UNIVERSITI PUTRA MALAYSIA

LIVENESS DETECTION IN FACIAL BIOMETRICS USING COMPLETE DYNAMIC LOCAL TERNARY PATTERN TECHNIQUE

SAJIDA PARVEEN

FK 2016 58

LIVENESS DETECTION IN FACIAL BIOMETRICS USING COMPLETE DYNAMIC LOCAL TERNARY PATTERN TECHNIQUE

By

SAJIDA PARVEEN

Thesis Submitted to the School Graduate Studies, Universiti Putra Malaysia, in Fulfillment of the Requirements for the Degree of Doctor of Philosophy

September 2016

DEDICATION

To my encouraging parents, my siblings

My beloved husband, my children and all family members

Abstract of thesis presented to the Senate of Universiti Putra Malaysia in fulfillment of the requirement for the degree of Doctor of Philosophy

LIVENESS DETECTION IN FACIAL BIOMETRICS USING COMPLETE DYNAMIC LOCAL TERNARY PATTERN TECHNIQUE

By

SAJIDA PARVEEN

September 2016

Chairman : Assoc. Prof. Sharifah Mumtaza binti Syed Ahmad Abdul Rahman, PhD
Faculty : Engineering

Facial biometric systems have recently received increased deployment in various applications such as surveillance, access control and forensic investigations. However, facial biometrics facing various tangible threats, one of them is spoofing attacks. A spoofing attack occurs when a person tries to masquerade as someone else by non-real faces such as photograph, video clips or dummy faces and thereby gaining advantages from applications. In order to identify the spoofing attacks on such biometric systems, face liveness detection countermeasure have been developed.

There are numerous ways to detect the liveness of face such as through motion analysis, texture analysis, identify life sign clues and thermal sensors. Recently, texture analysis has received more attention because of its non-intrusiveness; high efficiency and accuracy to discriminate face skin texture from spoof attacks. For this purpose, a numbers of texture descriptors have been proposed in the literature for face liveness detection. However, they exhibit some limitations in terms of noise with center pixel, manual setting of threshold (τ) value and ignorance of global intensity in the image.

Thus, a robust face liveness detection method based on Complete Dynamic Local Ternary Pattern (CDLTP) has been proposed in this thesis. The CDLTP was designed to overcome the limitations of reported texture descriptors. Weber's law was used to automatically set the threshold value in ternary pattern by considering the *sign*, *magnitude* and global *intensity* of the image. Its effectiveness has been tested and benchmarked against other existing texture descriptors (i.e. Local Binary Pattern (LBP), Local Ternary Pattern (LTP), Dynamic Local Ternary Pattern (DLTP), Complete Local Binary Pattern

(CLBP) and Complete Local Ternary Pattern (CLTP)) on self collected database and other publically available databases (i.e. NUAA, CASIA and REPLAY-ATTACK).

The evaluations have been carried out via statistical hypothesis testing and through liveness detection itself. The results have consistently demonstrated that CDLTP outperforms other techniques across various types of spoof mediums. The comparison analysis of CDLTP with other texture descriptors were also carried out on self collected and public domain face spoof databases. In all these experiments, the results obtained with CDLTP exceeds from the state-of-art.

Various score level fusion strategies have been adopted to evaluate the performances of the overall system which comprises both face liveness detection and face recognition systems. The achieved decisions from scores level fusion strategies proved that CDLTP based face liveness detection reduces 89% of vulnerability of face verification system against spoof attacks. The measured result of serial method in which the face liveness detection performed before face recognition system was found to be the most effective methods among other score level fusion strategies that were analyzed.

Abstrak tesis yang dikemukakan kepada Senat Universiti Putra Malaysia sebagai memenuhi keperluan untuk ijazah Doktor Falsafah

PENGESANAN RUPA MUKA YANG HIDUP UNTUK PENGESAHAN RUPA MUKA DENGAN MENGGUNAKAN CORAK TEMPATAN KETIGA YANG MENYELURUH DAN DINAMIK

Oleh

SAJIDA PARVEEN

September 2016

Pengerusi : Prof. Madya Sharifah Mumtaza binti Syed Ahmad Abdul Rahman, PhD
Fakulti : Kejuruteraan

Sistem biometrik berdasarkan rupa muka kini telah banyak digunakan di dalam pelbagai aplikasi seperti pengawasan, kawalan masuk dan penyiasatan forensik. Namun sistem biometrik berdasarkan rupa muka meghadapi pelbagai ancaman ketara, salah satu daripadanya ialah serangan penyamaran. Serangan penyamaran berlaku apabila seseorang cuba menyamar sebagai orang lain dengan menggunakan rupa muka seperti gambar, klip video atau muka tiruan dan sekali gus mendapat kelebihan daripada aplikasi tersebut. Untuk mengenalpasti serangan penmyamaran pada sistem biometrik itu, pengesanan rupa muka yang hidup telah dibangunkan.

Terdapat pelbagai cara untuk mengesan rupa muka yang hidup seperti melalui analisis pergerakan, analisis tekstur, mengenalpasti petunjuk tanda hidup dan pengesan haba. Terbaru, analisis tekstur telah mendapat perhatian yang lebih kerana ia bebas dari sifat menggangg; mempunyai kecekapan dan ketepatan yang tinggi untuk membezakan tekstur kulit muka daripada serangan penyamaran. Bagi tujuan ini, sejumlah penerang tekstur telah dicadangkan di dalam kajian untuk mengesan rupa muka yang hidup. Walau bagaimanapun, teknik tersebut mempunyai beberapa kekurangan dari segi gangguan terhadap piksel pusat, menetapan nilai ambang (τ) secara manual dan ketidakpekaan terhadap intensiti global di dalam imej.

