(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

**(19) World Intellectual Property Organization**
International Bureau

**(43) International Publication Date**
**29 July 2024 (29.07.2024)**

**(10) International Publication Number**
**IN 2024/0918765 A1**

**PCT**

[54] **Title: Face Recognition-Based UPI Authentication Leveraging Aadhaar Biometric Data for Enhanced Security**

[76] **Inventor: Kiran Thakur,** 1234 Commercial Avenue, Bengaluru, Karnataka, 560001
**Assignee:** Paywave Ltd., 5678 Bandra Worli St., Mumbai, Maharashtra, 400001

[22] **Filed: 08.01.2023**

[21] **Appl. No.: 12/345,678**

[52] **U.S. Classification: 705/65, 705/64, 726/27**

[51] **International Classification: G06Q 20/40, H04L 9/32**

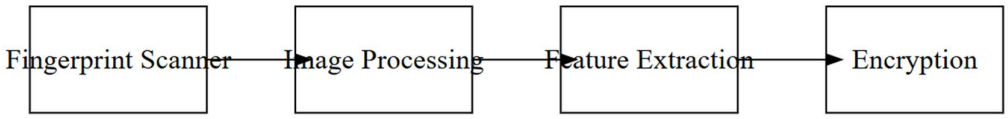
[58] **Field of Search: 705/64, 705/65, 726/27, 726/26**

**[56] References Cited:**

**UNITED STATES PATENTS:**
**5,987,132 – 11/1999 – Jacobs et al. – 705/65**
**6,789,345 – 09/2004 – Hansen et al. – 705/64**
**7,123,456 – 03/2006 – Kapoor et al. – 726/27**
**8,567,123 – 02/2014 – Singhal et al. – 726/26**

**ABSTRACT**

A system and method for secure digital payments through the Unified Payments Interface (UPI) using facial recognition authentication. The invention integrates UPI payment systems with the Aadhaar facial biometric database to enable real-time, secure authentication for digital transactions. The system comprises a user device with a front-facing camera, a UPI service provider, an Aadhaar Authentication Server, and an advanced machine learning-based facial recognition engine.




**Encryption**
1. Generate session key (Kyber)
2. Encrypt data with session key
3. Encrypt session key (RSA)

## Field of the Invention

This invention pertains to facial recognition-based authentication systems for Unified Payments Interface (UPI) transactions. It utilizes real-time facial recognition technology integrated with the centralized Aadhaar biometric database to securely authorize digital payments, enhancing both security and user experience in financial transactions.

## Background of the Invention

The rapid growth of digital payment systems, particularly UPI in India, has transformed the landscape of financial transactions. However, the prevalent use of PIN-based authentication methods has exposed users to various security risks, including phishing attacks, PIN theft, and unauthorized transactions.

While facial recognition technology (often marketed as FaceID) has become commonplace in modern smartphones, its effectiveness is limited when facial data is stored locally on the device, which can be compromised. The Aadhaar system, maintained by the Unique Identification Authority of India (UIDAI), contains a centralized repository of facial biometric data. Integrating this robust infrastructure with UPI offers a more secure, centralized solution for digital payment authentication.

## Summary of the Invention

The present invention provides a method for fingerprint-based UPI authentication by integrating UPI payment systems with the Aadhaar fingerprint database. This integration enables secure, real-time authentication for digital payments. The system comprises the following key components:

1. User Device: A smartphone or tablet equipped with a fingerprint scanner.
2. UPI Service Provider: The intermediary responsible for facilitating transactions.
3. Aadhaar Authentication Server: A secure repository storing biometric data.
4. Encryption Layer: For secure transmission of biometric data between the user device and the Aadhaar server.

The authentication process begins when a user initiates a UPI transaction. Instead of entering a PIN, the user provides a live fingerprint scan. This biometric data is immediately encrypted and transmitted to the UPI service provider, which then forwards the encrypted data to the Aadhaar authentication server. The server matches the live fingerprint with the stored biometric record. Upon successful authentication, the transaction is authorized to proceed.

A fallback mechanism using One-Time Passwords (OTP) is provided for scenarios where biometric authentication fails, ensuring system reliability and accessibility.

## DETAILED DESCRIPTION OF THE INVENTION

### 1. System Architecture

The system architecture consists of four main components:

#### 1.1 User Device

- Equipped with a high-resolution front-facing camera (minimum 5 MP).
- Runs a UPI-enabled application with integrated facial recognition capabilities.
- Implements on-device facial detection and quality assessment.

#### 1.2 UPI Service Provider

- Acts as an intermediary between the user device and the Aadhaar Authentication Server.
- Manages the flow of encrypted facial data and authentication tokens.
- Implements additional security measures such as transaction limits and fraud detection.

