Visvesvaraya Technological University

"Jnana Sangama", Belagavi-590 018, KARNATAKA, INDIA

A PROJECT REPORT ON

"BIOMETRIC AUTHENTICATION"

Submitted in partial fulfilment of the requirements for the award of the degree of

BACHELOR OF ENGINEERING IN

COMPUTER SCIENCE AND ENGINEERING

Submitted by:

Kalpitha S	**1JS19CS071**
Nithya M Kattimani	**1JS19CS109**
Palguni BM	**1JS19CS111**
R Sahana	**1JS19CS128**

Under the guidance of

Mrs. Impana K P

Assistant Professor

Department of Computer Science and Engineering

JSSATE, Bengaluru

JSS Academy of Technical Education, Bengaluru

Department of Computer Science and Engineering

2022 – 2023

JSS MAHAVIDYAPEETHA, BENGALURU

JSS ACADEMY OF TECHNICAL EDUCATION

JSS Campus, Uttarahalli-Kengeri Main Road, Bengaluru – 560060

Department of Computer Science and Engineering

CERTIFICATE

This is to certify that the Project work entitled "**BIOMETRIC AUTHENTICATION**" is a bonafide work carried out by **Ms. KALPITHA S (1JS19CS071), Ms. NITHYA M KATTIMANI (1JS19CS109), Ms. PALGUNI B M (1JS19CS111)** and **Ms. R SAHANA (1JS19CS128)** in partial fulfillment of the degree of Bachelor of Engineering in Computer Science and Engineering of the Visvesvaraya Technological University, Belgaum during the academic year 2022 – 2023. It is certified that all corrections and suggestions indicated for Internal Assessment have been incorporated in the report. The project has been approved as it satisfies the academic requirements in respect of the project work prescribed for the said degree.

Mrs. Impana KP	**Dr. P B Mallikarjuna**	**Dr.Bhimasen Soragaon**
Assistant Professor	Professor and Head	Principal
Dept. CSE, JSSATE-B	Dept. CSE, JSSATE-B	JSSATE-B

External Viva

Name of the Examiners	**Signature with Date**
1)…….	**1)……**
2)…….	**2)……**

ABSTRACT

With the rapid pace of technological growth, it is very important to secure user data. A robust technique that not only secures data but prevents it from various attacks is necessary. Such a technique is proposed in this article. Biometric authentication is one such practice seen today. In contrast to other forms of authentication, biometric recognition provides a strong link between a data record and an individual and it guarantees a high level of accuracy and security. But this biometric data can be used by attackers to get illegal access. A robust technique that not only secures data but prevents it from various attacks is necessary. Such a technique is proposed in this article. Biometric authentication (watermarking) is one such practice seen today. In contrast to other forms of authentication, biometric recognition provides a strong link between a data record and an individual and it guarantees a high level of accuracy and security. But this biometric data can be used by attackers to get illegal access. In order to prevent such acts, a robust technique known as zero-bit watermarking is proposed. The goal of this project is to identify someone who makes no mistakes, uses up less time, and avoids errors in small spaces. The process for fingerprint authentication divides identification into phases and gets rid of a lot of bogus prints at each phase. The high recognition rate of this results in significant time savings. Significant advancements in the industry demonstrate that for higher recognition, iris, and fingerprint biometrics still need quick, real-time, dependable, and strong algorithms.

ACKNOWLEDGEMENT

With utmost joy and satisfaction, we submit this Project Report on **"BIOMETRIC AUTHENTICATION"**. This has been completed as a part of the curriculum of Visvesvaraya Technological University.

The satisfaction that accompanies the successful completion of our project would be incomplete without mentioning the people who made it possible, whose constant guidance and encouragement crown all the efforts with success.

We take immense pleasure in thanking **Dr. Bhimasen Soragaon**, Principal, JSSATE, Bengaluru, for being kind enough to allow us to work on the Project in this institution.

We are also thankful to **Dr. Mallikarjuna P B**, Professor and Head of the Department of Computer Science and Engineering, for his cooperation and encouragement at all moments of approach.

We are thankful to **Ms. Shantala K V** and **Mrs. Shweta Kaddi**, Assistant Professors, and Project Coordinator, for their cooperation and support.

We are thankful to our Project guide **Mrs. Impana K P**, Assistant Professor, for her constant support and encouragement.

We wish to thank every teaching and non-teaching faculty of our department for always being there to support and guide us.

KALPITHA S (1JS19CS071)

NITHYA M KATTIMANI (IJSI9CS109)

PALGUNI B M (1JS19CS111)

R SAHANA (1JS19CS128)

TABLE OF CONTENTS

TABLE OF FIGURES

CHAPTER 1
INTRODUCTION

1.1 Overview

Data security is essential for protecting sensitive or personal information, complying with regulations, maintaining trust, and protecting intellectual property. Data breaches can result in identity theft, fraud, legal action, and damage to an organization's reputation. Securing data is necessary for complying with laws and regulations, building trust with customers, protecting intellectual property, and maintaining a competitive advantage. With the increasing amount of data being generated and stored, it is more important than ever for organizations to implement strong security measures to protect their data.

Biometrics is playing an increasingly important role in data security. Biometrics involves using a person's unique physical or behavioral characteristics, such as fingerprints, facial features, iris patterns, voiceprints, or even their gait, to authenticate their identity. Biometric authentication can be used to verify a person's identity and grant access to secure data or physical spaces. Biometric authentication is becoming more popular because it provides a more secure form of authentication than traditional methods such as passwords or PINs, which can be easily stolen or guessed.

Biometric data is unique to each individual and cannot be easily replicated, making it difficult for someone to impersonate another person. Biometric authentication provides a convenient and user-friendly way to access secure data or physical spaces without the need to remember passwords or carry physical keys or access cards.

Biometric authentication can be integrated into mobile devices, laptops, and other devices, making it easy to use and widely available. An image which needs to be secured is given as input along with the user’s iris and fingerprint. After combining all of these images, one-time password authentication takes place, and an encrypted image is generated. To see the original image that was uploaded, which is decrypting the image, we do the opposite of encryption.

The encrypted image is uploaded along with the same user's iris and fingerprint that were uploaded earlier to get the original image after a one-time password authentication. A mismatch error is displayed to the user in the event that the iris and fingerprint images are different or if the one-time password is incorrect.

1.2 Existing System

There are several existing systems for biometric authentication of data, including fingerprint recognition, facial recognition, iris recognition, voice recognition, behavioral biometrics, and multimodal biometrics. These systems use a person's unique physical or behavioral characteristics to verify their identity, providing a more secure, convenient, and user-friendly method of authentication than traditional methods such as passwords or PINs. Biometric authentication can be integrated into a variety of devices and applications, including smartphones, laptops, and physical access control systems. Many organizations are adopting biometric authentication to improve security, increase convenience, and reduce the risk of data breaches. However, it is important to ensure that these systems are secure and protect the privacy of user data. By implementing biometric authentication, organizations can increase the security of their data and protect sensitive information from unauthorized access. This method, is not so secure because different recognitions can be altered or forged, making the data vulnerable to attacks. Overall, there is a need for more reliable systems that enable users to effectively secure the data.

1.3 Problem Statement

The problem addressed in this report is the need for a more secure and reliable method of data authentication. Traditional methods of authentication, such as passwords and PINs, are vulnerable to hacking and fraud, leading to data breaches and security threats. To overcome these limitations, biometric authentication using iris and fingerprint data is a promising solution. However, there is a need to evaluate the accuracy, reliability, and security of such a system and to identify the challenges and limitations of implementing it. This aims to explore the potential of using iris and fingerprint biometrics for authentication purposes, examine the existing systems, and propose a solution for secure authentication. It also highlights the advantages of using multimodal biometrics for authentication and discusses the potential applications of this technology in various industries. By addressing the problem of data authentication, this aims to provide insights into the benefits and challenges of using iris and fingerprint biometrics to enhance security and protect sensitive data. The data that is to be stored is encrypted and secured with the help of biometric authentication. This project's objective is to create and authenticate the users data that is precise, inexpensive, and available to a variety of users.

1.4 Proposed System

The core of this study is to secure the user's data in an effective manner. Security measures such as encryption of the biometric data and the use of secure communication protocols are necessary to ensure the system is secure and protects user privacy. A proposed system for authentication using both iris and fingerprint biometrics involves enrolling the user's biometric data and using it to verify their identity during the authentication process. When a user attempts to access a secure system or physical space, they are prompted to present their iris and fingerprint for authentication. The system captures the biometric data and compares it to the stored data on file for that user. If both the iris and fingerprint data match, along with the one-time password generated in the authentication process the user is granted access. This system provides a high level of security and accuracy by combining two highly accurate and difficult-to-fake biometric factors. It also provides redundancy in case one biometric factor fails or is compromised. In case of an authentication failure, the user could be given the option to retry the authentication process or use an alternative authentication method. Overall, a biometric authentication system using both iris and fingerprint data can provide a more secure and convenient method of authentication compared to traditional methods such as passwords or Pins. For the benefit of this project, these operations will be at the backend and showing a user interface in the front-end for the user. This system seeks to be precise, reliable, and usable by a variety of users to secure data. It will not require any specialized tools or additional user training because it will be made to function with common computer hardware.

1.5 Advantages of Proposed System

There are several advantages to combining iris and fingerprint biometrics for authentication purposes:

- Increased accuracy: Iris and fingerprint biometrics are both highly accurate and difficult to fake. By combining these two biometric factors, the accuracy of the authentication process can be increased even further, reducing the risk of unauthorized access.

- Redundancy: Combining iris and fingerprint biometrics provides redundancy in case one biometric factor fails or is compromised. For example, if someone injures their finger or wears gloves, fingerprint authentication may not be possible. However, iris authentication can still be used in such situations. Similarly, if someone has an eye injury or wears contact lenses, iris authentication may not be possible, but fingerprint authentication can still be used.

- More secure: Combining multiple biometric factors, such as iris and fingerprint, can provide a more robust and secure form of authentication than using a single factor alone. Multimodal biometric authentication can help to overcome the limitations of individual biometric factors, such as false positives or false negatives, and increase the overall accuracy and reliability of the authentication process.

- Convenience: Biometric authentication using iris and fingerprint data is more convenient for users than traditional methods such as passwords or PINs. Users do not need to remember complex passwords or worry about forgetting them. Instead, they can simply present their biometric data to access secure systems or physical spaces.
- Usability: The proposed approach is made to be simple to use and does not call for further user training. It is intuitive and simple to use because it iris and fingerprints.

- Utility: The suggested method is made to be simple to use and does not call for further user training. It is intuitive and simple to use because it uses iris and fingerprints.

Overall, combining iris and fingerprint biometrics for authentication purposes provides increased accuracy, redundancy, security, and convenience, making it a promising solution for secure authentication in various industries and applications.

