Communications on Applied Nonlinear Analysis
ISSN: 1074-133X
Vol 33 No. 1s (2026)

AI-Driven Multimodal Fraud Detection Framework for UID Aadhaar e-KYC Using Biometric and Document Verification

Dr. N. Murali Krishna[1], Chandana Chintanippu[2], Shaik Azeem[3], and Boddu Krupa[4]

[1] Professor, Department of Artificial Intelligence and Data Science, Vignan Institute of Technology and Science, Deshmukhi, Yadadri Bhuvanagiri, Telangana, India

Email: muralinamana@gmail.com

[234] Department of Artificial Intelligence and Data Science, Vignan Institute of Technology and

Science, Deshmukhi, Yadadri Bhuvanagiri, Telangana, India

Email: chandanachintanippu@gmail.com, azeemshaik8074@gmail.com, boddukrupa17@gmail.com

Article History:

Received: 04-02-2026

Revised: 20-03-2026

Accepted: 10-04-2026

Abstract:
Electronic Know Your Customer verification is widely used in banking, government services, and digital platforms to verify user information during digital onboarding. However, most verification methods in use today are based on manual document verification or partially automated verification techniques, which may be time-consuming and prone to identity fraud. This paper proposes an AI-powered multimodal fraud detection framework for Aadhaar Card-based Electronic Know Your Customer verification. The framework is based on integrating document verification, biometric verification, and machine learning for fraud detection. The framework employs Optical Character Recognition technology for verification using user-provided Aadhaar Card images and biometric fingerprint verification for user identification. The extracted user information is further validated through registry cross-checking and One-Time Password email verification. Furthermore, a machine learning algorithm is also used to evaluate the verification process for fraud based on the outcomes of Optical Character Recognition technology, biometric fingerprint verification, and email verification. Additionally, an administrative interface is also proposed for monitoring verification records, fraud patterns, and authentication statistics. The experimental results demonstrate the effectiveness of the proposed framework in ensuring the reliability of verification and reducing fraud in digital identity verification systems.

Keywords: e-KYC, Aadhaar Verification, Optical Character Recognition, Biometric Authentication, Fraud Detection, Digital Identity Verification.

Introduction

Electronic Know Your Customer (e-KYC) solutions have been popularly used to verify user identities for banking, government, and other online services. As more services go online, there is a need to develop effective ways of authenticating users during remote identity verification. Traditionally, identity verification services have focused mainly on manual verification, where identity documents presented by users are scrutinized by relevant authorities. However, this process is often time-consuming, expensive, and becomes a problem when many users need to undergo verification at the same time. Furthermore, online services face problems such as fake

identity documents, duplication of identities, and identity theft, which have resulted in identity verification system fraud [1][4].

Recent developments in artificial intelligence, computer vision, and biometric identification have enabled the creation of automated identity verification systems. Optical Character Recognition (OCR) techniques have enabled identity verification systems to use machine-readable identity documents, where textual information is directly read from identity documents using OCR techniques. This reduces the time required to verify identities, making identity verification processes more efficient [6]. Biometric identification techniques, such as fingerprint identification, verify individuals using their unique physiological characteristics, thus enhancing security in identity verification systems [7].

The key contribution of this work is the integration of OCR-based document verification, biometric fingerprint authentication, registry validation, and machine learningbased fraud detection into a unified multimodal e-KYC verification framework.

1 Related Work

Recent advancements in the development of digital identity verification technologies have improved the efficiency and security of Electronic Know Your Customer (e-KYC) systems. Traditional KYC processes involved the verification of documents and physical presence along with the exchange of a number of papers. These processes were time-consuming and led to an increase in the cost of operations. Moreover, the chances of fraud were also high. In this context, modern Electronic Know Your Customer processes are increasingly using the services of automated technologies such as biometrics and Optical Character Recognition (OCR) for the efficient verification of identities [1][4].

The first form of digital identity verification was based on the verification of documents and the use of passwords. However, such processes are easily susceptible to identity theft and other types of attacks. In this context, the concept of biometrics has been introduced as a part of the Electronic Know Your Customer processes. Biometrics uses fingerprint recognition, facial recognition, and iris scans for the efficient verification of identities. Biometrics is considered more reliable than other types of verification processes [7].

