Image-Based Object Spoofing Detection

Valter Costa[1,2](✉), Armando Sousa[1,3], and Ana Reis[1,2]

[1] FEUP - Faculty of Engineering of the University of Porto,
Rua Dr. Roberto Frias s/n Porto, Porto, Portugal
ee09115@gmail.com

[2] INEGI - Institute of Science and Innovation in Mechanical and Industrial Engineering, Campus da FEUP, Rua Dr. Roberto Frias 400 Porto, Porto, Portugal

[3] INESC TEC - INESC Technology and Science (formerly INESC Porto), Campus da FEUP, Rua Dr. Roberto Frias Edifício I, Porto, Portugal

Abstract. Using 2D images in authentication systems raises the question of spoof attacks: is it possible to deceive an authentication system using fake models possessing identical visual properties of the genuine one? In this work, an anti-spoofing method approach for a wine anti-counterfeiting system is presented. The proposed method relies in two different color spaces: CIE L*u*v* and YC_rC_b, to distinguish between a genuine instance and a spoof attack. To evaluate the proposed strategy, two databases were used: a private database, with photos/2D attacks of cork stoppers, created for this work; and the public Replay-Attack database that is used for face spoofing detection methods testing. The results on the private database show that the anti-spoofing approach is able to distinguish with high accuracy a real photo from an attack. Regarding the public database, the results were obtained with existing methods, as the best HTER results using a single frame approach.

Keywords: Replay-attack database · Cork-Print-Attack Database
Spoofing detection · Face spoofing detection · Object spoofing detection

1 Introduction

In biometric-based authentication systems, the challenge of discriminating between a genuine subject and a spoof attack has been a hard task to tackle. Face recognition systems are an example of a biometric-based authentication systems vulnerable to spoof attacks. In this context, two types of attacks can be identified: (i) 2D attacks, including print and videos attacks characterized by the use of a printed photo or a recorded video from an authorized person; (ii) 3D attacks, described by the usage of a mask from an authorized person. This work focuses on the detection of 2D spoofing attacks for a different application. An image-based wine anti-counterfeiting system has been proposed in previous work [16]. In that work, each wine bottle is individually recognized using a photo of the cork stopper. As in face recognition systems, a problem of circumventing

R. P. Barneva et al. (Eds.): IWCIA 2018, LNCS 11255, pp. 189–201, 2018.
https://doi.org/10.1007/978-3-030-05288-1_15

the authentication system using a fake replica possessing identical visual features arises. To overcome this issue, an anti-spoofing approach based on color space transformations (YC_rC_b and CIE L*u*v*) is proposed. The anti-spoofing method was tested in a private database – Cork-Print-Attack database – built in the context of this work. This database includes photos of cork stoppers and photos of printed images of cork stoppers. To test the generalization of the proposed method for spoofing detection and be able to compare the results with other researchers' works, a public database named Replay-Attack [13] from Idiap Research Institute was used. This database comprises over 1300 video clips of photo/video attacks and real access for face spoofing detection. In order to perform a fair comparison with other works on the public database, only static methods were considered (a detailed explanation defining a static method can be found in Sect. 4). The main contributions of this work are:

- Proposing a 2D spoofing detection strategy for a wine anti-counterfeiting system;
- Finding that CIE L*u*v* color space provides valuable information for spoofing detection (to the best knowledge of the authors, this is the first work that uses this conversion in the context of spoofing detection);
- Achieving a HTER of 0.59% in the Replay-Attack database, which is the best reported result using a static approach.

The remainder of this paper is organized as follows: background work is presented in Sect. 2; Sect. 3 details the proposed approach for spoofing detection; the results and discussion are shown in Sect. 4; finally, Sect. 5 draws the conclusions for this work.

2 Related Work

Since no references were found regarding object spoofing detection, this section presents some works for face spoofing detection using a single frame approach. The methods considered in this review are based on generic features (non specific characteristics of the face). To identify a spoof attack, some researchers [13,15,20,33] have used LBP – Local Binary Patterns – by assuming that the texture a 2D spoof attack is different from a real attempt. Other approach is the usage of different color space/models. Some methods successfully tested on public databases can be found in [10–12,31]. A different approach is the evaluation of the image quality, referenced in the literature as image quality measures. Galbally and Marcel proposed a face anti-spoofing method, by combining 14 different image quality measures [23]. Wen et al. used specular reflection, blurriness, chromatic moment and color diversity to distinguish a real access from a spoof attack [17]. Alotaibi and Mahmood used a non-linear diffusion method based on anisotropic diffusion to identify an attack attempt [3]. In the context of face spoofing detection, several strategies have been proposed. Regarding object spoofing detection, no references were found. In the next section, a method for object spoofing detection is presented.

