International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 13 Issue: 06 | Jun 2026 www.irjet.net p-ISSN: 2395-0072

FAUD DETECTION IN CREDIT CARD WITH FACIAL BIOMETRIC

Sripriyan S, Sankara Narayan S T

[12]*Department of Cyber Forensics & Information Security Dr MGR Educational and Research Institute, Tamil Nadu, Chennai, India*

Abstract – *Credit card fraud has become one of the most pressing challenges in today's digitally connected world. As e-commerce continues to grow and online transactions become routine, fraudsters have evolved their tactics well beyond simple card theft exploiting vulnerabilities in authentication systems, intercepting sensitive data, and bypassing static verification methods. This paper presents a secure credit card transaction system that addresses these threats by integrating facial biometric authentication using the Grass man algorithm. Rather than relying on passwords, PINs, or one-time codes that can be stolen or intercepted, the proposed system captures and verifies the user's facial image in real time during every transaction, comparing it against a pre-enrolled biometric profile. The Grass man algorithm improves recognition robustness by representing facial features in a mathematical subspace framework, enabling accurate identification even under varying lighting conditions, facial expressions, and head orientations. Every verified transaction is recorded in a secure database with encrypted storage to prevent tampering. The result is an authentication framework that is simultaneously more secure and more user-friendly eliminating the cognitive burden of credential management while providing a proactive, identity-grounded barrier against unauthorized payments.*

Key Words: Credit Card Fraud, Grass man Algorithm, Facial Recognition, Biometric Authentication, Secure Transactions, Real-Time Verification, AES Encryption, E-Commerce Security, Identity Verification, MySQL

1. INTRODUCTION

The explosion of digital commerce over the past decade has fundamentally changed how people pay for goods and services. Online transactions are now a daily reality for billions of users worldwide, and credit cards remain the dominant payment instrument powering this ecosystem. Yet this convenience carries a hidden cost: every transaction represents an opportunity for fraud, and the tools available to bad actors have grown more sophisticated in parallel with the technology meant to stop them.

Traditional authentication mechanisms passwords, PINs, and CVV codes were designed for a different era. They share a common vulnerability: they authenticate knowledge, not identity. A fraudster who obtains a cardholder's credentials through phishing, skimming, or data breaches can impersonate that cardholder with complete success, because the system has no way to verify who is actually sitting at the keyboard. One-time passwords add a layer, but they too can be intercepted or socially engineered.

Biometric authentication offers a fundamentally different approach. By tying verification to a physical characteristic unique to the individual their face, fingerprint, or iris the system authenticates the person rather than their credentials. Facial recognition has emerged as the most practical biometric for digital payment contexts, requiring only a front-facing camera and no physical contact with a sensor.

This project introduces a secure credit card transaction platform that uses the Grass man algorithm for facial recognition. The Grass man approach represents facial features as subspaces on a mathematical manifold, achieving recognition accuracy that is substantially more robust than pixel-based methods particularly in real-world conditions involving inconsistent lighting, varied expressions, and natural head movement. When a user initiates a payment, the system captures their live facial image and verifies it against their enrolled biometric profile before any transaction is authorized. Unauthorized users regardless of whether they hold the physical card or know the PIN are blocked at this stage.

The sections that follow cover the problem in depth, examine the limitations of existing approaches, detail the proposed system design, describe its architectural components, and present the testing methodology and results that validate its effectiveness.

2. SYSTEM ANALYSIS

2.1 Problem Definition

The rapid expansion of digital banking, online retail, and contactless payment infrastructure has made credit cards indispensable and correspondingly attractive to fraudsters. Despite significant investment in security technology, the authentication methods most widely deployed today suffer from a structural flaw: they verify what a person knows, not who they are.
Passwords and PINs can be guessed, phished, or stolen. CVV codes are exposed whenever a physical card is lost or a

database is compromised. OTPs are vulnerable to SIM-swap attacks and man-in-the-middle interception. Even in combination, these methods cannot definitively answer the only question that really matters in fraud prevention: is the person initiating this transaction the person whose name is on the card?

Beyond authentication, existing systems suffer from a reactive posture. Fraud detection mechanisms typically operate after the fact, flagging suspicious patterns in transaction histories or triggering alerts when spending behaviour deviates from a baseline. By the time a fraudulent transaction is identified, the financial damage is often already done and reversal is uncertain.

