Pattern Recognition 62 (2017) 214–224

Contents lists available at ScienceDirect

Pattern Recognition

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

A spoof resistant multibiometric system based on the physiological and behavioral characteristics of fingerprint

Ishan Bhardwaj [a], Narendra D. Londhe [a,*], Sunil K. Kopparapu [b]

[a] National Institute of Technology Raipur, Raipur 492010, CG, India
[b] TCS Innovation Labs, Mumbai 400601, India

ARTICLE INFO

Article history:
Received 5 May 2016
Received in revised form
15 July 2016
Accepted 8 September 2016
Available online 17 September 2016

Keywords:
Biometrics
Fingerprint
Dynamics
Spoof attack
Multimodal
Behavioral
Fusion
LivDet
ATVS

ABSTRACT

Despite emerging as a prominent choice to serve the security concerns of person authentication applications, unimodal biometric systems are vulnerable to spoof attacks. Multimodal biometric systems can effectively minimize spoof attacks while improving the overall performance. In this paper, we present a multimodal system based on two modalities derived from multi instance fingerprint acquisition viz. fingerprint and the associated time dynamics. Extensive user verification and spoof resistance experiments conducted on virtual multimodal databases, created by combining ATVS and LivDet-13 fingerprint databases each with fingerprint dynamics database. Fusion is performed at match score level using sum and weighted sum rules. The empirical results demonstrate spoof resistance of the proposed multimodal system with significant performance improvement over unimodal and multi-instance fingerprint recognition systems. The performance of the proposed system is evaluated on well-known metrics like Detection Error Trade-off (DET) curves, equal error rate (EER), and Area Under the Curve (AUC).

1. Introduction

In the present era, biometrics has emerged as an established technique for person authentication due to its ergonomic benefits, scalability, and reliability properties. Biometrics can be defined as a means of person authentication based on physiological (fingerprint [1], face [2] and palm-print [3]) or behavioral characteristics (keystroke dynamics [4], signature [5], and gait [6]). It can facilitate various functionalities [7] including identification and verification of a person. In comparison to conventional password based systems, convenience of use, permanence, uniqueness, improved security, and implausibility of stolen or lost credentials are some of the advantages of biometrics [8]. The advantages of biometrics are not only attracting large number of researchers but are also resulting in real world deployments.

Although unimodal biometric systems have several advantages over the conventional password based authentication systems, they are susceptible to several issues that limit their usage [9–11] and thus need to be addressed by the research community. Even the well-established biometric techniques, like fingerprint, may require human compliance and are argued to be obtrusive and stigmatic by many researchers [12,13]. Some prime challenges include (a) problem of high intra class variability, (b) environmental conditions, (c) failure to enroll, (d) attacks, and (e) data acquisition issues like noise, rotation, displacement etc. [1]. Several studies [3,12,14] addressed users cognizance about the possible threats associated with biometrics and their reluctance to use the biometric based systems.

In biometrics, irrespective of the recognition performance of the biometric system, an attack is a serious threat to the security and privacy of the enrolled individuals [11,15]. Broadly, two types of attacks have been reported in literature, namely (a) indirect attacks which target vulnerabilities inside the system and (b) direct attacks, outside the digital limits of the system, usually at the sensor level [8]. While indirect attacks can be countered using firewalls, secure communication channel, and intrusion detection techniques, direct attacks cannot be handled by securing the system or network.

Spoofing is the simplest form of direct attack and also the most threatening [6,7]. Contrary to zero-effort attacks, where a person tries to break the system by using his own biometric data, in active impostor attack (spoofing) an impostor uses a genuine user's counterfeit biometric sample to circumvent the system. It is evident from history that fingerprint forgery in the forensic field exists almost from the advent of fingerprint as biometrics [8,16]. Typically spoofing attacks are carried out either by utilizing the residual fingerprint left behind on the sensor surface or by directly

* Corresponding author.
E-mail address: nlondhe.ele@nitrr.ac.in (N.D. Londhe).

http://dx.doi.org/10.1016/j.patcog.2016.09.003
0031-3203/

acquiring them from the target person. Spoof fingerprints can be contrived by materials like silicone, gelatin, clay, dental molding etc. with or without user cooperation [17,18].

Several solutions to these issues and vulnerabilities have been suggested in the literature and mainly fall under two categories: (a) software based techniques [14,18,19] and (b) hardware based techniques [20]. Software based detection techniques are generally less intrusive and cost effective but may lack reliability. Image processing techniques to improve the discrimination capability of the existing algorithm have been reported in the literature and more recently advance classification techniques are being deployed [15,21]. Hardware based techniques are comparatively more reliable but most often expensive and intrusive [20]. Liveness detection, defined as a process or technique that aids in determining whether the fingerprint presented is from a live or a spoof artifact, can be deployed at both the levels, hardware and software [8,22,23]. Most recent experiments on spoof fingerprint detection deal with dead or altered fingers [19,24]. In literature, liveness is seen as a separate task, i.e. only for detecting spoof finger impressions, and not for improving the recognition results. Thus the problem can be dealt in two ways: a dual classification problem (live versus spoof and genuine versus impostor) [16], or a single classification problem (ensemble of both) [25]. Various studies like Galbally et al. [19] explore the possibility to recreate high quality fingerprints from the spoof samples, making it difficult for techniques that assess the quality of the sample [26,27] to detect spoof fingerprints. Studies like [18] indicate that certain algorithms are more vulnerable if new materials (other than those used for training) are used for spoofing. A good overview of such issues and potential attacks is given in [8,15]. These facts inspire us to instigate an approach that can not only aid in building a robust system against spoof attacks, regardless of the spoof material used, but also be capable of improving the recognition accuracy of the system.