3 Proposed Approach

This work focuses on the problem of detecting a printed attack of a previously registered cork in the RIOTA recognition system [16], analogous to face spoofing attacks in face recognition systems (e.g., circumvention of face recognition systems using attacks with printed or video materials of authorized persons). As mentioned in the related work, several researchers have used color-based approaches for face spoofing detection. In spite of the RGB color space being the most used in video acquisition and display devices, according to Li et al. [31], it is not the most suitable color space to detect spoofing attacks, due to the correlation between red, green and blue that obstruct the separation between the luminance and chrominance information. The anti-spoofing scheme proposed in this work takes advantage of the use of two different color spaces: YC_rC_b and CIE L*u*v*, see Fig. 1. For each input frame or image in the RGB color space, a conversion to YC_rC_b and CIE L*u*v* is made. Then, 6 histograms are calculated, corresponding to each component of these two color spaces. Next, the six histograms are concatenated into a Feature Vector $FV = (Y, C_r, C_b, L, u, v)$ of size 1536 (six normalized histograms in the range of 0–255) that serve as input for the Extra Trees Classifier - ETC. Finally, the classifier decides if the input feature vector corresponds to an image of a genuine sample or it is a spoofing attack.

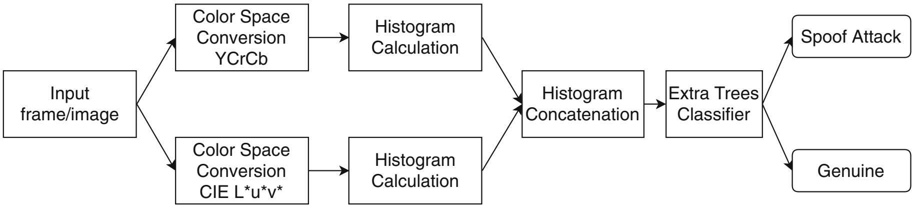

Fig. 1. Flowchart of the proposed anti-spoofing scheme.

The proposed approach is based on the idea that since two images of the same object (one of the real object and another of an attack; see Fig. 2) have different visual features, this information may be represented through its corresponding color histograms. Other works [11,12,22,31,35] demonstrated the effectiveness of combining different color spaces followed by a texture descriptor to detect a face spoof attack. In this work, only the histograms of YC_rC_b and CIE L*u*v* color spaces are used to train a classifier and identify an image spoof attack. The concept of this approach came from observing some regular distinctions in the YC_rC_b and CIE L*u*v* color histograms between two images (an image of a genuine sample and a printed attack) from the same cork stopper, as shown in Fig. 3. It can be seen that the luminance information in both color spaces has almost "regular shape"in the genuine photos (which does not happen in the print attack images); regarding the chrominance histograms, the "regular shape"

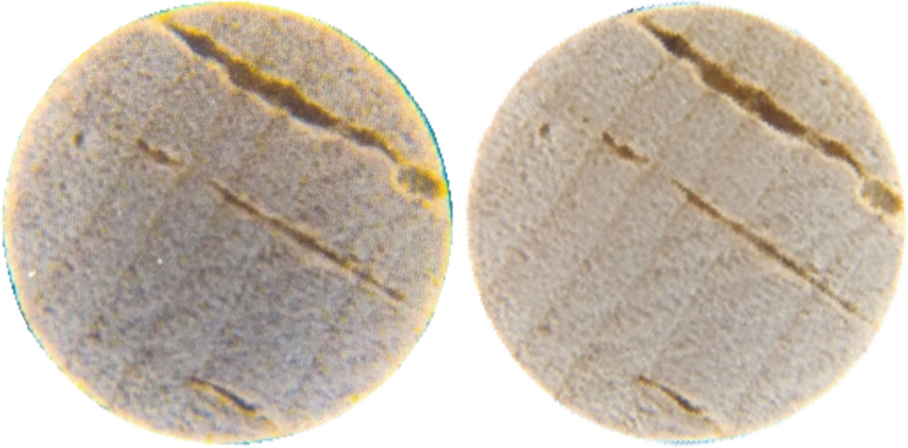

Fig. 2. Images of cork stopper examples: (left) an image of a printed cork stopper; (right) an image of a genuine cork stopper.

