UNIVERSITI PUTRA MALAYSIA

FACE LIVENESS DETECTION BASED ON IQA USING ANOVA FEATURE SELECTION

ENAS AKEEL RAHEEM ALKINANY

FK 2019 15

FACE LIVENESS DETECTION BASED ON IQA USING ANOVA FEATURE SELECTION

By

ENAS AKEEL RAHEEM ALKINANY

Thesis submitted to the School of Graduate Studies, Universiti Putra Malaysia, in Fulfilment of the Requirements for the Degree of Master of Science

April 2019

DEDICATION

To the purest heart I have known, My mother
To the beloved memory of my father
To my siblings, my husband, my daughter, all family members and friends
I humbly dedicate this effort.

Abstract of thesis presented to the Senate of Universiti Putra Malaysia in Fulfilment of the requirement for the degree of Master of Science

FACE LIVENESS DETECTION BASED ON IQA USING ANOVA FEATURE SELECTION

By

ENAS AKEEL RAHEEM ALKINANY

April 2019

Chairman: **Associate Professor Sharifah Mumtazah bt. Syed Ahmad Abdul Rahman, PhD**
Faculty : Engineering

In the past few decades, there has been a growing interest in Facial Biometric systems that became a trend in a wide range of technologies like security, access control and surveillance applications. However, Spoof attacks remain the main challenge faced by facial biometric systems. A spoof attack arises when an individual attempt to disguise as someone else by a fake face to get an unauthorized access to the system, a fake face could be a photograph, dummy face or even a video display. To overcome these attacks on such systems, face liveness detection has been produced.

There are various ways to detect the face liveness such by texture, motion analysis, determine a scenic clue or by using a thermal sensor. Two methods of detection were identified based on the necessity of user's cooperation with the system. One is known as intrusive which requires user interaction with the system such in motion detection and the other is non-intrusive were no user effort is needed. For this purpose, image quality assessment has been utilized in the literature for face anti-spoofing detection. Image quality measures (IQMs) are efficient, user friendly, non-intrusive, low cost and present a low degree of complexity in implementation. However, they exhibit some limitations in terms of accuracy and efficiency of the system.

Thus, an effective face liveness detection system based on image quality measures has been proposed in this thesis. The system was designed to conquer the limitations of accuracy in a trade off with high and cost ineffective feature extractor. System's effectiveness was evaluated and benchmarked with other existing related work on CASIA face anti-spoofing database and the expandability of proposed work was further proven on NUAA imposter database.

The feature set was selected based on IQMs discrimination power. Analysis of variance (ANOVA) was the statistical tool used to identify these IQMs. ANOVA was applied to find the p-value and F-score for each of the measures. A low p-value (high F score) for a test refers to an evidence to reject the null hypothesis. Then a feature selection strategy was further implemented to minimize the number of measures. The output measures have been employed as a feature extractor to design and develop the face liveness detection system. Image classification for real and fake samples was implemented by support vector machine (SVM). The system is restricted to 2D images.

The test results and evaluations have been implemented by the statistical analysis testing and by liveness detection system in terms of accuracy, half total error rate (*HTER*) and system's efficeincy. Results have consistently revealed that the proposed method outperforms other detection techniques over different types of spoofing attacks and mediums. The detection accuracy of the system was increased by nearly 13% while the computational load was decreased by approximately 50 % as compared to the state-of-art. The contribution of this work is to ensure the simplicity of detection system and improves its accuracy along with efficiency.

Abstrak tesis yang dibentangkan kepada SenatUniversiti Putra Malaysia dalam memenuhi keperluan ijazah Master Sains

SISTEM PENGECAMAN WAJAH BERDASARKAN IQA MENGGUNAKAN PILIHAN FEATURE ANOVA

Oleh

ENAS AKEEL RAHEEM ALKINANY

April 2019

Pengerusi : Profesor Madya Sharifah Mumtazah Syed Ahmad Abdul Rahman, PhD
Fakulti : Kejuruteraan

Dalam beberapa dekad kebelakangan ini, terdapat minat yang semakin mendalam terhadap sistem Biometrik Wajah yang menjadi tren dalam pelbagai teknologi seperti keselamatan, kawalan akses dan aplikasi pengawasan. Namun demikian, serangan tiruan atau *spoof* masih menjadi cabaran utama yang dihadapi oleh sistem biometrik wajah. Serangan tiruan muncul apabila seorang individu cuba untuk menyamar sebagai orang lain menggunakan wajah tiruan untuk mendapatkan akses memasuki sistem tanpa kebenaran; wajah tiruan boleh jadi satu fotograf, wajah tiruan, atau paparan video. Untuk mengatasi serangan seperti ini ke atas sistem, sistem pengecaman wajah telah dihasilkan.