CHAPTER 2

LITERATURE SURVEY

2.1 Biometric Accreditation Adoption Using Iris and Fingerprint

The paper "Biometric Accreditation Adoption using Iris and Fingerprint" by Ojasvi Dere and Srushti Gaikwad, published in July 2021, focuses on the use of iris and fingerprint biometrics, which are widely used for authentication purposes. The paper provides a comprehensive overview of the various techniques and technologies used in biometric authentication, including their advantages and limitations. It also discusses the challenges associated with the adoption of biometric accreditation, such as privacy concerns and the need for robust security measures. The authors propose a framework for the implementation of biometric accreditation using iris and fingerprint biometrics. The framework includes various stages such as enrollment, identification, verification, and revocation. They also discuss the various factors that need to be considered while implementing biometric accreditation, such as the choice of biometric technology, the accuracy of the system, and the cost-effectiveness of the solution.

2.2 Digital Watermarking Technology in Information security

The paper "Digital Watermarking Technology in Information Security" by Naga Lakshmi, Ruchitha, Lavanya, Sai Greeshmanth, and Bhanu Prakash, published in May 2022, emphasizes the importance of digital watermarking technology in information security, especially in the context of digital media such as images, audio, and video. It provides valuable insights into the implementation of digital watermarking technology, making it a useful resource for researchers and practitioners in the field of information security. Digital image watermarking using many methods has been valuable as a significant tool for image authorization, honesty verification, restricted detection, copyright safety, and digital safety of an image. Overall, digital image watermarking plays a crucial role in ensuring the security and integrity of digital images, and its use has become increasingly important in today's digital world.

2.3 Steganographic Scheme for Outsourced Biomedical Time Series Data Using an Intelligent Learning-A Research

The paper "Steganographic Scheme for Outsourced Biomedical Time Series Data Using an Intelligent Learning - A Research" by Harshala Pundkar and Dr. Atul Joshi, published in November 2019, proposes an intelligent learning-based watermarking scheme for outsourced biomedical time series data, which addresses the challenge of sharing data between owners and data mining experts in the healthcare field. The proposed scheme uses a modified mean modulation relationship of approximation coefficients in the wavelet domain to embed the watermark data. The scheme is based on intelligent learning and is more robust against various signal processing techniques and common attacks. Experimental results on EEG data with lifting wavelet transform show good imperceptibility and robustness of the proposed scheme. The conventional watermarking techniques are rule-based and do not directly deal with data synchronization, leading to reduced decoding performance when transmitted through a real communication channel. The proposed scheme overcomes this limitation and provides detectable evidence for the legal ownership of shared datasets without compromising their usability.

2.4 A Review on Color Image Watermarking based on Wavelet and QR Decomposition

The paper "A Review on Colour Image Watermarking based on Wavelet and QR Decomposition" by Divya Audichya and Dr. Vikas Soni, published in December 2019, discusses the challenges associated with colour image watermarking, such as the need for robustness, imperceptibility, and security. This paper presents a hybrid blind digital image watermarking technique that combines redundant discrete wavelet transform (RDWT) with singular value decomposition (SVD) to achieve a balance between imperceptibility and robustness. The proposed technique is non-blind, robust, and reversible and can be used for applications such as copyright protection, ownership verification, content authentication, and sensitive applications that require high robustness and reversibility. The experimental results show that the proposed algorithm is effective in resisting attacks such as rotation, scaling, blurring, contrast, JPEG compression, histogram equalization, affine transformation, mean filtering, and Gaussian noise, and the visual quality of the extracted original image is indistinguishable.

2.5 A Genetic Approach for Reversible Database Watermarking using Fingerprint masking

The paper " A Genetic Approach for Reversible Database Watermarking using Fingerprint masking " by J.Menaka Gandhi, T.J Shredha, S.Vishali, V.K. Vishnupriya, published in March 2020, discusses the challenges related to security and privacy of large datasets that are stored in the cloud or shared over the internet in encrypted format. It proposes the use of watermarking techniques to enforce proprietary rights on shared relational databases, but highlights that existing methods compromise the original data to a large extent, leading to a tradeoff between robustness, data quality degradation, malicious attacks, and data recovery. To address these issues, the paper introduces a new reversible database watermarking technique called Genetic Fingerprinting Algorithm using Histogram shifting (GFAHS), which encodes the original database along with the fingerprint of the owner and watermarks them together. The proposed technique is claimed to be robust and prevent illegal ownership violations.

CHAPTER 3

REQUIREMENTS

3.1 Functional Requirements

- Media/Carrier File: This file acts as a carrier file for our data. We can share this file after encrypting or hiding our data within it.
- Data File: This is the file or data which we want to hide in our carrier file. We can securely send this file by hiding or embedding it into other media files.
- Encryption Algorithm: This is the algorithm or lines of codes which we can apply to encrypt or to hide our data within a selected media file. After encryption, we will get an encrypted media file as an output. We can save or share this output. When the intended user receives the encrypted media file, then he/she requires the following in order to retrieve the original message:
- Decryption Algorithm: This is required to decrypt or extract the original data file from the received or saved encrypted media file. Users then can save this original message or data to a particular location on his/her computer.
- For fingerprint matching the model was trained on the fingerprint images dataset.

3.2 Non-Functional Requirements

Non-functional requirements describe how the system should work or, in other words, how the system or model should act. There are a variety of attributes that are considered non-functional system requirements. Performance, scalability, adaptability, portability, maintainability, and reliability are a few of them. Nonfunctional requirements are often known as system quality attributes. These are only attributes of a system in development, hence there are no codes to execute them. On the basis of client need, the traits might be prioritized. Only those requirements that are absolutely important for the project should be chosen. Some Non-Functional Requirements are as follows:

- Reliability

  The application should be good enough that people, or in this case, disabled people, can trust the model's predictions. If the people of special needs don't trust the application's expected outcome, it isn't very useful. People should be able to trust the application if it makes accurate detections.

- Maintainability

  Maintenance should not be complicated or tough because the application will be executed and run on a range of machines after deployment. Problem detection should be quick and easy if it creates issues or crashes at that time.

- Performance

  The performance of the iris and fingerprint biometric authentication system is characterized by its accuracy, speed, reliability, usability, and security. In terms of accuracy, the system offers high precision due to the uniqueness and stability of these biometric factors. The false acceptance rate (FAR) and false rejection rate (FRR) are important accuracy metrics for biometric authentication, and the iris and fingerprint biometric system has been shown to achieve low FAR and FRR values.

- Portability

  The application should not be restricted to a single or a small number of systems. It should also be available on other platforms. In this project, for example, we used the web server to make the model portable. User only needs to install/extract necessary files that are required to run the application., the entire application can be accessible via the internet platform.

- Scalability

  The structure should be versatile enough to allow for the inclusion of new features in the future. Scalability: The system can be scaled up or down to accommodate different numbers of users and devices. It can be implemented in small-scale applications such as home security systems, or in large-scale applications such as national identity databases.

- Flexibility

  This non-functionality feature refers to a system's inability to cope with changing events and conditions, resulting in its ineffectiveness lack adapting to new rules and approaches. When a system is adaptable, it will have little trouble reorganizing itself to accommodate the necessary changes. When approaches change, the application's flexibility becomes a critical factor. As a result, it's critical for a system to be adaptable and flexible enough to meet the demands.

3.3 Hardware Requirements for the Model

- System Processor required - Core i3 / i5 2.4GHz
- Hard Disk required - 500 GB
- Ram required - 4 GB

❖ Any desktop / Laptop system having these configurations is good

3.4 Software Requirements for the Model

- Operating system required - Windows XP/Windows 7/8/10
- Programming Language used - Python
- Framework needed - Flask
- IDLE used – Python IDLE, VS Code

CHAPTER 4

SYSTEM ARCHITECTURE AND DESIGN

4.1 System Design

System design is the process of defining the architecture, components, modules, interfaces, and data for a system to satisfy specified requirements. It involves creating a detailed technical specification for how the system will be built and how its components will work together to achieve the desired functionality and performance. System design can be applied to a wide range of systems, including software, hardware, and integrated systems that combine both. The design process typically involves several steps, including requirements analysis, architecture design, component selection, interface design, and testing. During the system design process, designers must consider factors such as reliability, maintainability, scalability, and security, as well as performance requirements like response time, throughput, and capacity. Once the system design is complete, it serves as a blueprint for the actual implementation of the system, providing a roadmap for the development team to follow and ensuring that the final product meets the requirements of the stakeholders.

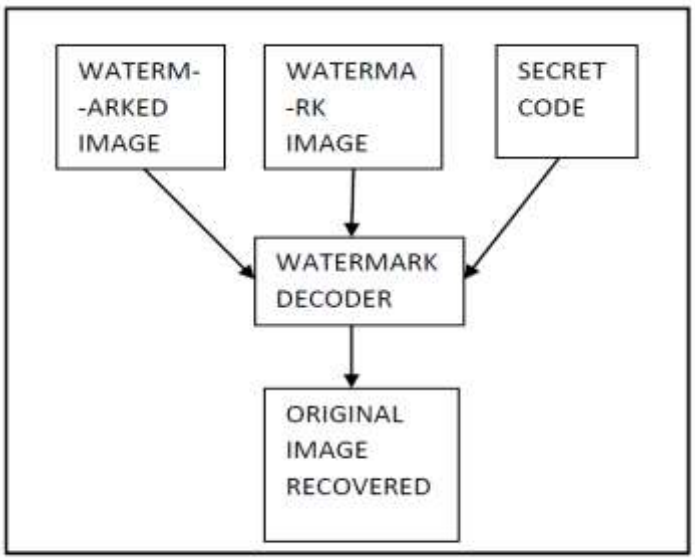


Fig -2: Original image reception at destination

Fig:4.1 Architecture Diagram

4.2 Object-Oriented Design

4.2.1 Class Diagram:

A class diagram is a type of diagram used in object-oriented programming (OOP) to visualize the structure of a system or software application. It shows the classes and their relationships to each other, including their attributes, methods, and associations.

A class is a blueprint or template for creating objects that encapsulate data and behavior. The class diagram displays the class name at the top, followed by its attributes (data members) and methods (functions). Arrows indicate relationships between classes, such as inheritance, composition, or association. In addition to classes, class diagrams may also include interfaces, abstract classes, and packages, which are used to organize related classes. They provide a high-level view of the system architecture and can be used to communicate design decisions to other developers or stakeholders. Class diagrams are often created during the analysis and design phase of software development and can be updated throughout the development lifecycle.

