



**College of Computer and Information Sciences  
Computer Science Department**



# **“Air Signature Using Smartwatch Motion Sensors”**

*CSC 496– Final Report*

**Prepared by:**

Maymona Turki Alotaibi	443200582
Atheer Abdullah AlAsiri	443200626
Rimas Saad AlBahli	443200631
Lama Faham AlOtobie	443201044

**Supervised by:**

**Dr. Rasha Mohmmad AlEidan**

Research project for the degree of Bachelor in Computer Science  
First Semester 1446

# I. Acknowledgements

In the name of Allah, whose blessings and guidance have enabled us to complete this project successfully.

We begin by expressing our sincere appreciation to the **Computer Science Department, the College of Computer and Information Sciences, and King Saud University** for providing us with the knowledge, tools, and academic environment that made this research possible.

We would like to express our sincere thanks to our supervisor, **Dr. Rasha Mohammad AlEidan**, for her continuous support, thoughtful guidance, and encouragement throughout the course of this research. Her insight and mentorship were key to shaping both the direction and success of our work.

We also extend our gratitude to **Dr. Najwa Altwaijry** and **Dr. Sarah Alotaibi** for their valuable feedback and constructive suggestions during our progress reviews, which significantly enriched the quality of our project.

Special thanks are due to all the **participants** who contributed their time and effort during the data collection process, your cooperation was essential in making this work possible.

Finally, we extend our heartfelt appreciation to our **families and friends** for their unwavering support, patience, and motivation. Your encouragement has been a vital part of our journey.

- **The Air Signature Team**

## II. English Abstract

In today's increasingly digital world, the demand for secure, portable, and user-friendly authentication systems is rising rapidly. Traditional password-based methods are proving inadequate against growing security threats, prompting a shift towards biometric solutions. This research proposes an innovative online authentication system based on air signature recognition using smartwatch motion sensors, particularly accelerometers and rotation. The system captures the unique motion patterns of handwritten signatures performed in the air, without the need for physical surfaces or specialized hardware.

A custom dataset of Arabic-language signatures was collected from 24 participants using an Apple Watch SE, including both genuine and forged samples. After applying essential preprocessing techniques such as rotation correction, differentiation, and normalization, the data was used to train multiple deep learning models, including BLSTM, CNN, ResNet, and a hybrid CNN-BLSTM. Among these, the Convolutional Neural Network (CNN) achieved the highest performance, reaching an impressive accuracy of 99.86%, demonstrating its strong capability in extracting spatial features and distinguishing between authentic and forged signatures.

Compared to traditional camera-based systems, the proposed smartwatch-based solution, which relies on motion sensors, a domain rarely explored in previous research, offers superior portability, enhanced privacy, and real-time processing.

Moreover, This research is one of the first to focus on air signature recognition for Arabic-language signatures using motion sensors. Our study presents a novel contribution to the field of biometric authentication. The results highlight the potential of wearable technology to transform identity verification across sectors such as banking, healthcare, and digital services.

### III. Arabic Abstract

مع التوسع السريع في الاعتماد على الأنظمة الرقمية في مختلف جوانب الحياة، أصبحت الحاجة إلى حلول تحقق أمانة، سهولة الاستخدام، وقابلية للحمل أمرًا بالغ الأهمية. لم تعد الطرق التقليدية القائمة على كلمات المرور كافية لمواجهة التهديدات الأمنية المتزايدة، مما أدى إلى الاعتماد على حلول بيومترية أكثر تطورًا. يتناول هذا البحث تطوير نظام تحقق مبتكر يعتمد على التوقيع الهوائي باستخدام مستشعرات الحركة في الساعات الذكية، وتحديدًا بيانات التسارع والدوران، لتمييز أنماط التوقيع اليدوي أثناء أدائه في الهواء، دون الحاجة إلى سطح مادي أو أجهزة متخصصة.

تم إنشاء مجموعة بيانات مخصصة لتوقيعات باللغة العربية، بمشاركة 24 متطوعًا، تم خلالها تسجيل توقيعات أصلية ومزورة باستخدام ساعة Apple Watch SE. بعد تنفيذ عدة خطوات للمعالجة المسبقة مثل تصحيح الاتجاه، والاشتقاق، والتطبيع، تم تدريب عدد من نماذج التعلم العميق على هذه البيانات، من ضمنها نماذج BLSTM، وCNN، وResNet، والنموذج الهجين CNN-BLSTM وقد حقق نموذج الشبكة العصبية الالتفافية (CNN) أعلى دقة وصلت إلى 99.86%، ما يؤكد قدرته العالية على استخلاص السمات المكانية والتمييز بدقة بين التوقيعات الأصلية والمزورة.

بالمقارنة مع الأنظمة التقليدية المعتمدة على الكاميرات، يتميز النظام المقترح المعتمد على مستشعرات الحركة وهو مجال لم يحظَ باهتمام كافٍ في الدراسات السابقة بكونه أكثر قابلية للنقل، ويوفر خصوصية أكبر، ويدعم المعالجة الفورية. ويُعدّ هذا البحث من أوائل الدراسات التي تركز على التعرف على التوقيعات الهوائية للغة العربية باستخدام مستشعرات الحركة، مما يشكل مساهمة مبتكرة في مجال المصادقة البيومترية. وتبرز النتائج إمكانات تقنيات الأجهزة القابلة للارتداء في إحداث نقلة نوعية في أنظمة التحقق من الهوية في مجالات مثل البنوك، الرعاية الصحية، والخدمات الرقمية.

## Table of Contents

I. Acknowledgements.....	2
II. English Abstract.....	3
III. Arabic Abstract .....	4
1. Introduction.....	9
1.1 Problem Statement.....	11
1.2 Goals and Objectives .....	12
1.3 Proposed Solution .....	13
1.4 Research Scope .....	14
1.5 Research Significance.....	15
1.6 Ethical and Social Implications .....	16
1.7 Report Organization.....	17
2. Background.....	18
2.1 Biometric Authentication.....	18
2.2 Signature Verification Techniques .....	19
2.3 Offline (Static) Signature Verification.....	19
2.4 Online (Dynamic) Signature Verification.....	19
2.5 Air Signature.....	20
2.6 Smartwatch Motion Sensors .....	21
2.7 Dynamic Time Wrapping .....	21
2.8 Deep Learning Techniques .....	21
2.8.1 Conventional Neural Networks (CNNs).....	22
2.8.2 Recurrent Neural Networks (RNNs).....	22
2.8.3 Bidirectional Long Short-Term Memory (BLSTM).....	23
3. Literature Review.....	24
3.1 Related Work On Air Signature.....	25
3.1.1 Camera-Based-System.....	25
3.1.2 Smartwatch-Based-System .....	27
3.1.3 Other-System .....	29
3.2 Table of Comparison.....	30
3.3 Discussion .....	31
3.3.1 Evolution in Air Signature Recognition Systems .....	31
3.3.2 Challenges.....	32
3.3.3 Advantages and Disadvantages.....	33
3.3.4 Datasets .....	33
3.4 Our Contribution.....	33
4. Data collection .....	34

4.1 Smartwatch selection & setup.....	34
4.2 Participant Recruitment & Data Collection Protocol.....	35
4.2.1 Participant Selection .....	35
4.2.2 Signature Recording Process & Sensor Data Acquisition & Features Collected ...	35
4.2.3 Challenges in Data Collection .....	35
4.3 Visual Representation of Data Collection and Pre-processing .....	36
5. Methodology .....	38
5.1 Pre-Processing Steps .....	38
5.1.1 Rotation.....	39
5.1.2 Differentiation.....	40
5.1.3 Normalization .....	41
5.1.4 Pairing .....	42
5.2 BLSTM Model design .....	45
5.2.1 Forward LSTM, Backward LSTM .....	45
5.2.2 Dense Layer with Activation function .....	46
5.2.3 Output Layer .....	46
5.3 Training and Evaluation Plan.....	47
5.3.1 Training.....	47
5.3.2 Testing & Evaluation .....	48
6. Experimental Design.....	49
6.1 Hypotheses.....	49
6.2 Experimental Setup .....	50
6.3 Experiments .....	51
6.3.1 Experiment 1 .....	52
6.3.2 Experiment 2 .....	53
6.3.3 Experiment 3 .....	54
6.3.4 Experiment 4 .....	55
7. Result and Discussion .....	56
7.1 Performance Comparison of Models .....	56
7.2 Discussion of Augmentation and Robustness.....	57
8. Applications of The Model .....	58
9. Conclusion & Future Work.....	61
9.1 Conclusion .....	61
9.2 Future work.....	62
References.....	63
Appendix.....	65

## Table of Figures

Figure 1 General Biometric System [4].....	18
Figure 2 Air Signing Process [3].....	20
Figure 3 Apple Watch SE (44mm).....	34
Figure 4 Smartwatch interface.....	34
Figure 5 Data collection process.....	35
Figure 6 Handwritten Signature.....	36
Figure 7 Raw Genuine Accelerometer.....	36
Figure 8 Raw Genuine Rotation.....	36
Figure 9 Raw Genuine Orientation.....	36
Figure 10 Processed Genuine Accelerometer.....	37
Figure 11 Processed Genuine Rotation.....	37
Figure 12 Processed Fake Accelerometer.....	37
Figure 13 Processed Fake Rotation.....	37
Figure 14 BLSTM Model Architecture.....	43
Figure 15 CNN Model Architecture.....	43
Figure 16 Hybrid CNN-BLSTM Model Architecture.....	44
Figure 17 ResNet Model Architecture.....	44
Figure 18 Interface 1.....	58
Figure 19 Interface 2.....	59
Figure 20 Interface 3.....	59
Figure 21 Interface 4.....	59
Figure 22 Interface 5.....	60
Figure 23 Interface 6.....	60
Figure 24 Interface 7.....	60

## Table of Tables

Table 1 Table of comparison.....	30
Table 2 Data after pre-processing.....	33
Table 3 Raw data representation.....	34
Table 4 BLSTM with Augmentation.....	52
Table 6 CNN with Augmentation.....	53
Table 8 Basic Hybrid Architecture.....	54
Table 9 Optimized Hybrid Architecture.....	54
Table 10 ResNet Model.....	55
Table 11 Experiments Result.....	56



# 1. Introduction

With the rapid advancement of technology and the increasing reliance on digital systems in various aspects of life, securing identity and authentication has become a top priority. Many applications, ranging from banking services to healthcare systems, require authentication solutions that are not only efficient but also user-friendly. Traditional password-based systems are increasingly vulnerable to security breaches, highlighting the need for innovative biometric authentication methods.

**Signature verification** has been widely used as a biometric authentication method due to its familiarity and ease of use. Traditional systems rely on **offline (static) verification**, where signatures are analyzed based on scanned images. However, with advancements in technology, **online (dynamic) signature verification** has emerged, capturing real-time data such as pressure, speed, and stroke order, enhancing security against forgery. This research explores a novel online method: air signature recognition using smartwatch motion sensors, offering a portable, secure, and contactless authentication solution [1] [2].

While traditional signature verification systems rely on **offline (static) verification** or dedicated devices such as digital tablets, the emergence of wearable technology opens new possibilities for developing innovative **online (dynamic) signature verification** authentication methods [1] [3].

## **Motivation:**

In an era where cyber threats and data breaches are becoming more frequent, relying solely on passwords or PINs is no longer sufficient for securing sensitive data. Signatures, which have long been used as a form of identity verification, are familiar to users and offer a more intuitive form of authentication. However, traditional signature verification (Off-line verification) methods that rely on scanned images or specialized tablets can be limited, especially in terms of portability and real-time applications [1] [4].

**An air signature** refers to the process of capturing a user's unique motion patterns while signing or performing specific gestures in the air using devices like smartwatches or other wearables [5]. Unlike traditional signatures, which depend on surfaces, the air signature relies on spatial movement data, providing a means of authentication without the need for a physical surface [3] [6].

### **Why Air Signature Recognition?**

The motivation behind this research stems from the increasing adoption of wearable technology, which presents an untapped opportunity to develop more secure and portable authentication systems. Smartwatches, with their embedded motion sensors, are widely available and are becoming a staple of modern, everyday digital lifestyles. Leveraging the accelerometer and rotation data from these devices to capture in-air signatures offers a novel approach that is contactless, intuitive, and convenient [2].

Air signature recognition differs from traditional systems as it relies on spatial movement data rather than a physical surface. This not only enhances the user experience by eliminating the need for additional hardware but also increases security since in-air signatures are naturally more difficult to forge. The ability to perform secure authentication using nothing more than a wristwatch can transform sectors such as banking, healthcare, and digital transactions by providing a seamless yet robust authentication mechanism.

The aim of this research is to develop a real-time, portable air signature recognition system using smartwatch sensors such as accelerometers and rotation to capture motion data [2]. The data will be analyzed using advanced machine learning techniques, such as Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs) to differentiate between genuine and forged signatures [7].

## 1.1 Problem Statement

This research explores the recognition of "Air Signatures" using smartwatches as a novel approach to user authentication. With the increasing prevalence of electronic transactions, the need for secure, intuitive, and user-friendly authentication methods has become critical. Traditional password-based systems are fraught with vulnerabilities such as data breaches and user errors, which have paved the way for alternative authentication techniques like biometrics [6] [2].

An air signature refers to the unique, in-air hand gestures or movements made by a user to sign, which can be captured by the motion sensors embedded in a smartwatch. These gestures, unlike traditional signatures captured on paper or digital devices, are executed in mid-air, leveraging the smartwatch's accelerometer, rotation, and other sensors to track and recognize motion patterns [7]. Despite the potential of air signatures for secure and portable authentication, research on this method, particularly through wearable devices like smartwatches, remains limited. Existing studies predominantly focus on signature verification using devices such as tablets, cameras, or signature pads, leaving a significant gap in research on smartwatch-based systems [2]. Recognizing air signatures presents unique challenges, including the accurate capture of wrist motion data, variability in signature gestures, and addressing limitations related to data sufficiency, accuracy, and the performance of models trained on small datasets [8]. These challenges underscore the need for robust algorithms that can handle motion data while ensuring reliable and secure authentication, especially in portable and wearable devices.

This research is significant as it aims to address this gap by investigating how smartwatches can be effectively utilized to recognize air signatures, thereby offering a modern, convenient, and secure solution for authentication. The study's findings will contribute to the development of more reliable authentication systems that balance user convenience with high security standards [5]. As wearable technology continues to gain traction, the importance of this research lies in its potential to enhance everyday security protocols while keeping pace with technological advancements.

## 1.2 Goals and Objectives

The aim of this project is to develop and verify a method for recognizing and validating handwriting signatures made in the air using smartwatch.

The goal is to differentiate between genuine and fake signatures based on the data collected by the smartwatch sensors (Accelerometer, Rotation).

**Objectives:** To achieve this goal, our objectives are as follows:

- Conduct an in-depth literature review of the researches to capture the signature (Camera-based system, Smartwatch-based system, and others).
- Collect relevant data using the smartwatch's sensors such as accelerometers and rotation, which are standard in smartwatches.
- Analysis and preprocessing of collected data, focus only on the signature area using different signal processing techniques such as filtering, segmentation, and normalization.
- Propose a smartwatch-based authentication system for recognizing and verifying signatures based on the collected data.
- Build the system by training the deep learning models.
- Test the model and evaluate its Performance in distinguishing between original and fake signature.
- implement a prototype of real-time air signature authentication system to test the model.

## 1.3 Proposed Solution

The proposed solution centers around leveraging the motion sensors embedded in smartwatches, such as accelerometers and rotation, to capture and analyze handwriting signatures made in the air.

