FACE SPOOF DETECTION USING CHROMATIC GRAPH AND HISTOGRAM CONCATENATION METHOD USING CLASSIFICATION TECHNIQUES

[1]Beena Arul Anand, [2]ProfA.S. Gaikwad

[1]MTech 2nd year student, [2]Assistant Professors,
[1,2] Department of Computer Science and Engineering,
[1,2]Deogiri Institute of Engineering and Management Studies, Aurangabad(MH), India

Abstract: Automatic facial recognition is now widely used in applications ranging from identity deduplication to mobile payment authentication. This popularity of facial recognition has raised concerns about face simulation attacks (also known as biometric sensor presentation attacks), where a photo or video of an authorized person's face can be used to gain access to facilities or services. While a number of face detection techniques have been proposed, the ability to place general implications has not been adequately addressed. We offer a robust and relatively robust face detection algorithm using image distortion analysis (IDA). Four different features (Specular reflection, blurry, color moment and color variety) were isolated to create a feature IDA class ensemble vector, which consists of several SVM classifiers that have been trained for counterfeit face forgery attacks. Different method (Eg printed photos and replayed videos) used to distinguish between genuine faces and pseudo faces. The proposed method extends to detecting multiple face fakes in the video using voting patterns. In addition, we have compiled a database of face forgery, MSU Mobile Face Spoofing database (MSU MFSD) using two mobile devices (Google Nexus 5 and MacBook Air) with three types of spoof attacks. (Photos printed with replay videos with iPhone 5S and iPad Air)

IndexTerms **– Face recognition, spoof detection, cross-database.**

I. INTRODUCTION

As a convenient user authentication technique, automatic face recognition attracts more attention in several access control applications, especially for unlocking mobile phones. With the launch of the facial unlocking feature in the Android mobile operating system, facial recognition has become another biometric authentication technique for mobile phones, similar to fingerprint authentication (Touch ID). In the iOS system, facial recognition does not require additional sensors because each smartphone comes with a front camera. However, as with other biological radiations [1], [2], we must address concerns about face-to-face attacks in facial recognition systems, especially in situations of unlimited awareness and lack of cooperation [3]. Receiving a person's face or video (such as with a digital camera or social networks) is easier than obtaining other biological characteristics such as fingerprints, fingerprints and iris. In addition, the cost of activating fake faces, such as printed photos, visualized images or videos that are reproduced is relatively low. The modern commercial face recognition system (COTS) is not well designed to distinguish fake faces from real faces. Figure 2 shows the face identification performance of the COTS face recognition system when faking faces due to probes. It was paired with a genuine face in the gallery. In this experiment, more than 70% of the probes (pseudo-faces) have been paired with the gallery by COTS11 at number 1, indicating that COTS1 can not effectively distinguish between genuine faces and deceived faces.

In this article, we study the problem of cross-database face counterfeiting[4] detection and propose fake face detection methods based on image distortion analysis (IDA). The contributions of this article can be summarized as follows:

i) Face detection algorithms using IDA, which are effective for capturing the actual distortion of false face images related to images of genuine faces.
ii) We created a face forgery database called MSU Mobile Face Spoof Database (MSU MFSD) using laptop cameras (MacBook Air3) and mobile phones (Google Nexus 54) and three types of attack media (iPad, iPhone, MSU MFSD database Help us evaluate [5] The general meaning of face detection algorithms in different cameras and lighting conditions with mobile devices for a subset of MSU MFSD databases (35 subjects). We have received permission from participants to disclose information of to the public

II. LITERATURE SURVEY

To our knowledge, one of the earliest studies on face spoof detection was reported in 2004 by Li et al. [6]. With the growing popularity of using face recognition for access control, this topic has attracted significant attention over the past five years [6], [7]–[8]. One of the major focus of the FP7 EU funded project, TABULA RASA [8], is "trusted biometrics under spoofing attacks". Here, we provide a brief summary of face spoof detection algorithms published in the literature along with their strengths and limitations in terms[9] of
(i) robustness and generalization ability, and
(ii) realtime response and usability. According to different types of cues used in face spoof detection, published methods can be categorized into four groups:
(i) motion based methods,
(iii) texture based methods,
(iii) method based on image quality analysis, and

