2017 International Conference on Security, Pattern Analysis,
and Cybernetics (SPAC)

Face liveness detection using color gradient features

Jixiang Dong
Bio-Computing Research Center, Shenzhen,
Harbin Institute of Technology
Shenzhen, China
2499679061@qq.com

Chunwei Tian
Bio-Computing Research Center, Shenzhen,
Harbin Institute of Technology
Shenzhen, China
chunweitian@163.com

Yong Xu
Bio-Computing Research Center, Shenzhen,
Harbin Institute of Technology
Medical Biometrics Perception and Analysis
Engineering Laboratory, Shenzhen, China.
Shenzhen, China
laterfall@hit.edu.cn

***Abstract*—Face liveness detection is widely used to detect face spoofing attacks. Most existing face liveness detection methods are mainly based on texture information of face images in the gray-scale space which ignored the chrominance information and other feature differences. In this paper, we introduced a novel modified color gradient feature into face liveness detection which used variant color roberts cross operator. This method can extract the color gradient information from the live faces or fake faces so that the proposed method has potential to achieve a better performance. Extensive experimental results on benchmark databases showed that the proposed variant color-gradient feature was very effective for face liveness detection.**

Keywords* —*Face liveness detection, variant color roberts cross operator, color-gradient feature

1. INTRODUCTION

Nowadays, a lot of face recognition methods have been proposed. For example, deep learning methods such as DeepID, DeepID2 have led to improved accuracy for face recognition [1-3]. However, it is vulnerable to face spoofing attacks that only need a photograph or a video clip of the valid user. They can be easily acquired from the internet in her or his personal online community even by using a phone camera to capture his or her face images [4-5].

There are three main face spoofing attacks: photographs print attack, video replay attack and 3D mask attack [6]. To address this security risk of face recognition, face spoofing detection attracts much attention of the researchers, and they have made efforts to explore how to distinguish the live faces from the fake faces based on different ways.

Based on different characteristics used in face liveness detection, existing face liveness detection methods can be mainly categorized into three groups: motion-based methods, texture-based methods and image quality-based methods. The implementations of these methods are as follows: motion-based methods mainly used the natural responses caused by facial movements to perform face liveness detection [7-8]. For example, these methods usually detected eye-blinking, mouth movement, and head rotation which need to firstly detect the face or localize the targets [9-10]. But these methods had a disadvantage that they could not prevent modified attacks such as cropped-eye or cropped-mouth photos which existed in the CASIA face anti-spoofing database [13]. Motion-based methods also contained the approaches that utilized the differences of facial movements between the foreground and background regions [7,11]. They calculated and used the optical flow to detect the motion correlations and facial expression [8,12]. Texture-based methods [14] generally used facial texture information of a single image to detect face liveness. These methods usually used Local Binary Pattern (LBP) [15] to identify texture patterns in spatial domain of an image. Some methods also used additional devices (e.g. a near infrared sensor) to identify the live faces or fake faces based on the different responses to wavelengths of skin and non-skin materials [16]. Image quality-based methods [6, 17] usually assumed that live faces lost image information in repeated capturing of the faces under the same condition. Thus, they usually applied Fourier transform or wavelet transform to extract frequency information of a single face image [13,18]. Further, some other image quality measures such as specular reflection features and blurriness features were also used to distinguish the live faces from fake faces [6,17].

Attackers are most likely to use prints or video of faces (e.g. face images or videos on the displayed screen of a mobile phone or a Table PC) to perform face spoofing attacks. When the low-quality fake face images are used by attack attempts, it can be easily to detect by using the texture or quality information in gray-scale space. Therefore, previous studies had achieved some acceptable performance. However, they ignored the importance of chrominance information and ignored other characteristic differences such as gradient feature [4, 19]. Thus, it had difficulty to detect the fake faces with high-quality. For example, when web-cameras can capture high-quality face images, it would make the fake faces have high quality which led to increasing difficulty for distinguishing the texture and quality information of the live faces from these of fake faces in gray-scale space. Compared to fake faces showing the specular reflection, the live faces show the diffusing reflection, the changes of light vary more acutely which would make the differences of gradient values between different pixels on the live faces greater than those on fake faces. As shown in the Fig. 1, an example of the average gradient differences of several live faces and fake faces on the replay-attack database [24]. Hence, when the live faces and fake faces have a high quality, they would also have gradient differences, especially in different color spaces. This could be effective to help us identity the live faces and fake faces.