- 1- **Data Collection via Smartwatch Sensors:** The project will utilize the accelerometer and rotation data from the smartwatch to record the dynamic movements associated with handwriting signatures. These sensors are ideal for capturing motion, making it possible to track the signature gestures performed in the air.
- 2- **Preprocessing and Signal Filtering:** Once the motion data is collected, preprocessing will focus on extracting the signature-specific segments from raw data. Signal processing techniques such as filtering (to remove noise), segmentation (to isolate relevant signature data), and normalization (to ensure uniformity) will be applied. This step is critical to ensure that only the relevant motion data is analyzed, enhancing the accuracy of the signature recognition process [9].
- 3- **Algorithm proposed for Recognition:** Based on the processed data, the next step will be to identify and implement the most suitable algorithm for signature recognition and validation. Machine learning models, particularly **Convolutional Neural Networks (CNNs)** and **Recurrent Neural Networks (RNNs)**, will be explored. CNNs are highly effective at feature extraction from spatial data, while RNNs are adept at understanding sequential patterns in time-series data, such as those captured during signature gestures.
- 4- **Model Training and Evaluation:** The proposed model will be trained using the processed data, where it will learn to differentiate between genuine signatures and forgeries. The system's effectiveness will be evaluated by measuring its accuracy in detecting authentic signatures, its speed in processing the data. A key aspect of evaluation will also involve comparing the accuracy with other-based signature approaches.
- 5- **Real-Time Application and Authentication:** The final solution will focus on developing a real-time air signature authentication system. This system will allow users to perform their signatures in the air while the smartwatch verifies their authenticity based on the trained model.

## 1.4 Research Scope

The research focuses on the development of a system for recognizing and verifying "Air Signatures" using smartwatches. The main goal is to utilize the sensors within smartwatches, such as accelerometers and rotation, to capture the motion data produced during signature gestures performed in the air. This data will be processed using machine learning techniques to distinguish genuine signatures from forgeries.

The research **Boundaries:**

### Inclusions:

- 1- **Data Collection:** The study will collect data exclusively through the sensors embedded in smartwatches, particularly accelerometers and rotation [2].
- 2- **Machine Learning Models:** Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs) will be used to process and classify the collected signature data [7] [3].
- 3- **Algorithm Development:** The focus will be on developing algorithms that can process motion data efficiently in real-time, with an emphasis on accuracy, speed [7].
- 4- **Comparison with Other System:** A comparison will be made with other system recognition Approaches to evaluate the advantages of smartwatch-based systems in terms of privacy, portability, and user-friendliness [8].
- 5- **System Evaluation:** The system's performance will be evaluated on metrics such as accuracy, and resistance to forgery attempts [5] [10].

### Exclusions:

- 1- **Hardware Development:** No new hardware (sensors or devices) will be developed; the research will solely rely on existing smartwatch technology.
- 2- **Non-Signature-based Data:** The research will not address non-signature motion data (gestures for other purposes) or authentication methods beyond handwritten air signatures.

### Research Questions:

- How accurately can a smartwatch capture and differentiate between genuine and forged air signatures using accelerometer and rotation data [2] ?
- Which machine learning models and algorithms are most effective in processing smartwatch motion data for air signature recognition [7] [3] ?
- How does the performance of a smartwatch-based air signature recognition system compare with traditional camera-based approaches in terms of accuracy, usability, and efficiency [8] ?
- What are the challenges in real-time processing of air signature data on wearable devices, and how can these be overcome?

## 1.5 Research Significance

The significance of this research lies in addressing the growing need for secure, portable, and user-friendly authentication systems in an increasingly digital world. Traditional authentication methods, such as passwords and PIN codes, are susceptible to security risks, including theft, guessing, and brute-force attacks [6]. By leveraging wearable technology, specifically smartwatches, to perform in-air signature recognition, this research introduces a novel biometric authentication approach that combines security, convenience, and accessibility [2].

### Potential Benefits:

**Enhanced Security:** The difficulty in forging a signature performed in the air increases the security of the authentication system. Each individual's unique hand gestures and motion data provide a biometric pattern that is hard to replicate [5] [8].

**Portability and Convenience:** Smartwatches, due to their widespread use and ease of wearability, present a highly portable solution. Users can authenticate themselves seamlessly without the need for additional hardware like tablets or signature pads [7].

**Real-time Processing:** The ability to process motion data from signatures in real-time enhances user experience by providing fast and efficient authentication [10].

### Overall Impact:

This research has the potential to revolutionize biometric authentication by utilizing the growing adoption of wearable devices. It could significantly improve security standards across various industries, such as banking, healthcare, and online transactions, where user identity verification is critical. Furthermore, it could inspire future developments in wearable authentication technologies, contributing to the broader field of human-computer interaction and biometric security.

By offering a secure and intuitive authentication system, this project not only fills a critical gap in biometric research but also aligns with the future trends of integrating advanced technology into everyday devices [3]. The potential societal impact includes making secure authentication methods more accessible, thereby improving overall cyber-security practices across multiple sectors.

## 1.6 Ethical and Social Implications

The "Air Signature Using Smartwatch motion sensors" project, approved by the King Saud University Higher Education Ethics Committee (Ref No: KSU-HE-25-485), introduces several ethical, legal, and social implications. By using biometric authentication, this research directly impacts issues related to security, privacy, and the protection of personal data. Biometric systems, while offering enhanced security, also raise concerns about data misuse, unauthorized access, and the ethical handling of sensitive information [11] [4].

### **Ethical Considerations:**

1. **Privacy:** Air signature data is a form of biometric information, and as such, it is critical to ensure that it is stored, processed, and transmitted securely to prevent unauthorized access. Ethical standards must be followed to protect individuals' biometric data from being misused, leaked, or shared without consent [6].
2. **Data Security:** Secure storage mechanisms are essential to protect users' air signature data. As with other forms of biometric authentication, the misuse or theft of such data could have severe consequences for users. Ensuring robust security measures is vital to maintaining trust and protecting user identity [2] [7].
3. **Informed Consent:** Users need to be fully aware of how their biometric data will be used, stored and shared. Informed consent should be obtained, ensuring that individuals understand the potential risks and benefits of participating in this system [6].

### **Social and Cultural Implications:**

1. **Accessibility:** The use of smartwatches for air signatures is more inclusive than systems that rely on specialized devices, offering a broader range of accessibility across different populations. However, cultural differences may affect the acceptance of such biometric systems, especially in regions where biometric technologies are viewed with skepticism [4].
2. **Equity:** The adoption of wearable technology raises questions about equitable access. While smartwatches are becoming more widespread, there are still segments of the population that may not have access to these devices. Ensuring that this technology does not inadvertently exclude, or disadvantage certain groups is an important social consideration [2] [12].

### **Legal Implications:**

- **Regulation Compliance:** Since this project involves biometric data collection, it must comply with data protection regulations such as the General Data Protection Regulation (GDPR) in Europe, which governs the handling of personal data, including biometrics [11] [6]. Strict adherence to legal frameworks that regulate the collection and use of biometric data will be essential to avoid legal risks.
- **User Autonomy:** The system must be designed in a way that respects user autonomy, giving users the ability to control their data, withdraw consent, and understand how their biometric information is being utilized [6] [7].
- **Impact on Society:** The integration of air signature technology using smartwatches represents a shift toward more portable and secure forms of biometric authentication. As these systems are adopted, they could contribute to enhanced security in various sectors, including banking, healthcare, and digital transactions. However, with this technological advancement comes the responsibility of ensuring that it is used ethically and inclusively [2] [13].



## 1.7 Report Organization

This report is organized to provide a structured and comprehensive presentation of our research process and findings.

It begins with the **Acknowledgments**, followed by both **English** and **Arabic abstracts**, which summarize the research objectives, methodology, and results.

### **Chapter 1 - Introduction**

Outlines the problem statement, research goals, proposed solution, scope, and significance of the study. It also addresses the ethical and social considerations involved.

### **Chapter 2 - Background**

offers a detailed background, covering biometric authentication, online and offline Signature Verification, air signature, smartwatch motion sensors, and relevant machine learning models.

### **Chapter 3 - Literature Review**

presents the literature review, including a table comparing previous works in the field of air signature systems. It concludes with a discussion section that summarizes the findings from the literature, addressing the challenges faced in earlier studies, the advantages and disadvantages of different approaches, the datasets used, and their limitations. Additionally, the contribution of this research is highlighted.

### **Chapter 4 - Data Collection**

Describes the process of collecting motion data using a smartwatch, including device setup, participant recruitment, signature recording, and challenges faced during data acquisition.

### **Chapter 5 - Methodology**

Details the preprocessing techniques and the proposed BLSTM model architecture, including layer descriptions and the rationale behind model selection. It also outlines the training and evaluation procedures.

### **Chapter 6 - Experimental Design**

Defines the research hypotheses and explains the experimental setup, including data partitioning, evaluation metrics, and descriptions of the four conducted experiments.

### **Chapter 7 - Results and Discussion**

Provides an analysis of the experimental outcomes, comparing the performance of different models, discussing the effect of data augmentation, and evaluating the system's robustness.

### **Chapter 8 - Application of the model**

Presents a practical usage scenario through a smartwatch interface, showcasing how the air signature system supports multi-factor authentication alongside traditional login methods.

### **Chapter 9 - Conclusion and Future work**

Summarizes the research outcomes, emphasizes the effectiveness of the proposed system, and outlines future directions for improvement

Figures, Tables, references, and appendix are provided to help clarify complex information.

## 2. Background

### 2.1 Biometric Authentication

In today's digital world, securing personal information and verifying identities is more important than ever. **Biometric authentication**, which is the science of establishing the identity of an individual [11], has emerged as a key solution in this space, utilizing unique biometric characteristics of a person such as fingerprint, facial features, speech, iris, palm print, signature, DNA, body odor and vein pattern etc. [4], biometric system can be a identification or verification (authentication) system:

- Identification (one-to-many):  
matching of a testing biometric sample against the entire database of trained biometric samples.
- Verification (one-to-one):  
matching a testing biometric sample against the claimed biometric samples in the database.

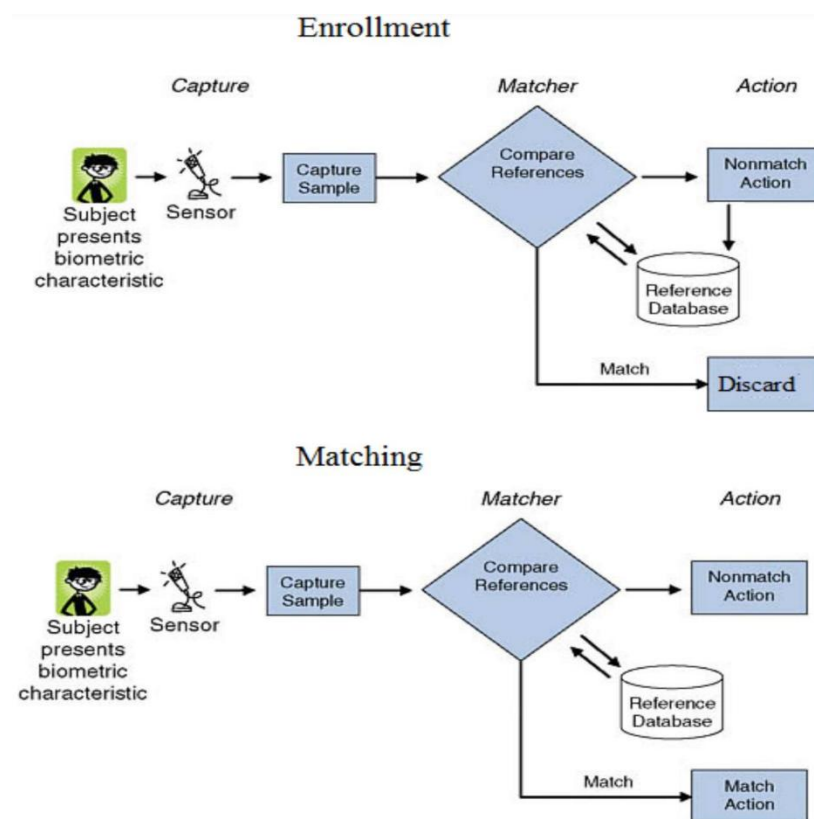


Figure 1 General Biometric System [4]

A general block diagram of a biometric authentication system is shown in **Figure 1**.

The **biometric authentication process** consists of two main steps:

1. Enrollment: is the initial process of capturing and storing a user's biometric signature as a reference template.
2. authentication (Matching): is the process of comparing a new biometric input against the stored template to verify the user's identity.

Each step involves capturing the biometric sample, converting it into a reference template, and comparing it with stored data [4]. This approach provides a more secure and convenient alternative to traditional password systems.

## 2.2 Signature Verification Techniques

**Signature verification** is a widely used biometric method for identity authentication due to its ease of use and familiarity in everyday transaction [14] [15]. It involves analyzing the unique characteristics of an individual's handwritten signature to confirm their identity. With advancements in technology, signature verification methods have evolved from traditional paper-based systems to more Advanced digital approaches [1] [14]. These methods can be broadly categorized into two types: **offline (static)** and **online (dynamic)** verification, each with its own techniques, strengths, and limitations. The following sections explore these two approaches, highlighting their applications and relevance to modern biometric systems.

### 2.3 Offline (Static) Signature Verification

**Offline signature verification**, also known as **static verification**, involves analyzing handwritten signatures that are written on paper and then scanned to create a digital image for analysis. In this approach, only the completed signature is available as a two-dimensional image, meaning that the system can only extract static features such as shape, texture, and geometric characteristics [1] [15]. Techniques used in offline signature verification include image processing methods such as granulometric size distributions, which analyze local shape descriptors based on the structure of the signature's visual elements [15].

However, since offline systems do not capture dynamic information like speed, pressure, or stroke sequence, they are generally more Vulnerable to skilled forgeries. As a result, the accuracy of these systems relies heavily on the quality of the scanned image and the robustness of the feature extraction algorithms used [15].

### 2.4 Online (Dynamic) Signature Verification

**Online signature verification**, also known as **dynamic verification**, captures real-time data as the signature is being written. This method involves using devices like digitizing tablets, including temporal information such as speed, pressure, and the sequence of strokes [14]. Unlike offline verification, online systems leverage dynamic characteristics that are unique to each individual's handwriting style, making it significantly harder to forge a signature. The real-time data collected includes time-based features like velocity and acceleration, which can be analyzed to differentiate between genuine and forged signatures [14] [1]. Due to its higher security and accuracy, online verification is widely used in applications that require robust authentication, such as secure banking systems and digital document signing. A new technique, known as **air signature**, is a type of Online signature verification which offers a novel way to authenticate signatures based on unique biometric patterns, and will be our focus in this research.

## 2.5 Air Signature

*Figure 2 Air Signing Process [3]*



**Air signature** systems allow individuals to sign their names or make specific gestures in the air as shown in **Figure 2**, captured through advanced sensors for authentication purposes. This contactless method addresses both security and hygiene concerns, making it a promising option for a variety of applications [3].

However, like all biometric systems, air signature recognition faces challenges related to **forgery and security**. Attackers may attempt to replicate a person's air signature, leading to potential security violations. To address this security concern, modern air signature systems must accurately distinguish between genuine signatures and forged signatures, while remaining efficient for real-time use. This highlights the need for secure and reliable algorithms capable of handling various authentication scenarios [4].

The **real-time gesture recognition** capability of air signature systems is essential for real-world applications. It requires the system to process and verify signatures quickly, without noticeable delay, to provide a seamless user experience. Achieving this in real-world applications often depends on the technology used to capture the signature. Among the various devices, smartwatches have become increasingly popular for this purpose due to their portability and built-in motion sensors.

## 2.6 Smartwatch Motion Sensors

**Smartwatch motion sensors**, particularly accelerometers, play a crucial role in air signature recognition by capturing the movement of the user's hand in three-dimensional space. These sensors allow for real-time identity verification by collecting motion data that shows the speed, direction, and pattern of in-air signing gestures [2]. Their integration into widely available wearable devices makes them ideal for portable and user-friendly biometric systems [2].