(iv) methods based on other cues

(i) Motion based methods

These methods are designed to counter the attack. The most important image is power: the subconscious movement of organs and muscles in the living face, such as blinking [10], mouth movements [11] and Rotate the head [12]. Since the motion is a relative property in the video frame, these methods are expected to have a better generalization ability than the method. Use the surface that will be mentioned below. However, the limitation of the method used is clear. The frequency of facial movements is limited by the human physiological rhythm, which ranges from 0.2 to 0.5 Hz [13], so it takes quite a long time (usually> 3 seconds) to accumulate stable power properties for face forgery detection. In addition, movement based methods can be easily avoided or confused by other movements such as background movements that are not related to facial movements or repetition in video attacks.

(ii) Texture based methods

In retaliation for both printed photographs and replayed videos, the surface-based method was proposed to separate the artifacts of the image in a fake image. [14] The author argued that surface features (such as LBP, DoG or HOG can distinguish artifacts in the face of forgery from genuine faces. Surface-based methods have been very successful in the Idiap database and CASIA Half Total Error Rate (HTER) 5 on the Idiap database has decreased from 13.87% in [14] and 7.60% in [15] to 6.62% in [16] By combining surface cues Which is different from the method of movement based on the method that uses the surface, requires only one image to detect counterfeiting However, the ability to generalize the methods used in many surfaces is not good. The study reported in [17] shows that for two methods, according to the surface (proposed in [4] and [16]), HTER is greatly increased under cross-database situations. (Where training sets and tests come from different face forgery databases) due to the data-driven nature of the surface-based methods, they can adapt to particular lighting and image conditions, so it cannot Well concluded with the database collected under different conditions.

(iii) Methods based on image quality analysis

Recent work [18] offers methods for detecting biometric liveness for iris, fingerprints and face images using 25 image quality measurements, including 21 full reference designs and 4 non-reference measurements. Compared to [19], our work is different in the following areas: (1) While 25 features are required in [20] for good results, no face data is considered in the design.Features Data for the detection of forged face. In contrast, four features are specifically designed for facial features in our methods, and we demonstrate the effectiveness of these features for detecting fake faces (2) while the author [21] Evaluate their methods in the Idiap-Replay database only. We use both the Idiap database and CASIA, which are two important public domain databases (3) Same database for training and testing In contrast, the proposed method aims to improve the generalization of capabilities under the situation of cross-database data which is rarely surveyed in the biological community.

(iv) Methods based on other cues

Facing face forgery using cues derived from sources other than 2D intensity images such as 3D depth [19], IR images [6], counterfeiting contexts [20] and sound [21]. However, these methods has sets additional requirements for users or face recognition systems, and hence has a narrower application range. For example, an IR sensor is required in [6]. Need to use a microphone and speech analyzer in [22] and must use many face photos taken from different perspectives in [19]. In addition, counterfeit context methods Proposed in [23] can be avoided by concealing counterfeit media.

In the situation within the database, it is assumed that counterfeiting media (Such as displaying photos and screens) cameras, environmental factors, and even those types that are known in face detection systems This assumption is not kept in most real situations. The performance of the internal database of face detection systems is just the upper bound in terms of performance that cannot be expected in real applications. Ii) In cross-database scenarios, we allow different types of media. Counterfeiting of cameras, cameras, environments and objects during the system development process and system deployment steps Therefore, the efficiency across this database reflects the actual performance of the system that can be expected in real applications. Iii) Existing methods, especially methods that use surface properties, commonly used properties (eg LBP) that can record face details and distinguish one from another (For face recognition purposes).

Therefore, when using the same features to distinguish genuine faces from pseudo-pages, they may have some redundant data for motion detection or personal information too. These two factors limit the ability to generalize the existing methods. To solve this problem, we have proposed a feature set based on image distortion analysis (IDA) with real-time response (Separated from a single image with effective calculations) and improved general performance in cross-database situations Compared to the existing method, the proposed method does not try to separate the features that capture the face details. But trying to capture the difference in the quality of the face due to the different reflecting properties of different materials such as the surface of the paper and the screen As a result, the experimental results show that the proposed method has a better generalization ability.