In this paper, we studied the gradient differences of live faces and fake faces (see Fig. 1) and proposed a novel variant color-gradient feature to detect face spoofing attacks by using modified color roberts cross operator [20] named variant color

978-1-5386-3016-7/17/$31.00 ©2017 IEEE

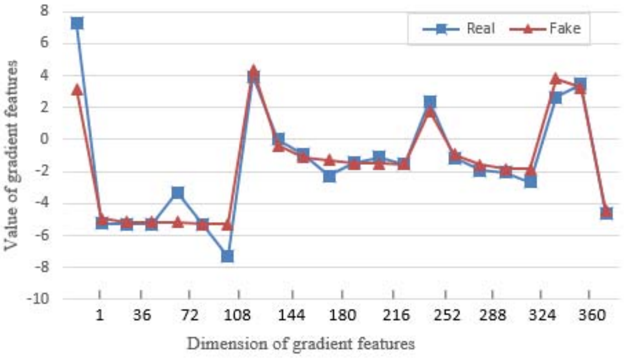


Fig.1. Illustration of gradient feature differences between live faces and fake faces

roberts cross operator (VCRCO). Experimental results on two challenging benchmark databases named CASIA face anti-spoofing and replay-attack databases showed that our proposed feature outperformed gray-scale gradient feature, especially, on the replay-attack database, our method achieved much better performance than other methods.

The remainder of this paper is organized as follows. Section 2 provides the proposed novel method. Section 3 presents results of a lot of experiments. Section 4 offers our conclusion.

2. THE PROPOSED FEATURE EXTRACTION METHOD

Inspired by the observation that the live face and fake face images have gradient differences as shown in Fig. 1. We proposed the variant color roberts cross operator to extract color gradient feature for detecting face spoofing attacks. This method extracted the joint multi-direction color-gradient information from the face images in different color spaces including HSV and YCrCb. Compared to the RGB color space, the HSV and YCrCb color space could have a perfect separation of the luminance and chrominance that could reduce the impact of the luminance for features [21].

2.1. Construction of the Feature

In this section, we extended gray-scale roberts cross operator to color variant roberts cross operator and described how to construct feature vectors based on the method proposed in this paper.

Let $R(i,j)$ be the gradient value of a pixel $x(i,j)$ in a color channel computed by variant roberts cross operator. It can be represented as follows:

$$R(i,j)=\frac{1}{4}(R^1(i,j)+R^2(i,j)+R^3(i,j)+R^4(i,j)) \tag{1}$$

where $R^1(i,j)$, $R^2(i,j)$, $R^3(i,j)$, and $R^4(i,j)$ represented the four different gradient values between diagonally adjacent pixels in different directions of pixel $x(i,j)$, which can be expressed as follows:

$$R^1(i,j)=\sqrt{(x(i,j)-x(i-1,j-1))^2+(x(i,j-1)-x(i-1,j))^2} \tag{2}$$

$$R^2(i,j)=\sqrt{(x(i,j)-x(i-1,j+1))^2+(x(i,j+1)-x(i-1,j))^2} \tag{3}$$

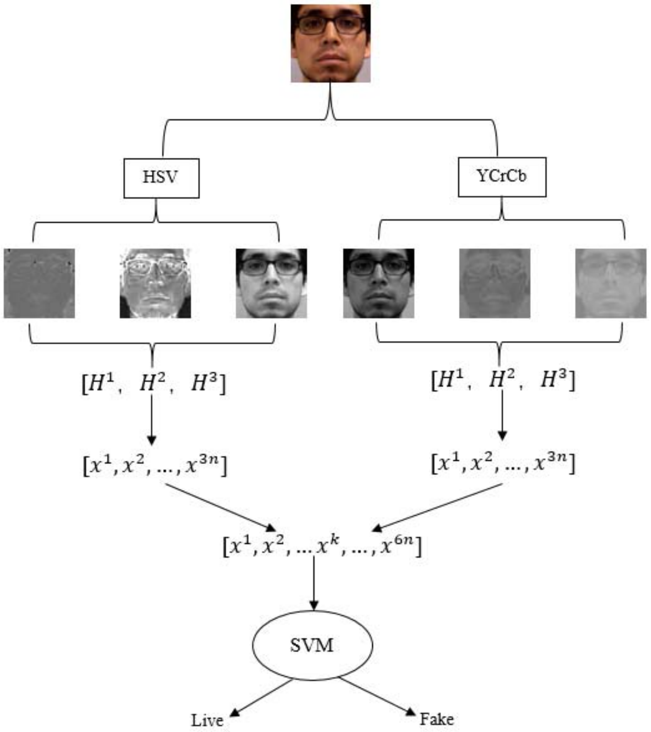

HSV
YCrCb
$[H^1,\ H^2,\ H^3]$
$[H^1,\ H^2,\ H^3]$
$[x^1, x^2, \ldots, x^{3n}]$
$[x^1, x^2, \ldots, x^{3n}]$
$[x^1, x^2, \ldots x^k, \ldots, x^{6n}]$
SVM
Live
Fake

Fig.2. The structure of the proposed method

$$R^3(i,j)=\sqrt{(x(i+1,j)-x(i,j-1))^2+(x(i+1,j-1)-x(i,j))^2} \tag{4}$$

$$R^4(i,j)=\sqrt{(x(i+1,j+1)-x(i,j))^2+(x(i+1,j)-x(i,j+1))^2} \tag{5}$$

After getting the gradient map of a face image via (1)-(5), we computed the gradient histogram H of a gradient face image by equation (6) in different color spaces:

$$H=\{H^1,\ldots,H^i,\ldots,H^c\} \tag{6}$$

where c represented different channels in color spaces, and c was equal to 6 in this paper which meant all channels in HSV and YCrCb color spaces were used.

On the basis of the above analysis, we could construct the gradient feature of a face image. Let H^i be a gradient histogram extracted from the $i-th$ channel of the color space S and S contained HSV and YCrCb color components. H^i could be defined as:

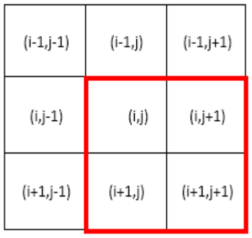
$$H^i=\{x_1^i,x_2^i,\ldots,x_n^i\} \tag{7}$$

where x_n^i represented the value of the $n-th$ dimension in the $i-th$ histogram. Each histogram had 64 dimensions, so n was equal to 64 in this paper. By concatenating all the gradient histograms defined in (6) and (7), we could represent the face images as a single gradient feature vector defined as:

$$X=\{x_1^1,x_2^1,\ldots,x_n^1,x_1^2,x_2^2,\ldots,x_n^2,x_1^6,x_2^6,\ldots,x_n^6\} \tag{8}$$

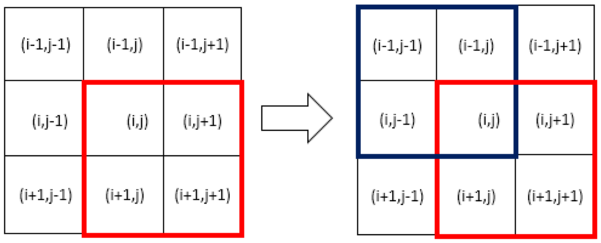
After extracting the color gradient feature, a linear SVM classifier [18] was used for classification. The flowchart of our proposed method to detect spoofing attacks was summarized in Fig. 2.

The original roberts cross operator proposed by roberts was a gray-scale gradient operator to extract gradient features. It computed the sum of the squares of the differences between



(i-1,j-1)	(i-1,j)	(i-1,j+1)
(i,j-1)	(i,j)	(i,j+1)
(i+1,j-1)	(i+1,j)	(i+1,j+1)

Fig.3. The original roberts cross operator in gray-scale space



(i-1,j-1)	(i-1,j)	(i-1,j+1)
(i,j-1)	(i,j)	(i,j+1)
(i+1,j-1)	(i+1,j)	(i+1,j+1)

(i-1,j-1)	(i-1,j)	(i-1,j+1)
(i,j-1)	(i,j)	(i,j+1)
(i+1,j-1)	(i+1,j)	(i+1,j+1)

Fig.4. The variant roberts cross operator in one channel of a color space

diagonally adjacent pixels to approximate the gradient of an image in the gray-scale space as shown in Fig. 3. However, it ignored the color information of images and only considered one direction of the pixel $x(i, j)$ ignoring the other directions that led to sever information loss. Thus, the proposed VCRCO could extract the joint color information and utilized the gradient information of the four directions of the pixel $x(i, j)$. Fig. 4 showed the variant roberts cross operator.

