Advances in Intelligent Systems and Computing 951

Francisco Martínez Álvarez
Alicia Troncoso Lora
José António Sáez Muñoz
Héctor Quintián
Emilio Corchado *Editors*

# International Joint Conference: 12th International Conference on Computational Intelligence in Security for Information Systems (CISIS 2019) and 10th International Conference on EUropean Transnational Education (ICEUTE 2019)

## Seville, Spain, May 13–15, 2019, Proceedings

International Conference on
CISIS
Computational Intelligence in Security for Information Systems

International Conference on
ICEUTE
EUROPEAN
Transnational Education

Springer

# Advances in Intelligent Systems and Computing

## Volume 951

**Series Editor**

Janusz Kacprzyk, Systems Research Institute, Polish Academy of Sciences,
Warsaw, Poland

**Advisory Editors**

Nikhil R. Pal, Indian Statistical Institute, Kolkata, India
Rafael Bello Perez, Faculty of Mathematics, Physics and Computing,
Universidad Central de Las Villas, Santa Clara, Cuba
Emilio S. Corchado, University of Salamanca, Salamanca, Spain
Hani Hagras, Electronic Engineering, University of Essex, Colchester, UK
László T. Kóczy, Department of Automation, Széchenyi István University,
Gyor, Hungary
Vladik Kreinovich, Department of Computer Science, University of Texas
at El Paso, El Paso, TX, USA
Chin-Teng Lin, Department of Electrical Engineering, National Chiao
Tung University, Hsinchu, Taiwan
Jie Lu, Faculty of Engineering and Information Technology,
University of Technology Sydney, Sydney, NSW, Australia
Patricia Melin, Graduate Program of Computer Science, Tijuana Institute
of Technology, Tijuana, Mexico
Nadia Nedjah, Department of Electronics Engineering, University of Rio de Janeiro,
Rio de Janeiro, Brazil
Ngoc Thanh Nguyen, Faculty of Computer Science and Management,
Wrocław University of Technology, Wrocław, Poland
Jun Wang, Department of Mechanical and Automation Engineering,
The Chinese University of Hong Kong, Shatin, Hong Kong

The series "Advances in Intelligent Systems and Computing" contains publications on theory, applications, and design methods of Intelligent Systems and Intelligent Computing. Virtually all disciplines such as engineering, natural sciences, computer and information science, ICT, economics, business, e-commerce, environment, healthcare, life science are covered. The list of topics spans all the areas of modern intelligent systems and computing such as: computational intelligence, soft computing including neural networks, fuzzy systems, evolutionary computing and the fusion of these paradigms, social intelligence, ambient intelligence, computational neuroscience, artificial life, virtual worlds and society, cognitive science and systems, Perception and Vision, DNA and immune based systems, self-organizing and adaptive systems, e-Learning and teaching, human-centered and human-centric computing, recommender systems, intelligent control, robotics and mechatronics including human-machine teaming, knowledge-based paradigms, learning paradigms, machine ethics, intelligent data analysis, knowledge management, intelligent agents, intelligent decision making and support, intelligent network security, trust management, interactive entertainment, Web intelligence and multimedia.

The publications within "Advances in Intelligent Systems and Computing" are primarily proceedings of important conferences, symposia and congresses. They cover significant recent developments in the field, both of a foundational and applicable character. An important characteristic feature of the series is the short publication time and world-wide distribution. This permits a rapid and broad dissemination of research results.

**** Indexing: The books of this series are submitted to ISI Proceedings, EI-Compendex, DBLP, SCOPUS, Google Scholar and Springerlink ****

More information about this series at http://www.springer.com/series/11156

Francisco Martínez Álvarez ·
Alicia Troncoso Lora · José António Sáez Muñoz ·
Héctor Quintián · Emilio Corchado
Editors

# International Joint Conference: 12th International Conference on Computational Intelligence in Security for Information Systems (CISIS 2019) and 10th International Conference on EUropean Transnational Education (ICEUTE 2019)

Seville, Spain, May 13–15, 2019, Proceedings

Springer

*Editors*
Francisco Martínez Álvarez
Data Science and Big Data Lab
Pablo de Olavide University
Seville, Spain

Alicia Troncoso Lora
Data Science and Big Data Lab
Pablo de Olavide University
Seville, Spain

José António Sáez Muñoz
University of Salamanca
Salamanca, Spain

Héctor Quintián
Department of Industrial Engineering
University of A Coruña
A Coruña, Spain

Emilio Corchado
University of Salamanca
Salamanca, Spain

ISSN 2194-5357 ISSN 2194-5365 (electronic)
Advances in Intelligent Systems and Computing
ISBN 978-3-030-20004-6 ISBN 978-3-030-20005-3 (eBook)
https://doi.org/10.1007/978-3-030-20005-3

© Springer Nature Switzerland AG 2020
This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.
The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.
The publisher, the authors and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, expressed or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

# Preface

This volume of Advances in Intelligent and Soft Computing contains accepted papers presented at CISIS 2019 and ICEUTE 2019, both conferences held in the beautiful and historic city of Seville (Spain), in May 2019.

The aim of the twelfth CISIS 2019 conference is to offer a meeting opportunity for academic and industry-related researchers belonging to the various, vast communities of computational intelligence, information security, and data mining. The need for intelligent, flexible behavior by large, complex systems, especially in mission-critical domains, is intended to be the catalyst and the aggregation stimulus for the overall event.

After a thorough peer review process, the CISIS 2019 International Program Committee selected 20 papers which are published in these conference proceedings achieving an acceptance rate of 30%. In this relevant edition, a special emphasis was put on the organization of special sessions. One special session was organized related to relevant topics as: From the least to the least: cryptographic and data analytics solutions to fulfil least minimum privilege and endorse least minimum effort in information systems.

In the case of 10th ICEUTE 2019, the International Program Committee selected 15 papers, which are published in these conference proceedings. Two special sessions were organized related to relevant topics as: Looking for Camelot: New Approaches to Asses Competencies; Innovation in Computer Science Education.

