Multimodal Biometric Border Control System

Salma Abdelmonem
Cybersecurity Department
Faculty of Computer and Information Sciences
Ain Shams University
Cairo, Egypt
2021170913@cis.asu.edu.eg

Nour Amr
Cybersecurity Department
Faculty of Computer and Information Sciences
Ain Shams University
Cairo, Egypt
2021170925@cis.asu.edu.eg

Abdelrahman Khaled
Cybersecurity Department
Faculty of Computer and Information Sciences
Ain Shams University
Cairo, Egypt
2021170914@cis.asu.edu.eg

Moamen Mahmoud
Cybersecurity Department
Faculty of Computer and Information Sciences
Ain Shams University
Cairo, Egypt
2021170919@cis.asu.edu.eg

Abdelrahman Mohamed
Cybersecurity Department
Faculty of Computer and Information Sciences
Ain Shams University
Cairo, Egypt
2021170916@cis.asu.edu.eg

Zeiad Mahmoud
Cybersecurity Department
Faculty of Computer and Information Sciences
Ain Shams University
Cairo, Egypt
2021170911@cis.asu.edu.eg

Beshoy Victor
Software Engineering Department
Faculty of Computer and Information Sciences
Ain Shams University
Cairo, Egypt
beshoyvictor@cis.asu.edu.eg

Hanan Hindy
Computer Science Department
Faculty of Computer and Information Sciences
Ain Shams University
Cairo, Egypt
hanan.hindy@cis.asu.edu.eg

Abstract— The growing popularity of travel in the modern world coupled with inadequate authentication methods at border locations has contributed to the rise of border security incidents. The dominant solution of this problem is Biometric Border Control Systems. Previous research has primarily focused on unimodal biometric systems, which may reduce security events, but are still insufficient for high-security environments such as airports, especially with the continuous increase in travelers. These types of systems are vulnerable to spoofing attacks, intra-class variation and noisy data. This study aims to contribute to the reduction of border security incidents and address the scarcity of advanced systems in the field of multimodal biometric authentication with liveness detection.

The proposed methodology involves the identification of individuals and spoofing detection through the integration of two biometric traits: fingerprint and face. The pre-trained model DenseNet121 is used with custom classification tasks for identity verification and liveness detection. The two public datasets used for fingerprints and faces are FVC2002 and NUAA PI respectively. An additional created dataset was used to enhance fingerprint spoofing detection. Using these datasets and a DenseNet121 backbone, the system accurately identified individuals and detected spoofing attempts for both biometric traits.

Keywords— Border Control Systems, unimodal biometric systems, multimodal biometric systems, fingerprint, face, identification, spoofing detection, DenseNet121, FVC2002, NUAA PI.

I. Introduction

In an era of globalization and increasing displacement, border criminals and unauthorized immigrants have dramatically increased within the last few years due to the absence of proper authentication methods at border locations [1]. Illegal crossings or unauthorized events at border locations can lead to consequences such as national security threats when terrorists or smugglers are allowed through, potentially endangering public safety. Another significant consequence is the global spread of diseases, which can occur when unauthorized travelers are granted entry, potentially leading to a pandemic. Therefore, protection against border attacks is of utmost priority and a key challenge for all nations [2].

Currently, the literature and research on cyber-threat landscape evolves around relevant infrastructures to the border control, such as ports, airports or defense systems [2]. While these areas are critical, the methods used for passenger control at borders often remain outdated. Typically, passenger controls are done manually by trained immigration officers who compare the passport and the physical appearance of the traveler, a process that is time-consuming, unreliable and prone to human error [1]. In other countries, this process is done by Automated Border Control (ABC) systems, but these systems often rely on unimodal biometric data, which can be insufficient for robust security.

This project aims to address these challenges by enhancing the performance of border control systems through the integration of multimodal biometrics. By integrating multiple biological features, higher security can be provided because these biological features have high uniqueness and unforgeability. Compared with traditional identity verification methods, multimodal biometric recognition technology does not require memorizing complex passwords or carrying identification documents, thus providing a more convenient user experience.

Based on the Global Passenger Survey conducted on 2024 by the International Air Transport Association (IATA) [3], 73% of the 10,000 travelers surveyed across 200 countries expressed a desire to use their biometric data. Biometric-based authentication systems have been successfully employed for three decades at the University of Georgia and for over a decade at the airports in San Francisco and Walt Disney World, with tens of thousands of daily users. The use of biometric technologies in many security applications has grown globally because of its major benefits with regard to authentication rate, universality, and security [4].

A common threat faced by biometric systems is spoofing, where attackers use fake fingerprints or facial masks to bypass security. To address this, the project incorporates liveness detection techniques, ensuring that only genuine biometric traits are accepted, preventing spoofing attempts [4]. In addition, the project uses encrypted biometric databases to safeguard biometric data from database breaches, which are increasingly common at border checkpoints. Encryption ensures that stored data is protected against unauthorized access or alteration, mitigating risks of identity theft or tampering [5].

The remaining sections of this paper are structured as follows: Section II discusses related work, Section III presents the datasets incorporated in this work, Section IV describes the proposed methodology, Section V reports the results and discusses the evaluation of the system, and finally, Section VI concludes the paper.