An **Accelerometer** measures **linear acceleration** across the x, y, and z axes, offering insights into the direction and intensity of hand movements. It has long been used in applications such as smartphone orientation detection, fitness tracking, and automotive impact sensing [12].

In addition to linear acceleration, the smartwatch records **rotation data** along the X, Y, and Z axes. This rotation data captures how the hand **rotates or tilts** during the signature, providing crucial insights into the angular aspects of the motion, and **Pitch, Roll, and Yaw** angles, which describe the device's angular orientation in three-dimensional space [16]:

- **Pitch:** Upward or downward rotation around the front-to-back axis (Y-axis)
- **Roll:** Side-to-side tilting around the left-right axis (X-axis)
- **Yaw:** Left or right rotation around the vertical axis (Z-axis)

The rotation sensors capture the angular motion of the hand, complementing the accelerometer's linear motion data. Although smartwatches typically include a gyroscope to measure rotational velocity, this project utilized the rotation and orientation data (X, Y, Z and Pitch, Roll, Yaw) provided by the device, effectively capturing the necessary angular information for signature recognition.

Together, linear acceleration and rotational movement data provide a comprehensive picture of spatial motion during air signature input. This dual-sensor approach enables more robust and accurate recognition by capturing both the directional (linear) and angular (rotational) aspects of the user's handwriting pattern.

## 2.7 Dynamic Time Wrapping

In the early stages of gesture recognition, techniques like **Dynamic Time Warping (DTW)** were widely used. DTW measures the similarity between two temporal sequences by aligning them, making it possible to recognize basic hand gestures. However, DTW has limitations in handling complex, real-time, and 3D movements that are characteristic of air signatures [17]. This has led researchers to explore more advanced methods for analyzing motion data [18].

## 2.8 Deep Learning Techniques

Deep learning has significantly advanced biometric authentication by enabling systems to learn complex patterns from motion data with high accuracy. In air signature recognition, deep learning models can process both spatial and temporal features of movement data collected from smartwatch sensors. Among the most prominent techniques used in this domain are **Convolutional Neural Networks (CNNs)** and **Recurrent Neural Networks (RNNs)**, each with unique strengths. This section introduces the models employed in this research, detailing their roles and advantages in air signature recognition.

### 2.8.1 Conventional Neural Networks (CNNs)

Convolutional Neural Networks (CNNs) are powerful deep learning models primarily used for processing spatial data, such as images or grid-structured signals. In air signature recognition, CNNs are employed to extract spatial features from motion data either by converting raw accelerometer readings into 2D/3D image-like formats or by directly modeling the signal's spatial patterns. These models can detect the trajectory, shape, and curvature of the signature by learning hierarchical representations through layers of convolutions and pooling operations [7].

One of the major advantages of CNNs is their ability to perform feature extraction automatically, reducing the need for handcrafted features. Architectures such as **ResNet (Residual Network)** and VGGNet are particularly notable. ResNet, for example, uses skip (residual) connections to enable the training of very deep networks by avoiding vanishing gradient problems, making it highly effective even with medium-sized datasets [7] [19]. This ability allows CNN-based systems to maintain high accuracy while minimizing overfitting, especially in scenarios where large, labeled datasets are limited.

A typical CNN architecture consists of:

- An **input layer** (for example a 3D static image derived from motion data),
- **Convolutional layers** with filters to detect local features,
- **Activation functions** (such as ReLU),
- **Pooling layers** for dimensionality reduction,
- And **fully connected layers** for final classification [20].

By preserving spatial relationships and extracting meaningful features, CNNs provide a robust foundation for recognizing distinct signature shapes and variations across users.

### 2.8.2 Recurrent Neural Networks (RNNs)

While CNNs are suited for spatial analysis, **Recurrent Neural Networks (RNNs)** excel in handling sequential and time-dependent data, such as the sensor readings recorded over time during an air signature. Unlike feedforward networks, RNNs maintain **memory of previous inputs** through recurrent connections, enabling them to model the temporal dependencies that characterize a user's signing behavior.

This temporal modeling is essential for distinguishing between genuine and forged signatures, as it captures how the signature is performed and not just what it looks like. Variations in timing, speed, and rhythm can all be captured effectively using RNNs, making them especially relevant for motion-based biometric systems [21].

However, standard RNNs often suffer from the vanishing gradient problem, making it difficult to learn long-range dependencies. To address this, **Long Short-Term Memory (LSTM)** networks were introduced. LSTM units include gating mechanisms (input, forget, and output gates) that control the flow of information, allowing the model to retain or discard information over time [22]. These improvements led to more stable and effective training for time-series tasks.

As we transition into our methodology section, we build upon this foundation by introducing **Bidirectional LSTM (BLSTM)** networks, which further improve performance by processing sequences in both temporal directions.

### 2.8.3 Bidirectional Long Short-Term Memory (BLSTM)

**BLSTM** is a specialized architecture that enhances traditional LSTM by incorporating two parallel LSTM layers:

- One processes the sequence in the forward direction (from start to end),
- The other processes it backward (from end to start).

The outputs of both directions are then combined to form a richer representation of the sequence. This is particularly advantageous in air signature recognition, where information from the entire motion sequence in both past and future contexts which helps the model better understand subtle patterns and timing variations [2] [3].

Compared to standard LSTM, BLSTM captures bidirectional dependencies, improving the system's ability to recognize signatures that may vary in orientation, duration, or stroke order. This enhanced temporal awareness makes BLSTM especially effective in applications with complex motion dynamics, such as air signatures.

In this research, the BLSTM model serves as the core of our proposed system. Its ability to handle time-sequential sensor data and distinguish between fine-grained variations in signing behavior makes it well-suited for robust biometric authentication.

### 3. Literature Review

Offline signature verification, centered on analyzing static, scanned images of handwritten signatures, has played a crucial role in shaping the field of biometric authentication.

Early foundational approaches like those of Sabourin et al. (1997) [15], introduced granulometric size distributions, a technique analyzing shape details at varying scales, to address local variability in handwritten signatures. Local variability refers to subtle differences within different parts of the same signature, significantly reducing error rates. Building on traditional techniques.

Lopes et al. (2022) [20], employed convolutional neural networks (CNNs) to automate offline signature verification, demonstrating over 85% precision by using data augmentation to enhance the robustness of their model. This approach mitigated challenges like limited datasets but struggled with high intra-class variability such as in variations of signatures from the same individual. a persistent issue in offline methods.

Similarly, Kao et al. (2020) [23], advanced deep learning applications in offline verification by focusing on local stroke patterns and unique features within segments of the signature. Their system achieved high accuracy rates (94.37%–99.96%) even when working with limited reference samples.

Srihari et al. (2000) [1], provided a broader perspective by surveying both online and offline handwriting recognition systems, with a particular focus on their applications in signature verification and writer identification. This study outlined the inherent limitations of offline methods, such as lower accuracy due to the lack of trajectory data, while also highlighting their cost-effectiveness and successful applications in domains like postal address recognition and check processing. The survey emphasized how techniques such as Hidden Markov Models (HMMs) have improved offline system performance by addressing challenges like geometric variations and noise reduction.

While these offline systems demonstrated considerable advancements, their reliance on static data limits adaptability to dynamic, real-time scenarios, underscoring the need for systems like air signature recognition, which leverage online methods for greater flexibility and accuracy.

Now we will be exploring the Related Works on Air signature using the smartwatch sensors which is a part of Online signature verification systems and our focus for this research.



## 3.1 Related Work On Air Signature

The field of air signature recognition, has seen significant advancements across various platforms, including camera-based, smartwatch-based, and other emerging systems. Each of these approaches leverages different technologies to capture, analyze, and authenticate signatures in the air, offering a promising alternative to traditional biometric methods. This review explores the development of air signature systems, categorized into three main types: camera-based, smartwatch-based, and other innovative methods. We examine key studies that have shaped the evolution of these systems, highlighting their contributions, limitations, and future potential in biometric security.

### 3.1.1 Camera-Based-System

One of the earliest foundational works in this area, Reinders et al (2007) [18], introduced dynamic time warping (DTW) as a method for recognizing gestures by analyzing temporal sequences. Although not originally focused on air signatures, this approach provided a starting point for tracking and analyzing hand gestures in 2D space. While the dataset used was small and custom-made, focusing on simple hand gestures, However, DTW's approach had limitations, such as its difficulty in handling more complex gestures in 3D or real-time settings, making it less useful for today's advanced air signature systems.

Malik et al (2018) [24], built on earlier gesture recognition work by introducing depth sensors to capture 3D hand movements. This shift from 2D to 3D allowed for more accurate verification, as depth features provided additional depth and volumetric details that enhance the accuracy of gesture recognition that DTW-based methods lacked. The authors built a custom-made dataset by capturing 3D in-air hand trajectories from 20 participants using depth sensors. The system achieved a low Equal Error Rate (EER) of 0.46%, showing its robustness. However, the need for specialized hardware (depth sensors) presents a challenge in terms of widespread accessibility and scalability.

As deep learning became more prevalent, Malik et al (2020) [8], addresses the growing need for electronic identity verification in virtual environments, emphasizing the importance of biometric systems, this paper advanced the field by using CNNs and personalized autoencoders to preprocess signature data. The system achieved an impressive EER of 0.055% and a 67.6% improvement in accuracy, significantly outperforming heuristic approaches like DTW. Despite the accuracy improvements, deep learning models typically require large datasets, so the authors custom-built medium-scale dataset of 1,800 signatures from 40 participants. This dataset collected using multiple cameras to capture 3D hand movements allowed the system to train more effectively by focusing on spatial and depth features.

Expanding on this, Deng et al. (2023) [13], the vulnerabilities of in-air signature systems, particularly against robot-level replay attacks, by extending traditional single-point fingertip tracking to multi-joint hand skeleton tracking. Their dataset consists of in-air signature data from 25 participants, each performing 40 signatures, captured using both RGB and depth cameras (Leap Motion). The system was trained on 20 signatures and tested on the remaining 20. Additionally, it was evaluated against robot replay attacks using 3D-printed hand models attached to a robotic arm, as well as simulated replays. This approach captures the complexity of inter-joint motions, significantly enhancing security and reducing the false acceptance rate compared to existing single-point tracking methods. However, the study has limitations with the system's effectiveness relies heavily on the precision of commercial hand-tracking interfaces, which can be affected by environmental factors like lighting conditions.

The most recent development in this category, Sarveswar Sarma (2024) [6], the limitations of traditional techniques, which rely on physical signatures and specialized hardware, making them less accessible and more vulnerable to forgery. To overcome these challenges, the authors propose an "Air Signature" solution, which enables users to sign documents in the air using a camera-based system. They introduced a CNN-based model that tracks single-finger movements using standard web cameras. Also leveraging three publicly available datasets: CEDAR, UTSig, and BHSig260. Additionally, the study incorporated a custom dataset captured using a palm detection model with the Mediapipe library. While this system makes signature verification more accessible by eliminating the need for specialized hardware, its False Acceptance Rate (FAR) of 5.39% and False Rejection Rate (FRR) of 7.48% indicate that it still requires improvement for high-security applications. Nevertheless, this study represents a major step forward in creating hardware-agnostic air signature verification systems

### 3.1.2 Smartwatch-Based-System

With the increasing use of wrist-worn devices for signature verification has introduced new methods to enhance security. Levy et al. [25] a verification system using motion signals from wrist-worn devices to achieve high accuracy without specialized digital signing tools. The study focused on challenges such as distinguishing genuine signatures from random and skilled forgeries, using machine learning models. Their approach achieved an EER of 2.36%, outperforming other systems in accuracy and reliability.

The rise of smartwatch-based systems has introduced new methods for air signature verification, due to the convenience and portability of wearable devices with most studies relying on custom datasets collected through motion sensors such as accelerometers and gyroscopes.

Li et al (2020) [2], was one of the earliest studies in this area, using smartwatch accelerometers and gyroscopes to verify handwritten signatures addressing the security flaws of traditional password systems. By processing raw motion data, additionally developed a custom dataset consisting of 400 signatures from 20 participants using an Apple Watch during the signing process. Participants provided both genuine and forged signatures, allowing the system to train on realistic forgery scenarios. By utilizing Siamese recurrent neural networks (RNNs), the system effectively distinguished between genuine and forged signatures, achieving an EER of 0.78%. The study demonstrates that siamese RNNs and smartwatch motion data offer an effective, low-error method for signature verification, with potential for broader applications in biometric security. However, it was limited by its relatively small dataset, which raises concerns about the model's generalizability across a wider population.

Expanding on this, Ramachandra et al (2020) [26], combined signature verification with text-based user verification, leveraging the accelerometer data captured during handwriting and signature activities. The proposed approach uses Continuous Wavelet Transform (CWT) for signal analysis and deep learning via ResNet50. The significantly larger dataset, involving 30 participants and generating 10,800 samples included handwritten signatures as well as text-based inputs, captured using two different smartwatches and on two mediums (paper and iPad). This system achieved near-perfect results in some scenarios, with a 0% EER when using the same smartwatch across all activities. However, the performance dropped significantly (up to 10.57% EER) when different devices were used, highlighting a key challenge in cross-device consistency which refers to the challenge of achieving consistent accuracy when using different smartwatch models or brands.

Building on these systems, Sato et al (2022) [3], focused on improving forgery resistance by using bidirectional LSTMs in a recurrent neural network (RNN). Which also developed a custom dataset, capturing in-air signature motions from 22 participants. The dataset included both genuine and forged signatures collected using a smartwatch's accelerometer and gyroscope. The system tackled common challenges like variability in signature length and orientation (Different users may have signatures of varying lengths, which can make standardization and comparison difficult) and orientation (The orientation of air signatures can change between attempts, potentially affecting recognition accuracy). achieving a strong EER of 0.83%. Despite its high accuracy, Although the study emphasized the limited diversity of its small number of participants, suggesting a need for more comprehensive testing to ensure robustness across different populations, it demonstrates the feasibility and effectiveness of in-air signature authentication as a secure, user-friendly alternative to traditional methods.

A more recent paper, Lim et al (2023) [27], addressed the need for computational efficiency in real-time hand gesture recognition systems, particularly in response to the challenges of hygiene and contactless interactions emphasized by the COVID-19 pandemic. The authors developed a custom dataset involving 25 participants, each providing various in-air hand gestures, to train their model. Their approach focused on using a shallow multi-scale Convolutional Neural Network (CNN) architecture to balance high accuracy with reduced computational requirements, achieving a notable 93% accuracy in recognizing in-air hand gesture signatures while minimizing training time. The system's efficiency made it highly suitable for real-time applications, particularly in environments where quick processing is crucial. Moreover, while the CNN architecture was effective on its own, the authors also explored the potential for integrating Recurrent Neural Networks (RNNs) to capture the temporal dynamics of hand gestures, creating a more complex convolutional recurrent neural network (CRNN) architecture. Despite these advantages, the paper did not fully address some of the challenges associated with real-world deployment, particularly regarding energy efficiency and resource management. As a result, while the study makes significant gains in computational efficiency, future work could focus on overcoming these limitations to ensure that the model is as practical in deployment as it is in experimentation.

Finally, Guo et al (2023) [7], introduced an innovative approach to in-air signature recognition by converting time-series motion data into 3D static images, allowing CNN models to better process signature data. They created a custom dataset of 440 signatures from 22 participants, including both genuine and forged signatures, and evaluated several CNN architectures, such as ResNet and VGG, against this dataset. The ResNet model achieved an impressive 99.85% accuracy, demonstrating the effectiveness of 3D transformation in capturing the complexity of motion-based signatures. However, while this approach proved powerful, it also highlighted challenges in preprocessing and the risk of overfitting on median-sized datasets.

### 3.1.3 Other-System

Besides camera- and smartwatch-based systems, other innovative methods have emerged, including smartphone and Wi-Fi-based approaches for air signature verification, have also relied on custom datasets to evaluate their performance.