III. PROPOSED SYSTEM

(i) System Architecture

When considering situations where genuine faces or faces are spoofed (Such as printed photos or videos that are replayed on the screen) will be presented to the camera in the same shooting environment. The main difference between the genuine face image and the fake is caused by the "shape and appearance of the floor".

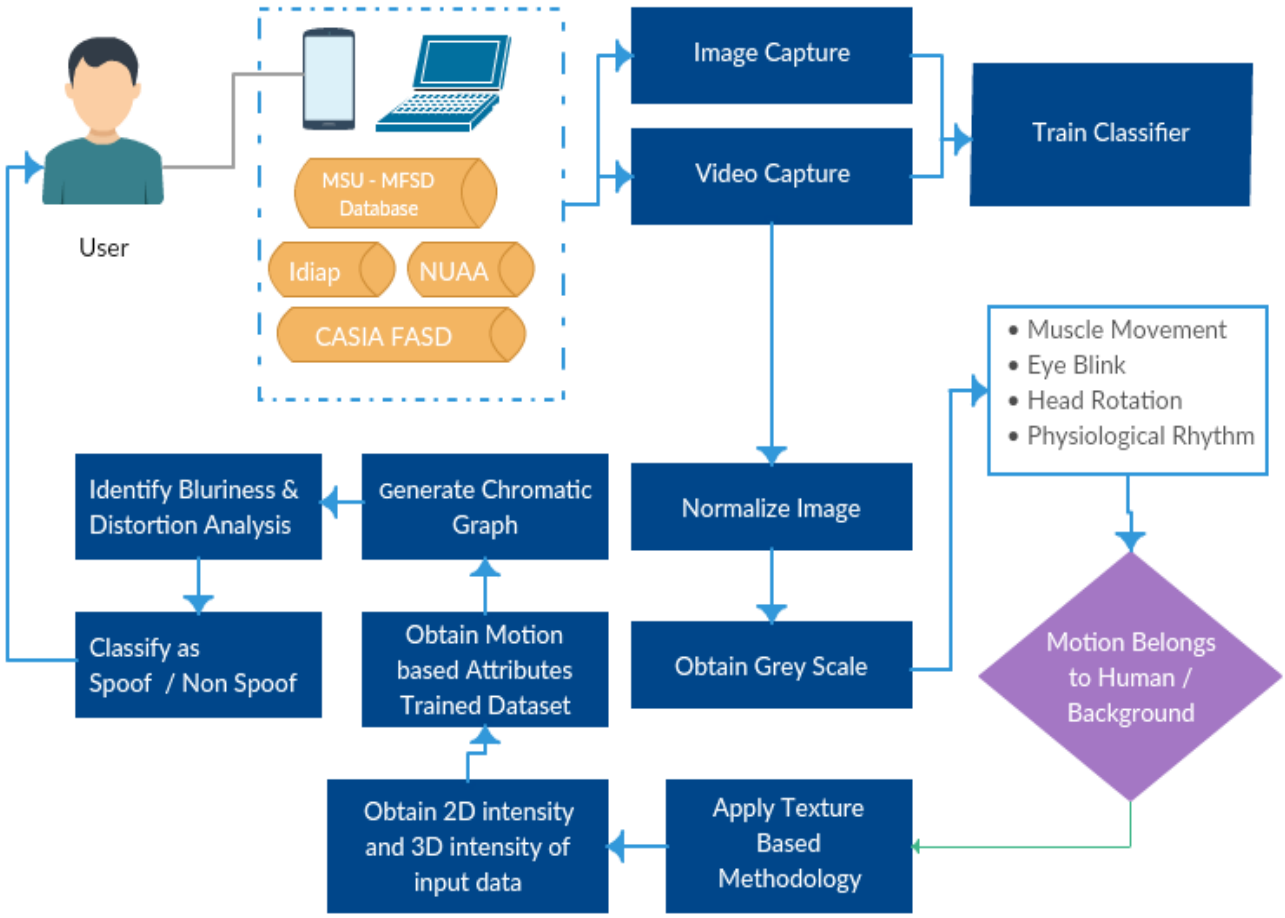

Figure1. Proposed Architecture

Surface of the front face of the camera according to the Dichromatic Reflection Model [24] Reflection I of the object at a specific position x can be broken down into diffuse reflection (Id) and specular reflection (Is):