The selection of papers was extremely rigorous in order to maintain the high quality of the conference, and we would like to thank the members of the Program Committees for their hard work in the reviewing process. This is a crucial process to the creation of a high standard conference, and the CISIS and ICEUTE conferences would not exist without their help.

CISIS 2019 and ICEUTE 2019 conferences enjoyed outstanding keynote speeches by distinguished guest speakers: Prof. Dieu Tien Bui (University of South-Eastern Norway, Norway), Prof. Juan Manuel Corchado (University of Salamanca, Spain) and Prof. Julien Jacques (University of Lyon, France).

CISIS 2019 special edition, as a follow-up of the conference, we anticipate further publication of selected papers in a special issue, in the prestigious Logic Journal of the IGPL (Oxford Academic).

Particular thanks go as well to the conference main sponsors, Startup Ole, IEEE SMC Spanish Chapter, the International Federation for Computational Logic, who jointly contributed in an active and constructive manner to the success of this initiative.

We would like to thank all the special session organizers, contributing authors, as well as the members of the Program Committees and the Local Organizing Committee for their hard and highly valuable work. Their work has helped to contribute to the success of the CISIS 2019 and ICEUTE 2019 events.

May 2019

Francisco Martínez Álvarez
Alicia Troncoso Lora
José António Sáez Muñoz
Héctor Quintián
Emilio Corchado

# CISIS 2019

## Organization

### General Chairs

| | |
|---|---|
| Francisco Martínez Álvarez | Pablo de Olavide University, Spain |
| Alicia Troncoso Lora | Pablo de Olavide University, Spain |
| Emilio Corchado | University of Salamanca, Spain |

### International Advisory Committee

| | |
|---|---|
| Ajith Abraham | Machine Intelligence Research Labs—MIR Labs, Europe |
| Michael Gabbay | King's College London, UK |
| Antonio Bahamonde | University of Oviedo at Gijón, Spain |

### Program Committee Chairs

| | |
|---|---|
| Emilio Corchado | University of Salamanca, Spain |
| Francisco Martínez Álvarez | Pablo de Olavide University, Spain |
| Alicia Troncoso Lora | Pablo de Olavide University, Spain |
| Héctor Quintián | University of A Coruña, Spain |

## Program Committee

| | |
|---|---|
| Adolfo R. De Soto | University of Leon, Spain |
| Agustin Martin Muñoz | CSIC, Spain |
| Alberto Peinado | Universidad de Malaga, Spain |
| Amparo Fuster-Sabater | CSIC, Spain |

| | |
|---|---|
| Ana I. González-Tablas | University Carlos III de Madrid, Spain |
| Andreea Vescan | Babes-Bolyai University, Cluj-Napoca, Romania |
| Angel Arroyo | University of Burgos, Spain |
| Angel Martin Del Rey | University of Salamanca, Spain |
| Antonio J. Tomeu-Hardasmal | University of Cadiz, Spain |
| Camelia Serban | Babes-Bolyai University, Cluj-Napoca, Romania |
| Carlos Cambra | University of Burgos, Spain |
| Carlos Pereira | ISEC, Portugal |
| Carmen Benavides | University of León, Spain |
| Cosmin Sabo | Technical University of Cluj-Napoca, Romania |
| Cristina Alcaraz | University of Malaga, Spain |
| David Alvarez Leon | University of León, Spain |
| David Arroyo | CSIC, Spain |
| Eduardo Solteiro Pires | UTAD University, Portugal |
| Enrique Onieva | University of Deusto, Spain |
| Fernando Tricas | University of Zaragoza, Spain |
| Francisco Martínez Álvarez | Pablo de Olavide University, Spain |
| Francisco Rodríguez-Sedano | University of León, Spain |
| Guillermo Morales-Luna | CINVESTAV-IPN, Mexico |
| Héctor Quintián | University of A Coruña, Spain |
| Hugo Scolnik | University of Buenos Aires, Argentina |
| Ioana Zelina | Technical University of Cluj-Napoca, North University Center in Baia Mare, Romania |
| Isaac Agudo | University of Malaga, Spain |
| Isaias Garcia | University of León, Spain |
| Javier Areitio | University of Deusto, Spain |
| Jesús Díaz-Verdejo | University of Granada, Spain |
| Joan Borrell | Universitat Autònoma de Barcelona, Spain |
| Jose A. Onieva | University of Malaga, Spain |
| José F. Torres | Pablo de Olavide University, Spain |
| Jose Luis Calvo-Rolle | University of A Coruña, Spain |
| Jose Luis Imana | Polytechnic University of Madrid, Spain |
| José Luis Casteleiro-Roca | University of A Coruña, Spain |
| Jose M. Molina | University Carlos III de Madrid, Spain |
| Jose Manuel Gonzalez-Cava | Universidad de La Laguna, Spain |
| Jose Manuel Lopez-Guede | Basque Country University, Spain |
| Josep Ferrer | Universitat de les Illes Balears, Spain |
| Juan Jesús Barbarán | University of Granada, Spain |
| Juan Pedro Hecht | University of Buenos Aires, Argentina |
| Leocadio G. Casado | University of Almeria, Spain |
| Lidia Sánchez-González | University of León, Spain |
| Luis Hernandez Encinas | ITEFI, Spain |
| Manuel Grana | University of Basque Country, Spain |
| Michal Choras | ITTI Ltd., Poland |

| | |
|---|---|
| Paulo Moura Oliveira | UTAD University, Portugal |
| Paulo Novais | University of Minho, Portugal |
| Petrica Pop | Technical University of Cluj-Napoca, North University Center at Baia Mare, Romania |
| Rafael Alvarez | University of Alicante, Spain |
| Rafael Corchuelo | University of Seville, Spain |
| Ramón-Ángel Fernández-Díaz | University of León, Spain |
| Raúl Durán | University of Alcalá, Spain |
| Robert Burduk | Wroclaw University of Technology, Poland |
| Roman Senkerik | TBU in Zlin, Czechia |
| Salvador Alcaraz | Miguel Hernandez University, Spain |
| Sorin Stratulat | Université de Lorraine, France |
| Castejon Limas | University of León, Spain |
| Urko Zurutuza | Mondragon University, Spain |
| Vicente Matellan | University of León, Spain |
| Wenjian Luo | University of Science and Technology of China, China |
| Zuzana Kominkova Oplatkova | Tomas Bata University in Zlin, Czechia |