Terdapat pelbagai cara untuk mengesan sesebuah wajah iaitu melalui tekstur, analisis pergerakan, menentukan klu pemandangan atau menggunakan pengesan haba. Dua metod pengecaman dikenalpasti berdasarkan keperluan kerjasama pengguna dengan sistem yang ada. Satu dikenali sebagai intrusif yang memerlukan pengguna berinteraksi dengan sistem seperti pengecaman pergerakan dan satu lagi bukan-intrusif di mana usaha dari pihak pengguna tidak diperlukan. Untuk tujuan ini, penilaian kualiti imej telah digunakan dalam literatur untuk mengesan anti-tiruan wajah. Pengukuran kualiti imej (IQMs) bersifat efisyen, mesra-pengguna, bukan-intrusif, kos rendah dan memberikan aras kompleksiti yang rendah dalam pelaksanaannya. Mereka memaparkan beberapa kekangan dari sudut ketepatan dan beban pengiraan sistem.

Oleh itu, sistem pengecaman wajah yang efektif berdasarkan pengukuran kualiti imej telah disarankan dalam tesis ini. Sistem ini direkacipta untuk mengatasi kekangan ketepatan dalam pertukaran dengan beban pengiraan yang tinggi dan menelan belanja yang besar. Keberkesanan sistem dinilai dan ditanda-aras dengan kajian sedia ada yang lain berkenaan pangkalan data anti-tiruan wajah CASIA dan kebolehlanjutan kajian yang disarankan telah dibuktikan ke atas pangkalan data tiruan NUAA.

Set fitur telah dipilih berdasarkan kuasa diskriminasi IQM. Analisis varian (ANOVA) adalah alat statistik yang digunakan untuk mengenalpasti IQM ini. ANOVA telah diaplikasi untuk mendapatkan nilai-p dan skor-F untuk setiap pengukuran. Satu nilai-p yang rendah (skor F tinggi) untuk sesuatu ujian merujuk kepada bukti dalam menolak hipotesis nul. Kemudian, satu strategi pemilihan fitur telah dilaksanakan lagi untuk meminimakan bilangan pengukuran. Pengukuran output telah digunakan sebagai pengestrak fitur untuk merekabentuk dan membangunkan sistem pengecaman wajah. Klasifikasi imej untuk sampel yang sebenar dan tiruan telah dilaksanakan oleh mesin vektor sokongan (SVM). Sistem tersebut dihadkan kepada imej-imej 2D.

Keputusan dan penilaian ujian telah dijalankan oleh pengujian analisis berstatistik dan sistem pengecaman wajah dari aspek ketepatan, separuh kadar jumlah ralat (HTER) dan beban pengiraan. Keputusan telah menunjukkan secara konsisten bahawa metod yang disarankan telah jauh lebih baik dari teknik-teknik pengesanan lain dari semua jenis serangan dan wadah tiruan yang berbeza. Ketepatan pengesanan dalam sistem meningkat oleh 13% sementara beban pengiraan berkurangan sebanyak 50 % berbanding dengan sistem yang lebih moden. Sumbangan kajian ini ialah memastikan kemudahan menggunakan sistem pengecaman dan mempertingkatkan ketepatannya seiring dengan keberkesanan pengiraannya.

ACKNOWLEGEMENTS

First, I'm truly grateful to "Almighty Allah" who surrounded me with strength and blessings and enabled me to fulfill the requirements of master's degree successfully.

I'd like to express my sincere gratitude to my supervisor Assoc. Prof. Dr. Sharifah Mumtazah bt. Syed Ahmad Abdul Rahman who supported and guided me through my study journey.

I'd also like to thank my supervisory committee member Assoc. Prof. Dr. Wan Azizun Wan Adnan for advices and guidance.

My deep appreciation and gratitude to all my family, my Husband and lovely daughter Jood, as well as my friends for their endless love, support and prayers in every moment of time.

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

Sharifah Mumtazah bt. Syed Ahmad Abdul Rahman, PhD
Associate Professor
Faculty of Engineering
Univerisiti Putra Malaysia
(Chairman)

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

ROBIAH BINTI YUNUS, 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 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: Enas Akeel Raheem Alkinany, GS48953

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

Figure **Page**

LIST OF ABBREVIATIONS

2D	Two Dimensions
3D	Three Dimensions
DB	Database
IQA	Image Quality Assessment
IQMs	Image Quality Measures
SVM	Support Vector Machine
ROC	Receiver Operating Characteristic
AUC	Area Under Curve
HTER	Half Total Error Rate
FPR	False Positive Rate
FNR	False Negative Rate

CHAPTER 1

INTRODUCTION

1.1 Background

Biometrics is a multidisciplinary field involved with measuring and mapping specific biological traits, e.g. fingerprints, face, palm veins, etc. to be used as an individualized code for recognition (Nixon, 2014). Biometric traits can be classified into two groups that are physical traits such as aforementioned examples and behavioral traits such as signature, voice and keystrokes. Biometric is essential for a wide range of technologies. However, one of the main obstacles facing biometric recognition systems is fraudulent identity which is conceptually referred as a spoofing attack.

Broadly, two types of attacks can be considered: indirect and direct attacks. Indirect attacks are performed inside the system, intruded by hackers or insiders, e.g. by tampering the feature extractor or the matcher, or by modifying the template database. Indirect attacks can be prevented by numerous measures including but not limited to anti-virus software, firewalls, encryption and intrusion detection. Direct attacks on the other hand, are performed at the sensor level outside the digital limits of the system and therefore, no mechanisms for digital protection can be used to anticipate it (Nixon, 2014).