Centralized transaction records stored without robust access controls are attractive targets for attackers. Conventional face recognition systems compound the problem with their own limitations standard methods often fail when image conditions are imperfect, reducing the practical reliability of biometric controls in real deployment environments. These combined weaknesses create a meaningful gap in digital payment security that requires a fundamentally different authentication paradigm.

2.2 Existing System

Current credit card transaction systems rely on a layered stack of authentication measures: card numbers and expiry dates for basic identification, CVV codes for card-present verification, PINs for in-person transactions, and OTPs delivered by SMS or email for online purchases. While this combination provides a baseline of protection, it is increasingly inadequate against the threat landscape that contemporary fraudsters operate within.

None of these methods verify physical identity. A stolen card, combined with a phished OTP, is sufficient to authorize a transaction in most systems today. Fraud detection in existing systems is predominantly reactive anomaly detection algorithms scan for unusual spending patterns, but they operate on statistical models that require time to trigger and generate significant false positive rates that frustrate legitimate users. The disadvantages of existing approaches can be summarized as follows:

- **Credential Vulnerability:** PINs, passwords, and OTPs are all susceptible to theft, phishing, or interception, providing fraudsters with a clear pathway to account takeover.
- **Reactive Detection:** Fraud is typically identified only after a transaction completes, by which time financial damage has already been done.
- **No Physical Identity Verification:** No mechanism exists to confirm that the person presenting credentials is the legitimate cardholder.
- **User Friction:** Complex authentication flows slow transaction completion and reduces user satisfaction.

2.3 Proposed System

The proposed system addresses these weaknesses by placing facial biometric verification at the center of the payment authorization flow. Every transaction requires the user to pass a real-time facial recognition check before payment is processed. The system captures a live facial image through the device camera, processes it using the Grass man algorithm, and compares the result against the user's enrolled biometric profile stored in the database. Only a verified match authorizes the transaction to proceed.

The Grass man algorithm's subspace-based recognition approach provides reliable accuracy even in non-ideal imaging conditions, making the system practical for real-world deployment. Encrypted storage protects all biometric and transaction data at rest. Real-time monitoring flags anomalous behavior immediately, enabling proactive rather than reactive fraud prevention. The advantages of this approach include:

- **Identity-Level Security:** Facial recognition ensures that only the genuine cardholder can authorize transactions, regardless of credential theft.
- **Real-Time Authorization:** Verification occurs at the moment of the transaction, blocking fraud before it occurs rather than detecting it afterward.
- **Simplified User Experience:** Biometric authentication eliminates the need to remember passwords, PINs, or wait for OTPs.
- **Encrypted Data Protection:** All sensitive user information and transaction records are stored with encryption, protecting against database breaches.

3. REQUIREMENTS SPECIFICATION

3.1 Hardware Specification

Processor : Dual Core, 2.6 GHz
RAM : 4 GB
Hard Disk : 320 GB
Compact Disk : 650 MB
Keyboard : Standard Keyboard
Monitor : 15-inch Colour Monitor

3.2 Software Specification

Operating System : Windows OS
Front End : HTML, CSS, JavaScript
Back End : Python 3.x
Database : MySQL Server
IDE : Python IDLE

4. DESIGN AND IMPLEMENTATION

4.1 Architecture Diagram

The system architecture provides the conceptual blueprint from which all design and implementation decisions flow. It defines the major structural components, their relationships, and the data pathways that connect them. The architecture is organized into three primary tiers: a presentation layer accessed by users and administrators through a web interface; an application layer that handles authentication, session management, and business logic; and a data layer that maintains encrypted records of users, products, transactions, and biometric templates.

At the core of the architecture sits the facial recognition module. Every payment flow routes through this component before reaching the payment processing engine. The primary system actors and their interactions are as follows: the Administrator manages products, employees, bookings, and user accounts; the User registers, browses products, initiates purchases, completes facial recognition, and processes payments; and the Database persists all system state with encrypted storage for sensitive fields.

4.2 Data Flow Diagram

The data flow diagrams describe how information moves through the system at increasing levels of detail. At the context level (Level 0), the system is represented as a single process that receives inputs from the Administrator and User actors and persists results to the Database, with all data flows carrying only encrypted or validated content.

At Level 1, the context process decomposes into its principal sub-processes: Admin Login handles administrative authentication; Add Product manages the product catalogue; Store the Data writes validated records to persistent storage; and Retrieve the Data responds to query requests from both actor types.

