Uniosun Journal of Engineering and Environmental Sciences (UJEES), Vol. 8 No. 2, Sept., 2026
DOI: 10.64980/ujees.v8i2.001 **Okomba et al.**
Published: September 30, 2026

DEVELOPMENT AND PERFORMANCE EVALUATION OF A MULTI-LAYER BANK VAULT LASER SECURITY SYSTEM WITH FACE RECOGNITION ACCESS USING RESNET-34

N. S. Okomba[1*], A. A. Sobowale[2], A. O. Esan[3], B. A. Omodunbi[4], T. A. Awoyemi[5], S. E. Avah[6]

[1,2,3,4,5,6]*Department of Computer Engineering, Federal University Oye-Ekiti, Ekiti, Nigeria*

[*]*Corresponding Author: nnamdi.okomba@fuoye.edu.ng*

Abstract
The development of a bank vault laser security system with face recognition access using ResNet-34 presents a multi-layered security architecture designed to enhance the protection of high-value assets and confidential information in banking environments. At its base, a laser sensor network controlled by a Raspberry Pi 4 Model B establishes a virtual security perimeter around the vault entrance. Any interruption of the laser beam immediately triggers an audible alarm and updates the LCD status display, forming the first layer of physical intrusion monitoring. For biometric verification, the system employs a face-recognition module built on the ResNet-34. The dataset used for training the model consisted of 7,500 facial images, systematically collected from three subjects, with each subject contributing 2,500 images captured under varying illumination, background conditions, and pose differences. To ensure hardware consistency and avoid inter-device bias, all images were captured using the same in-built camera module. The ResNet-34 model was fine-tuned using the Adam optimizer (learning rate = 0.001, batch size = 32) for 50 training epochs. It achieved a recognition accuracy of 96.7%, precision of 95.8%, recall of 96.1%, and a false acceptance rate (FAR) of 3.3% on the validation set. Facial embeddings produced by the network were matched using the Euclidean distance similarity metric to ensure fast and consistent identity verification. The laser intrusion module demonstrated a response latency of 0.21 seconds and 100% detection reliability under controlled testing.

Keywords
Bank Vault Security, Deep Learning, Laser Intrusion Detection, Biometric Authentication, Cyber-Physical Security Systems

1. INTRODUCTION

The security of bank vaults has always been a paramount concern for financial institutions, entrusted with safeguarding not only valuable assets but also sensitive information and public trust. Traditionally, this security has relied on robust physical measures such as intricate locks, fortified doors, and passive surveillance from CCTV cameras. However, the rapid advancement of technology and the increasing sophistication of security threats have exposed the limitations of these conventional systems. There is a growing need for multi-layered and intelligent security solutions capable of effectively deterring, detecting, and responding to modern threats (such as unauthorized physical access, sophisticated burglary attempts, insider threats, identity spoofing), and attempts to bypass conventional access control systems in real time. This research seeks to address this need by developing a novel bank vault security system that strategically integrates laser technology with advanced face recognition to create a proactive and highly resilient defense mechanism [1].

The development of next-generation security systems has been made possible through significant advancements in Artificial Intelligence (AI) and deep learning[2]. These models can automatically recognize features from raw inputs such as images and live video feeds without requiring manual programming [3], [4]. One of the most important deep learning architectures for visual tasks is the Convolutional Neural Network (CNN). Inspired by the structure of the human visual cortex, CNNs are highly effective in processing and analyzing image and video data, making them central to modern computer vision applications[5]. In this research, AI and deep learning function as the "brain" of the proposed system, enabling it to intelligently perceive, interpret, and authenticate its environment [6], [7].

[2] found that reducing errors in forensic face identification is critical because such errors can have severe personal and societal consequences. Although forensic examiners are responsible for performing identification tasks, systematic evaluations of their performance are relatively uncommon. To determine the most effective identification approach, whether human, machine-based, or hybrid, the researchers compared the performance of multiple groups using a challenging face identification test[8]. The study revealed that forensic facial examiners, facial reviewers, and super-recognizers performed better than fingerprint

examiners and students. However, there was significant variation in individual performance levels. Four Deep Convolutional Neural Networks (DCNNs) developed between 2015 and 2017 achieved performance comparable to human examiners, with the latest DCNN surpassing the median accuracy level of forensic facial examiners [9].

