symmetry

MDPI

Article

# Face Liveness Detection Based on Skin Blood Flow Analysis

**Shun-Yi Wang [1], Shih-Hung Yang [2,*], Yon-Ping Chen [1] and Jyun-We Huang [2]**

[1] Department of Electrical Engineering, National Chiao Tung University, Hsinchu 30010, Taiwan; sywang.ece04g@g2.nctu.edu.tw (S.-Y.W.); ypchen@cc.nctu.edu.tw (Y.-P.C.)

[2] Department of Mechanical and Computer-Aided Engineering, Feng Chia University, Taichung 40724, Taiwan; t9988776@gmail.com

* Correspondence: shyang@fcu.edu.tw; Tel.: +886-4-2451-7250 (ext. 3527)

Received: 6 November 2017; Accepted: 1 December 2017; Published: 7 December 2017

**Abstract:** Face recognition systems have been widely adopted for user authentication in security systems due to their simplicity and effectiveness. However, spoofing attacks, including printed photos, displayed photos, and replayed video attacks, are critical challenges to authentication, and these spoofing attacks allow malicious invaders to gain access to the system. This paper proposes two novel features for face liveness detection systems to protect against printed photo attacks and replayed attacks for biometric authentication systems. The first feature obtains the texture difference between red and green channels of face images inspired by the observation that skin blood flow in the face has properties that enable distinction between live and spoofing face images. The second feature estimates the color distribution in the local regions of face images, instead of whole images, because image quality might be more discriminative in small areas of face images. These two features are concatenated together, along with a multi-scale local binary pattern feature, and a support vector machine classifier is trained to discriminate between live and spoofing face images. The experimental results show that the performance of the proposed method for face spoof detection is promising when compared with that of previously published methods. Furthermore, the proposed system can be implemented in real time, which is valuable for mobile applications.

**Keywords:** spoof detection; skin blood flow; block-based color moment; public domain database

## 1. Introduction

To protect personal privacy, biometric authentication systems, such as face and fingerprint recognition systems, have gained considerable attention for their ability to confirm user identity. Thus, face and fingerprint recognition systems [1,2] have been extensively researched and implemented in various security systems. In recent decades, human face recognition systems have been widely studied due to their simplicity and effectiveness for performing user authentication in security systems. One of the most popular mobile operating systems, Android, even allows users to unlock their smartphones through face recognition. As the need for face-recognition-based unlocking techniques increases, determining how to deal with spoofing attacks becomes a critical authentication challenge [3]. Spoofing attacks launched against an authentication system may allow malicious invaders to gain access to the system and can therefore lead to the leakage of private data [4]. A face recognition system mainly conducts face representation and face matching when a face is detected by a face detection algorithm. For face representation, most methods extract facial landmarks by geometrical descriptors for both 2D and 3D faces, and are robust in dealing with expression and occlusion [5–7]. For face matching, multi-class classifiers are usually adopted, such as support vector machine (SVM) and Bayesian classifiers. These face recognition systems have achieved satisfactory performance in security and forensic applications. However, a recent study showed that state-of-the-art face recognition systems that use commercial software are vulnerable to spoofing attacks using face images [8]. The reason for this is that live and spoofing face images of the same user may be similar in the feature space when a high resolution spoofing face image is provided. Even the human eye cannot distinguish a live face image from a spoofing face image at first glance [9]. Such attacks on a secure system is a substantial problem because acquiring face images or video from a camera or social media is easier than acquiring other biometric traits, such as fingerprints. Therefore, detection of face liveness is a difficult problem for the face recognition system. It is important to design face liveness detection algorithms to discriminate between live and spoofing face images.

With the rapid development of multimedia technology, malicious invaders can easily collect photographs or video of a targeted person from the Internet. Figure 1 shows samples of live face image, printed face image, and displayed face image. Because printed photos and video replay attacks are more easily launched than 3D mask attacks, this study focused its examination on printed photos, displayed photos, and replayed video attacks. The purpose of this paper is to develop a face liveness detection algorithm which protects the biometric system from printed photos, displayed photos, and replayed video attacks.

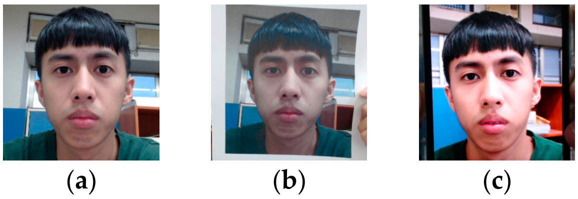


**Figure 1.** Examples of (**a**) a live face image, (**b**) a printed photo, and (**c**) a photo displayed on a mobile phone.

## 2. Related Work

Various studies have proposed several "face liveness" detection methods to protect against printed photo attacks and replayed attacks. These methods are based on motion, image quality, texture, and depth, and are as follows:

1. *Motion-Based Methods*: Motion-based methods aim to detect the natural responses of live faces, such as eye blinking [10,11], head rotation [12], and mouth movements [13]. Although these methods can successfully detect printed photo attacks, they are ineffective at identifying replayed video attacks, which present natural responses. Furthermore, they require multiple frames (usually >3 s) to estimate facial motions restricted by the human physiological rhythm [14].
2. *Image Quality Analysis-Based Methods*: Image quality analysis-based methods [15,16] capture the image quality differences between live and spoofing face images. Image quality degradations, which are caused by spoofing mediums (e.g., paper and screen), usually appear in spoofing face images, and printed photos and replayed videos displayed on a monitor can be detected using color space analysis [17]. Thus, these methods extract chromatic moment features to distinguish a live face image from a spoofing face image. These methods usually assess image quality by using whole images and are highly generalizable. However, image quality might be more discriminative in small and local areas of face images.
3. *Texture-Based Methods*: Texture-based methods [9,18] assume that the use of various spoofing mediums would result in distinct surface reflection and shape deformation, which lead to texture differences between live and spoofing face images. These methods are used to perform face spoof detection by extracting texture features from a single face image and can thus provide a quick response. However, the texture features may lack good generalizability to various facial expressions, poses, and spoofing schemes when the training data are collected from few subjects

and under limited conditions. Therefore, combining texture features and image quality features may improve the performance of face spoof detection.

