JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Deep representations for Face and Fingerprint Spoofing Detection

Dr.K.NIRANJAN REDDY [1], D.SAKETH [2], G.VINAY [3], G.VAISHNAVI [4] ,

[1]Head of the Department,Department Electronics and Communication Engineering,

[2.3.4]Student, Department of Electronics and Communication Engineering,

CMR Institute of Technology,

Hyderabad, Telangana, India.501401

***Abstract*—**

Biometrics systems have significantly improved person identification and authentication, playing an important role in personal, national, and global security. However, these systemsmight be deceived (or "spoofed") and, despite the recent advancesin spoofing detection, current solutions often rely on domain knowledge, specific biometric reading systems, and attack types. We assume a very limited knowledge about biometric spoofing at the sensor to derive outstanding spoofing detection systemsfor iris, face, and fingerprint modalities based on two deep learning approaches. The first approach consists of learning suitable convolutional network architectures for each domain, while the second approach focuses on learning the weights of the network via back-propagation. We consider nine biometric spoofing benchmarks each one containing real and fake samples of a given biometric modality and attack type and learn deep representations for each benchmark by combining and contrasting the two learning approaches.

1.INTRODUCTION

BIOMETRICS human characteristics and traits can successfully allow people identification and authentication and have been widely used for access control, surveillance,and also in national and global security systems [1]. In thelast few years, due to the recent technological improvements for data acquisition, storage and processing, and also the scientific advances in computer vision, pattern recognition,and machine learning, several biometric modalities have been largely applied to person recognition, ranging from traditional fingerprint to face, to iris, and, more recently, to vein and blood flow. Simultaneously, various *spoofing attacks* techniques have been created to defeat such biometric systems.

There are several ways to spoof a biometric system [2], [3]. Indeed, previous studies show at least eight different points of attack [4], [5] that can be divided into two main groups: *direct* and *indirect* attacks. The former considers the possibility to generate synthetic biometric samples, and is the first vulnerability point of a biometric security system acting at the sensor level. The latter includes all the remaining seven points of attacks and requires different levels of knowledge about thesystem, e.g., the matching algorithm used, the specific feature extraction procedure, database access for manipulation, and also possible weak links in the communication channels withinthe system.

The success of an anti-spoofing method is usually connectedto the modality for which it was designed. In fact, such systemsoften rely on expert knowledge to engineer features that are able to capture acquisition telltales left by specific types of attacks. However, the need of custom-tailored solutions for the myriad possible attacks might be a limiting constraint. Small changes in the attack could require the redesign of the entire system.

In this paper, we do not focus on custom-tailored solutions. Instead, inspired by the recent success of Deep Learning.

2.REVIEW OF LITERATURE

In this section, we review anti-spoofing related work for face and fingerprints, our focus in this paper.

A. Face Spoofing

We can categorize the face anti-spoofing methods into four groups [6]: user behaviour modelling, methods relying on extra devices [7], methods relying on user cooperation and, finally, data-driven characterization methods. In this section, we review data-driven characterization methods proposed in literature, the focus of our work herein.

Määttä et al. [8] used LBP operator for capturing printing artifacts and micro-texture patterns added in the fake biometric samples during acquisition. Schwartz et al. [6] explored colour,texture, and shape of the face region and used them withPartial Least Square (PLS) classifier for deciding whether a biometric sample is fake or not. Both works validated the methods with the Print Attack benchmark [9]. Lee et al. [10] also explored image-based attacks and proposed the frequencyentropy analysis for spoofing detection.

Mask-based face spoofing attacks have also been consideredthus far. Redgums et al. [11] dealt with the problem throughGabor wavelets: local Gabor binary pattern histogram sequences [12] and Gabor graphs [13] with a Gabor-phase based similarity measure [14]. redgums & Marcel [15] introducedthe 3D Mask Attack database (3DMAD), a public available 3D spoofing database, recorded with Microsoft Kinect sensor.