Oleh itu, kaedah pengesanan rupa muka yang hidup berasaskan pada corak ketiga tempatan yang lengkap dan dinamik (CDLTP) telah dicadangkan dalam tesis ini. CDLTP direka untuk mengatasi kekangan penerang tekstur yang dilaporkan terdahulu. Hukum Weber telah digunakan untuk menetapkan

secara automatik nilai ambang dalam corak ketiga dengan mengambil kira tanda, magnitud dan keamatan global di dalam imej. Keberkesanannya telah diuji dan telah dibandingkan dengan penerang tekstur terdahulu yang sedia ada (iaitu corak perduaan tempatan (LBP), corak ketiga tempatan (LTP), corak ketiga tempatan yang dinamik (DLTP), corak perduaan tempatan yang lengkap (CLBP) dan corak ketiga tempatan yang lengkap (CLTP)) dengan menggunakan pangkalan data yang dikumpulkan sendiri serta pangkalan data lain yang sedia ada (iaitu NUAA, CASIA dan REPLAY-ATTACK).

Penilaian yang telah dijalankan melalui pengujian hipotesis statistik dan melalui pengesanan rupa muka yang hidup itu sendiri. Keputusan secara konsisten telah menunjukkan bahawa prestasi CDLTP telah melebihi teknik-teknik lain merentasi pelbagai jenis media penyamaran. Analisis perbandingan CDLTP dengan penerang tekstur lain juga telah dijalankan pada pengkalan data yang dikumpul sendiri dan pangkalan data awam yang lain. Dalam semua ujikaji ini, keputusan yang diperolehi menunjukkan bahawa CDLTP melebihi dari teknik-teknik yang lain.

Pelbagai strategi gabungan skor telah diguna pakai untuk menilai prestasi keseluruhan sistem yang terdiri daripada kedua-dua sistem pengesanan rupa muka yang hidup dan dan sistem pengesaman rupa muka. Keputusan yang dicapai dari skor gabungan strategi telah membuktikan bahawa sistem pengesanan rupa muka yang hidup berasaskan CDLTP telah berjaya mengurangkan 89% daripada kelemahan sistem pengesahsatihan rupa muka terhadap serangan penyamaran. Keputusan yang diukur daripada kaedah bersiri di mana sistem pengesanan rupa muka yang hidup dilakukan sebelum sistem pengesaman muka didapati merupakan kaedah yang paling berkesan jika dibandingkan dengan strategi gabungan skor yang telah dianalisis.

ACKNOWLEDGEMENTS

First and foremost, I am very grateful and offer my humble gratitude to "ALMIGHTY ALLAH" who enable me to fulfill the requirements of Doctor of Philosophy (PhD) degree successfully and satisfactorily and provided me an opportunity to complete one of my life desires.

I would like to express my sincere gratitude to my supervisor, Associate Professor Dr. Sharifah Mumtaza bt. Syed Ahmad Abdul Rahman and also my supervisory committee members Dr. Marsyita bt. Hanafi and Dr. Wan Azizun bt. Wan Adnan for their guidance and advice throughout this work in making this a success.

My deepest appreciation to my family especially my husband and parents for their utmost support and encouragement without which all these would not be possible. I am thankful to my son Shazain and cute doughter Nitza for making me relax with their smile and always entertained me with their innocent and naughty activities. I am thankful to my siblings for the moral and unconditional support at every instant of time.

I certify that a Thesis Examination Committee has met on 28 September 2016 to conduct the final examination of Sajida Parveen on her thesis entitled "Liveness Detection in Facial Biometrics using Complete Dynamic Local Ternary Pattern Technique" in accordance with the Universities and University Colleges Act 1971 and the Constitution of the Universiti Putra Malaysia [P.U.(A) 106] 15 March 1998. The Committee recommends that the student be awarded the Doctor of Philosophy.

Members of the Thesis Examination Committee were as follows:

Syamsiah binti Mashohor, PhD
Senior Lecturer
Faculty of Engineering
Universiti Putra Malaysia
(Chairman)

Abd. Rahman bin Ramli, PhD
Associate Professor
Faculty of Engineering
Universiti Putra Malaysia
(Internal Examiner)

M. Iqbal bin Saripan, PhD
Professor
Faculty of Engineering
Universiti Putra Malaysia
(Internal Examiner)

Danilo Mandic, PhD
Professor
Imperial College London
United Kingdom
(External Examiner)

NOR AINI AB. SHUKOR, PhD
Professor and Deputy Dean
School of Graduate Studies
Universiti Putra Malaysia

Date: 3 November 2016

This thesis was submitted to the Senate of Universiti Putra Malaysia and has been accepted as fulfillment of the requirement for the degree of Doctor of Philosophy. The members of the Supervisory Committee were as follows:

Sharifah Mumtaza binti Syed Ahman Abdul Rahman, PhD
Associate Professor
Faculty of Engineering
Universiti Putra Malaysia
(Chairman)

Marsyita binti Hanafi, PhD
Lecturer
Faculty of Engineering
Universiti Putra Malaysia
(Member)

Wan Azizun binti Wan Adnan, PhD
Associate Professor
Faculty of Engineering
Universiti Putra Malaysia
(Member)

____

BUJANG BIN KIM HUAT, PhD
Professor and Dean
School of Graduate Studies
Universiti Putra Malaysia

Date:

Declaration by graduate student

I hereby confirm that:

- This thesis is my original work;
- Quotations, illustrations and citations have been duly referenced;
- This thesis has not been submitted previously or concurrently for any other degree at any other institutions;
- Intellectual property from the thesis and copyright of thesis are fully-owned by Universiti Putra Malaysia, as according to the Universiti Putra Malaysia (Research) Rules 2012;
- written permission must be obtained from supervisor and the office of Deputy Vice-Chancellor (Research and Innovation) before thesis is published (in the form of written, printed or in electronic form) including books, journals, modules, proceedings, popular writings, seminar papers, manuscripts, posters, reports, lecture notes, learning modules or any other materials as stated in the Universiti Putra Malaysia (Research) Rules 2012;
- There is no plagiarism or data falsification/fabrication in the thesis, and scholarly integrity is upheld as according to the Universiti Putra Malaysia (Graduate Studies) Rules 2003 (Revision 2012-2013) and the Universiti Putra Malaysia (Research) Rules 2012.The thesis has undergone plagiarism detection software.

Signature: ________________________ Date: ___________________

Name and Matric No.: Sajida Parveen, GS35270

Declaration by Members of Supervisory Committee

This is to confirm that:

- The research conducted and the writing of this thesis was under our supervision;
- Supervision responsibilities as stated in the Universiti Putra Malaysia (Graduate Studies) Rules 2003 (Revision 2012-2013) are adhered to.