4. *Depth-Based Methods*: Depth-based methods [12,19] estimate the depth information of a face to discriminate a live 3D face from a spoofing face presented on 2D planar media. The defocusing technique [20], near-infrared sensors [21], and light field cameras [22] are representative examples of these methods. Depth features can be used to effectively detect printed photos and video replay attacks. On the other hand, few studies have developed 3D depth analysis methods to estimate the 3D depth information of a face. An optical flow field-based approach is proposed to analyze the difference in the optical flow field between a planar object and a 3D face [12]. Another study exploits geometric invariants according to a set of facial landmarks for detecting replay attacks [19]. However, to estimate the depth information, these methods generally require multiple frames or a depth-measuring device, which might increase the cost of the systems.

To address the problems identified in the aforementioned methods, this study proposes a new framework, including two new features inspired by the texture-based method [18] and image distortion analysis [16], for face spoof detection. The experimental results showed that the proposed framework is competitive with state-of-the-art approaches, and the key contributions of this framework can be summarized as follows:

- The first feature highlights the distinct properties in red and green channels between live and spoofing face images. This feature can reveal skin blood flow differences between live and spoofing face images. This skin-related texture feature is extracted by the local binary pattern (LBP) operator in red and green channels and can detect both shape and color distortion. In other words, it combines the advantages of texture- and image quality analysis-based methods.
- The second feature is a block-based color moment that estimates the color distribution in the local regions of face images. This feature can preserve the local color distribution of face images and, further, provides more spatial information than does the color moment determined from a whole image. The local information helps discriminate between live and spoofing face images.

The proposed features were concatenated, along with a multi-scale local binary pattern (MLBP) feature, to construct a feature vector from a single image for providing a quick response. The feature vector was fed into an SVM to discriminate between live and spoofing face images. Four public domain databases, namely NUAA Photograph Imposter Database [23], CASIA Face Anti-Spoofing Database [24], Idiap Replay-Attack [9], and MSU Mobile Face Spoofing Database [16], were used to evaluate the performance of the proposed method. The experimental results demonstrated that the performance of the proposed method for face spoof detection is promising when compared with that of previously published methods. Furthermore, the proposed system requires less computational time (54.6 ms) and can thus be performed in real-time.

The remainder of this paper is organized as follows: Section 2 describes the proposed face spoof detection method in detail, Section 3 outlines the experimental results based on the public domain databases, and Section 4 presents a conclusion.

## 3. Face Livenss Detection

This section describes the individual steps of the proposed face liveness detection system, which are outlined in Figure 2. Faces were detected using the Viola–Jones face detection algorithm [25] when the coordinates were not available in the databases; thereafter, they were normalized into a 64 × 64 pixel image. Distortions in the specular reflection components and color distribution usually appear in spoofing face images due to the spoofing mediums. In this study, three features were set to extract discriminative information for the live and spoofing face images according to skin texture and color distortion analysis. Subsequently, the features were concatenated to create a feature vector, which was fed into an SVM for classification. In the subsequent subsections, these features are explained in greater detail.

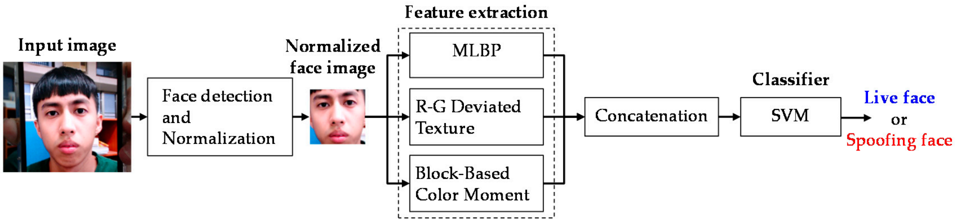


**Figure 2.** Proposed face liveness detection system.

### *3.1. Multi-Scale Local Binary Pattern*

As noted, live face images possess distinct surface reflection properties that distinguish them from 2D spoofing face images captured from printed photos and video replays. This differentiation is mainly due to specular and diffusion components. Thus, MLBP generalized from a LBP [26] was used as an image descriptor to extract the texture features related to reflection properties, which have been shown to have good discriminative ability for face spoof detection [18]. Furthermore, a uniform LBP operator [27] was employed to keep, at most, two bitwise transitions between 1 and 0 and to accumulate the other patterns in another bin. The uniform LBP operator for a pixel with value $g_c$ surrounded by $P$ neighborhood pixels in radius $R$ is defined as

$$LBP_{P,R}^{u2} = \begin{cases} \sum_{p=0}^{P-1} s(g_p - g_c)2^p & , \quad \text{if } U(LBP_{P,R}) \le 2 \\ P+1 & , \quad \text{otherwise} \end{cases} , \tag{1}$$

$$U(LBP_{P,R}) = |s(g_{P-1} - g_c) - s(g_0 - g_c)| + \sum_{p=1}^{P-1} |s(g_p - g_c) - s(g_{p-1} - g_c)|, \tag{2}$$

where $u2$ denotes a uniform pattern and $g_p$ denotes the $p$th neighborhood pixel value. A feature vector was then constructed by concatenating a uniform LBP histogram from the whole image.