$$I(x) = Id + Is = wd(x)S(x)E(x) + ws(x)E(x) \quad (1)$$

Where E (x) is the intensity of the incident light, wd (x) and ws (x) is a geometric factor for diffuse and specular reflections, respectively, and S (x) is a diffuse reflection ratio Due to the counterfeit 2D faces that have been modified from the original face image, the formation of the pseudo-facial image intensity I (x) can be created as follows.

$$I(x) = Id + Is = F(I(x)) + ws(x)E(x) \quad (2)$$

Please note that the equation (1) and (2) are just different forms of reflection between genuine faces and counterfeits and do not consider the quality of the final image after the camera captures in the equation (2). Instead of the diffuse reflection of the pseudo-face image I d by F (I (x)) because the diffuse reflection is determined by the distortion of the original face image. I(x).

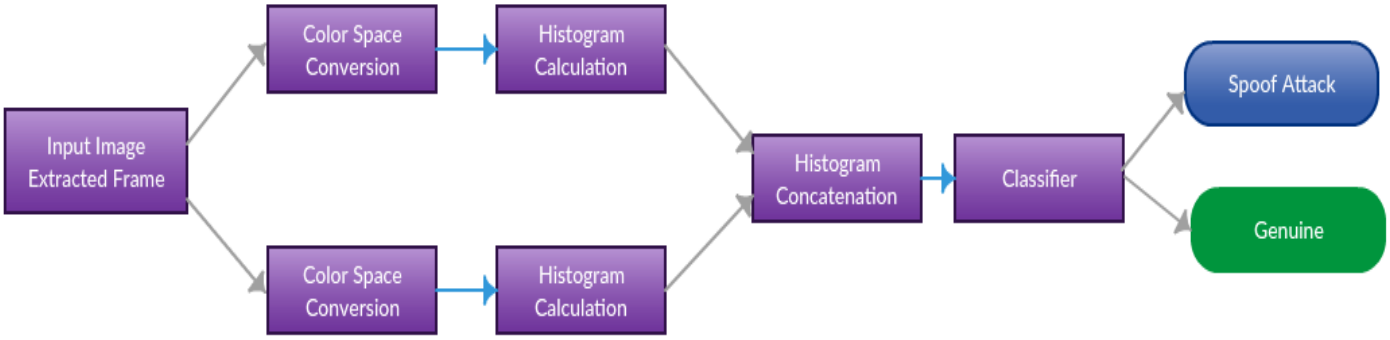

Figure 2.Flow Diagram

Therefore, the total distortion in I (x) compared to I (x) consists of two parts: i) Distortion in the diffraction component (I d) and ii) Distortion in both reflective elements (I s) of Which is related to counterfeiting media In particular, I relate to the original face image that I (x) while I am free from me (x). In addition, the distortion function F (x) in the diffuse reflection element can be modeled. Are

$$F(I(x)) = H(GI(x)) \quad (3)$$

Where G (x) is a low pass point distribution function (Makes the original face blurred) and H (x) as the histogram conversion function (Distortion of color intensity) Explanation of G (x) and H (x) In the attack, printed photos and video attacks, replay are detailed below. From this photographic model, we analyze the important differences between genuine faces and two types of pseudo faces. (Printing photos and videos repeatedly, playing repeatedly or attacking photos) studied in this article.

(ii) Pseudo Code

1) First select the brightest 0.1 percent pixel in the dark box frame from video or from a photo.

2) In these pixels, the strongest pixel in the input image is chosen as the ambient light estimate.

3) Based on the approximation of the transit map ~ tD (x) and brightness I'B (x), consider the probability of pixel values in areas.