2.2. Summary of Main Steps

In experiments, we extracted the color-gradient features from the normalized (64*64) face images. On the training stage, we used frames of each video in the training set to extract features to train a linear SVM model. On the test stage, frames of each test video in the test set were classified. The whole process of the proposed method included the training stage and the test stage. The training stage was described as follows.

Step 1: For each sequence $\{I_k\}$in the training dataset, where k was the index of frames, all frames were transformed into H, S, V, Y, Cr, and Cb channels $\{(C_k^1, C_k^2, ..., C_k^6)\}$ where C_k^i represented the image matrix in the $i-th$ channel of the $k-th$ frame.

Step 2: Computed the gradient map of $\{(C_k^1, C_k^2, ..., C_k^6)\}$ via (1)-(5) and their gradient histogram $H = \{(H^1, ..., H^6)\}$, where H^i was the histogram of each channel defined in (7) via (6).

Step 3: Concatenated all gradient histograms to gradient feature $X = \{x_1^1, x_2^1, ..., x_n^1, x_1^2, x_2^2, ..., x_n^2, x_1^6, x_2^6, ..., x_n^6\}$ via (6)-(8).

Step 4: Trained a linear SVM model M with a soft margin where the default parameter in the LIBSVM with C++ was used for the training dataset.

On the test stage, given a test sequence $\{I_k\}$, we extracted the color gradient feature using Steps 1, 2, 3, 4 described above. The test sequence was classified as a live face or fake face by using model M according to the following rule:

$$I_k = \begin{cases} 1 & if\ f(X) \geq T \\ -1 & if\ f(X) < T \end{cases} \tag{9}$$

where 1 represented the live face and -1 represented the fake face. T was a threshold value and used to determine the face was fake or live. For the replay-attack database, the threshold T was determined on the validation set provided in database when the False Acceptance Rate (FAR) approximately equals to the False Rejection Rate (FRR). As for the CASIA-fasd database, we achieved the best average threshold T by the 5-fold cross validation on the training dataset due to the lack of validation set in database.

3. EXPERIMENT

In this part, we firstly introduced two benchmark databases. Then, we compared the performance of original roberts gradient feature in gray-scale space, original color roberts gradient feature and variant color roberts gradient feature on two benchmark databases. We fairly compared the proposed method VCRCO with the state-of-the-art methods following the defined protocols of the databases. On the CASIA-fasd database, the Equal Error Rate (EER) that defined as the point along the ROC curve where the FAR equals to the FRR was used to express the correctness of the classification on the test set. Replay-attack database recommended using the Half Total Error Rate (HTER) on the test set where HTER meant the half of the sum of the FRR and FAR.

3.1. Databases for Evaluation

For evaluating the performance of our proposed method, we used the most challenging face anti-spoofing benchmark databases named CASIA Face Anti-spoofing and replay-attack that contained the recording of real client accesses and various spoofing attack ways.

The CASIA Face anti-spoofing database (CASIA-fasd) [13] published by Chinese Academy of Sciences Center for Biometrics and Security Research contained 600 video recordings of both real-access and spoofing attack attempts recorded from 50 genuine subjects corresponding to 20 training subjects and 30 test subjects respectively. Both live face and fake face samples were acquired by using three devices with three different camera resolutions: low resolution, normal resolution and high resolution. The test set could be divided into 7 scenarios containing image quality test, fake face test and overall test: low quality, normal quality, high quality, warped photo attacks, cut photo attacks, video attacks and overall test by combining all the scenarios.

The replay-attack database [24] consisted of 1200 video clips of both real-access and attack attempts to 50 subjects. Both live faces and fake faces were recorded in two different environment conditions: controlled and adverse. In order to enrich the various image media used in attacks, a high-resolution pictures and videos were taken for each live face under the same conditions. The database contained three type of attacks: print attacks (print paper), mobile attacks (smart phone screen) and highdef attacks (tablet screen). Specially, attacks contained two different modes: fixed-support attacks (the attack devices were fixed) and hand-support attacks (the attacks devices were held by hand).

