Engineering Applications of Artificial Intelligence 72 (2018) 368–381

Contents lists available at ScienceDirect

Engineering Applications of Artificial Intelligence

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

How far did we get in face spoofing detection?

Luiz Souza [a], Luciano Oliveira [a,*], Mauricio Pamplona [a], Joao Papa [b]

[a] IVISION Lab, Federal University of Bahia, Brazil
[b] RECOGNA Lab, São Paulo State University, Brazil

ARTICLE INFO

Keywords:
Face spoofing
Face recognition
Survey
Spoofing attack

ABSTRACT

The growing use of control access systems based on face recognition shed light over the need for even more accurate systems to detect face spoofing attacks. In this paper, an extensive analysis on face spoofing detection works published in the last decade is presented. The analyzed works are categorized by their fundamental parts, *i.e.,* descriptors and classifiers. This structured survey also brings a comparative performance analysis of the works considering the most important public data sets in the field. The methodology followed in this work is particularly relevant to observe temporal evolution of the field, trends in the existing approaches, to discuss still opened issues, and to propose new perspectives for the future of face spoofing detection.

1. Introduction

In the last decade, there has been an increasing interest in human automatic secure identification, being mainly based on unique personal biometric information (Jain et al., 2008). One of the main reasons for such focus concerns the high number of security breaches and transaction frauds in non-biometric systems, which are prone to be cracked due to inherent vulnerabilities (Meadowcroft, 2008), like stolen cards and shared passwords, just to name a few.

Biometrics may use physical or behavioral characteristics for identification purposes, and different alternatives have been explored over the years: fingerprint (Hasan and Abdul-Kareem, 2013; Marasco and Ross, 2015; Peralta et al., 2014), hand geometry (Al Eidan, 2013; Kah Ong Michael et al., 2012), palmprint (Tamrakar and Khanna, 2016), voice (Yadav and Mukhedkar, 2013; Choi et al., 2015), face (Zhao et al., 2003; Feng et al., 2016; Dora et al., 2017), and handwritten signature (Sanmorino and Yazid, 2012). Among those, face stands out for its acceptability and recognition cost, turning out to be one of the best option for a wide range of applications, from low-security uses (*e.g.,* social media and smartphone access control) to high-security applications (*e.g.,* border control and video surveillance in critical places).

This popularity, however, comes with a price: face recognition systems have become a major target of spoofing attacks. In such scenarios, an impostor attempts to be granted in an identification process by forging someone else's identity. As procedures to replicate human faces are very much standard nowadays (*e.g.,* photo and 3D printing), spoofing detection has become mandatory in any suitable face recognition system. Fig. 1 illustrates the complexity of this problem, and the following question can be raised: "Which half is real or fake?". It is sometimes a very challenging task, even for humans.

Several approaches for spoofing detection have been developed in the last decade. Recently, two main surveys on the subject present a comprehensive review (Galbally et al., 2014; Parveen et al., 2015): in Galbally et al. (2014), a survey on anti-spoofing methods focuses not only on face, but also on other biometric traits (*e.g.,* iris, voice, fingerprint); in Parveen et al. (2015), face anti-spoofing methods are discussed by considering the intrusiveness of each method, with few attention on comparative analysis and temporal evolution of the field. On the other hand, the proposed survey focuses only on face-oriented works, reviewing and analyzing the most relevant works on face spoofing detection in the literature towards depicting the advance of the detection methods in the last decade. An extensive set of face anti-spoofing methods is presented, also depicting the evolution of the existing works. In this sense, trends denoted throughout these years were pointed out, as well as open issues were remarked in order to provide new directions on research topics in the future. Next, the contributions of this survey are addressed and discussed in details with respect to the other existing surveys, with special attention to the gaps filled by the present work.

1.1. Contributions

To the best of our knowledge, there are only two surveys in the context of face spoofing detection (Galbally et al., 2014; Parveen et al.,

[*] Corresponding author.
E-mail addresses: luiz.otavio@ufba.br (L. Souza), lrebouca@ufba.br (L. Oliveira), mauricio@dcc.ufba.br (M. Pamplona), papa@fc.unesp.br (J. Papa).

https://doi.org/10.1016/j.engappai.2018.04.013
Received 17 June 2017; Received in revised form 9 April 2018; Accepted 13 April 2018

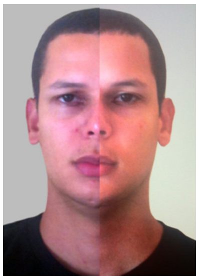

Fig. 1. Example of a half real (photo) and half fake face (photo of a photo). Which half is the real one? The answer is the one on the left.

2015). Although two face anti-spoofing competitions were organized (Chakka, 2011; Chingovska, 2013), and several data sets and methods have been published, the amount of gathered data and results were not still thorough and critically analyzed so far. Even these two existing surveys do not concentrate efforts to understanding the trends of this research field in terms of conception of the methods and results.