Kose et al. [16] demonstrated that a face verification system is vulnerable to mask-based attacks and, in another work, Kose et al. [17] evaluated the anti-spoofing method proposed by Määttä et al. [8] (originally proposed to detect photo-based spoofing attacks). Inspired by the work of Tan et al. [18], Koseet al. [19] evaluated a solution based on reflectance to detect attacks performed with 3D masks.

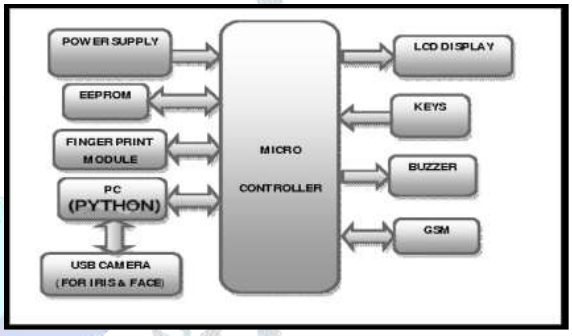
Finally, Pereira et al. [20] proposed a score-level fusion strategy in order to detect various types of attacks. In a follow-up work, Pereira et al. [21] proposed an anti-spoofing solution based on the dynamic texture, a spatio-temporal version of the original LBP. Results showed that LBP-based dynamic texturedescription has higher effectiveness than the original LBP.

B. Fingerprint Spoofing

We can categorize fingerprint spoofing detection methods roughly into two groups: hardware-based (exploring extra sensors) and software-based solutions (relying only on theinformation acquired by the standard acquisition sensor of the authentication system) [22].The validation considered the three benchmarks used in Livet 2009 – Fingerprint competition [23] captured with different optical sensors: Biometrical, Crossmatch, and Identic. Later work [24]explored the method in the presence of gummy fingers.

Ghiani et al. [25] explored Binarized Statistical Image Features (BSIF) originally proposed by Kannala et al. The BSIF was inspired in the LBP and LPQ methods. In contrastto LBP and LPQ approaches, BSIF learns a filter set by using statistics of natural images. The validation considered the LivDet 2011-Fingerprint competition benchmarks. Recent results reported in the LivDet 2013 Fingerprint Liveness Detection Competition show that fingerprint spoofing attack detection task is still an open problem with results still far from a perfect classification rate. We notice that most of the groups approach the problem with hard-coded features sometimes exploring quality metrics related to the modality (e.g., directionality and ridge strength),general texture patterns (e.g., LBP-, MBLTP-, and LPQ-based methods), and filter learning through natural image statistics. This last approach seems to open a new research trend, which seeks to model the problem learning features directly fromthe data. We follow this approach in this work, assuming littlea priori knowledge about acquisition-level biometric spoofing and exploring deep representations of the data.

3.BLOCK DIAGRAM



4.METHODOLOGY

How face detection works. Face detection application use AI algorithms, ML, statistical analysis and image processing to find human faces within larger images and distinguish them from nonface objects and non finger objects such as landscapes, buildings and other human body parts.

5.SYSTEM ANALYSIS

1. Input image
2. Database creation
3. Preprocessing
4. Evaluation Protocol
5. Convolutional neural network
6. Work Flow
7. Results

5.1 Preprocessing

A few basic preprocessing operations were executed on face and fingerprint images in order to properly learn representations for these benchmarks. This preprocessing led to images with sizes as presented in Table II and are described in the next two sections.

1)Face Images: Given that the face benchmarks considered in this work are video-based, we first evenly subsample 10 frames from each input video. Then, we detect the face position using Viola & Jones [82] and crop a region of 200 x 200 pixels centred at the detected window.

2)Fingerprint Images: Given the diverse nature of images captured from different sensors, here the preprocessing is defined according to the sensor type.

(a)Biometric: we cropped the central region of size in columns and rows corresponding to 70% of the original image dimensions.

(b)Italdata and Crossmatch: we cropped the central region of size in columns and rows respectively corresponding to 60% and 90% of the original image columns and rows.