The aim of this paper is to assess the possibility of using fingerprint dynamics as an assistive biometrics tool in addition to the well-established fingerprint modality. We examine the proposed multi-biometric system in various aspects, like its ability to discourage spoof attacks, improve the overall verification performance, etc. The experiments in this work compare individual and combined performance of the modalities for person verification. We follow the standard practice usually employed for modeling multi-biometric system when a multimodal dataset of desired modalities is not available [9,28–30] (fingerprints and fingerprint dynamics in our experiment). In this scenario modalities from different datasets are combined to form virtual personalities. For fingerprint we used two well-known publicly available databases, specifically collected for fingerprint direct attack study, and for fingerprint dynamics a self-constructed dataset (made available for download), consisting of samples from both genuine users and impostors (spoof samples). The main contributions of this paper are:

- Constructing virtual multimodal datasets by combining the fingerprint and fingerprint dynamics dataset.
- Exploiting the ability of fingerprint dynamics in multimodal scenario under spoof attack.
- Extensive user verification experimentation with different sensors and spoof materials.
- Comparative performance evaluation of the proposed multimodal system with unimodal and multi-instance systems.

The paper is organized as follows: description of the proposed system, a brief overview to related fields, and research efforts are presented in Section 2, description of databases and creation of multimodal database is given in Section 3, experimental results are described in Section 4, followed by the discussion and conclusions in Sections 5 and 6 respectively.

2. Our methodology

In this section a brief overview is given to the biometric technologies involved namely, fingerprint, fingerprint dynamics, and multimodal.

2.1. Fingerprint verification

There are many physiological and behavioral characteristics [8] that can uniquely epitomize an individual but none of them qualify as an impeccable solution [10]. However, fingerprint based authentication systems are an acceptable choice and are widely deployed for both identification [31] and verification task [17]. Eminence in forensics, high user acceptability, and feasibility to be embedded into portable devices are some of the merits among others that favor fingerprint as a prominent choice [11].

Like other counterparts fingerprint matching is also susceptible to several challenges [1,15], including direct and indirect attacks. There are many studies [17–19,24,27] that examine methods to circumvent fingerprint based biometric systems. Espinoza et al. [32] experimentally concluded that current state-of-the-art sensors can be deceived using spoof fingerprints, created with or without user cooperation. They also elaborate and measure the significance of quality of the spoof in attacks. Several techniques that achieve acceptable performance against inverse and linkage attacks, fail against active impostor (spoof) attacks [8,33]. This motivates us to contrive a methodology to counter these deficits.

2.2. Fingerprint dynamics

Various behavioral attributes of human actions are person dependent and hence can be effectively utilized to characterize an individual. One such attribute is the time dimension realizing the events during the course of a work [34]. Fingerprint dynamics can be simply described as ‘a process of time recording events’ [35], while users scan their fingers against the sensor [36]. Fingerprint dynamics, inspired by successful application of the keystroke dynamics for user authentication [4], represents behavioral characteristics of an individual. In keystroke dynamics, the time stamps representing the typing actions of a user are logged; along similar lines in fingerprint dynamics, the time information of multi-instance finger scan event performed in a sequence is recorded. However, unlike typical keystroke dynamics based systems, where the position or layout of different keys of the keyboard plays an important role in epitomizing a person, the fingerprint dynamics based system utilizes a single sensor unit for data acquisition. This aspect enables fingerprint dynamics modality to be acquired in conjunction with fingerprints of the user using the same sensor unit.

Fingerprint dynamics demands multi instance finger scan attempts. Fig. 1 represents an exemplary multi-instance finger scan of an individual and the associated time derived features. In literature [10,16] multiple instances of biometric trait are reported to contribute in improving the system performance by minimizing various associated issues that usually affect conventional systems based on a single instance. In a preliminary study [35] on fingerprint dynamics, we found that users develop a unique tendency when they often scan their fingers in a sequence that is unique to them. This behavioral characteristic tends to be inimitable at par to many other popular biometric traits. Let us say the timing stamps are acquired for n fingerprint scan actions per user involving k fingers of the user such that $k \leq n$. Note that the maximum value of k is limited to the number of fingers of a user (typically 10, including both hands), whereas n can be any value chosen by the user. Hence, the length of finger sequence is not limited to the value k, and it may involve repetitive use of the some finger.