Shao et al (2021) [5], introduced a system that used a combination of acoustic and motion sensors on smartphones to authenticate users via air signatures. The dataset from 50 participants allowed the authors to demonstrate the effectiveness of combining acoustic and motion data for signature verification, this hardware-agnostic solution achieved a high F-score of 97.1%, providing a promising alternative to traditional PIN- or fingerprint-based authentication. However, the system's reliance on inaudible acoustic signals raises concerns about environmental noise and interference, which could affect reliability in diverse real-world settings.

The latest development in this category, Jung et al (2021) [10], paper introduces a new way to identify users based on in-air handwritten signatures using Wi-Fi signals. The system captures signal changes caused by a person's hand movements, using an Intel 5300 Network Interface Controller (NIC) and a 2.4 GHz Wi-Fi router. To handle different user positions, the system uses transfer learning, which helps it adapt without needing to retrain from the beginning. The system also uses a Kernel and Range (KAR) space projection learning method to make the process faster. The study gathered Wi-Fi signal data from 100 participants using a VAIO laptop with Intel Core i5 and external antennas. Participants signed in the air at various positions and directions. The system, based on a pre-trained Convolutional Neural Network (CNN) model, in scenarios without wireless interference, the average EER is 0.13%, indicating high accuracy in identifying users. It also worked well despite issues like wireless interference and different signal speeds, showing promise for use in everyday settings. This research offers a simple, cost-effective method that doesn't require extra hardware. It faces limitations in scenarios with Wi-Fi signal interference, which can degrade accuracy and reliability in dynamic environments.

## 3.2 Table of Comparison

Table 1 Table of comparison

Reference	System Type	Model	Device	Sensors	Accuracy	Data Set	language used
[18], 2007	Camera-Based-System	MD-DTM	Two Camera	camera	high level	121 signature from 67 right-handed participants	Dutch Sign Language
[24], 2018		CNN, MD-DTW, IEF	Camera	Intel's Creative Sens3D camera	EER = 0.46%	600 signatures (15 genuine, 25 forgeries per participant) from 15 participants.	Not specified
[8], 2020		End-to-End Deep learning framework	depth Camera	Creative Sens3D, tri-axial accelerometer, RGB cameras	EER = 0.055%	1800 signatures from 40 participants	English
[13], 2023		CNN	Camera	Accelerometer, Gyroscope, Kinect, Leap Motion	F1-score = 0.983	1000 signature(40 per participant ) from 25 participants.	English
[6], 2024		CNN	Camera	Web Camera	FAR = 5.39% FRR = 7.48%	CEDAR UTSig BHSig260	Hindi , Bengali Persian Not specified
[2], 2020	Smartwatch-Based-System	RNN (BLSTM) , DTW	Apple watch series 3	Accelerometer , Gyroscope	EER = 0.78%	2900 pairs of signature from 20 participants	English
[26], 2020		CWT & ResNet50	LG & Sony smartwatch	accelerometer	EER=0 EER= 2.58-10.57	300 signatures from 30 participants	English
[3], 2022		RNN (BLSTM)	Smartwatch	Accelerometer , Gyroscope	EER = 0.83%	440 signature from 22 participants	Japanese, Chinese
[27], 2023		MS-CNN	Smartwatch	Accelerometer , Gyroscope	ERR = 0.83%	440 signature(10 forged ,10 genuine per participant)from 22 participants	Not specified
[7], 2023		CNN	Smartwatch	Accelerometer , Gyroscope	not provided	440 signatures(220 genuine-220 forgeries) from 22 participants	English
[5], 2021	Smartphone-Based-System	DTW, SVM	smartphone	Accelerometer, Gyroscope	F-score = 97.1%	3,300 signatures(10 registered, 10 Genuine,10 forged per participant) from 30 participants	English
[10], 2021	WIFI-Based-System	CNN 4 , CNN 6	Intel 5300 (NIC) 2.4 GHz Wi-Fi router	Wi-Fi transmitter (IpTime A1004 router)	EER (0.56% at 10kp/s), (3.94% at 1kp/s)	8000 signature from 100 participants	Not specified

### **3.3 Discussion**

This section displays the finding of our literature review, starting by showing the evolution of air signature recognition systems, challenges faced by various system types, the advantages and disadvantages of each approach, and the datasets used across the different methods explored in our research. We also highlight the unique contribution of our work, particularly in developing a smartwatch-based system for Arabic language air signatures.

#### **3.3.1 Evolution in Air Signature Recognition Systems**

The evolution of air signature systems has been driven by advancements in sensing technologies and machine learning algorithms. Early works such as camera-based systems laid the foundation for air signature capture, primarily relying on 2D or 3D hand gesture recognition through dynamic time warping [18].

These systems progressed to more complex frameworks utilizing deep learning techniques like Convolutional Neural Networks (CNNs), which significantly enhanced accuracy as shown in Table 1.

As technology advanced, research shifted towards portable devices, with a particular focus on smartwatches. Smartwatch-based systems, utilizing accelerometers and gyroscopes, emerged as a promising approach for air signature authentication. This transition highlights the trend towards more user-friendly, portable, and real-time systems.

### 3.3.2 Challenges

In the development of air signature recognition systems, each approach faces unique challenges that impact the effectiveness and usability of the systems. From Camera-Based systems to Smartwatch-Based systems and Other-Based systems, The challenges range from hardware dependencies to being affected by surroundings. These challenges must be addressed to ensure the systems' reliability, accuracy, and portability in real-world applications. Below we discuss challenges specific to each system type.

#### **- Camera-Based Systems**

Camera-based systems are known for their high accuracy, especially when using advanced sensors like RGB and depth cameras look Table 1. However, these systems face limitations in portability and scalability due to the reliance on specialized hardware. Moreover, environmental factors such as lighting and background noise can affect their performance.

#### **- Smartwatch-Based Systems**

Smartwatch-based systems bring the advantage of portability and real-time processing. However, the challenges here include variability in wrist motion, differences in user's signature styles, and limited battery life of the devices. Additionally, achieving consistency across different smartwatch models remains a significant challenge, as some studies report performance drops when using different devices [26] [3].

#### **- Other Systems Other**

approaches, such as Wi-Fi or smartphone-based systems, leverage innovative methods for air signature recognition. These systems often aim to eliminate the need for specialized hardware, but they introduce challenges related to signal interference and reliability in diverse environments.



### 3.3.3 Advantages and Disadvantages

Each air signature recognition system brings its own set of advantages and disadvantages. This system while offering new approaches to biometric authentication vary in their performance, usability, and scalability depending on the technology used. It's important to crucial to evaluate the strengths and limitations of each system.

The different Based Systems introduce different **Advantages**, Starting with **Camera-Based Systems**, which offered high precision and have shown strong performance in controlled environments. They can capture detailed 3D motion. which is advantageous for signature verification look Table 1. Secondary with the **Smartwatch-Based Systems** with the most advantage being highly portable and convenient for real-time applications. They also provide a more user-friendly experience by leveraging devices that users already own and wear [2] [3]. Lastly the **Other-Based Systems** like Wi-Fi-based approaches are cost-effective and Hardware-flexible, making them scalable for various of application, look at Table 1.

Following the Advantage, The systems also have **Disadvantages**, Firstly with **Camera-Based Systems** that require specialized equipment, Which limits their scalability and usability in everyday settings [24] [6]. which was solved with **Smartwatch-Based Systems** that also faced challenges with variability in signature styles and cross-device accuracy, as well as the limited battery life of wearable devices [3] [26]. look at Table 1. Finally with **Other-Based Systems** often struggle with environmental interferences, such as signal degradation, which can block performance in real-world scenarios.

### 3.3.4 Datasets

Across literature, datasets vary widely in size and language. Camera-based systems tend to use larger datasets, such as the CEDAR or UTSig datasets, which are predominantly in English Table 1. In contrast, smartwatch-based systems often rely on smaller, custom-built datasets, such as the 400-signature dataset used in a study involving an Apple Watch [2]. These datasets are generally in English, with very few addressing other languages.

## 3.4 Our Contribution

Our contribution focuses on developing an air signature recognition system using smartwatch motion sensors specifically tailored for Arabic-language signatures. This is a novel approach, as most existing research predominantly focuses on English or other languages Table 1. By introducing a system that leverages accelerometers and gyroscopes within smartwatches, we aim to provide a portable and real-time solution for Arabic speakers. This addresses a critical gap in the current literature, particularly in terms of dataset availability and language diversity. Our system builds on the advancements in smartwatch-based approaches, while specifically addressing the need for broader language integration in biometric security.

In summary, while previous research has explored various platforms for air signature recognition, our work is distinct in its focus on Arabic air signatures using smartwatches, contributing to both language variety and the growing field of wearable authentication systems.

## 4. Data collection

Data collection is a foundational step in this research, as it provides the raw motion data required to train, validate, and evaluate the proposed air signature recognition model. The main goal of this step is to gather motion signals from smartwatch sensors (accelerometer and rotation) while users perform in-air signatures. This chapter details the data collection process, including smartwatch selection, participant recruitment, signature recording, and key challenges faced during the acquisition of air signature data using smartwatch motion sensors.

### 4.1 Smartwatch selection & setup

To ensure accurate motion data collection, a smartwatch equipped with both an accelerometer and a rotation sensor was selected. The chosen device, An Apple Watch SE (44mm) shown in **Figure 3** was preferred due to its ease of data extraction, seamless integration with Apple's ecosystem, and user-friendly interface, making it a good choice for real-time motion data collection. The smartwatch was configured to record six motion features:

- Accelerometer data, on the three axes x, y and z.
- Rotation data, on the three axes x, y and z.
- Device attitude (orientation) readings: pitch, roll, yaw

Figure 3 Apple Watch SE (44mm)



A dedicated watch interface designed for this study shown in **Figure 4** and used on the smartwatch to record sensor data in real time, **Table 2** shows the 9-tuple of raw data representation of the in air-signature. While **Table 3** shows the 12-tuple after the pre-processing steps for each signature which will be discussed in section 5. Methodology, The recorded data was stored in CSV format for further preprocessing and analysis.

Figure 4 Smartwatch interface



Table 2 Raw data representation

Dimension	signal
1	x-axis accelerometer
2	y-axis accelerometer
3	z-axis accelerometer
4	x-axis rotation
5	y-axis rotation
6	z-axis rotation
7	pitch-axis attitude
8	roll-axis attitude
9	yaw-axis attitude

Table 3 Data after pre-processing

Dimension	signal
1	Rotated x-axis accelerometer
2	Rotated y-axis accelerometer
3	Rotated z-axis accelerometer
4	Rotated x-axis rotation
5	Rotated y-axis rotation
6	Rotated z-axis rotation
7	Derivative x-axis accelerometer
8	Derivative y-axis accelerometer
9	Derivative z-axis accelerometer
10	Derivative x-axis rotation
11	Derivative y-axis rotation
12	Derivative z-axis rotation

## 4.2 Participant Recruitment & Data Collection Protocol

### 4.2.1 Participant Selection

A total of 24 participants were voluntarily recruited to contribute to the study. Before participation, each individual was informed about the purpose of the research, the nature of data collection, and their rights regarding privacy and withdrawal. A consent form which is included in *Appendix A*, was provided, outlining the confidentiality of the collected data, the voluntary nature of participation, and the absence of any physical or emotional risks associated with the study. Only participants who provided signed consent were included in the data collection process.

### 4.2.2 Signature Recording Process & Sensor Data Acquisition & Features Collected

Each signature will be recorded under natural signing conditions without external restrictions. Participants will have the opportunity to practice their Arabic language signature's signing motion beforehand to ensure their genuine signatures are accurate and consistent. Forged signatures will be collected by having a randomly selected participants observe a genuine signature before attempting to replicate its structure and motion patterns. The data collection process shown in **Figure 5** included the following steps:

1. Participants were instructed to wear the smartwatch on their dominant wrist.
2. They were required to perform 7 genuine air signatures in the Arabic language to collect enough samples.
3. Then asked randomly to replicate another participant's signature, in a total of 7 forged air signature

The smartwatch recorded motion data continuously while users performed their signatures. The collected data was stored in CSV format with each signature session labeled as genuine or forged. After this process each participant will have 7 genuine and 7 forged signatures.

*Figure 5 Data collection process*



### 4.2.3 Challenges in Data Collection

During the data collection process, several challenges were encountered:

- **Signature consistency:** Ensuring that participants produced seven genuine signatures that closely matched each other was a challenge, as natural variations in writing style and movement could introduce inconsistencies.
- **Forgery attempts:** Some participants struggled to mimic signatures effectively, potentially affecting the dataset's balance.
- **Environmental factors:** External influences such as hand tremors impacted consistency.

### 4.3 Visual Representation of Data Collection and Pre-processing

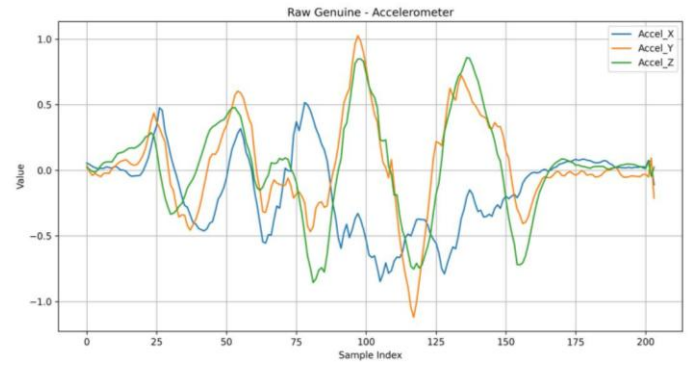
To provide a comprehensive understanding of the data collection, this section presents key visual elements illustrating the workflow.

To further clarify the collected data, **Figure 6** displays a handwritten signature, illustrating the intended signature as written by the participant.

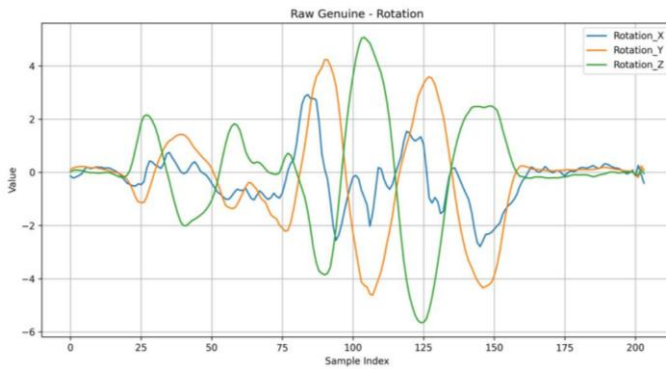
*Figure 6 Handwritten Signature*



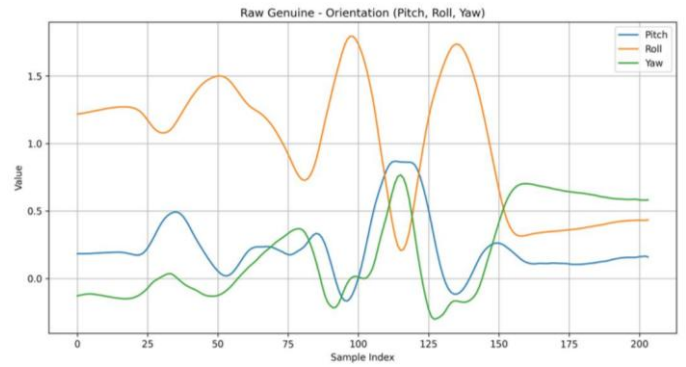
*Figure 7 Raw Genuine Accelerometer*



*Figure 8 Raw Genuine Rotation*

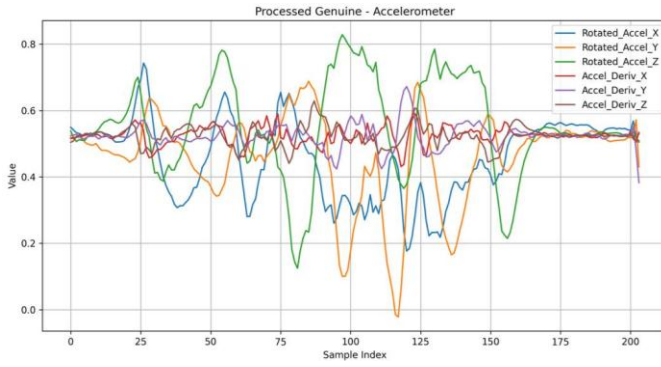


*Figure 9 Raw Genuine Orientation*

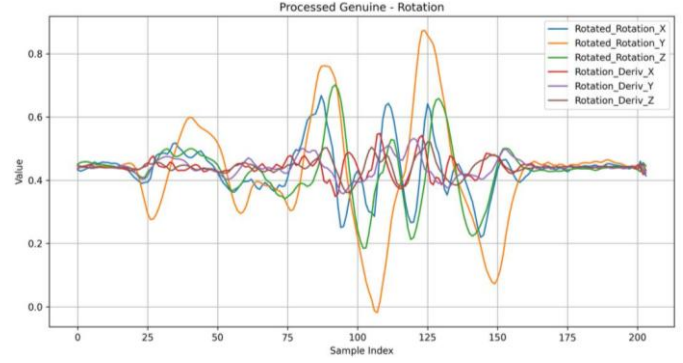


This is followed by **Figure 7**, **Figure 8** and **Figure 9** provides an analog visualization of the raw motion sensor readings ( accelerometer, rotation and orientation ) for one of the genuine signatures before the pre-processing step.