An embedded facial biometric solution for mobile phones are very trendy nowadays with built-in mobile cameras to authorize user's access to the phone by scanning user's face. Such solutions were also previously provided with computers web-cameras to perform the same service in computers, such as Dell, Lenovo, Asus, Toshiba, and Apple. However, spoofing attacks are still crucial threat to these solutions in spite of the high performance of their biometric systems.

Facial spoofing attacks occur when a person masquerades or falsifies his identity to gain an unauthorized access to the biometric system. With the wide spread of social media applications and millions of users around the world sharing their images online made it easier to reproduce a fake sample where face can be viewed on alternative mediums such as a printed copy, digital image and even a video display.

Facial biometric systems are still susceptible to various of spoofing attacks. Thus, it is of necessity to secure such systems by providing additional layer of security through liveness detection that allows the biometric system to verify whether the sample being captured by the recognition system is genuine (i.e. alive) or has been mimicked by an illegitimate user.

A block diagram of face liveness detection system architecture is shown in Figure 1.1, it is necessary to clarify the exact process of using liveness detection system which involves a user to present a biometric sample to the sensor, which is camera in our case. The face image is then preprocessed and tested by extracting its features. Last it is classified as real or fake using a certain classifier based on existing training data.

A fake sample can be detected by several clues or life signs like motions (i.e. lip movement, eye blinking or head rotation etc.) or a comparison of skin textures. A user's cooperation with the system is required to produce facial movement. Hence, such systems become vulnerable when it is forged with a video display attack or if the user cannot perform the desired movement due to health issues. This leads to high false positive rate in detection system. An opposite type of system that does not involve any user cooperation is based on analyzing facial skin texture and reflectance properties (Feng, Po, Li, & Yuan, 2016a) which is mostly uses one image to perform spoofing detection, which makes it easier and more economical to implement.

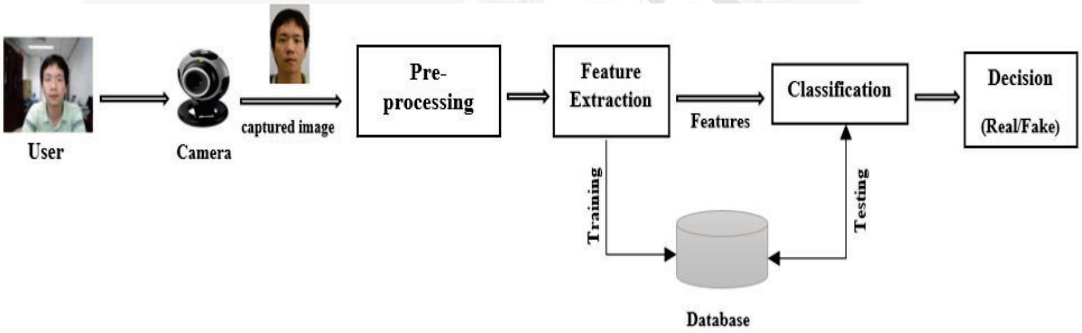

Figure 1.1: Block diagram of face liveness detection system

Lately, texture analysis has been widely utilized in liveness detection for being simple to implement, cost effective, and not intrusive in terms of user collaboration.

Image quality assessment (IQA) is one of the important methods utilized in image processing disciplines such as compression, recognition, restoration and similar applications. An image may contain various types of distortions like noise, contrast change and blur etc. Thus, it is very necessary to evaluate image quality. Conventionally, a subjective evaluation where humans assess the quality of an image based on requirements. Such process requires experts to rate image quality which is costly and time consuming. Therefore, an objective image quality assessment was of necessity. These quality metrics were based on the characteristics of the human visual system. There are two types of image quality measures (IQMs) classified based on their reliability on the existence of a reference image, full reference IQMs and no reference IQMs. the logic basis for using IQA in liveness detection is assisted by two factors, first is that IQA has been effectively implemented in earlier work for manipulation detection (Bayram, 2006), and steganalysis within forensics (Memon, 2003). And second is that different researchers have proposed liveness detection systems for both single and multibiometric systems which proved the effectiveness of using IQA for detection (Galbally & Marcel, 2014a; Galbally, Marcel, & Fierrez, 2014; S.A. Dhole, Patil, 2016)

1.2 Problem Statement

The general research problem lies in the vulnerability of face recognition systems to non-real faces (i.e. spoofing attacks) which is a serious security threat (Li, Correia, & Hadid, 2018) . However, several research efforts have attempted to overcome this problem by applying face liveness detection as an additional layer of security. Despite these trials, the performance of anti-spoofing system is still restrained by several challenges as explained below:

- In Previous related work where image quality assessment was utilized in face anti-spoofing , IQMs were chosen based on theoretical justification, no practical analysis and feature selection of used IQMs was experimentally established to select the best features prior to liveness detection system design which may result in system's efficiency degradation (Bhaskar & Aneesh, 2015; Galbally & Marcel, 2014a; Galbally et al., 2014; S.A. Dhole, Patil, 2016).
- Spoofing attacks are still serious threats specifically regarding the accuracy of the detection system in terms of total error rate achieved by the system during detection which can be affected by several factors such as the type of feature extractor being used, Type of sensor etc.(Galbally & Marcel, 2014b).

