques such as convolutional neural networks (CNNs).
- Bimodal system development: The facial and fingerprint recognition algorithms will be integrated to create a bimodal biometric system.
- Performance evaluation: The bimodal biometric system will be evaluated using a sample of individuals to determine its accuracy, reliability, and speed.

The project will be implemented using the following devices:

- Fingerprint scanner: This device will capture the fingerprint of the individual and convert it into a digital template for matching and identification.
- Camera: This device will capture an image of the individual’s facial features, which can be used for matching and identification.
- Raspberry Pi 4: the main aim of a Raspberry Pi is to serve as a compact and cost-effective computing platform for processing biometric data. It acts as the central processing unit in the bimodal biometric surveillance system, handling the data acquisition, pre-processing, feature extraction, matching, and decision-making tasks related to both fingerprint and facial recognition.
- Power supply: The biometric scanners and computer/server will require a stable source of power to operate.

1.5 PROJECT REPORT ORGANIZATION

Following is a quick explanation of each of the five chapters that make up this project: The project's idea, purpose, and objectives are discussed in Chapter 1. The second chapter looks at earlier and related research that is relevant to the topic and the literature review. Chapter 3 contains a comprehensive report on system design and execution. It displays the project's components. Chapter 4 contains an analysis and discussion of the findings. The final portion of the project, Chapter 5, offers thoughts on the findings and suggestions for additional research.

CHAPTER TWO

LITERATURE REVIEW

2.1 Introduction

The definition of terms, performance evaluations, review of related works, and real-world applications of bimodal fingerprint and facial biometric systems will abe covered in this literature review.

2.2 Definition of Terms

2.2.1 Biometrics

The utilization of distinctive physical or behavioral attributes to identify or confirm a person's identity is known as biometrics. These traits may consist of fingerprints, facial features, iris patterns, voice patterns, signature dynamics, or even voice patterns. Several industries use biometrics, including security, forensics, access control, and identification management. Biometrics aims to offer a quick, safe, and challenging-to-replicate method of confirming a person's identification.

2.2.2 Bimodal

Bimodal refers to the employment of a variety of modalities or approaches to complete a certain job or goal. Bimodal refers to the employment of multiple biometric modalities or approaches for the identification or authentication of biometric systems. Bimodal biometric technology combines the advantages of various biometric techniques to increase identification accuracy and reliability. For instance, a bimodal fingerprint and facial biometric system employ both facial and fingerprint scans to identify a person, adding an extra layer of protection and lowering the possibility of false positives or negatives.

2.2.3 Sensor

A sensor is a device that measures or detects a physical characteristic, such as temperature, light, sound, motion, or pressure, and then transforms that measurement into an electrical signal that a computer or other electronic device can read and interpret. Scientific research, industrial automation, and consumer goods are just a few of the many uses for sensors. Specialized sensors called biometric sensors are used to record biometric information like fingerprints, iris patterns, face features, etc. These sensors are used to record a person's biometric information, which is then processed by software to match and identify the person.

2.2.4 Biometric Matching Software

A person's identification can be verified or determined using biometric software based on physiological or behavioral traits like fingerprints, retinas or irises, voice and facial patterns, hand measurements, and speech patterns.

2.2.5 OpenCV

OpenCV (Open Source Computer Vision Library) is a well-known open-source software library for computer vision and machine learning. It offers a set of functions and algorithms for processing photos and videos, allowing for tasks like object detection, face recognition, image segmentation, and more. OpenCV is widely accessible because it supports a variety of computer languages, including C++, Python, and Java. It includes image filtering, feature recognition, and geometric transformations among its many capabilities for image and video analysis. OpenCV has become a critical tool for developers and academics working in computer vision, robotics, and related domains due to its vast set of features.

2.2.6 Python

Python is a widely used programming language for computers and it is used to create websites and applications, automate processes, and perform data analysis. It is a general-purpose language and can be used to develop a wide range of apps.

2.3 Related Works

2.3.1 “Sensor-assisted facial recognition: an enhanced biometric authentication system for Smartphones”

Muhammad Ejaz Ahmed, Majid Hussain, and Aboubaker Lasebae wrote a study in 2014 titled "Sensor-assisted facial recognition: an upgraded Biometric authentication system for Smartphones." To increase security and accuracy, the research suggests a new biometric authentication method for smartphones that combines facial recognition technology with sensor data.[4]

The authors highlight the benefits of facial recognition technology while discussing the drawbacks of conventional biometric identification methods like fingerprint recognition and PIN codes. They also point out that facial recognition technology alone is not always correct due to lighting, facial expressions, and other factors.

The scientists suggest incorporating sensor data from the accelerometer, gyroscope, and magnetometer to improve the accuracy of facial recognition to get around these restrictions. The accuracy of facial recognition in various lighting situations and facial expressions can be improved by using sensor data to track the user's head movement and the orientation of the phone.

The authors used a dataset of 500 photos taken in various lighting and face expressions to conduct tests to assess the efficacy of their suggested approach. The findings demonstrate that the suggested method, with an average accuracy rate of 96.6%, outperformed more established facial recognition systems in terms of accuracy rates.

The authors also review possible uses for their suggested method, such as e-commerce and mobile banking, where accuracy and security are crucial. They conclude that their suggested solution can offer a more reliable and secure means of biometric authentication for cell phones that are simple to integrate into already existing mobile applications.

In conclusion, the study recommends a cutting-edge biometric authentication system that combines facial recognition technology with sensor data to increase security and precision. The results of the trials the authors did to assess the effectiveness of their suggested method demonstrate that it attained a better accuracy rate than conventional facial recognition systems.

2.3.2 “Bimodal Biometric Verification with different fusion levels”

A bimodal biometric system that integrates the iris and facial modalities for identification is also suggested in a 2009 research paper by Anouar Ben Khalifa and Najoua Essoukri Ben Amara, titled Bimodal Biometric Verification with Different Fusion Levels. The efficiency and effectiveness of the bimodal system are investigated in the paper along with comparisons to those of unimodal systems.[5]

The suggested method begins by collecting the features from the iris and face modalities, respectively, using the Gabor filter and the Local Binary Pattern. Following that, the features are normalized and fused at many levels, including the decision, feature, and score levels.

The researchers employed the CASIA-IrisV3 database and the XM2VTS database, two publically accessible databases, to assess the efficiency of the suggested strategy. The findings demonstrated that, in aspects of the accuracy and false acceptance rate, the bimodal system performed better than the unimodal systems (FAR).

The study also discovered that the properties of the modalities and the particular application determine the appropriate fusion level. The maximum accuracy was sometimes obtained by fusing the scores at the decision level, while other times, fusing the features at the feature level was more successful.

The results of this study imply that the performance of bimodal biometric systems is significantly influenced by the fusion level. The properties of the modalities and the particular application might be taken into account to identify the ideal fusion level. Further study into the presented approach is intriguing because it can be applied to other biometric modalities.

The necessity for vast volumes of data to train the classifiers and the high computing cost of the fusion process are just two of the constraints of the proposed method that are covered in the study. To lower the computational cost of the fusion process, the researchers advise adopting parallel processing and efficient methods.

The research concludes with a thorough analysis of bimodal biometric verification with various fusion levels. The study's findings can be used as a guide for creating bimodal biometric systems that can deliver high reliability and accuracy in a variety of applications. The proposed strategy is promising for further study in biometric identification and authentication because it may be applied to different biometric modalities.

2.3.3 “Bimodal Biometric Identification with Palmprint and Iris Traits using Fractional Coefficients of Walsh, Haar, and Kekre Transforms”

In 2015 Dr. Sudeep D. Thepade and Rupali K. Bhondave suggest a new method for bimodal biometric identification using palmprint and iris traits.[6]

Bimodal biometric systems use two biometric features to improve identification accuracy and sturdiness. The Walsh, Haar, and Kekre transform' fractional coefficients are used in the proposed method to extract features from three separate transforms. These transforms are well-known for their capacity to extract valuable information from images and are frequently employed in image processing. The palmprint and iris images are represented by feature vectors made from the fractional coefficients of these transforms.

The features that were derived from the iris and palmprint pictures are combined using a weighted fusion approach in the suggested method. To maximize the effectiveness of the biometric identification system, the weights given to the traits are chosen using a genetic algorithm.