It has been found that the pixel intensity of the red channel of human skin is usually higher than that of either of the blue or green channels due to skin blood flow. Additionally, the reflectance characteristic of the red channel in live face images may be different from that in spoofing face images. Therefore, this study examined MLBP features in the red channel to determine facial texture according to three scales of LBP operators: $LBP_{8,1}^{u2}$, $LBP_{8,2}^{u2}$, and $LBP_{16,2}^{u2}$. The feature vector was a concatenation of a $LBP_{8,1}^{u2}$ histogram of nine overlapping image blocks and of $LBP_{8,2}^{u2}$ and $LBP_{16,2}^{u2}$ histograms over the whole image. Each image block was divided from a normalized 64 × 64 face image with a 16-pixel overlap to highlight the central regions of an image, which may provide key facial details. Thus, the dimensionality of the MLBP feature vector is 531 + 243 + 59 = 833. Notably, the parameters of MLBP, such as $P$, $R$, and the number of overlapping image blocks, were designed according to the suggestion of [18] due to their satisfactory performance.

### *3.2. Red–Green Deviated Texture*

It is known that skin blood flow in the face enables a live face to reflect red light and absorb green light [28]. A live face image therefore consists of a wider variety of intensity values and more detailed texture in the red channel than in the green channel. By contrast, a spoofing face image generated by a printer or displayed on a screen usually possesses a monotonic color distribution in both the red and green channels due to the imperfect color reproduction property of printing or display devices. The difference between red and green channels may help distinguish between live and spoofing face images. Furthermore, the specular and diffusion components in red and green channels of a live face image are different from those in a spoofing face image. This study therefore proposed a new feature, called the red–green (R–G) deviated texture, which is a dual-channel extraction based on the LBP operator for identifying the texture difference between the red and green channels.

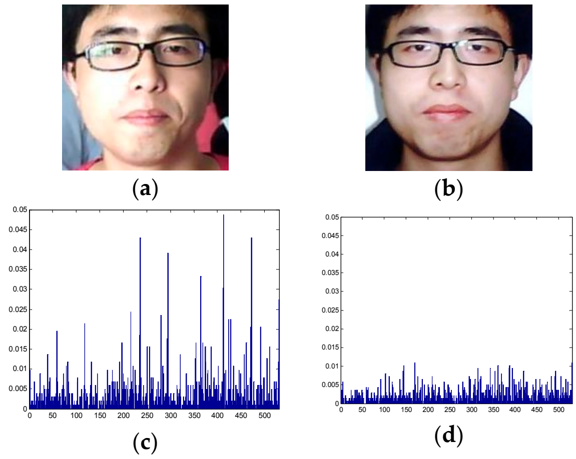
The R–G deviated texture is histogram-generated from a whole face image and is defined as $\mathbf{H}_{R-G} = \left(H^1_{R-G}, H^2_{R-G}, \cdots, H^{59}_{R-G}\right)$ with

$$H^i_{R-G} = \left| H^i_{LBP\_R} - H^i_{LBP\_G} \right|, \qquad i = 1, 2, \cdots, 59 \;, \tag{3}$$

where $H^i_{LBP\_R}$ and $H^i_{LBP\_G}$ denote the $i$th bin of the LBP histogram using $LBP^{u2}_{8,1}$ in the red and green channels, respectively. Notably, a uniform pattern [29] was adopted to implement a simple rotation invariant descriptor, which consists of at most two 1–0 or 0–1 transitions. Therefore, the LBP histogram used in this study is a 59-dimensional feature vector including 58 separate bins for uniform patterns and a single bin for all 198 nonuniform patterns.

Because the R–G deviated texture may contain discriminative information in small and local areas of an image, the normalized 64 × 64 face images in this study were divided into 3 × 3 blocks with 16-pixel overlapping. The R–G deviated texture was formed by concatenating the LBP histograms; it has a dimensionality of 531. This study analyzed the influence of the color channel on textures due to the skin blood flow differences between live and spoofing face images.

Figure 3 presents a graphical representation of the R–G deviated textures in live and spoofing face images, where the $y$ axis denotes the percentage of deviation between the red and green channels. As revealed by the figure, the texture difference between red and green channels in the live face image is larger than that in the spoofing face image. In other words, spoofing face images present a different texture distribution compared with that in live face images, which suggests that the R–G deviated texture may be a feature with the ability to differentiate between live and spoofing face images.



(**a**) (**b**)

(**c**) (**d**)

**Figure 3.** R–G deviated texture in (**a**) a live face image and (**b**) a spoofing face image; (**c**,**d**) Graphical representation of the R–G deviated texture in the live and spoofing images.

## 3.3. Block-Based Color Moment

Image chromaticity and contrast distortion are the major distortions that occur in a spoofing face image captured from printed photo and replayed video [16]. These distortions lead to color distribution differences between live and spoofing face images due to the imperfect color reproduction property of spoofing media, such as printers and screens.

Figure 4 shows the color distributions in the hue, saturation, and value (HSV) space of a live face image, a printed photo, and an on-screen photo. In general, printed photos tend to have less color contrast and saturation than do live face images. By contrast, on-screen photos tend to have more contrast and brightness than do live face images.