II. Related Work

This section provides a comprehensive literature review of the topics: Multimodal Biometric Systems (Section A), Presentation Attack Detection (Section B) and Biometric Security (Section C)

A. Multimodal Biometric Systems

Multimodal biometric systems address the shortcomings of unimodal systems, which rely on a single biometric trait (e.g., face or fingerprint alone) and are vulnerable to challenges such as spoofing attacks, intra-class variations, non-universality, and noisy data. By combining multiple biometric traits, multimodal systems compensate for individual modality limitations, achieving higher accuracy and robustness.

Tomar and Singh [6] propose a hybrid cascaded-fusion framework using fingerprint (Crossing Number) and face (PCA) on a self-generated dataset of 1000 images. It achieves 99.50% accuracy with max fusion at a 0.60 threshold, reducing verification time. Limitations include reliance on controlled datasets and potential image quality issues, with future plans to incorporate user-specific traits.

Thenuwara *et al.* [1] uses deep learning and machine learning (CNN, SoftMax, SVM) on BANCA and SDUMLA-HMT datasets. It improves traveler identification efficiency with face and ear modalities, achieving real-time processing and high accuracy via a multi-agent system. Challenges include agent interoperability, real-time processing demands, and data privacy, suggesting future work on efficient algorithms and security enhancements.

B. Presentation Attack Detection

Liveness detection ensures that biometric inputs come from a living subject, enhancing system trustworthiness. Spoofing attacks are one of the most common threats faced by biometric systems and hence must be thoroughly researched to reach ways to prevent them. A few of the recent studies in this area are discussed.

Yuan *et al.* [7] proposes a multimodal CNN with weighted feature fusion for fingerprint and face liveness detection, improving accuracy by combining features from multiple models. Tested on datasets like LivDet [8] and NUAA [9], it outperforms traditional methods in various scenarios, with lower error rates (ACE, FAR, FRR) and strong generalization across materials and sensors.

Ortega *et al.* [10] introduces FlyPAD, a dynamic PAD system for border control that detects attacks as travelers approach the e-gate. It handles five attack types using face tracking, verification, and SVM-based PAD adapted to distance ranges. Tested on two datasets, it achieved up to 76.2% accuracy, with the lowest ACER (0.016) at 1–2 meters. The system is effective, with future plans to support more attack types and spatio-temporal analysis.

In [11], Li and Ramachandra review deep learning methods for fingerprint presentation attack detection (PAD), highlighting their advantage over traditional techniques by learning complex patterns. Their review categorizes approaches into contact-based, contactless, and smartphone-based, and emphasizes the use of diverse spoof materials like silicone and gelatin. Public datasets like LivDet [8] are discussed for training and benchmarking.

Table II.1 outlines the methods and results of the main papers mentioned in Section A (Multimodal Biometric Systems).

Table II.1: Summary of Literature on Multimodal Biometric Systems

Author(s)	Methods used	Datasets	Results
[1]	• Deep Learning • Machine Learning	• (NIST BSSR1) • SDUMLA-HMT • BANCA • PRIVATE	(CNN and SoftMax) is Better than (CNN and SVM)
[6]	• Crossing Number (C.N). • Principal Component Analysis (PCA). • Score level fusion.	Self-generated	• 0.6 FAR • 0.4 FRR • 99.5% Accuracy

Table II.2 summarizes each of the papers mentioned in Section B.

Table II.2: Summary of Key Papers on Presentation Attack Detection

Author(s)	Methods used	Datasets	Results
[7]	• Multimodal convolutional neural networks (MCNN) • Weighted feature fusion	• LivDet 2011, 2013, 2015 • NUAA face dataset	• FLD and FaLD had low ACE values
[10]	• Machine Learning • Hardware-based PAD algorithms	• FRAV-ABC-OnTheFly • FRAV-ABC-RB-OnTheFly	Real border Scenario: • 0.016 ACER • 76.2% Accuracy
[11]	• Convolutional neural networks (CNNs) • Deep learning-based methods	• LivDet	• Deep learning-based methods show better PAD.

C. Biometric Security

Section C focuses on work relevant to biometric system applications and security. It also shows research done in ensuring data privacy and security through the implementation and compliance of standards such as the General Data Protection Regulation (GDPR) [12].

Dhakal [5] highlights the benefits of multi-biometric systems over unimodal ones, addressing security threats like spoofing and replay attacks. His work reviews protection methods such as biometric cryptosystems and multi-factor authentication, and outlines applications in law enforcement, military, and commercial sectors.

Tran *et al.* [13] review privacy-preserving biometric authentication methods, proposing a taxonomy of techniques like non-invertible transformations, biometric key generation, information hiding, and cryptographic protocols. This study emphasizes the need for secure, irreversible, and unlinkable biometric protection as a standard.

Abomhara and Yayilgan [14] focus on privacy and data protection best practices under the EU's GDPR [12], especially in processing biometric data. This work guides data controllers, drawing on lessons from the SMILE project, and explains that biometric data is generally prohibited but allowed under specific exemptions like consent, vital interests, or public interest. It emphasizes user rights, Data Protection by Design and by Default (DPbD), and the need for Data Protection Impact Assessments (DPIAs) for large-scale processing.

Table II.3 shows the methods, datasets and results of three key papers in this particular field.

