

**BIOMETRIC SMART LOCK USING CONVOLUTIONAL NEURAL
NETWORK AND K-NEAREST NEIGHBOR**



UNIVERSITI TEKNIKAL MALAYSIA MELAKA

BORANG PENGESAHAN STATUS LAPORAN

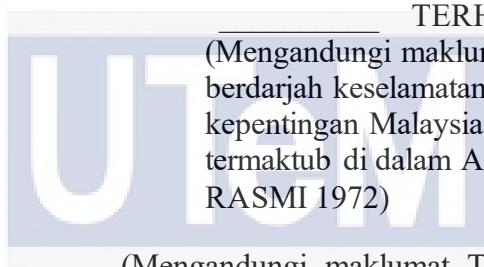
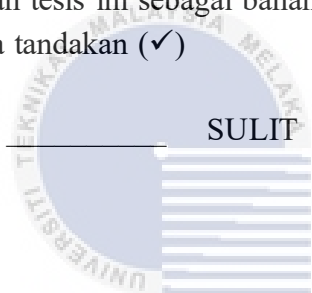
JUDUL: BIOMETRIC SMART LOCK USING CONVOLUTIONAL NEURAL NETWORK AND K -NEAREST NEIGHBOUR

SESI PENGAJIAN: 2022 / 2023

Saya: AMIRUL IAN RASHIDEE BIN MOHD JASNI

mengaku membenarkan tesis Projek Sarjana Muda ini disimpan di Perpustakaan Universiti Teknikal Malaysia Melaka dengan syarat -syarat kegunaan seperti berikut:

1. Tesis dan projek adalah hakmilik Universiti Teknikal Malaysia Melaka.
2. Perpustakaan Fakulti Teknologi Maklumat dan Komunikasi dibenarkan membuat salinan untuk tujuan pengajian sahaja.
3. Perpustakaan Fakulti Teknologi Maklumat dan Komunikasi dibenarkan membuat salinan tesis ini sebagai bahan pertukaran antara institusi pengajian tinggi.
4. * Sila tandakan (✓)



TERHAD
(Mengandungi maklumat yang berdarjah keselamatan atau kepentingan Malaysia seperti yang termaktub di dalam AKTA RAHSIA RASMI 1972)

(Mengandungi maklumat TERHAD yang telah ditentukan oleh organisasi / badan di mana penyelidikan dijalankan)

TIDAK TERHAD MALAYSIA MELAKA

(TANDATANGAN PELAJAR)

(TANDATANGAN PENYELIA)

Alamat tetap: #A Kampung Tobor,
Rampayan, Menggatal, Kota Kinabalu

Prof Madya Ts Dr Asmala bin Ahmad

Nama Penyelia

Sabah, 88450

Tarikh: 29/6/2023

Tarikh: 29/6/2023

CATATAN: * Jika tesis ini SULIT atau TERHAD, sila lampirkan surat daripada pihak berkuasa.

BIOMETRIC SMART LOCK USING CONVOLUTIONAL NEURAL NETWORK AND
K-NEAREST NEIGHBOR

AMIRUL IAN RASHIDEE BIN MOHD JASNI



This report is submitted in partial fulfillment of the requirements for the
Bachelor of Computer Science (Artificial Intelligence) with Honours.

FACULTY OF INFORMATION AND COMMUNICATION TECHNOLOGY
UNIVERSITI TEKNIKAL MALAYSIA MELAKA

2023

DECLARATION


I hereby declare that this project report entitled
**BIOMETRIC SMART LOCK USING CONVOLUTIONAL
NEURAL NETWORK AND K-NEAREST NEIGHBOUR**

is written by me and is my own effort and that no part has been plagiarized
without citations.

STUDENT :  Date : 4 / 4 / 2023
AMIRUL IAN RASHIDEE BIN MOHD JASNI

اونيورسيتي تيكنيكل مليسيا ملاك
UNIVERSITI TEKNIKAL MALAYSIA MELAKA

I hereby declare that I have read this project report and found
this project report is sufficient in term of the scope and quality for the award of
Bachelor of Computer Science (Artificial Intelligence) with Honours.