A number of studies have been conducted with the objective of exploring the use of different approaches for the development of Electronic Know Your Customer processes. For instance, Alwahaishi and Zdrálek have emphasized the importance of biometric verification for the improvement of the security of digital platforms [5]. Verma et al. proposed a paperless Electronic Know Your Customer framework based on the use of OCR and facial recognition for the efficient verification of identities[4]. Similarly, Karmoker et al. proposed a blockchain-based Electronic Know Your Customer framework for the efficient sharing of verified identities among different organizations [3].

2.1 Literature Review

Recent trends in digital identity verification have been based on biometric authentication and intelligent technologies to provide security and reliability to e-KYC systems. Jena et al. have proposed a multimodal biometric authentication system that uses fingerprint and facial recognition technologies to provide reliable identity verification systems. The proposed system uses deep learning models based on pre-trained CNN architectures to provide reliable identity

verification systems. It has been shown that multimodal biometric systems provide better security and reliability compared to single biometric systems [2].

Vadali et al. have proposed a secure identity verification framework for e-KYC systems that use computer vision and blockchain technologies for digital identity management systems. The proposed system supports Aadhaar-based authentication and facial recognition using techniques such as Histogram of Oriented Gradients (HoG) and convolutional neural networks. The proposed system ensures secure identity records by using blockchain technology [1].

From the above paragraphs, it is clear that a combination of biometric authentication systems, OCR-based document analysis systems, and identity management systems provide better reliability to digital identity verification systems.

Although various solutions have been proposed to use biometric and blockchain technology to verify an individual's identity, most existing solutions use limited verification mechanisms. In this regard, the proposed system uses OCR-based verification of Aadhaar documents, biometric fingerprint verification, database verification, and OTPbased verification of an email to develop a robust e-KYC system.

2 Proposed Methodology

The proposed framework for e-KYC ensures a secure route for automated identity verification and detection of fraud. It incorporates various technologies such as OCR, fingerprint biometric scanning, database registration checks, email verification via OTP, and machine learning-based detection of potential fraud. The entire process begins with a user uploading a picture of their Aadhaar card and a fingerprint scan using a user interface designed specifically for this process. OCR scanning is then implemented to identify and extract relevant information such as name, date of birth, and Aadhaar card number from the uploaded card image.

This information is then matched against user records in a database registration system to verify user identity. In addition to this, fingerprint scanning is implemented to verify user identity by matching it against a fingerprint database. Verification metrics such as fingerprint match score and OCR and database registration results are then analyzed by a potential fraud detection module to calculate the probability of potential fraud.

Finally, email verification using OTP is implemented by sending a one-time password to the user's registered email account to verify user identity and authenticity. Once this process is completed successfully, the identity information is stored in encrypted form in a database.

Methodology Steps

- The user has to upload three pieces of information using the verification interface. These are the Aadhaar card image, fingerprint image, and email address.
- The Aadhaar card image goes through the OCR process and obtains the identity information such as the user's name, Aadhaar number, and date of birth. This information is verified by cross-checking it with the registry information.
- The fingerprint goes through the verification process by comparing the fingerprint with the stored biometric information. This verifies the fingerprint.
- The verification metrics are generated. These include the similarity of the fingerprint and the confidence level of the OCR extraction.

- The fraud detection module verifies the information by comparing the verification information with the registry information and performing duplicate checks. This gives an idea of the chances of fraud.
- Another level of security is added by sending an OTP to the email address registered by the user for verification.
- The information is stored securely in the database after the verification process is completed using encryption.
- The verification information, fraud detection statistics, and system monitoring information are displayed on the dashboard for the administrator.