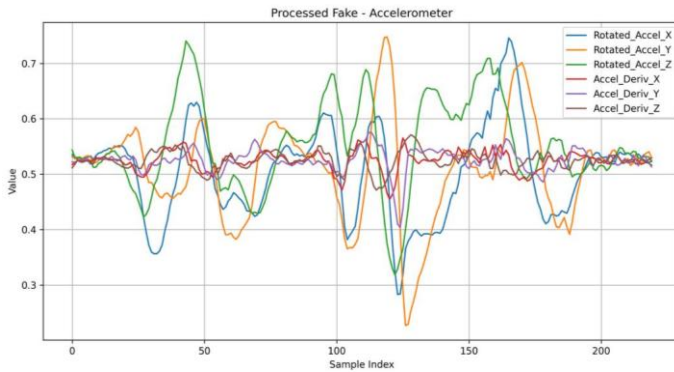
*Figure 10 Processed Genuine Accelerometer*



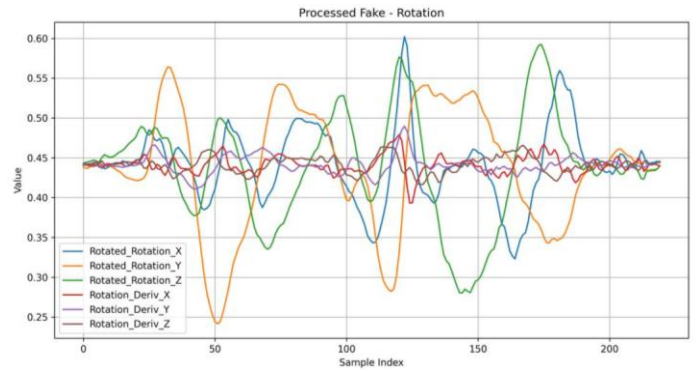
*Figure 11 Processed Genuine Rotation*



*Figure 12 Processed Fake Accelerometer*



*Figure 13 Processed Fake Rotation*



After completing the data collection process, we applied several preprocessing steps. **Figure 10** and **Figure 11** shows the analog visualization of the motion sensor readings after preprocessing, showing how the raw data was transformed into a structured format optimized for training the model.

While **Figure 12** and **Figure 13** presents the processed motion sensor readings Accelerometer and rotation signals respectively of the forged signature, highlighting the variations in movement patterns between genuine and forged signatures, offering insight into the distinguishing characteristics captured by the sensors.

These visual representations offer a comprehensive overview of the data collection and processing workflow. By showcasing both the raw and pre-processed sensor readings. This organized process ensure that the dataset is well-prepared for effective signature verification, enhancing the model's ability to distinguish between genuine and forged signatures with high accuracy.

With the data successfully collected and prepared, the next step in the next chapter involves designing the methodology for preprocessing, training, and evaluating the air signature recognition system based on the captured motion signals.

## 5. Methodology

This chapter details the methodology used to build our air signature recognition system, covering data preprocessing, then our BLSTM model design as shown in **Figure 14**. and the introduction to additional model CNN, Hybrid CNN-BLSTM, and ResNet. which are detailed further in Chapter 6., and lastly the training and evaluation process.

Building upon the collected data described in Chapter 4, we begin by detailing the preprocessing techniques applied to the raw motion data to prepare it for model input and analysis.

### 5.1 Pre-Processing Steps

Before feeding the raw three rotated Accelerometer readings ( $Accel_x, Accel_y, Accel_z$ ) and three rotated Rotation readings ( $Rotation_x, Rotation_y, Rotation_z$ ). that describe the motion sensor data into the model, several pre-processing steps are applied to ensure consistency, enhance feature quality, and prepare the data for effective learning, in this section we will discuss these steps:

### 5.1.1 Rotation

Rotation is applied to align the sensor data to a reference orientation. This step adjusts the three-axis Rotation and Accelerometer readings using the smartwatch's device attitude we extract along with the sensors data:

1. Rotate the object around its z-axis with angle Yaw.
2. Rotate the object around its new y-axis with angle Pitch.
3. Rotate the object around its new x-axis with angle Roll.

This is typically done using rotation matrices derived from the device's orientation. Aiming to eliminate variability caused by inconsistent signing orientations [3]. By adjusting the motion sensor data, the system improves the consistency of signature representation, essential for accurate authentication, after this step the data will be represented in 6 features, Three rotated Accelerometer readings ( $Accel_x, Accel_y, Accel_z$ ) and three rotated Rotation readings ( $Rotation_x, Rotation_y, Rotation_z$ ). the rotation step aligns the raw Accelerometer and Rotation data, but it doesn't introduce any additional derived features [3].

#### Rotation Formulas [16] :

To align motion signals in a consistent orientation, each raw sensor vector  $\mathbf{v}$  from (accelerometer or rotation readings) is rotated using a  $3 \times 3$  rotation matrix  $\mathbf{R}$ . This matrix is constructed from the device's attitude, its pitch (rotation around the x-axis), roll (y-axis), and yaw (z-axis):

$$\mathbf{R} = \mathbf{R}_{pitch} \cdot \mathbf{R}_{roll} \cdot \mathbf{R}_{yaw} \quad \text{Equation (1)}$$

The final rotated vector is computed by multiplying this matrix with the raw input vector:

$$[\mathbf{v}'_x, \mathbf{v}'_y, \mathbf{v}'_z] = \mathbf{R} \cdot [\mathbf{v}_x, \mathbf{v}_y, \mathbf{v}_z] \quad \text{Equation (2)}$$

This transformation ensures that all signature data is aligned in the same orientation, regardless of how the smartwatch was worn or how the user performed the gesture.

### 5.1.2 Differentiation

Because the changing rate of motion sensor readings can also contain discriminative information [3], we apply first-order differentiation on the rotated Rotation and Accelerometer data. This highlights the rate of change in motion, capturing the dynamics of speed and angular velocity during the signing process. The differentiated signals are then combined with the original rotated readings, enhancing the model's ability to distinguish between genuine and forged [2].

we applied first-order differentiation because it effectively captures the immediate rate of change in motion, which reflects key dynamics such as speed and angular velocity during the signature gesture. These features are particularly valuable for distinguishing between genuine and forged signatures. Higher-order derivatives, such as second-order differentiation (acceleration of acceleration), tend to amplify noise and can introduce instability in models trained on relatively small or noisy datasets.

After this step the data will be represented with 12 features which are ( $Accel_x, Accel_y, Accel_z, Rotation_x, Rotation_y, Rotation_z$ ) and the First-order differentiation of Accelerometer readings ( $Accel\_Driv_x, Accel\_Driv_y, Accel\_Driv_z$ ), lastly the First-order differentiation of Rotation readings ( $Rotation\_Driv_x, Rotation\_Driv_y, Rotation\_Driv_z$ )

#### Differentiation Formulas [28] :

With  $v_t$  represents the sensor value (Accelerometer or Rotation) at time  $t$ , the first-order differentiation (rate of change)  $\Delta v_t$  is calculated as:

$$\Delta v_t = \frac{v_t - v_{t-1}}{\Delta t} \quad \text{Equation (3)}$$

Where:

- $v_t$  : Sensor reading at time  $t$  .
- $v_{t-1}$  : Sensor reading at the previous time step.
- $\Delta t$  : Time difference between consecutive readings.



### 5.1.3 Normalization

Normalization ensures that all signatures have a consistent scale, irrespective of their size, this step helps fix differences caused by the lack of physical boundaries when signing in the air, such as varying signature scales. It ensures that every signature is standardized, making it easier to compare and analyze them [3]. By normalizing the data, we reduce the impact of large or small signature variations, improving the reliability and accuracy of the system. This step also doesn't introduce any additional derived features.

#### Normalization (Min-Max) Formulas [29] :

Normalization is applied to the raw motion data collected from the accelerometer and gyroscope sensors. Each individual sensor reading  $v$  is scaled using the minimum  $v_{min}$  and maximum  $v_{max}$  values observed for its corresponding axis (x, y, or z) across the dataset. This transformation ensures that all values lie within a standard range of 0 to 1, allowing motion patterns to be compared fairly across different signatures.

The Min-Max normalization formula is given by:

$$v' = \frac{v - v_{min}}{v_{max} - v_{min}} \quad \text{Equation (4)}$$

Where:

- $v$  : Original sensor reading (from either accelerometer or gyroscope)
- $v_{min}$  : Minimum value observed for that axis across the dataset
- $v_{max}$  : Maximum value observed for that axis across the dataset

This step is essential for improving model convergence during training and ensuring that features with different units or ranges do not dominate the learning process.

### 5.1.4 Pairing

The pairing process prepares the dataset for binary classification by generating labeled signature pairs. These include both genuine-genuine and genuine-forged combinations. Each pair is assigned a label indicating whether it represents a valid match or a forgery attempt. This step is essential for training the BLSTM model to distinguish between authentic and forged signatures based on temporal motion patterns [2].

More specifically, two genuine signatures from the same participant are paired and labeled as 1, representing a genuine match. In contrast, a genuine signature paired with a forged attempt of the same participant's signature is labeled as 0, representing a forgery. This binary labeling enables the model to learn discriminative features that characterize authentic signing behavior and identify inconsistencies typical of forgery attempts.

For each participant, 21 genuine-genuine pairs and 49 genuine-forged pairs are generated, resulting in a total of 70 labeled pairs per participant. These pairwise inputs are used during training and evaluation, allowing the BLSTM model to learn how the temporal dynamics of air signatures differ between true matches and imitations.

Each signature in the dataset consists of 12 pre-processed features. During the pairing step, the two signature samples are concatenated into a single input sequence. As a result, the final paired input contains 24 features per time step, 12 from the first signature and 12 from the second ensuring that the model receives full motion information from both inputs. These structured input sequences are saved in CSV format, with one row per time step and 24 columns representing the feature pair, followed by a label indicating whether the pair is a match (1) or a forgery (0).

This input structure allows the BLSTM to process both signatures simultaneously across time, enabling it to learn complex temporal relationships and subtle differences between matched and mismatched signature behavior.

Next, we introduce our first approach: the **Bidirectional Long Short-Term Memory (BLSTM)** model, as shown in **Figure 14**. We explain its architecture and how it leverages sequential motion data to differentiate between genuine and forged signatures.

Additional deep learning models explored in this study are introduced in **Chapter 6**, including:

- Second approach: The **Convolutional Neural Network (CNN)** model (**Figure 15**)
- Third approach: The **Hybrid CNN-BLSTM** model (**Figure 16**)
- Fourth approach: The **ResNet** model (**Figure 17**)

Each of these architectures investigates a different method of capturing spatial and temporal features from the motion signals for classification.