Table II.3: Summary of Key Papers on Biometric Security

Author(s)	Methods used	Datasets	Results
[5]	• Multi-biometric systems • Machine learning	Not mentioned	• Higher security and lower error rates
[13]	• Non-invertible Transformation • Direct Biometrics Key Generation • Information Hiding Techniques Protocol-based Protection	• FVC2002 DB1-4 • FVC2004 DB1-3 • FERET • CMU-PIE • FRGC • FEI • Extended Yale	• Hashing technique achieved 0% EER • The fuzzy extractor algorithm yielded EER of 4.5%.
[14]	• GDPR compliance • DPbD • DPIA	-	Guides data controllers under GDPR

III. Datasets

Two publicly available datasets of fingerprint and face images are incorporated into this project for the training and evaluation of the models utilized and configured. Additionally, a small scale single identity dataset was created to enhance spoofing detection and allow for the detection of actual attempts and not only software-generated ones. Each dataset is described below.

A. FVC2002

FVC2002 is the Second International Competition for Fingerprint Verification Algorithms [15] [16]. Four different databases (DB1, DB2, DB3 and DB4) were collected using different sensors/technologies. With a total of 110 identities, each database has 8 impressions of each identity's fingerprint, resulting in 880 fingerprints in each database and 3520 fingerprint images in all.

Table III.1 shows a description of each database.

Table III.1: FVC2002 Database [16]

Database	Sensor Type	Image Size	Resolution
DB1	Optical Sensor	388x374 (142 Kpixels)	500 dpi
DB2	Optical Sensor	296x560 (162 Kpixels)	569 dpi
DB3	Capacitive Sensor	300x300 (88 Kpixels)	500 dpi
DB4	SFinGe v2.51 [ref]	288x384 (108 Kpixels)	About 500 dpi

Samples from each database are shown in Figure III.1 below.

Figure III.1: Sample Fingerprint Images
From left to right: DB1 (real), DB2 (real), DB3 (real) and DB4 (spoofed)

B. Created Dataset

Due to limited resources, during the implementation of this project a small-scale fingerprint dataset was created to support the development of the spoof detection model. The dataset consists of fingerprint images from a single individual, captured using an R307 optical fingerprint sensor.

A total of 202 images were collected and divided between four databases, three of which contain spoofed images using different materials to simulate presentation attacks.

Table III.2 shows a description of each database.

Table III.2: Created Dataset Summary

Database/ Material Used	Sensor Type	Number of Images	Image Size	Resolution
Real	R307 Optical Sensor	101	256x288 (73.7 Kpixels)	500 dpi
Clay		49		
Tape		44		
Glue		8		

Samples from all databases are shown in Figure III.2 below.

Figure III.2: Sample Fingerprint Images
From left to right: Real, Clay, Tape and Glue

C. NUAA PI

NUAA Photo Imposter dataset [9] is property of the Nanjing University of Aeronautics and Astronautics. It contains images of real access attempts and print-attacks of 15 users with about 500 images each. There is a total of 5105 real images and 7509 fake images. The images contain frontal

faces with a neutral expression captured using a generic webcam. Users were also told to avoid eye-blinks and head movements. The attacks are performed using printed photographs on photographic paper and A4 paper. The dataset comprises three folders (DetectedFace, Raw, NormalizedFace) each containing two databases, Client and Imposter for genuine and spoofed images.

Table III.3 shows a description of each database.

Table III.3: Summary of each database in NUAA PI

Database	Contains	Sensor Type	Subfolders
Raw	Images in raw format	Generic Webcam	1. ClientFace 2. ImposterFace
DetectedFace	Images output by a face detector		
NormalizedFace	Geometrically normalized face based on eye coordinates		

Samples from each of the subsets in NUAA PI are shown in Figure III.3.

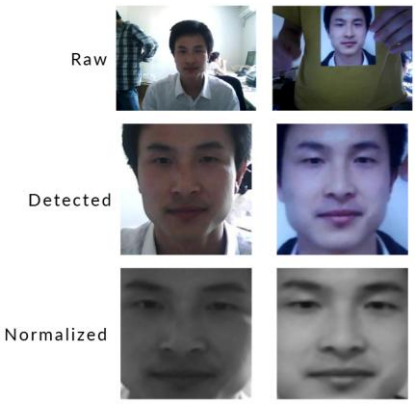

Figure III.3: Sample face images.
Each row has an image from ClientFace (Left), and ImposterFace (Right)

IV. Proposed Method

This paper proposes a cascade-based approach to achieving a multimodal biometric border control system. The biometric traits selected are fingerprints and faces as they are shown to be the most commonly used and known of as shown by the survey conducted by Labati *et al.* [17].

Motivated by the scarcity of multimodal biometric systems incorporating liveness detection and the gravity of security risks that could occur as a result of such attacks, the proposed method prioritizes spoofing detection along with the accurate verification of users. It also ensures data security and user privacy by complying with the GDPR.

The modules in this system are: biometric trait acquisition and enhancement, spoofing detection and identification using Artificial Intelligence (AI) models, feature extraction, and data security.

A. Biometric Trait Acquisition

The capturing of a user's fingerprint and face involves the use of sensors: a webcam to capture the face and the R307 fingerprint sensor [18] to capture the fingerprint.