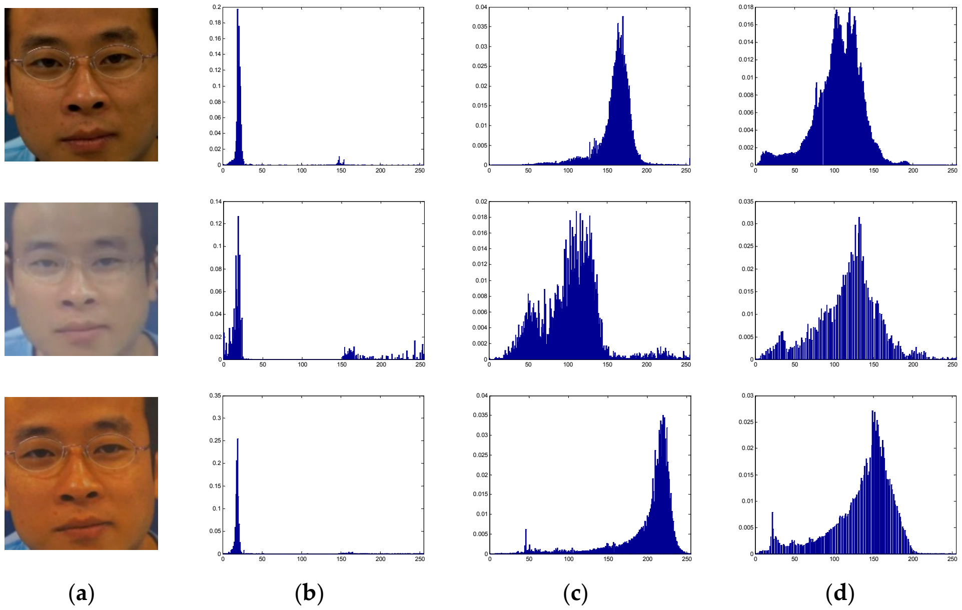


**Figure 4.** Examples of a live face image (**first row**), spoofing face image used in a printed photo attack (**second row**), and spoofing face image used in a video replay attack. Images were retrieved from the CASIA database. (**a**) Face image; (**b**) Histogram of the hue component; (**c**) Histogram of the saturation component; (**d**) Histogram of the value component.

In this study, the color distribution of an image was estimated to elucidate the chromatic differences between live and spoofing face images. First, the face image was converted from the RGB space to the HSV space. Subsequently, the mean, standard deviation, and skewness of the color distribution of an image were computed in the *i*th channel as follows:

$$E_i = \frac{1}{N}\sum_{j=1}^{N} p_{ij}, \tag{4}$$

$$\sigma_i = \sqrt{\frac{1}{N}\sum_{j=1}^{N}\left(p_{ij} - E_i\right)^2}, \tag{5}$$

$$s_i = \sqrt[3]{\frac{1}{N}\sum_{j=1}^{N}\left(p_{ij} - E_i\right)^3}, \tag{6}$$

where $p_{ij}$ denotes the *j*th image pixel value in the *i*th color channel, and $N$ is the total number of pixels. These three statistical moments of each channel are also known as color moment features [30]. Therefore, the dimensionality of the color moment feature vector is $3 \times 3 = 9$.

In [30], the color moment features were extracted from a whole face image. However, the color moment features can reveal distinct properties in small and local areas of face images. The local regions of face images may show larger color distribution differences between live and spoofing face images than do entire face images. This study therefore proposed a block-based color moment, which is a concatenation of color moment features calculated from the local regions of a face image. Face images were first divided into $2 \times 2$ blocks without overlapping; subsequently, the color moment features from each of the four blocks were extracted for each color channel. By concatenating all of the color moment features from the four blocks, a block-based color moment with 36 dimensions was constructed.

Finally, the MLBP features, block-based color moment, and R–G deviated texture feature were concatenated together to create a feature vector whose dimensionality was 833 + 531 + 36 = 1400. An SVM classifier [31] was then trained to discriminate between live and spoofing face images by using library LibSVM [32]. The objective of the SVM is to search for an optimal hyper-plane which separates the face images into live and spoofing face images with a maximum margin. A linear SVM was implemented for NUAA Photograph Imposter Database, CASIA Face Anti-Spoofing Database, and Idiap Replay-Attack, while a nonlinear SVM with the radial basis function kernel was implemented for MSU Mobile Face Spoofing Database in order to compare the proposed method with that developed by Wen et al. [16]. Notably, the linear SVM was trained with the default parameters due to their reliable performance. A parameter optimization was performed for the nonlinear SVM by cross-validation to ensure a fair comparison. Furthermore, the attributes were scaled to avoid numerical difficulties [33]. Because the R–G deviated texture and block-based color moment were extracted as the features, the proposed system required color images.

## 4. Empirical Work

The proposed face liveness detection system was evaluated using four public domain databases according to the training and testing protocols from [9,23,24]. This section first introduces the four public domain databases: NUAA Photograph Imposter Database [23], CASIA Face Anti-Spoofing Database [24], Idiap Replay-Attack [9], and MSU Mobile Face Spoofing Database [16]. Then, the empirical results including the effects of the color channel and individual features on the performance of the proposed method were demonstrated.

### *4.1. Face Spoofing Database*

Four public domain databases containing images of various 2D face spoof attacks were used to evaluate the performance of the proposed face liveness detection system. The system detected the face using the Viola–Jones face detection algorithm [25] and normalized the face image into a 64 × 64 pixel image. The properties of the four public domain databases are summarized as follows.

#### 4.1.1. NUAA Photograph Imposter Database

The NUAA Photograph Imposter Database [23] was created in 2010 and is currently one of the most widely used benchmark databases. This database contains 5105 live client and 7509 printed photo attack images from 15 Asian subjects in various environments and under different illumination conditions. The live client images were captured using a webcam (20 fps, 640 × 480 pixels), whereas the printed photo attack images were captured using a Canon camera (Canon, Inc., Lake Success, NY, USA) and were then printed on both A4 paper and photographic paper. Figure 5 shows a few samples of the live client and printed photo attack images available in the NUAA database.

