A REVIEW PAPER ON FACE RECONGNITION ALGORITHMS AND TECHNIQUES

[1]Sheikh Irfan Ul Haq, [2]Ms Rashmi, [3]Mr Gurbaj Singh

Chandigarh Engineering College Landran
Punjab Technical University, Jalandhar, Punjab, India.

Abstract: The face spoof technique was proposed to identify and detect the spoofed and non-spoofed images. The DWT technique is used to analyze the textual features present within the test images. There is a possibility that some exceptional disturbances are available like geometric disturbances and the artificial texture disturbances. The camera and the illumination subordinates are mostly responsible for such disturbances. A perfect camera with no defects should be used just to notice the difference between the geometric, the illumination and the texture based disturbances. To detect the whether the image is spoofed or non-spoofed already existed technique SVM classifier is used. The SVM based technique is proposed in the previous work for the detection of face spoof. The face spoof detection techniques are based on two steps, the first step is of feature extraction and second is of classification. The eigan based technique is applied for the feature extraction and SVM classifier is applied for the classification. To improve accuracy of the face spoof detection SVM classifier will be replaced with the KNN classifier. The Comparisons are made to analyze the performance of the proposed algorithm and the existing algorithm in terms of accuracy and time of execution.

Keywords*: *Face Detection, Face Recognition, Feature Extraction, Digital Image, Image Processing

INTRODUCTION

1.1 Face Detection

As a convenient user authentication technique, automatic face recognition has attracted increasing attention in different get to control applications, particularly for mobile phone unlocking. With the release of face unlocking functionality in the Android mobile operating system, face recognition turns into another biometric authentication technique for mobile phones, like fingerprint authentication (Touch ID) in the iOS system. Not at all like fingerprint authentication, face recognition does not require any additional sensor since every single advanced mobile phone come equipped with a front confronting camera. Be that as it may, like other biometric modalities, we have to address worries about face parody assaults on face recognition systems, especially in unconstrained detecting and uncooperative subject situations [1]. Face recognition has turned into an exceptionally dynamic area of research in recent years for the most part because of increasing security demands and its potential commercial and law enforcement applications. In spite of the fact that a trivial task for the human brain, face recognition has turned out to be greatly hard to imitate artificially, since the commonalities do exist between faces, they differ impressively in terms of age, skin, color and gender. The problem is further muddled by contrasting image qualities, facial expressions, background, and illumination conditions. The fundamental function of this step is to determine [2]

(1) Whether human faces appear in a given image, and

(2) Where these faces are located at.

The normal yields of this step are patches containing every face in the input image. So as to make additionally face recognition system more robust and simple to design, face alignment are performed to justify the scales and orientations of these patches. Other than serving as the pre-processing for face recognition, face detection could be utilized for region-of-interest detection, retargeting, video and image classification, and so on. After the face detection step, human-face patches are extracted from images. Specifically utilizing these patches for face recognition has a few disadvantages:

- In the first place, every patch as a rule contains more than 1000 pixels, which are too expensive to build a robust recognition system.

- Second, face patches might be taken from various camera alignments, with various face expressions, illuminations, and may suffer from occlusion and clutter.

To beat these drawbacks, feature extractions are performed to do information packing, dimension reduction, salience extraction, and noise cleaning [3]. After this step, a face patch is normally transformed into a vector with fixed dimension or a set of fiducially points and their corresponding locations. In the wake of formulizing the representation of every face, the last step is to perceive the identities of these faces. Keeping in mind the end goal to achieve automatic recognition, a face database is required to build. For every person, a few images are taken and their features are extracted and stored in the database. At that point when an input face image comes in, we perform face detection and feature extraction, and compare its feature to every face class stored in the database.

There have been many explores and algorithms proposed to deal with this classification problem, and we'll discuss them in later sections.