SUPERVISOR :  Date : 03/07/2023
PROFESOR MADYA GS. DR. ASMALA BIN AHMAD

DEDICATION

This project is dedicated to all the individuals who have experienced the inconvenience and potential safety risks associated with traditional locks and security systems. To those who have struggled with lost keys, forgotten passwords, or the fear of break-ins, this project represents a step forward in the pursuit of smarter, more intuitive security solutions.

In particular, we would like to dedicate this project to the countless homeowners, business owners, and property managers who have recognized the need for more advanced security measures but have struggled to find a solution that is both effective and user-friendly. It is our hope that this project will provide a viable alternative to traditional lock-and-key systems, making it easier and more convenient for everyone to secure their homes and businesses.

We also want to express our gratitude to our families, who have been a constant source of support and encouragement throughout this project. Their unwavering belief in our abilities and their willingness to lend a helping hand have been invaluable to us, and we would not have been able to accomplish this without them.

Finally, we would like to dedicate this project to the countless researchers, engineers, and developers who have dedicated their lives to advancing the field of biometrics and unlocking the potential of facial and fingerprint recognition technology. We stand on the shoulders of giants, and we are grateful for their contributions to this important and exciting field.

May this project serve as a testament to the power of innovation, dedication, and collaboration in creating a better and safer world for all.

ACKNOWLEDGEMENTS

I would like to take this opportunity to express our heartfelt gratitude to the following individuals and organizations for their invaluable contributions to this project: My project advisor, PROFESOR MADYA GS. DR. ASMALA BIN AHMAD, for providing us with guidance, feedback, and support throughout the entire project. Your expertise and insights in the field of biometric security systems have been instrumental in helping us navigate the complex and ever-changing landscape of this cutting-edge technology. Your dedication and commitment to my success have been truly inspiring, and I am grateful for the opportunity to work under your mentorship. Your enthusiasm and dedication have been instrumental in keeping us motivated and focused on the task at hand. The exchange of ideas, insights, and perspectives has enriched our understanding of the subject matter and enabled us to see the project from different angles. I appreciate your contributions and am proud to have collaborated with such talented and dedicated individuals. Finally, we would like to acknowledge our families and loved ones, especially our beloved parents, for their unwavering support and understanding throughout this project. Your encouragement, patience, and belief in our abilities have been the driving force behind my success. You have been my pillars of strength, providing me with the love, motivation, and emotional support that I needed to overcome the challenges and obstacles that we faced along the way. I am grateful for your sacrifices and proud to have you as our families. Without the support and contributions of these individuals and organizations, this project would not have been possible. I am honored to have had the opportunity to work on this project and grateful for what we have accomplished together.

ABSTRACT

Biometric Smart Lock using Convolutional Neural Network and K-Nearest Neighbors is a sophisticated security system that provides a secure and efficient alternative to traditional lock systems. The project uses the OpenCV library in Python, which provides robust image and video processing capabilities. The system consists of a camera and a fingerprint scanner, which capture the biometric information of the user. The camera captures the face of the user in real-time, which is processed using the Convolutional Neural Network classifier algorithm to detect and identify facial features. Once the face is recognized, the fingerprint scanner is activated to capture the user's fingerprint. The fingerprint data is then compared with a database of known fingerprints using the cv2.FlannBaseMatcher K-NN algorithm to find the most similar fingerprint. If the fingerprint matches with the database, the lock is unlocked, and the user gains access. The use of biometric information ensures that only authorized users are granted access, eliminating the need for traditional keys and passwords. The system's facial and fingerprint recognition capabilities provide an additional layer of security. The Convolutional Neural Network classifier algorithm is particularly well-suited for facial recognition, while the K-Nearest Neighbors algorithm is ideal for fingerprint matching. The project's focus on security and efficiency makes it an ideal solution for a wide range of applications, including home security, office security, and beyond. Overall, the Biometric Smart Lock using Convolutional Neural Network and K-Nearest Neighbors project provides an innovative and secure approach to lock systems that leverages the power of facial and fingerprint recognition technologies. The project's use of state-of-the-art algorithms and image processing techniques ensures fast and accurate recognition of the user's face and fingerprint.