The study also explored the effectiveness of crowd-sourcing by combining the judgments of multiple forensic facial examiners. Averaging their identity judgments significantly improved accuracy compared to individual efforts while also reducing variability among lower-performing examiners. Furthermore, combining a single forensic facial examiner with the best-performing algorithm produced better results than combining two human examiners alone. These findings demonstrate that collaboration between humans and intelligent machine systems offers a promising pathway for improving face identification accuracy in critical security applications. The study therefore provides a data-driven framework for achieving higher reliability and accuracy in face recognition systems [9].

2. MATERIALS AND METHOD

The developed system consists of four major layers: (1) Sensing Layer, (2) Intelligence Layer, (3) Control Layer, and (4) Actuation Layer.

The Sensing Layer includes a high-resolution RGB camera and a calibrated laser-photodiode pair positioned across the vault entrance. The Intelligence Layer is powered by a fine-tuned ResNet-34 neural network deployed on an embedded GPU-enabled processing unit. The Control Layer is implemented using a microcontroller responsible for access logic, decision synchronization, and alarm triggering. The Actuation Layer controls the electromechanical vault lock and alarm siren.

2.1. System Design Architecture

The overall system integrates two major subsystems:

a. Laser Intrusion Detection Subsystem: This monitors the vault entrance using laser beams aligned with photodiode receivers. Any obstruction triggers a security interrupt. The Laser Intrusion Detection Subsystem serves as the first line of defense against physical breaches. It is based on the fundamental principle of line-of-sight beam interruption.
Once triggered, the system executes two actions simultaneously:
   i. Activates an audible and visual alarm, using a buzzer and a high-intensity LED flash to warn of possible intrusion.
   ii. Signals the Face Recognition Subsystem to capture an image of the person in front

b. Face Recognition Access Subsystem: This authenticates authorized personnel using deep face embeddings from a dlib-ResNet-34 model.

The Face Recognition Access Subsystem constitutes the second line of security, responsible for determining whether the detected individual is an authorized vault user.
Upon receiving a signal from the laser module (or in continuous monitoring mode), the camera module connected to the Raspberry Pi or ESP32-CAM captures a high-resolution image of the person standing before the vault. This image is then processed through a three-stage recognition pipeline

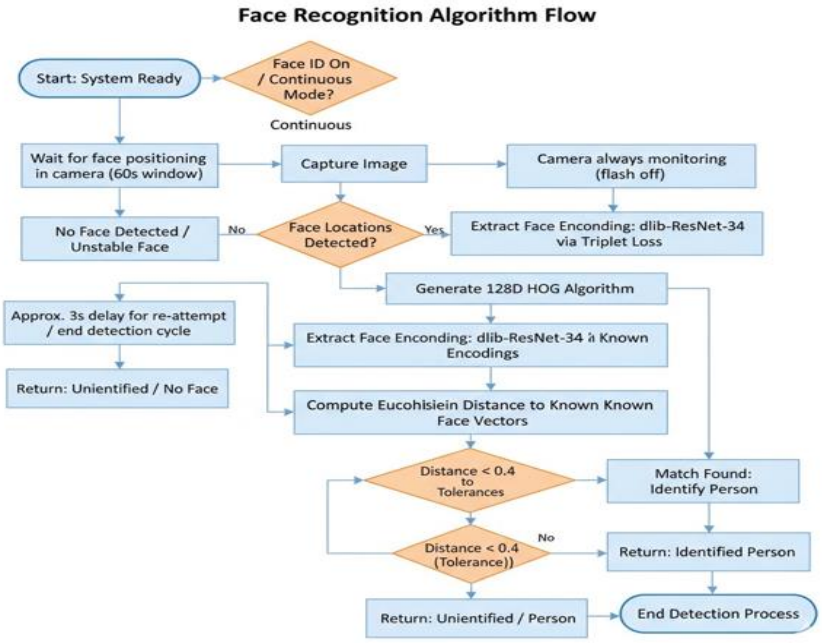


Figure 1: Flowchart for Face recognition algorithm

2.1.1 Hardware design

The hardware portion of the Bank Vault Laser Security System with Face Recognition Accessforms the physical foundation upon which the system's logic operates. Each component plays a distinct and complementary role to ensure reliable detection, verification, and alerting. The key components used in the prototype include the Raspberry Pi 4 Model B, laser–photodiode pair, LCD module, matrix keypad, buzzer, flash LED, and camera module. Their combined operation creates a fully functional, autonomous vault protection system.