(c)Swipe: As the images acquired by this sensor contain a variable number of blank rows at the bottom, the average number of non-blank rows M was first calculated from the training images. Then, in order to obtain images of a common size with non-blank rows, we removed their blank rows at the bottom and rescaled them to M rows. Finally, we cropped the central region corresponding to 90% of original image columns and M rows.

The rationale for these operations is based on the observation that fingerprint images in LivDet2013 tend to have a large portion of background content and therefore we try to discard such information that could otherwise mislead the representation learning process. The percentage of cropped columns and rows differs among sensors because they capture images of different sizes with different amounts of background.

5.2 Evaluation Protocol

For each benchmark, we learn deep representations from their training images according to the methodology described in Section IV-A for architecture optimization (AO) and in Section IV-B for filter optimization (FO). We follow the standard evaluation protocol of all benchmarks and evaluate the methods in terms of detection accuracy (ACC) and half total error rate (HTER), as these are the metrics used to assess progress in the set of benchmarks considered herein. Precisely, for a given benchmark and convolutional network already trained, results are obtained by:

1)Retrieving prediction scores from the testing samples.

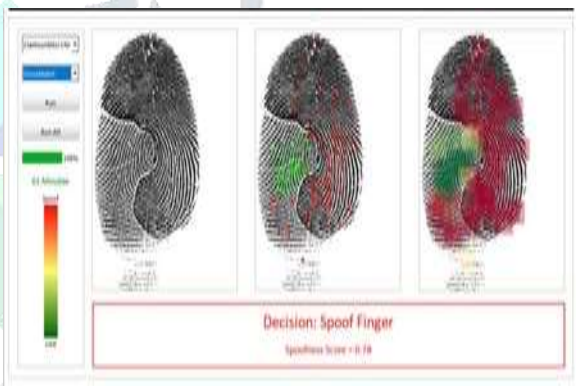
2)Calculating a threshold τ above which samples are predicted as attacks.

3)Computing ACC and/or HTER using τ and test predictions.

Here are some common approaches in anti-spoofing:

1. Texture Analysis
2. Motion Analysis

1. Texture Analysis



2.Motion Analysis

5.3 Convolutional neural network

Convolutional neural network (CNN) is a regularized type of feed-forward neural network that learns feature engineering by itself via filters (or kernel) optimization. Vanishing gradients and exploding gradients, seen during backpropagation in earlier neural networks, are prevented by using regularized weights over fewer connections.[1][2] For example, for each neuron in the fully-connected layer 10,000 weights would be required for processing an image sized 100 × 100 pixels. However, applying cascaded convolution (or cross-correlation) kernels,[3][4] only 25 neurons are required to process 5x5-sized tiles.[5][6] Higher-layer features are extracted from wider context windows, compared to lower-layer features.

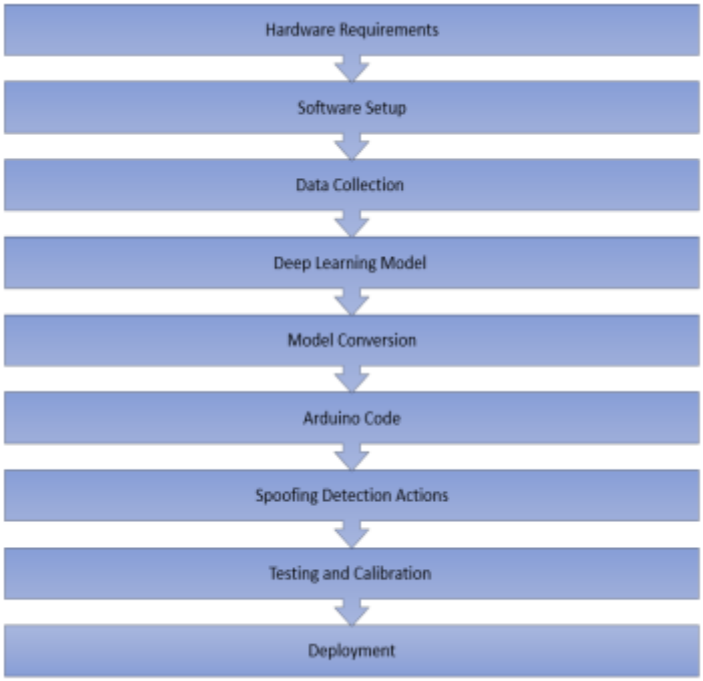
Applications:

1. Image recognition
2. Video analysis
3. Natural language processing
4. Anomaly Detection
5. Drug discovery
6. Time series forecasting
7. Cultural Heritage and 3D-datasets

Advantages

1. No require human supervision required.
2. Automatic feature extraction.
3. Highly accurate at image recognition & classification.
4. Weight sharing.
5. Minimizes computation.
6. Uses same knowledge across all image locations.
7. Ability to handle large datasets.
8. Hierarchical learning.

5.4 Work Flow



Our implementation for architecture optimization (AO) is based on Hyperopt-convnet which in turn is based on Theano . LibSVM is used for learning the linear clas- sifiers via Scikit-learn. The code for feature extraction runs onGPUs due to Theano and the remaining part is multithreaded and runs on CPUs. We extended Hyperopt-convnet in order to consider the operations and hyperparameters as described , we will make the source code freely available in Running times are reported with this software stack and are computed in an Intel i7 @3.5GHz with a Tesla K40 that, on average, takes less than one dayto optimize an architecture — i.e., to probe 2,000 candidate architectures .

5.5 Results

We evaluate the effectiveness of the proposed methods for spoofing detection. We show experiments for the architecture optimization and filter learning approaches along with their combination for detecting iris, face, and fingerprint spoofing on the nine benchmarks described. We also present results for the *spoof net*, which incorporates some domain-knowledge on the problem. We compare all of the results with the state-of-the-art counterparts. Finally,we discuss the pros and cons of using such approaches and their combination along with efforts to understand the type of features learned and some efficiency questions when testing the proposed methods.

6. CONCLUSIONS

In this work, we investigated two deep representation re- search approaches for detecting spoofing in different biometric modalities. On one hand, we approached the problem by learning representations directly from the data through architecture optimization with a final decision-making step atopthe representations. On the other,

we sought to learn filter weights for a given architecture using the well-known back-propagation algorithm. As the two approaches might seem naturally connected, we also examined their interplay when taken together. In addition, we incorporated our experience with architecture optimization as well as with training filter weight for a given architecture into a more interesting and adapted network, *spoof net*.

As the data tell it all, the decision to which path to follow can also come from the data. Using the evaluation/validation set during training, the researcher/developer can opt for optimizing architectures, learn filters or both. If training time is an issue and a solution must be presented overnight, it might be interesting to consider an already learned network that incorporates some additional knowledge in its design. In this sense, spoof net could be a good choice. In all cases, if the developer can incorporate more training examples, the approaches might benefit from such augmented training data. The proposed approaches can also be adapted to other biometric modalities not directly dealt with herein. The most important difference would be in the input type of data since all discussed solutions directly learn their representations from the data.

For the case of iris spoofing detection, here we dealt only with iris spoofing printed attacks and some experimental datasets using cosmetic contact lenses have recently become available allowing researchers to study this specific type of spoofing [7], [8]. For future work, we intend to evaluate such datasets using the proposed approaches here and also consider other biometric modalities such as palm, vein, and gait.

It is important to emphasise the interplay between the architecture and filter optimization approaches for the spoofing problem. It is well-known in the deep learning literature that when thousands of samples are available for learning, the filter learning approach is a promising path. Indeed, we could corroborate this through fingerprint benchmarks that considers a few thousand samples for training. However, it was not the case for faces and two iris benchmarks which suffer from the small sample size problem (SSS) and subject variability hindering the filter learning process. In these cases, the architecture optimization approach was able to learn representative and discriminative features providing comparable spoofing effectiveness to the SOTA results in almost all benchmarks, and specially outperforming them in three out of four SOTA results when the filter learning approach failed. It is worth mentioning that sometimes it is still possible to learn meaningful features from the data even with a small sample size for training. We believe this happens in more well-posed datasets with less variability between training/testing data as it is the case in which the AO approach achieved 99.38% just 0.37% behind the SOTA result.