The researchers used a publicly accessible database including the palmprint and iris pictures of 200 people to assess the efficacy of the suggested method. The results of the studies showed that the recommended method exceeds existing methods in terms of accuracy, resilience, and effectiveness. The proposed method achieves an identification rate of 98.5%, which is significantly higher than the rates attained by existing bimodal biometric systems.

The study's findings show that the proposed technique could be used in actual biometric identification systems. The biometric identification system is more accurate and resilient thanks to the use of various transforms and a weighted fusion technique, making it appropriate for a variety of applications. The proposed method is a potential direction for further study because the genetic algorithm used to optimize the weights can be modified to work with different biometric modalities.

2.3.4“A secured automated bimodal biometric electronic voting system.”

The research paper titled "A secured automated bimodal biometric electronic voting system" written in 2021 by Kennedy Okokpujie, John Abubakar, Samuel John, Etinosa Noma-Osaghae, Charles Ndujiuba, and Imhade Princess Okokpujie uses two biometric authentication techniques to ensure security and prevent electoral fraud. The method is intended to overcome several problems with conventional paper-based voting systems, such as vote-buying, multiple voting, and ballot stuffing. [7]

Before allowing voters to cast their ballots, the proposed method combines fingerprint and facial recognition technology to verify their identity. The system uses a secure authentication mechanism that confirms the user's identity before giving access to prevent illegal access to the voting system.

The voter registration module, the authentication module, the voting module, and the vote-counting module are all included in the system design that is described in the paper. The system can be utilized in a variety of elections, including national, regional, and local elections, and it is also made to be scalable.

The system's implementation is discussed, and the authors provide information on how well it worked in a test election. The results were accurate and transparent, and the technology was able to reliably identify voters and prevent repeated voting. The authors also claim that integrating the method into current electoral systems was simple and cost-effective.

To prevent electoral fraud, the paper's conclusion introduces a secure and trustworthy electronic voting system that makes use of bimodal biometric authentication techniques. The technology can be readily integrated into current election systems and is made to be scalable and affordable. The study's findings indicate that the proposed system would be a good way to address some of the problems with conventional paper-based voting systems.

.

2.3.5 "Face-Iris Multimodal Biometric Identification System"

The research paper titled "Face-Iris Multimodal Biometric Identification System" by Basma Ammour, Larbi Boubchir, Toufik Bouden, and Messaoud Ramdani published in 2020 combines Iris and facial features to increase identification accuracy. According to the report, depending just on a single biometric trait might lead to false positives or negatives, which is why such a system is necessary. [8]

The suggested system is divided into three primary phases: multimodal fusion, face detection and identification, and iris detection and recognition. The researchers employed a pre-trained deep-learning model dubbed VGGFace for face identification and recognition. They made use of OSIRIS, a piece of open-source software, for iris detection and recognition.

Score-level fusion and feature-level fusion were the researchers' two strategies employed in the multimodal fusion step. In score-level fusion, the sum rule, product rule, and min-max rule were used to merge the scores from the face and iris recognition systems. In feature-level fusion, principal component analysis (PCA) and linear discriminant analysis were used to merge the information from the face and iris recognition systems (LDA).

The suggested approach was evaluated using the CASIA-IrisV3-Interval and LFW (Labeled Faces in the Wild) datasets. Using the CASIA-IrisV3-Interval dataset and the LFW dataset, respectively, the results demonstrated that the multimodal fusion system performed better in terms of accuracy than the unimodal systems (facial and iris recognition), with error rates of 0.31 and 0.38 percent, respectively.

The benefits and drawbacks of the suggested system are also covered in the article. Improved accuracy and increased resistance to spoof assaults are two benefits. The system's computational complexity and the requirement for high-quality photographs of the face and iris are some of its drawbacks.

In conclusion, the identification system put out in this research offers a viable strategy for increasing the trustworthiness of biometric identification systems. By multimodal fusion, the system's resistance to spoof assaults and boost identification is strengthened, and accuracy overall is increased. To solve the system's limitations and assess its efficacy on a larger scale, additional research is necessary.

2.3.6 "A context-aware Multimodal Biometric Authentication for cloud-empowered systems"

To improve security and usability in cloud-based systems, the research paper "A context-aware Multimodal Biometric Authentication for cloud-empowered systems" by Abdeljebar Mansour, Mohamed Sadik, Essa d Sabir, and Mohamed Azmi published in 2016 suggests an approach to authentication systems utilizing a combination of physical features and contextual data. [9]

Four biometric characteristics—face, fingerprint, voice, and keystroke dynamics—are used by the proposed system. These characteristics are recorded by a variety of sensors, including cameras, microphones, and touchscreens. To improve the authentication process even further, the system additionally takes into account the user's environment's context, including the location, time, and activity.

Enrollment, training, and testing are the three fundamental stages of the authentication procedure. The user's contextual data and biometric characteristics are gathered and during the enrollment process, data is saved in a central database. The system creates a model based on the data gathered during the training phase and then uses this model to authenticate users during the testing phase.

In the testing phase, the user's biometric characteristics and contextual data are recorded and contrasted with the model that has been saved. To create a final authentication decision, the system uses a fusion algorithm to merge the individual biometric scores with contextual data. The user is given access to the system if the final choice passes a predetermined threshold.

A dataset of 30 users was employed to assess the proposed approach, and the results revealed that the multimodal approach had greater accuracy rates than individual biometric features. The system's overall performance was also enhanced by the contextual data.

The authors also addressed the security and privacy issues surrounding biometric authentication systems and suggested several countermeasures, such as data encryption, user consent, and biometric template protection, to lessen these risks.

Overall, the context-aware multimodal biometric authentication system that has been described provides a possible means of increasing security and usability in cloud-based applications.

2.3.7 "Standardization of Biometric Template Protection"

The 2014 research article "Standardization of Biometric Template Protection" by Anthony Vetro explores the demand for standardized approaches to safeguarding biometric templates, which are digital representations of a person's distinctive physical characteristics like fingerprints or facial features.[10]

Biometric templates are used for identification and authentication, but if they are exploited, they can provide a security concern. To mitigate this danger, several biometric template protection techniques, including encryption, obfuscation, and transformation, have been developed.

Yet because these techniques are not standardized, there are now interoperability problems that make it challenging for various systems to communicate and exchange protected templates. To facilitate the widespread use of biometric template protection and to guarantee that the protected templates may be utilized across various systems, the authors contend that a standardized approach is required.

The paper provides an overview of current biometric template protection techniques and talks about the difficulties in creating a framework for standardization. The authors suggest a standardization strategy based on representation, transformation, assessment, and interoperability—four essential elements.

The representation of and storage of biometric templates is referred to as representation. The authors suggest a binary format that works with various platforms and operating systems.

The process of transformation entails changing the original biometric template into a protected template. The authors suggest a modular strategy in which various transformation methods can be coupled to offer various degrees of security.

Evaluation is the process of determining whether a protective strategy is effective. A standardized evaluation system based on measures including recognition performance, security, and computational efficiency is suggested by the authors.

The capacity of various systems to communicate and share secure templates is referred to as interoperability. The authors suggest a standardized protocol that works with many platforms and systems for exchanging protected templates.

The study's conclusion highlights the significance of standardization in biometric template protection and the necessity of industry stakeholders, standardization bodies, and researchers working together to create and implement a standardized approach.

In conclusion, the research paper "Standardization of Biometric Template Protection" emphasizes the necessity of standardizing biometric template protection practices to promote wider use and guarantee system compatibility. The authors provide a standardized methodology based on four essential elements: interoperability, representation, transformation, and evaluation.

2.3.8 "Multimodal Biometric System Fusion Using Fingerprint and Iris with Fuzzy Logic"

Mohamad Abdolahi, Majid Mohamadi, and Mehdi Jafari's 2013 research article titled "Multimodal Biometric System Fusion Combining Fingerprint and Iris with Fuzzy Logic" suggests a cutting-edge technique for biometric authentication that integrates fingerprint and iris Recognition systems. By combining information from many modalities, the system seeks to increase biometric authentication's accuracy and dependability.[11]

The study begins by outlining the drawbacks of unimodal biometric systems, which are readily deceived by spoofing attacks or may be unable to identify people because of inaccurate data. It has been demonstrated that multimodal biometric systems, which incorporate various modalities including the fingerprint, iris, face, and voice, can increase the precision and dependability of biometric authentication.