3.1 System Architecture

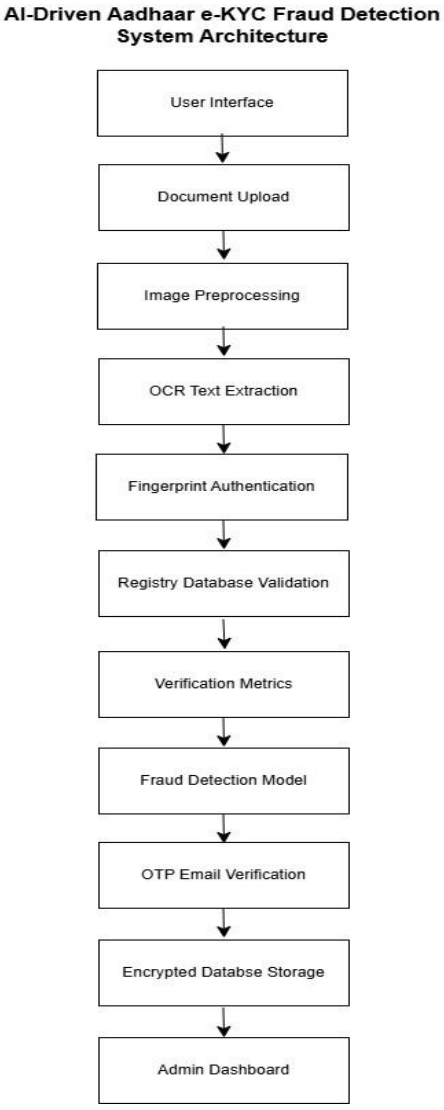


Fig. 1. System Architecture

The proposed AI-based Aadhaar eKYC fraud detection system comprises several modules, which are integrated with one another in order to complete the process of verification, authentication, fraud risk assessment, and storage of verified data in a secure manner. The architecture proposed in the paper incorporates the concepts of Optical Character Recognition,

fingerprint authentication, registry cross-referencing, fraud probability assessment, and OTP-based authentication.

Architecture Workflow

- User Interface: The user interface is the web interface through which the user enters the system, initiating the process of identity verification.
- Document Upload: The user needs to upload the image of the Aadhaar card, fingerprint image, and email address for verification.
- Image Preprocessing: The uploaded image is preprocessed, including image resizing, noise removal, etc.
- OCR Text Extraction: The Optical Character Recognition process identifies the details from the uploaded image, including name, date of birth, and Aadhaar number.
- Fingerprint Authentication: The fingerprint image is used for authentication of the user's identity.
- Registry Database Validation: The extracted data is validated with the registry data.
- Verification Metrics: The proposed architecture measures the verification metrics, including the confidence level of the Optical Character Recognition process, fingerprint score, and uniqueness of the data.
- Fraud Detection Model: The machine learning algorithm assesses the risk of fraud.
- OTP Email Verification: The user's email address is verified using the one-time password sent to the email.
- Encrypted Database Storage: The verified data is stored in the database with encryption.
- Admin Dashboard: The admin interface monitors the entire process, including verification, fraud, and the entire process.

3.2 Algorithm

The AI-powered Aadhaar e-KYC system follows a step-by-step process that ensures automatic identity verification and detection of fraudsters.

- **Step 1: Input Phase**

The user will be required to provide identity information by uploading a picture of the Aadhaar card, a fingerprint image, and an email address using the verification tool.

- **Step 2: Image Preparation**

The Aadhaar card image will be processed by adjusting its size, converting it into grayscale format, and reducing noise in the image to obtain accurate text from the image.

- **Step 3: Text Extraction using OCR**

Optical Character Recognition will be used to extract important information such as name, Aadhaar card number, date of birth, and gender from the uploaded image.

- **Step 4: Registry Cross-Check**

The obtained information will be checked against a database to confirm whether it matches records in the database.

- **Step 5: Biometric Fingerprint Check**

The uploaded fingerprint image will be matched against a database that contains fingerprint information to confirm whether it matches.

- **Step 6: Verification Metric Scoring**

Verification metrics will be calculated based on OCR results, fingerprint matching results, and checks for duplicate records.

- **Step 7: Fraud Analysis**

A machine learning model will be used to evaluate the results obtained from the previous step and estimate whether there is a high probability of fraud.

- **Step 8: OTP Verification using Email**

A one-time password will be sent to the registered email account, and the user will be required to enter the correct OTP.

- **Step 9: Secure Data Archiving**

The identity information will be stored in a database after a successful verification process.

- **Step 10: Monitoring and Outcome**

The final result will be displayed to the user, and administrative records will be updated with authentication and fraud detection results.

3 System Implementation and Results

The framework is designed to streamline the process of Aadhaar e-KYC verification by utilizing Python-based tools that integrate various aspects such as document verification, biometric authentication, fraud detection, and email verification into a single process.