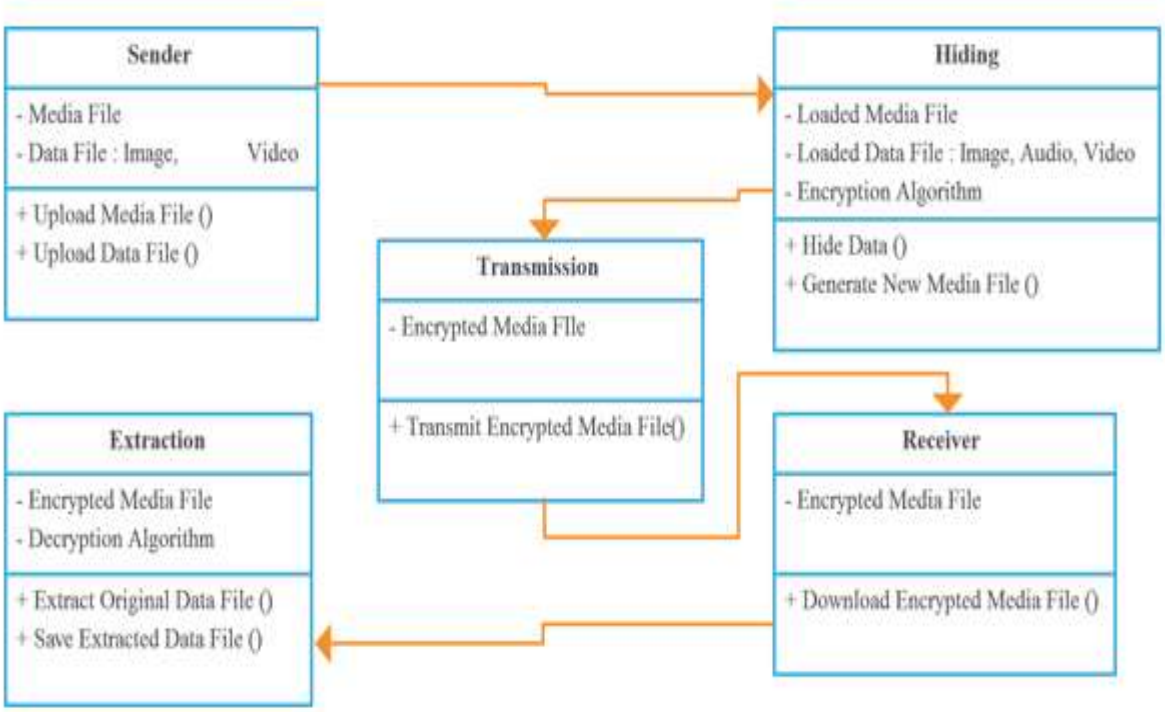


Fig:4.2.1 Class Diagram

4.2.2 Data Flow Diagram:

A dataflow outline is a tool for referring to knowledge progression from one module to the next module as shown in Fig 4.3.2. This graph gives the data of each module's info. The map has no power flow and there are no circles at the same time.

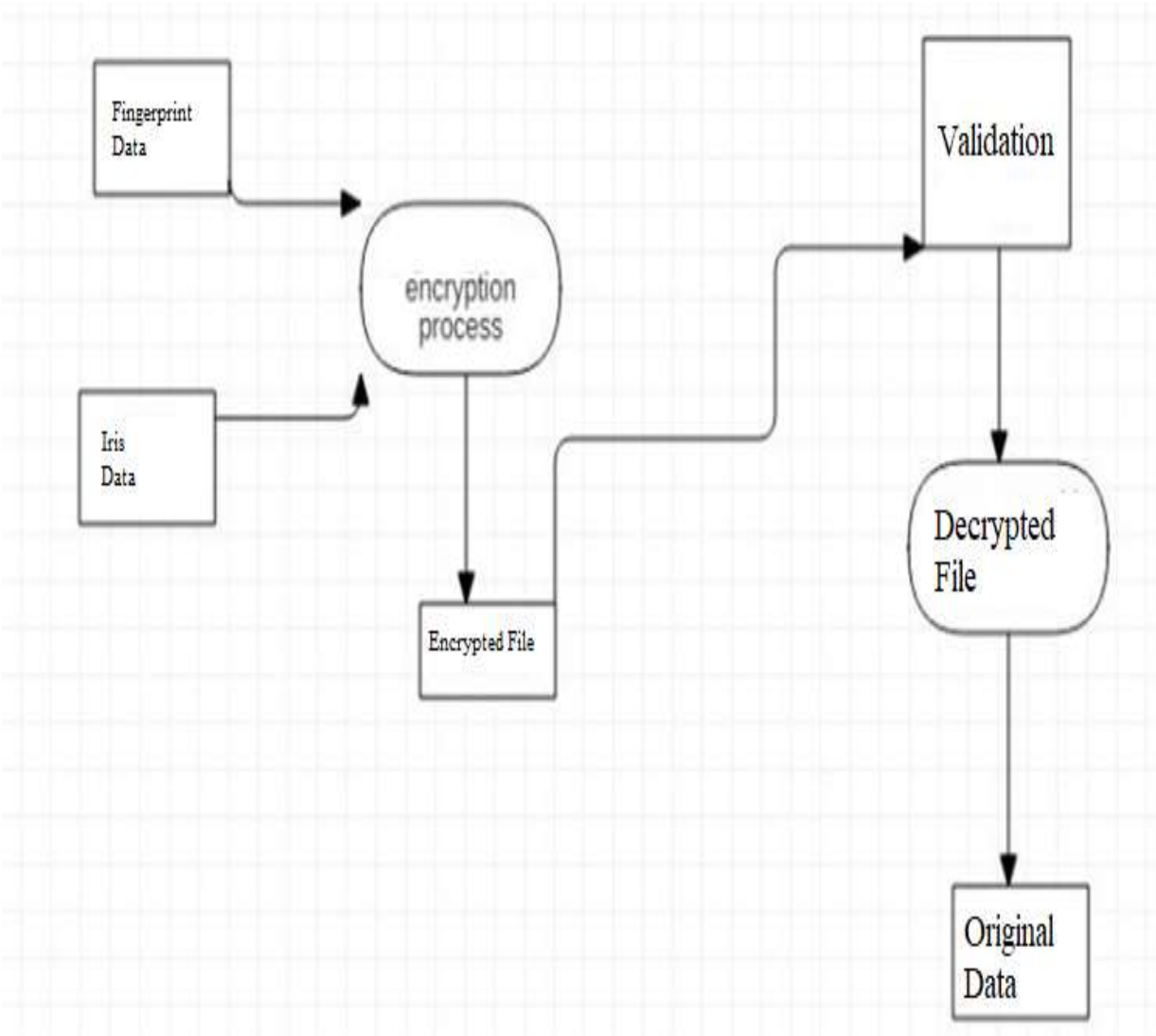


Fig:4.2.2 Data Flow Diagram

4.2.3 Use Case Diagram:

A Use Case Diagram is a lot of situations that reflect a client-frame relationship. A use case chart shows the entertainer-to-use relationship. Usage cases and on-screen characters are the two main elements of a usage case diagram. An on-screen character refers to a user or other person connected with the demonstrated process. A use case chart in Figure 4.3.3 is an out-of-the-box perspective that speaks to some activity each module will perform to complete an errand.

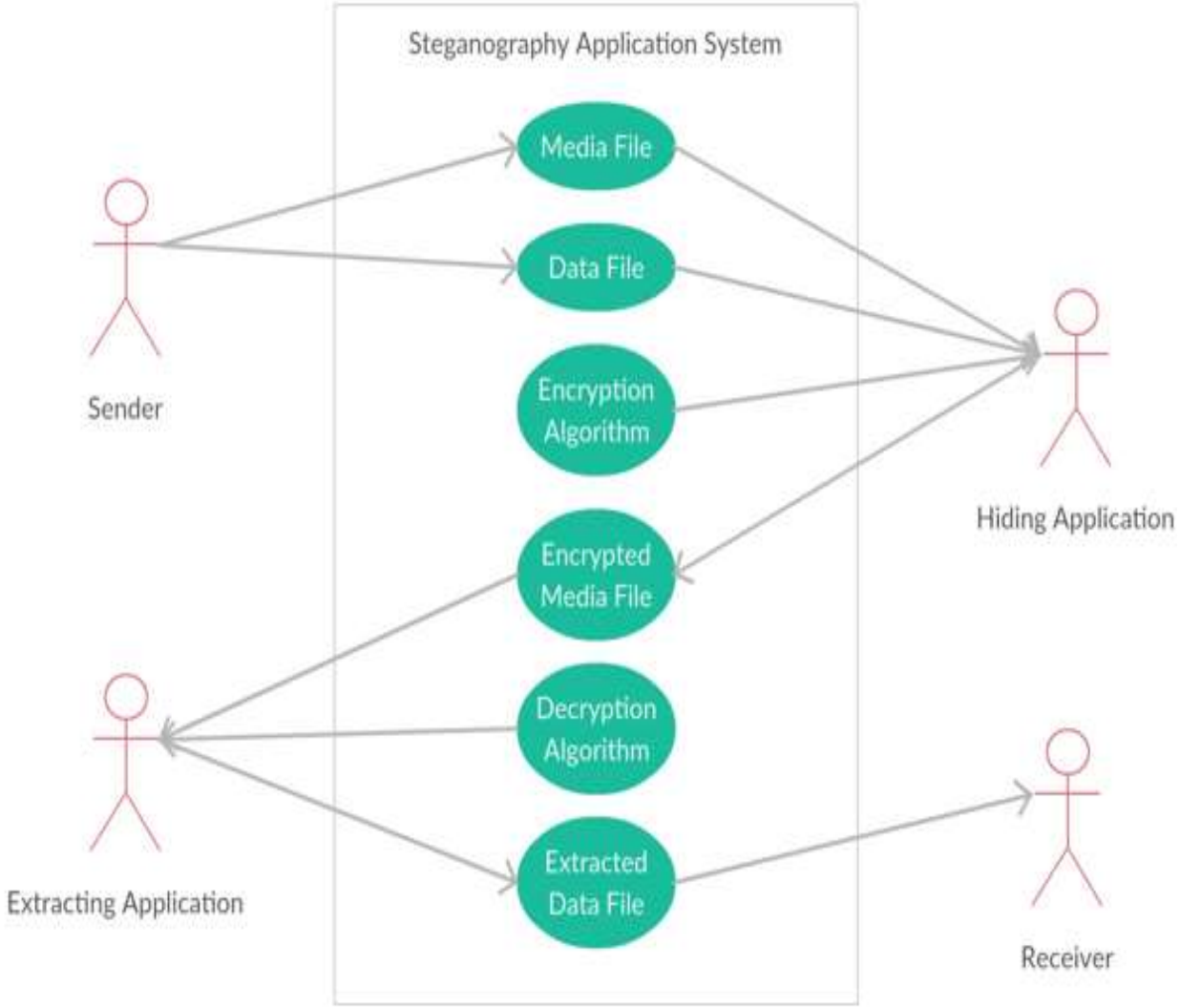


Fig 4.2.3 Use Case Diagram

4.2.4 Sequence Diagram

A sequence diagram is a type of interaction diagram that shows how objects in a system interact with each other over time to complete a particular task or use case. It depicts the messages exchanged between the objects in chronological order to represent the sequence of events that occur during the execution of a scenario. Sequence diagrams typically have two dimensions, vertical and horizontal. The vertical dimension represents time, while the horizontal dimension represents the objects or actors involved in the interaction. Each object or actor is represented as a lifeline, which is a dashed line extending downward from the object or actor's name, and the messages sent between them are represented by arrows.

Sequence diagrams can also show various types of messages, including synchronous and asynchronous messages, self-messages, and return messages. Synchronous messages are sent and received in a blocking manner, while asynchronous messages are sent and received in a non-blocking manner. Self-messages are used to represent a message sent by an object to itself. Sequence diagrams are commonly used during the design phase of software development to model the behavior of a system and validate the correctness of the design. They are also useful for documenting and communicating the system's behavior to stakeholders and developers.