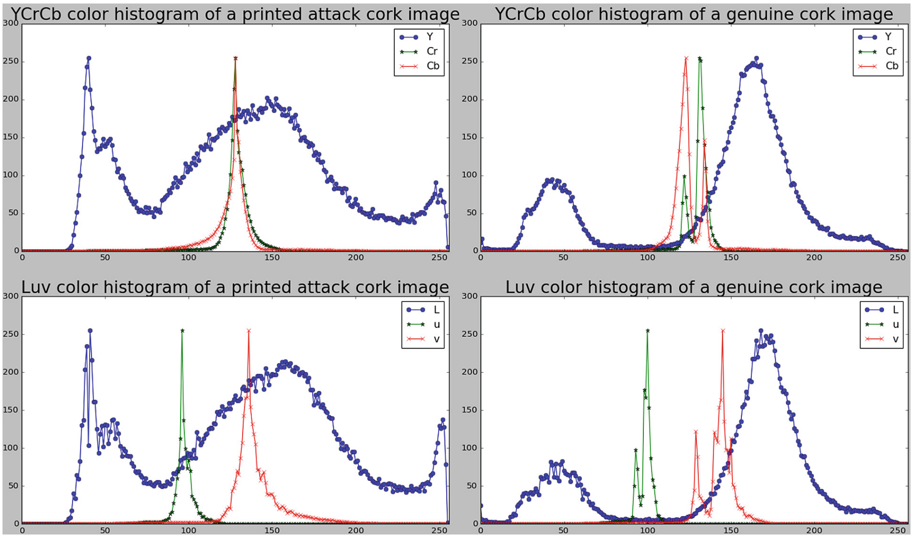

Fig. 3. YC_rC_b and CIE L*u*v* color histograms for two images of the same cork stopper: (left) column histograms of a printed attack cork image; (right) column histograms of a genuine cork image.

appears in the images from the print attacks. This behavior was detected in some pair image samples, which formulated the hypothesis of this work: is there enough information in the YC_rC_b and CIE L*u*v* color histograms to train a classifier to distinguish between an image of a genuine cork and a printed attack?

3.1 L*u*v* Color Space

The CIE L*u*v* color space was introduced by the International Commission on Illumination (also known as CIE from its French title, the Commission Internationale de l'Eclairage) in 1976 [9]. The RGB conversion to CIE L*u*v* is described in Eqs. (1), (2) and (3). Equations (4), (5) and (6) are intermediate steps and normalizations needed for this color space conversion.

$$L \leftarrow \begin{cases} 116 * \sqrt[3]{Y} & for \quad Y > 0.008856 \\ 903.3 * Y & for \quad Y \leq 0.008856 \end{cases} \tag{1}$$

$$u \leftarrow 13 \times L \times (u' - u_n) \quad where \quad u_n = 0.19793943 \tag{2}$$

$$v \leftarrow 13 \times L \times (v' - v_n) \quad where \quad v_n = 0.46831096 \tag{3}$$

$$u' \leftarrow 4 \times \frac{X}{X + 15 \times Y + 3 \times Z} \tag{4}$$

$$v' \leftarrow 9 \times \frac{X}{X + 15 \times Y + 3 \times Z} \tag{5}$$

$$\begin{bmatrix} X \\ Y \\ Z \end{bmatrix} \leftarrow \begin{bmatrix} 0.412453\ 0.357580\ 0.180423 \\ 0.212671\ 0.715160\ 0.072169 \\ 0.019334\ 0.119193\ 0.950227 \end{bmatrix} \cdot \begin{bmatrix} R \\ G \\ B \end{bmatrix} \tag{6}$$

To convert the L, u and v in a 8-bit image, these components need to be normalized. As such, $L \leftarrow 255 \times L/100$, $u \leftarrow 255/(354 \times (u + 134))$ and $v \leftarrow 255/(262 \times (v + 140))$.

3.2 YC_rC_b Color Space

This model is mostly used in compression for TV transmission and was defined by ITU - International Telecommunication Union in ITU-R BT.601 standard [27]. Y corresponds to the luminance or luma component obtained from RGB after gamma correction, C_r signifies how far the red component is from luma and C_b denotes how far the blue component is from luma.

$$Y \leftarrow 0.299 \times R + 0.587 \times G + 0.114 \times B \tag{7}$$

$$C_r \leftarrow (R - Y) \times 0.713 + \delta \tag{8}$$

$$C_b \leftarrow (B - Y) \times 0.564 + \delta \tag{9}$$

For 8-bit image representation $\delta = 128$.