1) Face Detection and Capturing

This is done using the Caffe model [19] to detect faces in an image or video frame, followed by using Dlib's 68-point shape predictor [20] to ensure the frontal directionality of the face. In the case of the face being aligned, an image is captured in a 5 second span.

Caffe's deep learning face detector runs on a Single-Shot Detector (SSD) framework with a ResNet base network. This is a pre-trained face detection model that localizes faces within an image.

Dlib's 68-point shape predictor is a pre-trained facial landmark detector used to estimate the location of 68 (x,y)-coordinates that map to facial structures on the face. These landmarks can be used to ensure that the face is facing forward with relaxed facial expressions.

2) Fingerprint Acquisition

The R307 fingerprint module is an optical sensor with Transistor-Transistor Logic (TTL) interface. The sensor is connected to the PC through a USB-TTL. A digital circuit diagram created using Cirkit Designed is displayed in Figure IV.1 to show wiring connections between the R307 fingerprint sensor and the USB-TTL converter.

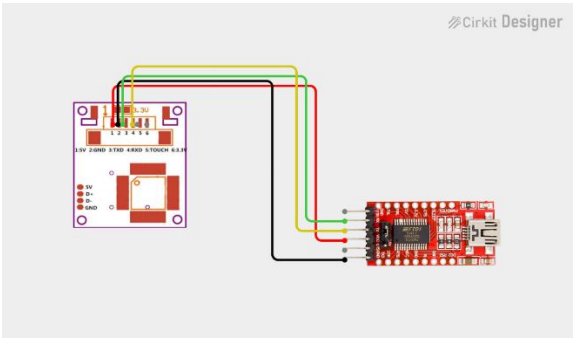

Figure IV.1: R307 Fingerprint Sensor Digital Circuit Diagram
The visual highlights VCC (Red), GND (Black), TX to RX (Green), and RX to TX (Yellow) lines for correct serial communication setup

A few protocols and resources of the R307 sensor need to be mentioned before continuing to ensure correct utilization. Communication is carried out through the transferring and receiving of data packets. Figure IV.2 shows the format of an R307 data packet.

Header	Adder	Package identifier	Package length	Package content (instuction/data/Parameter)	Checksum

Figure IV.2: R307 Data Packet Format

The definition of the data packet is shown in Table IV.1. This is essential for the proper extraction of fingerprint image data from the data packet.

The module provides an *Image Buffer*, a resource that stores fingerprint images in a resolution of 256*288 pixels. Finally, instructions that enable operations such as the capturing and uploading of fingerprint images are incorporated into the module for convenience. The required instructions for this work are:

- GenImg: captures fingerprint images and stores it in the *ImageBuffer*.
- UpImage: uploads the image in the *ImageBuffer* to the computer.

Table IV.1: R307 Definition of a Data Packet

Name	Symbol	Length	Description	
Header	Start	2 bytes	Fixed value of 0xEF01; High byte transferred first.	
Adder	ADDER	4 bytes	Default value is 0xFFFFFFFF, which can be modified by command. High byte transferred first and at wrong adder value, module will reject transfer.	
Package identifier	PID	1 byte	01H	Command packet.
			02H	Data packet: Data packet shall not appear alone in executing processes, must follow command packet or acknowledge packet.
			07H	Acknowledge packet.
			08H	End of Data packet.
Package length	LENGTH	2 bytes	Refers to the length of package content (command packets and data packets) plus the length of Checksum (2 bytes). Unit is byte. Max length is 256 bytes. And high byte is transferred first.	
Package contents	DATA	—	It can be commands, data, command's parameters, acknowledge result, etc. (fingerprint character value, template are all deemed as data);	
Checksum	SUM	2 bytes	The arithmetic sum of package identifier, package length and all package contents. Overflowing bits are omitted. High byte is transferred first.	

3) Fingerprint Image Enhancement

Raw images captured from the sensor contain noise and gaps in between the patterns of a fingerprint: ridges and valleys. These features must be highlighted before feature extraction is carried out on them.

The *fingerprint-enhancer* [21] library in Python was taken advantage of in this phase to enhance fingerprint images. This library enhances ridge-valley structure in grayscale fingerprint images, making them more suitable for feature extraction. Its main features are orientation estimation, frequency estimation, Gabor filtering and block-wise processing.

B. Spoofing Detection and Identification Models

The AI models configured in this project use DenseNet-121 [22], pre-trained on ImageNet [23], as a backbone due to its dense connectivity and efficiency in feature extraction for image classification tasks. Figure IV.3 below shows DenseNet-121's architecture.

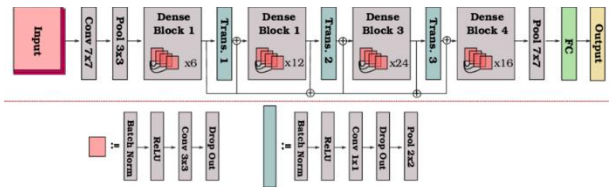

Figure IV.3: DenseNet-121 Model Architecture [22]

1) Fingerprint Identification Model

Due to the complexity of the fingerprint identification and spoofing detection tasks, a two-model approach is proposed. This is instead of using one multi-task model for both objectives where one task could hinder the other's performance. Each of the two models have a custom classifier configured specifically to match their task.