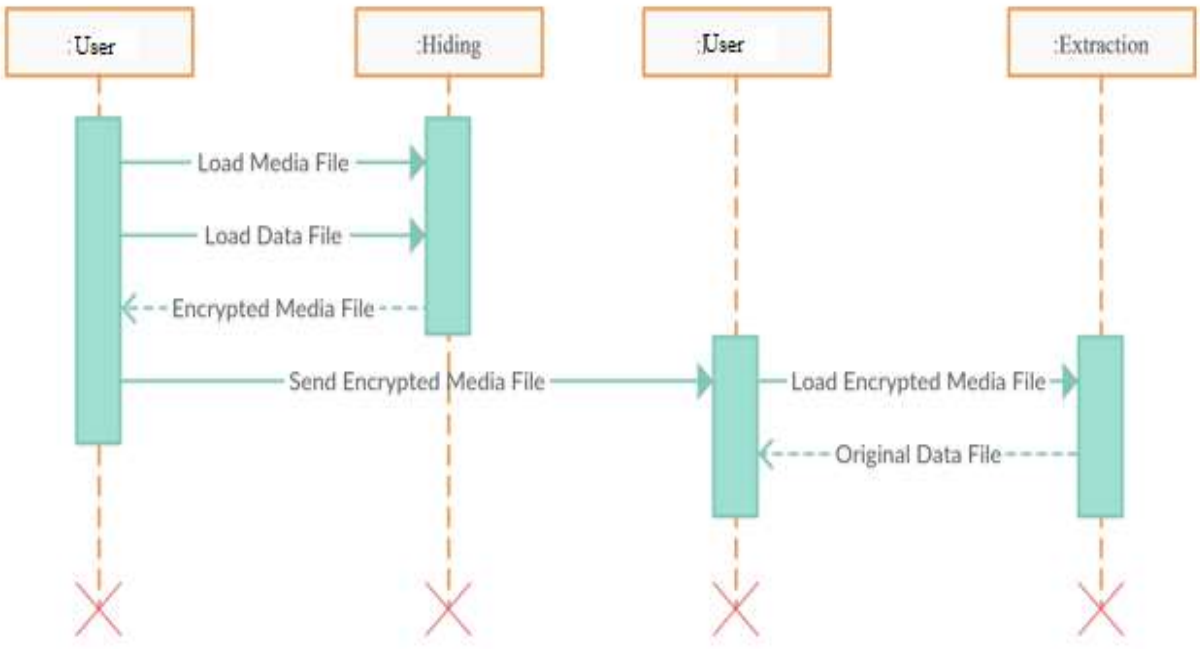


Fig 4.2.4 Sequence Diagram

4.2.5 Activity Diagram

An activity diagram is a type of behavioral diagram in UML that models the flow of control from activity to activity within a system or business process. It describes the steps involved in completing a specific task or activity and the order in which they occur. The diagram consists of nodes and edges that represent the activities and transitions between them. Activity diagrams are useful for visualizing business workflows, software processes, and system behavior, and are commonly used during the requirements analysis and design phases of software development. They can also be used to model complex logic and decision-making processes.

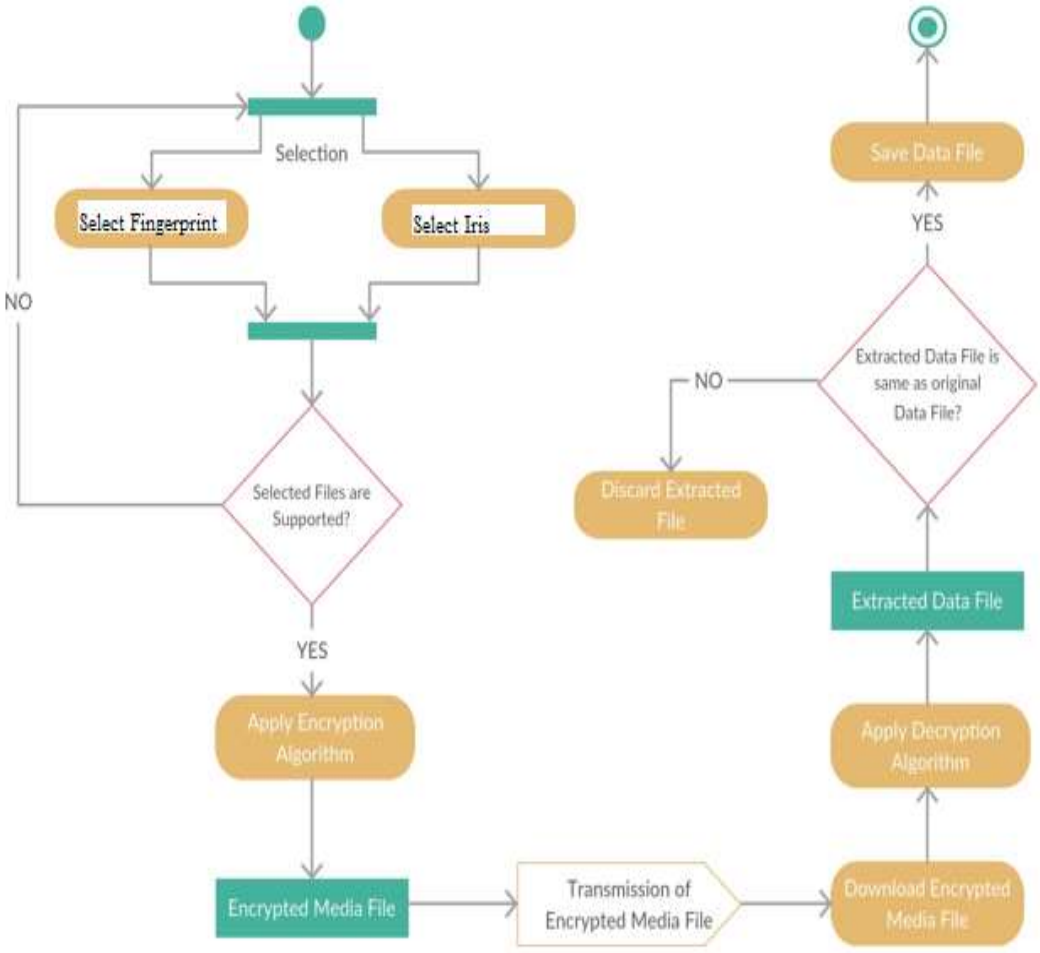


Fig:4.2.5 Activity Diagram

4.3 Modules

4.3.1 Finger Print detection Using CNN

Convolutional Neural Network (CNN) to recognize fingerprints. This is a supervised learning task, so the code uses a dataset of fingerprint images along with their corresponding labels (real or fake) to train the network.

- Importing the necessary libraries such as numpy, cv2, os, tflearn, etc.
- Defining some parameters such as image size, learning rate, etc.
- Reading the dataset of fingerprint images, which are located in two separate directories for real and fake fingerprints.
- Preprocessing the images, which involves resizing them, converting them to grayscale
- Creating the CNN architecture using the TFLearn library, which includes input layers, convolutional layers, pooling layers, fully connected layers, and output layers.
- Training the CNN using the fingerprint dataset, and saving the trained model in a file for future use.

Steps:

1. Import necessary libraries including OpenCV for image processing, NumPy for numerical operations, os for working with files and directories, shuffle for shuffling data, and tqdm for a progress bar.
2. Define the directories where training and test images are located, the size of the images to be processed, the learning rate for the model, and the name of the model.
3. Define a function to label the images based on whether they are fake or live. The function returns a one-hot encoded label indicating whether the image is fake or live.
4. Define a function to create the training dataset. The function loops over each image in the training directory, labels it using the label_img() function, reads the image, resizes it to the required size, and appends it and its label to a list. The function then shuffles the data and saves it as a Numpy array.
5. Define a function to process the test dataset. The function loops over each image in the test directory, reads it, resizes it to the required size, and appends it and its corresponding filename to a list. The function then shuffles the data and saves it as a Numpy array.

6. Call the create_train_data() function to create the training dataset.Define a convolutional neural network using the TFLearn library. The network consists of multiple convolutional layers and fully connected layers.
7. Check if the model file already exists and load it if it does.
8. Split the training data into training and validation sets.
9. Reshape the training and validation data to the required dimensions.
10. Train the model on the training data and validate it on the validation data. The model is trained for 10 epochs, and the results are displayed using the show_metric parameter.
11. Save the trained model.

4.3.2 Iris Detection

Iris detection is a biometric identification technique that uses the unique patterns in the iris of the eye to identify individuals. Daugman's algorithm is a commonly used technique for iris detection and recognition, which involves several steps. First, an image of the eye is captured using a digital camera or other imaging device.

The image is then preprocessed to remove noise and enhance the contrast of the iris region. Next, the iris region is isolated using techniques such as edge detection and segmentation. The circular boundary of the iris is then located using a process called circular Hough transform.Once the boundary is identified, the iris region is divided into a series of concentric circles or annuli.

For each annulus, a set of wavelet coefficients is computed using a 2D Gabor filter. These coefficients represent the texture and patterns in the iris region.The wavelet coefficients are normalized to remove variations due to factors such as illumination and camera distortion. The normalized coefficients are then compared to a database of pre-registered iris templates using a similarity measure such as Hamming distance.

If the similarity between the templates is above a certain threshold, the iris is considered a match and the individual is identified. Daugman's algorithm has been shown to be highly accurate and robust for iris recognition, making it a popular choice for biometric identification applications.

Steps

1. Define a function called daugman that takes in a grayscale image, center point, starting and ending radii, and a step size as input.
2. Create an empty list called intensities and a mask array of the same size as the input image.
3. Create a list of radii values ranging from start_r to end_r with a step of step.
4. For each radius value in the list, draw a circle on the mask array with the given center and radius, and apply a bitwise AND operation between the grayscale image and the mask array to obtain the pixels within the circle.
5. Normalize the pixel values by dividing the sum of pixel intensities within the circle by the circle's circumference.
6. Append the normalized intensity value to the intensities list, and reset the mask array to all zeros.
7. Compute the intensity differences between adjacent radii in the intensities list, and apply a Gaussian blur to the resulting array to obtain a smoothed intensity profile.
8. Find the index of the maximum value in the smoothed intensity profile, and return the intensity value and radius at that index.
9. Define another function called find_iris that takes in a grayscale image, starting and ending radii for the daugman function, and step sizes for points and radii as input.
10. Find the height and width of the input image, and check if it is a square image.
11. Define a range of points within the central 1/3 of the image, and obtain all possible combinations of these points using the itertools.product function.
12. For each point in the list of all possible combinations, apply the daugman function to obtain the intensity value and radius with the maximum intensiveness delta.
13. Find the index of the maximum intensity value among all the points, and return the corresponding point coordinates and radius as output.