There are two general applications of face recognition, one is called identification and another is called verification. Face identification implies given a face image, we need the system to tell who he/she is or the most possible or valid identification; while in face verification, given a face image and a guess of the identification, we need the system to inform true or false concerning the guess [4].

With a specific end goal to produce a system for recognition, we generally require data sets for building categories and compare similarities between the test data and every category. A test data is generally called a "query" in image retrieval written works, and we will utilize this term throughout this report. Beginning from the data sets side, we first perform dimension reduction on the stored raw data. After dimension reduction, every raw data in the data sets is transformed into a set of features, and the classifier is for the most part trained on these feature representations. At the point when a query comes in, we perform a similar dimension reduction procedure on it and enter its features into the trained classifier. The yield of the classifier will be the optimal class (some of the time with the classification accuracy) label or a rejection note (return to manual classification) [5].

1.2 Face Spoofing

Biometrics alludes to technologies that measure and analyze human body characteristics. Biometrics traits can be categorized into two classes:

- Physical characteristics, for example, fingerprints, faces or iris patterns and
- Behavioral characteristics, for example, voice, signature or strolling patterns (step).

Be that as it may, a standout amongst the most predominant challenges in numerous biometric recognition systems is the likelihood of identity theft, which is reasonably known as spoofing attack. Some stolen biometrics data can be effectively exploited and mimicked by impostors to gain unauthorized access to the biometric system, without the consent of the genuine user. Cases of spoofing attacks on biometrics systems incorporate the utilization of artificial fingers, contact focal point with retinal patterns and recorded voice. The state-of-the-art spoofing identification techniques for facial biometrics in light of liveness detection are presented in a portion of the work.

Generally, fake faces can be categorized into two classes: positive and negative. The positive class, otherwise called the genuine face, has limited variation, though the negative class incorporates the spoof faces on photographs, dummy or recorded videos. Facial biometrics spoofing techniques involve setting genuine photographs, playing video recording and so forth in front of the camera. A human photo represents planar objects with just a single static facial expression. Be that as it may, it lacks the three-dimensional (3D) information and gives less physiological clues than videos. These limitations of still photographs are frequently exploited in liveness detection for facial biometrics. Be that as it may, the challenges in facial detection increase for spoofing attacks that involve the utilization of camcorders. These days, videos of a genuine user with facial expressions, eye flicker and head movement can be effortlessly caught utilizing amazing cameras. The biometric system can be spoofed by utilizing a 3D corporeal model which is known as synthesis attack. Dummy models can normally reproduce rigid head movement by rotation yet can't imitate the lip movement, eye flicker and facial expressions. Recently, studies on the face liveness detection have been generally explored with a specific end goal to tackle the problem of spoofing attacks. Face liveness detection involves a procedure of verifying whether the face image presented to recognition system is real (i.e. alive) specimen or has been reproduced synthetically and is along these lines fraudulent [7].

1.2.1 Methods for Face Spoofing Detection

With the growing popularity of utilizing face recognition for get to control, this topic has attracted significant attention in the course of recent years. There are different face spoof detection algorithms which shift as indicated by their strengths and limitations in terms of (i) robustness and speculation ability, and (ii) real-time response and usability. As per different types of cues utilized as a part of face spoof detection, published methods can be categorized into four groups:

(i) Motion based methods,

(ii) Texture based methods,

(iii) Method based on image quality analysis, and

(iv) Methods based on other cues [8].

(i) Motion based methods: These methods, planned basically to counter printed photo attacks, catch a vital sign for vitality: the subconscious motion of organs and muscles in a live face, for example, eye blink, mouth development and head rotation.

(ii) Texture based methods: To counter the printed photo and replayed video attacks, texture based methods were proposed to extract image artifacts in spoof face images. Texture based methods have achieved significant success on the Idiap and CASIA databases. Unlike motion based methods, texture based methods require just a single image to detect a spoof.