4) The brightness map effectively compensates for Dark Channel when the it is incorrect and to obtain a more accurate approximation of the data. ~ TE (x)

5) If ~ tD (x) ≥ thD, the brightness is usually not as bright as the ambient light , this may result in reflection if the subject is a photo used in front of camera.

6) If I ~ B (x) ≥ US and ~ tD (x) <THD shows the local image is not in line with Dark Channel , the face clarity is usually brighter than ambient light and the transmission will be evaluated as a printed photo.

7) Therefore, the assessment of transmission should increase. In this case, the delivery map and the brightness map are very different, so we use the weighted average of both maps to get accurate map estimates. To prevent excessive values, we add the beta δ to the constant and use δ = 0.1

8) Obtain different face shapes such as eyes, nose, mouth, forehead and calculate skin likelyhood using color chromacity method.

9) Perform motion based detection to see if it is a still image or contains any movement including muscles, eyes etc.

10) Using linear regression model perform classification and obtain whether the input subject is a spoof or genuine.

(iii) Attacks and their types

Printed photo attack

In printed photo attack, I(x) is first transformed to the printed ink intensity on the paper and then to the final image intensity through diffusion reflection from the paper surface. During this transformation, G(·) and H(·) are determined by the printer frequency and chromatic fidelity. For high resolution color printer, the distortion of G(·) can be neglected, but not for H(·), since it has been reported that the color printing process usually reduces the image contrast [24]. Therefore, 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. Therefore, G(·) is determined by the frequency band width of the LCD panel, the distortion of which can be neglected. H(·) is related to the LCD color distortion and intensity transformation properties.

In addition to diffuse reflection differences, the specular reflection of the pseudo-face is also different from the genuine face caused by the pseudo-spherical surface. Because the surface of the tablet / mobile phone and the glossy ink layer on the printed paper are often reflected around the pseudo-face image [25]. While the original 3D face is reflective, it is only in the exact position. (Such as the tip of the nose, glasses, forehead, cheeks, etc.). Therefore, combining special reflections from all facial images can capture distorted images in the form of pseudo images.

There may be other distortions appearing in the face image, such as geometric distortion. (Such as paper warping) and artificial surface patterns However, dist these distortions depend on the camera and the illumination. For example, geometric distortion varies according to brightness and artificial surface patterns can only be seen with high quality cameras [26]. So we focus on four common sources of image distortion in pseudo-face images.(Specular reflection, blurry, intensity, color and variety of colors) and the corresponding feature design for face forgery detection.

For short-term spoof attacks, faces are often tricked into mobile phone cameras. The reason is forged media. (The paper printed on the screen, tablet and mobile phone screen) is usually of a limited size and the attacker must be placed near the camera to cover the boundaries of the media used to attack As a result [27], deceived faces tend not to receive focus and blurred images due to not receiving focus can be used as another queue for anti-counterfeiting.

(iv) Chromatic Moment Features

The captured face image tends to show a different color distribution compared to the color in the genuine face image. This problem is caused by incomplete color creation properties of print and display media. The deterioration of this color was explored in [28] for the detection of captured images. But did not know the effectiveness of spoof face detection since the exact color distribution depends on the brightness and the variety of the camera, we propose to invent unchangeable features to detect unusual colors in the face that are spoofed. That is, first, we convert the normal face image from the RGB area to the HSV area (Hue, Saturation and Value). Then calculate the mean, deviation and skewness of each channel as a color feature. Since these three properties are equivalent to three statistical periods in each channel, so-called color-time properties In addition to these three features, the percentage of pixels in the smallest and highest histogram of each channel is also used as two additional features.

(v) Color Diversity Features

Another important difference between genuine faces and fake faces is the variety of colors. In particular, genuine faces tend to have more colors. This variety tends to fade away in the face that falsifies due to loss of color reproduction during image / video reception. In this article, we follow the method used in [29] to measure the variety of colors of images. First, measure the color (with 32 steps in the red, green and blue channels respectively) in normal face images. Two measurements are combined from the color distribution: i) Histograms count the number of colors that appear most frequently, the top 100, and ii) the number of different colors that appear in normal face images.