4.3.3 Encryption and Decryption

For encryption of the image that is being uploaded the Rubix cube approach is used The Rubik's cube encryption method is a type of encryption that uses a Rubik's cube as a substitute for a traditional encryption algorithm. It is a symmetric key encryption method, meaning that the same key is used for both encryption and decryption. The plaintext is divided into fixed-length blocks and each block is mapped onto a unique configuration of the Rubik's cube by rotating the faces of the cube according to a predetermined algorithm. The resulting scrambled cube configuration is then transmitted as the ciphertext. To decrypt the ciphertext, the receiver uses the same Rubik's cube and algorithm to rotate the cube faces back to their original positions. While the method is easy to implement and flexible in terms of changing the encryption key, it is vulnerable to brute force attacks and chosen-plaintext attacks. It should, therefore, be used with caution and in conjunction with other security measures to ensure the protection of sensitive information.

Steps

1. Create an instance of the RubikCubeCrypto class by passing an image object to the constructor.
2. Generate the encryption key by calling the create_key method with the following parameters:

- alpha: A hyperparameter value used to generate the two vectors Kr and Kc, which are used in the encryption and decryption process.
- iter_max: The maximum number of iterations to perform during the encryption and decryption process.
- key_filename: The name of the file in which the generated key will be saved.

3. Load an encryption key from a file by calling the load_key method and passing the name of the key file as a parameter.
4. Perform the rolling rows stage of the encryption/decryption process by calling the roll_row method with the following parameter:

   encrypt_flag: A boolean flag that determines whether to perform encryption or decryption. If set to True, encryption will be performed. If set to False, decryption will be performed.

5. Perform the shifting columns stage of the encryption/decryption process by calling the roll_column method with the following parameter:

- encrypt_flag: A boolean flag that determines whether to perform encryption or decryption. If set to True, encryption will be performed. If set to False, decryption will be performed.

6. Perform the XOR stage of the encryption/decryption process by calling the xor_with_key method with the following parameter:
    - encrypt_flag: A boolean flag that determines whether to perform encryption or decryption. If set to True, encryption will be performed. If set to False, decryption will be performed.
7. Save the encrypted or decrypted image by calling the save_image method and passing the name of the output file as a parameter.

Steps 4, 5, and 6 can be repeated iter_max a number of times to increase the strength of encryption or decryption. The output of each stage is fed as input to the next stage.

CHAPTER 5

IMPLEMENTATION TECHNOLOGIES

5.1 Introduction

The acknowledgment of an application or execution of an arrangement, thought, model, plan, determination, standard, calculation, or strategy is known as usage. At the end of the day, a program, program part, or any other PC framework through programming and arrangement recognizes a specialized determination or calculation. Numerous usages may exist for a given particular standard.Execution is one of the most significant periods of the Software Development Life Cycle (SDLC). It covers all procedures for the proper functioning of new programming or equipment, including set-up, design, execution, testing, and implementation of important charges. It codes the framework using a certain language of programming and moves the structure into an actual framework.

5.2 Overview of System Implementation

This project is implemented considering the following aspects:

• Usability aspect

• Technical aspect

5.2.1 Usability aspect

Python is a high-level, multiple-purpose programming language. Its design philosophy places a strong emphasis on code readability through the use of off-side rule-based considerable indentation.Python uses garbage collection and has dynamic typing. It supports a variety of paradigms for programming, including structured, object-oriented, and functional programming.Python is a language structure in addition to its objectively oriented approach, which aids programmers in creating logically clear code for both big and small projects. Python is created dynamically and garbage is gathered. It supports a variety of programming paradigms, including object-oriented, functional, and structured programming (partly procedural). Python features a robust tape frame and the pre-programmed memory of the executives. It supports a variety of ideal programming models, such as object-set, fundamental, useful, and procedural models. It includes a huge and thorough standard library.Python mediators are available for some working frameworks. The Python system's primary execution, CPython, uses an open-source network-based enhancement approach. Python and CPython are

in charge of the non-profit Python Software Foundation.

5.2.2 Technical aspect

The technical aspect of the project's implementation is carried out according to the following principle:

5.2.2.1 OpenCV:

OpenCV is a software library for computer vision and machine learning. It is a standard infrastructure for computer vision applications created in order to speed up the incorporation of artificial intelligence into products by providing features for computer vision and image processing tasks. Either the built-in camera or a web camera can be used to provide input with the VideoCapture() function.

5.2.2.2 Utils:

Classes and functions of general utility are found in the utils module and are used frequently throughout. Pip can be used to install the package (this is the suggested approach): pip installs python-utils. Common Python scripting chores like converting text to numbers and verifying if a string is in Unicode or bytes format are made simple with this module.

5.2.2.3 Numpy:

Nearly all branches of research and engineering use the free source Python library known as NumPy (Numerical Python). It is the established standard for manipulating numerical data in Python and forms the basis of both the PyData and scientific Python ecosystems. The majority of other Python data science and scientific programs, including Pandas, SciPy, Matplotlib, scikit-learn, and scikit-image, make substantial use of the NumPy API. Data structures for multidimensional arrays and matrices are available in the NumPy library (more on this is covered in the next sections). It offers ways to effectively manipulate the homogeneous n-dimensional array object and array. Numerous mathematical operations can be carried out on arrays with NumPy. It provides a vast library of high-level mathematical functions that work on these arrays and matrices.

5.2.2.4 Tqdm

This allows you to create progress bars with just a few lines of code, which can be very useful for visualizing the progress of long-running computations. The library provides several styles of progress bars, including a simple text-based progress bar

5.2.2.5 Tensorflow

TensorFlow is designed to provide a flexible and efficient platform for building and training machine learning models. It supports a wide variety of machine learning algorithms and techniques, including deep neural networks, convolutional neural networks, recurrent neural networks, and more. TensorFlow provides a high-level interface for building and training machine learning models, as well as a lower-level API for more advanced users who want more control over the training process.

5.3 Implementation Support

5.3.1 Installation of Python IDLE

The following are the requirements for the Windows Operating System installation of Python IDLE:

• Windows 7/8/10
• Minimum 4 GB RAM
• Minimum 5 GB disk space
• 3.3 or higher or Python 2.7 Python

5.4 Algorithm Used

5.4.1 Daugman's Algorithm

The Daugman algorithm is a computer vision algorithm used for iris recognition, which is a type of biometric authentication. The algorithm works by analyzing the unique patterns in the iris, such as its texture and color, to create a mathematical model of the iris that can be used to identify individuals.

The iris is first isolated from an image of the eye using edge detection and other techniques. Then, the circular boundary of the iris is located by analyzing the intensity profile of the image along concentric circles.

Next, the iris is divided into a number of wedge-shaped regions, and the texture of each region is analyzed using a process called wavelet decomposition. This produces a set of complex coefficients that describe the texture of each region.

Finally, these coefficients are converted into a binary iris code using a process called quantization, and the resulting code is compared to a database of previously recorded iris codes to identify the individual.

The Daugman algorithm is known for its high accuracy, and has been used in a variety of applications, including border control, banking, and healthcare.

5.4.1.1 Implementation

1. Image Acquisition: A high-resolution image of the iris is acquired using an infrared camera or a high-resolution camera with appropriate lighting.
2. Iris Localization: The iris region is located in the acquired image using image processing techniques such as edge detection, thresholding, and Hough transform.
3. Normalization: The iris region is normalized to a fixed size and orientation to remove any variations caused by the camera's angle, pupil dilation, or eyelid occlusion.
4. Feature Extraction: The normalized iris region is divided into concentric circular bands, and the texture features are extracted using Gabor filters. The extracted features are represented as a binary code, known as an IrisCode.
5. Matching: The IrisCode of the input image is compared with the stored IrisCodes in the database using Hamming distance or other similarity metrics. The image is accepted as a match if the Hamming distance is below a predefined threshold.
6. Template Update: If the input image is accepted as a match, the IrisCode is added to the database or used to update the existing template for the corresponding subject.
7. Enrollment: If the input image is not found in the database, the user is prompted to enroll by providing additional images for template creation.

5.4.2 CNN Algorithm

CNN (Convolutional Neural Network) is a deep learning algorithm commonly used for image classification, object detection, and other computer vision tasks. The CNN algorithm is designed to learn and identify patterns in images by using a hierarchical structure of layers, each of which performs a specific operation on the input.

The basic building blocks of a CNN are convolutional layers, pooling layers, and fully connected layers. Convolutional layers apply a set of learnable filters to the input image, producing a set of output feature maps. Pooling layers downsample the feature maps by applying a pooling operation (e.g. max pooling) to each local region of the feature maps. Finally, fully connected layers process the output of the convolutional and pooling layers to produce the final classification or regression output.CNNs are typically trained using large labeled datasets, such as ImageNet, and use backpropagation to adjust the weights of the filters in the convolutional layers in order to minimize the loss function.

During the training process, the network gradually learns to recognize and extract useful features from the input images, allowing it to accurately classify new images that it has not seen before.

Overall, CNNs are an extremely powerful and widely used algorithm in the field of computer vision and have been applied to a wide range of applications, including self-driving cars, medical image analysis, and facial recognition.

5.4.3 Rubik's Cube Algorithm

Rubik's Cube encryption algorithm is a symmetric key encryption algorithm that uses a Rubik's Cube as the encryption key. It is a relatively simple encryption algorithm that can be used to encrypt small amounts of information.The basic idea behind the Rubik's Cube encryption algorithm is to use the orientation of the Rubik's Cube as the encryption key. The orientation of the cube is determined by the position of each of the cube's faces. By scrambling the cube in a specific way, it is possible to generate a unique encryption key that can be used to encrypt a message.

5.4.3.1 Rubik's Cube-Based Encryption Algorithm

Let I_o represent an α-bit gray scale image of the size $M \times N$. Here, I_o represent the pixels values matrix of image I_o. The steps of encryption algorithm are as follows:

(1) Generate randomly two vectors K_R and K_C of length M and N, respectively. Element $K_R(i)$ and $K_C(j)$ Each take a random value of the set $\mathscr{A} = \{0, 1, 2, \ldots, 2^{\alpha} - 1\}$. Note that both K_R and K_C must not have constant values.

(2) Determine the number of iterations, $\mathrm{ITER}_{\max}$, and initialize the counter ITER at 0.

(3) Increment the counter by one: ITER = ITER + 1.

(4) For each row i of image I_o,

(a) compute the sum of all elements in the row i, this sum is denoted by $\alpha(i)$

$$\alpha(i) = \sum_{j=1}^{N} \mathrm{I}_o(i, j), \quad i = 1, 2, \ldots, M. \tag{1}$$

(b) compute modulo 2 of $\alpha(i)$, denoted by $M_{\alpha(i)}$,

(c) row i is left, or right, circular-shifted by $K_R(i)$ positions (image pixels are moved $K_R(i)$ positions to the left or right direction, and the first pixel moves in last pixel.), according to the following:

$$\begin{aligned} &\text{if} \quad M_{\alpha(i)} = 0 \longrightarrow \text{right circular shift} \\ &\text{else} \longrightarrow \text{left circular shift.} \end{aligned} \tag{2}$$

(5) For each column j of image I_o,

(a) compute the sum of all elements in the column j, this sum is denoted by $\beta(j)$,

$$\beta(j) = \sum_{i=1}^{M} \mathrm{I}_o(i, j), \quad j = 1, 2, \ldots, N. \tag{3}$$

(b) compute modulo 2 of $\beta(j)$, denoted by $M_{\beta(j)}$.