Table IV.2 lists the primary hyperparameters and training setup used in the fingerprint identification model and the results achieved will be discussed in Section V.A.1).

Table IV.2: Fingerprint Identification AI Model Configurations

Training Parameters and Settings	**Value**
Learning Rate	0.0001
Batch Size	32
Dropout Rate	0.6
Number of Epochs	55
Databases Used	DB1, DB2, DB3
Images Enhanced (Yes/No)	Yes
Data Split (Train/Validate/Test)	Stratified 70/15/15 split between DBs 1,2 and 3
Data Preprocessing/ Augmentation	Normalization: 1-channel images
	RandomHorizontalFlip: 0.5% probability
	RandomVerticalFlip: 0.5% probability
	RandomRotation: ±15 degrees

2) Fingerprint Spoofing Detection

Fingerprint presentation attacks can occur using different materials, making them harder to detect. Training the model only on FVC2002 was insufficient as it only allows the detection of software-generated fingerprints resembling FVC2002's DB4 and not actual spoofing attempts. For that reason, the fingerprint spoofing detection model was trained on both FVC2002 and the created dataset using Tape, Clay and Glue.

Table IV.3 below shows the primary hyperparameters and training setup used in the spoofing detection model.

Table IV.3: Fingerprint Spoofing Detection Model Configurations

Training Parameters and Settings	**Value**
Learning Rate	0. 0001
Batch Size	32
Dropout Rate	0.5
Number of Epochs	10
Databases Used	DB1, DB2, DB3, DB4, Real Created, Fake Created
Images Enhanced (Yes/No)	No
Data Split (Train/Validate/Test)	Stratified 70/15/15 split between Real and Fake images.
Data Preprocessing/ Augmentation	Normalization: using ImageNet statistics [23].
	RandomHorizontalFlip: 0.5% probability
	RandomVerticalFlip: 0.5% probability
	RandomRotation: ±15 degrees
	ColorJitter: ±0.2 brightness, ±0.2 contrast

The results achieved after testing this model are presented and discussed in Section V.A.2).

3) Face Identification and Spoofing Model

Since the datasets publicly available for faces are much larger than those for fingerprint images, training the model on two tasks was easier and the risk of one task constraining the other was less. Therefore, a single multi-task model with a custom classifier was used for identification and spoofing.

Table IV.4 presents the primary hyperparameters and training setup used in the face module AI model. The accuracy achieved after the standard testing of this multi-task model is shown in Section V.

Table IV.4: Face Module AI Model Configurations

Training Parameters and Settings	Value
Learning Rate	0. 001
Batch Size	32
Dropout Rate	0.5
Number of Epochs	10
Features Extracted	512
Database(s) Used	DetectedFace
Images Enhanced (Yes/No)	No
Data Split (Train/Validate/Test)	Random 80/10/10
Data Preprocessing	Normalization: using ImageNet statistics [23].

4) Feature Extraction and Recognition

The models designed for fingerprint and face identification and spoofing detection are utilized to extract features from users and take decisions based on thresholds.

Features are extracted by attaching a forward hook to the intermediate layer, DenseBlock3, of the DenseNet-121 model architecture (see Figure IV.3) used for both the fingerprint and face modules. A forward hook is attached to capture a layer's output. DenseBlock3 is a deep feature extraction layer that captures complex, high-level patterns in the input image. In the fingerprint model, it learns to detect patterns such as ridge flow, bifurcations, and minutiae, while in the face model, it focuses on key facial regions, symmetry, and expression-invariant features.

Following the extraction of features from an image, they need to be converted into a one-dimensional feature vector. During spoofing detection, the logits produced from the model are transformed into probabilities using SoftMax. For identification, a feature vector is compared to another feature vector using cosine similarity and verification is confirmed according to a threshold.

If the probability of spoofing, calculated with the help of SoftMax, exceeds a threshold of 0.80 (decided after experimentation) then the fingerprint or face image is declared as a spoofing attempt.

Different thresholds are set for the identification of fingerprints and faces. For fingerprints, the cosine similarity score must be greater than 0.95 for the user to be verified, and for faces the score must exceed 0.98; both thresholds were decided after experimentation and testing of different scenarios.

5) Data Security

Data security is reached by complying with the GDPR [12], particularly with articles such as 32 (1) (a) and 32 (2). These pronounce that the pseudonymization and encryption of personal data must be done, as well as enforcing different levels of security and ensuring accountability.

The encryption and hashing of data in this project is done using Python's *cryptography* library [24]. The Advanced Encryption Standard (AES) is made use of for encryption, and the Secure Hash Algorithm (SHA-256) for hashing.

To abide by Article 32 (1) (a), travelers' and officers' personal information, such as their names, passport numbers and biometric feature vectors, are encrypted. In addition to recorded incident IDs (e.g. spoofing attempt, identity mismatch) and details. Moreover, officers' passwords are hashed.

Different roles and permissions are defined in this project with logging to ensure accountability (Article 32 (2)). The roles and permissions are:

- Junior: Log viewing and incident management.
- Admin: Log viewing, incident management and user enrolment.
- Manager: Log viewing, incident management, user enrolment, officer enrolment and officer permission adjustment.