(vi) Classification

We propose to use the ensemble classifier model by training multiple spoof classifiers in different groups of spoof attack examples. For specific counterfeiting databases, we create separate training samples as follows: First, counterfeiting examples are divided into K groups based on attack types. Secondly, the specific training set was created by combining all genuine samples and one group of counterfeiting examples resulting in the K training set. In our experiments, we found that by training the [29] two classifiers (K = 2) For two separate groups of attacks, such as typing attacks and repeated attacks, band selection is better than training a single classifier on all databases.

In the testing phase of the vector, the input feature will be entered into all component classifiers and the results will be combined to achieve the final result. We have evaluated two types of fusion grades: rules, sums and minimum rules.

Multi-frame fusion because the face detection counterfeit classifier works on a single image, thus offering a multi-frame fusion format to achieve a more stable face-to-face detection performance for video. The results of the classification of each frame are combined by means of voting to obtain counterfeit detection scores for the video. Face video is set to genuine if more than 50% frames are classified as genuine face pictures. Due to some published methods for video counterfeit detection performance using N frames, the expansion of multi-frame fusion allows us to compare the performance of the proposed method with modern video, which gives the same length in Test video [30].

The major drawback of these three counterfeit databases is that all are recorded by high quality web cameras or digital cameras. There is no public domain forgery database using a mobile phone camera as a capture device. The front camera of the mobile phone has the following additional challenges for face forgery detection: i) They tend to have lower resolution, narrow dynamic range and incorrect metering capabilities and autofocus. Therefore, videos or images shot with these cameras are usually of low quality due to blur. Due to the deterioration of the quality of these images, both in the face of genuine faces and counterfeits, they will reduce the difference between genuine and fake face images in terms of face details and image distortion Mobile phone counterfeiting database not only makes the face detection function more difficult But to simulate the real situation better, such as the face unlocking application on the Android smartphone using the front camera

(vii) Cross-database Spoof Detection

In addition to the performance of internal databases, we are interested in cross-database performance of different face counterfeiting detection methods. Since the IDA feature does not have any face characteristics, they are expected to have the ability to generalize across the database better than the surface feature. In this experiment, we compare the performance across databases of different properties using three pseudo databases (Idiap, CASIA and MSU). Evaluate the performance of the data groups across two groups: Idiap-vs-MSU and vice versa. And CASIA (H) -vs-MSU and vice versa As we mentioned in the second section, these three databases are short distance spoofing databases, but are captured with very different cameras.

IV. CONCLUSION

In this article, we solved the problem of face forgery detection, especially in cross-database situations. While most published methods use motion or surface features, we propose to detect face forgery using image distortion analysis (IDA). Four types of IDA features (special reflectivity, diffraction Blur, time, color and variety of colors) are designed to capture image distortion in the face of a spoofed image. The four different features are concatenated together, resulting in a 121-dimensional IDA feature vector. The ensemble classifier consists of two components that are trained for different spoof attacks, used for the identification of true and deceived faces. We have compiled a face forgery database called MSU MFSD using two mobile devices (Android Nesus 5 and MacBook Air 13). According to our knowledge, this is the first mobile counterfeit database. A subset of this database consists of 35 subjects that will be disclosed to the public.(http://biometrics.cse.msu.edu/ pubs / database.html).

Assessment of the public domain database twice (Idiap and CASIA), including the MSU MFSD database, shows that the proposed method is better than this method. Modernity in the situation of internal database testing and higher efficiency than basic methods of cross-database situations. Our recommendations for future work in face detection include: i) Understand the characteristics and requirements of simulations, use cases for face forgery detection ii) gather large databases and agents that consider User population (age, gender, illumination in interesting use cases and iii) develop strong, effective and efficient features (For example, through the conversion of properties for selected use scenario scenarios and iv) consider user-specific training for counterfeit detection.