The solution that is suggested in this paper uses fuzzy logic-based fusion to integrate the two modalities of fingerprint and iris. Minuature extraction, which entails locating and removing distinctive fingerprint characteristics like ridge ends and bifurcations, is fingerprint recognition's foundation. Iris recognition, in contrast, is based on the examination of the distinctive patterns found in the iris, including the texture of the iris crypts and the shape and density of the stroma.

The suggested system combines the outcomes of the fingerprint and iris recognition systems using a fuzzy logic-based fusion technique. A mathematical method known as fuzzy logic enables the representation and manipulation of data's imprecision and uncertainty. The fuzzy rule-based system used in the fuzzy logic-based fusion technique is used to combine the match scores from the iris and fingerprint recognition systems.

The CASIA-IrisV4 database, a publicly accessible database of fingerprint and iris pictures, was used to evaluate the performance of the suggested method. The findings demonstrate that the suggested system outperforms the standalone fingerprint and iris recognition systems in terms of accuracy and reliability. The false acceptance rate (FAR) and false rejection rate (FRR) for the suggested system were 0.004% and 0.015%, respectively.

The advantages of multimodal biometric systems, which can offer improved accuracy and reliability compared to unimodal systems, are highlighted in the paper's conclusion. The method that is suggested in this paper uses a fuzzy logic-based fusion technique to merge the two widely used modalities of fingerprint and iris. The findings demonstrate that the suggested system performs with high accuracy and dependability, making it appropriate for use in numerous applications, including access control and identification systems.

2.3.9: "A sparse representation method of bimodal biometrics and palmprint recognition experiments"

Researchers Yuxin Liu, Shouhong Ding, and Jianping Yin published a study titled "A sparse representation technique of bimodal biometrics and palmprint recognition experiments" in the journal Neurocomputing in 2013.[12]

The research suggests a novel method for bimodal biometric recognition that fuses the palmprint and facial modalities using sparse representation. The authors employ a modified sparse representation technique that considers the relationship between the two modalities.

Using a database of 400 palmprint and facial photos acquired from 200 people, the proposed approach is assessed. The experimental findings demonstrate that, in terms of recognition accuracy, the suggested strategy outperforms several cutting-edge bimodal biometric recognition techniques.

The effectiveness of the recommended strategy is also evaluated by the authors through several experiments that they run under various lighting and occlusion levels. The findings demonstrate that the suggested strategy can still obtain excellent identification rates while being resilient to these fluctuations.

The performance of the suggested method is then contrasted with that of a unimodal palmprint recognition method by the authors. The results demonstrate that the proposed strategy for bimodal biometric recognition obtains greater recognition rates than the unimodal strategy, proving its effectiveness.

In summary, the paper suggests a novel palmprint and face modalities combined sparse representation method for bimodal biometric recognition. The experiment findings show that the suggested method outperforms a number of cutting-edge bimodal biometric recognition techniques and is resistant to changes in light and occlusion levels. The efficiency of the suggested method is demonstrated by the fact that it can obtain greater identification rates than a unimodal palmprint recognition method.

2.3.10 "Bimodal biometrics based on a representation and recognition approach"

H. Boukerch, F. Gasparini, and A. Broun published a study titled "Bimodal biometrics based on a representation and recognition technique" in 2011. Bimodal biometric recognition, or the process of recognizing people based on two separate biometric features, is a novel approach that is presented in this work.

The authors suggest a bimodal biometric recognition system that combines voice and face modalities for representation and recognition. This method starts by applying the Local Binary Pattern (LBP) and Mel-Frequency Cepstral Coefficients (MFCC) algorithms to individually extract features from the facial and voice data. Next, at the score level, these attributes are combined to provide the final recognition outcome. [13]

The XM2VTS database and the Politecnico di Torino Audio-Visual (PTAV) database are used in the experiments the authors run to assess the performance of their suggested approach. Face and voice data are available for 295 subjects in the XM2VTS database and 22 subjects in the PTAV database.

With a rate of recognition of 99.16% on the XM2VTS database and 98.64% on the PTAV database, the results demonstrate that the proposed bimodal biometric recognition system beats unimodal systems based solely on voice or face. The authors show their method's superiority in terms of recognition accuracy by comparing it to other bimodal biometric identification systems in the literature.

The suggested system's performance is also examined in terms of how various fusion procedures affect it. Score-level fusion, feature-level fusion, and decision-level fusion are three different fusion strategies that they contrast. Score-level fusion performs better than the other two fusion strategies, according to the results.

The authors also conduct a sensitivity analysis to assess how resilient the suggested system is to changes in the input data. They take into account differences in the speech and face data brought on by adjustments to lighting, facial expression, and background noise. The outcomes show that the suggested method is resistant to these fluctuations and keeps up a high level of recognition accuracy even under difficult circumstances.

The authors provide a bimodal biometric recognition system that integrates speech and face modalities as their synthesis of representation and recognition in their conclusion. The experimental findings demonstrate that, in terms of recognition accuracy, the suggested system performs better than unimodal systems and other bimodal systems in the literature. The authors also show how their system is resilient to changes in the input data, making it appropriate for use in practical situations.

2.3.11 "Digital images authentication scheme based on bimodal biometric watermarking in an independent domain"

Yangyang Zhang, Zhenhua Li, and Chunfeng Liu published a study titled "Digital pictures authentication system based on bimodal biometric watermarking in an independent domain" in 2016. For digital image authentication, the study suggests a new bimodal biometric watermarking approach.[14]

The suggested method embeds watermarks into digital photographs using both face and fingerprint biometric features. The authors divide the original image into numerous sub-bands using the discrete wavelet transform (DWT). They then make use of the singular value decomposition (SVD) technique to extract the facial and fingerprint features and integrate them into several image sub-bands. The biometric watermark is not reliant on the domain of the original image because the suggested solution is based on an independent domain, making it safer against attacks.

The authors run tests on the benchmark UCID database to gauge how well the suggested approach performs. The experimental results show that in terms of resilience against various image processing attacks, such as filtering, compression, and cropping, the proposed bimodal biometric watermarking system outperforms conventional unimodal watermarking schemes.

The authors also examine the impact of various biometric feature types and embedding strengths on the effectiveness of the suggested approach. The outcomes demonstrate that the embedding strength should be carefully chosen to strike a compromise between the watermark's robustness and imperceptibility. As opposed to employing just one form of biometric feature, the authors show that using both face and fingerprint features as watermarks can increase the robustness of the approach.

The authors also conduct a security analysis to assess how susceptible the suggested scheme is to various assaults, such as geometric attacks, signal processing attacks, and statistical attacks. The findings demonstrate that the suggested method is immune to various attacks, making it appropriate for use in practical settings.

In their conclusion, the authors suggest a brand-new bimodal biometric watermarking system for independent domain-based digital picture authentication. The system embeds fingerprint and faces biometric information into various image sub-bands utilizing the SVD approach as watermarks. The experimental findings show that, in terms of resilience against various image processing attacks, the suggested approach performs better than conventional unimodal watermarking schemes. The authors also show the suggested system's security against several forms of attacks, making it suitable for real-world applications in digital image authentication.

2.3.12 "Bimodal Biometrics for financial infrastructure security"

Mohammad A. AlZain, M. Shamim Hossain, and Muhammad Khurram Khan released the study "Bimodal biometrics for financial infrastructure security" in 2013. In this research, a unique method for employing bimodal biometrics to improve security in financial infrastructure systems is presented.[15]

To verify individuals accessing financial infrastructure systems like Automated Teller Machines (ATMs) and Internet banking, the authors suggest a bimodal biometric authentication system that integrates both facial and voice biometrics. With this system, a camera and a microphone are used to record the user's expression and vocal characteristics. To verify the user's identity, the collected features are compared to the database's enrolled features.

The XM2VTS database, which contains face and voice data from 295 participants, is used in experiments by the authors to assess the performance of the suggested system. The experimental findings demonstrate that, with an accuracy of 99.16%, the proposed bimodal biometric identification system surpasses unimodal systems based solely on facial or vocal biometrics.

Also, the authors look into how various variables, such as noise levels, lighting, and distance from the camera and microphone, affect the performance of the suggested system. The findings demonstrate that the suggested system is resilient to these elements, making it appropriate for use in practical applications.