ABSTRAK

Kunci Pintar Biometrik menggunakan Convolutional Neural Network dan KNearest Neighbors adalah sistem keselamatan yang canggih yang menyediakan alternatif yang selamat dan efisien untuk sistem kunci tradisional. Projek ini menggunakan pustaka OpenCV dalam bahasa Python, yang menyediakan kebolehan pemprosesan imej dan video yang kukuh. Sistem ini terdiri daripada kamera dan pengimbas cap jari, yang merekod maklumat biometrik pengguna. Kamera mengambil gambar wajah pengguna secara langsung, yang diproses menggunakan algoritma pengelas Convolutional Neural Network untuk mengesan dan mengenal pasti ciri-ciri wajah. Setelah wajah dikenali, pengimbas cap jari diaktifkan untuk menangkap cap jari pengguna. Data cap jari kemudian dibandingkan dengan pangkalan data cap jari yang diketahui menggunakan algoritma `cv2.FlannBaseMatcher` K-NN untuk mencari cap jari yang paling serupa. Jika cap jari sepadan dengan pangkalan data, kunci akan terbuka, dan pengguna akan memperoleh akses. Penggunaan maklumat biometrik memastikan hanya pengguna yang dibenarkan diberi akses, menghapuskan keperluan untuk kunci dan kata laluan tradisional. Kemampuan pengenalan wajah dan cap jari sistem memberikan lapisan keselamatan tambahan. Algoritma pengelas Convolutional Neural Network khususnya sesuai untuk pengenalan wajah, manakala algoritma KNearest Neighbors sesuai untuk pemadanan cap jari. Fokus projek pada keselamatan dan kecekapan menjadikannya penyelesaian yang sesuai untuk pelbagai aplikasi, termasuk keselamatan rumah, keselamatan pejabat, dan lain-lain. Secara keseluruhan, projek Kunci Pintar Biometrik menggunakan Convolutional Neural Network dan KNearest Neighbors menyediakan pendekatan yang inovatif dan selamat untuk sistem kunci yang memanfaatkan teknologi pengenalan wajah dan cap jari. Penggunaan algoritma canggih dan teknik pemprosesan imej memastikan pengenalan wajah dan cap jari pengguna yang cepat dan tepat.

TABLE OF CONTENTS

	PAGE
DECLARATION	III
DEDICATION	IV
ACKNOWLEDGEMENTS	V
ABSTRACT	VI
ABSTRAK	VIII
TABLE OF CONTENTS	VIII
LIST OF TABLES	XIII
LIST OF FIGURES	XIII
LIST OF ABBREVIATIONS	XV
LIST OF ATTACHMENTS	XVI
CHAPTER 1: INTRODUCTION.....	1
1.1 Introduction	1
1.2 <u>Problem Statement</u>	<u>2</u>
1.3 Research Question	2
1.4 Objectives	3
1.5 Scope	4
1.5.1 Module to be developed	4
1.5.2 Target User	5
1.6 Project Significance.....	5
1.7 Expected Output	6

1.8	Conclusion	6
CHAPTER 2: LITERATURE REVIEW AND PROJECT METHODOLOGY ..		7
2.1	Introduction	6
2.2	Facts and Findings.....	6
2.2.1	Facial Recognition	6
2.2.1.1	Existing System of Convolutional Neural Network Facial Recognition	11
2.2.2	Fingerprint Recognition	13
2.2.2.1	Existing System of K-Nearest Neighbor Fingerprint Recognition	11
2.3	Project Methodology	20
2.3.1	Project Understanding	20
2.3.2	Data Understanding	21
2.3.3	Data Preparation	21
2.3.4	Modelling.....	22
2.3.5	Evaluation	23
2.3.6	Deployment.....	23
2.4	Project Requirement	24
2.4.1	Software Requirement	24
2.4.2	Hardware Requirement.....	23
2.5	Project Schedule and Milestones	27
2.6	Conclusion	28
CHAPTER 3: ANALYSIS		30