Level 2 expands the user-facing transaction flow into finer sub-processes: Enrolment captures and stores the user's biometric profile during registration; Product Purchase manages the shopping cart and order creation; Face Recognize performs the Grass man-based identity verification; and Billing Process finalizes payment and records the transaction. Each sub-process has clearly defined input and output data flows to and from the Database.

4.3 Use Case Diagram

The use case diagram captures the functional scope of the system from the perspective of its actors. The Administrator Interacts with five primary use cases: Login, Add Employee, Add Product, View Booking Details, and View User Details. The User interacts with six use cases: Register, Login, Purchase Product, Face Recognition, Make Payment, and View Order History. The Face Recognition use case is a precondition of the Payment use case, reflecting the dependency that payment authorization has on successful biometric verification.

4.4 Collaboration Diagram

The collaboration diagram illustrates the sequence of object interactions that occur during a payment transaction. The User object initiates the sequence by triggering the Product Purchase use case. The system creates a Booking Record and transitions to the Payment Module, which calls the Face Recognition Module. The Face Recognition Module queries the Biometric Database, applies the Grass man algorithm, and returns a match or no-match result. On a successful match, the Payment Module confirms the transaction. On failure, the module increments the failed-attempt counter and, after three consecutive failures, invokes the Card Block routine.

4.5 Database Design

The database consists of seven normalized tables hosted on MySQL Server with encryption applied to sensitive fields. The principal table structures are defined as follows.

Table 1: regtb User Registration Table

Field	Type	Constraints
id	BIGINT	NOT NULL, PRIMARY KEY
Firstname	NVARCHAR(50)	NULL
Lastname	NVARCHAR(50)	NULL
Gender	NVARCHAR(50)	NULL
Age	NVARCHAR(50)	NULL
Mobile	NVARCHAR(50)	NULL
Email	NVARCHAR(50)	NULL
Address	NVARCHAR(50)	NULL
Username	NVARCHAR(50)	NULL
Password	NVARCHAR(50)	NULL
Status	NVARCHAR(50)	NULL

Table 2: Protb - Product Table

Field	Type	Constraints
id	BIGINT	NOT NULL, PRIMARY KEY
Company	NVARCHAR(50)	NULL
ProductType	NVARCHAR(50)	NULL
ProductName	NVARCHAR(50)	NULL
Price	NVARCHAR(50)	NULL
About	NVARCHAR(50)	NULL
Image	NVARCHAR(50)	NULL

Table 3: booktb - Booking / Transaction Table

Field	Type	Constraints
id	BIGINT	NOT NULL, PRIMARY KEY
UserName	NVARCHAR(50)	NULL
BookingId	NVARCHAR(50)	NULL
Qty	DECIMAL(18,0)	NULL
Amount	DECIMAL(18,0)	NULL
CardType	NVARCHAR(50)	NULL
CardNo	NVARCHAR(50)	NULL
CvNo	NVARCHAR(50)	NULL
Date	NVARCHAR(50)	NULL

Table 4: carttb - Shopping Cart Table

Field	Type	Constraints
id	BIGINT	NOT NULL, PRIMARY KEY
UserName	NVARCHAR(50)	NULL
ProductName	NVARCHAR(50)	NULL
Price	DECIMAL(18,0)	NULL
Qty	DECIMAL(18,0)	NULL
Tprice	DECIMAL(18,0)	NULL
Image	NVARCHAR(50)	NULL
Status	NVARCHAR(50)	NULL
Date	NVARCHAR(50)	NULL
Company	NVARCHAR(50)	NULL
BookingId	NVARCHAR(50)	NULL

5. TESTING

5.1 Introduction

Testing is a structured, systematic process that validates whether the system behaves as intended across a comprehensive range of inputs, conditions, and usage scenarios. For a security-critical application like this one where authentication failures can result in fraudulent financial transactions rigorous testing is not optional. The testing objectives are threefold: to uncover defects before deployment; to verify that all functional specifications are correctly implemented; and to confirm that non-functional requirements for performance, security, and reliability are met under realistic operating conditions.