To facilitate the development process[1], two public libraries were used: OpenCV[2] and scikit-learn[3] [39].

4 Performance Evaluation

The evaluation of the proposed anti-spoofing method is reported in this section. First, it presents the metrics used for the evaluation. Then, it gives details about the databases used in the tests. Next, it presents the results and compares the work with other researchers' works found in the literature. Finally, it discusses the results obtained.

4.1 Evaluation Metrics

The evaluation metric used in this work is the HTER - Half Total Error Rate [4], see Eq. (10). HTER is the mean value between the FAR - False Acceptance Rate, Eq. (11) and FRR - False Rejection Rate, Eq. (12). The effectiveness of an attack is measured by FAR. Analogously, FRR relates to the measure of a system to reject genuine instances.

$$HTER(\%) = \frac{FAR + FRR}{2} * 100 \tag{10}$$

$$FAR = \frac{FP}{FP + TN} \tag{11}$$

$$FRR = \frac{FN}{TP + FN} \tag{12}$$

In an ideal spoofing detection system, both FAR and FRR should be 0. Another metric commonly used to evaluate a biometric system is the EER - Equal Error Rate. This error rate is obtained at the threshold that provides the same FAR and FRR.

4.2 Cork-Print-Attack Database

The Cork-Print-Attack database was conceived to test and gauge the anti-spoofing method proposed in this work. It comprises 2200 photos from 200 cork stoppers, see Table 1. The photos were captured using 4 different smartphone rear cameras. Two types of paper were used to reproduce the visual aspect of a cork stopper: (i) photo paper, and (ii) printer paper. Two different printers were also used. The printed attacks have the correct correspondence in the genuine set and were printed at the same scale of the genuine sample. The diameter of the corks used ranges from 19 mm to 23.5 mm.

[1] The source code of this work is available at: https://github.com/ee09115/spoofing_detection.

[2] https://opencv.org/.

[3] http://scikit-learn.org/stable/index.html.

Table 1. Cork-print-attack database characterization.

Genuine			Print		
ID	#Photos	Camera	ID	#Photos	Camera
④	300	Xperia Z1 compact	①	300	Xperia Z3 compact
⑤	200	Xperia Z1 compact	②	300	Xperia Z3 compact
⑥	200	Xperia SP	③	300	Xperia Z1 compact
⑦	300	Asus Zenfone 2	⑧	100	Asus Zenfone 2
⑨	100	Asus Zenfone 2	⑩	100	Xperia Z3 compact

Table 2. Photos division of the cork-print-attack database into three distinct folds: training set, development set and testing set.

Train		Devel		Test	
#Photos	ID	#Photos	ID	#Photos	ID
200	①	100	①	100	⑨
200	②	100	②	100	⑩
200	③	100	③	-	-
200	④	100	④	-	-
100	⑤	100	⑤	-	-
100	⑥	100	⑥	-	-
200	⑦	100	⑦	-	-
-	-	100	⑧	-	-

The 2200 photos were divided in three different folds: training set, development set and testing set. The distribution of the photos is shown in Table 2. The corks stoppers used in the training and developments folds are not present in the testing set (in other words, there are no overlapping photos between the training/development sets and the test set).

4.3 Replay-Attack Database

The Replay-Attack database[4] consists of 1300 video clips of photo and video attacks recorded under different lightning conditions of 50 clients [13]. These clips are divided in four different folds: (i) training set – comprising 60 videos of real-accesses and 300 video attacks; (ii) development set – containing 60 videos of real-accesses and 300 attack videos; (iii) testing set – consisting of 80 videos of real-accesses and 400 attack videos; and (iv) enrollment set – including 100 videos of real-accesses. According to the protocol defined for this database, the train set is used to train the classifier, the development set is used to calibrate

[4] https://www.idiap.ch/dataset/replayattack.

the threshold (at the EER – Equal Error Rate point), and the testing set should be used to report the results of the proposed anti-spoofing approach.

4.4 Results

This subsection presents the results achieved exploring the private and public database. Table 3 presents the results obtained exploring the Cork-Print-Attack database.

Table 3. HTER on Cork-Print-Attack database.

Cork-print-attack database results		
Method	EER(%) Dev	HTER (%) Test
Proposed approach: YC_rC_b+Luv+ETC	1.5	**2.5**

The results reached with the Replay-Attack database are exhibited in Table 4.