1.3 Research Objectives

The main objective of this work is to design and implement efficient and accurate face liveness detection system based on image quality assessment. To achieve this objective, the following is set to be done:

1. To extract a pool of IQA facial features and analyze their effectiveness statistically based on discrimination power.
2. To create an algorithm for selecting the best IQMs to build a feature extractor.
3. To evaluate a face liveness detection system using the feature extractor.

1.4 Research Scope

The scope of our research is to design and develop a face liveness detection system. The system basically lies in three steps image input and pre-processing step, feature extraction step and classification step. The proposed work aims to improve the performance by improving the feature extraction process. A utilization of statistical analysis method of ANOVA is to be performed. The maximum number of IQMs already used by researchers was 30 (Bhaskar & Aneesh, 2015) therefor the study is restricted to 30 general purpose IQMs to be examined for feature selection. The study is based on scenic clues of both image sequence and static image and restricted to 2D images. The work is to be evaluated in terms of the half total error rate and the accuracy of the system and its efficeincy in terms of the number of IQMs being used in the design of the feature extractor. CASIA-FAS database (Z. Zhiwei et al., n.d.) with three different image qualities, high quality, normal and low quality is to be utilized for benchmarking and NUAA imposter database was used to prove the expandability of feature on different types of databases.

1.5 Thesis Layout

This thesis is formulated into five chapters. The outlines of each chapter are described below:

Chapter 1 produces a general introduction to the research area and points out the current problems in designing an image quality assessment-based liveness detection system. It also identifies the objectives and the scope of the research.

Chapter 2 provides a systematic literature review of face liveness detection techniques. The theoretical background of Image quality assessment and its manipulation in face liveness detection are also presented. The statistical Analysis using analysis of variance (ANOVA), feature selection and image classification using support vector machine (SVM) are also presented in this chapter.

Chapter 3 introduces the detailed methodology of the proposed work and the design process flow of feature extractor and liveness detection system.

The test results of the statistical analysis, feature selection and the proposed face liveness detection system on CASIA-FAS and NUAA databases are discussed in chapter 4. Subsequently a conclusion is drawn in chapter 5 with suggestions for future directions.

REFERENCES

A, K. G. D. E. S. (2016). Short term re-identification of Automatic Teller Machine (ATM) users via face and body appearance features. In *2016 4th International Conference on Biometrics and Forensics (IWBF)* (pp. 1–6). IEEE. https://doi.org/10.1109/IWBF.2016.7449682

Agarwal, A., Singh, R., & Vatsa, M. (2016). Face anti-spoofing using Haralick features. In *2016 IEEE 8th International Conference on Biometrics Theory, Applications and Systems, BTAS 2016*. https://doi.org/10.1109/BTAS.2016.7791171

Ajani, K. (2012). Triage; a literature review of key concepts. *Journal of the Pakistan Medical Association*, *62*(5), 487–489. https://doi.org/10.1049/el

Akhtar, Z., & Foresti, G. L. (2016). Face Spoof Attack Recognition Using Discriminative Image Patches. *Journal of Electrical and Computer Engineering*, *2016*. https://doi.org/http://dx.doi.org/10.1155/2016/4721849

Akhtar, Z., Michelon, C., & Foresti, G. L. (2014). Liveness detection for biometric authentication in mobile applications. In *Proceedings - International Carnahan Conference on Security Technology* (Vol. 2014-Octob). https://doi.org/10.1109/CCST.2014.6986982

Alotaibi, A., & Mahmood, A. (2016). Enhancing computer vision to detect face spoofing attack utilizing a single frame from a replay video attack using deep learning. In *Proceedings - 2016 International Conference on Optoelectronics and Image Processing, ICOIP 2016* (pp. 1–5). https://doi.org/10.1109/OPTIP.2016.7528488

Arashloo, S. R., Kittler, J., & 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. https://doi.org/10.1109/TIFS.2015.2458700

Arathy, P. J., & Nair, V. V. (2016). Analysis of Spoofing Detection using Video Subsection Processing. In *Proceedings of the International Conference on Informatics and Analytics - ICIA-16* (pp. 1–6). https://doi.org/10.1145/2980258.2980416

Bashier, H. K., Hoe, L. S., Han, P. Y., Ping, L. Y., & Li, C. M. (2014). Face Spoofing Detection Using Local Graph Structure. *International Conference on Computer, Communications and Information Technology*, 14–17. https://doi.org/10.2991/ccit-14.2014.70

Bayram, S. (2006). Image manipulation detection. *Journal of Electronic Imaging*, *15*(4), 041102. https://doi.org/10.1117/1.2401138

Bhaskar, A., & Aneesh, R. P. (2015). Advanced algorithm for gender prediction with image quality assessment. *2015 International Conference on Advances in Computing, Communications and Informatics, ICACCI 2015*, 1848–1855. https://doi.org/10.1109/ICACCI.2015.7275887

Binny Reeba, Y., & Shanmugalakshmi, R. (2015). Spoofing face recognition. In *ICACCS 2015 - Proceedings of the 2nd International Conference on Advanced Computing and Communication Systems* (pp. 3–7). https://doi.org/10.1109/ICACCS.2015.7324132

Boser, B. E., Guyon, I. M., & Vapnik, V. N. (1992). A Training Algorithm for Optimal Margin Classifiers. In *Proceedings of the fifth annual workshop on Computational learning theory*. Pittsburgh, Pennsylvania, USA.

