Multimodal Biometric System

Ajita Rattani
Indian Institute of Technology Kanpur, India

Hunny Mehrotra
Indian Institute of Technology Kanpur, India

Phalguni Gupta
Indian Institute of Technology Kanpur, India

INTRODUCTION

Personal identification is a fundamental activity within our society. This identification is made possible by the emergence of the new concept of biometrics. Biometrics is the science of identifying or verifying an individual based on the physiological or behavioral characteristics like face, fingerprint, iris, signature, voice, retina, handwriting, and so forth. Biometric identifiers for personal authentication reduce or eliminate reliance on tokens, PINs, and passwords. It can be integrated into any application that requires security, access control, and identification or verification of people (Jain, Ross, & Prabhakar, 2004).

A wide variety of applications require reliable verification schemes to confirm the identity of an individual requesting their service. They have an edge over traditional security methods in that they cannot be easily stolen or shared. A biometric system can be either an identification system or a verification (authentication) system, defined as:

- **Identification—One to Many:** Biometrics can be used to determine a person's identity even without his knowledge or consent. For example, scanning a crowd with a camera and using face recognition technology, one can determine matches against a known database.
- **Verification—One to One**: Biometrics can also be used to verify a person's identity. For example, one can grant physical access to a secure area in a building by using finger scans or can grant access to a bank account at an ATM by using face recognition.

Biometric authentication requires comparison of a registered or enrolled biometric sample (biometric template or identifier) against a newly captured biometric sample (e.g., the one captured during a login). A simple biometric system has a sensor module, a feature extraction module, and a matching module. However, it is found that none of these individual modules (face, fingerprint, iris, signature) are 100% reliable or efficient, thus in order to further increase its reliability, several biometrics traits are fused together on the basis of one of the following fusion rule such as sum rule, min-max rule, and so forth, and the decision is made based on the final score. The multimodal systems are able to meet the stringent performance requirements imposed by various applications (Jain & Ross, 2004).

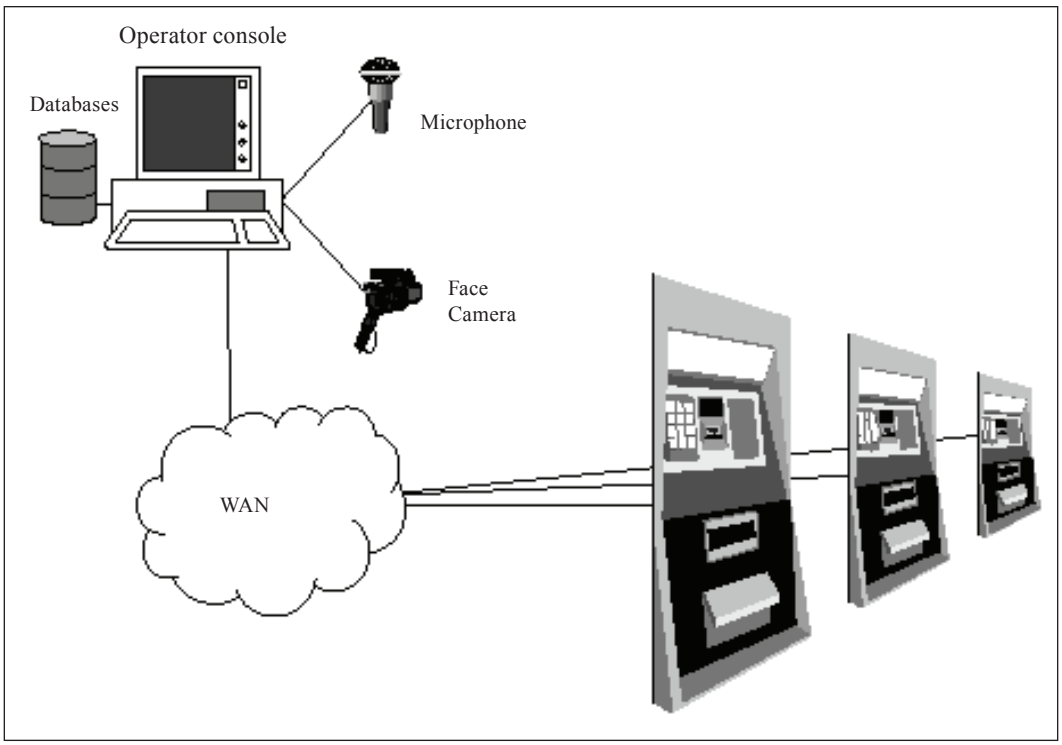
Multimodal systems also address the problem of non-universality: it is possible for a subset of users not to possess a particular biometric. For example, the feature extraction module of a fingerprint authentication system may be unable to extract features from fingerprints associated with specific individuals, due to the poor quality of the ridges. In such instances, it is useful to acquire multiple biometric traits for verifying the identity. Multimodal biometrics systems are expected to be more reliable due to the presence of multiple, fairly independent pieces of evidence.