The authors would like to clarify that the HTER results in Table 4 only refer to static methods (i.e., methods using only a single image to detect spoof attack). When comparing to methods based on liveness detection and/or the use of time windows, there are some methods yielding better results than the proposed approach, like in [21,24,34,45,46] and some works achieving worse HTER results, such as in [7,8,22,26,30,37,38,42,51]. Naturally, these kind of methods cannot be applied in the cork-print-attack database because cork is a non-living organism and all the information available is a single image.

4.5 Discussion

The results presented in Table 3 suggest that the proposed cork spoofing detection approach is adequate for the wine anti-counterfeiting system. The tests on the private database were performed without embedding the spoofing detection approach in the wine anti-counterfeiting system. Since the wine authentication system relies on the match of local feature descriptors and not all of the print attacks are recognized as genuine, when incorporating this method in the wine authentication system, the FAR will most likely decrease. As such, the overall HTER will probably drop as well.

Regarding the Replay-Attack database, the results demonstrate that the combination of YC_rC_b and CIE L*u*v* is capable of challenging the state-of-art methods specifically designed for face spoofing detection. To enhance the performance, a texture descriptor may be used after the color space conversion. Some authors have exposed the gains of using a texture descriptor as in [11,12,22,31,35].

Table 4. HTER on Replay-Attack database.

Replay-attack database results		
Method	EER(%)	HTER (%)
	Dev	Test
Radiometric transforms [19]	-	0.8
DEND-CLUSTERING-ensemble [1]	-	5.0
MAXDIST-ensemble [1]	-	5.0
CTMF [50]	-	4.4
Unicamp [14]	9.83	15.62
ATVS [14]	0.83	12.00
MUVIS [14]	0.00	1.25
PRA Lab [14]	0.00	1.25
Client specific MsLBP [28]	-	1.45
Client specific HOG [28]	-	3.58
Client specific LBP-TOP+SVM [15]	-	3.95
LBP+SVM [33]	-	13.87
LBP_{3x3}^{u2}+SVM [13]	14.84	15.16
HSV-YC_bC_r+C-SURF+PCA [10]	0.1	2.2
IQA+LDA [23]	-	15.2
CNN [2]	-	10
CNN [36]	-	0.75
CNN [25]	-	4.74
Radiometric transforms [18]	-	2.75
Kernel fusion (MBSIF-TOP+MLPQ-TOP) [5]	1.67	1.00
DPCNN [32]	-	4.3
LBP+DoG+HOG+IQA [20]	1.6	1.0
Multiscale (HSV+YC_bC_r)+SVM [12]	-	3.1
LSP+SVM [49]	13.72	12.50
IDA+SVM [17]	-	7.41
HSV+YC_bC_r+SVM [11]	-	2.8
YC_bC_r+HSV+SVM [31]	-	2.9
Non-linear Diffusion+CNN [3]	-	10
LBP + GS-LBP [41]	0.17	3.13
Color texture CNN + SVM [51]	0.1	0.9
CTMF [50]	4.0	4.4
CNN [6]	0.79	0.72
FDL-270 [44]	5.92	5.21
Skin blood flow + SVM [48]	-	4.92
FASNet [29]	-	1.2
ResNet-50[47]	1.16	1.28
GIF + IQA [40]	1.02	1.31
LiveNet [43]	7.68	5.74
Proposed approach: YC_rC_b+Luv+ETC	0.074	**0.59**

5 Conclusions

This work presented an anti-spoofing method based on two different color space transforms and histograms calculation using a single image for a wine anti-counterfeiting system. The results showed that the combination of YC_rC_b and CIE L*u*v have proved to be a reliable choice for cork spoofing detection. To test how good the proposed method can generalize, a public database named Replay-Attack database was used. The results achieved on the public database are able to compete with the state-of-art results. Moreover, using a single image/frame approach the reported HTER is the lowest found in the literature. Finally, the results confirm the hypothesis raised in this work: the combination of YC_rC_b and CIE L*u*v* color histograms provide enough discrimination for image spoofing detection applications.

Acknowledgments. Authors gratefully acknowledge the funding of Project NORTE-01-0145-FEDER-000022 - SciTech - Science and Technology for Competitive and Sustainable Industries, co-financed by Programa Operacional Regional do Norte (NORTE2020), through Fundo Europeu de Desenvolvimento Regional (FEDER).