The process works as follows:

The user is required to upload a photo of their Aadhaar card using the application's user interface. The application uses Optical Character Recognition to identify and extract important identity-related information such as name, date of birth, gender, and Aadhaar card number from the uploaded image.

For identity verification, a fingerprint scan is made and compared with a fingerprint template. The information obtained from the OCR process is also verified against a database to identify duplicates.

The framework uses a Random Forest classifier-based module for fraud detection that considers various factors such as OCR results, fingerprint matching, identity duplicates, and document validity. On the basis of this analysis, it predicts the probability and verifies whether it is a genuine or fraudulent transaction.

The framework also incorporates a process for email verification using OTP to verify whether the user has access to the registered email account or not. Once the process is completed successfully, the identity information is stored in a database in encrypted form. The framework also incorporates a module that allows administrators to monitor and track various aspects such as verification activity, fraud detection, and authentication trends.

4 Performance Evaluation

The effectiveness of the proposed AI-based Aadhaar e-KYC verification system is determined by how well it works, how reliable it is, and how well it can detect fraud. To carry out these tests, multiple Aadhaar document samples were fed into the verification system to determine how well the system could handle them. The system integrates OCR-based extraction from documents, fingerprint-based verification, registry verification, fraud probability, and email-based one-time password verification.

During the test phase, various identity verification scenarios were conducted to determine how well the system could extract data from Aadhaar documents, verify identity using fingerprints, and detect fraud. During these tests, the OCR system was successful in extracting key identity details such as name, date of birth, and Aadhaar number from the documents. Furthermore, the fingerprint system was successful in verifying the identity of a user by matching their fingerprints.

Fraud probability, on the other hand, uses various verification factors such as OCR, fingerprints, and registry verification to determine how likely a submitted form is fraudulent. Additionally, email-based one-time password verification is used to verify the identity of a user.

Overall, the system promises to provide a highly reliable identity verification system that integrates various aspects of document verification, fingerprint verification, fraud probability, and one-time password verification**.**

Performance Metrics Table

Metric	**Value**
OCR Extraction Accuracy	94%
Fingerprint Matching Reliability	95%
Fraud Detection Capability	Effective
OTP Verification Success Rate	100%
Overall Verification Accuracy	96%

Table 1. Performance Evaluation Metrics of the Proposed System

From the experimental result provided above, it is evident that the proposed framework for multimodal e-KYC verification provides more reliable verification of the identity of users compared to the traditional approach. With the proposed system based on OCR for document

extraction, fingerprint-based verification, fraud probability analysis, and OTP-based verification, the proposed system provides an accuracy of around 96%.