Signature: ____________________________
Name of
Chairman of
Supervisory
Committee: ____________________________

Signature: ____________________________
Name of
Member of
Supervisory
Committee: ____________________________

Signature: ____________________________
Name of
Member of
Supervisory
Committee: ____________________________

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

LBP	Local Binary Pattern
LTP	Local Ternary Pattern
DLTP	Dynamic Local Ternary Pattern
CLBP	Complete Local Binary Pattern
CLTP	Complete Local Ternary Pattern
CDLTP	Complete Dynamic Local Ternary Pattern
ILTP	Improved Local Ternary Pattern
ELTP	Enhanced Local Ternary Pattern
PDF	Probability Density Function
2-D	Two Dimensions
ROC	Receiver Operating Characteristic
S_CDLTP	Sign- Complete Dynamic Local Ternary Pattern
M_CDLTP	Magnitude- Complete Dynamic Local Ternary Pattern
C_CDLTP	Center- Complete Dynamic Local Ternary Pattern
WLD	Weber Local Descriptor
LPQ	Local Phase Quantization
BSIF	Binarized Statistical Image Features
LCPD	Local Contrast-Phase Descriptor

CHAPTER 1

INTRODUCTION

1.1 Background

Biometrics refers to technologies designed either to verify or recognize the identity of a person based on one or more physical or behavioral characteristics (Rejman-Greene, 2005) such as faces, fingerprints, irises, voices and gates. The biometric technologies are widely used in different areas ranging from governmental to private sectors and from personal computers to commercial purposes. Biometrics makes the system more secure, private and convenient to use (Jain and Ross, 2007). Nevertheless, similar to any other system, biometric is also vulnerable to malicious attacks particularly spoofing attacks.

A spoof attack is defined as an attempt by a person to masquerade as an authentic biometric user by using his reproduced biometric traits for gaining illegitimate access to the biometric system (Edrogmus and Marcel, 2014). This can be done through an artificial finger, a contact lens on an eye or a mask over a face because our faces are visible, voices can be recordable, and fingerprints are left on mostly everything a person touches.

There are a numbers of different computer companies currently operating in the market that provide embedded face biometric solution with built-in webcams that authenticate users by scanning their faces such as Lenovo, Dell, Asus, Apple and Toshiba. However, spoofing attacks (or copy attacks) are still serious threats to these solutions despite high performances for biometric accuracy for verification and identification.

Face spoof attacks are very cheap and easy to capture and reproduce as compared to the other biometrics. Particularly with the advancement of digital camera devices and availability of social media, facial images can be captured from far distance or can be downloaded from social websites. The reproduction of fake facial specimen is also a simple task whereby faces can easily be shown on different mediums such as on printed photos, or playback images / videos on portable electronic devices.

Face biometrics based systems are very vulnerable in the real world and may encounter various spoof attacks. The trust of users in biometric based applications can be increased by securing the system with an additional layer of liveness detection which enables the system to differentiate between live and spoof face specimen.

Face liveness detection is an effective countermeasure to face spoofing attacks. In the Face liveness detection system as shown in the Figure 1.1. According to that the user needs to show his or her face in front of the system's camera. The camera captures a facial image and passes that image to the feature extraction module. The result obtained from this stage is used to differentiate between original facial samples from fake samples. Hence, original samples will further be treated in order to get verified and fake one are to be rejected automatically by the system.

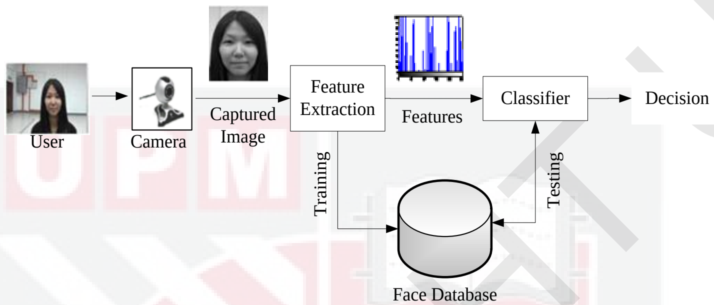

Figure 1.1: Block diagram of face liveness detection system

The appearance of a fake face can be identified through several clues including detection of several life signs such as motions (i.e. eye blink, head rotation, lip movement etc) and comparison of textures of skin. The former requires a user to be cooperative with the system for producing spontaneous facial movement. Thus, such type of systems become powerless when someone spoofs with video attacks or if the user could not match the perfect desired movement because of health issues (i.e. which lead to a high level of false positive in spoofing detection).

Motion based methods does not get much attention in the research field because of its intrusiveness (Anjos et al. 2014). This limit of work, leads toward the cause of dependency on user's movement for liveness detecting such as head and mouth movement. While, the non-intrusive based face liveness detection systems are getting much more attention and a number of methods have been proposed for such purposes.

The second approach is often based on analysis of facial appearance properties, such as texture and reflectance (Anjos et al. 2014). Most of the methods in this category differentiate the live face from the spoof by using only one image, which make them cheaper in processing. The main advantage over motion based attack is this; no user cooperation is needed in analysis of facial appearance properties.

Most recently, texture analysis for face liveness detection has become widely used because of the tremendous advantages such as simple implementation, lower complexity in calculation and non-intrusiveness in terms of user involvement. Texture analysis mainly depends on the texture feature extraction and classifiers. For calculating the texture features, there are a number of texture descriptors which are used in the feature extraction module. A common descriptor includes Local Binary Pattern (Ojala et al. 1994) and it's various extended versions.

1.2 Problem Statement

- **Current limitation of existing databases**
  Spoof specimens can breach the security of face verification systems in a number of ways by using various possible attacks such as mask, printed photograph, 3D model or video display device and etc. Currently, in publicly available databases such as NUAA face imposter database (Tan et al. 2010), REPLAY-ATTACK and CASIA face anti-spoofing database (Zhang et al. 2012) the available face spoof attacks are limited in variations and still rather limited as compared to the other possible measures that can be used for spoofing attempts. In order to conduct a more robust research in face liveness detection, a challenging database is required to collect that should cover more types of display media and paper material for face spoof attacks for the texture based approaches.