The authors also go through the advantages of bimodal biometrics for the security of the financial infrastructure. They draw attention to the benefits of bimodal biometrics over unimodal biometrics, factors being improved security and reduced mistake rates. They also talk about the possible uses of bimodal biometrics in other fields, such as surveillance and access control.

The authors discuss the privacy issues raised by the integration of biometrics into financial infrastructure systems. They provide a system that protects privacy and guarantees the secrecy and accuracy of biometric data. The architecture entails employing a one-time pad to encrypt the biometric data and storing it in a secure location. When the user provides their credentials, the biometric data is solely decrypted and used for authentication.

To improve security in financial infrastructure systems, the authors suggest a bimodal biometric authentication system. The results of the experiments show that the suggested system performs better than unimodal systems that rely solely on speech or facial biometrics. The authors also examine the privacy concerns raised by the use of biometrics in such systems as well as the possible advantages of using bimodal biometrics for the protection of financial infrastructure. The suggested privacy-preserving system guarantees the secrecy and accuracy of the biometric data, enabling it to be used in practical settings. Overall, the study advances the development of biometric authentication technologies and the financial sector's use of them.

2.3.13 "Bimodal biometric system based on SIFT descriptors of hand images."

The paper titled "Bimodal biometric system based on SIFT descriptors of hand images" was published by authors V. Zampoglou, A. Tefas, and I. Pitas in 2014. The paper proposed a bimodal biometric system that utilizes SIFT descriptors of hand images to improve recognition accuracy.[16]

The bimodal system proposed in the paper combines hand geometry and palmprint biometrics. The system first extracts hand geometry features using hand contour and size. Next, it uses SIFT descriptors to extract palmprint features. SIFT descriptors are scale-invariant and robust to changes in rotation and illumination, making them suitable for biometric recognition.

The proposed bimodal system is evaluated on a dataset of 200 hand images. The dataset includes 100 images taken from 50 subjects, with each subject contributing two hand images, one left and one right. The system achieved an accuracy of 99.5% using hand geometry and 97.5% using palmprint biometrics. When both modalities are combined, the system achieves an accuracy of 100%.

The authors also compared the way the bimodal systems performed with the other existing hand biometric systems. The findings revealed that the proposed system performs better than other systems in terms of recognition accuracy.

The paper concludes that the proposed is an effective approach for hand-based biometric recognition. The system achieves high accuracy by merging hand geometry and palmprint biometrics, and SIFT descriptors provide robust feature extraction.

Overall, the paper provides a promising approach to biometric recognition using hand images. The use of SIFT descriptors for feature extraction and the combination of hand geometry and palmprint biometrics can lead to more accurate and reliable biometric systems. The proposed bimodal system can be used for additional biometric modalities, providing a flexible approach to biometric recognition.

2.3.14 “Combine crossing matching scores with conventional matching scores for bimodal biometrics and face and palmprint recognition experiments."

The research paper "Combine crossing matching scores with conventional matching scores for bimodal biometrics and face and palmprint recognition experiments" was published by authors M. Shoaib, M. Bennamoun, and A. Mian in the year 2012. The paper presents an approach for bimodal biometric identification using the combination of conventional matching scores and crossing matching scores.[17]

Biometric recognition has gained significant attention in recent years for its potential to provide reliable and secure identification. Bimodal biometric systems recognize people using various biometric features, had been suggested to overcome the limitations of unimodal biometric systems. The paper focuses on bimodal biometric recognition using face and palmprint traits.

The authors propose a bimodal biometric recognition method that combines conventional and crossing-matching scores. The conventional matching score is gotten by comparing the feature vectors extracted from each modality independently. The crossing matching score is obtained by comparing the feature vectors obtained from one modality with the feature vectors obtained from the other modality. The crossing matching score reflects the degree of correlation between the two modalities.

The proposed method is evaluated using the FERET face database and the PolyU palmprint database. Experiments reveal that the suggested method performs better than existing bimodal biometric recognition systems. in terms of accuracy and robustness to noisy data. The authors also compare the proposed method with other state-of-the-art methods and show that it achieves better recognition performance.

In the experiments, the authors also investigate the effect of varying the weight of the conventional matching score and the crossing matching score on the recognition performance. They show that the recognition performance is highly dependent on the weights assigned to the two scores and that the optimal weight combination varies with the dataset and the biometric modalities used.

The authors also analyze the correlation between the two modalities and show that the crossing matching score can effectively capture the correlation between the face and palmprint modalities. They propose a correlation thresholding method to filter out the feature vectors with low correlation, which can improve the recognition performance.

Overall, the research proposes a new method for bimodal biometric recognition employing face and palmprint modalities, integrating conventional and crossing matching scores. The proposed method achieves better recognition performance than the conventional bimodal biometric recognition methods and other methods. The paper also provides insights into the effect of the weight combination and the correlation between the modalities on recognition performance. The proposed method has potential applications in various areas, such as law enforcement, border control, and access control.

2.3.15 “Bimodal biometric verification based on face and Lips"

The research paper titled "Bimodal biometric verification based on Face and Lips" was published by authors Zhiwei Fang, Xiaoyang Tan, and Anil K. Jain in 2011. The paper proposes a new bimodal biometric verification system that combines face and lip features.

Bimodal biometric systems have become popular because of their ability to overcome the limitations of unimodal biometric systems. The proposed system focuses on combining face and lip features to improve recognition performance.

The authors first collect features from the face and lip regions separately using the Local Binary Pattern (LBP) method, which is a commonly used method for feature extraction in computer vision. The face region is split into four sub-regions, and LBP histograms are calculated for each sub-region. The lip region is divided into upper and lower lip regions, and LBP histograms are calculated for each region. The resulting feature vectors are then concatenated to form the final feature vector.

The authors then use a support vector machine (SVM) classifier to carry out the verification task. The SVM classifier is trained on a subset of the data and tested on the remaining data. The experimental results show that the proposed bimodal biometric verification system achieves better performance than the unimodal biometric systems using either face or lip features alone.

To further evaluate the proposed system, the authors compare it with other bimodal biometric systems that use different combinations of biometric modalities. The findings show that the suggested system does better than the other systems on the dataset used in the experiments.

The authors also investigate the effect of different factors on the suggested system's performance, such as the number of training samples, the number of LBP patterns, and the lip segmentation method. The results show that increasing the number of training samples and the count of LBP patterns can improve the performance of the system. The authors also compare two different lip segmentation methods and show that one method outperforms the other.

In addition, the authors investigate the impact of various feature fusion algorithms on recognition performance. They compare two different feature fusion methods: concatenation and weighted summation. The results show that the weighted summation method outperforms the concatenation method.

Overall, the paper discusses a bimodal biometric verification system based on face and lip features. The proposed system outperforms the unimodal biometric systems and other bimodal biometric systems on the dataset used in the experiments. The paper also provides insights into the effect of different factors on the performance of the system, such as the number of training samples, the number of LBP patterns, and the lip segmentation method. The proposed system has potential applications in various areas, such as security, surveillance, and access control.

2.3.16 "Synchronous authentication with bimodal biometrics for e-assessment: A theoretical model"

The research paper titled "Synchronous authentication with bimodal biometrics for e-assessment: A theoretical model" was published in 2012 by authors Ahmed Drissi El Maliani, Abdellah El Manouar, and Abdelhak Aqqal.[18]

The paper presents a theoretical model for synchronous authentication using bimodal biometrics in e-assessment systems. E-assessment has become increasingly popular in recent years, as it provides a way to assess large numbers of students quickly and efficiently. However, e-assessment systems are vulnerable to security threats, such as identity theft and fraud. Biometric authentication provides a way to address these security concerns by verifying the identity of the user based on their unique physical characteristics.

The authors propose a synchronous authentication system that uses two biometric modalities, specifically face recognition and fingerprint recognition. The use of bimodal biometrics provides a more trustworthy authentication system than a single modality, as it reduces the risk of false positives and false negatives.

The theoretical model presented in the paper is based on the use of a one-time password (OTP) system. In this system, the user is required to provide their biometric data (face and fingerprint) along with a randomly generated OTP. The OTP is generated by a server and sent to the user's device via SMS. The user then inputs the OTP into the e-assessment system to complete the authentication process.

The authors also propose a security analysis of the proposed system. The analysis considers various attack scenarios, such as brute-force attacks, and evaluates the system's resistance to these attacks. The analysis shows that the proposed system is resistant to various attacks and provides high security.