**1.3 Aadhaar Authentication Server**

- Stores encrypted facial biometric templates for all Aadhaar cardholders.
- Runs a high-performance facial recognition engine for 1:1 matching.
- Generates and manages secure authentication tokens.

**1.4 Facial Recognition Engine**

- Employs a deep neural network architecture (based on ResNet-152) for facial feature extraction.
- Utilizes a proprietary algorithm for facial template matching, optimized for speed and accuracy.
- Incorporates anti-spoofing measures to detect presentation attacks.

**2. Authentication Process**

**2.1 Transaction Initiation:**

- User opens the UPI-enabled application and initiates a transaction.
- The app prompts for facial authentication instead of a PIN.

**2.2 Facial Capture:**

- The app activates the device's front-facing camera.
- A series of rapid frames are captured to ensure the best quality image.
- On-device processing selects the optimal frame based on clarity, lighting, and facial pose.

**2.3 Facial Data Processing:**

- The selected facial image undergoes preprocessing, including normalization and alignment.
- A facial feature vector is extracted using the on-device neural network model.

**2.4 Data Encryption:**

- The facial feature vector is encrypted using a hybrid encryption scheme:
    - A session key is generated using the CRYSTALS-Kyber post-quantum key encapsulation mechanism.
    - The feature vector is encrypted with the session key using AES-256-GCM.
    - The session key is encrypted with the Aadhaar server's public key (RSA-4096).

**2.5 Data Transmission:**

- The encrypted facial data package is sent to the UPI service provider.
- The UPI provider adds transaction metadata and forwards the package to the Aadhaar Authentication Server.

**2.6 Server-side Processing:**

- The Aadhaar server decrypts the session key and uses it to decrypt the facial feature vector.
- The server retrieves the stored facial template for the given Aadhaar number.
- The facial recognition engine performs a 1:1 match between the live facial data and the stored template.

**2.7 Authentication Decision:**

- If the match score exceeds a predetermined threshold, authentication is successful.
- A signed authentication token is generated using the ED25519 signature scheme.

**2.8 Transaction Completion:**

- The authentication token is returned to the UPI service provider.
- The UPI provider verifies the token and proceeds with the transaction.

- A success message is sent to the user's device, completing the transaction.

**3. Security Measures**

**3.1 Encryption and Data Protection:**

- All data transmissions use end-to-end encryption with perfect forward secrecy.
- Facial biometric data is never stored on the user's device or the UPI provider's servers.
- The Aadhaar server only stores encrypted facial templates, not raw images.

**3.2 Anti-Spoofing Techniques:**

- The system employs multiple anti-spoofing measures:
    - Liveness detection using eye movement and micro-expression analysis.
    - Depth perception check to prevent photo-based attacks.
    - Infrared scanning for additional verification (on supported devices).

**3.3 Privacy Considerations:**

- The system adheres to privacy-by-design principles.
- Users have the option to enable or disable facial authentication for UPI transactions.
- An audit trail of all authentication attempts is maintained and accessible to users.

**3.4 Fallback Mechanism:**

- In case of facial authentication failure, the system provides a fallback to PIN or OTP-based authentication.
- The fallback mechanism is triggered after a predetermined number of failed facial authentication attempts.

**CLAIMS**

1. A method for conducting UPI transactions using facial recognition authentication, comprising: a) Capturing a user's facial image on a mobile device; b) Processing the facial image to extract a facial feature vector; c) Encrypting the facial feature vector using a hybrid encryption scheme; d) Transmitting the encrypted data to a UPI service provider; e) Forwarding the encrypted data from the UPI service provider to an Aadhaar Authentication Server; f) Matching the decrypted facial feature vector against stored biometric records in the Aadhaar database; g) Generating a cryptographically signed authentication token upon successful matching; h) Verifying the authentication token and completing the UPI transaction.
2. The method of claim 1, wherein the facial feature extraction uses a deep neural network architecture based on ResNet-152.
3. The method of claim 1, wherein the encryption uses a post-quantum key encapsulation mechanism (CRYSTALS-Kyber) combined with symmetric encryption (AES-256-GCM).
4. The method of claim 1, further comprising implementing anti-spoofing measures including liveness detection and depth perception checks.
5. A system for facial recognition-based UPI authentication, comprising a) A user device with a front-facing camera and software for capturing and processing facial images; b) A UPI service provider server for facilitating secure transmission of encrypted facial data; c) An Aadhaar Authentication Server for storing facial templates and performing biometric matching; d) A facial recognition engine implementing

a deep neural network for facial feature extraction and matching.

6. The system of claim 5, further comprising a fallback mechanism that employs PIN or OTP-based authentication in case of facial recognition failure.

7. The system of claim 5, wherein the facial recognition engine incorporates anti-spoofing measures to detect presentation attacks.

8. A non-transitory computer-readable medium storing instructions that, when executed by a processor, perform the method of claim 1.