- **Limitation in commonly used texture descriptors**
  Ideally for texture analysis, the common texture descriptor such as Local Binary Pattern (LBP) (Ojala et al. 1994) should be powerful enough to provide reliable features to classify a particular texture; which is in this case, to identify live skin texture. Mostly, in LBP and it's all other extended descriptors utilized two values i.e. central and neighbor pixel in each pattern for calculating local binary difference. In these texture descriptors, the limitation in terms of noise with central pixel is appeared in many cases, which are observed in similar micro-structures showed in Figure 1.2. The solution of this limitation is proposed in Local Ternary Pattern (Tan and Triggs, 2010), which is basically robust to the central pixel noise because of its three level quantization. Later on, this technique also encounters the limitation in terms of setting threshold value manually for every application.

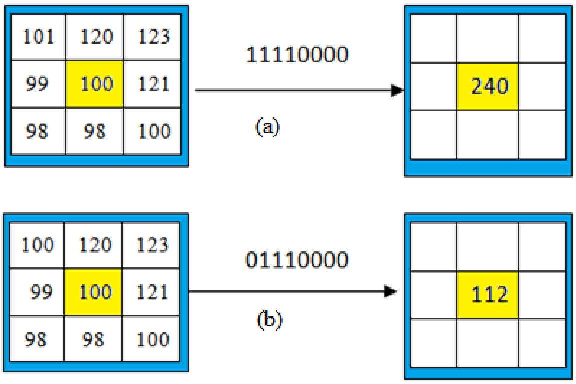

Figure 1.2: Similar LBP patch coding limitation

To overcome this problem, Improved Local Ternary Pattern (ILTP) (Yang and Sun, 2011), Dynamic Local Ternary Pattern (DLTP) (Ibrahim et al. 2014) and Extended Local Ternary Pattern (ELTP) (Zhenyu et al. 2014) have been proposed. These all texture descriptors also poses another limitation which is the sharing of the same code but actually both have different gray value distribution as shown in Figure 1.3 that $LBP_{8,1}$ = 219, in positive LTP =145 and in negative LTP =32. The reason is only to concentrate on local features where as the global feature of the image is neglected in these texture descriptors.

Thus for calculating global features, Complete Local Binary Pattern (CLBP) (Guo et al. 2010) and Complete Local Ternary Pattern (CLTP) (Rassem and Khoo, 2014) were introduced. Such limitations on current texture descriptors i.e. LBP, LTP, DLTP etc degraded the performances, thus there is a need to design a more robust descriptor.

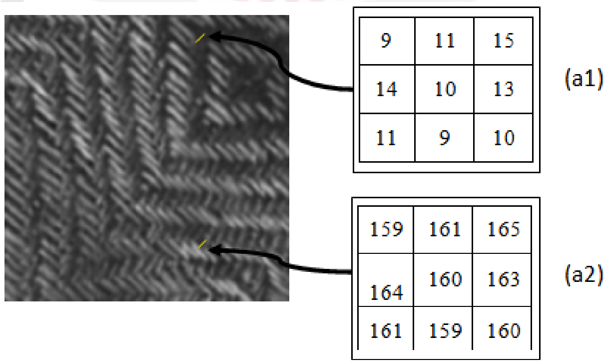

Figure 1.3: Micro structure of different gray values with similar code (a1) light (a2) dark regions

- **Study on the statistical differentiating properties of texture descriptors across various spoof techniques is not reported**
  Study on the effectiveness of the face descriptor across various spoof medium has been little reported. Most treat them as generic. Hence, there is a need to analyze the effects of various spoof attacks on face liveness detection in order to define the level of attack affected according to the different spoof medium.

- **Study on the effect of various decision fusion techniques from liveness detection and face verification modules is rarely reported**
  Face liveness detection does not suppose to serve as a standalone system. The combined operation of face verification and face liveness detection is rarely reported and limited fusion strategies are being evaluated (Wild et al. 2016). There is need to incorporate the face descriptor in face liveness detection and investigate the effectiveness with different score fusion method with face verification.

1.3 Research Objectives

The primary aim of this work is to propose a robust non-intrusive face liveness detection method based on skin texture analysis. In order to achieve this aim, following objectives have been set:

1. To design a robust face texture descriptor and analyze its statistical discriminating properties across various types of spoof attacks

2. To design a non-intrusive face liveness detection method based on proposed feature descriptor

3. To improve the effectiveness of score fusion techniques between face liveness detection and face verification modules.

1.4 Scope of Research Work

The scope of this research work is to design a face liveness detection method for facial biometrics. The proposed method is based on texture analysis of static images. The performance of proposed method is to be analyzed in terms of accuracy of the system. In order to evaluate the performance of a face liveness detection module with joint operation of face verification by using proposed texture descriptor, the serial and parallel score fusion strategies are employed. Three publicly available facial spoof databases e.g. NUAA face imposter database (Tan et al. 2010), REPLAY-ATTACK and CASIA (Zhang et al. 2012) are utilized for benchmarking.

1.5 Organization of Thesis

This thesis is organized into five chapters. The summary of each chapter is given below:

Chapter 1 provides a general introduction to the research area and identifies the current problems in designing of texture descriptor for face liveness detection system that motivated this research. It also introduces the objectives and scope of research as well.

Chapter 2 presents a thorough literature review and theoretical background about face spoofing attacks and face liveness detection schemes. It also covers currently used face spoof databases along with the limitations. The background and history of texture analysis descriptor and its usage in face liveness detection is also provided in this chapter. The recent face verification techniques are also discussed in this chapter.

Chapter 3 provides database collection and compilation of face spoof database and face verification database. It also describes the design aspects of Complete Dynamic Local Ternary Pattern descriptor. The models for decision fusion strategies of face liveness detection and face verification systems are also elaborated in this chapter.

The testing results of proposed mathematical model on collected face spoof database with different texture analysis of spoof attacks, face liveness detection and score fusion model of embedded system are presented in chapter 4. Finally the conclusion is provided in chapter 5.

REFERENCES

Abraham, R. A. L. P. H. (1978). Marsden, Foundation of Mechanics.*Addison-Wesley, Read-ing, Mass*, *2*, 65-114.