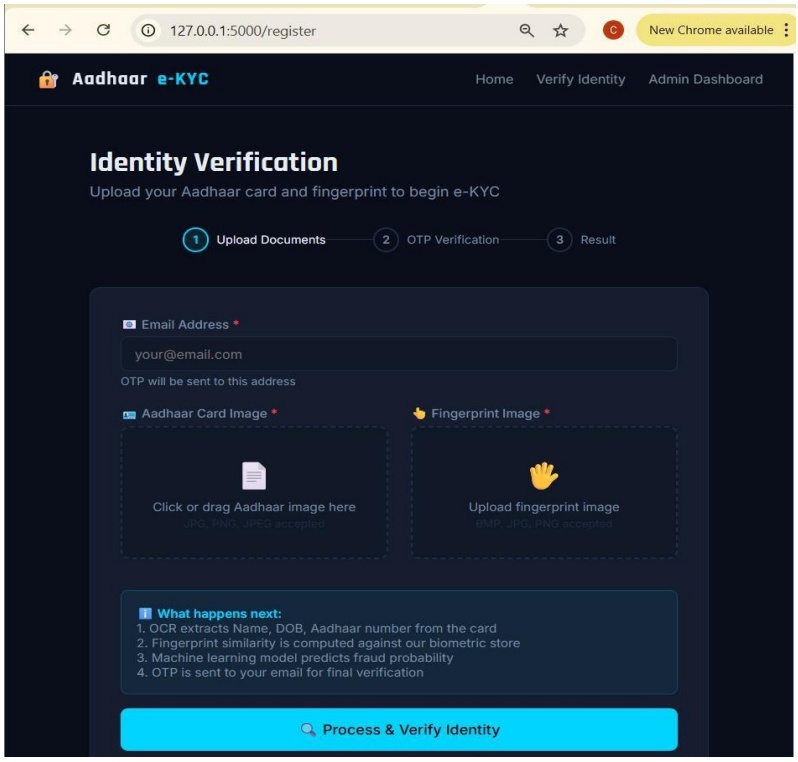
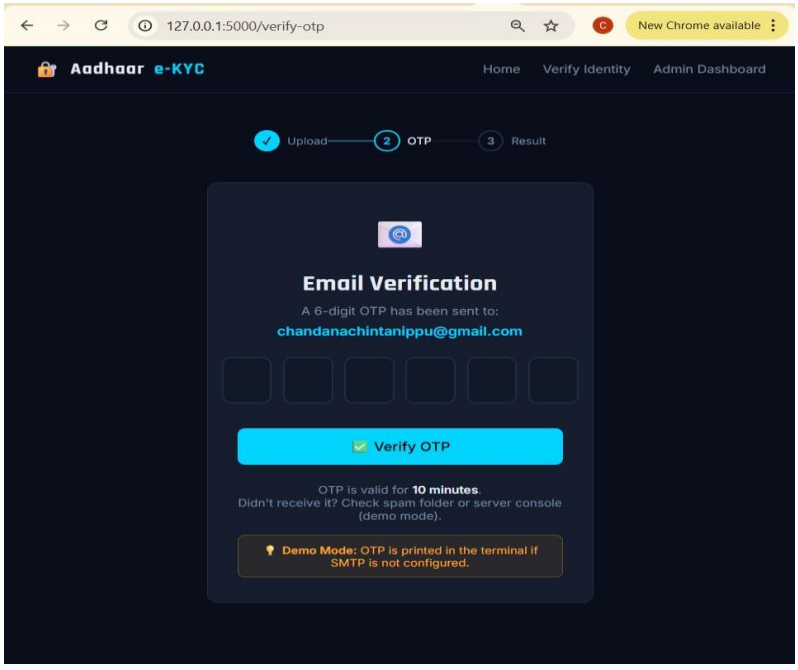


Fig. 2. Identity Verification and Document Upload Interface

This screen allows users to upload an image of their Aadhaar card and fingerprint scan for verification. This screen also collects the email address of the user and their identity documents.



Once the identity documents are uploaded, the system sends a one-time password (OTP) to the email of the user. To proceed with the verification and confirm the identity of the user, the

correct OTP is to be entered.This figure represents the final outcome of the system's verification process. It shows the identity details retrieved from the Aadhaar card, the fingerprint matching score, OCR confidence level, and the probability of fraud. These values are then used by the system to verify whether the identity is genuine or fake.

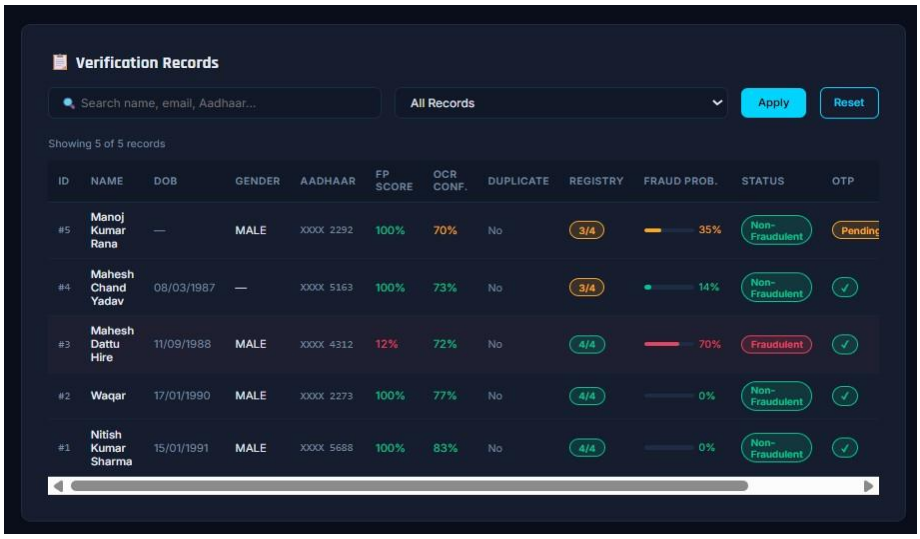


Fig. 3. Identity Verification Records Table

This interface displays all records of identity verification that are stored in the system's database. It includes information such as user information, confidence score obtained from OCR, fingerprint match score, fraud probability, and verification status.