Figure 14 BLSTM Model Architecture

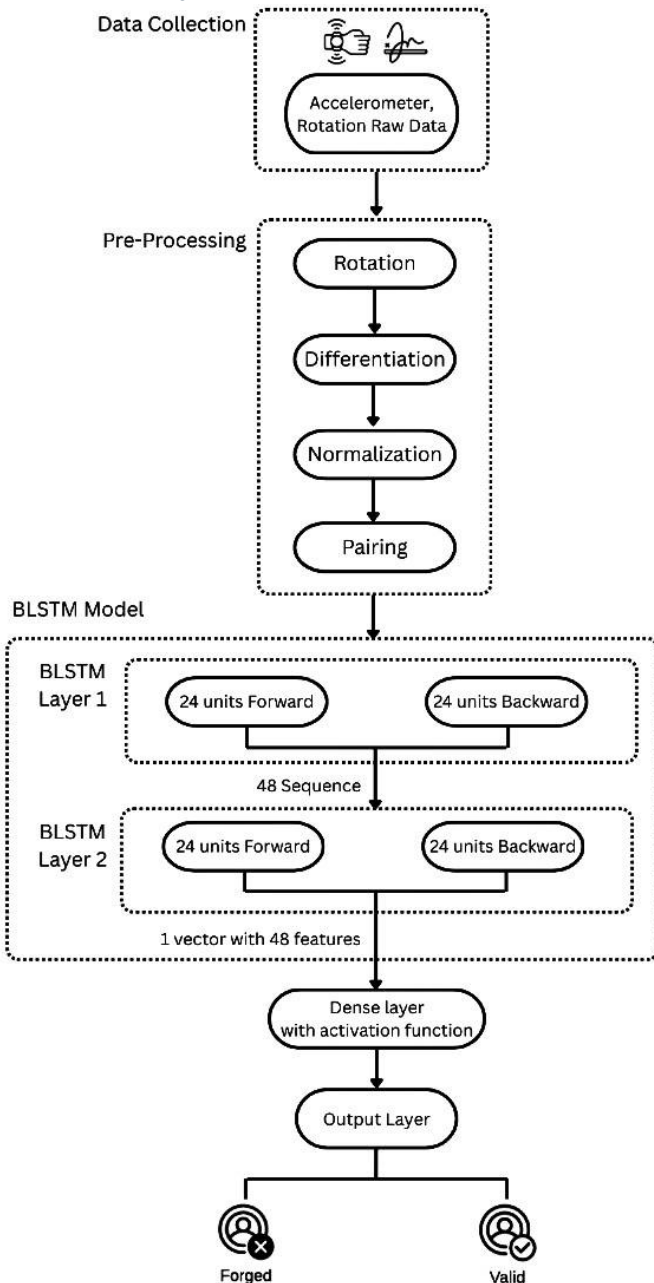


Figure 15 CNN Model Architecture

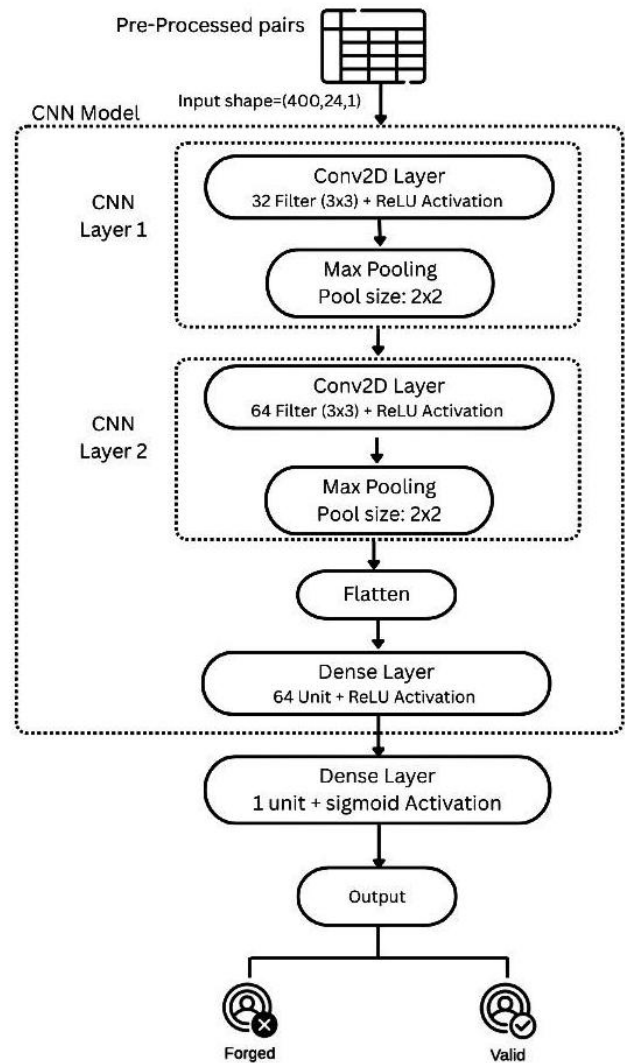


Figure 16 Hybrid CNN-BLSTM Model Architecture

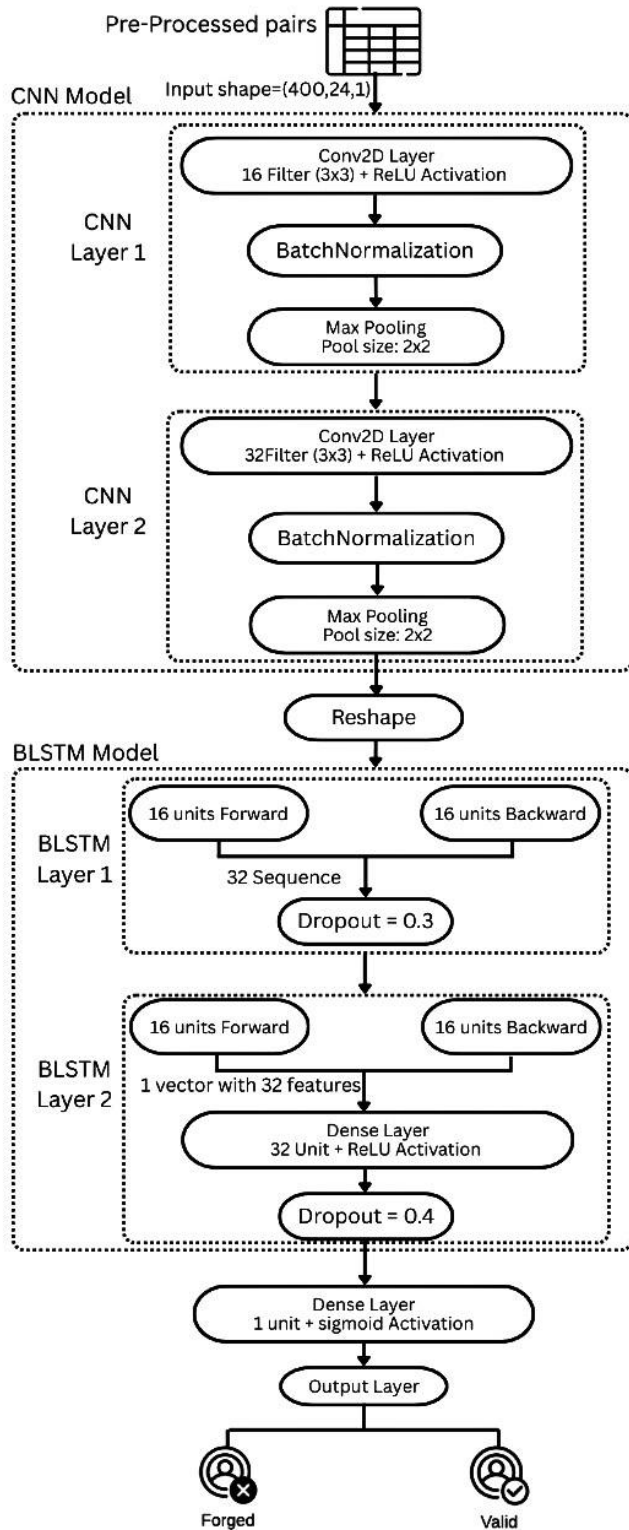
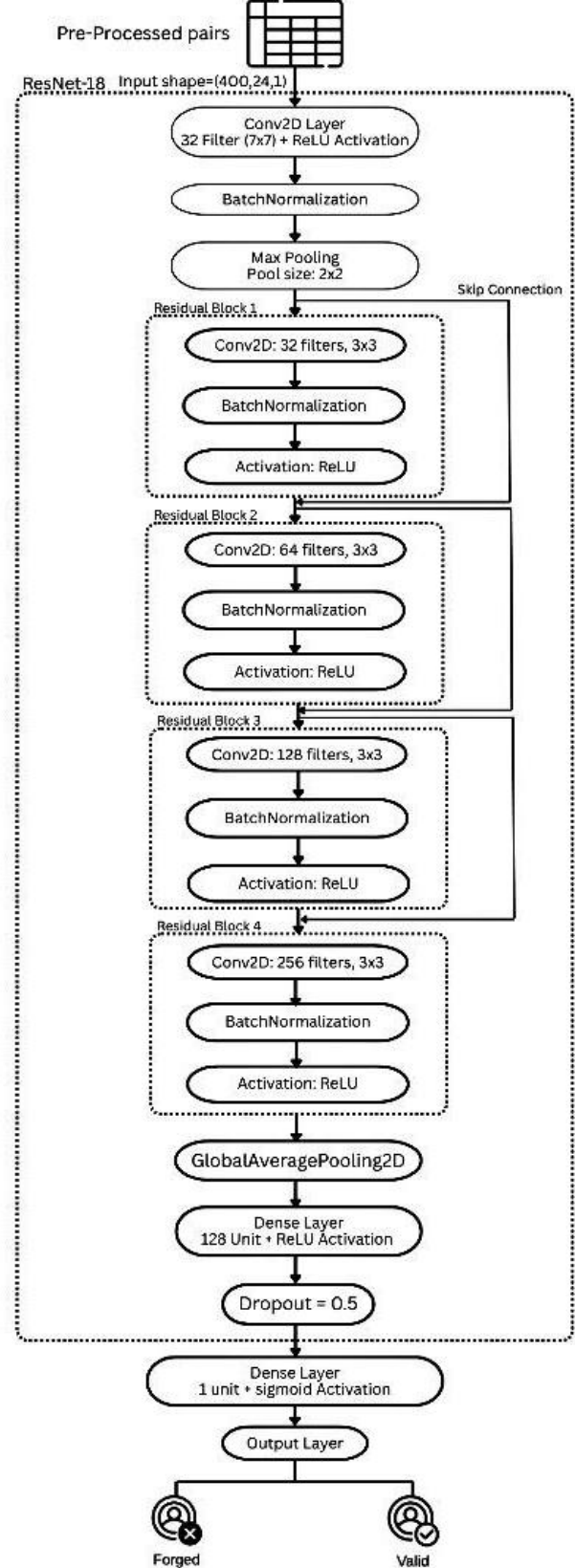


Figure 17 ResNet Model Architecture



## 5.2 BLSTM Model design

Once the motion data is collected and Pre-processed, the **Feature Extraction** process begins. This step focuses on analyzing the temporal and spatial characteristics of the recorded signals to identify distinctive patterns within the air signature. Using the **Bidirectional Long Short-Term Memory (BLSTM) model** in Figure 4, the system processes sequential motion data and captures critical dependencies, such as changes in velocity, direction, and orientation. The BLSTM's ability to learn temporal and spatial relationships enables it to extract unique motion features that are essential for accurate recognition and authentication [21].

### 5.2.1 Forward LSTM, Backward LSTM

The Bidirectional Long Short-Term Memory (BLSTM) model employed in this study is designed to capture temporal dependencies in the motion signals of air signatures. Unlike standard LSTM networks, a BLSTM processes the input sequence in both directions: forward (from the beginning to the end of the sequence) and backward (from the end to the beginning). The outputs of these two passes are integrated to provide a comprehensive representation of the sequence, leveraging both past and future dependencies [3]. This dual-directional processing allows the model to incorporate both past and future context at each time step, which is particularly valuable for distinguishing between subtle variations in signature patterns.

This bidirectional approach is highly beneficial for applications such as handwritten signature verification using smartwatch motion sensors, where the input consists of accelerometer and rotation data representing multi-dimensional, time-varying signals. In this context, BLSTMs process the variations in hand movement over time, detecting subtle differences in motion dynamics between genuine and forged signatures. The forward pass models the progression of the signature as it unfolds, while the backward pass captures concluding trends and overall structure, providing insights into how a signature might end and return to baseline movements [2].

The BLSTM model architecture consists of two stacked bidirectional LSTM layers, each with 24 memory units in both directions, which is appropriate for small to medium datasets [2]. The first BLSTM layer returns a sequence of hidden states, one for each time step, preserving the full temporal structure of the input. This sequence is then passed into the second BLSTM layer, which outputs a single fixed-length vector that summarizes the entire sequence. This vector represents a compressed encoding of the motion pattern and is used as the input to the subsequent dense layer for classification.

### 5.2.2 Dense Layer with Activation function

The fixed-length output vector produced by the final BLSTM layer is passed to a **dense (fully connected) layer**, which transforms the learned temporal features into a form suitable for classification. This vector serves as a compact representation of the motion dynamics captured from the input signature pair. The dense layer compute a weighted transformation of the input vector using the equation [22] :

$$\mathbf{z} = \mathbf{W} \cdot \mathbf{h} + \mathbf{b} \quad \text{Equation (5)}$$

Where:

- $\mathbf{h}$  : the output vector from the second Bidirectional LSTM layer
- $\mathbf{W}$  : the learned weight matrix of the dense layer
- $\mathbf{b}$  : the bias vector
- $\mathbf{z}$  : the input to the activation function

The weights and bias are learned during training to optimize classification performance. Once the logits ( $\mathbf{z}$ ) are computed, they are passed through an activation function to convert them into interpretable probabilities.

Since this study performs binary classification, we use the **Sigmoid** activation function to convert the computed logits ( $\mathbf{z}$ ) into a probability value between 0 and 1, as shown below [30] :

- For binary classification tasks, a **Sigmoid** function is used:

$$\text{Sigmoid}(\mathbf{z}) = \frac{1}{(1 + e^{-\mathbf{z}})} \quad \text{Equation (6)}$$

The output of the classifier is a probability that reflects the likelihood that the input pair represents a genuine signature match. This final step bridges the temporal features extracted by the BLSTM layers to the decision-making process, enabling the model to make accurate predictions based on the input motion sequence.

### 5.2.3 Output Layer

The output layer represents the final stage of the model, converting the logits ( $\mathbf{z}$ ) from the dense layer into final predictions, determining whether the input signature is genuine or forged. Using the **Sigmoid** activation function to produce a probability score from the dense layer's output [30] :

#### **Sigmoid Output :**

A decision threshold is set to interpret the sigmoid output [30] :

Output  $\geq 0.5$  : Classified as Valid Signature  
Output  $< 0.5$  : Classified as "Forged Signature"

This binary output enables the system to make accurate and interpretable decisions during authentication, supporting robust classification in real-time biometric verification.

## 5.3 Training and Evaluation Plan

The model was developed and optimized using the labeled data, which consists of both pairs of (genuine, genuine) with a label of 0 and (genuine, forged) is labeled as 1. The data is preprocessed into 12 feature vectors per signature before training. The dataset is divided into three subsets: **training (77%)**, **validation (9%)**, and **testing (14%)**. This split is designed to balance the need for sufficient training data to learn complex patterns, while preserving enough unseen data for reliable evaluation and tuning:

- **Training set (77%)**: The largest portion of data is allocated here to allow the model to effectively learn the distinguishing features of genuine and forged signatures. A larger training set helps the model generalize better by exposing it to diverse variations during learning.
- **Validation set (9%)**: A smaller, but representative, subset used during training to tune hyperparameters such as learning rate, optimizer choice, and regularization methods. This set helps prevent overfitting by allowing evaluation on unseen data during training iterations.
- **Testing set (14%)**: This final portion is kept completely separate and used only after training completes, providing an unbiased assessment of the model's generalization and performance on completely new data.

The choice of these percentages reflects common practices in machine learning, where typically 70-80% of data is used for training, 10-15% for validation, and the remainder for testing. The exact split can vary depending on the dataset size and application but is tuned here to maximize both model performance and reliable evaluation.

### 5.3.1 Training

During the training phase, we tested different combinations of loss functions, optimizers, and hyperparameter settings to find the best configuration for our air signature recognition models. This process was done in an iterative way, where adjustments were made based on validation results to improve accuracy and efficiency.

Since air signature sequences can have different lengths, we used zero-padding to standardize the input sequences for all models. This helped ensure that the models processed the data in a consistent format while retaining important temporal information. The models were trained using the augmented dataset, which expanded the original 1,680 samples to 5,040 by applying techniques like controlled noise and smoothing. This allowed the models to learn from a wider variety of signature patterns, improving their ability to generalize to real-world scenarios.

### 5.3.2 Testing & Evaluation

After training, the model will be evaluated on the unseen test set. This test set contains data that the model has not encountered during training or validation, This evaluation assesses the model's generalization capability and its ability to accurately classify new, previously unobserved data.

#### Evaluation Metrics

The model's performance will be assessed using the following metrics [33] :

- **Accuracy:** The overall proportion of correctly classified samples.
- **Precision:** The proportion of predicted positive cases (genuine pairs) that are actually correct.
- **Recall (Sensitivity):** The proportion of actual positive cases that are correctly identified by the model.
- **F1 Score:** The harmonic mean of precision and recall, useful when evaluating class imbalance.
- **False Acceptance Rate (FAR):** The rate at which forged signatures are incorrectly accepted as genuine.
- **False Rejection Rate (FRR):** The rate at which genuine signatures are incorrectly rejected as forgeries.

The **equations** for the performance's metrics [33] :

$$F1\ Score = 2 \cdot \frac{Precision \cdot Recall}{Precision + Recall} \quad \text{Equation (11)}$$

$$False\ Acceptance\ Rate\ (FAR) = \frac{Number\ of\ False\ Acceptances}{Total\ Number\ of\ Negative\ Class\ Samples} \quad \text{Equation (12)}$$

- **False Acceptances** are when the system classifies a forged signature as valid.
- **Total Negative Class Samples** are the total number of forged signatures in the test set.

$$False\ Rejection\ Rate\ (FRR) = \frac{Number\ of\ False\ Rejections}{Total\ Number\ of\ Positive\ Class\ Samples} \quad \text{Equation (13)}$$

- **False Rejections** are when the system classifies a valid signature as forged.
- **Total Positive Class Samples** are the total number of genuine signatures in the test set.



## 6. Experimental Design

This chapter explains how the experiments were designed and carried out to evaluate the air signature authentication system. The main goal of the experiments is to verify whether the system can accurately distinguish between genuine and forged air signatures by analyzing motion data captured from a smartwatch. The independent variable in the experiments is the type of signature whether it is real or fake, while the dependent variables include the system's performance metrics such as accuracy and error rates. To ensure the reliability and fairness of the results, the collected data was randomly divided into training, validation, and test sets, and preprocessed to minimize variability caused by differences in wrist movement or device positioning. Various deep learning models were tested, including BLSTM, CNN, hybrid CNN-BLSTM, and ResNet architectures, alongside data augmentation techniques that introduce realistic variations to enhance model generalization.