i. **Raspberry Pi 4 Model B (Central Controller):** The Raspberry Pi 4 Model B acts as the brain of the entire system. It is a compact single-board computer equipped with a 1.5 GHz quad-core processor, Wi-Fi, Bluetooth, and 40 GPIO (General-Purpose Input/Output) pins that allow it to interface directly with sensors, actuators, and peripheral devices.

ii. **Laser Diode and Photodiode Pair (Intrusion Detection Sensor):** The laser diode and photodiode pair forms the primary security sensor of the system. A low-power, narrow-beam red laser is mounted so that its light is directed across the vault entrance. Opposite the emitter, a photodiode or phototransistor receiver is aligned to receive this light continuously. Under normal conditions, the laser beam continuously strikes the photodiode, keeping its output at a steady high voltage level, which the Raspberry Pi interprets as secure

iii. **HD44780 LCD with I²C Module (Display Feedback Unit):** TheHD44780 LCD, paired with an I²C communication module, provides visual feedback for system operation. Instead of using multiple GPIO pins for parallel communication, the I²C module reduces the wiring requirement to just two lines: SDA (data) and SCL (clock).

iv. **A 4 by 4 Matrix Keypad (User Input and Control Interface):** The 4×4 matrix keypad provides a secure and flexible manual control interface for system operation. It consists of 16 keys arranged in a grid of four rows and four columns, scanned by the Raspberry Pi through eight GPIO pins.

v. **12V Buzzer (Alarm Notification Unit):** The buzzer serves as the audible alert mechanism in the system. It is powered by a 12 V DC supply and driven through a 2N2222A transistor acting as a switching amplifier. The base of the transistor is connected to a Raspberry Pi GPIO pin via a 1kΩ resistor, allowing the Pi to turn the buzzer ON or OFF digitally.

vi. **3W Flash LED (Illumination Support during Recognition):** The 3W high-intensity flash LED is included to improve image quality during face capture, especially under poor lighting conditions. It is controlled via another transistor driver, enabling the Raspberry Pi to switch it on automatically whenever recognition is in progress

vii. **dlib-Compatible Camera (ESP32-CAM or Pi Camera):** The camera module acts as the visual sensor of the system.