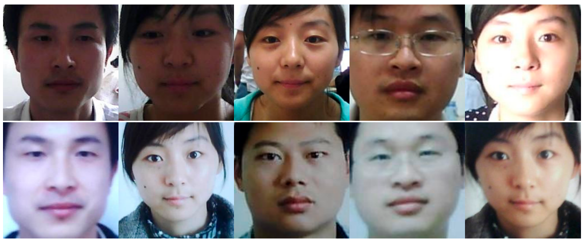


**Figure 5.** Samples of live face images (**top row**) and spoofing face images (**bottom row**) in the NUAA database.

#### 4.1.2. CASIA Face Anti-Spoofing Database

The CASIA Face Anti-Spoofing Database [24] was launched in 2012 and contains images of three types of spoofing attacks: printed photo attack, printed photos with perforated eye regions, and video replay attacks. This database contains 150 live and 450 spoofing videos collected from 50 Asian subjects, which were captured in triplicate using a low-quality camera (640 × 480), a normal quality camera

(480 × 640), and a high-quality Sony NEX-5 camera (Sony, Tokyo, Japan) (1920 × 1080). Figure 6 shows examples of each of the three types of spoofing attacks.

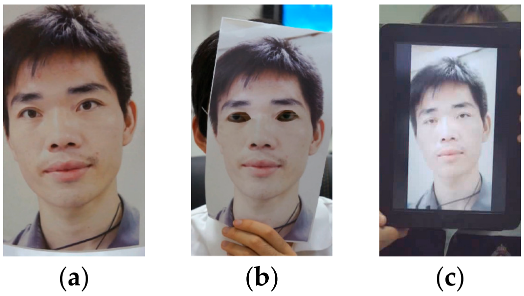


**Figure 6.** Samples of spoofing attack images in the CASIA database. (**a**) Printed photo attack; (**b**) Printed photo with perforated eye regions; (**c**) Video replay attack.

### 4.1.3. Idiap Replay-Attack

Idiap Replay-Attack [9] emerged in 2012 and consists of three types of spoofing attack videos: printed photos, mobile phone attacks, and tablet attacks. This database contains 200 live and 1000 spoofing attack videos collected from 50 subjects who are identified as Caucasian, Asian, or African. The live face videos were collected using a MacBook Webcam (Apple Inc., Cupertino, CA, USA) (320 × 240 pixels), whereas the spoof face videos were collected using a Canon PowerShot SX150 IS camera (Canon, Inc., Lake Success, NY, USA) (1280 × 720 pixels). Additionally, the videos are captured under two types of stationary conditions: with a fluorescent lamp against a uniform background or in daylight against a nonuniform background. Furthermore, each attack video is captured in both hand-based and fixed-support modes. Figure 7 shows the face samples of the live and spoofing face images. This study followed the protocols specified in [9] and, thus, adopted all frames in the training set to train the classifier and those in the developing set to determine the threshold value. The classifier was then tested using all of the frames in the testing set of Idiap Replay-Attack.

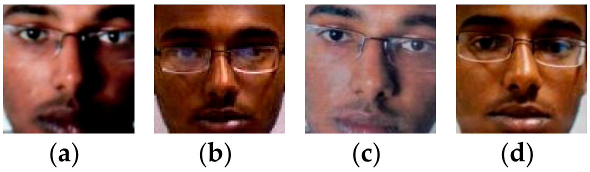
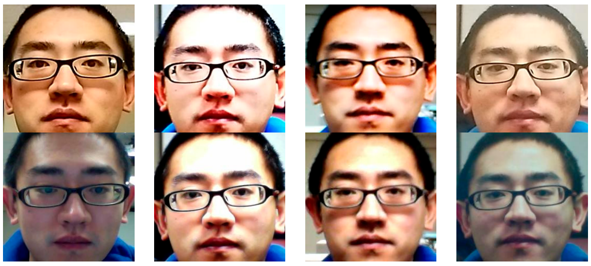


**Figure 7.** Face samples in Idiap Replay-Attack. (**a**) Live face image; (**b**) Spoofing face image used in printed photo attacks; (**c**) Spoofing face image used in mobile phone attacks; (**d**) Spoofing face image used in tablet attacks.

### 4.1.4. MSU Mobile Face Spoofing Database

The MSU Mobile Face Spoofing Database [16] was launched in 2015 and contains both printed photos and replayed video attacks. In total, this database contains 110 live videos and 330 spoofing attack videos collected from 35 subjects who are identified as Caucasian (70%), Asian (28%), or African (2%). Similar to Idiap Replay-Attack, live face videos were captured using a MacBook Air laptop camera (Apple Inc., Cupertino, CA, USA) (640 × 480 pixels) and Google Nexus 5 mobile phone camera (Google, Mountain View, CA, USA) (720 × 480 pixels), whereas the spoof face videos were captured using a Canon 550D SLR camera (Canon, Inc., Lake Success, NY, USA) (1920 × 1088 pixels) and iPhone 5s camera (Apple Inc., Cupertino, CA, USA) (1920 × 1080 pixels). Each video is at least 9 s long, with 30 fps. Because the face images are captured on a mobile phone, the MSU database can simulate mobile phone unlocking applications. Furthermore, the printed photos are of higher quality than those from other databases due to the use of a state-of-the-art color printer (HP Color Laserjet CP6015xh). The videos are replayed on two attack media (iPad Air and iPhone 5S screens). Figure 8 shows samples of some live and spoofing face images found in the database.