Finally, it is important to take all the results discussed herein with a grain of salt. We are not presenting the final word in spoofing detection. In fact, there are important additional research that could finally take this research another step forward. We envision the application of deep learning representations on top of pre-processed image feature maps (e.g., LBP-like feature maps, acquisition-based maps exploring noise signatures, visual rhythm representations, etc.). With an n-layer feature representation, we might be able to explore features otherwise not possible using the raw data. In addition, exploring temporal coherence and fusion would be also important for video-based attacks.

ACKNOWLEDGMENT

We are extremely grateful to Dr.M.JangaReddy, Director, Dr.B.Satyanarayana, Principal and Dr.K.Niranjan Reddy, Head of Department ,Electronics and Communication Engineering, CMR Institute of Technology for their inspiration and valuable guidance during the entire duration.

We are extremely thankful to our guide Dr.K.Niranjan Reddy, Head of the Department, ECE , CMR Institute of Technology for his constant guidance, encouragement and moral support throughout the project.

REFERENCES

[1] A. K. Jain and A. Ross, *Handbook of Biometrics*. Springer, 2008, Introduction to biometrics, pp. 1–22.

[2] C. Rathgeb and A. Uhl, "Attacking iris recognition: An efficient hill- climbing technique," in *IEEE/IAPR International Conference on Pattern Recognition (ICPR)*, 2010, pp. 1217–1220.

[3] ——, "Statistical attack against iris-biometric fuzzy commitment schemes," in *IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops (CVPRW)*, 2011, pp. 23–30.

[4] J. Galbally, J. Fierrez, and J. Ortega-garcia, "Vulnerabilities in biometric systems: Attacks and recent advances in liveness detection," *Database*,vol. 1, no. 3, pp. 1–8, 2007, available at http://atvs.ii.uam.es/files/2007 SWB VulnerabilitiesRecentAdvances_Galbally.pdf.

[5] N. K. Ratha, J. H. Connell, and R. M. Bolle, "An analysis of minutiae matching strength," in *International Conference on Audio-and Video- Based Biometric Person Authentication*, 2001, pp. 223–228.

[6] W. Robson Schwartz, A. Rocha, and H. Pedrini, "Face spoofing detection through partial least squares and low-level descriptors," in *IEEE Int. Joint Conference on Biometrics (IJCB)*, 2011, pp. 1 –8.

[7] D. Yi, Z. Lei, Z. Zhang, and S. Li, "Face anti-spoofing: Multi-spectral approach," in *Handbook of Biometric Anti-Spoofing*, ser. Advances in Computer Vision and Pattern Recognition, S. Marcel, M. S. Nixon, andS. Z. Li, Eds.S. Z. Li, Eds. Springer London, 2014, pp. 83–102.

[8] J. Määttä, A. Hadid, and M. Pietikäinen, "Face spoofing detection from single images using micro-texture analysis," in *IEEE Int. Joint Conference on Biometrics (IJCB)*, 2011, pp. 1 – 7.

[9] A. Anjos and S. Marcel, "Counter-measures to photo attacks in face recognition: a public database and a baseline," in *International Joint Conference on Biometrics 2011*, 2011, pp. 1–7.

[10] T.-W. Lee, G.-H. Ju, H.-S. Liu, and Y.-S. Wu, "Liveness detection usingfrequency entropy of image sequences," in *IEEE Int. Conference on Acoustics, Speech, and Signal Processing (ICASSP)*, 2013, pp. 2367– 2370.

[11] N. Erdogmus and S. Marcel, "Spoofing 2D face recognition systems with 3D masks," in *Int. Conference of the Biometrics Special Interest Group (BIOSIG)*, 2013, pp. 1–8.