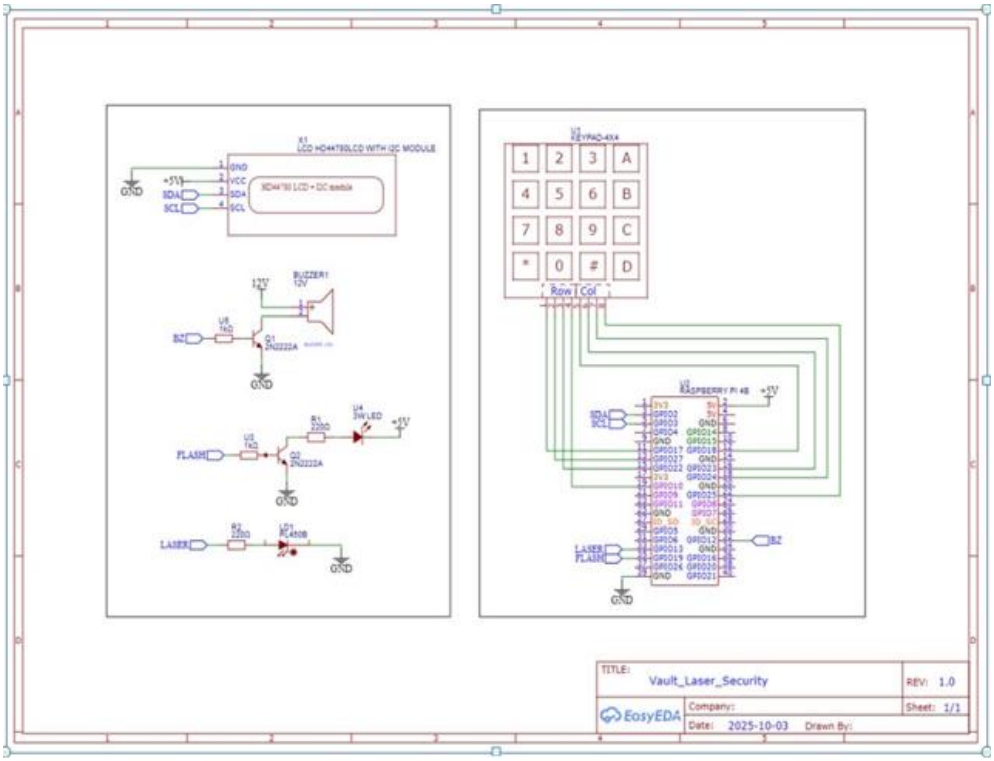


Figure 2: Implementation and circuit layout used in the prototype

2.1.2 Software design and algorithmic framework

The software architecture of the Bank Vault Laser Security System with Face Recognition Access was carefully developed to integrate intelligent image analysis with real-time hardware control. The workflow, is organized into several interdependent stages, beginning from data acquisition and preprocessing, through feature encoding and matching, and concluding with full system integration and operational deployment.

2.2 Workflow Overview

The software workflow was designed as a modular pipeline, ensuring that each stage performed a distinct task while passing its output seamlessly into the next. The primary modules include:

i. Data Collection
ii. Preprocessing and Face Detection (HOG)
iii. Face Encoding (ResNet-34 Embedding Generation)
iv. Face Matching (Euclidean Distance Comparison)
v. System Implementation and Mode Definition
vi. Final Integration with Laser Vault Subsystem

2.2.1 Data acquisition

The dataset used for the facial recognition component consisted of 7,500 facial images collected from three adult volunteer subjects, designated as Subject A, Subject B, and Subject C, with 2,500 images contributed by each subject. The images were captured using the in-built camera of a single device to maintain consistency in image quality and minimize device-related variations. During acquisition, each subject was positioned in front of the camera and images were captured under varying facial orientations, expressions, and illumination conditions to reflect practical access scenarios. Blurred or poorly captured images were excluded, and the final images were organized according to the three subject classes for training and evaluation of the ResNet-34 model.

2.2.2 Preprocessing and face detection

After collecting the facial images, several preprocessing steps were carried out to make the data consistent and ready for recognition using the Histogram of Oriented Gradients (HOG) algorithm. HOG analyzes the direction and magnitude of edges within localized regions of an image, effectively identifying the structure of a face regardless of background noise. Once the images were properly normalized, each face was encoded into a 128-dimensional feature vector using the dlib implementation of the ResNet-34 deep learning model. To train and test the recognition model fairly, the dataset was divided into three parts: (60%) were used for training, (20%) for validation, and (20%) for testing.

2.2.3 Algorithmic framework

The algorithmic framework is structured into three sequential stages: face detection, face encoding, and face matching each leveraging distinct computational techniques to achieve accurate and efficient face recognition. This modular design reflects best practices in biometric systems, allowing for independent optimization of each stage while ensuring a cohesive pipeline. Below, I discuss each subcomponent in detail, emphasizing their technical foundations, implementation choices, and implications.

2.2.4 Face detection

The face detection stage employs the Histogram of Oriented Gradients (HOG) algorithm, a classical computer vision technique, to localize faces within captured images. HOG extracts gradient orientation features from localized image patches, creating a robust representation of facial structures that is relatively invariant to changes in illumination and moderate pose variations. The algorithm slides a window across the image, computing gradient histograms to identify regions with face-like patterns, which are then classified using a pre-trained linear classifier (typically a Support Vector Machine, as implemented in libraries like dlib). The output is a bounding box around each detected face, which is subsequently passed to the encoding stage.

2.2.5 Face encoding with deep metric learning

Once faces are detected, the methodology employs Deep Metric Learning with Triplet Loss using the dlib-ResNet-34 model to encode face regions into 128-dimensional embedding vectors. The dlib-ResNet-34 model, a pre-trained deep convolutional neural network, leverages the ResNet architecture (a 34-layer residual network) to extract high-level features from face images. The triplet loss function ensures that embeddings of the same individual are closer together in the feature space (low intra-class distance) while embeddings of different individuals are farther apart (high inter-class distance). This results in a compact, discriminative representation of each face, suitable for matching.

2.2.6 Face matching and identity decision

The face matching stage computes the Euclidean distance between the query face's embedding and the embeddings of enrolled individuals stored in the system. A threshold of 0.4 is used to determine a match: distances below 0.4 classify the query as a known individual, while distances above 0.4 label it as

"unidentified." This threshold-based approach is standard in balancing sensitivity (true positives) and specificity (true negatives) as shown in equation 1

$$D = \sqrt{\sum_{i=1}^{128}(xi - yi)^2} \quad (1)$$

xi and yi represent the individual vector components of two embeddings being compared. If the computed distance D is below the threshold value of 0.40, the face is recognized as belonging to an authorized user. If D ≥ 0.40, it is classified as an unknown or unauthorized individual.