5.2 Types of Testing

Unit testing validates each individual module in isolation. Functional Testing verifies that collections of related modules interact correctly. Integration Testing examines the handoffs between the authentication layer, face recognition engine, and payment processor. White Box Testing confirms that all internal decision paths are exercised correctly. Black Box Testing validates system behavior from the user perspective. System Testing evaluates the fully integrated application against its complete requirements specification. Validation Testing confirms that the system satisfies the stated business objectives. Acceptance Testing evaluates usability, reliability, and overall satisfaction in realistic usage scenarios.

5.3 Test Cases

Table 5: Test Cases Summary

S.No	Scenario	Input	Expected Output	Actual Output
1	Admin Login	Username & Password	Dashboard access	Login successful
2	User Registration	Personal details	Account created	Stored in database
3	User Login	Username & Password	Home page	Login successful

4	Face Recognition — Authorized	Enrolled user image	Auth passed	Transaction authorized
5	Face Recognition — Unauthorized	Unknown user image	Auth failed	Transaction blocked
6	Payment with Correct PIN	Card no. + correct PIN	Payment processed	Transaction confirmed
7	Card Block after 3 Failures	Incorrect PIN x3	Card blocked	Status set to Blocked

5.4 Test Data

The testing process made use of a comprehensive dataset designed to exercise every module under both normal and edge-case conditions. User registration test data included accounts with varied personal details, duplicate entries to trigger validation rejection, and intentionally malformed inputs to test error handling. The biometric test dataset consisted of facial images of enrolled users captured under multiple lighting conditions, with different expressions and head orientations, alongside images from non-enrolled individuals to test unauthorized access rejection.

Payment module test data included valid card information paired with correct PINs, valid card numbers with incorrect PINs, expired card details, and invalid entries. Multiple consecutive failed authentication attempts were used to verify the card-blocking mechanism. Transaction records were reviewed after testing to confirm that all confirmed payments were correctly persisted and no fraudulent transactions appeared in the booking database.

5.5 Test Report

All primary modules passed their respective test cases with the expected results. The registration module correctly stored valid user records and rejected incomplete or duplicate entries. The face recognition module demonstrated strong performance across varied image conditions: enrolled users were correctly identified in all high-quality image scenarios and in the majority of challenging conditions.

Unauthorized users were consistently rejected. Integration testing confirmed that the face recognition result correctly gates the payment flow no payment was processed in any test case where facial verification failed. The card-blocking mechanism triggered correctly after three consecutive failed PIN entries. The overall test results validate that the system achieves its core objectives of fraud prevention, accurate biometric authentication, and secure transaction processing.

6. SYSTEM IMPLEMENTATION

6.1 Module Descriptions

The system is organized into two primary role contexts Administrator and User each exposing a set of purpose-built modules.

- **Admin Login:** Provides secure credential-based access to the administrative interface. Session management ensures that administrative privileges persist only for the duration of an authenticated session.
- **Add Employee / Product:** Enables administrators to maintain the product catalogue and employee records. All entries are validated before storage to prevent duplicate or malformed records.
- **View Booking Details:** Presents a consolidated view of all purchase transactions, including booking identifiers, product information, user identity, payment status, and transaction dates.
- **View User Details:** Provides centralized access to the registered user database, supporting search, filter, and account management operations.
- **User Registration:** Captures personal details and creates a new account after validation. The module prevents duplicate registrations and provides clear feedback on entry errors.
- **User Login:** Authenticates registered users using username and password with session state established on successful login.
- **Product Purchase:** Allows users to browse the product catalogue, review item details, and add items to a shopping cart. Order placement triggers the payment flow.
- **Face Recognition:** Captures a live facial image from the user's camera and compares it against the stored biometric profile using the Grass man algorithm. A match authorizes payment; a mismatch blocks the transaction and logs the attempt.
- **Make Payment:** Collects payment card details and processes the transaction following successful biometric verification. Cards are automatically blocked after three consecutive failed PIN entries.

6.2 Grass man Algorithm

The Grass man algorithm is the mathematical engine at the heart of the system's biometric authentication capability. It belongs to a class of methods known as subspace-based recognition, which represent complex, high-dimensional data such as a facial image as points on a lower-dimensional geometric structure called the Grass man manifold. Each facial image is transformed into a subspace representation that captures the essential geometric relationships between

facial features while discarding noise and irrelevant variation.

During enrolment, the user's facial images are processed and their subspace representations are stored in the biometric database. During a transaction, the system captures a live facial image, computes its subspace representation, and measures the geometric distance between the live subspace and the stored template on the Grass man manifold. This distance metric quantifies similarity in a mathematically principled way unlike pixel-by-pixel comparison, it is inherently robust to variation in lighting, expression, and head angle.