References

1. Akhtar, Z., Foresti, G.L.: Face spoof attack recognition using discriminative image patches. J. Electr. Comput. Eng. 1–14 (2016). http://www.hindawi.com/journals/jece/2016/4721849/
2. Alotaibi, A., Mahmood, A.: Enhancing computer vision to detect face spoofing attack utilizing a single frame from a replay video attack using deep learning. In: 2016 International Conference on Optoelectronics and Image Processing (ICOIP), pp. 1–5. IEEE (2016). http://ieeexplore.ieee.org/document/7528488/
3. Alotaibi, A., Mahmood, A.: Deep face liveness detection based on nonlinear diffusion using convolution neural network. Signal Image Video Process. **11**(4), 713–720 (2017). https://doi.org/10.1007/s11760-016-1014-2
4. Anjos, A., Marcel, S.: Counter-measures to photo attacks in face recognition: a public database and a baseline. In: 2011 International Joint Conference on Biometrics (IJCB), pp. 1–7. IEEE (2011). http://ieeexplore.ieee.org/document/6117503/
5. Arashloo, S.R., Kittler, J., Christmas, W.: Face spoofing detection based on multiple descriptor fusion using multiscale dynamic binarized statistical image features. IEEE Trans. Inf. Forensics Secur. **10**(11), 2396–2407 (2015). http://ieeexplore.ieee.org/document/7163625/
6. Atoum, Y., Liu, Y., Jourabloo, A., Liu, X.: Face anti-spoofing using patch and depth-based CNNs. In: 2017 IEEE International Joint Conference on Biometrics (IJCB), pp. 319–328. IEEE (2017). http://ieeexplore.ieee.org/document/8272713/
7. Benlamoudi, A., Aiadi, K.E., Ouafi, A., Samai, D., Oussalah, M.: Face antispoofing based on frame difference and multilevel representation. J. Electron. Imaging **26**(4), 043007 (2017). https://doi.org/10.1117/1.JEI.26.4.043007
8. Bharadwaj, S., Dhamecha, T.I., Vatsa, M., Singh, R.: Computationally efficient face spoofing detection with motion magnification. In: 2013 IEEE Conference on Computer Vision and Pattern Recognition Workshops, pp. 105–110. IEEE (2013). http://ieeexplore.ieee.org/document/6595861/

9. Billmeyer, F.W.: Color Science: Concepts and Methods, Quantitative Data and Formulae, 2nd ed., by Gunter Wyszecki and W. S. Stiles, John Wiley and Sons, New York, 1982, 950 pp. Price: $75.00. Color Res. Appl. **8**(4), 262–263 (1983). https://doi.org/10.1002/col.5080080421
10. Boulkenafet, Z., Komulainen, J., Hadid, A.: Face anti-spoofing using speeded-up robust features and fisher vector encoding. IEEE Signal Process. Lett. 1 (2016). http://ieeexplore.ieee.org/document/7748511/
11. Boulkenafet, Z., Komulainen, J., Hadid, A.: Face spoofing detection using colour texture analysis. IEEE Trans. Inf. Forensics Secur. **11**(8), 1818–1830 (2016). http://ieeexplore.ieee.org/document/7454730/
12. Boulkenafet, Z., Komulainen, J., Xiaoyi Feng, Hadid, A.: Scale space texture analysis for face anti-spoofing. In: 2016 International Conference on Biometrics (ICB), pp. 1–6. IEEE (2016). http://ieeexplore.ieee.org/document/7550078/
13. Chingovska, I., Anjos, A., Marcel, S.: On the effectiveness of local binary patterns in face anti-spoofing. In: 2012 BIOSIG - Proceedings of the International Conference of Biometrics Special Interest Group (BIOSIG), pp. 1–7 (2012)
14. Chingovska, I., et al.: The 2nd competition on counter measures to 2D face spoofing attacks. In: 2013 International Conference on Biometrics (ICB), pp. 1–6. IEEE (2013). http://ieeexplore.ieee.org/document/6613026/
15. Chingovska, I., dos Anjos, A.R.: On the use of client identity information for face antispoofing. IEEE Trans. Inf. Forensics Secur. **10**(4), 787–796 (2015). http://ieeexplore.ieee.org/document/7031941/
16. Costa, V., Sousa, A., Reis, A.: Preventing wine counterfeiting by individual cork stopper recognition using image processing technologies. J. Imaging **4**(4), 54 (2018). http://www.mdpi.com/2313-433X/4/4/54
17. Wen, D., Han, H., Jain, A.K.: Face spoof detection with image distortion analysis. IEEE Trans. Inf. Forensics Secur. **10**(4), 746–761 (2015). http://ieeexplore.ieee.org/document/7031384/
18. Edmunds, T., Caplier, A.: Fake face detection based on radiometric distortions. In: 2016 Sixth International Conference on Image Processing Theory, Tools and Applications (IPTA), pp. 1–6. IEEE (2016). http://ieeexplore.ieee.org/document/7820995/
19. Edmunds, T., Caplier, A.: Face spoofing detection based on colour distortions. IET Biom. **7**(1), 27–38 (2018). http://digital-library.theiet.org/content/journals/10.1049/iet-bmt.2017.0077
20. Farmanbar, M., Toygar, Ö.: Spoof detection on face and palmprint biometrics. Signal Image Video Process. **11**(7), 1253–1260 (2017). https://doi.org/10.1007/s11760-017-1082-y
21. Feng, L., et al.: Integration of image quality and motion cues for face anti-spoofing: a neural network approach. J. Vis. Commun. Image Represent. **38**, 451–460 (2016). http://linkinghub.elsevier.com/retrieve/pii/S1047320316300244
22. de Freitas Pereira, T., et al.: Face liveness detection using dynamic texture. EURASIP J. Image Video Process. **2014**(1), 2 (2014). https://jivp-eurasipjournals.springeropen.com/articles/10.1186/1687-5281-2014-2
23. Galbally, J., Marcel, S.: Face anti-spoofing based on general image quality assessment. In: 2014 22nd International Conference on Pattern Recognition, pp. 1173–1178. IEEE (2014). http://ieeexplore.ieee.org/document/6976921/
24. Gan, J., Li, S., Zhai, Y., Liu, C.: 3D convolutional neural network based on face anti-spoofing. In: 2017 2nd International Conference on Multimedia and Image Processing (ICMIP), pp. 1–5. IEEE (2017). http://ieeexplore.ieee.org/document/8221060/