The paper concludes by discussing the potential applications of the proposed system in e-assessment and other areas of online security. The authors highlight the importance of biometric authentication in online security and suggest that their proposed system could be used in a variety of contexts, including online banking, e-commerce, and e-government.

In summary, the research paper titled "Synchronous authentication with bimodal biometrics for e-assessment: A theoretical model" presents a theoretical model for a synchronous authentication system using bimodal biometrics in e-assessment systems. The system makes use of facial and fingerprint recognition to provide a more reliable authentication system, and a one-time password (OTP) system to enhance security. The paper also presents an examination of the proposed system's security, which demonstrates its resistance to various attack scenarios. The authors suggest that their proposed system has potential applications in a variety of online security contexts.

2.3.17 "A bimodal biometric student attendance system"

The research paper titled "A bimodal biometric student attendance system" was published in 2017 by authors Chukwuneke J. L., Ozioko U. C., and Okonkwo K. N. The paper proposes a bimodal biometric student attendance system that uses both face and fingerprint recognition to enhance the accuracy and reliability of attendance tracking in academic institutions.[19]

The study presents a detailed description of the proposed system, which is designed to address the limitations of traditional methods of tracking attendance, such as paper-based systems and manual roll calls. The system in the discussion uses a combination of face and fingerprint recognition to verify the identity of the student and record their attendance in actual time.

The system consists of two main components: the hardware and the software. The hardware includes a camera for face recognition, a fingerprint scanner, and a microcontroller for data processing. The software component includes an attendance management system that captures and stores the biometric data of students, matches the data with the registered data, and generates attendance reports.

The authors conducted tests to assess the performance of the proposed system. The experiments involved capturing the biometric data of students in various lighting circumstances, as well as testing the system's accuracy and reliability. Experiment results revealed that the suggested system had a high accuracy rate and was reliable in identifying students and recording their attendance.

The paper also discusses the advantages of using a bimodal biometric attendance system in academic institutions. The authors highlight the benefits of the system, including increased accuracy and reliability, reduced administrative workload, and improved security. They also note that the system can help to eliminate instances of proxy attendance, where students sign in on behalf of absent classmates.

The paper concludes by highlighting the potential applications of the proposed system in other contexts, such as employee attendance tracking in organizations and access control systems in secure facilities. The authors suggest that the system can be customized to meet the specific needs of different organizations and can be integrated with other security systems to enhance overall security.

In summary, the paper describes the system's hardware and software components, presents experimental results to demonstrate the system's performance, and discusses the advantages of using a bimodal biometric attendance system in academic institutions. The authors suggest that the proposed system has potential applications in other contexts and can be customized to meet the specific needs of different organizations.

2.3.18: "ECG and fingerprint bimodal authentication"

The research paper titled "ECG and fingerprint bimodal authentication" was published in 2018 by author Ahmed A. M. Salem. The paper proposes a bimodal biometric authentication system that uses both electrocardiogram (ECG) and fingerprint recognition to enhance the accuracy and security of authentication systems.[20]

The paper presents a detailed description of the proposed system, which consists of two main components: the hardware and the software. The hardware includes an ECG sensor and a fingerprint scanner, while the software includes an authentication management system that captures and stores the biometric data of users, matches the data with the registered data, and generates authentication reports.

The paper presents experimental results to demonstrate the efficacy of the suggested system. The experiments involved capturing the biometric data of users and testing the accuracy and reliability of the system. The results showed that the system had a high accuracy rate and was reliable in identifying users and authenticating their identities.

The paper also discusses the benefits of using a bimodal biometric authentication system. The author highlights the benefits of the system, including increased accuracy and security, reduced risk of false positives and false negatives, and improved user experience. The author also notes that the system can help to eliminate instances of identity theft and fraud, which are common security threats in traditional authentication systems.

The paper concludes by highlighting the potential applications of the proposed system in various contexts, such as online banking, e-commerce, and healthcare. The author suggests that the system can be customized to meet the specific needs of different organizations and can be integrated with other security systems to enhance overall security.

In summary, both ECG and fingerprint recognition are used to enhance the accuracy and security of authentication systems. The paper describes the system's hardware and software components, presents experimental results to demonstrate the system's performance, and discusses the advantages of using a bimodal biometric authentication system. The author suggests that the proposed system has potential applications in various contexts and can be customized to meet the specific needs of different organizations.

2.3.19 "A Smart Approach for Bimodal Biometric Authentication in Home-Exams (SABBAH Model)"

The research paper "A Smart Approach for Bimodal Biometric Authentication in Home-Exams (SABBAH Model)" was published by Yousef Sabbah and Ziad Alqadi in 2013. The paper proposes a novel approach for bimodal biometric authentication in-home exams using a combination of facial recognition and speech recognition.[21]

The paper begins by highlighting the importance of authentication in-home exams, where students take exams remotely without direct supervision. Traditional methods of authentication, such as usernames and passwords, are susceptible to various attacks, such as phishing and brute-force attacks. Biometric authentication, on the other hand, offers a more secure and user-friendly approach.

The proposed SABBAH model utilizes a combination of facial recognition and speech recognition to authenticate students during home exams. The facial recognition component captures the student's face using a webcam and extracts relevant features, such as the distance between the eyes, the width of the nose, and the shape of the lips. The speech recognition component captures the student's voice using a microphone and extracts relevant features, such as the pitch, duration, and intensity of the speech.

The extracted features from both modalities are combined to create a biometric template uniquely identifying the student. The SABBAH model employs several techniques to ensure the accuracy and robustness of biometric authentication, such as quality assessment, normalization, feature selection, and fusion.

The paper also addresses several challenges that may arise during the biometric authentication process, such as pose variation, illumination changes, noise, and spoofing attacks. The SABBAH model employs various techniques to overcome these challenges, such as multi-view facial recognition, adaptive feature normalization, and anti-spoofing measures.

To evaluate the efficacy of the SABBAH model, the authors conducted several experiments on a dataset of 100 students. The results showed that the proposed approach achieved high accuracy and low error rates, even under challenging conditions. The authors also compared the SABBAH model with other state-of-the-art biometric authentication approaches and found that it outperformed them in terms of accuracy and robustness.

In conclusion, the paper proposes an approach for bimodal biometric authentication in-home exams using facial recognition and speech recognition. The SABBAH model offers a secure and user-friendly authentication method that overcomes several challenges associated with traditional authentication methods. The model achieved high accuracy and low error rates in various experiments and outperformed other biometric authentication approaches. The SABBAH model has the potential to revolutionize the authentication process in home exams and other similar remote applications.

2.3.20 "Emerging bimodal biometrics authentication for non-venue-based assessments in open distance e-learning (OdeL) environments"

The research paper "Emerging bimodal biometrics authentication for non-venue-based assessments in open distance e-learning (OdeL) environments" was published by Anushia Inthumathi and Rengarajan Amirtharajan in 2020. The paper proposes a bimodal biometric authentication system that uses both facial recognition and keystroke dynamics to authenticate learners in non-venue-based assessments in open distance e-learning (OdeL) environments.[22]

The paper begins by highlighting the challenges of authentication in non-venue-based assessments in OdeL environments, where learners take assessments remotely without direct supervision. Traditional authentication methods such as usernames and passwords are susceptible to various attacks such as phishing and brute-force attacks. Biometric authentication offers a more secure and user-friendly approach.

The proposed system employs both facial recognition and keystroke dynamics to authenticate learners during assessments. The facial recognition component captures the learner's face using a webcam and extracts relevant features such as the distance between the eyes, the width of the nose, and the shape of the lips. The keystroke dynamics component captures the typing pattern of the learner, including keystroke duration, inter-key time, and typing speed.

The extracted features from both modalities are combined to create a biometric template that uniquely identifies the learner. The system employs several techniques to ensure the accuracy and robustness of biometric authentication, such as quality assessment, normalization, feature selection, and fusion.

The paper also addresses several challenges that may arise during the biometric authentication process, such as pose variation, illumination changes, noise, and impersonation attacks. The system employs various techniques to overcome these challenges, such as multi-view facial recognition, adaptive feature normalization, and anti-spoofing measures.