Adler, A. and Schuckers S. A. C. (2009). Biometric vulnerabilities, Overview. *Encyclopedia of Biometrics*, 1: 160-168. *Springer US*

Akhloufi, M. and Bendada, A. (2010). Locally adaptive texture features for multispectral face recognition. *IEEE International Conference on Systems Man and Cybernetics (SMC),* 3308-3314.

Akhtar, Z., Fumera, G., Marcialis, G. L. and Roli, F. (2011). Robustness analysis of likelihood ratio score fusion rule for multimodal biometric systems under spoof attacks. *IEEE International Carnahan Conference on Security Technology (ICCST),* 237-244

Anjos, A., Marcel, S. (2011). Counter-measures to photo attacks in face recognition: a public database and a baseline. *IEEE International joint conference on Biometrics (IJCB),* 1-7.

Anjos, A., Chakka, M. M. and Marcel, S. (2013). Motion-based counter-measures to photo attacks in face recognition. *IET Biometrics*, 3(3): 147-158.

Anjos, A., Komulainen, J., Marcel, S., Hadid, A., and Pietikäinen, M. (2014). Face anti-spoofing: Visual approach. In *Handbook of Biometric Anti-Spoofing* (pp. 65-82). Springer London.

Arashloo, S. R., Kittler, J. and Christmas, W. (2015). Face spoofing detection based on multiple descriptor fusion using multiscale dynamic binarized statistical image features. *IEEE Transactions on Information Forensics and Security,* 10(11): 2396-2407.

Bao, W., Li, H., Li, N. and Jiang, W. (2009). A liveness detection method for face recognition based on optical flow field. *International Conference on IEEE Image Analysis and Signal Processing. IASP 2009.* 233-236.

Barron, J. L., Fleet, D. J. and Beauchemin, S. S. (1994). Performance of optical flow techniques. *International journal of computer vision*, 12(1): 43-77.

Bartlett, M. S., Movellan, J. R. and Sejnowski, T. J. (2002). Face recognition by independent component analysis. *IEEE Transactions on Neural Networks,* 13(6): 1450-1464.

Belhumeur, P. N., Hespanha, J. P. and Kriegman, D. J. (1997). Eigenfaces vs. fisherfaces: Recognition using class specific linear projection. *IEEE*

Transactions on Pattern Analysis and Machine Intelligence, 19(7): 711-720.

Biggio, B., Akhtar, Z., Fumera, G., Marcialis, G. L., Roli, F. (2012). Security evaluation of biometric authentication systems under real spoofing attacks. *IET biometrics*, 1(1): 11-24.

Bland, J. M. and Altman, D. G. (1996). Statistics notes: measurement error. *BMJ Clinical Research*, 313(7059): 744. British Medical Association, BMJ Publishing Group

Bradley, A. P. (1997). The use of the area under the ROC curve in the evaluation of machine learning algorithms. *Pattern recognition,* 30(7): 1145-1159.

Caetano Garcia, D., and de Queiroz, R.L. (2015). Face-Spoofing 2D-Detection Based on Moiré-Pattern Analysis *Information Forensics and Security, IEEE Transactions on*, *10*(4): 778-786.

Cai, D., He, X., Han, J. and Zhang, H. J. (2006). Orthogonal laplacian faces for face recognition. *IEEE Transactions on Image Processing,* 15(11): 3608-3614.

Cai, L., Xiong, C., Huang, L. and Liu, C. (2015a). A Novel Face Spoofing Detection Method Based on Gaze Estimation. *Computer Vision-ACCV 2014,* 547-561. Springer International Publishing.

Cai, L., Huang, L. and Liu, C. (2015b). Person-specific Face Spoofing Detection for Replay Attack Based on Gaze Estimation. *Biometric Recognition,* 201-211. Springer International Publishing.

Cardinaux, F., Sanderson, C. and Marcel, S. (2003). Comparison of MLP and GMM classifiers for face verification on XM2VTS. *Audio-and Video-Based Biometric Person Authentication*. Springer Berlin Heidelberg, 911-920.

Chetty, G. (2010). Robust audio visual biometric person authentication with liveness verification. In *Intelligent Multimedia Analysis for Security Applications*, 59-78. Springer Berlin Heidelberg.

Chetty, G. and Wagner, M. (2006). Multi-level liveness verification for face-voice biometric authentication. *IEEE Biometric Consortium Conference, Biometrics Symposium: Special Session on Research at the*, 1-6. Baltimore, Maryland.

Choudhury, T., Clarkson, B., Jebara, T. and Pentland, A. (1999). Multimodal person recognition using unconstrained audio and video. *International Conference on Audio- and Video-based Biometric Person Authentication (AVBPA'99),* Washington DC, 176-181.

Chaudhuri, B. B., Sarkar, N. and Kundu, P. (1993). Improved fractal geometry based texture segmentation technique. *IEE Proceedings E (Computers and Digital Techniques)*, *140*(5): 233-242.

Chingovska, I., Anjos, A., Marcel, S. (2012). On the effectiveness of local binary patterns in face anti-spoofing. *IEEE International Conference on Biometric Special Interest Group (BIOSIG),* Darmstadt, 6-7.

Chingovska, I., Anjos, A. and Marcel, S. (2013a). Anti-spoofing in action: joint operation with a verification system. *IEEE Conference on Computer Vision and Pattern Recognition Workshops (CVPRW),* 98-104.

Chingovska, I., Yang, J., Lei, Z., Yi, D., Li, S. Z., Kähm, O., Glaser, C., Damer, N., Kuijper, A., Nouak, A., Komulainen, J., Pereira, T., Anjos, A., Gupta, S., Khandelwal, S., Bansal, S., Rai, A., Krishna, T., Goyal, D., Waris, M. A., Zhang, H., Ahmad, I., Kiranyaz, S., Gabbouj, M., Tronci, R., Pili, M., Sirena, N., Roli, F., Galbally, J., Fierrez, J., Pinto, A., Pedrini, H., Schwartz, W. S., Rocha, A. and Marcel, S. (2013b). The 2nd competition on counter measures to 2D face spoofing attacks. *IEEE International Conference on Biometrics (ICB),* 1-6.