25. Gragnaniello, D., Sansone, C., Poggi, G., Verdoliva, L.: Biometric spoofing detection by a domain-aware convolutional neural network. In: 2016 12th International Conference on Signal-Image Technology and Internet-Based Systems (SITIS), pp. 193–198. IEEE (2016). http://ieeexplore.ieee.org/document/7907465/
26. Kim, I., Ahn, J.., Kim,D.: Face spoofing detection with highlight removal effect and distortions. In: 2016 IEEE International Conference on Systems, Man, and Cybernetics (SMC), pp. 004299–004304. IEEE (2016). http://ieeexplore.ieee.org/document/7844907/
27. ITU: ITU-R Recommendation BT.601-5: Studio encoding parameters of digital television for standard 4:3 and wide-screen 16:9 aspect ratios. Technical report, ITU, Geneva, Switzerland (1995)
28. Yang, J., Lei, Z., Yi, D., Li, S.Z.: Person-specific face antispoofing with subject domain adaptation. IEEE Trans. Inf. Forensics Secur. **10**(4), 797–809 (2015). http://ieeexplore.ieee.org/document/7041231/
29. Karray, F., Campilho, A., Cheriet, F. (eds.): Image Analysis and Recognition. LNCS, vol. 10317. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-59876-5
30. Komulainen, J., Hadid, A., Pietikainen, M., Anjos, A., Marcel, S.: Complementary countermeasures for detecting scenic face spoofing attacks. In: 2013 International Conference on Biometrics (ICB), pp. 1–7. IEEE (2013). http://ieeexplore.ieee.org/document/6612968/
31. Li, L., Correia, P.L., Hadid, A.: Face recognition under spoofing attacks: countermeasures and research directions. IET Biom. **7**(1), 3–14 (2018). http://digital-library.theiet.org/content/journals/10.1049/iet-bmt.2017.0089
32. Li, L., Feng, X., Boulkenafet, Z., Xia, Z., Li, M., Hadid, A.: An original face anti-spoofing approach using partial convolutional neural network. In: 2016 Sixth International Conference on Image Processing Theory, Tools and Applications (IPTA), pp. 1–6. IEEE (2016). http://ieeexplore.ieee.org/document/7821013/
33. Maatta, J., Hadid, A., Pietikainen, M.: Face spoofing detection from single images using micro-texture analysis. In: 2011 International Joint Conference on Biometrics (IJCB). pp. 1–7. IEEE (2011). http://ieeexplore.ieee.org/document/6117510/
34. Manjani, I., Tariyal, S., Vatsa, M., Singh, R., Majumdar, A.: Detecting silicone mask-based presentation attack via deep dictionary learning. IEEE Trans. Inf. Forensics Secur. **12**(7), 1713–1723 (2017). http://ieeexplore.ieee.org/document/7867821/
35. Määttä, J., Hadid, A., Pietikäinen, M.: Face spoofing detection from single images using texture and local shape analysis. IET Biom. **1**(1), 3 (2012). http://digital-library.theiet.org/content/journals/10.1049/iet-bmt.2011.0009
36. Menotti, D., et al.: Deep Representations for iris, face, and fingerprint spoofing detection. IEEE Trans. Inf. Forensics Secur. **10**(4), 864–879 (2015). http://ieeexplore.ieee.org/document/7029061/
37. Asim, M., Ming, Z., Javed, M.Y.: CNN based spatio-temporal feature extraction for face anti-spoofing. In: 2017 2nd International Conference on Image, Vision and Computing (ICIVC), pp. 234–238. IEEE (2017). http://ieeexplore.ieee.org/document/7984552/
38. Pan, S., Deravi, F.: Facial action units for presentation attack detection. In: 2017 Seventh International Conference on Emerging Security Technologies (EST), pp. 62–67. IEEE (2017). http://ieeexplore.ieee.org/document/8090400/
39. Pedregosa, F., et al.: Scikit-learn: machine learning in Python. J. Mach. Learn. Res. **12**, 2825–2830 (2011)

