Pattern Recognition 47 (2014) 2673–2688

Contents lists available at ScienceDirect

Pattern Recognition

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

A review of biometric technology along with trends and prospects

J.A. Unar [a,b,*], Woo Chaw Seng [a,**], Almas Abbasi [a]

[a] Faculty of Computer Science & Information Technology, University of Malaya, 50603 Kuala Lumpur, Malaysia
[b] Department of Information Technology, Quaid-e-Awam University of Engineering, Science & Technology, Nawabshah, Sindh, Pakistan

ARTICLE INFO

Article history:
Received 9 February 2013
Received in revised form
14 November 2013
Accepted 27 January 2014
Available online 5 February 2014

Keywords:
Biometrics
Fingerprint
Face
Iris
Retina
Behavioral biometrics
Gait
Voice
Soft biometrics
Multi-modal biometrics

ABSTRACT

Identity management through biometrics offer potential advantages over knowledge and possession based methods. A wide variety of biometric modalities have been tested so far but several factors paralyze the accuracy of mono-modal biometric systems. Usually, the analysis of multiple modalities offers better accuracy. An extensive review of biometric technology is presented here. Besides the mono-modal systems, the article also discusses multi-modal biometric systems along with their architecture and information fusion levels. The paper along with the exemplary evidences highlights the potential for biometric technology, market value and prospects.

1. Introduction

The ever increasing criminal and terrorist acts in public places, government/private properties resulted in chaotic scenarios thereby making the existing surveillance systems questionable – "*How effective is the surveillance system to prevent unlawful activities*?", "*Does the system guarantee the required level of security*?", "*Does the system distinguish an unauthorized user from an impostor reliably*?", "*Is the system user friendly*?". In early stages, the identity management systems relied on cryptographic methods requiring the users to remember a secret text (password) or keep something with them (token, card) or a combination of both to prove their identity. Consequently, the population is flooded with passwords and tokens to gain access to required resources for instance; access control, computer logins, e-mail checking, making bank transactions, border control, welfare disbursements etc. However, the users challenged the efficacy of such systems through the queries such as, "*What happens, if I forget my password/token*?", "*What will be the consequences, if I lost my card*?", "*What type of loss I have to bear, if my password is divulged to an unauthorized person?*", "*How many passwords I have to remember*?", "*How many cards I have to keep in my wallet?*", "*How does the system know who is requesting access to particular resources?*" and finally, "*Is there any alternative which is more convenient and reliable?*". As an answer, the research community proposed the idea of human identification based on physiological or behavioral attributes of individuals very often termed as "Biometrics". Computer science describes biometrics as automatic recognition of individuals through their unique physiological (fingerprint, face, iris etc.) or behavioral (voice, gait, signature etc.) attributes [1,2]. Although biometrics is not the perfect solution but it offers several advantages over knowledge and possession based approaches in the way that there is no need to remember anything, biometric attributes cannot be lost, transferred or stolen, offer better security due to fact that these attributes are very difficult to forge and require the presence of genuine user while granting access to particular resources. Inspired from the development of Bertillon's system in 1883 to Sir John Galton's elementary fingerprint recognition system in 1903, the research community devoted their efforts to discover several biometric modalities. Any physiological or behavioral attribute can qualify for being a biometric trait unless it satisfies the criteria such as (*i*) *universality*: possessed by all humans, (*ii*) *distinctiveness*: discriminative amongst the population, (*iii*) *Invariance*: the selected biometric attribute must exhibit invariance against time, (*iv*) *collectability*: easily collectible in terms of acquisition, digitization and feature extraction from the population, (*v*) *performance*: pertains

* Corresponding author at: University of Malaya, Artificial Intelligence Department, Faculty of Computer Science & Information Technology, 50603 Kuala Lumpur, Malaysia.
** Corresponding author.
E-mail addresses: jawedunar@siswa.um.edu.my, jawedunar@yahoo.com (J.A. Unar), cswoo@um.edu.my (W.C. Seng), alma@siswa.um.edu.my (A. Abbasi).