3.2. Results

We firstly presented the effectiveness of the proposed color-gradient feature. From the Fig. 5 and Fig. 6, we can see that the proposed color-gradient feature significantly improved performance compared to gradient feature in gray-scale space. When comparing the different color space, we can clearly see that the HSV-based color-gradient achieved the best overall performance. In addition, we can also observe that the variant gradient feature could have more effectiveness than original gradient feature in same color space. For example, the variant-hsv-roberts feature has the better performance than the original-hsv-roberts feature. As can be seen in Fig. 5 and Fig. 6, although, the color-gradient feature based HSV representations were more effective than features extracted from YCrCb color space for most test subsets. we can observe that the color-gradient feature at the fusion of HSV and YCrCb color spaces effectively lower the HTER and EER on test set compared to single color space.

Table 1 presented the performance evaluation of the proposed method and the state-of-the-art methods proposed in previous literatures on the test set of the benchmark databases. From Table 1, we can firstly see that the proposed method had the best performance on the challenging replay-attack database. In addition, on the challenging CASIA-fasd database, our proposed method had a competitive result and outperformed the most previous methods. Although, we could see that the performance of our proposed method was worse than that of the color-texture based method on the CASIA-fasd database, and the reason was that the most face samples of the live faces and fake faces in the CASIA-fasd database had low image quality or high similarity which led to the poor color-gradient information. Therefore, the performance of our proposed method was relatively weak in comparison with the color-texture method.

In order to gain insight into the effectiveness of color features and gradient features, we conducted some other evaluation. In the experiments, we evaluated the performance on benchmark databases using the color features, gradient features and original color-gradient features, respectively. Table 1 indicated that color-gradient features obtained a significant performance enhancement and the variant color-gradient feature could further improve the performance.

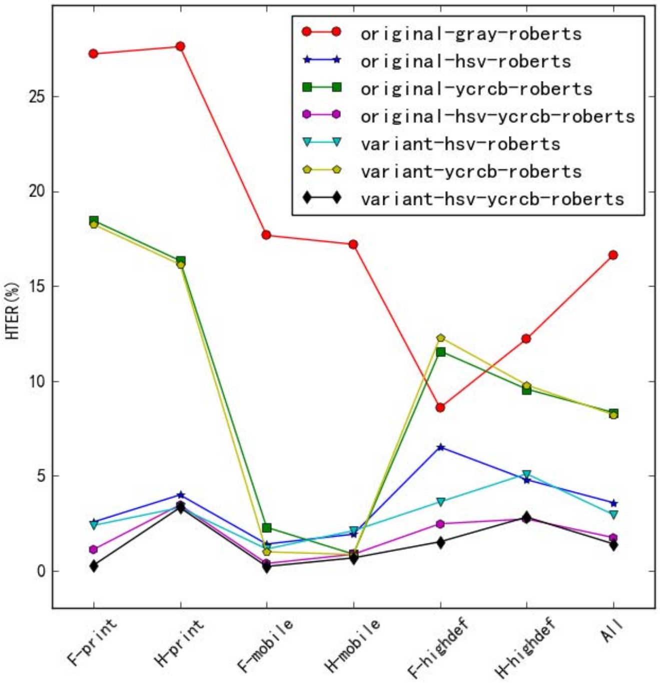


Fig.5. the performance of different features on the test set of replay-attack database

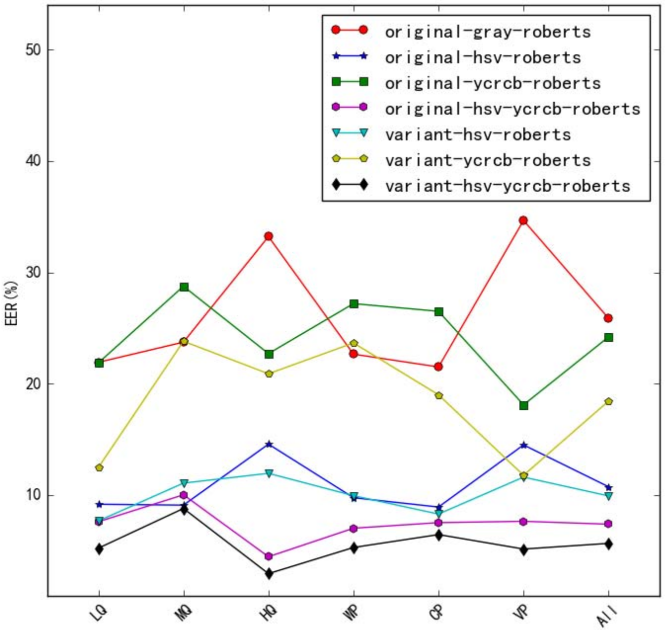


Fig.6. the performance of different features on the test set of CASIA-fasd database