REFERENCES

[1] Di Wen, Member, IEEE, Hu Han, Member, IEEE and Anil K. Jain, Fellow, IEEE, "Face Spoof Detection with Image Distortion Analysis," in Proc. CVPR Workshops, 2012, pp. 124–129.
[2] N. Evans, T. Kinnunen, and J. Yamagishi, "Spoofing and countermeasures for automatic speaker verification," in Proc. INTERSPEECH, 2013, pp. 925–929.
[3] L. Best-Rowden, H. Han, C. Otto, B. Klare, and A. K. Jain, "Unconstrained face recognition: Identifying a person of interest from a media collection," IEEE Trans. Inf. Forensics Security, vol. 9, no. 12, pp. 2144– 2157, Dec 2014.
[4] 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.
[5] 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.
[6] Z. Zhang, D. Yi, Z. Lei, and S. Z. Li, "Face liveness detection by learning multispectral reflectance distributions," in Proc. FG, 2011, pp. 436–441.
[7] A. Anjos and S. Marcel, "Counter-measures to photo attacks in face recognition: A public database and a baseline," in Proc. IJCB, 2011, pp. 1–7.
[8] X. Tan, Y. Li, J. Liu, and L. Jiang, "Face liveness detection from a single image with sparse low rank bilinear discriminative model," in Proc. ECCV, 2010, pp. 504–517.
[9] 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.
[10] L. Sun, G. Pan, Z. Wu, and S. Lao, "Blinking-based live face detection using conditional random fields," in Proc. AIB, 2007, pp. 252–260.
[11] W. Bao, H. Li, N. Li, and W. Jiang, "A liveness detection method for face recognition based on optical flow field," in Proc. IASP, 2009, pp. 233–236.
[12] 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.
[13] J. Li, Y. Wang, T. Tan, and A. K. Jain, "Live face detection based on the analysis of fourier spectra," in Proc. SPIE: Biometric Technology for Human Identification, 2004, pp. 296–303.
[14] "The TABULA RASA project." [Online]. Available: http://www. tabularasa-euproject.org/
[15] K. Kollreider, H. Fronthaler, M. I. Faraj, and J. Bigun, "Real-time face detection and motion analysis with application in "liveness" assessment," IEEE Trans. Inf. Forensics Security, vol. 2, no. 3, pp. 548–558, 2007.
[16] 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.
[17] T. de Freitas Pereira, A. Anjos, J. De Martino, and S. Marcel, "Can face anti-spoofing countermeasures work in a real world scenario?" in Proc. ICB, 2013, pp. 1–8.
[18] J. Yang and S. Z. Li, "Face Liveness Detection with Component Dependent Descriptor," in Proc. IJCB, pp. 1–6, 2013.
[19] T. Wang and S. Z. Li, "Face Liveness Detection Using 3D Structure Recovered from a Single Camera," in Proc. IJCB, 2013, pp. 1–6.
[20] J. Komulainen, A. Hadid, and M. Pietikainen, "Context based Face Anti- ¨ Spoofing," in Proc. BTAS, 2013, pp. 1–8.
[21] G. Chetty, "Biometric liveness checking using multimodal fuzzy fusion," in Proc. IEEE FUZZ, 2010, pp. 1–8.
[22] J. Galbally, S. Marcel, and J. Fierrez, "Image quality assessment for fake biometric detection: Application to iris, fingerprint, and face recognition," IEEE Trans. Image Process., vol. 23, no. 2, pp. 710–724, 2014.
[23] H.-Y. Wu, M. Rubinstein, E. Shih, J. Guttag, F. Durand, and W. T. Freeman, "Eulerian video magnification for revealing subtle changes in the world," ACM Trans. on Graphics, vol. 31, no. 4, 2012.
[24] S. A. Shafer, "Using color to separate reflection components," Color Research and Application, vol. 10, no. 4, pp. 210–218, 1985.
[25] O. Bimber and D. Iwai, "Superimposing dynamic range," in Proc. ACM SIGGRAPH Asia, no. 150, 2008, pp. 1–8.
[26] Pittsburgh Pattern Recognition (PittPatt), PittPatt Software Developer Kit (acquired by Google), http://www.pittpatt.com/.
[27] Q. Yang, S. Wang, and N. Ahuja, "Real-time specular highlight removal using bilateral filtering," in Proc. ECCV, 2010, pp. 87–100.

[28] 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.
[29] 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.
[30] 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.