3.1	Introduction	29
3.2	Problem Analysis	29
3.3	Requirement Analysis.....	33
3.4	Data Requirement Analysis	33
3.4.1	Functional Requirement	34
3.4.2	Non-Functional Requirement	36
3.4.2.1	Performance Analysis	36
3.4	Conclusion	29
CHAPTER 4: DESIGN.....		40
4.1	Introduction	40
4.2	High Level Design	40
4.2.1	System Architecture	41
4.2.1.1	Main User Interface Design	42
4.2.1.2	Setting User Interface Design	43
4.2.1.3	Input Design	44
4.2.1.4	Technical Design.....	45
4.2.1.5	Output Display Design	42
4.3	Detailed Design	52
4.3.1	Face Recognition Module	52
4.3.1.1	Load Data and Import Library	52
4.3.1.2	Extract Features of Input	52

4.3.1.3 Save Model In Pickle File	52
4.3.1.4 Create Facial Recognition Function	53
4.3.2 Fingerprint Recognition Module.....	53
4.3.2.1 Load Data and Import Library	53
4.3.2.2 Extract Features of Input	53
4.3.2.3 Similarity Index.....	54
4.3.2.4 Create Fingerprint Recognition Function	54
4.4 Conclusion	54
REFERENCES	55



LIST OF TABLES	PAGE
Table 2.1 : Software Requirements for Biometric Smart Lock Using CNN and KNN.....	25
Table 2.2 : Project Gantt Chart Schedule.....	28
Table 2.3 : Project Activity Description.....	28
Table 3.1: Fingerprint Data.....	34
Table 3.2: Facial Data.....	34
Table 3.3: User Information.....	35
Table 3.4 : Non-Functional Requirements.....	37-38
Table 5.1 Backup Management.....	62
Table 5.2 : Implementation Status.....	63-64
Table 6.1.1 : Test Organization.....	65-66
Table 6.1.2 System Tester.....	66-68
Table 6.2 : Test Environment.....	69
Table 6.3 : Test Schedule.....	69
Table 6.4 Classes of Tests.....	70-71
Table 6.5 : Test Description For Facial Recognition Module.....	71-72
Table 6.6 : Test Description For Fingerprint Recognition Module.....	73
Table 6.7 : Test Description For Authentication Module.....	74
Table 6.8 : Test Description For User Experience.....	74
Table 6.9 : Test Data.....	75
Table 6.10 Face Recognition Functionality Test Result.....	75-76
Table 6.11: Performance Evaluation of Face Recognition based on Distance Measurement.....	76-77
Table 6.12: Performance Evaluation of Face Recognition based on Face Orientation.....	78
Table : Table 6.13: Performance Evaluation of Face Recognition based on Lighting condition.....	80-81
Table 6.14 : True Positive and False Negative Test (Register User).....	82
Table 6.15: False Positive and True Negative Test (Unregister).....	82-83
Table 6.16 Fingerprint Recognition Functionality Test Result.....	84
Table 6.17: Performance Evaluation of Fingerprint Recognition based on Finger's Orientation.....	85
Table 6.18: Performance Evaluation of Fingerprint Recognition Across Finger Moisture Level.....	87
Table 6.19 : True Positive and False Negative Test (Register User).....	88
Table 6.20: False Positive and True Negative Test (Unregister).....	88-89
Table 6.21 Authentication Module Functionality Test Result.....	90
Table 6.22: Attempt to bypass authentication without proper credentials.....	90-91
Table 6.23: Attempt to Access authentication with proper credentials.....	92-93
Table 6.24: Test the system's ability to handle concurrent authentication requests.....	93
Table 6.25 : User Experience Survey Scale.....	95
Table 6.26 : User Experience Survey Question.....	95