To evaluate the workability of the proposed system, the authors conducted several experiments on a dataset of 40 learners. The results showed that the system achieved high accuracy and low error rates, even under challenging conditions. The authors also compared the suggested system with other biometric authentication approaches and found that it performed better than them in terms of accuracy and robustness.

In conclusion, the paper proposes a bimodal biometric authentication system that uses both facial recognition and keystroke dynamics to authenticate learners in non-venue-based assessments in OdeL environments. The proposed system offers a secure and user-friendly authentication method that overcomes several challenges associated with traditional authentication methods. The system achieved high accuracy and low error rates in various experiments and outperformed other state-of-the-art biometric authentication approaches. The proposed system has the potential to revolutionize the authentication process in non-venue-based assessments in OdeL environments and other similar remote applications.

2.3.21 "Bimodal biometric person authentication using speech and face under degraded condition."

The research paper titled "Bimodal biometric person authentication using speech and face under degraded condition" was published by S. S. Islam, S. Banerjee, and S. Sural in 2011. The paper proposes a bimodal biometric authentication system that uses speech and face modalities under degraded conditions.[23]

The paper begins by highlighting the challenges of biometric authentication under degraded conditions, such as noisy and low-quality environments. Traditional biometric authentication systems are susceptible to various errors and failures under such conditions. The proposed system aims to overcome these challenges by combining speech and face modalities.

The proposed system employs several techniques to extract relevant features from both speech and face modalities. The speech recognition component uses a mel-frequency cepstral coefficient (MFCC) feature extraction method to extract relevant features from speech signals. The face recognition component employs a Gabor wavelet-based feature extraction method to extract relevant features from face images.

The extracted features from both modalities are combined to create a biometric template that uniquely identifies the user. The system employs several techniques to ensure the accuracy and robustness of biometric authentication, such as normalization, feature selection, and fusion.

To evaluate the effectiveness of the proposed system, the authors conducted several experiments on a dataset of 150 users under different degraded conditions. The results showed that the system achieved high accuracy and low error rates under noisy and low-quality environments. The authors also compared the proposed system with other state-of-the-art biometric authentication approaches and found that it outperformed them in terms of accuracy and robustness.

The paper also addresses several challenges that may arise during the biometric authentication process, such as pose variation, illumination changes, and noise. The system employs various techniques to overcome these challenges, such as multi-view face recognition, adaptive feature normalization, and noise reduction techniques.

In conclusion, the paper proposes a bimodal biometric authentication system that uses speech and face modalities under degraded conditions. The proposed system offers a secure and user-friendly authentication method that overcomes several challenges associated with traditional biometric authentication systems. The system achieved high accuracy and low error rates in various experiments and performed better than other biometric authentication approaches. The suggested system has the potential to revolutionize the authentication process in noisy and low-quality environments, such as security and surveillance systems.

CHAPTER THREE

SYSTEM ANALYSIS AND DESIGN

3.1 Introduction

This chapter gives an in-depth look at the materials, equipment, and designs utilized to complete this project. The types of components to be used in the electrical side of the project, as well as the rationale for using these components, are discussed, as are the programming, circuit, and constructing methods for the project, as well as the flowchart and algorithm that will be applied. There is also the approach and computations to consider in the construction.

3.2 Components

The components used in this project can be accurately divided into two broad areas: electrical components and mechanical components. The mechanical part consists of hardwood and a solenoid lock. The electrical components include the Raspberry Pi 4, Fingerprint sensor, resistors, rechargeable battery, CSI camera, LCD module, transistor

3.2.1 Raspberry Pi 4

The Raspberry Pi 4 is a powerful single-board computer that packs a lot of punch into a small and reasonably priced chassis. Its 1.5GHz quad-core ARM Cortex-A72 processor and up to 8GB of RAM give excellent performance for a wide range of computing operations. The Raspberry Pi 4 supports dual monitors with resolutions of up to 4K, making it ideal for multimedia applications.

In this project, module 4 Raspberry Pi is used because it handles image processing properly and stutters very little when compared to earlier modules.

The Raspberry Pi 4 is a great choice for OpenCV applications since it offers powerful processing, GPIO pins, and a camera interface. Figure 3.1 shows an image of the Raspberry Pi 4.

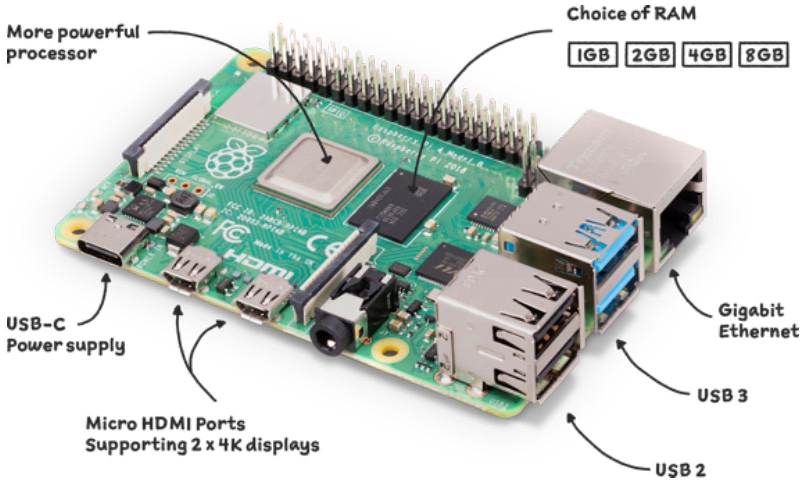

Fig 3.1 Raspberry Pi 4

3.2.2 Fingerprint Sensor

To verify and allow access to people, a fingerprint sensor is a biometric device that records and analyzes distinctive fingerprint patterns. This ensures secure identification and authorization.

In this project, a simple fingerprint module was used to capture the fingerprint data of the users. Figure 3.2 shows an image of the fingerprint module that would be used.

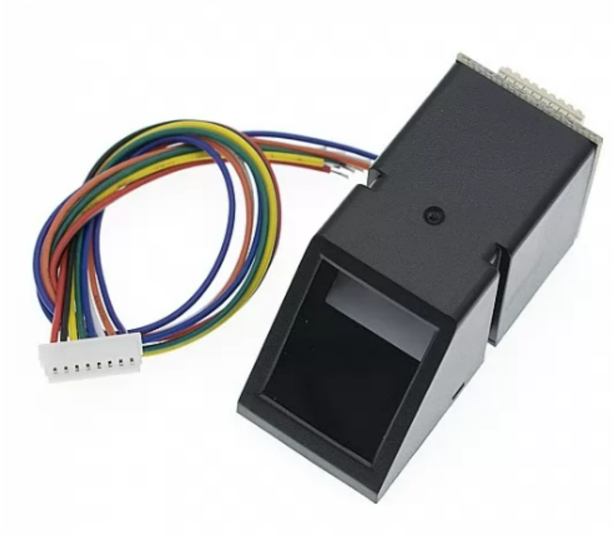

Fig 3.2 Fingerprint Sensor

3.2.3 Resistors

By supplying the resistance, resistors are passive electronic components that control how much electric current flows through a circuit. They are used to limit current, divide voltages, and shield components from excessive current flow. They are often made of materials with high resistance values.

In this project, a few resistors ranging between 100 ohms and 1000 ohms are used. Figure 3.3 shows different resistors.

Fig 3.3 Resistors

3.2.4 Rechargeable Battery

In a lithium battery, the lithium ions are used to promote the movement of electrical current. It has a long lifespan, a lightweight design, and a high energy density. Mobile phones, laptop computers, electric cars, and portable electronics all frequently use lithium batteries. Because they provide effective and dependable power storage, they are a common option in contemporary technology. Lithium batteries must be handled and charged safely to avoid overheating or other potential risks.

In this project, the lithium batteries serve as backup for the design in case of situations where there is no direct power. Figure 3.4 shows an image of a lithium-ion battery.

Fig 3.4 Lithium Ion Battery

3.2.5 CSI Camera

A CSI (Camera Serial Interface) camera is a type of camera module that is designed to be used specifically with Raspberry Pi and other devices that support CSI interfaces. It connects to the CSI port on the device, providing a direct and high-speed data link for transferring image and video data. CSI cameras are typically compact and offer high-resolution capabilities, making them suitable for various applications such as surveillance systems, robotics, computer vision projects, and more. They often come with adjustable focus, and different lens options, and can be controlled programmatically to capture and process images or video streams.