Although the GDPR does not explicitly mention password security, this project implements common password and authentication guidelines to further enhance its security. The guidelines followed are:

- The minimum password length should be eight characters.
- Passwords should contain at least one character from each of the four-character categories: uppercase, lowercase, numeric and special characters.
- Passwords should never be stored in plaintext but should be encrypted using strong encryption algorithms.
- Users must authenticate with Multi-Factor Authentication (MFA) [25] techniques.

Since this project is based on the authentication of users using a multimodal biometric system, MFA for admin log ins is achieved here using credentials and the officer's fingerprint and face.

V. Results and Discussion

The trained models are tested and evaluated first on the datasets used, then in real-life scenarios. Section V: Results and Discussion starts with presenting the accuracies achieved during standard model testing.

A. Standard Model Testing

1) Fingerprint Identification Model

Under the settings shown in Table IV.2, the fingerprint identification model achieved an accuracy of 90.40%, presented in Table V.1.

Table V.1: Fingerprint Identification AI Model Results

Identification Accuracy
90.40%

2) Fingerprint Spoofing Detection Model

Under the settings shown in Table IV.3, the fingerprint spoofing detection model achieved an accuracy of 99.82% (Table V.2).

Table V.2: Fingerprint Spoofing Detection Model

Spoofing Accuracy
99.82%

The results of 90.40% identification and 99.82% spoofing detection are satisfactory numbers, but the system must be tested in real-life scenarios to ensure its robustness before deployment. This is shown in Section V.B.

3) Face Identification and Spoofing Detection AI Model

The multi-task model used for face identification and spoofing detection resulted in 99.60% identification accuracy and 100.00% spoofing detection accuracy when configured as shown in Table IV.4. The accuracies achieved are presented in Table V.3.

Table V.3: Face Module AI Model Results

Identification Accuracy	Spoofing Detection Accuracy
99.60%	100.00%

Similar to the fingerprint models, the results here seem to be adequate, however, only through real-time testing will the decision whether to deploy these models in high security environments be taken.

Different real-life scenarios are tested in the next section, V.B.

B. *Real Time Testing*

During the real-time testing of these models, several scenarios were tested and a decision threshold was determined based on them. The final thresholds determined were 0.80 for fingerprint and face spoofing detection, 0.95 for fingerprint identification and 0.98 for face identification. The thresholds must be high enough to prevent impersonation attempts between similar looking individuals, but low enough to allow genuine attempts when an individual could look slightly different than his/her saved image. Although this balance is important to prevent inconveniencing genuine travelers, in the context of a border crossing, security is of higher importance than convenience.

Table V.4 shows the thresholds for each phase.

Table V.4: Decision Thresholds for each Phase

Phase	Threshold
Spoofing Detection	0.80
Fingerprint Identification	0.95
Face Identification	0.98

This section presents some of the scenarios tested using the designed models. The images used for testing are shown in figures, followed by their results presented in a table.

For spoofing attempts, the SoftMax probability is generated using the model's logits and then a decision is taken based on the threshold. Two different spoofing attempts were tested for each biometric.

For identification, the cosine similarity between the features of the user attempting to get verified and the user ID's features in the database is found. The verification is decided based on the threshold. Impersonation and genuine attempts were tested.

1) *Fingerprint Spoofing Attempts*

a) *Using Tape*

This is a spoofing attempt using tape around the user's finger. Figure V.1 shows the captured image using the R307 sensor.

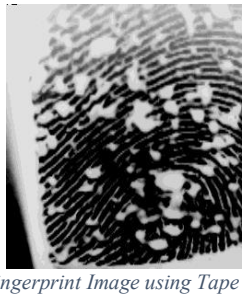

Figure V.1: Fingerprint Image using Tape (Spoofing)

This image was detected as a spoofing attempt with 99.01% certainty.

Table V.5: SoftMax Output and Prediction Result – Taped Fingerprint

SoftMax Probability	Prediction Result using Threshold 0.80
0.9901	Spoofing Detected

b) *Software-generated Fingerprint*

A software-generated fingerprint using SFinGe [26] was uploaded to the system and tested. Figure V.2 shows the generated fingerprint.

Figure V.2: Software-generated Fingerprint using SFinGe [26]

This trial was declared as a spoofing attempt with a probability of 99.60%. Since 99.60% exceeds the threshold of 80.00%, the system detects and prevents this attack.

Table V.6: SoftMax Output and Prediction Result - Software-generated Fingerprint

SoftMax Probability	Prediction Result using Threshold 0.80
0.9960	Spoofing Detected

2) *Face Spoofing Attempts*

a) *Spoofed Face Image from a Passport*

The passport was held in front of the webcam to capture the face image. Figure V.3 shows the detection and capturing of this spoofed image.

Figure V.3: ID Face Image Detection (Left) and Captured Face Image (Right)

This scenario was announced as a spoofing attempt by the system with 100.00% confidence.

Table V.7: SoftMax Output and Prediction Result - Passport Face Image

SoftMax Probability	Prediction Result using Threshold 0.80
1.00	Spoofing Detected

b) *Spoofed Face Image using a 4*3 Headshot*

A 4*3 headshot was held up to the webcam to test another spoofing technique. The 4*3 headshot tested is shown in Figure V.4.