This chapter is organized into four main parts: the experimental hypotheses, the experimental setup including tools and configurations, a breakdown of the different experiments conducted, and a discussion of the results.

### 6.1 Hypotheses

The experimental phase of this research is guided by the following hypotheses, each aimed at validating key aspects of the proposed air signature authentication system. These hypotheses are designed to explore the causal relationship between the type of signature input (independent variable) and the authentication performance of the model (dependent variable).

- **Signature Distinguishability:**  
Smartwatch motion sensor data (accelerometer and rotation) can effectively distinguish between genuine and forged air signatures based on their motion patterns.
- **Linguistic-Specific Characteristics:**  
Arabic air signatures exhibit unique biomechanical and spatial-motion features that make them suitable for use in biometric authentication systems.
- **Model Robustness:**  
A deep learning model trained on smartwatch motion data can achieve high classification accuracy and low error rates (EER, FAR, FRR), even in the presence of inter-user variability and forgery attempts.

These hypotheses is the foundation for the experiments and will be tested using a randomized, balanced dataset and performance evaluation metrics. The results will determine the model's reliability, efficiency, and its applicability to Arabic air signature authentication.

## 6.2 Experimental Setup

The experimental setup is designed to evaluate the effectiveness of the proposed air signature authentication system using a custom-collected dataset. The goal is to determine how variations in motion data that are captured during genuine and forged air signatures impact the authentication accuracy of the model.

In this study:

- The **independent variable** is the type of signature (genuine or forged).
- The **dependent variables** are the model's performance metrics, including accuracy, Equal Error Rate (EER), False Acceptance Rate (FAR), and False Rejection Rate (FRR).
- **Nuisance variables**, such as variations in participant signing styles, wrist movement inconsistencies, and device orientation, were addressed through preprocessing steps such as rotation alignment, differentiation, and normalization.

To ensure unbiased evaluation, randomization was applied when splitting the dataset. Signatures were randomly divided into **training (77%)**, **validation (9%)**, and **testing (14%)** subsets using scikit-learn's `train_test_split` function, with stratification based on signature label (genuine or forged) to maintain class balance.

The model architecture used in this study is a **Bidirectional Long Short-Term Memory (BLSTM)** network, which is well-suited for analyzing sequential motion data. A temporal average pooling layer is applied to the BLSTM outputs to produce a fixed-length feature vector. This is followed by a dense layer and an activation function for binary classification.

The implementation was carried out using **Python**, with **NumPy** and **Pandas** used for data preprocessing, and **TensorFlow** and **PyTorch** used to define and train the deep learning model.

To enhance generalizability and reduce overfitting, **data augmentation techniques** were explored which add slight noise or rotate the signals within realistic bounds. The system's final performance was evaluated using the specified metrics to assess its real-world viability for biometric authentication.

## 6.3 Experiments

To evaluate the performance and robustness of different deep learning models for air signature recognition, a series of experiments were conducted using the collected smartwatch motion data. These experiments are designed to compare multiple architectures and assess the impact of data augmentation techniques, which included adding controlled Gaussian noise and smoothing to simulate real-world variations in signing behavior on model performance. The original dataset had 1,680 air signature samples. To help the models learn better and handle different signing styles, we used data augmentation to increase the dataset size to 5,040 samples. This means we created extra samples by making small changes to the original data, like rotating the motions a little or adding slight variations. We used this bigger, augmented dataset with all the models we tested BLSTM, CNN, the hybrid CNN-BLSTM, and ResNet, so they could perform better and be more reliable at telling real signatures from fake ones.

Specifically, the experiments include a BLSTM model, a CNN-based model to observe how spatial feature learning responds to augmentation. A hybrid approach combining CNN and BLSTM is also tested to examine whether combining spatial and temporal modeling improves classification accuracy. Finally, a ResNet-based model is evaluated to explore the benefits of deep residual learning in this context. All models are trained and evaluated under consistent conditions using the same dataset splits, performance metrics, preprocessing pipeline, and a sigmoid activation function in the output layer to ensure fairness and enable meaningful comparisons.

### 6.3.1 Experiment 1: BLSTM Model

In the first experiment of this study, we tested a model built using a Bidirectional Long Short-Term Memory (BLSTM) architecture to classify pairs of air signatures as either genuine or forged. BLSTM is a type of Recurrent Neural Network (RNN) that is particularly good at working with time-series data because it can remember patterns over time. By processing data in both forward and backward directions, the BLSTM is able to pick up on dependencies in the signature that might happen at different points in time, which is especially useful for modeling handwriting movements.

Our BLSTM model had two stacked bidirectional LSTM layers, each with 24 units. The first layer outputs a sequence of hidden states, while the second layer condenses this into a single vector that summarizes the whole motion pattern. After that, a dense layer with a sigmoid activation function was used to classify the signature pair as genuine or forged. This design allows the model to learn both long-term patterns and small variations in the motion data, making it effective at telling apart real and fake signatures.

#### BLSTM With Augmentation:

The BLSTM model trained with augmented data achieved strong performance across all evaluation metrics (**Table 4**). It reached an accuracy of 97.73%, with precision and F1 Score both at 97.73%, indicating reliable and balanced classification of both genuine and forged signatures. The False Rejection Rate (FRR) was 4.25%, reflecting the model's effectiveness in correctly accepting genuine signatures, while the False Acceptance Rate (FAR) remained low at 1.42%, demonstrating strong resistance to forgery. These results show that the BLSTM architecture, when trained on a diverse and enriched dataset, is well-suited for capturing temporal motion dynamics in air signature verification and provides a robust foundation for motion-based biometric authentication.

Table 4 BLSTM with Augmentation

BLSTM	With Augmentation
Accuracy	0.9773
Precision	0.9773
F1 Score	0.9773
FAR	0.0142
FRR	0.0425

### 6.3.2 Experiment 2: CNN Model

The Convolutional Neural Network (CNN) used in our signature verification project processes each signature as a matrix with 400 time steps and 24 features that represent motion sensor data from a smartwatch. This (400, 24) matrix is reshaped to (400, 24, 1) to match the input format expected by CNNs, similar to a grayscale image with a single channel. Through a series of convolutional and pooling layers, the network learns spatial patterns across both the time and feature dimensions. These patterns represent unique aspects of the user's writing dynamics, enabling the model to distinguish between genuine and forged signatures. The output from the final convolutional layer is flattened and passed through fully connected layers, ending with a sigmoid function to classifies the input as either a forged (label = 0) or a genuine (label = 1) signature. To enhance model generalization and reduce overfitting, data augmentation techniques were later applied. This involved artificially expanding the training dataset by introducing minor variations to the original signals, effectively doubling the number of training samples. By exposing the CNN to a wider range of signature variations, the model became more robust in distinguishing between genuine and forged inputs, even when faced with subtle inconsistencies in previously unseen data.

#### CNN With Augmentation:

The CNN model trained with augmented data achieved outstanding performance across all evaluation metrics (**Table 5**). It recorded an accuracy of 99.86% and a near-perfect F1 Score of 99.76%, indicating excellent balance and confidence in distinguishing between genuine and forged signatures. Precision reached 99.53%, showing that nearly all predicted genuine signatures were correctly classified, as a result minimizing the risk of falsely accepting forgeries. Notably, the False Rejection Rate (FRR) was 0%, meaning the model successfully accepted all genuine signatures. Meanwhile, the False Acceptance Rate (FAR) was just 0.20%, reflecting the model's strong resistance to forgery. These results highlight the CNN's robustness and reliability in handling signature variability, making it a highly effective solution for motion-based biometric authentication using smartwatch data.

*Table 5 CNN with Augmentation*

CNN	With Augmentation
Accuracy	0.9986
Precision	0.9953
F1 Score	0.9976
FAR	0.002
FRR	0

### 6.3.3 Experiment 3: Hybrid CNN-BLSTM Model

In this experiment, a hybrid model was developed to combine the spatial feature extraction capabilities of Convolutional Neural Networks (CNN) with the temporal modeling strengths of Bidirectional Long Short-Term Memory (BLSTM) networks. The architecture began with two CNN layers containing 32 and 64 filters, respectively, applied to the input motion data. After extracting local spatial features, the output was reshaped and passed through two stacked BLSTM layers to capture sequential patterns in the user's air signature dynamics. This initial version of the hybrid model did not employ any regularization techniques such as Batch Normalization or Dropout, which limited its ability to generalize.

#### Basic Hybrid Architecture

The performance of this basic hybrid architecture (**Table 6**) was suboptimal. The model achieved an accuracy of 83.85%, with a precision of 78.16% and an F1 Score of 70.47%, indicating that it struggled to maintain a balanced classification of both genuine and forged signatures. Most notably, the False Rejection Rate (FRR) was high at 35.85%, meaning over one-third of genuine signatures were incorrectly rejected. The False Acceptance Rate (FAR) stood at 7.69%, further reflecting the model's vulnerability to forgery. These results suggest that, while the combination of CNN and BLSTM has potential, the model suffered from overfitting and lacked mechanisms to stabilize training or control feature learning.

Table 6 Basic Hybrid Architecture

Basic Hybrid	
Accuracy	0.8385
Precision	0.7816
F1 Score	0.7047
FAR	0.0769
FRR	0.3585

#### Optimized Hybrid Architecture

To address these issues, a simplified and optimized version of the hybrid model was implemented. The number of CNN filters was reduced to 16 and 32, and the BLSTM units decreased from 24 to 16 in each direction to lower the model complexity. In addition, Batch Normalization was introduced after each CNN layer to stabilize learning, and Dropout was added between the BLSTM layers to improve generalization. Batch Normalization standardizes the outputs of layers to speed up and stabilize training, while Dropout randomly deactivates neurons during training to prevent overfitting.

Table 7 Optimized Hybrid Architecture

Optimized Hybrid	
Accuracy	0.9788
Precision	0.9805
F1 Score	0.964
FAR	0.0081
FRR	0.0519

These architectural refinements led to a substantial improvement in model performance. The optimized hybrid model (**Table 7**) achieved an accuracy of 97.88%, precision of 98.05%, and an F1 Score of 96.40%, while the FRR dropped to 5.19% and FAR to 0.81%. These results demonstrate that targeted simplification and regularization significantly enhance the hybrid model's ability to accurately classify air signatures and resist overfitting, making it a more viable candidate for real-world biometric authentication systems.

### 6.3.4 Experiment 4: ResNet Model

In this experiment, a simplified version of the **ResNet-18 architecture** was adapted for the air signature verification task. ResNet (Residual Network) is a type of deep convolutional neural network that uses **residual blocks** with shortcut connections to address the vanishing gradient problem common in deep models. These skip connections enable more effective gradient flow and allow the network to learn deeper, more abstract representations without degradation in performance.

The customized ResNet-18 model used in this project begins with a convolutional layer, followed by four residual blocks with increasing filter sizes. Each block allows the model to capture both low-level and high-level spatial features from the motion signals. After the final residual block, global average pooling is applied to reduce dimensionality while preserving the most important spatial information. The pooled features are then passed through a fully connected dense layer with a sigmoid activation function to perform binary classification, predicting whether the input signature pair is genuine (label = 1) or forged (label = 0).

The ResNet model (**Table 8**) demonstrated strong generalization capabilities. It achieved an accuracy of 97.62%, precision of 97.60%, and an F1 Score of 95.96%, indicating reliable performance in distinguishing between genuine and forged signatures. The False Rejection Rate (FRR) was 5.63%, showing moderate sensitivity to genuine signature variability, while the False Acceptance Rate (FAR) was low at 0.99%, reflecting strong resistance to forgery. These results highlight the effectiveness of deep residual learning in capturing complex spatial patterns, making ResNet a robust and competitive architecture for motion-based biometric authentication in wearable systems.

Table 8 ResNet Model

ResNet	
Accuracy	0.9762
Precision	0.976
F1 Score	0.9596
FAR	0.0099
FRR	0.0563

## 7. Result and Discussion

To evaluate the effectiveness of air signature recognition using smartwatch motion data, based on the four main experiments shown in **Table 9** using different deep learning architectures: BLSTM, CNN, a Hybrid CNN-BLSTM model, and a ResNet variant. Each experiment aimed to classify genuine and forged signature pairs and assess model robustness, accuracy, and forgery resistance.

The evaluation focused on accuracy, precision, recall, F1 Score, False Acceptance Rate (FAR), and False Rejection Rate (FRR), providing a comprehensive assessment of each model's performance and robustness.

*Table 9 Experiments Result*

Model	Accuracy	Precision	F1 Score	FAR	FRR
BLSTM	97.73%	97.73%	97.73%	1.42%	4.25%
CNN	99.86%	99.53%	99.76%	0.20%	0%
Hybrid (Basic)	83.85%	78.16%	70.47%	7.69%	35.85%
Hybrid (Optimized)	97.88%	98.05%	96.40%	0.81%	5.19%
ResNet	97.62%	97.60%	95.96%	0.99%	5.63%

### 7.1 Performance Comparison of Models

The performance of the four tested models reveals key differences in how each architecture handles the classification of genuine versus forged air signatures. While all models showed competency in motion-based biometric authentication, their effectiveness varied across different evaluation metrics, especially in their sensitivity to forgery (FAR) and genuine signature variability (FRR).

The **CNN model** consistently outperformed all others, achieving the **highest accuracy (99.86%)** and **perfect FRR (0.00%)**, making it the most reliable in recognizing genuine signatures without introducing user frustration. Its **low FAR (0.20%)** also demonstrated strong resistance to forgeries. These results highlight CNN's strength in learning spatial patterns from motion data and confirm that data augmentation substantially boosts generalization.

The **BLSTM model**, trained on augmented data, demonstrated strong performance in air signature classification. It achieved an **accuracy of 97.73%**, The **FRR was 4.25%** showing the model's ability to accurately accept legitimate signatures, while the **FAR remained low at 1.42%**, Maintaining robustness against forgery. These results confirm the BLSTM's effectiveness in capturing temporal dynamics in motion signals when trained on a diverse dataset, and highlight its suitability for real-time, sequential biometric authentication.

The **optimized Hybrid CNN-BLSTM model** narrowed the performance gap, achieving **97.88% accuracy** and reducing **FRR to 5.19%**, with a strong **FAR (0.81%)**. This suggests that combining CNN's spatial learning with BLSTM's temporal modeling can provide a robust solution when properly regularized. However, because this model is more complex and



requires more tuning, it may not be the most efficient choice unless the extra accuracy is absolutely needed.

Finally, the **ResNet-based model** performed competitively **97.62% accuracy**, benefiting from deep residual learning for complex pattern extraction. Its **FAR was low at 0.99%**, reflecting strong resistance to forgeries, while its **FRR was 5.63%**, showing moderate sensitivity to genuine signature variation. These results suggest that ResNet is a reliable option for spatial pattern recognition, though its performance can be affected by intra-class variability in genuine signatures.

**In summary:**

- **CNN** leads in overall accuracy, precision, and real-world reliability.
- **BLSTM** shows strong temporal pattern recognition and performs effectively when trained on diverse, augmented data, demonstrating reliable classification in motion-based authentication.
- **Hybrid CNN-BLSTM** offers balanced performance when optimized, effectively combining spatial and temporal features.
- **ResNet** demonstrates strong generalization and forgery resistance, though it is slightly more sensitive to genuine signature variation.

## **7.2 Discussion of Augmentation and Robustness**

Across all models, data augmentation consistently improved performance, especially in reducing the FRR. This is critical in biometric systems, where false rejection of legitimate users can degrade user experience. The augmented CNN model, in particular, exhibited exceptional robustness, achieving near-perfect classification with minimal error rates. The results support the hypothesis that data augmentation enhances the model's ability to generalize to unseen variations in signing behavior, making the system more reliable in real-world applications.