(iii) Methods based on image quality analysis: A recent work proposed a biometric liveness detection strategy for iris, unique mark and face images utilizing 25 image quality measures, including 21 full-reference measures and 4 non-reference measures. By complexity, the proposed approach intends to improve the speculation ability under cross-database situations, which has seldom been explored in the biometrics community [10].

(iv) Methods based on other cues: Face spoof countermeasures utilizing cues derived from sources other than 2D intensity image, for example, 3D depth, IR image and voice have likewise been proposed. Be that as it may, these methods impose extra requirements on the user or the face recognition framework, and thus have a narrower application range.

1.2.2 Cross-database and Intra-database methods

In spite of the fact that various face spoof detection methods have been reported, to our knowledge, none of them generalizes well to cross-database scenarios. In particular, there is a lack of investigation on how face spoof detection methods perform in cross-database scenarios. The fundamental differences between intra-database and cross-database scenarios are as follows:

i) In an intra-database situation, it is assumed that the spoof media (e.g., photo and screen display), camera, environmental factors, and even the subjects are known to a face liveness detection system. This assumption does not hold in a large portion of the real scenarios. The intra-database performance of a face liveness detection system is just the upper bound in terms of performance that can't be expected in real applications.

ii) In cross-database situation, we allow differences of spoof media, cameras, environments, and subjects during the system development stage and the system deployment stage. Subsequently this cross-database performance better reflects the actual performance of a system that can be expected in real applications [11].

iii) Existing methods, particularly methods utilizing texture features, ordinarily utilized features (e.g., LBP) that are capable of capturing facial details and differentiating one subject from the other (with the end goal of face recognition). As a result, when similar features are utilized to differentiate a genuine face from a spoof face, they either contain some redundant information for liveness detection or information that is excessively person particular. These two factors limit the speculation ability of existing methods. To take care of this issue, we have proposed a feature set based on Image Distortion Analysis (IDA) with real-time response (extracted from a single image with efficient computation) and better speculation performance in the cross-database situation. Compared to the current methods, the proposed method does not try to extract features that capture the facial details, yet try to capture the face image quality differences because of the different reflection properties of different materials, e.g., facial skin, paper, and screen. As a result, experimental results demonstrate that the proposed method has better speculation ability.

1.3 Image Distortion Analysis for Face Spoofing

In mobile applications, the real-time response of face spoof detection requires that a decision be made based on a limited number of frames, e.g., close to 30 frames (_1 sec. for videos of 30 fps). Subsequently, we intend to design discriminative features that are capable of differentiating amongst genuine and spoof faces based on a single frame. Given a situation where a genuine face or a spoof face, (for example, a printed photo or replayed video on a screen) is presented to a camera in a similar imaging environment, the main difference amongst genuine and spoof face images is expected to the "shape" and characteristics of the facial surface in front of the camera [12].

Printed photo attack: In printed photo attack, I(x) is initially transformed to the printed ink intensity on the paper and afterward to the final image intensity through diffusion reflection from the paper surface. During this transformation, G(x) and H(x) are determined by the printer frequency and chromatic fidelity. In this way, image distortion in printed photo attack can be approximated by a contrast degrading transformation.

Replay video attack: In replay video attack, I(x) is transformed to the radiating intensity of pixels on LCD screen. In this way, G(x) is determined by the frequency band width of the LCD panel, the distortion of which can be neglected. H(x) is related to the LCD shading distortion and intensity transformation properties. Other than the difference in diffuse reflectance, the specular reflectance of the spoof face likewise differentiates from that of the genuine face, which is caused by the spoof medium surface. Because of the lustrous surface of tablet/mobile phone and the glossy ink layer on the printed paper, there is usually a specular reflection around the spoof face image. While for a genuine 3D face, specular reflection is just located in particular locations, (for example, nose tip, glasses, forehead, cheeks, and so forth.). In this manner, pooling the specular reflection from the entire face image can likewise capture the image distortion in spoof faces [13]. The capturing distortion can apply to both genuine and spoof faces. The spoof faces are more vulnerable to such distortion since they are usually captured in close distance to conceal the discontinuity of spoof medium frame. For instance, defocused blurriness is ordinarily observed in both printed photo and replayed video attacks. Based on the above analysis, the major distortions in a spoof face image include:

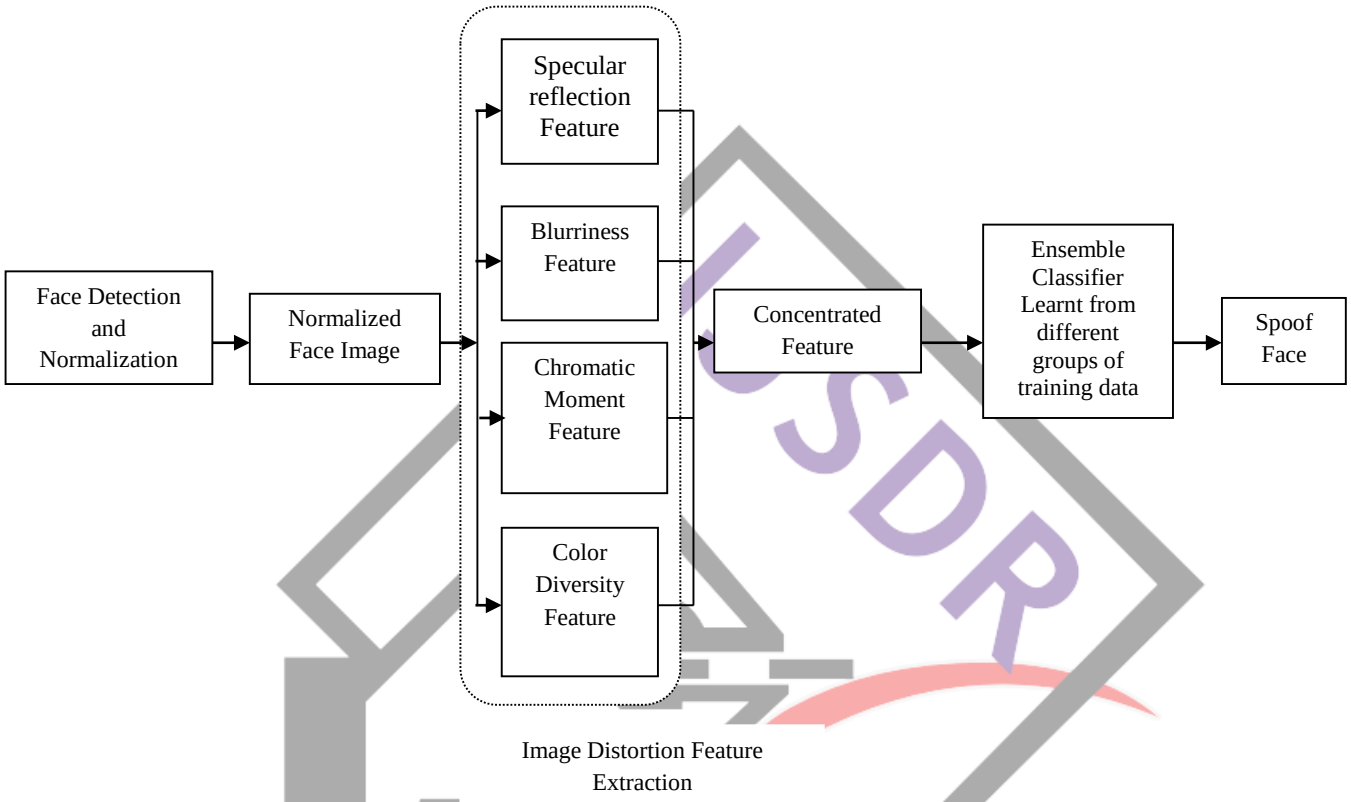
(1) Specular reflection from the printed paper surface or LCD screen;

(2) Image blurriness due to camera defocus;

(3) Image chromaticity and contrast distortion due to imperfect color rendering of printer or LCD screen; and

(4) Color diversity distortion due to limited color resolution of printer or LCD screen.