*Figure V.4: 4*3 Headshot (Spoofed)*

The results from this test were a SoftMax spoofing probability of 91.46%, hence this attack was also detected.

*Table V.8: SoftMax Output and Prediction Result - 4*3 Headshot*

SoftMax Probability	Prediction Result using Threshold 0.80
0.9146	Spoofing Detected

3) Fingerprint Identification

a) Impersonation Attempt

A Person D tries to falsely identify as Person E. The captured fingerprints of both persons are shown in Figure V.5.

Figure V.5: Person D's Fingerprint (Left) and Person E's Fingerprint (Right)

The 0.95 threshold was able to detect the impersonation attempt. Table V.9 shows the similarity score and the decision taken.

Table V.9: Matching Score and System Decision - Impersonation Attempt

Similarity Score	Result using Threshold 0.95
0.9454	Identity Mismatch

b) Genuine Attempt

Person A attempts to identify as his/herself. The newly captured fingerprint and the one whose feature vector is stored are shown in Figure V.6.

Figure V.6: Newly Captured Fingerprint (Left) and Saved Fingerprint (Right)

The fingerprint image on the left is the newly captured one of Person A. However, the one on the right is whose feature vector is stored in the database. The cosine similarity between the newly captured image and the stored image is found and shown in Table V.10.

Since the similarity score exceeds the threshold, this genuine attempt was verified.

Table V.10: Matching Score and System Decision - Genuine Verification Attempt

Similarity Score	Result using Threshold 0.95
0.9634	Identity Verified

4) Face Identification

a) Impersonation Attempt

Person D attempts to impersonate Person F. The captured faces of both persons are shown in Figure V.7

Figure V.7: Person D (Left) and Person F (Right)

Table V.11: Matching Score and System Decision in an Impersonation Attempt

Similarity Score	Result using Threshold 0.98
0.9771	Identity Mismatch

A 0.98 threshold detected this impersonation attempt successfully.

b) Genuine Attempt

Person G identifying as themselves. Figure V.8 shows his captured images.

Figure V.8: Two Captured Face Images of Person G

Table V.12: Matching Score and System Decision in a Genuine Verification Attempt

Similarity Score	Result using Threshold 0.98
0.9940	Identity Verified

The real-time tests proved that using the current identification threshold, genuine attempts are unlikely to be incorrectly detected as impersonations, hence avoiding inconveniencing genuine users. It also showed the robustness of the 0.80 spoofing threshold; ensuring the detection of more sophisticated attacks.

Table V.13 sums up all the results achieved both during standard and real-time testing.

Table V.13: Standard and Real-time Testing Results

	Standard Testing	Real-Time Testing	
	Accuracy	Spoofing Attempts Detected	Impersonation Attempts Detected
Fingerprint Spoofing Detection	99.82%	10/10	
Face Spoofing Detection	100.00%	9/10	
Fingerprint Identification	90.40%		8/10
Face Identification	99.60%		9/10

VI. Conclusion

This paper presented the design and implementation of a cascade-based multimodal biometric border control system that integrates both face and fingerprint recognition, with spoof detection capabilities using deep learning models. It utilized a DenseNet-121 backbone with custom classifier heads for identity verification and spoofing detection, along with image processing techniques for fingerprint enhancement. Three datasets were used for the training and evaluation of the models: FVC2002, NUAA PI, and a created dataset. The work implemented in this study yielded accuracies of 90.40% and 99.60% for fingerprint and face identification respectively, and 99.82% and 100.00% for fingerprint and face spoofing detection respectively.

In addition to that, data security and privacy of the travelers was ensured by complying with the GDPR and implementing encryption, hashing and password guidelines.

The main contribution of this work is the addition of liveness detection to multimodal biometric systems. Unlike some of the existing systems that focus solely on identity verification, this system ensures both the accurate identification and verification of users, as well as the prevention of spoofing attacks using different materials. This was achieved by creating a dataset using Tape, Clay and Glue as spoofing materials, so not only can the system detect software generated fingerprints but real attempts as well. These results build towards allowing this project to be deployable in high security environments.

Future work can extend this study by expanding the dataset for greater diversity of identities and materials used during spoofing attacks. Added to this could also be the detection of the specific material used in an attack. Furthermore, achieving better accuracies and error rates is always an important goal.

Evaluating the system in an uncontrolled environment with varying lightning and backgrounds is an essential step to prepare the system for real-world deployment. Additionally, to achieve security in critical environments such as border checkpoints, future enhancements should address data transmission security and system communication channels to ensure no attackers hijack the system and falsely authenticate themselves.

Finally, another potential improvement involves integrating a mobile application that securely stores the user's e-passport data, enabling a seamless and contactless border crossing experience.

References

[1] S. S. Thenuwara, C. Premachandra and H. Kawanaka, "A multi-agent based enhancement for multimodal biometric system at border control," *Array,* vol. 14, p. 100171, 2022.

[2] C. P. and S. E., "Cyber-threat landscape of border control infrastructures," *International Journal of Critical Infrastructure Protection,* vol. 36, p. 100503, 2022.