Boulkenafet, Z., Komulainen, J., & Hadid, A. (2016). Face Spoofing Detection Using Colour Texture Analysis. *IEEE Transactions on Information Forensics and Security*, *11*(8), 1818–1830. https://doi.org/10.1109/TIFS.2016.2555286

C, R. R. R. K. M. S. B. (2016). Face Presentation Attack Detection Across Spectrum using Time-Frequency Descriptors of Maximal Response in Laplacian Scale-Space. In *2016 Sixth International Conference on Image Processing Theory, Tools and Applications (IPTA)* (pp. 0–5). IEEE. https://doi.org/10.1109/IPTA.2016.7820961

Chingovska, I., Yang, J., Lei, Z., Yi, D., Li, S. Z., Kahm, O., … Marcel, S. (2013). The 2nd competition on counter measures to 2D face spoofing attacks. *Proceedings - 2013 International Conference on Biometrics, ICB 2013*, 1–6. https://doi.org/10.1109/ICB.2013.6613026

Chingovska, Ivana, Anjos, A., & Marcel, E. (2012). On the effectiveness of local binary patterns in face anti-spoofing. *International Conference of the Biometrics Special Interest Group*, 1–7. https://doi.org/10.1038/ng.3293

Chingovska, Ivana, Anjos, A. R. Dos, & Marcel, S. (2014). Biometrics evaluation under spoofing attacks. *IEEE Transactions on Information Forensics and Security*, *9*(12), 2264–2276. https://doi.org/10.1109/TIFS.2014.2349158

D., B., & M., R. (2006). Analysis of Gene Expression Data. In *Pharmacometrics: The Science of Quantitative Pharmacology* (pp. 473–507). Springer. https://doi.org/10.1002/9780470087978.ch18

Das, D., & Chakraborty, S. (2014). Face liveness detection based on frequency and micro-texture analysis. In *2014 International Conference on Advances in Engineering and Technology Research, ICAETR 2014* (pp. 3–6). https://doi.org/10.1109/ICAETR.2014.7012923

De Freitas Pereira, T., Anjos, A., De Martino, J. M., & Marcel, S. (2013). LBP-TOP based countermeasure against face spoofing attacks. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *7728 LNCS*(PART 1), 121–132.

https://doi.org/10.1007/978-3-642-37410-4_11

Erdogmus, N., & Marcel, S. (2013). Spoofing in 2D face recognition with 3D masks and anti-spoofing with Kinect. *IEEE 6th International Conference on Biometrics: Theory, Applications and Systems, BTAS 2013*. https://doi.org/10.1109/BTAS.2013.6712688

Eskicioglu, M., & Fisher, P. S. (1995). Image Quality Measures and Their Performance. *IEEE Transactions on Communications*, *43*(12), 2959–2965. https://doi.org/10.1109/26.477498

Feng, L., Po, L.-M., Li, Y., & Yuan, F. (2016a). Face liveness detection using shearlet-based feature descriptors. *Journal of Electronic Imaging*, *25*(4), 043014. https://doi.org/10.1117/1.jei.25.4.043014

Feng, L., Po, L.-M., Li, Y., & Yuan, F. (2016b). Face liveness detection using shearlet-based feature descriptors. *Journal of Electronic Imaging*, *25*(4), 043014. https://doi.org/10.1117/1.JEI.25.4.043014

Feng, L., Po, L. M., Li, Y., Xu, X., Yuan, F., Cheung, T. C. H., & Cheung, K. W. (2016). Integration of image quality and motion cues for face anti-spoofing: A neural network approach. *Journal of Visual Communication and Image Representation*, *38*. https://doi.org/10.1016/j.jvcir.2016.03.019

Fernandes, S. L., & Bala, G. J. (2016). Developing a Novel Technique for Face Liveness Detection. *Physics Procedia*, *78*(December 2015), 241–247. https://doi.org/10.1016/j.procs.2016.02.039

Fisher, R. A. (1921). On the probable error of a coefficient of correlation an found from a small sample. *Metron*, *1*, 3–32. https://doi.org/10.1093/biomet/9.1-2.22

Galbally, J., & Marcel, S. (2014a). Face anti-spoofing based on general image quality assessment. *Proceedings - International Conference on Pattern Recognition*, 1173–1178. https://doi.org/10.1109/ICPR.2014.211

Galbally, J., & Marcel, S. (2014b). Face anti-spoofing based on general image quality assessment. In *Proceedings - International Conference on Pattern Recognition* (pp. 1173–1178). https://doi.org/10.1109/ICPR.2014.211