Fig 1. Face spoof detection algorithm based on Image Distortion Analysis



LITERATURE REVIEW

Samarth Bharadwaj, et.al, "Computationally efficient face spoofing detection with motion magnification," 2013

For a robust face biometric system, a reliable anti-spoofing approach must be deployed to circumvent the print and replay attacks. A few techniques have been proposed to counter face spoofing, however a robust solution that is computationally efficient is still unavailable. This paper presents another approach for spoofing detection in face videos utilizing motion magnification. Eulerian motion magnification approach is used to enhance the facial expressions commonly exhibited by subjects in a captured video [15]. Next, two types of feature extraction calculations are proposed: (i) a configuration of LBP that provides improved performance compared to other computationally expensive texture based approaches and (ii) motion estimation approach utilizing HOOF descriptor. The HOOF descriptors acquired from motion magnified videos provide state-of-the-art performance on the Print Attack and Replay Attack datasets in terms of precision and computational efficiency. On the Print Attack and Replay Attack spoofing datasets, the proposed framework improves the state-of-art performance; particularly HOOF descriptor yielding a near perfect half total error rate of 0% and 1.25% individually.

Jukka Komulainen, et.al," Context based Face Anti- Spoofing," 2013

The face recognition community has at long last started giving careful consideration to the long-neglected problem of spoofing attacks and the quantity of countermeasures is gradually increasing. Genuinely great results have been reported on the publicly available databases yet it is reasonable to assume that there exists no superior anti-spoofing procedure because of the varying nature of attack situations and acquisition conditions. Hence, to approach the problem of face spoofing as a set of attack-particular sub-problems, methods are proposed that are solvable with a proper combination of complementary countermeasures. Inspired by how we humans can perform reliable spoofing detection just based on the avail-capable scene and context information, this work provides the first investigation in research literature that attempts to detect the presence of spoofing medium in the observed scene [16]. The paper experiments with two publicly available databases comprising of a few fake face attacks of different nature under

varying conditions and imaging qualities. The experiments demonstrate excellent results past the state of the art. All the more importantly, cross-database evaluation depicts that the proposed approach has promising speculation capabilities.

Ivana Chingovska, et.al," On the effectiveness of local binary patterns in face anti-spoofing", 2014

Spoofing attacks are one of the security traits that biometric recognition systems are proven to be vulnerable to. Whenever spoofed, a biometric recognition system is bypassed by presenting a copy of the biometric evidence of a valid user. Among all biometric modalities, spoofing a face recognition system is particularly easy to perform: all that is required is a simple photograph of the user. In this paper, we address the problem of detecting face spoofing attacks. In particular, we inspect the potential of texture features based on Local Binary Patterns (LBP) and their variations on three types of attacks: printed photographs, and photos and videos displayed on electronic screens of different sizes [18]. The LBP based anti-spoofing method guarantees different levels of certainty for different types of attacks and different databases. A few attacks can beguile this counterfeit more effectively than others. There is no consistency in the results with regards to the types of attacks, nor the attacks from different databases. Our belief is this is not valid just for texture-based methods, but rather likewise for methods that approach the problem from different viewpoint. For this purpose, we introduce REPLAY-ATTACK, a novel publicly available face spoofing database which contains all the mentioned types of attacks. We conclude that LBP, with 15% Half Total Error Rate, demonstrate moderate discriminability when confronted with a wide set of attack types.