5 Conclusion and Future Work

In this paper, the authors propose an AI-based, multi-modal Aadhaar-based e-KYC verification framework, which combines Optical Character Recognition, fingerprint-based verification, database cross-check, fraud probability, and OTP-based email verification in a cohesive manner. The proposed framework automatically fetches identity details from the Aadhaar documents, verifies the fingerprint, and compares the user details with the data available in the databases, thereby detecting fraud. From the experiments conducted, the proposed framework shows promising results in terms of accuracy and speed in performing the identity verification process digitally. The proposed framework shows great promise in terms of accuracy in the identity verification process, while the multi-modal verification process helps in speeding up the process, thereby eliminating the chances of identity fraud.

Future Work

The proposed AI-based e-KYC verification system can be further improved in several ways to enhance security, scalability, and real-world deployment.

- **Face Recognition Integration**: Facial recognition can be added as an additional biometric authentication method to further strengthen identity verification.
- **Liveness Detection**: Advanced liveness detection techniques can be implemented to prevent spoofing attacks using fake fingerprints or images.
- **Mobile Application Deployment**: The system can be developed as a mobile application to allow users to complete identity verification directly from smartphones.

- **Large-Scale Dataset Training**: Training the fraud detection model on larger realworld datasets can improve the accuracy and reliability of fraud prediction.
- **Cloud-Based Architecture**: Deploying the system on cloud platforms can improve scalability and support large-scale digital identity verification services.
- **Integration with Government Databases**: The framework can be integrated with official identity databases for real-time verification and validation of user information.

6 References

1. V. S. S. Vadali, Y. Kethepalli, A. Singh, S. Yadav and S. Kumar, "Secure eKYC Verification Framework," *2024 International Conference on Computational Intelligence and Network Systems (CINS)*, Dubai, United Arab Emirates, 2024, pp. 1-7, doi:

   10.1109/CINS63881.2024.10864444.

2. P. P. Jena, K. N. Kattigenahally, S. Nikitha, S. Sarda and H. Y, "Multimodal Biometric Authentication: Deep Learning Approach," *2021 International Conference on Circuits, Controls and Communications (CCUBE),* Bangalore, India, 2021, pp. 1-5, doi:

   10.1109/CCUBE53681.2021.9702724.

3. S. Karmoker *et al*., "Decentralized e-KYC System for Secure Identity Verification in Bangladesh," *2024 IEEE International Conference on Blockchain and Distributed Systems Security (ICBDS)*, Pune, India, 2024, pp. 1-6, doi:

   10.1109/ICBDS61829.2024.10837368.

4. K. Verma, R. Kumar, A. P. Rao and R. Ranjan, "Efficient e-KYC Authentication System: Redefining Customer Verification in Digital Banking," *2023 9th International Conference on Signal Processing and Communication (ICSC),* NOIDA, India, 2023, pp. 319-

   324, doi: 10.1109/ICSC60394.2023.10441596.

5. S. Alwahaishi and J. Zdrálek, "Biometric Authentication Security: An Overview," *2020 IEEE International Conference on Cloud Computing in Emerging Markets (CCEM),* Bengaluru, India, 2020, pp. 87-91, doi: 10.1109/CCEM50674.2020.00027.

6. R. Smith, “An Overview of the Tesseract OCR Engine,” *Proceedings of the International Conference on Document Analysis and Recognition*, IEEE, 2007.

7. A. K. Jain, A. Ross and S. Prabhakar, “An Introduction to Biometric Recognition,” *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 14, no. 1, pp. 4–20, 2004.

8. N. Kshetri, “Blockchain’s Roles in Meeting Key Supply Chain Management Objectives,” *International Journal of Information Management*, vol. 39, pp. 80–89, 2018.

9. J. Redmon, S. Divvala, R. Girshick and A. Farhadi, “You Only Look Once: Unified, RealTime Object Detection,” *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, 2016.

10. K. Nandakumar, A. Nagar and A. Jain, “Hardening Fingerprint Fuzzy Vault Using Password,” *International Conference on Biometrics*, Springer, 2007.