Pattern Recognition Letters 79 (2016) 80–105

Contents lists available at ScienceDirect

Pattern Recognition Letters

journal homepage: www.elsevier.com/locate/patrec

50 years of biometric research: Accomplishments, challenges, and opportunities☆

Anil K. Jain[a,1,*], Karthik Nandakumar[b], Arun Ross[a]

[a] Department of Computer Science and Engineering, Michigan State University, East Lansing, MI 48824, USA
[b] IBM Research Singapore, 9 Changi Business Park Central 1, 486048 Singapore

ARTICLE INFO

Article history:
Received 4 February 2015
Available online 12 January 2016

Keywords:
Biometrics
Fingerprints
Face
Iris
Security
Privacy
Forensics

ABSTRACT

Biometric recognition refers to the automated recognition of individuals based on their biological and behavioral characteristics such as fingerprint, face, iris, and voice. The first scientific paper on *automated* fingerprint matching was published by Mitchell Trauring in the journal Nature in 1963. The first objective of this paper is to document the significant progress that has been achieved in the field of biometric recognition in the past 50 years since Trauring's landmark paper. This progress has enabled current state-of-the-art biometric systems to accurately recognize individuals based on biometric trait(s) acquired under controlled environmental conditions from cooperative users. Despite this progress, a number of challenging issues continue to inhibit the full potential of biometrics to automatically recognize humans. The second objective of this paper is to enlist such challenges, analyze the solutions proposed to overcome them, and highlight the research opportunities in this field. One of the foremost challenges is the design of robust algorithms for representing and matching biometric samples obtained from uncooperative subjects under unconstrained environmental conditions (e.g., recognizing faces in a crowd). In addition, fundamental questions such as the distinctiveness and persistence of biometric traits need greater attention. Problems related to the security of biometric data and robustness of the biometric system against spoofing and obfuscation attacks, also remain unsolved. Finally, larger system-level issues like usability, user privacy concerns, integration with the end application, and return on investment have not been adequately addressed. Unlocking the full potential of biometrics through inter-disciplinary research in the above areas will not only lead to widespread adoption of this promising technology, but will also result in wider user acceptance and societal impact.

1. Introduction

> *"It is the purpose of this article to present, together with some evidence of its feasibility, a method by which decentralized automatic identity verification, such as might be desired for credit, banking or security purposes, can be accomplished through automatic comparison of the minutiae in finger-ridge patterns."*
> – *Mitchell Trauring, Nature, March 1963*

In modern society, the ability to reliably identify individuals in real-time is a fundamental requirement in many applications including forensics, international border crossing, financial transactions, and computer security. Traditionally, an exclusive possession of a token, such as a passport or an ID card, has been extensively used for identifying individuals. In the context of computer systems and applications, knowledge-based schemes based on passwords and PINs are commonly used for person authentication.[2] Since both token-based and knowledge-based mechanisms have their own strengths and limitations, the use of two-factor authentication schemes that combine both these authentication mechanisms are also popular.

Biometric recognition, or simply biometrics, refers to the automated recognition of individuals based on their biological and behavioral characteristics [39]. Examples of biometric traits that have been successfully used in practical applications include face, fingerprint, palmprint, iris, palm/finger vein, and voice. The use of DNA, in the context of biometrics (as opposed to just forensics), is also beginning to gain traction. Since biometric traits are generally inherent to an individual, there is a strong and reasonably

☆ This paper has been recommended for acceptance by S. Sarkar.

* Corresponding author. Tel.: +1 517 355 9282; fax: +1 517 432 1061.
E-mail addresses: jain@cse.msu.edu (A.K. Jain), nkarthik@sg.ibm.com (K. Nandakumar), rossarun@cse.msu.edu (A. Ross).

[1] IAPR Fellow.

[2] Authentication involves verifying the claimed identity of a person.