[12] W. Zhang, S. Shan, W. Gao, X. Chen, and H. Zhang, "Local gabor binary pattern histogram sequence (lgbphs): a novel non-statistical model for face representation and recognition," in *IEEE Int.*

Conference on Computer Vision (ICCV), vol. 1, 2005, pp. 786–791.

[13] L. Wiskott, J.-M. Fellous, N. Kuiger, and C. Von der Malsburg, "Face recognition by elastic bunch graph matching," *IEEE Trans. Pattern Anal.Mach. Intell.*, vol. 19, no. 7, pp. 775–779, 1997.

[14] M. Günther, D. Haufe, and R. P. Würtz, "Face recognition with disparity corrected gabor phase differences," in *Int. Conference on Artificial Neural Networks and Machine Learning (ICANN)*, 2012, pp. 411–418.

[15] N. Erdogmus and S. Marcel, "Spoofing in 2d face recognition with 3d masks and anti-spoofing with kinect," in *IEEE Int. Conference on Biometrics: Theory Applications and Systems (VISAPP)*, 2013, pp. 1–6.

[16] N. Kose and J.-L. Dugelay, "On the vulnerability of face recognition systems to spoofing mask attacks," in *IEEE Int. Conference on Acoustics, Speech, and Signal Processing (ICASSP)*, 2013, pp. 2357–2361

[17] ——, "Countermeasure for the protection of face recognition systems against mask attacks," in *IEEE Int. Conference and Workshops on Automatic Face and Gesture Recognition (FG)*, 2013, pp. 1–6.

[18] X. Tan, Y. Li, J. Liu, and L. Jiang, "Face liveness detection from a single image with sparse low rank bilinear discriminative model," in *EuropeanConference on Computer Vision (ECCV)*, 2010, pp. 504–517.

[19] N. Kose and J.-L. Dugelay, "Reflectance analysis based countermeasuretechnique to detect face mask attacks," in *Int. Conference on Digital Signal Processing (DSP)*, 2013, pp. 1–6.

[20] T. de Freitas Pereira, A. Anjos, J. De Martino, and S. Marcel, "Can face anti-spoofing countermeasures work in a real world scenario?" in *IAPR Int. Conference on Biometrics (ICB)*, 2013, pp. 1–8.

[21] T. Freitas Pereira, J. Komulainen, A. Anjos, J. De Martino, A. Hadid,M. Pietikainen, and S. Marcel, "Face liveness detection using dynamic texture," *EURASIP Journal on Image and Video Processing*, vol. 2014, no. 1, p. 2, 2014.

[22] L. Ghiani, D. Yambay, V. Mura, S. Tocco, G. Marcialis, F. Roli, and S. Schuckcrs, "Livdet 2013 – fingerprint liveness detection competition," in *International Conference on Biometrics (ICB)*, 2013, pp. 1–6. [Online]. Available: http://prag.diee.unica.it/fldc/

[23] G. L. Marcialis, A. Lewicke, B. Tan, P. Coli, D. Grimberg,A. Congiu, A. Tidu, F. Roli, and S. A. C. Schuckers, "Livdet 2009– first international fingerprint liveness detection competition," in Int. Conference on Image Analysis and Processing (ICIAP), ser. Lecture Notes in Computer Science, P. Foggia, C. Sansone, and M. Vento, Eds., vol. 5716. Springer, 2009, pp. 12–23. [Online]. Available: http://prag.diee.unica.it/LivDet09

[24] J. Galbally, F. Alonso-Fernandez, J. Fierrez, and J. Ortega-Garcia, "A high performance fingerprint liveness detection method based on quality related features," *Future Generation Computer Systems*, vol. 28, no. 1, pp. 311–321, 2012.

[25] D. Yambay, L. Ghiani, P. Denti, G. Marcialis, F. Roli, and S. Schuckers, "Livdet 2011 – fingerprint liveness detection competition," in *IAPR Int. Conference on Biometrics (ICB)*, 2012, pp. 208–215. [Online]. Avail- able: http://people.clarkson.edu/projects/biosal/fingerprint/index.php

L,