LIST OF FIGURES	PAGES
Figure 2.1: Type of 2-Dimension Facial Recognition	7
Figure 2.2: Convolutional Neural Network Process for Facial Recognition	8
Figure 2.3: Eigenfaces Process for Facial Recognition	9
Figure 2.4: Fisherfaces Process for Facial Recognition	10
Figure 2.5: Local Binary Pattern Process for Facial Recognition	11
Figure 2.6 : Type of Fingerprint Recognition Algorithm	14
Figure 2.7 : SIFT-KNN Fingerprint Recognition Process	14
Figure 2.8 : Correlation-Based Matching Fingerprint Recognition Process	16
Figure 2.9:Neural Network-Based Matching Fingerprint Recognition Process	17
Figure 2.10 : Singular Point Detection Fingerprint Recognition Process	18
Figure 2.11 : CRISP-DM process model	21
Figure 3.1: Flowchart of Biometric Smart Lock with CNN and KNN	31
Figure 3.2: Flowchart of Fingerprint Recognition Model	32
Figure 3.3: Flowchart of Facial Recognition Model	33
Figure 3.4 Use Case of Biometric Smart Lock Using Convolutional Neural Network and K-Nearest Neighbor	37
Figure 4.1: IANIC Smart Lock System Architecture using CNN and KNN	43
Figure 4.2 : Main User Interface Design	44
Figure 4.3: Setting User Interface Design	45
Figure 4.4 Facial Recognition Input design	46
Figure 4.5 Fingerprint Recognition Input design	46
Figure 4.6 OTP Input design	47
Figure 4.7 Technical Design for CNN Face Recognition Analysis	47
Figure 4.8 Technical Design for KNN Fingerprint Recognition Analysis	48
Figure 4.9 Technical Design for Lock Control Analysis	48
Figure 4.10 Technical Design for OTP Module Analysis	49
Figure 4.11: Valid Output Display Design for Face Recognition Module	50
Figure 4.12: Invalid Output Display Design for Face Recognition Module	50
Figure 4.13: Valid Output Display Design for Face Recognition Module	50
Figure 4.14: Invalid Output Display Design for Face Recognition Module	51
Figure 4.15: Default Lock Status	51
Figure 4.16: Valid Authentication Lock Status	52

Figure 4.17: Invalid Authentication Lock Status	52
Figure 5.1: Overall Software Development Environment Setup	5752
Figure 5.2: List Of Project Requirements 1	5852
Figure 5.3 : List Of Project Requirements 2	5952
Figure 5.4 : Firebase realtime database API	6052
Figure 5.5 : Place to download the json file in Setting.....	6052
Figure 5.6 : Json File inside coding	6052
Figure 5.7 : ZK4500 Fingerprint Demo	6152
Figure 6.1 : 40 cm Face Recognition Distance	7752
Figure 6.2 : 70cm Face Recognition Distance	7752
Figure 6.3 : 100cm Face Recognition Distance	7852
Figure 6.4: 0° Face Orientation Recognition	7952
Figure 6.5: 45° Face Orientation Recognition	7952
Figure 6.6: 90° Face Orientation Recognition	8052
Figure 6.7: Morning Natural Light Testing Face Recognition.....	8152
Figure 6.8: Dim Night Lamp Test Face Recognition.....	8152
Figure 6.9: 0° Finger Orientation Recognition	8652
Figure 6.10: 45° Finger Orientation Recognition	8652
Figure 6.11: 90° Finger Orientation Recognition	8652
Figure 6.12 : Histogram of Question 1 Survey	9552
Figure 6.13 : Histogram of Question 2 Survey	9652
Figure 6.14 : Histogram of Question 3 Survey	9652
Figure 6.15 : Histogram of Question 4 Survey	9752
Figure 6.16 : Histogram of Question 5 Survey	9752

LIST OF ABBREVIATIONS

FYP	-	Final Year Project
OTP	-	One Time Password
KNN	-	K-Nearest Neighbor
CNN	-	Convolutional Neural Network
CV2	-	Computer Vision 2 Library
OpenCV	-	Open Source Computer Vision Library
LBP	-	Local Binary Pattern
LDA	-	Linear Discriminant Analysis
PCA	-	Principal Component Analysis
LFW	-	Labeled Face In Wild
IJB-A	-	IARPA Janus Benchmark A
RAM	-	Random Access Memory
SIFT	-	Scale-Invariant Feature Transform
FVC	-	Fingerprint Verification Competition
NumPy	-	Numerical Python
SDK	-	Software Development Kit
IDE	-	Integrated Development Kit
CCTV	-	Closed Circuit Television
ZK	-	Company Name
CRISP	-	Cross Industry Standard Process
DM	-	Data Mining