Galbally, J., & Marcel, S. (2014c). Face anti-spoofing based on general image quality assessment. *Proceedings - International Conference on Pattern Recognition*, 1173–1178. https://doi.org/10.1109/ICPR.2014.211

Galbally, J., Marcel, S., & Fierrez, J. (2014). Image quality assessment for fake biometric detection: Application to Iris, fingerprint, and face recognition. *IEEE Transactions on Image Processing*, *23*(2), 710–724. https://doi.org/10.1109/TIP.2013.2292332

Galbally, J., Marcel, S., & Fierrez, J. (2015). Biometric Antispoofing Methods: A Survey in Face Recognition - IEEE Journals &amp; Magazine, *2*.

https://doi.org/10.1109/ACCESS.2014.2381273

Garcia, D. C., & Ricardo L. de Queiroz. (2015). Face-Spoofing 2D-Detection Based on Moiré-Pattern Analysis. *IEEE Transactions on Information Forensics and Security*, *10*(4), 778–786. https://doi.org/10.1109/TIFS.2015.2411394

Giulia Boato, F. G. B. D. N. Q.-T. P. D.-T. D.-N., & Department. (n.d.). Face spoofing detection using LDP-TOP. In *2016 IEEE International Conference on Image Processing (ICIP)*. Phoenix Convention Center, Phoenix, Arizona, USA: IEEE. https://doi.org/10.1109/ICIP.2016.7532388

Guyon, I. (2003). An Introduction to Variable and Feature Selection. *Journal of Machine Learning Research*, *3*, 1157–1182.

Hyogo, Y., Kiyota, N., Otsuki, N., Goto, S., Imamura, Y., Chayahara, N., … Minami, H. (2018). Thrombotic Microangiopathy with Severe Proteinuria Induced by Lenvatinib for Radioactive Iodine-Refractory Papillary Thyroid Carcinoma. *Case Reports in Oncology*, pp. 735–741. https://doi.org/10.1159/000494080

J, C. N. S.-T. (2014). *An introduction to support vector machines and other kernel-based learning methods*. Cambridge: Cambridge University Press. https://doi.org/10.1017/CBO9780511801389

JafariBarani, M., Faez, K., & Jalili, F. (2014). Implementation of Gabor Filters Combined with Binary Features for Gender Recognition. *International Journal of Electrical and Computer Engineering (IJECE)*, *4*(1), 108–115. Retrieved from http://iaesjournal.com/online/index.php/IJECE/article/view/4348

Kahm, O., & Damer, N. (2012). 2D face liveness detection: An overview. *BIOSIG-Proceedings of the IEEE International Conference of the. Biometrics Special Interest Group (BIOSIG).*, 171–182. Retrieved from http://cs.emis.de/LNI/Proceedings/Proceedings196/171.pdf

Kose, N., & Dugelay, J. L. (2012). Classification of captured and recaptured images to detect photograph spoofing. *2012 International Conference on Informatics, Electronics and Vision, ICIEV 2012*, 1027–1032. https://doi.org/10.1109/ICIEV.2012.6317336

Li, L., Correia, P. L., & Hadid, A. (2018). Face recognition under spoofing attacks: countermeasures and research directions. *IET Biometrics*. https://doi.org/10.1049/iet-bmt.2017.0089

Liu, A., Lin, W., & Narwaria, M. (2012). Image quality assessment based on gradient similarity. *IEEE Transactions on Image Processing*, *21*(4), 1500–1512. https://doi.org/10.1109/TIP.2011.2175935

M. C Hanumantharaju, M. Ravishankar, D. R. R. V. (2013). A Novel Full Reference Color Image Quality Assessment based on Energy Computation in Wavelet Domain. *Journal of Intelligent Systems*, *22*(2).

Machine learning for beginners and beyond | SAS. (n.d.). Retrieved May 15, 2019, from https://www.sas.com/en_us/insights/articles/analytics/machine-learning-for-beginners-and-beyond.html

Mann, P. S. (2009). *Introductory Statistics (7th Ed)* (7th ed.). United States of America: JOHN WILEY & SONS, INC. Retrieved from http://www.wiley.com/college/mann

Martini, M. G., Hewage, C. T. E. R., & Villarini, B. (2012). Signal Processing : Image Image quality assessment based on edge preservation. *Signal Processing : Image Communication*, *27*(8), 875–882. https://doi.org/10.1016/j.image.2012.01.012

Memon, N. (2003). Steganalysis Using Image Quality Metrics. *IEEE Transactions on Image Processing*, *12*(2), 221–229. https://doi.org/10.1109/TIP.2002.807363

Mittal, A., Moorthy, A. K., & Bovik, A. C. (2011). Blind/referenceless image spatial quality evaluator. In *Conference Record - Asilomar Conference on Signals, Systems and Computers* (pp. 723–727). IEEE. https://doi.org/10.1109/ACSSC.2011.6190099

Mittal, A., Soundararajan, R., & Bovik, A. C. (2013). Making a completely blind image quality analyzer. *IEEE Signal Processing Letters*, *20*(3), 209–212. https://doi.org/10.1109/LSP.2012.2227726