Galbally et al. (2014) published a survey based on a chronological evolution of multimodal anti-spoofing methods. Although a special attention was given to face anti-spoofing, other biometric traits were also presented and discussed. A proposed timeline takes into consideration fingerprint, iris, and face anti-spoofing detection competitions, being the latter one organized by one of the authors of the survey (Galbally et al., 2014). In regard to face-driven works, the authors provided an extensive and comprehensive description of different types of face attacks and public image data sets. The face anti-spoofing methods, categorized by Galbally et al., were according to three levels: sensor, features, and multi-modal fusion, but being only two levels employed to classify the analyzed works. Sixteen existing works compose the face study part, which was characterized by the level of the technique, type of attack, public image data set used, and a single error rate. At the end, a discussion was addressed showing that although competitive laboratory performances were achieved, some people were successfully able to hack the fingerprint recognition system of the Iphone 5s. In Galbally et al. (2014), also, some discussion about performance of face anti-spoofing methods resided in general considerations about cross-data set performance evaluation (in order to turn methods' evaluation more thoroughly accomplished), new relevant features acquired on facial blood flow, and new hardware that could be used along with cameras to improve face anti-spoofing detection. The remainder of the survey in Galbally et al. (2014) discusses philosophical aspects of performing an anti-spoofing detection approach within face recognition systems.

Parveen et al. (2015) followed a general architecture comprised of a sensor, pre-processing, feature extraction, and classification steps as a basis for a taxonomy of face anti-spoofing detection methods. The methods are categorized as non-intrusive or intrusive ones, addressed according to the stillness or motion detection presented in the detection process, respectively. Twenty-nine face anti-spoofing methods were studied, and the results of the existing works were individually analyzed over public image data sets. An experimental analysis was carried out by means of four error measures: *half total error rate* (HTER), *equal error rate* (EER), *area under curve* (AUC) and *accuracy* (ACC). At the end in Parveen et al. (2015), some pros and cons are highlighted with regard to implementation complexity, user collaboration and attack coverage.

Differently from Galbally et al. (2014), which spread out the discussion on various anti-spoofing methods using different traits, we present an extensive survey that is focused on the evolution of particularly face spoofing detection methods and existing benchmarks. Instead of following a more generic categorization as those proposed in Galbally et al. (2014) and Parveen et al. (2015), all gathered works here were organized in terms of their main component parts, *i.e.,* descriptors and classifiers (see Section 2). This taxonomy was devised to help the reader to better understand the processes behind each countermeasure, and to unveil technical trends concerning different types of attacks. Since all works comprise features and learning methods, this organization seems to be the best to depict a big picture of the state-of-the-art research related to face spoofing detection.

Despite the other two surveys, our work resorts to a quantitative and analytical methodology (see Section 3) in order to support the analysis of trends of the existing face anti-spoofing approaches (see Section 4). A comparison of several methods was accomplished over the most currently used public data sets, taking into account the bias of the metrics used to assess face anti-spoofing performance (with several perfect results), differently from Galbally et al. (2014) and Parveen et al. (2015), where the results were individually analyzed. The goal is to numerically show how far spoofing detectors got considering only face. In order to fulfill such purposes, sixty-one face anti-spoofing methods were gathered (including the works that participated in the two competitions). Previous surveys did not include any in-depth assessment of existing face spoofing detection approaches (Galbally et al., 2014; Parveen et al., 2015), leaving unclear which ways should be followed and what need to be done in technical terms, considering only face spoofing detection. Differently from the philosophical and general discussion found in Galbally et al. (2014), concerning facts and challenges in the spoofing detection domain, the numerical-driven evaluation of the area allows suggesting other ways to evaluate the performance (avoiding supposedly perfect results), as well as new future research topics (*e.g.*, deep learning Fan et al., 2014, and collaborative clustering Cornujols et al., 2018) to be applied in face anti-spoofing methods (see Section 4).

1.2. Methodology

This compilation of works is based on a literature search in the following data sets: Scopus,[1] IEEE Xplore,[2] Engineering Village.[3] and Google Scholar[4] On these sources, articles were consulted considering all publications with the following keywords: **face recognition, face spoofing detection, face liveness detection, countermeasure against spoofing attacks and face anti-spoofing detection methods**. The choice of the articles was made according to the following criteria: (i) they should follow the same protocol when evaluating the study; (ii) they should indicate the results using at least one of the metrics discussed in Section 3.2, (iii) they should be comparable to other studies using the same data set, and finally (iv) they must be peer-reviewed.

It is noteworthy that there were two competitions on face spoofing detection referred in Chakka (2011), Chingovska (2013). The results obtained by the competition teams were analyzed, and the names of the groups and universities were used as references to the methods used in the first face spoofing detection competition, such as: Ambient Intelligence Laboratory (AMILAB), Center for Biometrics and Security Research, Institute of Automation, Chinese Academy of Sciences (CASIA), Idiap Research Institute (IDIAP), Institute of Intelligent Systems and Numerical Applications in Engineering, *Universidad de Las Palmas de Gran Canaria* (SIANI), Institute of Computing, Campinas University (UNICAMP) and Machine Vision Group, University of Uolu (UOLU) (Chakka, 2011). As well as, the names CASIA, Fraunhofer Institute for Computer Graphics Research (IGD), joint team from IDIAP, UOLU, UNICAMP and CPqD Telecom & IT Solutions (MaskDown), the LNM Institute of Information Technology, Jaipur (LNMIIT), Tampere University of Technology (MUVIS), University of Cagliari (PRA Lab), *Universidad Autonoma de Madrid* (ATVS) and UNICAMP refer to the teams that participated in the second face spoofing detection competition (Chingovska, 2013). Throughout this text, these team names will be cited as the reference of the method in the competition (Chakka, 2011 or Chingovska, 2013).

[1] http://www.scopus.com/.

[2] http://ieeexplore.ieee.org/Xplore/home.jsp.

[3] http://www.engineeringvillage.com/.

[4] https://scholar.google.com.