Cheng, F. L., John, C. L. and Alice, C. L. (2013). Analysis of variance and chi-square tests. *Statistics for Business and Financial Economics,* 544-612. Springer New York

Cristianini, N. and Shawe-Taylor, J. (2000). The learning methodology. *An introduction to support vector machines and other kernel-based learning methods*, 1-8. Cambridge university press.

Crest, R. (2011). *Super Real Face Mask*. *Beautiful/Decay*. Retrieved 10 October 2015, from http://beautifuldecay.com/2011/10/17/super-real-face-mask/

Davidian, M. and Louis, T. A. (2012). Why statistics?. *Science*, 336(6077): 12-12.

Ekman, G. (1959). Weber's law and related functions. *The Journal of Psychology*, 47(2): 343-352.

De Freitas Pereira, T., Anjos, A., De Martino, J. M. and Marcel S. (2013). LBP-TOP based countermeasure against face spoofing attacks. *ACCV 2012 Workshop, Part 1, LNCS 7728*, Springer, Berlin, Heidelberg, 121-132.

De Freitas Pereira, T., Komulainen, J., Anjos, A., De Martino, J. M., Hadid, A., Pietikäinen, M. and Marcel, S. (2014). Face liveness detection using dynamic texture. *EURASIP Journal on Image and Video Processing*, 2014(1): 1-15.

Dixon, W. J. and Massey, F. J. (1969). *Introduction to statistical analysis,* 344(2): 244-256. New York: McGraw-Hill.

Edrogmus, N., Marcel, S. (2014). Introduction. *Handbook of biometric anti-spoofing: trusted biometrics under spoofing attacks*, 1-11. Springer Verlag London.

Everitt, B. S. and Skrondal, A. (2002). The Cambridge dictionary of statistics. 4th edition. 306-307. *Cambridge University Press, New York.*

Frischholz, R. W. and Werner, A. (2003). Avoiding replay-attacks in a face recognition system using head-pose estimation. *IEEE International Workshop on Analysis and Modeling of Faces and Gestures, 2003. AMFG 2003.* 234-235

Galbally, J. and Marcel, S. (2014). Face anti-spoofing based on general image quality assessment. *IEEE 22nd International Conference on Pattern Recognition (ICPR),* 1173-1178

Galbally, J. and Marcel, S. (2014). Face anti-spoofing based on general image quality assessment. *IEEE 22nd International Conference on Pattern Recognition (ICPR),* 1173-1178

Gipp, B., Beel, J., Rössling, I. (2007). The ePassport in detail. *ePassport: The World's New Electronic Passport. A Report about the ePassport's Benefits, Risks and it's Security,* 17-33. Create Space Independent Publishing Platform.

Gragnaniello, D., Poggi, G., Sansone, C. and Verdoliva, L. (2015). An investigation of local descriptors for biometric spoofing detection. *IEEE Transactions on Information Forensics and Security,* 10(4): 849-863.

Guo, Z., Zhang, L. and Zhang, D. (2010). A completed modeling of local binary pattern operator for texture classification. *IEEE Transactions on Image Processing,* 19(6): 657-1663.

Hadid, A. (2008). The local binary pattern approach and its applications to face analysis. *IEEE First Workshops on Image Processing Theory, Tools and Applications (IPTA),* 1-9.

He, D. C. and Wang, L. (1990). Texture unit, texture spectrum, and texture analysis. *IEEE Transactions on Geoscience and Remote Sensing,* 28(4): 509-512.

He, X., Yan, S., Hu, Y., Niyogi, P. and Zhang, H. J. (2005). Face recognition using Laplacian faces. *IEEE Transactions on Pattern Analysis and Machine Intelligence,* 27(3): 328-340.

Housam, K. B., Lau, S. H., Pang, Y. H., Liew, Y. P. and Chiang, M. L. (2014). Face Spoofing Detection Based on Improved Local Graph Structure. *IEEE International Conference on Information Science and Applications (ICISA),* 1-4.

Huang, T., Xiong, Z. and Zhang, Z. (2011). Face recognition applications. In *Handbook of Face Recognition*, 617-638. Springer London.

Hubbard, R. (2004). Alphabet soup slurring the distinctions between p's and a's in psychological research. *Theory and Psychology*, 14(3): 295-327.

Ibrahim, M., Efat, M. I. A., Shamol, H. K., Khaled, S. M., Shoyaib, M. and Abdullah-Al-Wadud, M. (2014). Dynamic local ternary pattern for face recognition and verification. *8th WSEAS International Conference on Computer Engineering and Applications*, 146-151. Tenerife, Spain.

International Biometric Group. (2008). Biometrics Market and Industry Report 2009-2014. *International Biometric Group*.

Jain, A., Bolle, R. and Pankanti, S. (2006). Introduction to biometrics. *Biometrics: personal identification in networked society*, 479:1-41. Springer Science and Business Media.

Jain, A. K., Flynn, P. and Ross, A. A. (2007). Introduction to biometrics. *Handbook of biometrics*. 1-22. Springer Science and Business Media.

Jee, H. K., Jung, S. U., Yoo, J. H. 2006. Liveness detection for embedded face recognition system. *International Journal of Biological and Medical Sciences*, 1(4): 235-238.

Kähm, O. and Damer, N. (2012). 2D face liveness detection: An overview. *IEEE BIOSIG-Proceedings of the International Conference of the Biometrics Special Interest Group (BIOSIG), ,* 1-12.

Kant, C. and Sharma, N. (2013). Fake Face Recognition Using Fusion of Thermal Imaging and Skin Elasticity. *IJCSC*, 4(1): 65-72.

Kannala, J. and Rahtu, E. (2012). Bsif: Binarized statistical image features. *IEEE 21st International Conference on Pattern Recognition (ICPR),* 1363-1366.

Kim, S., Yu, S., Kim, K., Ban, Y., Lee, S. (2013). Face liveness detection using variable focusing. *International Conference on Biometrics (ICB),* 1-6. Madrid, Spain.

Kollreider, K., Fronthaler, H., Bigun, J. (2008). Verifying liveness by multiple experts in face biometrics. *IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops, CVPRW'08.* 1-6.

Kose, N., Dugelay, J. L. (2012). Classification of captured and recaptured images to detect photograph spoofing. *IEEE APR International Conference on Informatics, Electronics and Vision*, Dhaka, 1027–1032.