(c) column j is down, or up, circular-shifted by $K_C(i)$ positions, according to the following:

$$\begin{aligned} &\text{if} \quad M_{\beta(j)} = 0 \longrightarrow \text{up circular shift} \\ &\text{else} \longrightarrow \text{down circular shift.} \end{aligned} \tag{4}$$

Steps 4 and 5 above will create a scrambled image, denoted by I_{SCR}.

(6) Using vector K_C, the bitwise XOR operator is applied to each row of scrambled image I_{SCR} using the following expressions:

$$\begin{aligned} \mathrm{I}_1(2i - 1, j) &= \mathrm{I}_{\mathrm{SCR}}(2i - 1, j) \oplus K_C(j), \\ \mathrm{I}_1(2i, j) &= \mathrm{I}_{\mathrm{SCR}}(2i, j) \oplus \mathrm{rot}\,180\,(K_C(j)). \end{aligned} \tag{5}$$

where $\oplus$ and rot $180(K_C)$ represent the bitwise XOR operator and the flipping of vector K_C from left to right, respectively.

(7) Using vector K_R, the bitwise XOR operator is applied to each column of image I_1 using the following formulas:

$$\begin{aligned} \mathrm{I}_{\mathrm{ENC}}(i, 2j-1) &= \mathrm{I}_1(i, 2j-1) \oplus K_R(j), \\ \mathrm{I}_{\mathrm{ENC}}(i, 2j) &= \mathrm{I}_1(i, 2j) \oplus \mathrm{rot}\,180\left(K_R(j)\right). \end{aligned} \tag{6}$$

with rot $180(K_R)$ indicating the left to right flip of vector K_R.

(8) If ITER = $\mathrm{ITER}_{\max}$, then encrypted image I_{ENC} is created and encryption process is done; otherwise, the algorithm branches to step 3.

Vectors K_R, K_C and the max iteration number $\mathrm{ITER}_{\max}$ are considered as secret keys in the proposed encryption algorithm. However, to obtain a fast encryption algorithm it is preferable to set $\mathrm{ITER}_{\max} = 1$ (single iteration). Conversely, if $\mathrm{ITER}_{\mathrm{MAX}} > 1$, then the algorithm is more secure because the key space is larger than for $\mathrm{ITER}_{\mathrm{MAX}} = 1$. Nevertheless, in the simulations presented in Section 3, the number of iterations $\mathrm{ITER}_{\max}$ was set to one.

5.4.3.2 Rubik's Cube-Based Decryption Algorithm

The decrypted image, I_o, is recovered from the encrypted image, I_{ENC}, and the secret keys, K_R, K_C, and $\text{ITER}_{\max}$ as follows in the following.

(1) Initialize ITER = 0.

(2) Increment the counter by one: ITER = ITER + 1.

(3) The bitwise XOR operation is applied on vector K_R and each column of the encrypted image I_{ENC} as follows:

$$\begin{aligned} \mathrm{I}_1(i, 2j-1) &= \mathrm{I}_{\text{ENC}}(i, 2j-1) \oplus K_R(j), \\ \mathrm{I}_1(i, 2j) &= \mathrm{I}_{\text{ENC}}(i, 2j) \oplus \text{rot } 180\left(K_R(j)\right). \end{aligned} \tag{7}$$

(4) Then, using the K_C vector, the bitwise XOR operator is applied to each row of image I_1:

$$\begin{aligned} \mathrm{I}_{\text{SCR}}(2i-1, j) &= \mathrm{I}_1(2i-1, j) \oplus K_C(j), \\ \mathrm{I}_{\text{SCR}}(2i, j) &= \mathrm{I}_1(2i, j) \oplus \text{rot } 180\left(K_C(j)\right). \end{aligned} \tag{8}$$

(5) For each column j of the scrambled image I_{SCR},

(a) compute the sum of all elements in that column j, denoted as $\beta_{\text{SCR}}(j)$:

$$\beta_{\text{SCR}}(j) = \sum_{i=1}^{M} \mathrm{I}_{\text{SCR}}(i, j), \quad j = 1, 2, \ldots, N, \tag{9}$$

(b) compute modulo 2 of $\beta_{\text{SCR}}(j)$, denoted by $M_{\beta_{\text{SCR}}(j)}$,

(c) column j is down, or up, circular-shifted by $K_C(i)$ positions according to the following:

$$\begin{aligned} &\text{if } \; M_{\beta_{\text{SCR}}(j)} = 0 \longrightarrow \text{up circular shift} \\ &\quad \text{else} \longrightarrow \text{down circular shift.} \end{aligned} \tag{10}$$

(6) For each row i of scrambled image I_{SCR},

(a) compute the sum of all elements in row i, this sum is denoted by $\alpha_{\text{SCR}}(i)$:

$$\alpha_{\text{SCR}}(i) = \sum_{j=1}^{N} \mathrm{I}_{\text{SCR}}(i, j), \quad i = 1, 2, \ldots, M, \tag{11}$$

(b) compute modulo 2 of $\alpha_{\text{SCR}}(j)$, denoted by $M_{\alpha_{\text{SCR}}(j)}$,

(c) row i is then left, or right, circular-shifted by $K_R(i)$ according to the following:

$$\begin{aligned} &\text{if } \; M_{\alpha_{\text{SCR}}(j)} = 0 \longrightarrow \text{right circular shift} \\ &\quad \text{else} \longrightarrow \text{left circular shift.} \end{aligned} \tag{12}$$

(7) If $\text{ITER} = \text{ITER}_{\max}$, then image I_{ENC} is decrypted and the decryption process is done; otherwise, the algorithm branches back to step 2.

5.5 Flask

Flask is a Python web framework that allows developers to easily build web applications. It is a lightweight and flexible framework that provides a simple and intuitive way to create web applications quickly and easily.With Flask, developers can handle HTTP requests and responses, render templates, and work with databases, among other things. Flask is designed to be modular, so developers can add the functionality they need by installing and using extensions.One of the benefits of Flask is that it has a small learning curve, making it easy for beginners to get started building web applications. Flask also provides a lot of flexibility, allowing developers to build web applications of all sizes, from small personal projects to large enterprise applications. Overall, Flask is a popular choice among Python developers due to its simplicity, flexibility, and ability to build web applications quickly and easily.

5.5.1 Installation

1. Install Python

Flask is a Python framework, so you'll need to have Python installed on your computer first. You can download the latest version of Python from the official website: https://www.python.org/downloads/windows/

2. Open the Command Prompt

Open the Command Prompt by pressing the Windows key + R, typing "cmd" in the Run box, and pressing Enter.

3. Install Flask

Type the following command in the Command Prompt to install Flask using pip, which is a package manager for Python:

pip install flask

This will download and install Flask along with any dependencies it requires.

4. Verify the installation

Once the installation is complete, you can verify that Flask is installed by typing the following command in the Command Prompt:

python -c "import flask; print(flask.__version__)"

If everything is installed correctly, this command will output the version number of Flask.

CHAPTER 6

PSEUDOCODE

In the fields of programming and algorithms, the phrase "pseudo-code" is commonly used. It is a paradigm for programming that enables a programmer to depict the execution of an algorithm. It's a representation of a created algorithm, to put it simply. Pseudo-codes are widely used to represent algorithms because they are easily understood by programmers of all levels of programming experience. As the name suggests, pseudo-code is made up code or a representation of code that anyone with a fundamental understanding of programming can understand.

The purpose of using pseudocode is to increase the effectiveness of the central idea of an algorithm. Prior to starting the actual coding, it is used to plan an algorithm by outlining the structure of the program. In the traditional sense, pseudocode is not a programming language. Therefore, it cannot be converted into an executable program. It uses brief phrases or basic English language syntaxes to write program code before being converted into a specific programming language. By doing this, top-level flow errors may be found and the programming data flows that will be incorporated into the final program can be understood. Because conceptual issues have previously been resolved, this saves time during actual programming.

6.1 Pseudo Code of the Program

1. Encryption Process:

- Select the original image, iris image, and fingerprint image.
- Encrypt the three images using a secure encryption algorithm.
- Confirm user identity through a Telegram OTP.
- Encrypted images will be generated and displayed on the UI for reference’s sake.

2. Decryption Process:

- Select the encrypted image, iris image, and fingerprint image.
- Decrypt the encrypted image using the appropriate decryption algorithm and the iris and fingerprint images as decryption keys.
- Confirm user identity through a Telegram OTP.
- If user identity is confirmed, display the decrypted original image.