Furthermore, the experiments validate the design and preprocessing pipeline used in this research. The combination of rotation alignment, differentiation, normalization, and pairing prepared the data in a way that allowed each model to capture meaningful motion patterns. This confirms that smartwatch motion sensors can reliably differentiate between genuine and forged air signatures when paired with suitable deep learning architectures.

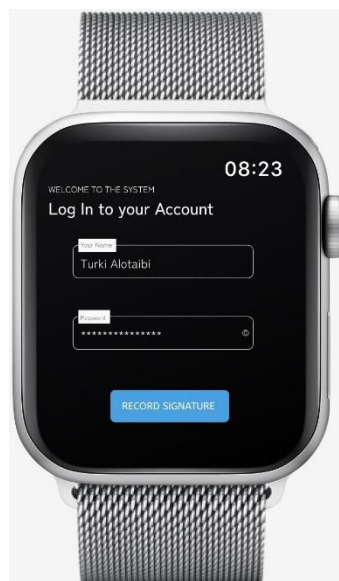
## 8. Applications of The Model

To demonstrate the practical implementation of our air signature verification system, we developed a series of smartwatch interface prototypes that simulate a real-time user authentication flow. These interfaces represent how the trained model can be integrated into a functional, user-friendly application for everyday identity verification.

### Scenario: Air Signature Authentication via Smartwatch

In this system, air signature verification is used as an additional security layer alongside traditional login credentials (name and password), providing a multi-factor authentication mechanism. The following outlines a typical user interaction flow within the application, starting with the initial registration process:

#### 1. Signature Enrollment



*Figure 18 Interface 1*

During the initial setup, using our interface (**interface 1**) the user is asked to log in to their Account using their name and their password they use in the organization system, Then asked to perform several genuine air signatures in the smartwatch. The system then pre-processes the recorded signatures and stores them securely as reference for future authentication.

## 2. User Login Interface



Figure 19 Interface 2

Upon launching the app, the user is presented with a login screen (**interface 2**) to enter their name and password. This step acts as the first layer of authentication before activating biometric verification.

## 3. Signature Capture



Figure 20 Interface 3



Figure 21 Interface 4

After successful login, the user is prompted to perform an air signature as a second verification step. By tapping the “Start Recording” button (**interface 3**), the smartwatch begins capturing motion data using its accelerometer and rotation sensors. The user performs their signature in the air, then tap the “Stop Recording” button (**interface 4**) the system will save the captured signature.

#### 4. Verifying the signature



Figure 22 Interface 5

The system processes the captured signature data and compares it to the registered signature stored in the registration phase using the trained model (**interface 5**).

#### 5. Verification Result



Figure 23 Interface 6



Figure 24 Interface 7

##### - Accepted

If the signature is verified as genuine, the user is granted access to the system (**interface 6**)

##### -Rejected

If the signature is verified as forged, the user access to the system is denied (**interface 7**)

## 9. Conclusion & Future Work

### 9.1 Conclusion

This research presents a novel and practical approach to biometric authentication through the development of an air signature recognition system using smartwatch motion sensors. By leveraging the accelerometer and rotation data available in modern smartwatches, the system captures the dynamic and unique patterns of users' in-air handwritten signatures, enabling secure, contactless, and portable identity verification.

Throughout the study, we addressed critical challenges in motion variability, forgery detection, and small dataset limitations. The data collection process involved 24 participants generating both genuine and forged Arabic-language signatures, contributing to the development of a more inclusive and language-diverse biometric system. Preprocessing techniques, such as rotation alignment, differentiation, and normalization were essential to standardizing motion data and improving feature quality.

Several deep learning models were implemented and evaluated, including four main approaches: BLSTM, CNN, Hybrid CNN-BLSTM, and ResNet architectures. Among them, the CNN model with data augmentation achieved the highest performance, recording an accuracy of 99.86% and a perfect False Rejection Rate (FRR) of 0.00%, confirming its robustness in distinguishing between authentic and forged signatures. While strong in sequence learning, the BLSTM model was sensitive to the natural variation across genuine signatures. Lastly, The Hybrid and ResNet models also performed strongly, combining spatial-temporal learning and deep feature extraction.

The results validate the potential of smartwatch-based air signature recognition as a reliable alternative to traditional biometric systems. Compared to camera-based or specialized hardware solutions, making it highly applicable in real-world scenarios such as banking, healthcare, and secure mobile authentication.

Finally, this project contributes to advancing wearable biometric authentication by focusing on Arabic signature and leveraging widely accessible devices. It lays a strong foundation for future exploration into cross-platform adaptability, enhanced explainability, and larger dataset inclusion.

## 9.2 Future work

As future works, to further enhance the system's performance and real-world applicability, several improvements are proposed:

### **Larger and More Diverse Dataset**

Expanding the dataset with more participants of varying demographics and signature styles will improve the model's generalization and reduce overfitting [2] [3].

### **Explainable AI (XAI)**

Incorporating explainability techniques, Can help reveal which temporal or spatial patterns the model relies on, improving transparency and user trust in biometric systems [23].

### **Optimization Techniques**

To improve training efficiency and model generalization, future work can explore early stopping and hyperparameter tuning Which help identify the best model configurations, while early stopping prevents overfitting by halting training once validation performance plateaus. These strategies can reduce computation time and improve reliability, especially for real-time systems [27].

### **Smartwatch Application Development**

Building a full smartwatch application that handles real-time data acquisition, preprocessing, and inference will enable standalone authentication without external systems.

### **Cross-Device and Cross-Platform Robustness**

Future systems must ensure consistent performance across various smartwatch brands and models. Cross-device variability significantly impacts accuracy [26], Which highlights the need to teach the model how to adapt to different devices.

## References

- [1] R. Plamondon and S. N. Srihari, "On-Line and Off-Line Handwriting Recognition: A Comprehensive Survey," 2000.
- [2] G. Li and H. Sato, "Handwritten Signature Authentication Using Smartwatch Motion Sensors," in *Proceedings - 2020 IEEE 44th Annual Computers, Software, and Applications Conference, COMPSAC 2020*, Institute of Electrical and Electronics Engineers Inc., Jul. 2020, pp. 1589–1596. doi: 10.1109/COMPSAC48688.2020.00-28.
- [3] G. Li and H. Sato, "Sensing In-Air Signature Motions Using Smartwatch: A High-Precision Approach of Behavioral Authentication," *IEEE Access*, vol. 10, pp. 57865–57879, 2022, doi: 10.1109/ACCESS.2022.3177905.
- [4] K. Dharavath, F. A. Talukdar, and R. H. Laskar, "Study on biometric authentication systems, challenges and future trends: A review," in *2013 IEEE International Conference on Computational Intelligence and Computing Research, IEEE ICCIC 2013*, IEEE Computer Society, 2013. doi: 10.1109/ICCIC.2013.6724278.
- [5] Y. Shao, T. Yang, H. Wang, and J. Ma, "Airsig: Smartphone authentication by signing in the air," *Sensors (Switzerland)*, vol. 21, no. 1, pp. 1–24, Jan. 2021, doi: 10.3390/s21010104.
- [6] P. Sarveswarasarma, T. Sathulakjan, V. J. V. Godfrey, and T. D. Ambegoda, "Air Signing and Privacy-Preserving Signature Verification for Digital Documents," May 2024, [Online]. Available: <http://arxiv.org/abs/2405.10868>
- [7] Y. Guo and H. Sato, "Smartwatch In-Air Signature Time Sequence Three-Dimensional Static Restoration Classification Based on Multiple Convolutional Neural Networks," *Applied Sciences (Switzerland)*, vol. 13, no. 6, Mar. 2023, doi: 10.3390/app13063958.
- [8] J. Malik, A. Elhayek, S. Guha, S. Ahmed, A. Gillani, and D. Stricker, "Deepairsig: End-to-end deep learning based in-air signature verification," *IEEE Access*, vol. 8, pp. 195832–195843, 2020, doi: 10.1109/ACCESS.2020.3033848.
- [9] H. Nagashima and Y. Kato, "APREP-DM: a Framework for Automating the Pre-Processing of a Sensor Data Analysis based on CRISP-DM," Institute of Electrical and Electronics Engineers, 2019, p. 6.
- [10] J. Jung, H. C. Moon, J. Kim, D. Kim, and K. A. Toh, "Wi-Fi Based User Identification Using In-Air Handwritten Signature," *IEEE Access*, vol. 9, pp. 53548–53565, 2021, doi: 10.1109/ACCESS.2021.3071228.
- [11] A. Jain, P. Flynn, and A. Ross, *Handbook of Biometrics*. Springer, 2008. doi: 10.1007/978-0-387-71041-9.
- [12] M. Dadafshar, "Accelerometer and Gyroscopes Sensors: Operation, Sensing, and Applications."
- [13] Z. Deng, L. Huang, and C. Wang, "Enhanced In-air Signature Verification via Hand Skeleton Tracking to Defeat Robot-level Replays," in *ACM International Conference Proceeding Series*, Association for Computing Machinery, Dec. 2023, pp. 451–462. doi: 10.1145/3627106.3627195.
- [14] A. K. Jain, F. D. Griess, and S. D. Connell, "On-line signature verification," 2002. [Online]. Available: [www.elsevier.com](http://www.elsevier.com)
- [15] R. Sabourin, G. Genest, and F. J. Prêteux, "Off-Line Signature Verification by Local Granulometric Size Distributions," 1997.
- [16] A. Janota, V. Šimák, D. Nemec, and J. Hrbček, "Improving the precision and speed of Euler angles computation from low-cost rotation sensor data," *Sensors (Switzerland)*, vol. 15, no. 3, pp. 7016–7039, 2015, doi: 10.3390/s150307016.
- [17] Y. Lou, H. Ao, and Y. Dong, "Improvement of Dynamic Time Warping (DTW) algorithm," in *Proceedings - 14th International Symposium on Distributed Computing*

- and Applications for Business, Engineering and Science, DCABES 2015, Institute of Electrical and Electronics Engineers Inc., Mar. 2016, pp. 384–387. doi: 10.1109/DCABES.2015.103.
- [18] M. J. T. Reinders, E. Hendriks, G. A. Ten Holt, M. J. T. Reinders, and E. A. Hendriks, “Multi-dimensional dynamic time warping for gesture recognition,” 2007. [Online]. Available: <https://www.researchgate.net/publication/228740947>
  - [19] Y. Lecun, Y. Bengio, and G. Hinton, “Deep learning,” May 27, 2015, *Nature Publishing Group*. doi: 10.1038/nature14539.
  - [20] J. A. P. Lopes, B. Baptista, N. Lavado, and M. Mendes, “Offline Handwritten Signature Verification Using Deep Neural Networks,” *Energies (Basel)*, vol. 15, no. 20, Oct. 2022, doi: 10.3390/en15207611.
  - [21] N. Hassan, A. S. M. Miah, and J. Shin, “A Deep Bidirectional LSTM Model Enhanced by Transfer-Learning-Based Feature Extraction for Dynamic Human Activity Recognition,” *Applied Sciences (Switzerland)*, vol. 14, no. 2, Jan. 2024, doi: 10.3390/app14020603.
  - [22] I. Goodfellow, A. Courville, and Y. Bengio, “Deep Learning,” MIT Press. Accessed: Nov. 26, 2024. [Online]. Available: <https://www.deeplearningbook.org/>
  - [23] H. H. Kao and C. Y. Wen, “An offline signature verification and forgery detection method based on a single known sample and an explainable deep learning approach,” *Applied Sciences (Switzerland)*, vol. 10, no. 11, Jun. 2020, doi: 10.3390/app10113716.
  - [24] J. Malik, A. Elhayek, S. Ahmed, F. Shafait, M. I. Malik, and D. Stricker, “3DAirSig: A framework for enabling in-air signatures using a multi-modal depth sensor,” *Sensors (Switzerland)*, vol. 18, no. 11, Nov. 2018, doi: 10.3390/s18113872.
  - [25] A. Levy, B. Nassi, Y. Elovici, and E. Shmueli, “Handwritten Signature Verification Using Wrist-Worn Devices,” *Proc ACM Interact Mob Wearable Ubiquitous Technol*, vol. 2, no. 3, pp. 1–26, Sep. 2018, doi: 10.1145/3264929.
  - [26] R. Ramachandra, S. Venkatesh, K. Raja, and C. Busch, “Handwritten signature and text based user verification using smartwatch,” in *Proceedings - International Conference on Pattern Recognition*, Institute of Electrical and Electronics Engineers Inc., 2020, pp. 5099–5106. doi: 10.1109/ICPR48806.2021.9412048.
  - [27] A. Lim, F. Chuen, K. Wee How, Y. Han, and Y. H. Yen, “In-Air Hand Gesture Signature Recognition Using Multi-Scale Convolutional Neural Networks.” [Online]. Available: [www.joiv.org/index.php/joiv](http://www.joiv.org/index.php/joiv)
  - [28] X. Wen *et al.*, “A first-order differential data processing method for accuracy improvement of complementary filtering in micro-UAV attitude estimation,” *Sensors (Switzerland)*, vol. 19, no. 6, Mar. 2019, doi: 10.3390/s19061340.
  - [29] J. Han, M. Kamber, and J. Pei, “Data Preprocessing,” in *Data Mining*, Elsevier, 2012, pp. 83–124. doi: 10.1016/b978-0-12-381479-1.00003-4.
  - [30] S. R. Dubey, S. K. Singh, and B. B. Chaudhuri, “Activation Functions in Deep Learning: A Comprehensive Survey and Benchmark,” Sep. 2021, [Online]. Available: <http://arxiv.org/abs/2109.14545>
  - [31] S. Raghuram, A. S. Bharadwaj, S. K. Deepika, M. S. Khadabadi, and A. Jayaprakash, “Digital Implementation of the Softmax Activation Function and the Inverse Softmax Function,” in *4th International Conference on Circuits, Control, Communication and Computing, I4C 2022*, Institute of Electrical and Electronics Engineers Inc., 2022, pp. 64–67. doi: 10.1109/I4C57141.2022.10057747.
  - [32] K. He, X. Zhang, S. Ren, and J. Sun, “Delving Deep into Rectifiers: Surpassing Human-Level Performance on ImageNet Classification,” in *2015 IEEE International Conference on Computer Vision (ICCV)*, IEEE, Dec. 2015, pp. 1026–1034. doi: 10.1109/ICCV.2015.123.




- [33] V. L. B. De Mel and D. Mel, "Survey of Evaluation Metrics in Facial Recognition Systems," 2023, doi: 10.13140/RG.2.2.10974.20805.


## Appendix

### A. Participant Consent Form:

The consent form used during participant recruitment and data collection, ensuring ethical compliance and informed participation.



### Air Signature Using Smartwatch Motion Sensors



جامعة الملك سعود  
King Saud University  
College of Computer and  
Information Sciences  
Computer Science Department

#### Participant Consent Form

**Purpose of the Study:**  
This study aims to develop a secure authentication system by analyzing motion data collected through smartwatches.

**Participation Details:**

- You will be asked to perform air signatures using a smartwatch.
- Both genuine and forged signatures will be recorded for research purposes.
- The study involves no physical or emotional risks.

**Confidentiality:**  
Your data will be anonymized and stored securely. It will only be used for research purposes and will not be shared without your explicit consent.

**Voluntary Participation:**  
Participation is completely voluntary, and you may withdraw at any time without penalty.

**Consent Statement:**  
I have read and understood the study details provided above. By signing below, I consent to participate in this research.

**Participant Name:** \_\_\_\_\_

**Contact Information:**

Phone Number: \_\_\_\_\_ Email Address: \_\_\_\_\_

**Signature:** \_\_\_\_\_ **Date:** \_\_\_\_\_

**Researcher Name:** \_\_\_\_\_

**Signature:** \_\_\_\_\_ **Date:** \_\_\_\_\_