LIST OF ATTACHMENTS

		PAGE
Appendix A	Sample of data	57
Appendix B	Sample of Source Code	59



CHAPTER 1: INTRODUCTION

1.1 Introduction

In the modern world, security concerns are becoming increasingly prevalent, and traditional locks are no longer sufficient to provide the necessary protection against theft and other safety issues. In response to this need, various technologies have been developed, including facial recognition and password-protected locks, which have proven to be less than perfect. Despite their numerous advantages, they are still vulnerable to accuracy issues. The purpose of this report is to present a project that aims to develop a biometric smart lock using Convolutional Neural Network (CNNs) and K-nearest neighbour (kNN) to make it more secure than traditional locks. The system will require both facial and fingerprint recognition to access the lock, overcoming the problems associated with using just one recognition technology.

The project will develop software that provides facial and fingerprint recognition with high accuracy, increasing the safety of locks and ensuring the security and accuracy of user identification and authentication. The modules to be developed include the face and fingerprint recognition module, the data management module, and the authentication module. The target users of this system are homeowners, business owners, tech-savvy users, and travelers.

This objectives of the project, are to identify the requirement for developing facial and fingerprint recognition system, develop the facial and fingerprint recognition technique based on Convolutional Neural Network and K-Nearest Neighbour, and to test the system through quantitative and qualitative approaches. The end result will be a web-based software that allows the user to upload both facial and fingerprint images for training the algorithm to identify the user's biometric information. The system is expected to only let the rightful owner access the lock and eliminate any small noises that may interfere with the recognition. The development of this system is expected to benefit users by allowing them to maintain enhanced privacy and security over their belongings and places. This chapter will provide an overview of the project, its objectives, and the technologies involved in its development.

1.2 Problem Statement

- 1) Most biometric-based lock systems consider only single biometric recognition and therefore are less secured.
- 2) Most biometric-based lock systems used a single machine learning technique and therefore are less reliable.
- 3) Most biometric-based lock systems are not thoroughly tested in which their true performance are questionable.

1.3 Research Questions

- 1) What are the essential requirements and concerns for designing a successful facial and fingerprint recognition system capable of meeting the objectives of diverse applications and stakeholders, such as accuracy, speed, security, privacy, and user experience.
- 2) How can the Convolutional Neural Network (CNNs) and K-nearest neighbor (kNN) algorithms be enhanced and coupled to achieve high accuracy and efficiency in facial and fingerprint recognition while addressing issues like image quality, lighting, and occlusion.
- 3) What are the most effective and dependable techniques for evaluating the facial and fingerprint recognition system in different scenarios and applications, and how can user feedback and usability testing be incorporated into the review process to guarantee the system satisfies enduser needs.

1.4 Objectives

1. To identify the requirement for developing facial and fingerprint recognition system
2. To develop the facial and fingerprint recognition technique based on Convolutional Neural Network and K-Nearest Neighbour
3. To test the system through quantitative and qualitative approaches.



1.5 Scope

1.5.1 Module to be developed

There are 4 module to be developed.

1. Facial Recognition Module

In this module user will be responsible for capturing and processing facial data to identify and authenticate users. Module will use an A.I technique such as K-Nearest Neighbour (KNN).

2. Fingerprint Recognition Module

This module will capture and process user's fingerprint data to identify and authenticate users. Module will use an A.I. technique is feature extraction model.

3. Data Management Module

This module will store both user's facial and fingerprint data, ensuring secure storage and retrieval of user information.

4. Authentication Module

Authentication module will combine and integrate the other module to authenticate the user's biometric with data that has been stored in storage

1.5.2 Target User

The target user of this project is as follows:

- 1) Homeowners: individuals who want to secure their homes with a hightech lock system that offers added security and convenience.
- 2) Business Owners: companies and organizations that need to secure their offices.
- 3) Tech-savvy Users: Individuals who are interested in high-tech solutions and who appreciate the convenience and security of biometric recognition technology.
- 4) Travellers : people who need a secure and convenient way to access their airbnb listings or rental properties.