http://dx.doi.org/10.1016/j.patcog.2014.01.016
0031-3203

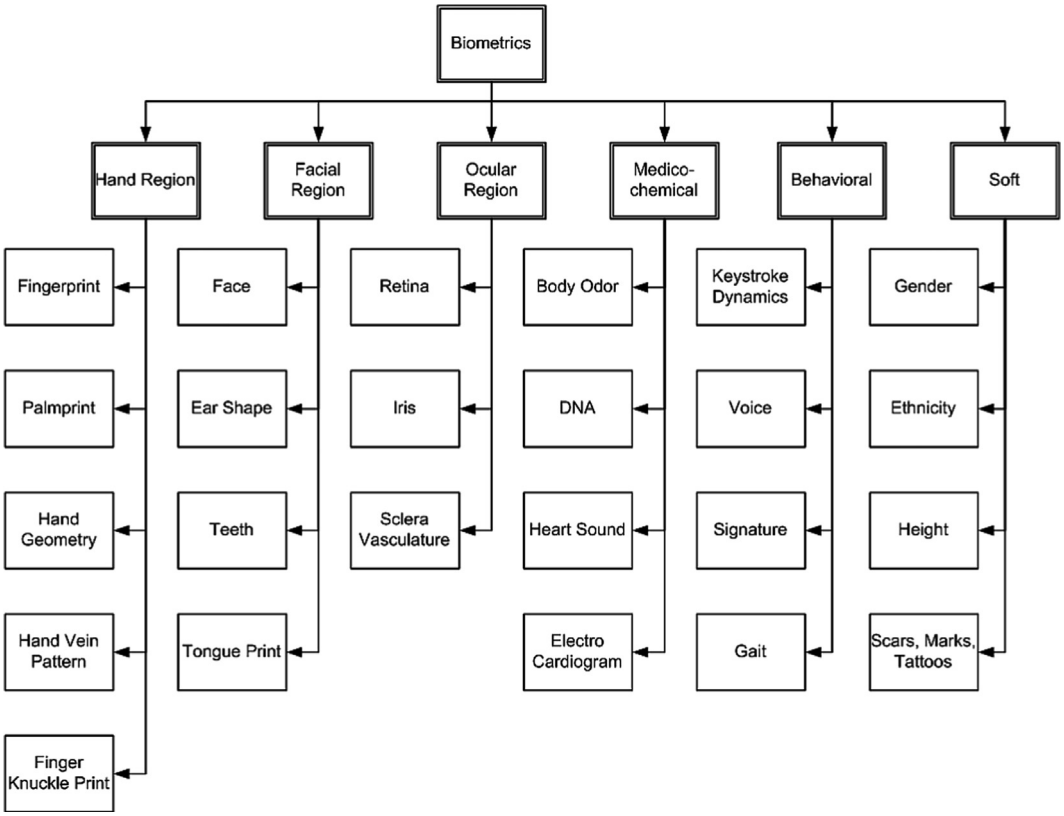

Fig. 1. Classification of biometric modalities.

to the availability of resources and imposition of real constraints in terms of data collection and guarantee to achieve high accuracy, (*vi*) *acceptability*: willingness of population to submit that attribute to recognition system and (*vii*) *circumvention*: prone to imitation or mimicry in case of fraudulent attacks against the recognition system [1]. Based on the criteria, several distinctive human characteristics are identified and tested. Instead of the broad categories (physiological, behavioral and soft attributes), for convenience the physiological modalities can be further sub-divided into different sub-categories according to their respective position in human body such as (*i*) hand region attributes, (*ii*) facial region attributes, (*iii*) ocular and periocular region attributes, (*iv*) behavioral attributes, and (*v*) medico-chemical attributes. The sub-division is illustrated in Fig. 1.

The article is written with an intention to provide an in-depth overview of biometric technology to the readers. In contrast to several reviews on the subject, this work provides additional information which is lacking in other review articles, such as

i) The paper provides details about each biometric modality along with prominent recognition techniques and public data sets available to the researchers.
ii) The article contains a rough quantitative analysis of individual techniques in terms of accuracy.
iii) The paper discusses multimodal biometrics in detail which has not been well covered in other review articles on the subject.
iv) The paper contains current market statistics along with future prospects for biometric based identification and authentication.

Rest of the article comprises of four sections, whereas, Section 2 provides basic concepts consisting composition, classification, operational scenarios and performance issues related to biometric systems. Section 3 discusses biometric modalities as per aforementioned classification along with advantages, disadvantages, matching techniques and available data sources for researchers. Section 4 throws light on the limitations of mono-modal biometric systems followed by an overview of multi-modal biometric systems. Finally, Section 5 presents the recent market trend and thorough analysis with examples towards adoption of biometric solutions followed by concluding remarks.

2. Biometric systems

A biometric system is a pattern recognition system which matches the salient or discriminatory features of acquired image (probe image) with the features of pre-stored images (gallery image). For doing so, every biometric system comprises of (*i*) *Image acquisition module*: this acquires the image of a biometric trait and submits it to the system for further processing, (*ii*) *Feature extraction module*: processes the acquired image thereby extracting the salient or discriminatory features, (*iii*) *Matcher module*: matches the extracted features of probe image with those of gallery image to obtain a match score whereas, an embedded decision making module verifies or rejects the claimed identity based on the match score and (*iv*) *Database module*: contains the digital representation of previously acquired samples very often termed as templates. Fig. 2 illustrates the composition of a typical biometric system.

2.1. Modes of operation

A biometric system operates in one of the following modes:

2.1.1. Verification

This is very often referred as positive recognition. The user after submitting the biometric signature to the system claims a particular identity through a PIN, login name, etc. In response, the recognition system validates or voids user's claim by making a 1:1