## Special Sessions

### From the Least to the Least: Cryptographic and Data Analytics Solutions to Fulfil Least Minimum Privilege and Endorse Least Minimum Effort in Information Systems

#### Program Committee

| | |
|---|---|
| Víctor Gayoso Martínez (Organizer) | CSIC, Spain |
| Agustín Martín (Organizer) | CSIC, Spain |
| Alberto Peinado | Universidad de Malaga, Spain |
| Amalia Orúe | CSIC, Spain |
| Araceli Queiruga | Universidad de Salamanca, Spain |
| David Arroyo | CSIC, Spain |
| Luis Hernández | Institute of Physical and Information Technologies (ITEFI), Spain |
| Sara Cardell | UNICAMP Universidade Estadual de Campinas, Brazil |
| Slobodan Petrovic | Gjøvik University College, Norway |

## CISIS 2019 Organizing Committee

| | |
|---|---|
| Francisco Martínez Álvarez | Pablo de Olavide University, Spain |
| Alicia Troncoso Lora | Pablo de Olavide University, Spain |
| José F. Torres Maldonado | Pablo de Olavide University, Spain |
| David Gutiérrez-Avilés | Pablo de Olavide University, Spain |
| Rubén Pérez Chacón | Pablo de Olavide University, Spain |
| Ricardo L. Talavera Llames | Pablo de Olavide University, Spain |
| Federico Divina | Pablo de Olavide University, Spain |
| Gualberto Asencio Cortés | Pablo de Olavide University, Spain |
| Miguel García-Torres | Pablo de Olavide University, Spain |
| Cristina Rubio-Escudero | University of Seville, Spain |
| María Martínez-Ballesteros | University of Seville, Spain |
| Álvaro Herrero | University of Burgos, Spain |
| José Antonio Sáez-Muñoz | University of Salamanca, Spain |
| Héctor Quintián | University of A Coruña, Spain |
| Emilio Corchado | University of Salamanca, Spain |

# ICEUTE 2019

## Organization

### General Chairs

| | |
|---|---|
| Francisco Martínez Álvarez | Pablo de Olavide University, Spain |
| Alicia Troncoso Lora | Pablo de Olavide University, Spain |
| Emilio Corchado | University of Salamanca, Spain |

### Program Committee Chairs

| | |
|---|---|
| Emilio Corchado | University of Salamanca, Spain |
| Francisco Martínez Álvarez | Pablo de Olavide University, Spain |
| Alicia Troncoso Lora | Pablo de Olavide University, Spain |
| Héctor Quintián | University of A Coruña, Spain |

### Program Committee

| | |
|---|---|
| Antonio Morales Esteban | University of Seville, Spain |
| Carlos Cambra | University of Burgos, Spain |
| Damián Cerero | University of Seville, Spain |
| Federico Divina | Pablo de Olavide University, Spain |
| Francisco Gómez-Vela | Pablo de Olavide University, Spain |
| Francisco Martínez Álvarez | Pablo de Olavide University, Spain |
| Héctor Quintián | University of A Coruña, Spain |
| José F. Torres | Pablo de Olavide University, Spain |
| José Lázaro Amaro Mellado | University of Seville, Spain |
| Jose Manuel Gonzalez-Cava | University of La Laguna, Spain |
| Khawaja Asim | Pakistan Institute of Engineering and Applied Sciences (PIEAS), Pakistan |
| Miguel García-Torres | Universidad Pablo de Olavide, Spain |

## Special Sessions

### Looking for Camelot: New Approaches to Asses Competencies

### Program Committee

| | |
|---|---|
| Araceli Queiruga-Dios (Organizer) | University of Salamanca, Spain |
| Agustín Martín Muñoz | CSIC, Spain |
| Ángel Martín del Rey | University of Salamanca, Spain |
| Ascensión Hernández Encinas | University of Salamanca, Spain |
| Cristina M. R. Caridade | Coimbra Superior Institute of Engineering, Portugal |
| Daniela Richtarikova | SjF STU, Slovakia |
| Deolinda Rasteiro | Coimbra Superior Institute of Engineering, Portugal |
| Fatih Yilmaz | Ankara Hacı Bayram Veli University, Turkey |
| Ion Mierlus-Mazilu | Technical University of Civil Engineering of Bucharest, Bucharest |
| José Javier Rodriguez Santos | University of Salamanca, Spain |
| José María Chamoso Sánchez | University of Salamanca, Spain |
| Juan J. Bullon Perez | University of Salamanca, Spain |
| Luis Hernandez Encinas | Institute of Physical and Information Technologies (ITEFI), Spain |
| María Jesús Sánchez Santos | University of Salamanca, Spain |
| María José Cáceres García | University of Salamanca, Spain |
| Marie Demlova | Czech Technical University in Prague, Czechia |
| Michael Carr | DIT, Ireland |
| Snezhana Gocheva-Ilieva | University of Plovdiv Paisii Hilendarski, Bulgaria |
| Víctor Gayoso Martínez | CSIC, Spain |

### Innovation in Computer Science Education

### Program Committee

| | |
|---|---|
| Cristina Rubio-Escudero (Organizer) | University of Seville, Spain |
| María Martínez-Ballesteros (Organizer) | University of Seville, Spain |
| José C. Riquelme (Organizer) | University of Seville, Spain |
| Damián Cerero | University of Seville, Spain |
| Francisco Martínez Álvarez | Universidad Pablo de Olavide, Spain |
| Héctor Quintián | University of A Coruña, Spain |

| | |
|---|---|
| José F. Torres | Pablo de Olavide University, Spain |
| Samuel Conesa | Pablo de Olavide University, Spain |