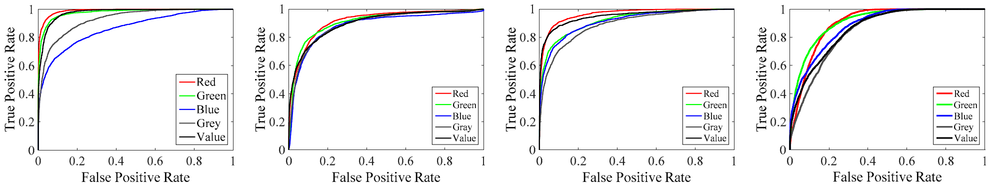


(**a**) (**b**) (**c**) (**d**)

**Figure 8.** Face samples in the MSU database that were captured using the cameras in a Google Nexus 5 mobile phone (**top row**) and MacBook Air (**bottom row**). (**a**) Live face images; (**b**) Spoofing face images replayed on an iPad Air screen; (**c**) Spoofing face images replayed on an iPhone 5S screen; (**d**) Spoofing face images used in a printed photo attack.

## 4.2. Effects of Different Color Channels

The MLBP used in this study could extract texture features from a specific color channel of a facial image. In this section, the influence of various color channels (i.e., red, green, and blue channels in the RGB space; the luminance channel in the YUV space where Y is the luminance, and U and V are the chrominance; and the luminance channel in the HSV space) on the proposed face liveness detection system in the four public domain databases is reviewed. Notably, only the MLBP was extracted as the feature vector, which was then fed into the SVM classifier. Figure 9a–d present the receiver operating characteristic (ROC) curves of various color channels in the NUAA, CASIA, Idiap, and MSU databases, respectively. The Grey and Value lines represent the luminance channels in the YUV and HSV spaces, respectively. As described in the earlier text, the red channel provided the best performance among all color channels. This finding indicated that the texture features in the red channel offer information that helps discriminate between live and spoofing face images.



(**a**) (**b**) (**c**) (**d**)

**Figure 9.** Face spoofing detection performance on the (**a**) NUAA; (**b**) CASIA; (**c**) Idiap; and (**d**) MSU databases, using the MLBP to extract features from various color channels.

## 4.3. Effects of Different Features

The proposed face liveness detection system utilizes a combination of three features: the MLBP, R–G deviated texture, and the block-based color moment. The effects of individual features and various combinations of the features were analyzed, and the results are listed in Table 1. For all combinations, the face detection and classifier were identical to the proposed face liveness detection system. The performance of the system using various features from each database was evaluated by calculating the accuracy rate, as follows:

$$Accuracy\ rate = \frac{TP + TN}{N} \times 100(\%), \tag{7}$$

where $N$ denotes the total number of face images (including live and spoofing face images), and $TP$ and $TN$ indicate the numbers of correctly identified live and spoofing face images, respectively. In addition to the accuracy rate, ROC curve data were collected, and the area under the ROC curve (AUC) was calculated as another performance index of the proposed face spoof detection system. Notably, methods that have larger AUCs are generally considered to be more accurate methods. The training and testing protocols for the four public domain databases were identical to those used in [9,23,24].

**Table 1.** Face spoofing detection performance (%) regarding various combinations of features in images from the four public domain databases where values in bold indicate the best results among the features.

| Feature | NUAA | | CAISA | | Idiap | | MSU | |
|---|---|---|---|---|---|---|---|---|
| | Accuracy | AUC | Accuracy | AUC | Accuracy | AUC | Accuracy | AUC |
| (i) | 80.04 | 91.68 | 82.90 | 90.52 | 86.04 | 90.12 | 75.99 | 86.82 |
| (ii) | 85.60 | 92.46 | 80.72 | 86.08 | 87.13 | 92.79 | 85.15 | 91.17 |
| (iii) | 72.48 | 90.97 | 85.66 | 89.27 | 84.76 | 92.28 | 78.19 | 86.64 |
| (iv) | 73.60 | 91.34 | 89.03 | 91.85 | 91.56 | 93.78 | 79.19 | 87.72 |
| (v) | 95.45 | 99.29 | 90.72 | 95.13 | 93.74 | 97.46 | 82.13 | 90.44 |
| (vi) | 95.52 | 99.34 | 91.70 | 95.35 | 95.52 | 98.73 | 88.45 | 93.89 |
| (vii) | **98.56** | 99.85 | 88.59 | 94.00 | 92.59 | 97.13 | 86.31 | 92.57 |
| (viii) | 92.16 | 99.43 | 90.02 | 94.27 | 92.01 | 97.08 | 88.68 | 94.47 |
| (ix) | 96.69 | **99.96** | **93.24** | **96.57** | **96.55** | **99.34** | **90.06** | **95.71** |

i–ix: MLBP, R–G deviated texture, color moment, block-based color moment, MLBP + color moment, MLBP + block-based color moment, MLBP + R–G deviated texture, R–G deviated texture + block-based color moment, and proposed feature, respectively.

Notably, the color moment in [16] was calculated from a whole image (i.e., without dividing the image into blocks), whereas the block-based color moment used in the present study was calculated from the four individual blocks of an image. We assumed that the color moments may be more discriminative in small and local areas of the image than the moments calculated from a whole image. Therefore, the images were divided into 2 × 2 blocks without overlap for examination. The feature vector of the block-based color moment was formed by concatenating the color moments calculated from each individual block. As shown in Table 1, the block-based color moment (iii) achieved better performance than did a single color moment calculated from a whole image (iv), in terms of both the accuracy rate and AUC, in all of the databases. In other words, the color moments in the local areas of an image provided more spatial information about the face and were more discriminative than was the color moment calculated from a whole image.