CHAPTER 7

RESULTS

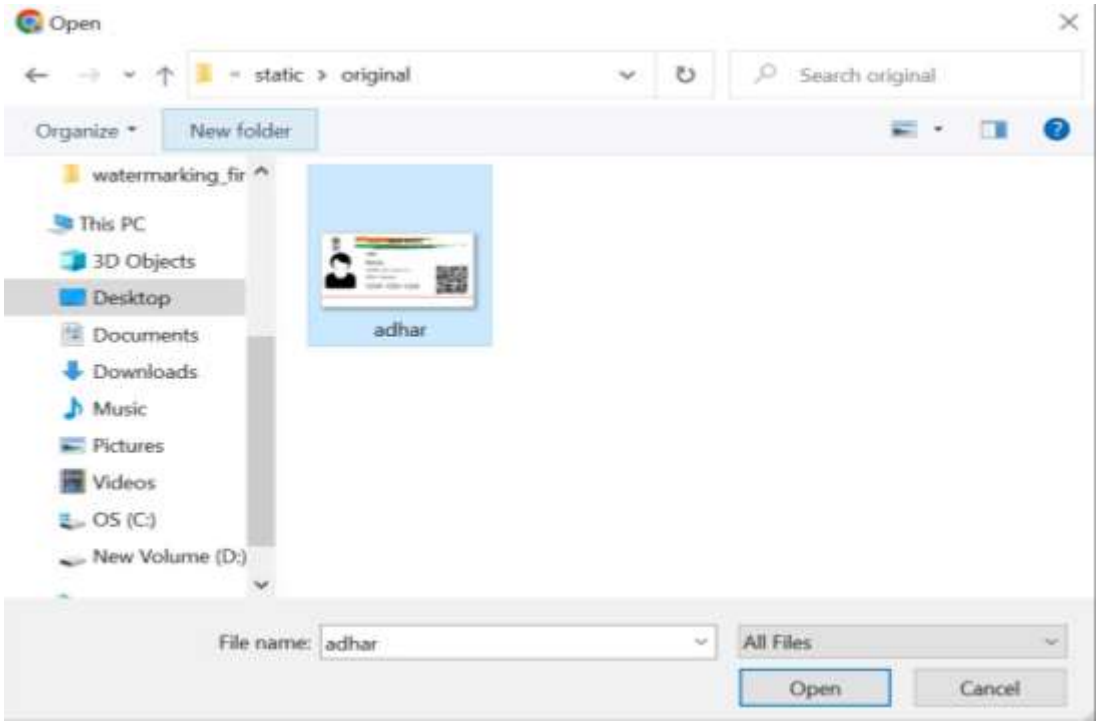


Figure 7.1: Image selection for Encryption

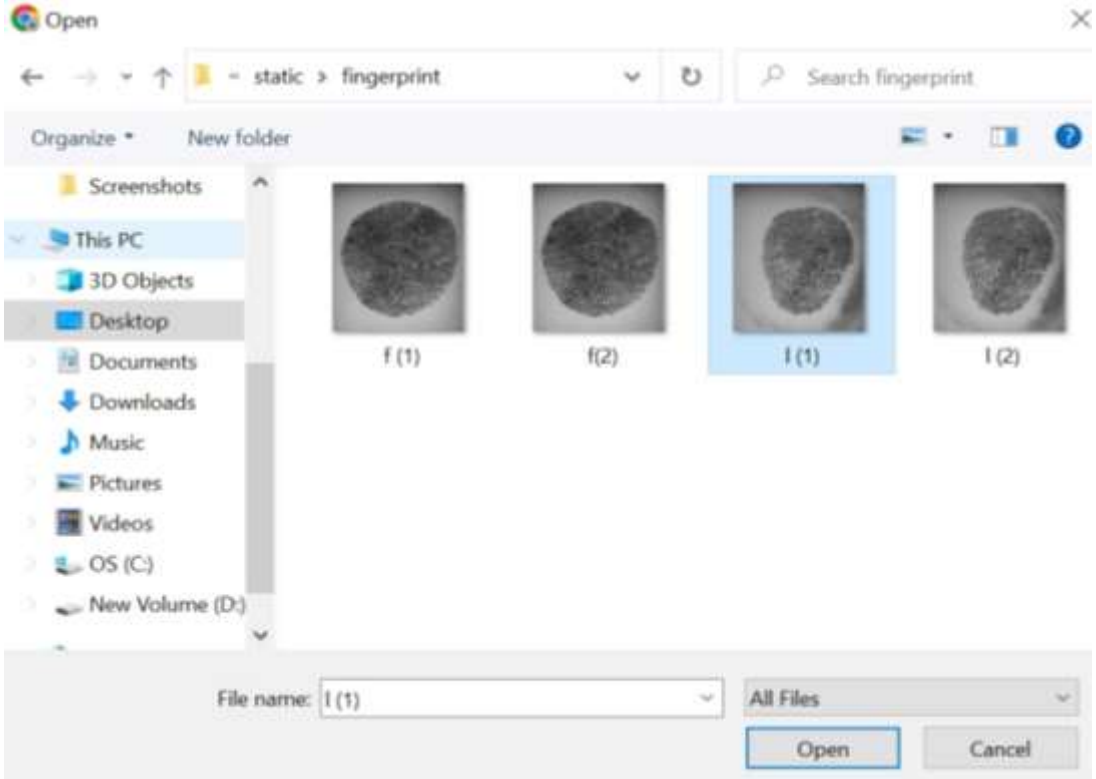


Figure 7.2: Image selection for Fingerprint

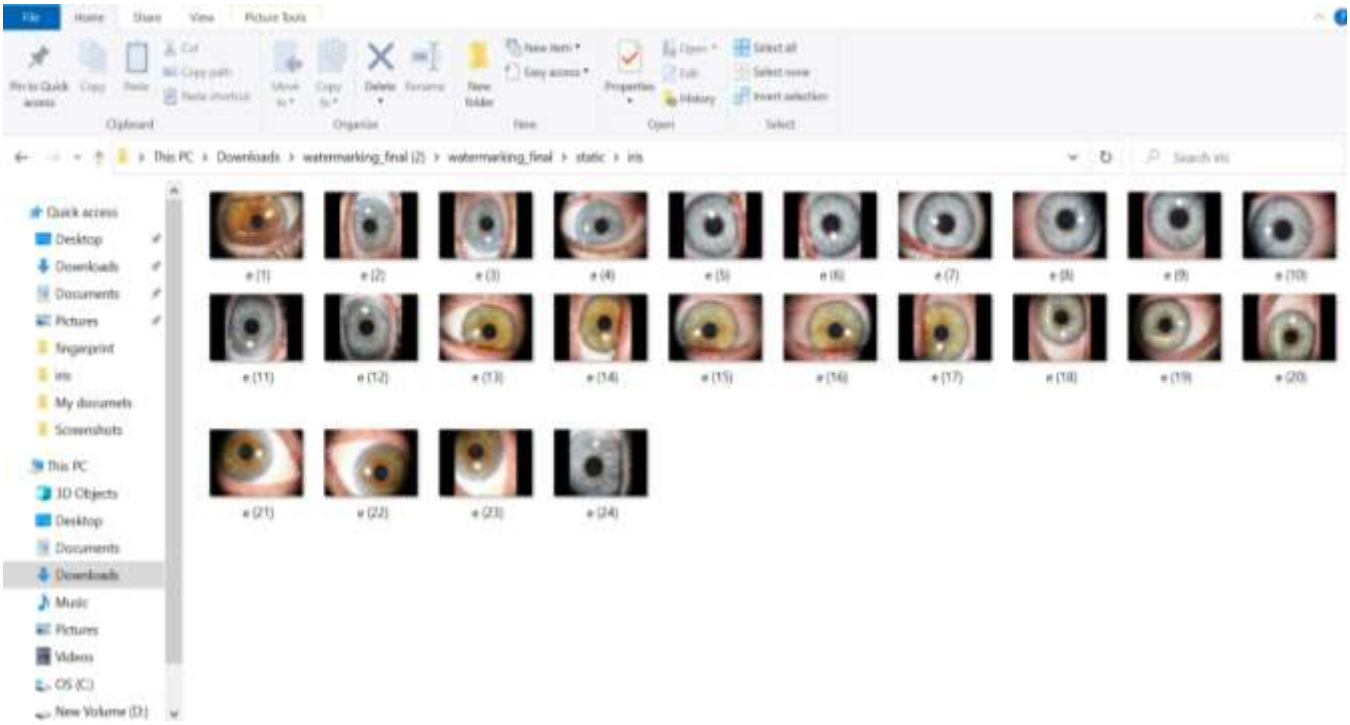


Figure 7.3: Image selection for Iris

Figure 7.4: Requirements for Encryption

Figure 7.5: Encryption Process

Figure 7.6: OTP Verification

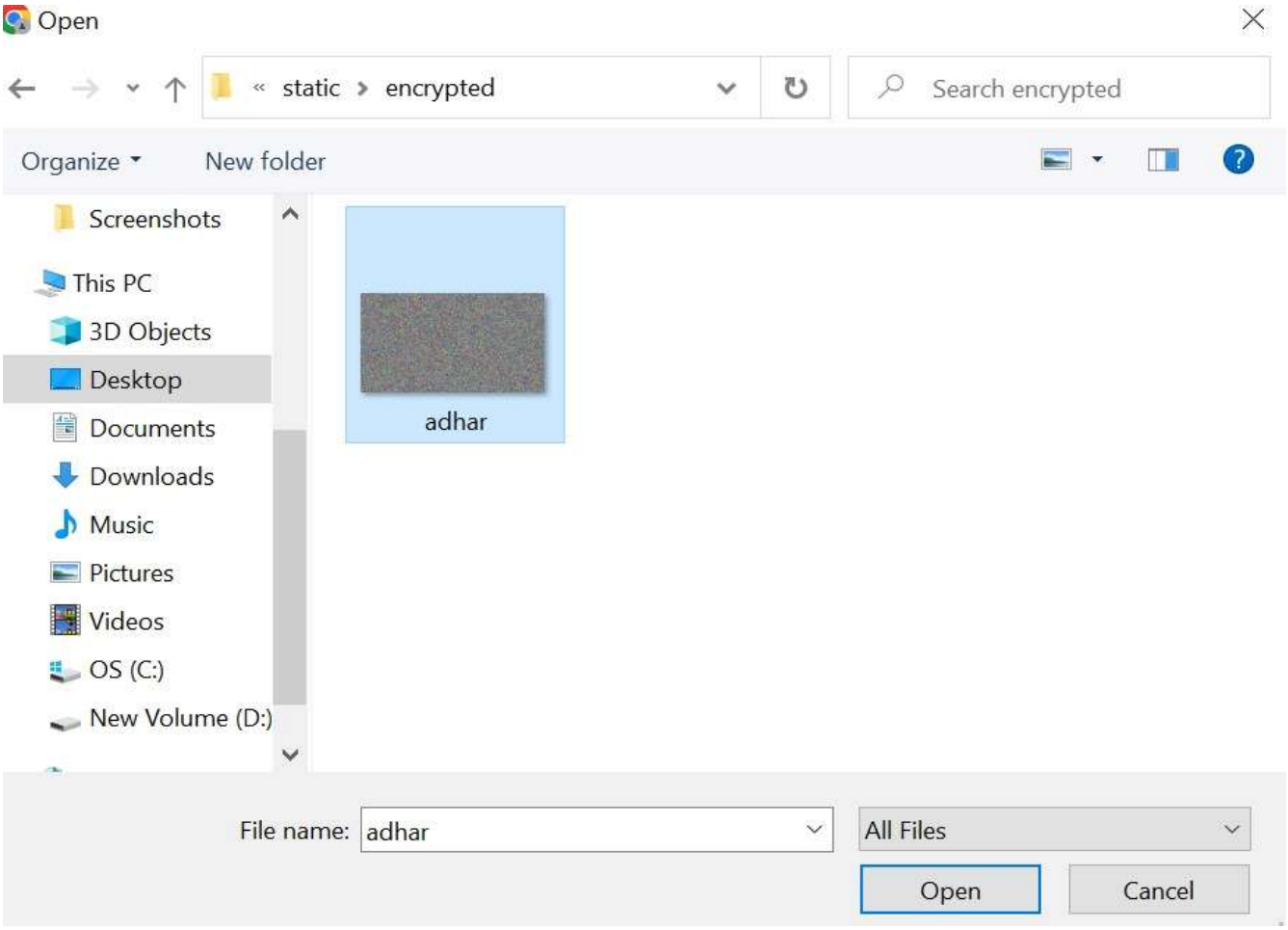


Figure 7.7: Image Selection for Decryption

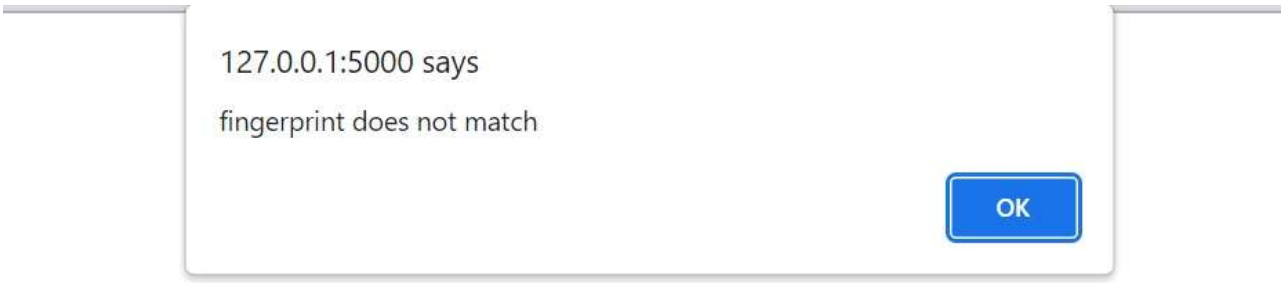


Figure 7.8: Fingerprint Mismatch

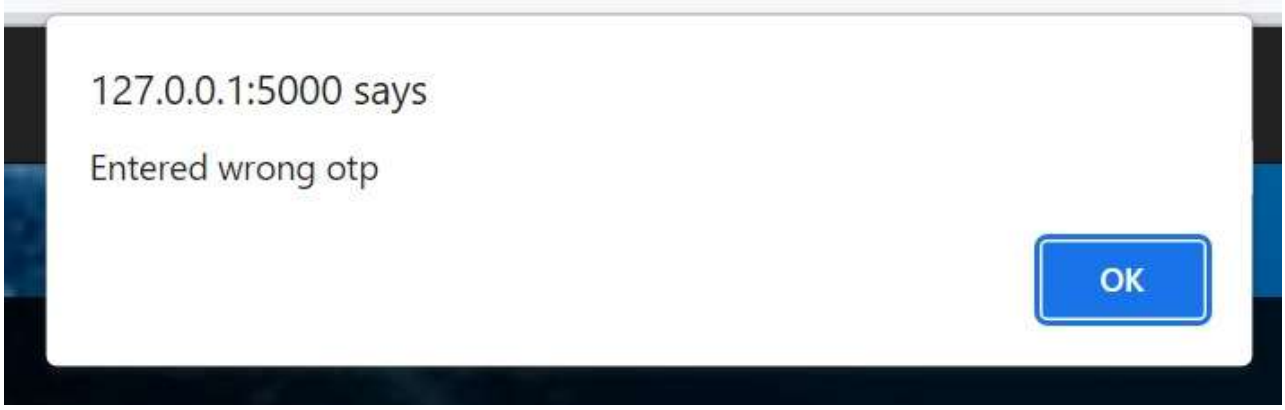


Figure 7.9: OTP Mismatch

Figure 7.10: Decryption Process

CHAPTER 8

CONCLUSION AND FUTURE ENHANCEMENTS

8.1 Conclusion

In conclusion, the use of biometric authentication systems, particularly those that combine iris and fingerprint recognition, offers a promising solution for secure and convenient authentication. The iris and fingerprint biometric system provides high accuracy, fast authentication times, reliability, usability, and security. Additionally, the system has several functional requirements, such as enrolment, integration, flexibility, scalability, security, user interface, monitoring, and maintenance.

However, the potential for biometric data theft or breaches, and the need for standardization and interoperability. Nonetheless, the benefits of iris and fingerprint biometric authentication systems make them an attractive solution for various industries and applications, from healthcare to finance to law enforcement. As technology continues to evolve, the future of biometric authentication looks promising, and iris and fingerprint recognition systems will continue to play an essential role in securing our data and identity.

Moreover, the combination of iris and fingerprint biometric authentication with One-Time Password (OTP) provides an even more secure and reliable method of authentication. The use of OTP adds an additional layer of security by requiring the user to provide a unique code along with their biometric data to gain access. This combination offers many advantages, such as reducing the risk of fraud, protecting against identity theft, and ensuring that only authorized users can access sensitive information

In conclusion, iris and fingerprint authentication provide a highly secure and accurate method for verifying user identity, making it a valuable tool for securing data. The combination of both biometric modalities can further enhance the system's performance, and future enhancements can improve the system's security and usability. Overall, iris and fingerprint authentication is a promising technology for protecting against identity theft and securing sensitive data.

8.2 Future Enhancements

Iris and fingerprint authentication can be used to enhance the security of data in various fields such as ATM machines, banking systems, and government documents. By combining both iris and fingerprint authentication, the system can ensure a high level of security and accuracy in verifying the user's identity.
Future enhancements, such as continuous authentication and cloud-based authentication, can also be integrated to further improve the system's security and reliability.

For example, in ATM machines, iris and fingerprint authentication can replace traditional PIN-based systems, reducing the risk of fraud and identity theft. The system can also be enhanced with continuous authentication, which can detect any unusual behavior and alert the system to potential fraud. Cloud-based authentication can allow for centralized management of biometric data, making it easier to implement and maintain across multiple ATM machines and locations.

In banking systems, iris and fingerprint authentication can be used to secure online transactions and account access. The system can also be enhanced with blockchain integration, which can provide a tamper-proof and decentralized record of user authentication. Machine learning algorithms can also be used to analyze user behavior and detect any anomalies or suspicious activity.

In government documents, iris and fingerprint authentication can be used to verify the identity of individuals accessing sensitive information or documents. The system can be enhanced with multimodal biometric authentication, combining multiple biometric modalities such as face recognition and voice recognition, to provide an even higher level of security. Interoperability and standardization can also be integrated to facilitate seamless integration with different government systems and agencies.