## ICEUTE 2019 Organizing Committee

| | |
|---|---|
| Francisco Martínez Álvarez | Pablo de Olavide University, Spain |
| Alicia Troncoso Lora | Pablo de Olavide University, Spain |
| José F. Torres Maldonado | Pablo de Olavide University, Spain |
| David Gutiérrez-Avilés | Pablo de Olavide University, Spain |
| Rubén Pérez Chacón | Pablo de Olavide University, Spain |
| Ricardo L. Talavera Llames | Pablo de Olavide University, Spain |
| Federico Divina | Pablo de Olavide University, Spain |
| Gualberto Asencio Cortés | Pablo de Olavide University, Spain |
| Miguel García-Torres | Pablo de Olavide University, Spain |
| Cristina Rubio-Escudero | University of Seville, Spain |
| María Martínez-Ballesteros | University of Seville, Spain |
| Álvaro Herrero | University of Burgos, Spain |
| José Antonio Sáez-Muñoz | University of Salamanca, Spain |
| Héctor Quintián | University of A Coruña, Spain |
| Emilio Corchado | University of Salamanca, Spain |

# Contents

General Track

**Special Session: From the Least to the Least: Cryptographic and Data Analytics Solutions to Fulfill Least Minimum Privilege and Endorse Least Minimum Effort in Information Systems**

Special Session: Looking for Camelot: New Approaches to Asses Competencies

Special Session: Innovation in Computer Science Education

# General Track

# Perturbing Convolutional Feature Maps with Histogram of Oriented Gradients for Face Liveness Detection

Yasar Abbas Ur Rehman(✉), Lai-Man Po, Mengyang Liu, Zijie Zou, and Weifeng Ou

Department of Electronic Engineering,
City University of Hong Kong, Kowloon, Hong Kong
{yaurehman2-c,mengyaliu7-c,zijiezou2-c,
weifengou2-c}@my.cityu.edu.hk, eelmpo@cityu.edu.hk

**Abstract.** Face anti-spoofing in unconstrained environment is one of the key issues in face biometric based authentication and security applications. To minimize the false alarms in face anti-spoofing tests, this paper proposes a novel approach to learn perturbed feature maps by perturbing the convolutional feature maps with Histogram of Oriented Gradients (HOG) features. The perturbed feature maps are learned simultaneously during training of Convolution Neural Network (CNN) for face anti-spoofing, in an end-to-end fashion. Extensive experiments are performed on state-of-the-art face anti-spoofing databases, like OULU-NPU, CASIA-FASD and Replay-Attack, in both intra-database and cross-database scenarios. Experimental results indicate that the proposed framework perform significantly better compare to previous state-of-the-art approaches in both intra-database and cross-database face anti-spoofing scenarios.

**Keywords:** Convolution Neural Networks · Face liveness detection · Histogram of Oriented Gradients

## 1 Introduction

Preserving the privacy of individuals using their biometric traits has been a prevailing issue in biometric based user authentication systems. Among various biometric traits like fingerprint, palm vein and iris; face biometric based user authentication systems have been widely used in mobile applications, boarder security, and automatic transactions [1]. However, face biometric based user authentication systems are highly vulnerable to face spoofing attacks, also known as Presentation Attacks (PA). These face PA vary from a simple photographic image to complex and expensive 3D realistic Mask. Due to surge in the availability of high-end cameras, printers and display screens, and the easy access to user face information from social media like Facebook, twitter, WeChat and Instagram etc., face PA could be easily developed with limited resources. As such, it has become indispensable to develop a robust face anti-spoofing system that can detect and classify a range of face PA with high accuracy and low tolerance [2].

F. Martínez Álvarez et al. (Eds.): CISIS 2019/ICEUTE 2019, AISC 951, pp. 3–13, 2020.
https://doi.org/10.1007/978-3-030-20005-3_1

To detect face PA, a wide range of face anti-spoofing (also known as face liveness detection) algorithms and systems have been proposed in literature. These face liveness detection algorithms and systems can be divided into two broader categories, i.e. Hand-crafted features based liveness detection systems [3] and deep Convolution Neural Networks (CNN) [4] based face liveness detection systems. Although, the performance of face liveness detection methods using CNN in intra-database scenarios has been quite remarkable [5], it only imply an upper bound on the performance of face liveness detection method under evaluation. Further, improving the performance of face liveness detection in cross-database domain is still an open research problem [6]. To make matters worse, current face anti-spoofing databases possesses low diversity, number of samples and environmental scenarios. Most face anti-spoofing techniques proposed so far have focused only on liveness detection (binary classification) problem without paying much attention to engineering the hidden layers of CNN classifiers. Recently, CNN classifiers have shown to improve its performance when trained with an additional domain knowledge data [7–9].

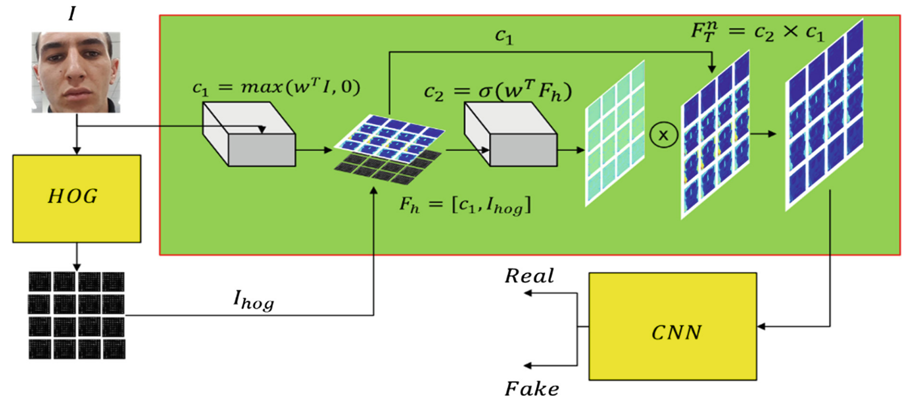

**Fig. 1.** Proposed approach for perturbing convolutional feature maps with HOG features for face liveness detection

Motivating by these facts, in this paper, we propose a novel approach for face liveness detection by perturbing the hidden convolutional layers of CNN with Histogram of Oriented Gradient (HOG) features. As shown in Fig. 1, before feeding an RGB face image to the CNN classifier, the HOG features of face image are computed first. The HOG features in the form of a 2-dimensional matrix is then concatenated with each output feature map of a candidate convolutional layer of CNN. Afterwards, the concatenated HOG features and convolutional feature maps are passed through a convolution layer to compute a weight matrix. The computed weight matrix is then multiplied with the convolution feature maps of candidate convolution layer to generate perturbed feature maps. These perturbed feature maps are then passed through the rest of the layers in the CNN for face liveness detection.