4. CONCLUSION

In this paper, we proposed a novel variant color-gradient feature to approach the problem of face liveness detection by extracting the color gradient information from the face images. We investigated the effectiveness of color gradient feature and also showed that the variant color multi-direction roberts cross operator could extract rich color-gradient information from face images in different color spaces which had better performance than the original gradient feature. Extensive experimental results on challenging face anti-spoofing databases showed that the proposed VCRCO achieved excellent performance. Especially, the VCRCO had the best results than the state-of-the-art-methods on replay-attack database.

TABLE 1. The performance comparison between the proposed method and state-of-the-art methods on the test set of the benchmark databases

Method	replay-attack	CASIA-fasd
	HTER	EER
Motion [25，30]	11.70	26.60
LBP [24]	13.87	18.21
CDD [26]	-	11.80
LBP-TOP [27]	7.60	10.00
IQA [17]	15.20	32.40
IDA [6]	7.41	12.90
DMD [28]	3.75	21.75
Spectral cubes [29]	2.75	14.00
Color-LBP [22]	2.90	6.20
Color-texture [4]	2.80	**2.10**
original-gray- roberts	16.62	26.32
hsv-ycrcb	6.93	14.79
original-hsv-ycrcb- roberts	1.83	7.52
The proposed method	**1.41**	5.68

ACKNOWLEDGEMENT

This paper is partially supported by Guangdong Province high-level personnel of special support program (No. 2016TX03X164) and supported by National Natural Science Foundation of China (No. 61332011).

REFERENCES

[1] Y. Sun, X. Wang, and X. Tang, "Deep learning face representation from predicting 10,000 classes," in IEEE Conference on Computer Vision and Pattern Recognition, pp. 1891–1898, 2014.

[2] Y. Sun, X. Wang, and X. Tang, "Deep learning face representation by joint identification-verification," vol. 27, pp. 1988–1996, 2014.

[3] K. Guo, S.Wu, and Y. Xu, "Face recognition using both visible light image and near-infrared image and a deep network," Caai Transactions on Intelligence Technology, vol. 2, no. 1,pp. 39–47, 2017.

[4] Z. Boulkenafet, J. Komulainen, and A. Hadid, "Face spoofing detection using colour texture analysis," IEEE Transactions on Information Forensics & Security, vol. 11, no. 8, pp.1818–1830, 2016.

[5] W. Kim, S. Suh, and J. J. Han, "Face liveness detection from a single image via diffusion speed model," IEEE Transactions on Image Processing A Publication of the IEEE Signal Processing Society, vol. 24, no. 8, 2015.

[6] D. Wen, H. Han, and A. K. Jain, "Face spoof detection with image distortion analysis," IEEE Transactions on Information Forensics & Security, vol. 10, no. 4, pp. 746–761, 2015.

[7] Y. Kim, J. H. Yoo, and K. Choi, "A motion and similarity based fake detection method for biometric face recognition systems," IEEE Transactions on Consumer Electronics, vol. 57, no. 2, pp. 756–762, 2011.

[8] W. Bao, H. Li, N. Li, and W. Jiang, "A liveness detection method for face recognition based on optical flow field," in International Conference on Image Analysis and Signal Processing, pp. 233–236, 2009.

[9] B. Y, M. Fang, D. Tao, J. Yin. "Submodular asymmetric feature selection in cascade object detection." Thirtieth AAAI Conference on Artificial Intelligence AAAI Press, pp.1387-1393, 2016.

[10] Z. Chen, J. Li, Z. Chen, X. You. "Generic Pixel Level Object Tracker Using Bi-Channel Fully Convolutional Network," International Conference on Neural Information Processing, 2017.