Moorthy, A. K., & Bovik, A. C. (2010). A two-stage framework for blind image quality assessment. In *Proceedings - International Conference on Image Processing, ICIP* (Vol. 17, pp. 2481–2484). https://doi.org/10.1109/ICIP.2010.5651745

Nill, N. B., & Bouzas, B. (1992). Objective image quality measure derived from digital image power spectra. *Optical Engineering*, *31*(4), 813–825. https://doi.org/10.1117/12.56114

Nixon, M. S. (2014). *Handbook of Biometric Anti-Spoofing*. Verlag London: Springer. https://doi.org/10.1007/978-1-4471-6524-8

NUZZO, R. (2014). Scientific method: Statistical errors. *Nature*, 150–152. https://doi.org/10.1038/506150a

O., O. E., O., O. S., A., O. J., Adebayo, A.-A., O., A.-A., & B., E. K. (2013). Facial Image Verification and Quality Assessment System FaceIVQA. *International Journal of Electrical and Computer Engineering (IJECE)*, *3*(6), 863–874. Retrieved from http://iaesjournal.com/online/index.php/IJECE/article/view /5034

Parveen, S., Ahmed, S. M. S., Abbas, N. H., Naeem, N., & Hanafi, M. (2016). Texture analysis using local ternary pattern for face anti-spoofing. *Sci. Int*, *28*(2), 965–971.

Parveen, S., Mumtazah, S., Ahmad, S., Hanafi, M., Azizun, W., & Adnan, W. (2015). Face anti-spoofing methods. *Current Science*, *108*(NO. 8,).

Patel, K., Han, H., & Jain, A. K. (2016). Secure Face Unlock: Spoof Detection on Smartphones. *IEEE Transactions on Information Forensics and Security*, *11*(10), 2268–2283. https://doi.org/10.1109/TIFS.2016.2578288

Peng, J., & Chan, P. P. K. (2014). Face liveness detection for combating the spoofing attack in face recognition. In *International Conference on Wavelet Analysis and Pattern Recognition* (Vol. 2014-Janua, pp. 176–181). https://doi.org/10.1109/ICWAPR.2014.6961311

Pravallika, P. (2016). SVM Classification For Fake Biometric Detection Using Image Quality Assessment: Application to iris, face and palm print P. In *2016 International Conference on Inventive Computation Technologies (ICICT)*. Coimbatore, India: IEEE. https://doi.org/10.1109/INVENTIVE.2016.7823189

Pudil, P., Novovicova, J., & Kittler, J. (1994). Floating search methods in feature selection. *Pattern Recognition Letters*, *15*(11).

Raghavendra, R., Raja, K. B., & Busch, C. (2016). Detecting morphed face images. In *2016 IEEE 8th International Conference on Biometrics Theory, Applications and Systems, BTAS 2016*. https://doi.org/10.1109/BTAS.2016.7791169

Ravibabu, V. (2014). A Vary Approach to Face Recognition Veritable Mechanisms for Android Mobile against Spoofing. In *IEEE International Conference on Computational Intelligence and Computing Research*. IEEE. https://doi.org/10.1109/ICCIC.2014.7238290

Rencher, A. C. (2012). Methods of Multivariate Analysis, Second Edition. *IIE Transactions*. A JOHN WILEY & SONS, INC. PUBLICATION. https://doi.org/10.1080/07408170500232784

Roli, B. B. Z. A. G. F. G. L. M. F. (2012). Security evaluation of biometric authentication systems under real spoofing attacks. *IET Biometrics*, *1*(1), 11–24.

Rumsey, D. (2010). *Statistics Essentials Dummies*. Indiana, Canada: Wiley Publishing,INC.

S.A. Dhole, Patil, A. A. (2016). System for Multi-biometric Detection. *2016 International Conference on Inventive Computation Technologies (ICICT)*, *3*(2).

Sankur, B. (2002). Statistical evaluation of image quality measures. *Journal of Electronic Imaging*, *11*(2), 206. https://doi.org/10.1117/1.1455011

Shao, R., Lan, X., Yuen, P. C., & Member, S. (2018). Joint Discriminative Learning of Deep Dynamic Textures for 3D Mask Face Anti-spoofing. *IEEE*

Transactions on Information Forensics and Security, *PP*(8), 1. https://doi.org/10.1109/TIFS.2018.2868230

Sheikh, H. R. (2004). Image information and visual quality. In *IEEE International Conference on Acoustics, Speech, and Signal Processing* (Vol. 3, pp. 709–712). Fairmont Queen Elizabeth Hotel, Montreal, Quebec, Canada: IEEE. https://doi.org/10.1109/ICASSP.2004.1326643

Shih, F. Y. (2010). *Image processing and pattern recognition _ fundamentals and techniques*. USA: Wiley Publishing,INC.

Shoniregun, C. A., & Crosier, S. (2008). *Securing Biometrics Applications*. Boston, MA: Springer US.

Silpa, K., & Mastani, S. A. (2012). Comparison Of Image Quality Metrics. *International Journal of Engineering Research & Technology (IJERT)*, 1–5.