Tiago de Freitas Pereira, et.al," LBP-TOP based countermeasure against face spoofing attacks", 2012

User authentication is an important step to protect information and in this field face biometrics is advantageous. Face biometrics is natural, easy to use and less human-invasive. Tragically, recent work has revealed that face biometrics is vulnerable to spoofing attacks utilizing low-tech cheap supplies. This article presents a countermeasure against such attacks based on the LBP-TOP operator consolidating both space and time information into a single multi-resolution texture descriptor [19]. Experiments did with the REPLAY ATTACK database demonstrate a Half Total Error Rate (HTER) improvement from 15:16% to 7:60%. Remark that results with SVM classifier ought to be taken with care because with the increase of the multi-resolution range, the SVM classifier tends to over-train on the information. Be that as it may, experiments with simpler classifiers, for example, LDA, demonstrated that the LBP-TOP multi-resolution approach still demonstrated an incredible potential against face spoofing in different sort of attacks situations, beating the state of art results.

Nesli Erdogmus et.al," Spoofing in 2D face recognition with 3D masks and anti-spoofing with kinect," 2013

The problem of detecting face spoofing attacks (presentation attacks) has recently gained a merited popularity. For the most part focusing on 2D attacks forged by showing printed photos or replaying recorded videos on mobile devices, a critical bit of these studies ground their arguments on the flatness of the spoofing material in front of the sensor. In this paper, we inspect the spoofing potential of subject-specific 3D facial masks for 2D face recognition [20]. Also, we break down Local Binary Patterns based countermeasures utilizing both color and depth data, obtained by Kinect. For this purpose, we introduce the 3D Mask Attack Database (3DMAD), the first publicly available 3D spoofing database, recorded with a low-cost depth camera. Extensive experiments on 3DMAD demonstrate that effortlessly attainable facial masks can pose a serious threat to 2D face recognition systems and LBP is a powerful weapon to eliminate it. For reproducible research, the source code is made publicly available, together with the database and its protocols. A conceivable extension to this work is to explore the spoofing performances in 3D face recognition systems and to devise methods to detect attacks utilizing pure 3D data, instead of 2.5D. Also, encourage investigation should be possible on spoofing the spoofing potential of every mask separately.

Nicholas Evans, et.al," Spoofing and countermeasures for automatic speaker verification," 2013

It is widely acknowledged that most biometric systems are vulnerable to spoofing, otherwise called imposture. While vulnerabilities and countermeasures for other biometric modalities have been widely studied, e.g. face verification, speaker verification systems remain vulnerable. This paper gives an overview of recent research in spoofing and countermeasures for ASV [21]. While plainly ASV systems can be vulnerable to spoofing, most vulnerability discussed in this paper involves relatively high-cost, high-technology attacks. Moreover, countermeasures, some of them relatively trivial, can possibly detect spoofing attacks with manageable impacts on system ease of use. This paper portrays some specific vulnerability studied in the literature and presents a brief survey of recent work to create spoofing countermeasures. The paper concludes with a discussion on the requirement for standard datasets, metrics and formal evaluations which are expected to assess vulnerabilities to spoofing in realistic scenarios without prior knowledge. Additionally work ought to dissect the potential for spoofing through risk assessment and address a few weaknesses in the current research methodology.

Ajita Rattani, et.al," Analysis of user-specific score characteristics for spoof biometric attacks," 2012

A few studies in biometrics have confirmed the existence of user-specific score characteristics for genuine and zero-effort impostor score distributions. As an important consequence, biometric users contribute disproportionately to the FRR (false reject rate) and FAR (false acknowledge rate) of the system [22]. This phenomenon is otherwise called the Doddington zoo impact. Recent studies indicate the vulnerability of unimodal and multi-biometric systems to spoof attacks. The point of this study is to break down the score characteristics for spoof attacks. Such an analysis will 1) enhance our comprehension of the Doddington zoo impact under spoof attacks; and 2) allow us to design biometric classifiers that are more robust to such attacks. The commitments of this paper

are as follows: a) looking at the existence of user-specific score characteristics for spoof attacks and b) breaking down the correlation between user-specific score characteristics obtained on genuine (and also zero-effort impostor) and non zero-effort impostor (spoof) score distributions. Experiments conducted on the LivDet09 spoofed fingerprint database confirm that biometric user-groups exhibit different degrees of vulnerability to spoof attacks too. Further, moderate negative correlation may exist between users who are difficult to perceive and their vulnerability to spoof attacks.