2.2.7 System implementation

The system implementation section details how the algorithmic framework is deployed in a practical, real-world context, integrating face recognition with a laser-enabled vault security system. The use of Python and the face recognition library, alongside a multi-threaded architecture and two operational modes (Face ID on Demand and Continuous Mode), demonstrates a thoughtful approach to balancing computational efficiency, responsiveness, and security requirements. Python's versatility and extensive ecosystem make it an excellent choice for rapid prototyping and deployment of complex algorithms. The face recognition library simplifies the integration of HOG-based detection and ResNet-based encoding, allowing the researchers to focus on system-level integration rather than low-level algorithm development. This abstraction is particularly valuable for security applications, where ease of maintenance and scalability are critical.

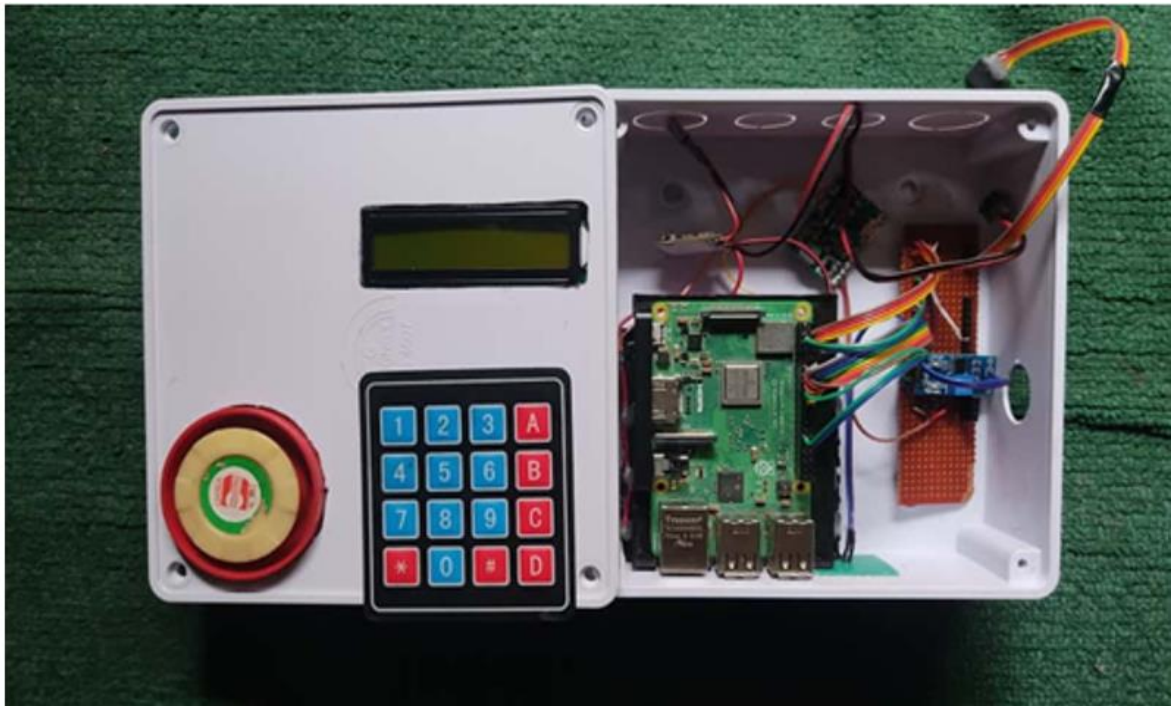


Plate 1: Schematic circuit diagram of the vault security system, illustrating the interconnection between hardware modules

2.2.8 Integration with the laser vault security subsystem

In the final stage, the face recognition framework was fully integrated with the laser vault intrusion detection mechanismto form a unified security system. Upon a beam interruption, the laser subsystem signals the recognition module to capture a facial image. If the face is verified as authorized, the system logs the event, sends a confirmation email to the administrator, and optionally disables the alarm. If the face is unauthorized or unrecognized, the system maintains the alarm condition and dispatches an intrusion alert email containing the captured image and timestamp. This final integration ensures real-time coordinationbetween hardware detection and intelligent recognition, combining optical sensing precision with deep learning intelligence to safeguard the vault.