Table 1 also reveals that the R–G deviated feature achieves better performance than do the other individual features in the NUAA and MSU databases, but not in the Idiap or CASIA database. This feature also achieved the lowest AUC (86.08%) among all individual features in the CASIA database. The result indicated that the difference between the red and green channels in live face images is distinct from those in the spoof face images in the NUAA and MSU databases, but the same is not true in the Idiap or CASIA database. By contrast, the block-based color moment achieved better performance than the other individual features in both the Idiap and CASIA databases, but not in the NUAA or MSU databases. Furthermore, this feature achieved the highest AUC (93.78%) among all individual features in the Idiap database. This result showed that spoof attack images possess imperfect color reproduction properties, which lead to a color distribution that is distinct from that in the live face images in both the Idiap and CASIA databases. Therefore, this color-based feature can discriminate between live and spoofing face images in these two databases.

Most of the combinations of the features (v–viii) achieved better performance than did the individual features (i–iv). For example, the R–G deviated feature improved when it was combined with the MLBP in the NUAA database: combining these two features enhanced the AUC by 7.39% and generated the highest AUC of 99.85%. The block-based color moment also improved when it was combined with the MLBP in the CASIA, Idiap, and MSU databases. Combining these two features enhanced the AUC by 3.5%, 4.95%, and 2.72% in the CASIA, Idiap, and MSU databases, respectively, and generated the highest AUCs of 95.35% and 98.73% in the CASIA and Idiap databases, respectively. Both the R–G deviated feature alone and combined with the MLBP achieved the optimum performance in the NUAA database. Furthermore, both the block-based color moment alone and combined with the MLBP achieved the optimum performance in the CASIA and Idiap databases. The MLBP was helpful in differentiating reflectance between live and spoofing face images. However, among all combinations, none of these combinations achieved the best performance (regarding either the accuracy rate or AUC) in all databases. By contrast, the proposed face liveness detection system combined all three features to further improve spoofing image identification. Specifically, the AUC results were 96.57%, 99.34%, and 95.71% in the CASIA, Idiap, and MSU databases, respectively. Although the proposed method had a lower accuracy rate than did the method combining the MLBP and R–G deviated texture, the proposed method achieved the highest AUC (99.96%) in the NUAA database. This finding confirmed that the proposed method has an excellent ability to discriminate between live and spoofing face images and can accurately identify spoofing face images in all of the databases.

## 5. Performance Evaluation

In this section, the proposed method is compared with previously published methods from [16,18,23,34,35], which adopted various preprocessing techniques, features, and classifiers. First, the performance indices that are used to measure the performance of a face liveness detection system are described. Subsequently, the performance of different face spoofing detection methods is compared.

### *5.1. Performance Index*

The performance of a face liveness detection system was determined based on its accuracy rate (in the NUAA database), equal error rate (EER) (in the CASIA and MSU databases), and half total error rate (HTER) (in the Idiap database). Face liveness detection system errors can be divided into false acceptance (wherein a spoofing face image is classified as a live face image) and false rejection (wherein a live face image is classified as a spoofing face image). The HTER is defined as half of the sum of the false acceptance rate (FAR) and false rejection rate (FRR) and is calculated as

$$\mathrm{HTER}(\tau) = \frac{\mathrm{FAR}(\tau) + \mathrm{FRR}(\tau)}{2}, \tag{8}$$

where $\tau$ denotes the threshold of a classifier. FAR and FRR are the ratios of incorrectly classified spoofing face images and live face images, respectively, and are defined as follows:

$$\mathrm{FAR}(\tau) = \frac{\text{\# of false acceptance}}{\text{\# of spoofing faces}}, \tag{9}$$

$$\mathrm{FRR}(\tau) = \frac{\text{\# of false rejection}}{\text{\# of real faces}}. \tag{10}$$

Typically, when the FAR increases, the FRR decreases; the lower the HTER, the better the method is. Additionally, the EER is defined as a point in an ROC curve where the FAR equals the FRR; the lower an EER value, the better the classification ability of a detection system is.

Table 2 reveals the abilities of different face liveness detection systems that were applied to identify live and spoofing face images in four public domain databases.

**Table 2.** Performance of various spoofing detection methods for images in the four public domain databases. N/A means not applicable and values in bold indicate the best results among the methods.

| Method | Classifier | NUAA | | CASIA | Idiap | MSU |
|---|---|---|---|---|---|---|
| | | Accuracy | AUC | EER | HTER | EER |
| Määttä et al. [18] | Nonlinear SVM | 92.70% | 99.00% | N/A | N/A | N/A |
| Tan et al. [23] | Sparse nonlinear logistic regression | 84.50% | 95.00% | N/A | N/A | N/A |
| Kim et al. [35] | Linear SVM | **98.45%** | N/A | N/A | 12.50% | N/A |
| Pinto et al. [34] | Linear SVM | N/A | N/A | 14.00% | N/A | N/A |
| Wen et al. [16] | Ensemble SVM | N/A | N/A | 12.90% | 7.41% | 8.58% |
| Proposed method | Linear SVM | 96.69% | **99.96%** | **7.01%** | **4.92%** | 10.20% |
| Proposed method [1] | Nonlinear SVM | N/A | N/A | N/A | N/A | **7.23%** |

[1] A nonlinear support vector machine (SVM) was adopted to compare the proposed method with that developed by Wen et al. [16] in the MSU database.