Zhiwei Zhang, et.al," A face antispoofing database with diverse attacks," 2012

Face anti-spoofing has now attracted intensive attention, aiming to assure the reliability of face biometrics. We see that currently the greater part of face anti-spoofing databases focus on data with little variations, which may restrain the speculation performance of trained models since potential attacks in certifiable are probably more complex. In this paper we discharge a face anti-spoofing database which covers an assorted scope of potential attack variations [23]. Specifically, the database contains 50 genuine subjects, and fake faces are produced using the high quality records of the genuine faces. Three imaging qualities are considered, specifically the low quality, normal quality and high quality. Three fake face attacks are implemented, which include warped photo attack, cut photo attack and video attack. In this manner every subject contains 12 videos (3 genuine and 9 fake), and the final database contains 600 video clips. Test protocol is provided, which comprises of 7 scenarios for a thorough evaluation from every single conceivable angle. A baseline algorithm is additionally given for comparison, which explores the high recurrence information in the facial region to decide the liveness. We trust such a database can serve as an evaluation platform for future researches in the literature.

Di Wen, et.al," Face Spoof Detection with Image Distortion Analysis", 2015

Automatic face recognition is presently widely used in applications ranging from de-duplication of identity to authentication of mobile payment. This popularity of face recognition has raised concerns about face spoof attacks (otherwise called biometric sensor presentation attacks), where a photo or video of an authorized person's face could be used to gain access to offices or services. While a number of face spoof detection techniques have been proposed, their speculation capacity has not been adequately addressed. We propose an efficient and rather robust face spoof detection algorithm based on Image Distortion Analysis (IDA) [24]. Four different features (specular reflection, haziness, chromatic moment, and color diversity) are extracted to frame the IDA feature vector. A gathering classifier, comprising of various SVM classifiers trained for different face spoof attacks (e.g., printed photo and replayed video), is used to distinguish amongst genuine and spoof faces. The proposed approach is extended to multi-frame face spoof detection in videos utilizing a voting based scheme. We additionally collect a face spoof database, MSU Mobile Face Spoofing Database (MSU MFSD), utilizing two mobile devices (Google Nexus 5 and MacBook Air) with three types of spoof attacks (printed photo, replayed video with iPhone 5S and iPad Air). Experimental results on two public-domain face spoof databases (Idiap REPLAY-ATTACK and CASIA FASD), and the MSU MFSD database demonstrate that the proposed approach outperforms state-of-the-art methods in spoof detection. Our results likewise highlight the difficulty in separating genuine and spoof faces, particularly in cross-database and cross-device scenarios.

References

[1] Q. Yang, S. Wang, and N. Ahuja, "Real-time specular highlight removal using bilateral filtering," in Proc. ECCV, 2010, pp. 87–100.

[2] V. Christlein, C. Riess, E. Angelopoulou, G. Evangelopoulos, and I. Kakadiaris, "The impact of specular highlights on 3D-2D face recognition," in Proc. SPIE, 2013.

[3] R. Tan and K. Ikeuchi, "Separating reflection components of textured surfaces using a single image," IEEE Trans. Pattern Anal. Mach. Intell., vol. 27, no. 2, pp. 178–193, Feb. 2005.

[4] J.-F. Lalonde, A. A. Efros, and S. G. Narasimhan, "Estimating the natural illumination conditions from a single outdoor image," Int. J. Comput. Vision, vol. 98, no. 2, pp. 123 – 145, 2011.

[5] H. Han, S. Shan, X. Chen, S. Lao, and W. Gao," Separability oriented preprocessing for illumination-insensitive face recognition," in Proc. ECCV, 2012, pp. 307–320.