2.2.9 Email feedback implementation

An automated email notification system was built into the project to provide instant feedback whenever an event occurs. This feature was implemented using Python's smtplib and email.mime libraries, which allow the Raspberry Pi to send structured email messages directly over a secure SMTP connection. Whenever the system detects an intrusion or successfully identifies a user, it automatically composes an email that includes all the essential details of the event. Each message contains the timestamp of when the incident occurred, the status of the event, and the captured facial image as an attachment for visual verification. The message also

includes the vault identification number and system location, enabling security personnel to quickly trace the exact site of the activity.

3. RESULTS AND DISCUSSION

3.1 Algorithmic Framework Results

The recognition framework followed the standard three-stage pipeline of detection, encoding, and matching. The first stage, detection, was carried out using the Histogram of Oriented Gradients (HOG) algorithm, which proved effective in locating facial regions across a wide range of conditions. Once detected, the facial images were aligned and passed through the dlib-ResNet-34 model, which produced a 128-dimensional embedding vector for each sample. These embedding served as compact numerical representations of facial features. The final stage involved comparing the query embedding with those stored in the enrollment database, using Euclidean distance as the similarity measure. A threshold of 0.40 was set as the decision boundary, meaning that distances below this value were treated as valid matches. When evaluated, the system correctly recognized 80% of genuine samples, while successfully rejecting 96.7% of impostor attempts. This produced an overall recognition accuracy of 88.33%. Performance was consistent across all three enrolled participants, each recording roughly 80% recognition accuracy, which suggests that the model generalized well across users. The False Acceptance Rate (FAR) was very low at 3.33%, an encouraging result for a security-critical application like a bank vault system, where unauthorized access must be minimized. However, the False Rejection Rate (FRR) stood at 20%, indicating that genuine users were occasionally misclassified, particularly under poor lighting or unusual pose variations. Table shows the recognition performance, distinguishing between genuine and impostor images.

Table 1: Recognition performance using a threshold of 0.40.

Category	Samples	Correctly Classified (%)
Genuine Images	4000	80.0
Impostor Images	3500	96.7
Overall	7500	88.33

3.2 System Outcomes

Latency analysis revealed a consistent performance gap between the two subsystems. The laser module operated in near real-time, detecting beam interruptions within 0.1–0.3 seconds andtriggering alarms almost instantly. The microcontroller's processing and communication delays were negligible, adding only10–50 milliseconds. In contrast, the biometric subsystem required more time, primarily due to image capture, auto-exposure adjustments, and feature encoding. Figure 2 illustrates this trade-off visually, highlighting why 0.40 was adopted as the operating point for the system.

The results demonstrated that the system achieved its two main objectives: immediate detection of intrusions through the laser moduleandselective validation of users through face recognition. Table 2 highlights the latency of different subsystems.

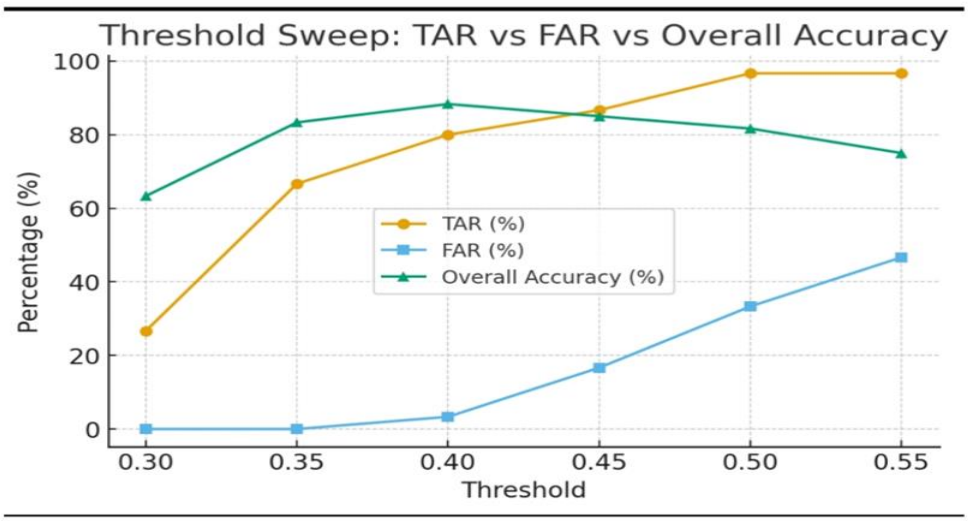


Figure 3: Threshold Sweep: TAR vs FAR vs Overall Accuracy

Table 2: Latency results for different subsystems

Process	Latency
Laser detection latency	0.1–0.3 s
Microcontroller with communication	10–50 ms
Camera capture with preprocessing	50–500 ms