Kollreider, K., Fronthaler, H. and Bigun, J. (2008). Verifying liveness by multiple experts in face biometrics. *IEEE Computer Vision and Pattern Recognition Workshops. (CVPRW 2008)* Anchorages, AK, 23-28.

Kollreider, K., Fronthaler, H., Bigun, J. (2009). Non-intrusive liveness detection by face images. *Image and Vision Computing*, 27(3): 233–244.

Kollreider, K., Fronthaler, H., Faraj, M. I., Bigun, J. (2007). Real-time face detection and motion analysis with application in "liveness" assessment. *IEEE Transactions on Information Forensics and Security, 2*(3): 548-558

Komulainen, J., Hadid, A., Pietikainen, M., Anjos, A. and Marcel, S. (2013b). Complementary countermeasures for detecting scenic face spoofing attacks. *IEEE International Conference on Biometrics (ICB),* 1-7.

Komulainen, J., Hadid, A. and Pietikäinen, M. (2013a). Face spoofing detection using dynamic texture. *Computer Vision-ACCV 2012 Workshops,* 7728:146-157. Springer Berlin Heidelberg.

Lagorio, A., Tistarelli, M., Cadoni, M., Fookes, C. and Sridharan, S. (2013). Liveness detection based on 3D face shape analysis. *IEEE International Workshop on Biometrics and Forensics (IWBF),* 1-4.

Li, J., Wang, Y., Tan, T. and Jain, A. K. (2004). Live face detection based on the analysis of fourier spectra. *Defense and Security*, 296-303. International Society for Optics and Photonics.

Lu, J., Plataniotis, K. N. and Venetsanopoulos, A. N. (2003). Face recognition using LDA-based algorithms. *IEEE Transactions on Neural Networks,* 14(1): 195-200.

Määttä, J., Hadid, A. and Pietikainen, M. (2011). Face spoofing detection from single images using micro-texture analysis. *IEEE International joint conference on Biometrics (IJCB),* 1-7.

Mäenpää, T. and Pietikäinen, M. (2005). Texture analysis with local binary patterns. *Handbook of Pattern Recognition and Computer Vision*, *3*: 197-216.

Marcel, S. and Bengio, S. (2002). Improving face verification using skin color information. *16th International Conference on Pattern Recognition Proceeding*, 378-381.

Marcel, S., Keomany, J. and Rodriguez, Y. (2006). *Robust-to-illumination face localisation using active shape models and local binary patterns* (No. LIDIAP-REPORT-2006-016).

Materka, A. and Strzelecki, M. (1998). Texture analysis methods–a review. *Technical university of lodz, institute of electronics, COST B11 report, Brussels*, 9-11.

Mei, L., Yang, D., Feng, Z. and Lai, J. (2015). WLD-TOP Based Algorithm against Face Spoofing Attacks. *Biometric Recognition,* 135-142. Springer International Publishing.

Menotti, D., Chiachia, G., Pinto, A., Robson Schwartz, W., Pedrini, H., Falcao, X. A. and Rocha, A. (2015). Deep Representations for Iris, Face, and Fingerprint Spoofing Detection. *IEEE Transactions on Information Forensics and Security,* 10(4): 864-879.

Menotti, D., Chiachia, G., Pinto, A., Robson Schwartz, W., Pedrini, H., Xavier Falcao, A. and Rocha, A. (2015). Deep Representations for Iris, Face, and Fingerprint Spoofing Detection. *IEEE Transactions on Information Forensics and Security,* 10(4): 864-879.

Moghaddam, B., Jebara, T. and Pentland, A. (2000). Bayesian face recognition. *Pattern Recognition*, 33(11): 1771-1782.

Nuzzo, R. (2014). Statistical errors. *Nature*, 506(7487): 150-152.

Nanni, L., Lumini, A. and Brahnam, S. (2012). Survey on LBP based texture descriptors for image classification. *Expert Systems with Applications*, *39*(3): 3634-3641.

Ojala, T., Pietikainen, M. and Harwood, D. (1994). Performance evaluation of texture measures with classification based on Kullback discrimination of distributions. In *Pattern Recognition, Proceedings of the 12th IAPR International Conference on Computer Vision and Image Processing*, 1(1): 582-585.

Ojala, T., Pietikäinen, M. and Mäenpää, T. (2000). Gray scale and rotation invariant texture classification with local binary patterns. *Computer Vision-ECCV 2000*. Springer Berlin Heidelberg. 1842: 404-420.

Ojala, T., Pietikäinen, M. and Harwood, D. (1996). A comparative study of texture measures with classification based on featured distributions. *Pattern recognition*, 29(1): 51-59.

Ojala, T., Pietikäinen, M., Mäenpää, T. (2002). Multiresolution gray-scale and rotation invariant texture classification with local binary patterns. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 24(7): 971-987.

Pan, G., Sun, L., Wu, Z. and Lao, S. (2007). Eyeblink-based anti-spoofing in face recognition from a generic webcamera. *11th International Conference on Computer Vision, ICCV 2007. IEEE*, 1-8.

Pan, G., Wu, Z., Sun, L. (2008). Liveness detection for face recognition. *Recent Advances in Face Recognition,* 235-252. InTech, Austria.

Pan, G., Sun, L., Wu, Z. and Wang, Y. (2011). Monocular camera-based face liveness detection by combining eyeblink and scene context. *Telecommunication Systems*, *47*(3-4): 215-225.

Park, U., Choi, H. C., Jain, A. K., and Lee, S. W. (2013). Face tracking and recognition at a distance: A coaxial and concentric PTZ camera system. *IEEE Transactions on Information Forensics and Security*, *8*(10): 1665-1677.

Peixoto, B., Michelassi, C. and Rocha, A. (2011). Face liveness detection under bad illumination conditions. *Image Processing (ICIP), 18th IEEE International Conference on*, 3557-3560.

Pietikäinen, M., Hadid, A., Zhao, G. and Ahonen, T. (2011). Computer Vision Using Local Binary Patterns. *Computational Imaging and Vision,* 40(1): 3-12. Springer-Verlag London Limited.