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

1.6 Project Significance

The creation of a biometric smart lock based on facial and fingerprint recognition technology is critical in today's environment, when traditional locks no longer provide enough protection against theft and safety hazards. This project intends to solve customers' worries about the accuracy and security of existing lock systems by providing a more dependable and efficient alternative. This system will improve the security and accuracy of user identification and authentication by utilising advanced algorithms such as Convolutional Neural Network and k-nearest neighbour. By providing a safe and secure way to access their homes and properties, the project is expected to benefit homeowners, business owners, tech-savvy users, and travellers.

1.7 Expected Output

The end result of the project will be desktop-based system that enables the user to upload both facial and fingerprint images for training the algorithm to identify the user's biometric information. Users then can have a safe and secure lock that can only be accessed by them and not the other way around. The system is expected to only let the owner of the lock access it. Any small noises such as a thin layer of dust, a drop of hair, or any salt and paper noise will be removed by the system using image enhancement processing. Users should be able to unlock the door in an instant if they are the rightful owner. Hopefully, the system will benefit users and allow them to maintain enhanced privacy and security over their belongings and places.

1.8 Conclusion

Finally, the introduction of a biometric smart lock that uses facial and fingerprint recognition technology is an important step towards improving security and privacy for homes, company owners, tech-savvy users, and travellers. The project's goal was to create software that delivers high-accuracy facial and fingerprint identification while also maintaining the security and reliability of user data to prevent unauthorised access. Face and fingerprint recognition modules, data management modules, and authentication modules were built. The ultimate product is a web-based software that allows users to upload both facial and fingerprint photos in order to teach the algorithm to recognise the user's biometric information. The mechanism is designed to allow only the rightful owner to open the lock and to remove any little noises that might interfere with the recognition. Overall, this project met its goals and provided an innovative solution to the current security risks associated with traditional lock systems.

CHAPTER 2: LITERATURE REVIEW AND PROJECT METHODOLOGY

2.1 Introduction

Because of their convenience and increased security over traditional locks, biometric smart locks have become an increasingly popular security solution. Biometric authentication, such as fingerprint or face recognition, can offer a more secure and dependable method of access management. However, factors like as lighting variations, facial expressions, positions, occlusions, and noise can all have an impact on the operation of biometric smart locks. Various methods and techniques, including the usage of Convolutional Neural Network (CNN) and K-Nearest Neighbour (KNN) algorithms, have been proposed to increase the recognition accuracy and robustness of biometric smart locks.

2.2 Facts and Findings

In this section, we'll talk about a range of relevant subjects that have to do with the project itself and can aid in our comprehension of it and its successful execution.

2.2.1 Facial Recognition

A type of biometric technology called facial recognition employs machine learning algorithms to recognise human faces. Convolutional Neural Networks (CNNs), Eigenfaces, Local Binary Patterns (LBP), and Fisherfaces are a few of the methods utilised in facial identification.

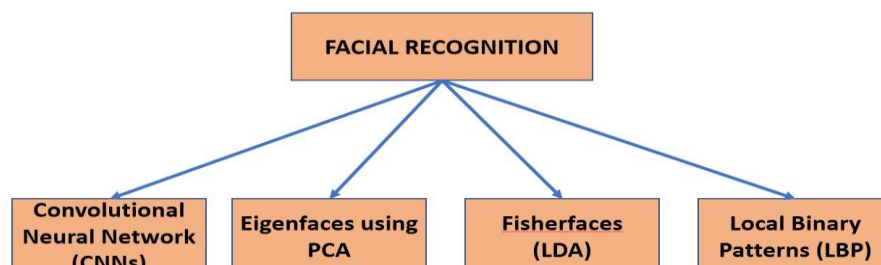


Figure 2.1 : Type of 2-Dimension Facial Recognition (Kortli et al., 2020)