http://dx.doi.org/10.1016/j.patrec.2015.12.013
0167-8655/

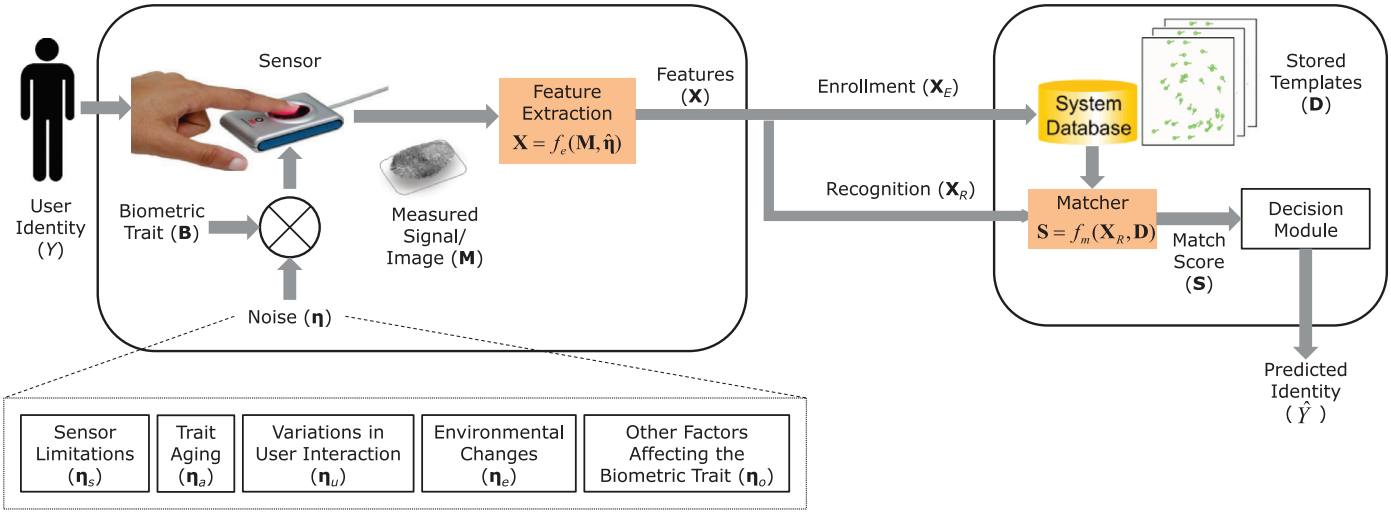

Fig. 1. Operation of a typical biometric system. The two fundamental problems in biometric recognition involve finding an invariant feature representation and designing a robust matcher for a given representation scheme.

permanent link between a person and his/her biometric traits. Thus, biometric recognition can be used to identify individuals in surveillance operations where covert recognition[3] is required or in scenarios where a person may attempt to conceal their true identity (e.g., by using forged documents to claim social welfare benefits). Consequently, the application domain of biometrics far exceeds that of passwords and tokens. In applications such as border control, forensics, surveillance, de-duplication,[4] and chain-of-custody,[5] the use of biometric solutions has clear-cut advantages over passwords or tokens.

However, the emergence of biometrics does not necessarily supplant the use of passwords or tokens in authentication applications. While biometrics can mitigate some of the limitations associated with the use of passwords, biometric systems themselves are vulnerable to spoof attacks, linkability attacks (linking users across applications based on their biometric data), and can incur additional hardware and software costs. Further, the acquisition process introduces variations in the biometric data of an individual (referred to as intra-subject variations) that may lead to false non-matches and false matches. False matches can lead to identity creep, where an adversary, after repeated attempts, manages to take on the identity of a legitimate user of the system. The lack of secrecy (e.g., face images on social media sites) and distinctiveness (e.g., face images of identical twins) of biometric traits pose additional problems to biometric-based authentication schemes. Given the above limitations, a multi-factor authentication mechanism that judiciously combines biometrics with passwords and/or tokens may be a better approach to security in many applications [65].

1.1. Motivation and objectives

The first known research publication on automated biometric recognition was the one published by Mitchell Trauring in the journal Nature in 1963 on fingerprint matching [91]. The development of automated biometric systems based on other traits such as voice [73], face [12], and signature [55] also started in the 1960s. Subsequently, biometrics systems based on traits like hand geometry [24] and iris [19] were developed. In this sense, 50 years have passed since the first paper on automated biometric recognition was published.

In a 2007 article, Wayman [97] tracked the major developments in biometrics in the United States from the 1960s to the 1990s, and observed the following: *"A quick overview of biometric history shows that much of what we consider to be "new" in biometrics was really considered decades ago. There is much left to be done, but the most efficient route will be to consider that which is really yet undiscovered, not wasting time repeating the studies of years ago. Even in 2005, it is much too early to speculate on what the first decade of the new millennium will ultimately hold for biometrics. It seems clear, however, that the industry will continue to grow and that technical and human improvements to the systems will be made."*

In line with the above observation from Wayman, the objective of this paper is to summarize the progress in biometric recognition so as to understand *how this field emerged*, *where we are now*, and *where we should go from here*. We believe that this assessment of biometrics research would shed light on the cross-disciplinary nature of problems in biometric recognition, highlight the tremendous opportunities for both basic and applied research in biometrics, and motivate budding scientists and engineers to consider biometric recognition as their field of study.

2. Biometric recognition framework

A typical biometric recognition system has two stages of operation, namely, the enrollment stage and the recognition stage (see Fig. 1). In the enrollment stage, the biometric system acquires the biometric trait of an individual, extracts a salient feature set from it and stores the extracted feature set in a database (often referred to as a template), along with an identifier associating the feature set with an individual. During the recognition stage, the system once again acquires the biometric trait of an individual, extracts a feature set from it, and compares this feature set against the templates in the database in order to determine a match or to verify a claimed identity.

In the enrollment stage, a biometric sensor scans the biometric trait (**B**) of a user (*Y*) to obtain a digital representation (**M**). Since the scanned biometric trait may be affected by various sources of noise ($\boldsymbol{\eta}$) during the sensing process, a quality check is generally performed to ensure that the acquired biometric data can be reliably processed by successive modules. In order to facilitate

[3] In a covert scenario, the subject's biometric traits are acquired without the subject's explicit knowledge and surreptitiously used for recognition purposes.

[4] De-duplication involves the removal of duplicate "identities", where, for example, a single individual may have multiple passports under different names.

[5] This is to keep track of individuals who handle the physical evidence collected during the course of a legal proceeding.