The main contribution of this paper can be summarized as follows:

- We propose a novel approach for face liveness detection by perturbing the convolutional feature maps with HOG features.
- Further, we propose an end-to-end scheme to simultaneously generate perturbed feature maps and supervise a CNN network using the generated perturbed feature maps for face liveness detection.
- We provide a comprehensive experimental evaluation of the proposed system, evaluating various activation functions for generating perturbing weight matrix and their effect on face liveness detection in general. Further, we evaluate the performance of the proposed system in both intra-database and cross-database face liveness detection scenarios on challenging face anti-spoofing databases like OULU [10], CASIA [10] and Replay-Attack [11].

The rest of this paper has been organized as follows. In Sect. 2, we review the state-of-the-art work done in face liveness detection. In Sect. 3, we discuss our proposed method for face liveness detection. In Sect. 4, we provide experimental results and discussions. Finally in Sect. 5, we conclude the paper with a conclusion and possible future research directions.

## 2 Literature Review

The remarkable success of CNNs in various computer vision tasks, including classifying face spoofing attacks, have provided a way to categorize face anti-spoofing classifiers into two broader domains, i.e. Hand-crafted features based classifiers and learnable or dynamic features based classifiers. Hand-crafted features based classifiers utilize liveness cues in a face image such as motion [11–13], texture [14–16] and spectral energy contents [17]. Approaches that utilized texture information for face anti-spoofing applications were proved to be quite robust in detection of different types of PA. On the other hand, learnable or dynamic feature based classifiers, like CNNs, learn features directly from the raw data fed to it. Therefore, the features learn by CNN classifiers are dynamic and represent a wide range of patterns in the data as compared to fixed feature based classifiers [18].

In [4], a CNN architecture was proposed for the combined detection of fingerprint, iris and face liveness detection. Although, the authors obtained benchmark accuracy for face liveness detection; no cross-database results for face liveness detection were reported. In [19], an LBP-net, that combine LBP feature maps with CNN, was proposed for classification of live face and PA. In [20], face-depth estimation and individual facial regions like eyes, mouth, nose and eyebrows were utilized using a two stream CNN and an SVM with score level-fusion for face liveness detection. In [21], facial depth maps were obtained from kinetic sensors and combined with texture features extracted from CNN for face liveness detection. In [22], a spatio-temporal representation was learned from the input face sequences by utilizing an LSTM (Long Short Term Memory)-CNN.

In [23], spatio-temporal representation was obtained from the energy representation of each color channel in RGB face images. This spatio-temporal representation of face images was then fed to the CNN classifier for face liveness detection. Recently, in [24], a combination of hand-crafted features like LBP and deep features from CNN were utilized for face liveness detection. To overcome the high-dimensionality problem, a PCA was utilized first before feeding the combined features to an SVM classifier for the detection of PA. Similarly, in [25], the discriminative feature maps at different layers of VGG-Net's [26] were obtained first using PCA. These discriminative feature maps were then utilized to train an SVM classifier for face liveness detection.

# 3 Methodology

## 3.1 Generating Perturbed Feature Maps

Let suppose an input face image is represented as $I$, and a corresponding HOG features in the form of 2D matrix is represented as $I_{hog}$. Additionally, let the output feature maps of the candidate convolution layer is represented as $c_i$, where $i$ represents the position of the candidate convolutional layer in a CNN. In this work, we select $i = 1$, (the first layer of the proposed CNN). For generating the perturbed feature maps, we first concatenated each feature maps of $c_1$ layer with hog features $I_{hog}$. Assuming there are $n$ feature maps in a candidate convolutional layer, this process generate a $2n$ dimensional hybrid tensor $F_h$.

$$F_h^n = [[c_1(1), I_{hog}], \ldots, [c_1(n), I_{hog}]] \tag{1}$$

Each $n^{th}$ element of the hybrid tensor $F_h$ is then passed through a convolution layer having a single shared weight matrix $w^T$ and a sigmoid activation. We represent the output of this convolution layer as $c_2$.

$$c_2 = \sigma([w^T * [c_1(1), I_{hog}], \ldots, w^T * [c_1(n), I_{hog}]]) \tag{2}$$

In Eq. (2), * represents convolutional operation. After obtaining the feature maps from convolutional layer $c_2$, we calculate the Hadamard product of convolutional feature maps $c_1$ and $c_2$ to obtain the perturbed feature maps $F_n^T$ using Eq. (3).

$$F_T^n = c_2 \circ c_1 \tag{3}$$

The perturbed feature maps $F_n^T$ encapsulating both convolutional features and HOG features are passed through the rest of convolution layers in the CNN in the usual fashion for predicting the input face image being live or PA. Figure 2 shows an example of face samples from OULU-NPU face anti-spoofing database and corresponding class activation maps from layer $c_1$ and corresponding perturbed class activation maps. A quick comparison between the class activation maps from layer $c_1$ and the perturbed class activation maps indicated that the perturbed class activation maps boost the response of the convolutional feature maps in the discriminative regions selected by convolution layer $c_1$.