BACKGROUND

Uni-modal systems, besides having high error rates, have to contend with a variety of problems such as *noise in sensed data, intra-class variations, interclass similarities, non-universalities,* and *spoof attacks.* Some examples of noise in sensed data are fingerprint image with a scar. *Intra-class variations* are typically caused by a user who is incorrectly interacting with the sensor or due to changes in the biometric characteristics of a user over a period of time. In a biometric

Copyright © 2008, IGI Global, distributing in print or electronic forms without written permission of IGI Global is prohibited.

Figure 1. Multimodal system



system comprising a large number of users, there may be *interclass similarities* in the feature space of multiple users. Another source is *non-universality*: the biometric system may not be able to acquire meaningful biometric data from a subset of users. *Spoof attacks* are especially relevant when behavioral traits such as signature and voice are used.

Multimodal biometric systems overcome limitations of uni-modal biometric systems by consolidating the evidence obtained from different sources. These sources can be of the following forms and are shown in Figure 2 (Ross & Jain, 2004):

i. **Multiple sensors for the same biometric:** More than one sensor is used to grab images, and then these images are fused together and analyzed for better results (e.g., optical and solid state fingerprint sensors).
ii. **Multiple instances of the same biometric:** Multiple instances of an individual are processed and fused to generate the final result (e.g., multiple face images of a person obtained under different pose/lightning condition).
iii. **Multiple representations and matching algorithms for the same biometric:** Multiple representations and classifiers are applied on the same biometric data to generate the final result (e.g., multiple face matchers like PCA and LDA).
iv. **Multiple units of the same biometric:** Multiple units of an individual are used to check the authenticity of a person (e.g., left and right iris images).
v. **Multiple biometric traits:** Multiple modalities are used to test the authenticity of a person (e.g., face, fingerprint, and iris).

In the multi-biometrics system, different classifiers/modalities for recognition are combined at one of the four levels—sensor level, feature extraction level, matching score level, and decision level—and it performs better compared to individual recognizers and classifiers. Ross and Jain (2003) have presented an overview of multimodal biometrics and have proposed various levels of fusion, various possible scenarios, the different modes of operation, integration strategies, and design issues. A multimodal system can operate in one of three different modes: serial mode, paral-

6 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/chapter/multimodal-biometric-system/13515

Related Content

Investing in IT Security: How to Determine the Maximum Threshold
Amanda Eisenga, Travis L. Jonesand Walter Rodriguez (2012). *International Journal of Information Security and Privacy (pp. 75-87).*
www.irma-international.org/article/investing-security-determine-maximum-threshold/72725

Assessing the Value of Executive Leadership Coaches for Cybersecurity Project Managers
Darrell Norman Burrell (2022). *Research Anthology on Business Aspects of Cybersecurity (pp. 349-362).*
www.irma-international.org/chapter/assessing-the-value-of-executive-leadership-coaches-for-cybersecurity-project-managers/288686

Access Management as a Security Critical Factor: A Portuguese Telecommunications Company Case Study
Pedro Fernandes Anunciaçãoand Eliana Nunes (2021). *International Journal of Risk and Contingency Management (pp. 12-25).*
www.irma-international.org/article/access-management-as-a-security-critical-factor/284441

Globalization and Data Privacy: An Exploratory Study
Robert L. Totterdale (2010). *International Journal of Information Security and Privacy (pp. 19-35).*
www.irma-international.org/article/globalization-data-privacy/46101

Implementing Information Security Using Multimodal Biometrics
Vinita Jindaland Divya Singhal (2021). *Handbook of Research on Cyber Crime and Information Privacy (pp. 338-355).*
www.irma-international.org/chapter/implementing-information-security-using-multimodal-biometrics/261737