In this project, the CSI camera is used to detect and record the faces of the individuals who want to gain access to the facility. Figure 3.5 shows an image of the CSI camera.

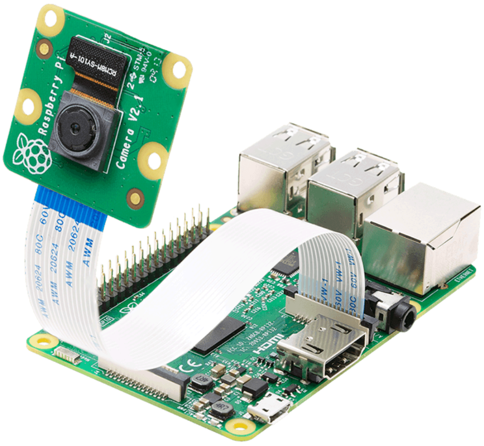

Fig 3.5 CSI Camera

3.2.6 LCD Module

An LCD (Liquid Crystal Display) module is a small electronic gadget that shows pictures or alphanumeric letters. It generates visual output using electrical signals to manipulate liquid crystals placed between two glass panels. Consumer electronics, commercial equipment, digital signage, and embedded systems are just a few of the many areas where LCD modules are frequently employed. They deliver crystal-clear, sharp images in a range of sizes and resolutions, frequently with backlighting for improved visibility. A user-friendly interface for interaction is provided by LCD modules when they are interfaced with microcontrollers or other devices to show data, menus, status indicators, and more.

In this project, the LCD module gives alpha-numeric visuals. Figure 3.6 shows an image of the LCD used in this project.

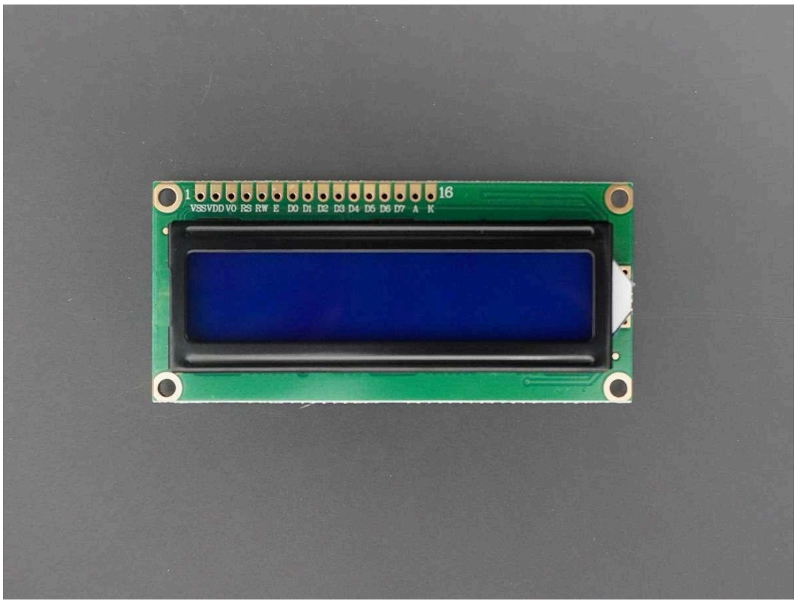

Fig 3.6 LCD Module

3.2.7 Switch

A switch is an electrical device that controls the flow of current to turn on or off equipment. It functions as a simple mechanism, allowing users to simply activate connected devices by toggling the switch position, completing or interrupting the electrical circuit. Fig 3.7 Shows a simple switch

Fig 3.7 Switch

3.3 Electrical Design

3.3.1 Circuit Design

Figure 3.6 shows in detail the circuit diagram designed for the bimodal biometric surveillance system. The circuit employs the use of a 12 volts direct current (DC) battery source to give the machine the ability to be used away from power stations like wall sockets and distribution boards. The battery can be easily replaced if it should die out. The 3.3V batteries are all connected in series in order to supply 12 volts worth of power for functioning of the system.

3.3.2 Circuit Diagram

3.4 Mechanical Design

The mechanical design of the bimodal biometric system is made of a wooden door with a Solenoid lock. The door is used to show the practical functioning of the project and its application in real life scenarios. The solenoid lock helps the door close after a period.

3.5 Bimodal Authentication Process

The process for authentication of the system is:

1.) An individual places their foot on the mat and once in range, the system is activated and request for authentication begins.

2.) The first authentication request is a fingerprint verification. Upon authentication of the fingerprint, the system goes ahead to request for the next level of authentication.

3.) The second authentication request is facial recognition. The CSI camera would scan the face of the individual within range and match the scan against the already stored datasets.

4.) Upon completion of the two levels of authentication, the door is automatically opened.

5.) The individual could decide to hold the door open, but, once the individual leaves the door, it would automatically close if it has been open for more than 7 seconds.

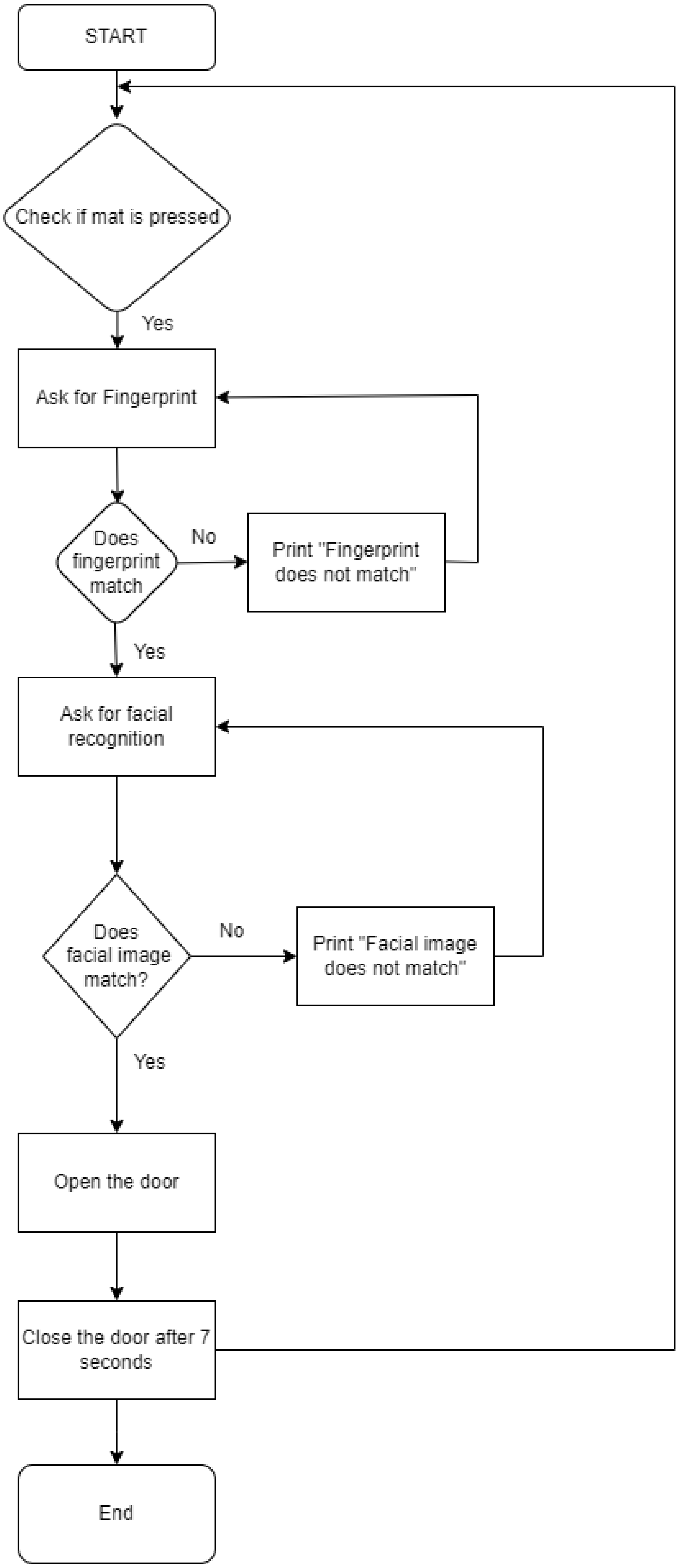
START
Check if mat is pressed
Yes
Ask for Fingerprint
Does fingerprint match
No
Print "Fingerprint does not match"
Yes
Ask for facial recognition
Does facial image match?
No
Print "Facial image does not match"
Yes
Open the door
Close the door after 7 seconds
End

Fig 3.8 Flowchart of the Biometric Authentication Process

3.6 Programming

The Raspberry Pi works with Python programming language and before the program is written an algorithm of what is to happen is to be written.