[7] F. Crete, T. Dolmiere, P. Ladret, and M. Nicolas, "The blur effect: perception and estimation with a new no-reference perceptual blur metric," in Proc. SPIE: Human Vision and Electronic Imaging XII, 2007.

[8] P. Marziliano, F. Dufaux, S. Winkler, and T. Ebrahimi, "A no-reference perceptual blur metric," in Proc. ICIP, vol. 3, 2002, pp. 57–60.

[10] B. E. Boser, I. M. Guyon, and V. N. Vapnik, "A training algorithm for optimal margin classifiers," in Proc. 5th ACM Workshop on Computational Learning Theory, 1992, pp. 144–152.

[11] A. Bashashati, M. Fatourechi, R. K. Ward, and G. E. Birch, "A survey of signal processing algorithms in brainccomputer interfaces based on electrical brain signals," Journal of Neural Engineering, vol. 4, no. 2, pp. R32–R57, 2007.

[12] C. Hou, F. Nie, C. Zhang, D. Yi, and Y. Wu, "Multiple rank multi-linear SVM for matrix data classification," Pattern Recognition, vol. 47, no. 1, pp. 454 – 469, 2014.

[13] Y. Lin, F. Lv, S. Zhu, M. Yang, T. Cour, K. Yu, L. Cao, and T. Huang," Large-scale image classification: Fast feature extraction and svm training," in Proc. IEEE CVPR, June 2011, pp. 1689–1696.

[14] C.-C. Chang and C.-J. Lin, "LIBSVM: A library for support vector machines," ACM Trans. Intell. Syst. Technol., vol. 2, no. 3, pp. 27:1–27, May 2011.

[15] S. Bharadwaj, T. I. Dhamecha, M. Vatsa, and R. Singh, "Computationally efficient face spoofing detection with motion magnification," in Proc. CVPR Workshops, 2013, pp. 105–110.

[16] J. Komulainen, A. Hadid, and M. Pietik¨ainen, "Context based Face Anti- Spoofing," in Proc. BTAS, 2013, pp. 1–8.

[18] I. Chingovska, A. Anjos, and S. Marcel, "On the effectiveness of local binary patterns in face anti-spoofing," in Proc. IEEE BIOSIG, 2012, pp.1–7.

[19] T. de Freitas Pereira, A. Anjos, J. M. De Martino, and S. Marcel," LBP-TOP based countermeasure against face spoofing attacks," in Proc. ACCV Workshops, 2012, pp. 121–132.

[20] N. Erdogmus and S. Marcel, "Spoofing in 2D face recognition with 3D masks and anti-spoofing with kinect," in Proc. IEEE BTAS, 2013, pp.1–6.

[21] N. Evans, T. Kinnunen, and J. Yamagishi, "Spoofing and countermeasures for automatic speaker verification," in Proc. INTERSPEECH, 2013, pp. 925–929.

[22] A. Rattani, N. Poh, and A. Ross, "Analysis of user-specific score characteristics for spoof biometric attacks," in Proc. CVPR Workshops, 2012, pp. 124–129.

[23] Z. Zhang, J. Yan, S. Liu, Z. Lei, D. Yi, and S. Z. Li, "A face antispoofing database with diverse attacks," in Proc. ICB, 2012, pp. 26–31.

[24] Di Wen, Hu Han, and Anil K. Jain," Face Spoof Detection with Image Distortion Analysis", IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, Vol. 4, No. 3, 2015, pp. 90-102.

[25] Santosh Tirunagari, Norman Poh, David Windridge, Aamo Iorliam, Nik Suki, and Anthony T.S. Ho., "Detection of Face Spoofing Using Visual Dynamics", 2014, IEEE TRANS. ON INFORMATION FORENSICS AND SECURITY

[26] Saptarshi Chakraborty and Dhrubajyoti Das, "AN OVERVIEW OF FACE LIVENESS DETECTION", 2014, International Journal on Information Theory (IJIT), Vol.3, No.2