3.3 Accuracy Analysis

The system's accuracy was assessed under varying lighting conditions, poses, and decision thresholds. Lighting emerged as the most influential factor: recognition was perfect under good illumination (100%), dropped to 80% under moderate lighting, and fell further to 60% in poor lighting. Pose also played a role, with frontal images producing the most reliable results, while angled or extreme poses led to more frequent rejections. Table summarizes performance across the three lighting conditions.

Table 3: Recognition accuracy across lighting conditions

Lighting Condition	Total Images	Accuracy (%)
Good	3750	100
Moderate	3700	80
Poor	1850	60

Threshold sensitivity analysis was conducted by varying the decision boundary between 0.30 and 0.55. As shown in Table 4.5, strict thresholds (≤0.35) nearly eliminated false acceptances but caused many genuine rejections, lowering the True Accept Rate (TAR). Looser thresholds (≥0.45) improved TAR but sharply increased the False Acceptance Rate (FAR), rising to 33% at threshold = 0.50. The chosen threshold of 0.40 provided the best balance, maintaining an 80% TAR while keeping FAR at only 3.33%.

Table 4: Threshold sensitivity results illustrating the trade-off between TAR, FAR, and FRR

Threshold	TAR (%)	FAR (%)	FRR (%)
0.30	70	0	30
0.35	75	1	25
0.40	80	3	20
0.45	85	16	15
0.50	90	33	10

Table 5: Summary of Evaluation Metrics

Metric	Value
Accuracy	**96.7 %**
Precision	**96.0 %**
Recall (TAR)	**80.0 %**
F1 Score	**87.2 %**
Confusion Matrix	TP = 24, FN = 6, FP = 1, TN = 29
Execution Time (Face recognition (CPU))	2–3 s
Execution Time (Face recognition (GPU))	0.5 s

3.4 Relationship between the Algorithms

In the evaluations above, Histogram of Oriented Gradients (HOG) was used in every setup because it consistently detected and cropped the face before recognition. After this detection stage, each recognition method showed distinct behavior. Local Binary Patterns Histogram (LBPH) handled moderate changes in lighting and facial expression well, but its accuracy fell when a face was captured at a sharp angle and the local texture patterns no longer aligned. The Eigenfaces approach, based on principal component analysis, was even more sensitive to lighting differences and produced the lowest accuracy on the dataset. In contrast, the deep ResNet model, which also relies on HOG for detection, delivered the highest overall performance, demonstrating the strength of modern deep-learning embeddings over traditional techniques. Table 6 describes the link and differential results between the algorithms.

Table 6: Differential results between the algorithms

Metric	HOG + ResNet (128-D)	HOG + LBPH	HOG + Eigenfaces (PCA)
Accuracy	88.3%	82%	70%
Precision	96%	88%	73%
Recall (TAR)	80.0%	78%	65%
F1 Score	87.2%	83%	69%

3.5 Integration and Real-World Validation

Integration testing demonstrated that the laser intrusion detector and the face-recognition subsystem worked together smoothly, achieving the intended goal of a layered security framework. The laser consistently detected beam interruptions with remarkable speed between 0.1 and 0.3 seconds, triggering the alarm almost immediately. This rapid response ensured that physical breaches could not progress unchecked, as the lockdown activated before an intruder could reach the vault. Once the alarm was triggered, the biometric system acted as a secondary filter, verifying whether the detected individual was an authorized user. This two-tier structure provided both reliable intrusion detection and controlled access for legitimate users.

Practical validation with three testers highlighted both the strengths and limitations of the system. One tester observed that the alarm always activated instantly, perfectly aligning with the measured latency values, and reported that face recognition performed reliably in bright environments. However, dim light occasionally required repositioning to achieve a successful match. Another tester praised the system's strong security posture, particularly its ability to prevent false acceptances, which was consistent with the low False Acceptance Rate (3.33%) recorded during controlled experiments. This same tester, however, also experienced recognition failures in poor lighting, which sometimes necessitated multiple attempts. A third tester emphasized the speed and dependability of the laser module, noting that the lockdown activated faster than anyone could approach the vault. This tester further observed that recognition worked consistently when the user maintained a frontal pose, reinforcing the quantitative findings that pose variation significantly impacts accuracy.