If the computed distance falls below a predefined threshold, the faces are deemed to match and the user is authenticated. If the distance exceeds the threshold, authentication fails and the transaction is blocked. The practical significance of this approach is its robustness: standard recognition methods degrade sharply under real-world imaging conditions, while the Grass man method maintains high accuracy across exactly these conditions which are unavoidable in real-world online payment scenarios.

7. CONCLUSION AND FUTURE WORK

7.1 CONCLUSION

This paper has presented a secure credit card fraud detection and transaction authorization system that addresses the fundamental vulnerability of contemporary payment authentication: the reliance on credentials rather than identity. By integrating Grass man algorithm-based facial recognition into the payment flow, the system ensures that every transaction is authorized by the genuine cardholder not simply by someone who possesses their card details.

The Grass man algorithm's subspace representation delivers recognition accuracy that holds up under real-world imaging conditions, making the system practically viable. Testing validated that the system correctly authenticates enrolled users, blocks unauthorized access attempts, and prevents payment processing when biometric verification fails. The card-blocking mechanism adds a secondary layer of protection against brute-force PIN attacks. Overall, the system demonstrates that identity-level authentication is both technically achievable and practically deployable in a digital payment context.

7.2 FUTURE WORK

Several promising directions exist for extending the capabilities of this system. The most impactful near-term enhancement would be the integration of deep learning techniques alongside the Grass man approach. Convolutional neural network architectures trained on large facial datasets have demonstrated state-of-the-art performance under extreme conditions severe occlusion, aging, and very low light that remain challenging for subspace methods alone. Multi-modal biometric authentication represents another high-value extension. Supplementing facial recognition with fingerprint or iris verification would create a multi-factor biometric system, particularly valuable for high-value transactions. On the infrastructure side, replacing the centralized database with a block chain ledger for transaction records would provide immutability and tamper-evidence properties highly desirable in financial contexts. Mobile platform optimization and post-quantum cryptography integration should also be considered as medium-term priorities.

ACKNOWLEDGEMENT

The authors gratefully acknowledge the guidance of faculty advisors and peer reviewers at Dr.MGR Educational and Research Institute whose feedback shaped this work. The open-source communities behind Python, Flask, MySQL, and the mathematical libraries underlying the Grass man implementation provided foundational tools without which this project would not have been possible.

REFERENCES

[1] Heinold, B., "A Practical Introduction to Python Programming," 2021.

[2] Kneusel, R. T., Practical Deep Learning: A Python-Based Introduction. No Starch Press, 2021.

[3] Dhruv, A. J., Patel, R., and Doshi, N., "Python: The Most Advanced Programming Language for Computer Science Applications," Science and Technology Publications, 2021, pp. 292-299.

[4] Sundnes, J., Introduction to Scientific Programming with Python. Springer Nature, 2020.

[5] Hill, C., Learning Scientific Programming with Python. Cambridge University Press, 2020.

[6] Turk, M. and Pentland, A., "Eigenfaces for Recognition," Journal of Cognitive Neuroscience, vol. 3, no. 1, pp. 71-86, 1991.

[7] Hamm, J. and Lee, D. D., "Grassmann Discriminant Analysis: A Unifying View on Subspace-Based Learning," Proc. 25th ICML, 2008.

[8] Zhao, W., Chellappa, R., Phillips, P. J., and Rosenfeld, A., "Face Recognition: A Literature Survey," ACM Computing Surveys, vol. 35, no. 4, pp. 399-458, 2003.

[9] Li, S. Z. and Jain, A. K., Handbook of Face Recognition. Springer, 2011.

[10] Zhang, J. and Yuen, P. C., "Grass mannian Learning for Facial Expression Recognition," IEEE Trans. Neural Netw. Learn. Syst., 2018.

[11] Python Software Foundation, Python Language Reference. Available: https://www.python.org/

[12] Flask Documentation, Pallets Projects. Available: https://flask.palletsprojects.com/

[13] MySQL Documentation, Oracle Corporation. Available: https://dev.mysql.com/doc/

[14] https://medium.com/javarevisited/10-free-python-tutorials-and-courses-from-google-microsoft-and-coursera-for-beginners-96b9ad20b4e6 https://realpython.com/