40. Peng, F., Qin, L., Long, M.: POSTER: non-intrusive face spoofing detection based on guided filtering and image quality analysis. In: Deng, R., Weng, J., Ren, K., Yegneswaran, V. (eds.) SecureComm 2016. LNICST, vol. 198, pp. 774–777. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-59608-2_49
41. Peng, F., Qin, L., Long, M.: Face presentation attack detection using guided scale texture. Multimed. Tools Appl. **77**(7), 8883–8909 (2018). https://doi.org/10.1007/s11042-017-4780-0
42. Pinto, A., Pedrini, H., Schwartz, W.R., Rocha, A.: Face spoofing detection through visual codebooks of spectral temporal cubes. IEEE Trans. Image Process. **24**(12), 4726–4740 (2015). http://ieeexplore.ieee.org/document/7185398/
43. Rehman, Y.A.U., Po, L.M., Liu, M.: LiveNet: Improving features generalization for face liveness detection using convolution neural networks. Expert Syst. Appl. **108**, 159–169 (2018). http://linkinghub.elsevier.com/retrieve/pii/S0957417418302811
44. Stuchi, J.A., et al.: Improving image classification with frequency domain layers for feature extraction. In: 2017 IEEE 27th International Workshop on Machine Learning for Signal Processing (MLSP), pp. 1–6. IEEE (2017). http://ieeexplore.ieee.org/document/8168168/
45. Tian, Y., Xiang, S.: Detection of video-based face spoofing using LBP and multiscale DCT. In: Shi, Y.Q., Kim, H.J., Perez-Gonzalez, F., Liu, F. (eds.) IWDW 2016. LNCS, vol. 10082, pp. 16–28. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-53465-7_2
46. Tirunagari, S., Poh, N., Windridge, D., Iorliam, A., Suki, N., Ho, A.T.S.: Detection of face spoofing using visual dynamics. IEEE Trans. Inf. Forensics Secur. **10**(4), 762–777 (2015). http://ieeexplore.ieee.org/document/7047832/
47. Tu, X., Fang, Y.: Ultra-deep neural network for face anti-spoofing. In: Liu, D., Xie, S., Li, Y., Zhao, D., El-Alfy, E.S. (eds.) Neural Information Processing, vol. 10635, pp. 686–695. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-70096-0_70
48. Wang, S.Y., Yang, S.H., Chen, Y.P., Huang, J.W.: Face liveness detection based on skin blood flow analysis. Symmetry **9**(12), 305 (2017). http://www.mdpi.com/2073-8994/9/12/305
49. Kim, W., Suh, S., Han, J.-J.: Face liveness detection from a single image via diffusion speed model. IEEE Trans. Image Process. **24**(8), 2456–2465 (2015). http://ieeexplore.ieee.org/document/7084662/
50. Zhang, L.B., Peng, F., Qin, L., Long, M.: Face spoofing detection based on color texture markov feature and support vector machine recursive feature elimination. J. Vis. Commun. Image Represent. **51**, 56–69 (2018). http://linkinghub.elsevier.com/retrieve/pii/S1047320318300014
51. Zhao, X., Lin, Y., Heikkila, J.: Dynamic texture recognition using volume local binary count patterns with an application to 2D face spoofing detection. IEEE Trans. Multimed. **20**(3), 552–566 (2018). http://ieeexplore.ieee.org/document/8030131/