Additionally, continuous authentication can be used to monitor the user's biometric data throughout the session, while integrating blockchain technology can provide a tamper-proof and decentralized record of user authentication. Machine learning algorithms can also be used to analyze and learn from the user's biometric data, improving the accuracy and speed of authentication.

Cloud-based authentication can allow for centralized storage and management of biometric data, making it easier to implement and maintain across multiple devices and platforms. Interoperability and standardization across different biometric systems can also enhance the system's scalability and facilitate seamless integration. Finally, improving the user experience, such as better accessibility and simpler authentication processes, can encourage greater adoption of the technology.

Overall, the combination of iris and fingerprint authentication can provide a high level of security for data in various fields, and future enhancements can further improve the system's security, reliability, and usability.

CHAPTER 9

REFERENCES

1) https://ieeexplore.ieee.org/
2) https://www.nec.com/en/global/solutions/biometrics/iris/index.html
3) https://www.sciencedirect.com/topics/computer-science/biometric-authentication
4) https://www.researchgate.net/publication/2893819_Combining_Face_and_Iris_Biometrics_for_Identity_Verification
5) https://www.irjet.net/archives/V8/i7/IRJET-V8I7774.pdfedito

DrillBit

The Report is Generated by DrillBit Plagiarism Detection Software

Submission Information

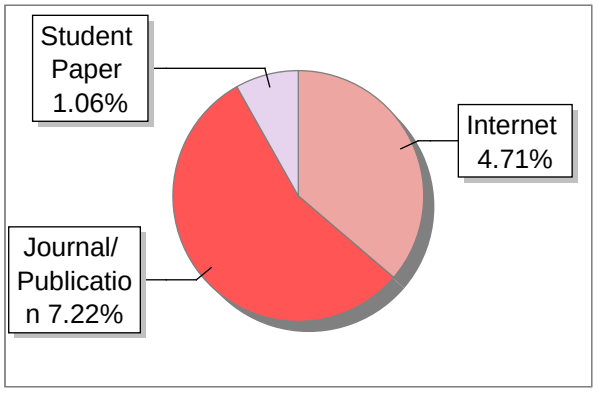
Author Name	Kalpitha S
Title	BIOMETRIC AUTHENTICATION
Paper/Submission ID	746115
Submission Date	2023-05-19 14:35:40
Total Pages	43
Document type	Project Work

Result Information

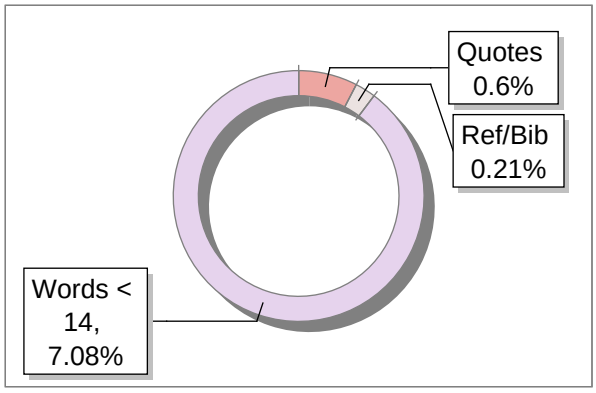
Similarity **13 %**

1 10 20 30 40 50 60 70 80 90

Sources Type



Report Content



Exclude Information

Quotes	Not Excluded
References/Bibliography	Excluded
Sources: Less than 14 Words Similarity	Excluded
Excluded Source	**0 %**
Excluded Phrases	Not Excluded

A Unique QR Code use to View/Download/Share Pdf File

DrillBit

DrillBit Similarity Report

13	33	B
SIMILARITY %	MATCHED SOURCES	GRADE

A-Satisfactory (0-10%)
B-Upgrade (11-40%)
C-Poor (41-60%)
D-Unacceptable (61-100%)

LOCATION	MATCHED DOMAIN	%	SOURCE TYPE
1	bmsce.ac.in	1	Publication
2	dochero.tips	1	Internet Data
3	peacedentistry.com	1	Internet Data
4	www.epa.gov	1	Publication
5	AUTOMATED AEROPONIC FARMING CONTROLLED AND MONITORED BY MANUEL FERNANDO MATEUS GASOLIN Yr-2021 SUBMITTED TO JNTUH COLLEGE OF ENG	1	Student Paper
6	vtechworks.lib.vt.edu	1	Publication
7	www.mdpi.com	1	Internet Data
8	dspace.nwu.ac.za	<1	Publication
9	bmcmedimaging.biomedcentral.com	<1	Internet Data
10	repository.sustech.edu	<1	Publication
11	IEEE 2018 IEEE International Symposium on Signal Processing and Inf, by Ahmed, Ramsha Hass- 2018	<1	Publication
12	Thesis Submitted to Shodhganga Repository	<1	Publication

13	Choosing the proper autoencoder for feature fusion based on data complexity and by Pulgar-2019	<1	Publication
14	www.rrce.org	<1	Publication
15	epdf.tips	<1	Internet Data
16	Article Published in MODERN PROCESS TRENDS by 'Sanderfer' - www.crosstalkonline.org	<1	Publication
17	The fifth biennial international conference on augmentative and alternative comm by DeRuyter-1988	<1	Publication
18	das.nebraska.gov	<1	Internet Data
19	docplayer.net	<1	Internet Data
20	biomedres.info	<1	Internet Data
21	IMAGE CAPTIONING USING DEEP LEARNING TECHNIQUES BY 19031D6406 Yr-2021 SUBMITTED TO JNTU	<1	Student Paper
22	Automatic Detection of Tuberculosis in Chest Radiography Usi, ISSN 2319-7242, - www.ijecs.in	<1	Publication
23	citeseerx.ist.psu.edu	<1	Internet Data
24	repository-tnmgrmu.ac.in	<1	Publication
25	www.cs.ox.ac.uk	<1	Publication
26	pingpdf.com	<1	Internet Data
27	www.ncbi.nlm.nih.gov	<1	Internet Data
28	Patient-Derived Xenograft Models for Endometrial Cancer Research by Moiola-2018	<1	Publication
29	www.smec.ac.in	<1	Publication

30	arxiv.org	<1	Publication
31	FINE GRAINED TWO FACTOR PROTECTION MECHANISM FOR DATA SHARING IN CLOUD STORAGE BY 19S41F0001 YR-2021 SUBMITTED TO JNTU	<1	Student Paper
33	www.ijert.org	<1	Internet Data
59	www.scribd.com	<1	Internet Data