## 3.2 CNN Architecture

The proposed CNN has been shown in Table 1. The input to the proposed CNN is real world face image $I$ and corresponding HOG features $I_{hog}$. As shown in Table 1, the output from the convolution layer conv_d1 is concatenated with input face image HOG features $I_{hog}$. Further, to ease the flow of gradient across the CNN architecture, we further map the 3 convolution layers, following the perturbation layer, using 1 × 1 convolution layers. At the end of the CNN architecture, all the feature maps from convolution layers 4, 5, 6 and 7 are concatenated followed by global average pooling layer that average all the feature maps and provide an output vector, which was then fed to the fully-connected layer with 2-way soft-max activation. Since global average pooling has no parameter to learn, a direct relationship can be established between the convolution layers and output of soft-max. We further used a dropout of 0.2 after each max-pooling layer and regularization factor of 0.0005 in each convolution layer except for the perturbation layer $c_2$.

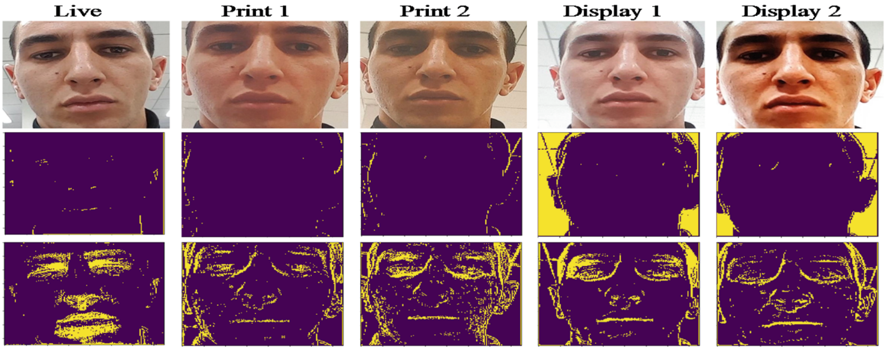

**Fig. 2.** Top row: Samples of face images from OULU face anti-spoofing database. Middle row: Corresponding convolutional layer $c_1$ feature maps and Bottom row: Corresponding perturbed feature maps $F_T^n$. The convolution feature maps and perturbed feature maps are represented in binary format by thresholding every pixel $p > 0.5$.

**Table 1.** Configuration of proposed CNN architecture

| Layer name | Kernel size | Output channel | Input |
|---|---|---|---|
| Conv_d1 | 3 × 3 | 16 | $I$ |
| **Perturbation layer** | 3 × 3 | 16 | $[I_{hog}, \text{Conv\_d1}]$ |
| Conv_1 | 3 × 3 | 32 | **Perturbation layer** |
| Max-pool_1 | 2 × 2 | 32 | Conv_1 |
| Conv_2 | 3 × 3 | 64 | Max-pool_1 |
| Max-pool_2 | 2 × 2 | 64 | Conv_2 |
| Conv_3 | 3 × 3 | 128 | Max-pool_2 |

(*continued*)

**Table 1.** (*continued*)

| Layer name | Kernel size | Output channel | Input |
|---|---|---|---|
| Max-pool_3 | 2 × 2 | 128 | Conv_3 |
| Conv_4 | 1 × 1 | 2 | Max-pool_3 |
| Conv_5 | 1 × 1 | 2 | Conv_1 |
| Conv_6 | 1 × 1 | 2 | Conv_2 |
| Conv_7 | 1 × 1 | 2 | Conv_3 |
| **F1 = concatenate** [Conv_4, Conv_5, Conv_6, Conv_7] | | | |
| Global average pooling | - | 8 | F1 |
| Fc1 | 10 | 2 | Global average pooling |
| 2 way soft-max | | | |

### 3.3 Training

We train the proposed CNN for a total of 20 epochs. The initial learning rate was set to 0.01, which was reduced by a factor of 0.1 after 10th and 15th epoch. The batch-size was set to 32. Before feeding the training data to the proposed CNN, samples in the training data were randomly shuffled. The proposed network took approximately 40 min to train on GTX 1080 GPU. Each epoch took approximately between 120 s to 128 s depending on the size of the input face image.

## 4 Experimental Results and Discussions

We first analyze various activation functions for generating perturbed feature maps weight matrix and their effect on face liveness detection performance. Afterwards, we present the analysis and discussion of the proposed system in intra-database and cross-database face liveness detection tests. Further we evaluated the performance of the proposed system using Half Total Error Rate (HTER), Equal Error Rate (EER), Bona Fide Presentation Classification Error Rate (BPCER), Attack Presentation Classification Error Rate (APCER) and Average Classification Error Rate (ACER). For intra-database evaluation, we utilized the BPCER, APCER and their average ACER metric. For cross-database evaluation, we utilized HTER value. Since HTER is threshold dependent, the threshold computed at EER point on the development set was used calculate the HTER on the database under consideration.

### 4.1 Effect of Activation Functions on Perturbed Feature Maps

We first analyzed the effect of utilizing various activation functions in generating perturbed feature maps for face liveness detection. Particularly, we evaluated the effect of three activation functions i.e., rectified linear unit (ReLU), exponential linear unit (ELU) and sigmoid activation function. Table 2 shows the performance of the final CNN classifier on face liveness detection using each activation function. It can be clearly seen in Table 2 that the use of sigmoid activation function provide best performance compared to using other activation functions. Further, we found that sigmoid activation function weight the pixels in the convolutional feature maps according to their magnitude.

## 4.2 Intra-database Face Liveness Detection

For the intra-database face liveness detection analysis, we utilized the BPCER, APCER and their average ACER metric. The operating threshold value for the test set was determined using the EER point on the development set. Table 3 shows the performance of the proposed system on intra-database face liveness detection tests. We represent the CNN classifiers without using the perturbation as "conventional" and the one using perturbation as "proposed" from now on. It can be seen in Table 3 that the proposed approach obtain a lowest ACER of 4.74%, 1.08% and 0.17% as compared to obtaining an ACER of 7.13%, 1.17% and 0.60% using conventional approach on OULU, CASIA and Replay-Attack face anti-spoofing databases. This indicated that the utilization of perturbed feature maps add new information to the following convolution layers of the CNN to leverage the classification decision of an input face image being considered as live or fake.