[11] Z. He., X. Li, X. You, D. Tao, YY. Tang. "Connected Component Model for Multi-Object Tracking." IEEE Transactions on Image Processing A Publication of the IEEE Signal Processing Society, vol. 25, no. .8, pp. 3698-3711, 2016.

[12] Z. He, S. Yi, YM. Cheung, X. Yon, Tang YY. "Robust Object Tracking via Key Patch Sparse Representation," IEEE Transactions on Cybernetics, no.47 pp.354-364, 2017.

[13] Z. Zhang, J. Yan, S. Liu, and Z. Lei, "A face antispoofing database with diverse attacks," in Iapr International Conference on Biometrics, pp. 26–31, 2012.

[14] J. Maatta, A. Hadid, and M. Pietikainen, "Face spoofing detection from single images using micro-texture analysis," in International Joint Conference on Biometrics, pp. 1–7, 2011.

[15] T. Ojala, M. Pietikainen, and T. Maenpaa, "Gray scale and rotation invariant texture classification with local binary patterns," IEEE Transactions on Pattern Analysis & Machine Intelligence, vol. 1842, no. 7, pp. 404–420, 2000.

[16] Z. Zhang, D. Yi, Z. Lei, and S. Z. Li, "Face liveness detection by learning multispectral reflectance distributions," in IEEE International Conference on Automatic Face & Gesture Recognition and Workshops, pp. 436–441, 2011.

[17] J. Galbally and S. Marcel, "Face anti-spoofing based on general image quality assessment," in International Conference on Pattern Recognition, pp. 1173–1178, 2014.

[18] J. Li, Y. Wang, and A. K. Jain, "Live face detection based on the analysis of fourier spectra," Proc Spie, vol. 5404, pp. 296–303, 2004.

[19] J. Y. Choi, K. N. Plataniotis, and M. R. Yong, "Using colour local binary pattern features for face recognition," IEEE International Conference on Image Processing (ICIP). IEEE, vol. 119, no. 5, pp. 4541–4544, 2010.

[20] L. G. Roberts, "Machine perception of three-dimensional solids," vol. 20, pp. 31-39, 1963.

[21] Lukac, Rastislav, and Konstantinos N. Plataniotis, eds. Color image processing: methods and applications. CRC press, 2006.

[22] Z. Boulkenafet, J. Komulainen, and A. Hadid, "Face antispoofing based on color texture analysis," in Image Processing (ICIP), 2015 IEEE International Conference on, pp.2636–2640, IEEE, 2015.

[23] C. C. Chang and C. J. Lin, LIBSVM: A library for support vector machines. ACM, 2011.

[24] I. Chingovska, A. Anjos, and S. Marcel, "On the effectiveness of local binary patterns in face anti-spoofing," in Biometrics Special Interest Group, pp. 1–7, 2012.

[25] A. Anjos and S. Marcel, "Counter-measures to photo attacks in face recognition: A public database and a baseline," in International Joint Conference on Biometrics, pp. 1–7, 2011.

[26] J. Yang, Z. Lei, S. Liao, and S. Z. Li, "Face liveness detection with component dependent descriptor," in Biometrics (ICB),2013 International Conference on, pp. 1–6, IEEE, 2013.

[27] J. Komulainen, A. Hadid, and M. Pietikainen, "Face spoofing detection using dynamic texture," Eurasip Journal on Image& Video Processing, vol. 2014, no. 1, pp. 1-15, 2014.

[28] S. Tirunagari, N. Poh, D. Windridge, A. Iorliam, N. Suki, and A. T. S. Ho, "Detection of face spoofing using visual dynamics," IEEE Transactions on Information Forensics & Security, vol. 10, no. 4, pp. 762–777, 2015.

[29] A. Pinto, H. Pedrini, W. R. Schwartz, and A. Rocha, “Face spoofing detection through visual codebooks of spectral temporal cubes.,” IEEE Transactions on Image Processing A Publication of the IEEE Signal Processing Society, vol. 24, no. 12, pp. 4726-4720, 2015.

[30] T. de Freitas Pereira, A. Anjos, J. M. De Martino, and S. Marcel, “Can face anti-spoofing countermeasures work in a real world scenario?” in Biometrics (ICB), 2013 International Conference on, pp. 1–8 , IEEE, 2013