Ramadan, R. M. and Abdel-Kader, R. F. (2009). Face recognition using particle swarm optimization-based selected features. *International Journal of Signal Processing, Image Processing and Pattern Recognition*, 2(2): 51-65.

Rassem, T. H. and Khoo, B. E. (2014). Completed local ternary pattern for rotation invariant texture classification. *The Scientific World Journal*, 2014(2014): 1-10.

Ratha, N., Connell, J., Bolle, R. M., and Chikkerur, S. (2006, August). Cancelable biometrics: A case study in fingerprints. IEEE *18th International Conference on Pattern Recognition (ICPR'06),* 4: 370-373.

Ratha, N. K., Connell, J. H. and Bolle, R. M. (2001). An analysis of minutiae matching strength. In *Audio-and Video-Based Biometric Person Authentication*. 2091: 223-228. Springer Berlin Heidelberg.

Rejman-Greene, M. (2005). Privacy issues in the application of biometrics: a european perspective. *Biometric systems*, 335-359. Springer London.

Sanderson, C. and Paliwal, K. K. (2003). Fast features for face authentication under illumination direction changes. *Pattern Recognition Letters*, 24(14): 2409-2419.

Satterthwaite, F. E. (1946). An approximate distribution of estimates of variance components. *Biometrics bulletin*, 2(6): 110-114.

Schuckers, S. A. C. (2002). Spoofing and anti-spoofing measures. *Information Security technical report*, *7*(4): 56-62.

Schwartz, W. R., Rocha, A. and Pedrini, H. (2011). Face spoofing detection through partial least squares and low-level descriptors. *International Joint Conference on Biometrics (IJCB)*, 11–13.

Shoniregun, C. A., and Crosier, S. (2008). Research overview and biometric technologies. *Securing Biometrics Applications*, 1-30. Springer Science+Business Media, LLC.

Soetjahjo, A. T. M. J. (2006). *Mathematical analysis of dynamic process models; index, inputs and interconnectivity*. TU Delft, Delft University of Technology.

Sun, L., Huang, W. and Wu, M. (2011). TIR/VIS correlation for liveness detection in face recognition. *Computer Analysis of Images and Patterns,* 114-121. Springer Berlin Heidelberg.

Szwoch, M., Pieniążek, P. (2012). Eye blink based detection of liveness in biometric authentication systems using conditional random fields. *Computer Vision and Graphics*. 669-676. Springer Berlin Heidelberg.

Tabula Rasa. (2010). *Trusted Biometrics Under Spoofng Attacks*. Retrieved on 25 January 2016, from http://www.tabularasa-euproject.org/demonstrations

Tan, X., Li, Y., Liu, J. and Jiang, L. (2010a). Face liveness detection from a single image with sparse low rank bilinear discriminative model. *Computer Vision–ECCV,* 504-517. Springer Berlin Heidelberg.

Tan, X. and Triggs, B. (2010b). Enhanced local texture feature sets for face recognition under difficult lighting conditions. *IEEE Transactions on Image Processing,* 19(6): 1635-1650.

Tipping, M. E. and Bishop, C. M. (1999). Probabilistic principal component analysis. *Journal of the Royal Statistical Society: Series B (Statistical Methodology)*, 61(3): 611-622.

Tirunagari, S., Poh, N., Windridge, D., Iorliam, A., Suki, N. and Ho, A. T. (2015). Detection of face spoofing using visual dynamics. *IEEE Transactions on Information Forensics and Security,* 10(4): 762-777.

Tirunagari, S., Poh, N., Windridge, D., Iorliam, A., Suki, N. and Ho, A. T. S. (2015). Detection of face spoofing using visual dynamics. *IEEE Trans. Inf. Forensics Security*, 10(4): 762–777.

Tolba, A. S., El-Baz, A. H. and El-Harby, A. A. (2006). Face recognition: A literature review. *International Journal of Signal Processing*, 2(2): 88-103.

Trier, O. D., and Taxt, T. (1995). Evaluation of binarization methods for document images. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, *17*(3), 312-315.

Tronci, R., Muntoni, D., Fadda, G., Pili, M., Sirena, N., Murgia, G., Ristori, M. and Roli, F. (2011). Fusion of multiple clues for photo-attack detection in face recognition systems. *IEEE International Joint Conference on Biometrics (IJCB),* 1-6.

Turk, M. and Pentland, A. P. (1991). Face recognition using eigenfaces. *Computer Vision and Pattern Recognition, 1991. Proceedings CVPR'91. IEEE Computer Society Conference on*, 586-591.

Verma, J. P. (2013). Chi-square test and its application. *Data Analysis in Management with SPSS Software*, 69-101. Springer India.

Wang, T., Yang, J., Lei, Z., Liao, S., Li, S. Z. (2013). Face liveness detection using 3d structure recovered from a single camera. *International Conference on Biometrics (ICB),* 1-6.

Wen, D., Han, H. and Jain, A. K. (2015). Face spoof detection with image distortion analysis. *IEEE Transactions on Information Forensics and Security,* 10(4): 746-761.

Wild, P., Radu, P., Chen, L. and Ferryman, J. (2016). Robust multimodal face and fingerprint fusion in the presence of spoofing attacks. *Pattern Recognition*, 50:17-25.

Yan, J., Zhang, Z., Lei, Z., Yi, D. and Li, S. Z. (2012). Face liveness detection by exploring multiple scenic clues. *IEEE12th International Conference on Control Automation Robotics and Vision (ICARCV),* 188-193.

Yang, W. and Sun, C. (2011). Face recognition using improved local texture patterns. *IEEE Intelligent Control and Automation (WCICA), 2011 9th World Congress on*, 48-51.

Zhang, Z., Yan, J., Liu, S., Lei, Z., Yi, D. and Li, S. Z. (2012). A face antispoofing database with diverse attacks. *5th IAPR international conference on Biometrics (ICB),* 26-31.

Zhang, J. and Tan, T. (2002). Brief review of invariant texture analysis methods. *Pattern recognition*, 35(3): 735-747.

Zhenyu, W., Rong, H., Wankou, Y. and Changyin, S. (2014). An enhanced Local Ternary Patterns method for face recognition. *33rd Chinese Control Conference (CCC),* 4636-4640.