**Table 2.** Performance in (%) of using various activation functions in the perturbation layer

| Activation | OULU (Development) | | | OULU (Test) | | |
|---|---|---|---|---|---|---|
| | BPCER | APCER | ACER | BPCER | APCER | ACER |
| ReLU | 6.33 | 1.59 | 3.96 | 8.97 | 3.43 | 6.20 |
| ELU | 6.14 | 1.51 | 3.83 | 9.10 | 3.18 | 6.14 |
| Sigmoid | **5.63** | **1.39** | **3.51** | **7.40** | **2.07** | **4.74** |

**Table 3.** Performance in (%) of conventional and proposed approach on intra-database face anti-spoofing tests

| Method | OULU (Development) | | | OULU (Test) | | |
|---|---|---|---|---|---|---|
| | BPCER | APCER | ACER | BPCER | APCER | ACER |
| Conventional | 6.44 | 1.65 | 4.03 | 11.36 | 2.90 | 7.13 |
| Proposed | **5.63** | **1.39** | **3.51** | **7.40** | **2.07** | **4.74** |
| | | | | **CASIA (Test)** | | |
| Conventional | | | | 2.63 | 0.79 | 1.71 |
| Proposed | | | | **1.60** | **0.58** | **1.08** |
| | **Replay-attack (Development)** | | | **Replay attack (Test)** | | |
| Conventional | **1.23** | 0.69 | **0.96** | 0.93 | 0.28 | 0.60 |
| Proposed | 2.35 | **0.41** | 1.38 | **0.04** | **0.29** | **0.17** |

### 4.3 Cross-Database Face Liveness Detection

For the cross-database analysis, we trained the face anti-spoofing system on one database and tested it on the other database. The operating threshold was determined by development set or the testing set of the face anti-spoofing database on which the face anti-spoofing system was trained on. Table 4 shows the performance of the conventional approach and the proposed approach on cross-database face anti-spoofing tests. It can be seen in Table 4, that the proposed method obtain better performance in cross-database tests when trained on OULU face anti-spoofing database as compared to conventional approach. When trained with OULU face anti-spoofing database, the proposed method obtain an all-time lower HTER of 9.62% and 10.31% on CASIA and Replay-Attack database as compared to the conventional approach.

On the other hand, the conventional approach obtain better performance when trained on CASIA face anti-spoofing database. Further, when trained on Replay-Attack database, we found that the conventional approach and the proposed approach obtain comparable performance. Further analyses of the CNN classifier trained with CASIA and Replay-Attack face anti-spoofing database in the Table 4 show higher percentages of HTER as compared to the CNN classifier trained with OULU face anti-spoofing database. This suggest that there is a certain bias in these database toward certain types of PA.

**Table 4.** HTER in (%) on cross-database tests

| Training set | Database | Conventional | Proposed |
|---|---|---|---|
| OULU | CASIA | 11.10 | **9.62** |
| | Replay-Attack | 17.83 | **10.31** |
| CASIA | OULU | **18.32** | 26.82 |
| | Replay-Attack | **27.70** | 31.54 |
| Replay-Attack | OULU | 25.88 | **24.90** |
| | CASIA | **11.55** | 11.76 |

### 4.4 Comparison with State-of-the-Art Approaches

We further compared the cross-database face anti-spoofing performance, in terms of % HTER, of the proposed method with state-of-the-art face anti-spoofing approaches in Table 5. It can be seen in Table 5 that the proposed method, when trained on OULU database, obtain an all-time lower HTER of 9.62% and 10.31% on CASIA and Replay Attack databases. However, when trained on CASIA database, we found that the proposed method obtain an HTER of 31.54% on Replay Attack database. The reason of this degradation in HTER is because the CASIA database was collected under uniform capturing (illumination) conditions compared to OULU and Replay Attack databases, which were collected under different capturing environments.

**Table 5.** Comparison of the proposed method and state-of-the-art face liveness detection methods. HTER in (%) on cross-database scenarios

| Method | CASIA* | Replay-attack** |
|---|---|---|
| Pinto et al. [17] | 50.0 | 34.4 |
| Siddiqui et al. [27] | 44.6 | 35.4 |
| Boulkenafet et al. [15] | 37.7 | 30.3 |
| Li et al. [6] | 36.0 | 27.4 |
| Manjain et al. [28] | 27.4 | 22.8 |
| **Proposed** | **11.76** | **31.54** |
| **Proposed†** | **9.62** | **10.31** |

* Train set: Replay-Attack
** Train set: CASIA
† Train set: OULU

## 5 Conclusion and Future Work

In this paper, we proposed a novel approach to face liveness detection by introducing perturbation in the convolutional feature maps. The proposed perturbation approach added only a minor parameter overhead in the CNN, while achieving significant performance improvement for face liveness detection task both in intra-database and cross-database scenarios. Further, we found that the proposed method, when trained on challenging face anti-spoofing database, like OULU, further improved the performance of face liveness detection in cross-database face anti-spoofing scenarios. This further demands that the face anti-spoofing databases should contain different variations in not only in imaging qualities and types of PA instruments, but also in environmental conditions to further facilitate the development of face anti-spoofing research.

Future work include evaluation of perturbing the convolutional layers of CNN using various hand-crafted features, such as Local Binary Patterns (LBP), Shearlet features and wavelet features. We believe that the information induced by these hand-crafted features in a CNN can further improve its robustness, efficiency and reliability in face liveness detection applications.

**Acknowledgements.** The work in this paper was supported by City University of Hong Kong under the research project with grant number 7004430.