Silva, A. M. De, & P.H.W.Leong. (2015). Feature Selection. In *Grammer-based feature Generation for Time-SSerieS Prediction* (SpringerBr, pp. 13–25). Springer. https://doi.org/10.1007/978-981-287-411-5

Soundararajan, R., & Bovik, A. C. (2012). RRED indices: Reduced reference entropic differencing for image quality assessment. *IEEE Transactions on Image Processing*, *21*(2), 517–526. https://doi.org/10.1109/TIP.2011.2166082

Suneet Betrabet, C. K. B. (2015). Structural Similarity Based Image Quality Assessment Using Full Reference Method. *International Journal of Scientific Engineering and Technology*.

Tan, X.; Li, Y.; Liu, J.; Jiang, L. (2010). Face liveness detection from a single image with sparse low rank bilinear discriminative model. In E. Daniilidis, K., Maragos, P., Paragios, N. (Ed.), *Proceedings of the 11th European Conference on Computer Vision* (p. Volume 6316,pp. 504–517). Heraklion, Greece: Lecture Notes in Computer Science. Springer: Berlin/Heidelberg, Germany.

Thomas Huang, Ziyou Xiong, and Z. Z. F. (2011). *Handbook of Face Recognition*. (S. Z. Li & A. K.Jain, Eds.). USA: Springer.

Vert, J., & Sch, B. (2004). A primer on kernel methods. In *Kernel Methods in Computational Biology*.

Wang, Z., Bovik, A. C., Sheikh, H. R., & Simoncelli, E. P. (2004). Image quality assessment: From error visibility to structural similarity. *IEEE Transactions on Image Processing*, *13*(4), 600–612. https://doi.org/10.1109/TIP.2003.819861

Wang, Z., Simoncelli, E., & Bovik, A. C. (2003). Multiscale structural similarity for image quality assessment. In *The Thrity-Seventh Asilomar Conference on Signals, Systems & Computers, 2003* (Vol. 2, pp. 1398–1402). CA,USA: IEEE. https://doi.org/10.1109/ACSSC.2003.1292216

Waris, M., Zhang, H., Ahmad, I., Kiranyaz, S., & Gabbouj, M. (2013). EUSIPCO 2013 1569744187 Analysis Of Textural Features For Face Biometric Anti-Spoofing. *EUSIPCO*, 1–5.

Wen, D., Han, H., & Jain, A. K. (2015). Face spoof detection with image distortion analysis. *IEEE Transactions on Information Forensics and Security*, *10*(4), 746–761. https://doi.org/10.1109/TIFS.2015.2400395

Yang, J., Lei, Z., Yi, D., & Li, S. Z. (2015). Person-Specific Face Antispoofing With Subject Domain Adaptation. *IEEE Transactions on Information Forensics and Security*, *10*(4), 797–809. https://doi.org/10.1109/TIFS.2015.2403306

Yao, S., Lin, W., Ong, E., & Lu, Z. (2005). Contrast signal-to-noise ratio for image quality assessment. In *Susu Yao, Weisi Lin, EePing Ong, & Zhongkang Lu. (2005). Contrast signal-to-noise ratio for image quality assessment. IEEE International Conference on Image Processing 2005*. IEEE. https://doi.org/doi:10.1109/icip.2005.1529771

Yeh, C. (2018). Face Liveness Detection Based on Perceptual Image Quality Assessment Features with Multi-scale Analysis. In *2018 IEEE Winter Conference on Applications of Computer Vision Face*. Nevada , U.S: IEEE. https://doi.org/10.1109/WACV.2018.00012

Yuming Li, Lai-Man Po , Xuyuan Xu, Litong Feng, F. Y. (2016). Face liveness detection and recognition using shearlet based feature descriptors. *ICASSP*, 874–877.

Z. Zhiwei et al. (n.d.). A face antispoofing database with diverse attacks,. In *Proc. Int. Conf. on Biometrics (ICB), 2012, pp. 26–31.*

Zhou Wang, Sheikh, H. R., & Bovik, A. C. (2002). No-reference perceptual quality assessment of JPEG compressed images. In *Proceedings. International Conference on Image Processing* (Vol. 1, pp. I-477-I–480). IEEE. https://doi.org/10.1109/ICIP.2002.1038064

BIODATA OF STUDENT

Enas Akeel Raheem received her Bachelor of Science degree in Computer Engineering – Software Engineering branch from University of Technology (UOT), Baghdad, Iraq in June 2013.

She joined the same department of Computer Engineering later on November 2013 till now as a tutor. She worked in software engineering branch laboratories as lab. Tutor, she was also appointed as the head of Department Media Unit and participated in many department's subcommittees.

Currently, she is pursuing her master's degree in University Putra Malaysia. Her field of study is biometric.

LIST OF PUBLICATIONS

Articles

Statistical Analysis of Image Quality Measures for Face Liveness Detection. *Springer LNEE (Lecture Notes in Electrical Engineering). **(Published)***

Insight on Face Liveness Detection: A Systematic Literature Review. *International Journal of Electrical and Computer Engineering (IJECE).* (***Accepted)***