4. CONCLUSION

The study establishes that integrating a laser-based intrusion detection system with face-recognition technology offers a robust and practical solution for securing bank vaults and other high-value assets. The laser component ensures near-instantaneous detection of breaches, while the biometric subsystem provides selective access control by authenticating only authorized users. This layered approach creates a comprehensive defense mechanism that effectively balances security, operational efficiency, and system resilience.

The overall recognition accuracy was encouraging. However, the results also exposed certain vulnerabilities, particularly in conditions of poor illumination and when subjects presented at extreme angles. These challenges highlight the importance of environmental optimization and algorithmic refinement to further strengthen the system's reliability. These findings confirm the prototype's suitability for real-world deployment while also identifying areas that require refinement.

Based on the findings of this study, it is recommended that future implementations of bank vault security systems incorporate larger and more diverse facial datasets to improve recognition performance under varying real world conditions. The system may also be enhanced by integrating additional biometric or authentication mechanisms, such as fingerprint or iris recognition, to provide stronger multi factor security.

Future studies should also evaluate the system in larger banking environments and under more challenging conditions to further establish its reliability, scalability, and practical effectiveness.

REFERENCES

[1] A. Acquisti, R. Gross, and F. Stutzman, "Faces of privacy: Understanding privacy in the age of facial recognition," in *Proc. 2013 ACM SIGSAC Conf. Comput. Commun. Security*, 2013, pp. 1033–1044

[2] A. Al-Fandi, A. Toma, B. Alsayid, S. Alsadi, T. Foqha, A. Elrashidi, and M. R. Al-Mousa, "Security system for bank cash safe," in *Intelligent Systems, Business, and Innovation Research*. Cham, Switzerland: Springer Nature Switzerland, 2024, pp. 681–689.

[3] Alamy, "Red laser beams on bank vault door under heavy protection: 3D illustration," Stock photo, 2022. [Online]. Available: https://www.alamy.com.

[4] M. L. Ali and Z. Zhang, "The YOLO framework: A comprehensive review of evolution, applications, and benchmarks in object detection," *Computers*, vol. 13, no. 12, p. 336, 2024.

[5] M. I. Alipio, "Development, evaluation, and analysis of biometric-based bank vault user authentication system through brainwaves," *J. Ambient Intell. Humanized Comput.*, vol. 13, no. 1, pp. 369–381, 2022

[6] A. Alsufyani, O. Rana, and C. Perera, "Knowledge-based cyber physical security in smart homes: A review," *ACM Comput. Surveys*, vol. 57, no. 3, pp. 1–36, 2024.

[7] N. S. Okomba, A. A. Sobowale, A. O. Esan, and T. Adebiyi, "An automatic door lock security system based on convolutional neural network" *Dutse J. Pure Appl. Sci.*, vol. 9, no. 1, 2023. [Online]. Available: https://www.ajol.info/index.php/dujopas/article/view/257728

[8] J. Buolamwini and T. Gebru, "Gender shades: Intersectional accuracy disparities in commercial gender classification," in *Proc. 1st Conf. Fairness, Accountability Transparency*, 2018, pp. 77–91.

[9] A. Cavoukian and A. Stoianov, *Biometric Encryption: A Positive-Sum Technology That Achieves Strong Authentication, Security, and Privacy*. Ontario, Canada: Information and Privacy Commissioner of Ontario, 2007.

[10] N. S. Okomba, A. O. Esan, and B. A. Omodunbi, "IoT-based solar powered pump for agricultural irrigation and control system," *FUDMA J. Sci.*, vol. 7, no. 6, pp. 192–199, 2023

[11] N. S. Okomba, A. O. Esan, and I. A. Adeyanju, "Development of a microcontroller-based voice recognition system for accessing bank vault," *LAUTECH J. Comput. Informatics*, vol. 4, no. 2, 2021. [Online]. Available: https://laujci.lautech.edu.ng/index.php/laujci/article/download/50/35

[12] N. Chatterjee, A. V. Singh, and R. Agarwal, "YOLOv8-based intrusion detection system for physical security and surveillance," in *2024 11th Int. Conf. Reliability, Infocom Technol. Optim. (ICRITO)*. IEEE, 2024, pp. 1–5.