## References

1. Galbally, J., Marcel, S., Fierrez, J.: Biometric antispoofing methods: a survey in face recognition. IEEE Access **2**, 1530–1552 (2014)
2. Sepas-Moghaddam, A., Pereira, F., Correia, P.L.: Light field based face presentation attack detection: reviewing, benchmarking and one step further. IEEE Trans. Inf. Forensics Secur. **13**(7), 1696–1709 (2018)
3. Kim, W., Suh, S., Han, J.-J.: Face liveness detection from a single image via diffusion speed model. IEEE Trans. Image Process. **24**, 2456–2465 (2015)

4. Menotti, D., Chiachia, G., Pinto, A., Schwartz, W.R., Pedrini, H., Falcao, A.X., Rocha, A.: Deep representations for iris, face, and fingerprint spoofing detection. IEEE Trans. Inf. Forensics Secur. **10**, 864–879 (2015)
5. Rehman, Y.A.U., Po, L.M., Liu, M.: LiveNet: improving features generalization for face liveness detection using convolution neural networks. Expert Syst. Appl. **108**, 159–169 (2018). https://doi.org/10.1016/j.eswa.2018.05.004
6. Li, H., Li, W., Cao, H., Wang, S., Huang, F., Kot, A.C.: Unsupervised domain adaptation for face anti-spoofing. IEEE Trans. Inf. Forensics Secur. **13**, 1794–1809 (2018)
7. Yang, J., Lei, Z., Li, S.Z.: Learn convolutional neural network for face anti-spoofing (2014). arXiv Preprint: arXiv:1408.5601
8. Yang, J., Lei, Z., Yi, D., Li, S.Z.: Person-specific face antispoofing with subject domain adaptation. IEEE Trans. Inf. Forensics Secur. **10**, 797–809 (2015)
9. Li, L., Xia, Z., Hadid, A., Jiang, X., Roli, F., Feng, X.: Face presentation attack detection in learned color-liked space, pp. 1–13. arXiv:1810.13170v1
10. Boulkenafet, Z., Komulainen, J., Li, L., Feng, X., Hadid, A.: OULU-NPU: a mobile face presentation attack database with real-world variations. In: Proceedings of the 12th IEEE International Conference on Automatic Face and Gesture Recognition (FG 2017), pp. 612–618. IEEE (2017)
11. de Freitas Pereira, T., Komulainen, J., Anjos, A., De Martino, J.M., Hadid, A., Pietikäinen, M., Marcel, S.: Face liveness detection using dynamic texture. EURASIP J. Image Video Process. **2014**, 2 (2014)
12. Kim, Y., Yoo, J.-H., Choi, K.: A motion and similarity-based fake detection method for biometric face recognition systems. IEEE Trans. Consum. Electron. **57**, 756–762 (2011)
13. Anjos, A., Chakka, M.M., Marcel, S.: Motion-based counter-measures to photo attacks in face recognition. IET Biom. **3**, 147–158 (2013)
14. Wen, D., Han, H., Jain, A.K.: Face spoof detection with image distortion analysis. IEEE Trans. Inf. Forensics Secur. **10**, 746–761 (2015)
15. Boulkenafet, Z., Komulainen, J., Hadid, A.: Face spoofing detection using colour texture analysis. IEEE Trans. Inf. Forensics Secur. **11**, 1818–1830 (2016)
16. Gragnaniello, D., Poggi, G., Sansone, C., Verdoliva, L.: An investigation of local descriptors for biometric spoofing detection. IEEE Trans. Inf. Forensics Secur. **10**, 849–863 (2015)
17. Pinto, A., Pedrini, H., Schwartz, W.R., Rocha, A.: Face spoofing detection through visual codebooks of spectral temporal cubes. IEEE Trans. Image Process. **24**, 4726–4740 (2015)
18. Krizhevsky, A., Sutskever, I., Hinton, G.E.: ImageNet classification with deep convolutional neural networks. In: Advances in Neural Information Processing Systems, pp. 1097–1105 (2012)
19. de Souza, G.B., da Silva Santos, D.F., Pires, R.G., Marana, A.N., Papa, J.P.: Deep texture features for robust face spoofing detection. IEEE Trans. Circuits Syst. II Express Briefs **64**, 1397–1401 (2017). https://doi.org/10.1109/tcsii.2017.2764460
20. Atoum, Y., Liu, Y., Jourabloo, A., Liu, X.: Face anti-spoofing using patch and depth-based CNNs. In: Proceedings of the IEEE International Joint Conference on Biometrics (IJCB), pp. 319–328 (2017)
21. Wang, Y., Nian, F., Li, T., Meng, Z., Wang, K.: Robust face anti-spoofing with depth information. J. Vis. Commun. Image Represent. **49**, 332–337 (2017)
22. Xu, Z., Li, S., Deng, W.: Learning temporal features using LSTM-CNN architecture for face anti-spoofing. In: 2015 3rd IAPR Asian Conference on Pattern Recognition (ACPR), pp. 141–145 (2015)
23. Lakshminarayana, N.N., Narayan, N., Napp, N., Setlur, S., Govindaraju, V.: A discriminative spatio-temporal mapping of face for liveness detection. In: 2017 IEEE International Conference on Identity, Security and Behavior Analysis (ISBA), pp. 1–7 (2017)

24. Nguyen, D.T., Pham, T.D., Baek, N.R., Park, K.R.: Combining deep and handcrafted image features for presentation attack detection in face recognition systems using visible-light camera sensors. Sensors (Switzerland) **18** (2018). https://doi.org/10.3390/s18030699
25. Li, L., Feng, X., Boulkenafet, Z., Xia, Z., Li, M., Hadid, A.: An original face anti-spoofing approach using partial convolutional neural network. In: 2016 6th International Conference on Image Processing Theory Tools and Applications (IPTA), pp. 1–6 (2016)
26. Simonyan, K., Zisserman, A.: Very deep convolutional networks for large-scale image recognition (2014). arXiv Preprint: arXiv:1409.1556
27. Siddiqui, T.A., Bharadwaj, S., Dhamecha, T.I., Agarwal, A., Vatsa, M., Singh, R., Ratha, N.: Face anti-spoofing with multifeature videolet aggregation. In: 2016 23rd International Conference on Pattern Recognition (ICPR), pp. 1035–1040 (2016)
28. Manjani, I., Tariyal, S., Vatsa, M., Singh, R., Majumdar, A.: Detecting silicone mask based presentation attack via deep dictionary learning. IEEE Trans. Inf. Forensics Secur. **12**, 1713–1723 (2017)