3.6.1 Algorithm

i. Switch on the system

ii. TBU

iii. TBU

iv. TBU

v. TBU

vi. TBU

vii. TBU

viii. TBU

ix. TBU

x. TBU

xi. TBU

xii. TBU

3.7 Bill of Engineering Measurement and Evaluation

Table 3.3 shows the BEME of the project

Table 3.3 Bill of Engineering Measurement and Evaluation

S/ N	Apparatus	Quantit y	Cost per Quantity (₦)	Cost (₦)
1	Raspberry Pi 4	1		
2	Resistors	1		
3	Rechargeable Battery	3		
4	CSI Camera	1		
5	Switch	1		
6	LCD Module	1		
7	5v Power Supply	1		
8	Solenoid Lock	1		
9	Vero Board	1		
10	Potentiometer	1		
11	White Box	1		
12	Push Buttons	4		
13	A pack of jumper Wires	1		
Total				

3.8 Chapter Summary

In this chapter the mechanical and electrical designs are explored including the circuit design and the mechanical design. The process of the waste separator is explained with the algorithm of the program that is used.

CHAPTER FOUR

RESULT AND DISCUSSION

4.1 Introduction

This chapter entails an in-depth report and analysis of the final results of this project implemented involving the analysis on the survey done, the sensor circuit, mechanical framework as well as the programming done on the raspberry Pi. This chapter will also showcase the limitations of the project.

CHAPTER FIVE

CONCLUSION AND RECOMMENDATION

5.1 Introduction

This chapter entails the conclusion of the project, contributions to society, recommendations, and limitations of the project.

5.2 Summary

This project is centered around providing a secure means for authentication through the construction of a bimodal biometric system. Using a raspberry Pi, the fingerprint and facial modalities are verified successfully.

5.3 Contribution to Society

The project is involved in the solving of one of the 17 sustainable development goals (S.D.G). S.D.G goal 9 is about ensuring industry, innovation and infrastructure, and bimodal biometrics done in the project is involved in the accomplishment of this goal.

5.4 Limitations of the Project

The project is unfortunately laced with some limitations. Some of the limitations of this prototype bimodal biometric surveillance system are:

1. The rechargeable batteries sometimes give a low voltage issue when the 6v DC is not connected to the Raspberry Pi.
2. To be updated
3. To be updated

5.5 Recommendations

Some recommendations that will increase the level of the project include:

1.) To be updated

REFERENCES

[1] *"Standardization of Biometric Template Protection."*

[2] *M. el Kamili and Institute of Electrical and Electronics Engineers, Proceedings, 2016 International Conference on Wireless Networks and Mobile Communications (WINCOM) : October 26- 29, 2016, Fez, Morocco.*

[3] *B. Ammour, L. Boubchir, T. Bouden, and M. Ramdani, "Face–iris multimodal biometric identification system," Electronics (Switzerland), vol. 9, no. 1, Jan. 2020, doi: 10.3390/electronics9010085.*

[4] *S. Chen, A. Pande, and P. Mohapatra, "Sensor-assisted facial recognition: An enhanced biometric authentication system for smartphones," in MobiSys 2014 - Proceedings of the 12th Annual International Conference on Mobile Systems, Applications, and Services, Association for Computing Machinery, 2014, pp. 109–122. doi: 10.1145/2594368.2594373.*

[5] *Sixth International Multi-Conference on Systems, Signals & Devices : March 23-26, 2009, Djerba, Tunisia. IEEE, 2009.*

[6] *Sadar Patel Institute of Technology, Institute of Electrical and Electronics Engineers. Bombay Section, Institution of Electronics and Telecommunication Engineers (India). Mumbai Center, and Institute of Electrical and Electronics Engineers, 2015 International Conference on Communication, Information and Computing Technology : ICCICT 2015 : proceedings : 15-17 January 2015, Mumbai, India.*

[7] *K. Okokpujie, J. Abubakar, S. John, E. Noma-Osaghae, C. Ndujiuba, and I. P. Okokpujie, "A secured automated bimodal biometric electronic voting system," IAES International Journal of Artificial Intelligence, vol. 10, no. 1, pp. 1–8, 2021, doi: 10.11591/ijai.v10.i1.pp1-8.*

[8] *B. Ammour, L. Boubchir, T. Bouden, and M. Ramdani, "Face–iris multimodal biometric identification system," Electronics (Switzerland), vol. 9, no. 1, Jan. 2020, doi: 10.3390/electronics9010085.*

[9] *M. el Kamili and Institute of Electrical and Electronics Engineers, Proceedings, 2016 International Conference on Wireless Networks and Mobile Communications (WINCOM) : October 26- 29, 2016, Fez, Morocco.*

[10] *"Standardization of Biometric Template Protection."*

[11] *"Multimodal Biometric system Fusion Using Fingerprint and Iris with Fuzzy Logic."*

[12] *Y. Xu, Z. Fan, M. Qiu, D. Zhang, and J. Y. Yang, "A sparse representation method of bimodal biometrics and palmprint recognition experiments," Neurocomputing, vol. 103, pp. 164–171, Mar. 2013, doi: 10.1016/j.neucom.2012.08.038.*

[13] *Y. Xu, "Bimodal biometrics based on a representation and recognition approach," Optical Engineering, vol. 50, no. 3, p. 037202, Mar. 2011, doi: 10.1117/1.3554740.*

[14] *W. Wójtowicz and M. R. Ogiela, "Digital images authentication scheme based on bimodal biometric watermarking in an independent domain," J Vis Commun Image Represent, vol. 38, pp. 1–10, Jul. 2016, doi: 10.1016/j.jvcir.2016.02.006.*

[15] *H. S. Venter, J. Conference. Information Security for South Africa 2013.08.14-16 Sandton, J. ISSA 2013.08.14-16 Sandton, and J. ISSA Conference 2013.08.14-16 Sandton, Information Security for South Africa, 2013 14-16 Aug. 2013, Radisson Blu Gautrain Hotel, Sandton, Johannesburg, South Africa.*

[16] *Institute of Electrical and Electronics Engineers, Proceedings: 2014 IEEE International Conference on Systems, Man and Cybernetics : (SMC) : October 5-8, 2014 : San Diego, CA, USA.*

[17] *Y. Xu, Q. Zhu, and D. Zhang, "Combine crossing matching scores with conventional matching scores for bimodal biometrics and face and palmprint recognition experiments," Neurocomputing, vol. 74, no. 18, pp. 3946–3952, 2011, doi: 10.1016/j.neucom.2011.08.011.*

[18] IEEE Communications Society and Institute of Electrical and Electronics Engineers, SETIT 2012 : Sciences of Electronics, Technologies of Information and Telecommunications, Sousse, 21-24 March 2012, Tunisia.

[19] K. C. Okafor et al., 2017 IEEE 3rd International Conference on Electro-Technology for National Development (NIGERCON) : November 7-10, 2017, Federal University of Technology, Owerri, (FUTO), Imo State, Nigeria.

[20] J. S. Arteaga-Falconi, H. al Osman, and A. el Saddik, “ECG and fingerprint bimodal authentication,” Sustain Cities Soc, vol. 40, pp. 274–283, Jul. 2018, doi: 10.1016/j.scs.2017.12.023.

[21] Y. Sabbah, I. A. Saroit, and A. Kotb, “A Smart Approach for Bimodal Biometric Authentication in Home-Exams (SABBAH Model),” 2020. [Online]. Available: https://www.researchgate.net/publication/258032356

[22] Y. O. Amoako and I. O. Osunmakinde, “Emerging bimodal biometrics authentication for non-venue-based assessments in open distance e-learning (OdeL) environments,” 2020.

[23] Institute of Electrical and Electronics Engineers. and Bangalore. Indian Institute of Science, 2011 National Conference on Communications (NCC) : NCC 2011 : Indian Institute of Science, Bangalore, India, 28-30 January 2011. IEEE, 2011.