[3] International Air Transport Association, "Annual Report of the Air Transport Industry," June 2024. [Online]. Available: https://www.iata.org/contentassets/c81222d96c9a4e0bb4ff6ced0126f0bb/iata-annual-review-2024.pdf. [Accessed October 2024].

[4] U. Sumalatha, K. K. Prakasha, S. Prabhu and V. C. Nayak, "A Comprehensive Review of Unimodal and Multimodal Fingerprint Biometric Authentication Systems: Fusion, Attacks, and Template Protection," *IEEE Access,* vol. 12, pp. 64300-64334, 2024.

[5] S. Dhakal, *Multi-Biometric Systems: Their Application and Security,* Turku University of Applied Sciences, 2021.

[6] P. Tomar and R. C. Singh, "Cascade-based Multimodal Biometric Recognition System with Fingerprint and Face," *Macromolecular Symposia,* vol. 397, no. 1, p. 2000271, 2021.

[7] C. Yuan, S. Jiao, X. Sun and Q. M. Jonathan Wu, "MFFFLD: A Multimodal-Feature-Fusion-Based Fingerprint Liveness Detection," *IEEE Transactions on Cognitive and Developmental Systems,* vol. 14, no. 2, pp. 648-661, 2022.

[8] Liveness Detection Competition Series, *LivDet,* 2021.

[9] X. Tan, Y. Li, J. Liu and L. Jiang, "Face Liveness Detection from a Single Image with Sparse Low Rank Bilinear Discriminative Model," in *European Conference on Computer Vision*, 2010.

[10] D. Ortega-Delcampo, A. Fernández-Isabel, I. M. de Diego, C. Conde and E. Cabello, "Dynamic Facial Presentation Attack Detection for Automated Border Control Systems," *Computers & Security,* vol. 92, p. 101744, 2020.

[11] L. Hailin and R. Ramachandra, "Deep Learning based Fingerprint Presentation Attack Detection: A Comprehensive Survey," *ACM Computing Survey Journal,* p. 29, 2023.

[12] European Union, "General Data Protection Regulation," 2018. [Online]. Available: https://gdpr-info.eu/. [Accessed Feburary 2025].

[13] Q. N. Tran, B. P. Turnbull and J. Hu, "Biometrics and Privacy-Preservation: How Do They Evolve?," *IEEE*

Open Journal of the Computer Society, vol. 2, pp. 179-191, 2021.

[14] M. Abohamra and S. Y. Yayilgan, *An Example of Privacy and Data Protection Best Practices,* 2022.

[15] D. Maltoni, D. Maio, S. Prabhakar and F. J., Handbook of Fingerprint Recognition, 2022.

[16] Second International Competition for Fingerprint Verification Algorithms, "FVC2002," 2002. [Online]. Available: http://bias.csr.unibo.it/fvc2002/. [Accessed 20 June 2025].

[17] R. D. Labati, A. Genovese, E. Muñoz, V. Piuri, F. Scotti and G. Sforza, "Biometric Recognition in Automated Border Control: A Survey," *ACM Computing Surveys,* vol. 49, no. 2, pp. 1-39, 2016.

[18] Hangzhou Grow Technology Co., Ltd, "R307 Fingerprint Module User Manual," Feb 2011. [Online]. Available: https://www.openhacks.com/uploadsproductos/r307_fingerprint_module_user_manual.pdf. [Accessed 15 June 2025].

[19] V. Olufemi, "Face Detection With OpenCV," Medium, 2020. [Online]. Available: https://medium.com/@victorolufemi/face-detection-c27228ccc6f.

[20] A. Rosebrock, "Training a custom dlib shape predictor," pyimagesearch, 2019. [Online]. Available: https://pyimagesearch.com/2019/12/16/training-a-custom-dlib-shape-predictor/.

[21] L. Hong, Y. Wan and A. Jain, "Fingerprint image enhancement: algorithm and performance evaluation," *IEEE Transactions on Pattern Analysis and Machine Intelligence,* vol. 20, no. 8, pp. 777-789, 1998.

[22] G. Huang, Z. Liu, L. van der Maaten and K. Q. Weinberger, *Densely Connected Convolutional Networks,* 2018.

[23] J. Deng, W. Dong, R. Socher, L.-J. Li, K. Li and L. Fei-Fei, "ImageNet: A large-scale hierarchical image database," in *2009 IEEE Conference on Computer Vision and Pattern Recognition*, 2009.

[24] PyCA, *cryptography,* 2014.

[25] "Multi-Factor Authentication: Benefits, Best Practices & More," FORTINET, [Online]. Available: https://www.fortinet.com/resources/cyberglossary/multi-factor-authentication?utm_source=blog&utm_medium=blog&utm_campaign. [Accessed 20 June 2025].

[26] R. Cappelli, D. Maltoni, D. Maio and A. Erol, "Synthetic fingerprint-image generation," in *Proceedings 15th International Conference on Pattern Recognition. ICPR-2000*, 2000.

[27] A. Khaled, A. Sohsah, N. Bahgat, S. Abdelmonem, Z. Mahmoud and M. Mahmoud, "Multimodal Biometric Border Control System," Github Repository, 2025. [Online]. Available: https://github.com/Abdellrhman-Khaled/Graduation-Project.git. [Accessed 25 June 2025].