### 5.2. Comparison with Other Methods in NUAA Database

For the NUAA database, our proposed method achieved an accuracy rate of 96.69%. This is slightly worse than the method proposed by Kim et al. [35] but outperforms the other two methods [18,23]. Furthermore, our proposed method achieved an AUC of 99.96%, which exceeds those achieved by [18] (AUC = 99%) and [23] (AUC = 95%). Kim et al. [35] did not include AUC results in their study. This finding indicated that our proposed method can effectively classify live and spoofing face images in the NUAA database. Figure 10 shows ten examples of correctly classified images. Because the live face images are captured under adequate illumination and lighting conditions, the texture-based feature can capture facial textures from live face images. Furthermore, the proposed method also captured the color distortion, shape deformation, and surface reflection from the spoofing face images. Figure 11 presents five examples of misclassified spoofing face images in the NUAA database. Notably, there were no false rejection results (i.e., no live face images were misclassified). This result implied that the spoofing face images that were dimly lit or too bright or those that had an unknown light reflection were often misclassified by the proposed method. Although some correctly classified images were recorded under bright conditions (e.g., the last two images of the first row in Figure 10), the misclassified spoofing face images (e.g., the third image in Figure 11) were recorded under a "too bright" condition, which created an unclear texture. One possible reason for such misclassification is the lack of detailed texture information due to the dim light and too bright conditions. Additionally, there is a large portion of the background shown in the cropped images (e.g., the fourth image in Figure 11). Thus, the face detector might affect the performance of the proposed face spoofing detection method.

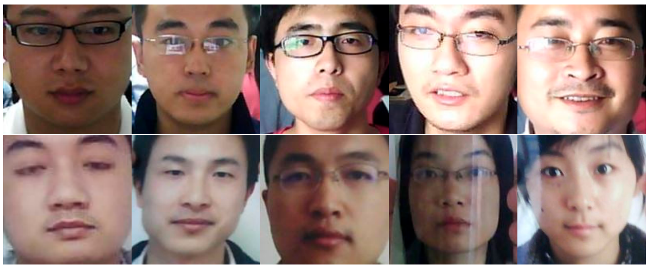


**Figure 10.** Ten examples of correctly classified images in the NUAA database by using our proposed method.

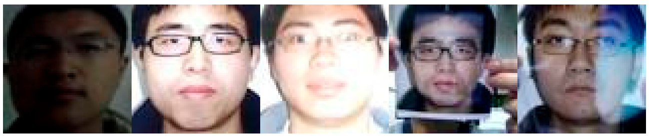


**Figure 11.** Five examples of misclassified spoofing face images in the NUAA database by using our proposed method.

### *5.3. Comparison with Other Methods in CASIA Database*

For the CASIA database, the proposed method achieved a lower EER (7.01%) than did the other methods. The CASIA database consists of low-quality subset (L), normal-quality subset (N), and high-quality subset (H) images. To analyze the influence of quality on image classification, the proposed method was applied to each subset. The results indicated an EER of 2.9%, 7.32%, and 9.96% on the L, N, and H subsets, respectively. Thus, the proposed method performed optimally on the L subset but degraded the N and H subsets. One possible reason for this result is that the faces were normalized into 64 × 64 pixel images, and the facial details may have been compressed in the N and H subsets.

Figure 12 shows ten examples of correctly classified face images that were captured with adequate and white light sources. Conversely, Figure 13 shows ten examples of misclassified images that were captured with an unknown white balance adjustment, in a dim or too bright light environment, or with oversaturated exposure. These images may have been misclassified because of the failure of color-based features, such as R–G deviated texture and the block-based color moment, for spoofing detection due to poor illumination. Furthermore, images with non-neutral facial expressions (e.g., images in the last column in Figure 13) were often misclassified. Facial expression can affect the facial texture; thus, non-neutral facial expressions can lead to the failure of texture-based features. Another possible reason is the imbalance in the proportion of face images with and without non-neutral facial expressions in the training set.

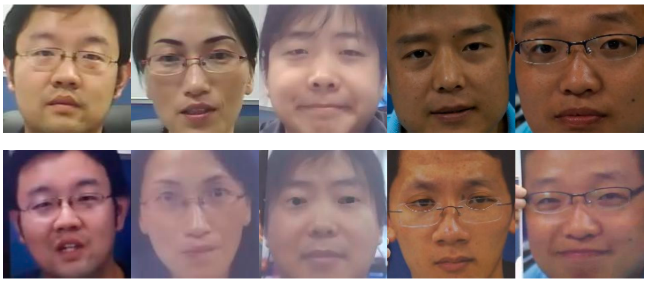


**Figure 12.** Ten examples of correctly classified images in the CASIA database by using the proposed method. (**top row**) live face images; (**bottom row**) spoofing face images.

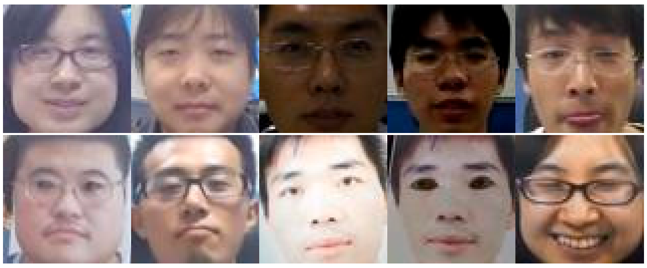


**Figure 13.** Ten examples of misclassified images in the CASIA database by using the proposed method. (**top row**) live face images; (**bottom row**) spoofing face images.

### *5.4. Comparison with Other Methods in Idiap Database*

For the Idiap database, the proposed method achieved an HTER of 4.92%, which is the lowest HTER among all of the studied methods. Although the proposed method was slightly worse at classifying images in the NUAA database than the method in [35] (in terms of the accuracy rate), the HTER of the method in [35] for images in Idiap database was 12.5%. Notably, the Idiap database is much larger than the NUAA database, and contains various types of spoofing face samples, including printed photos, displayed photos, and replayed videos. Furthermore, Idiap database includes images of subjects variously identified as Caucasian, Asian, and African. This diversity implies that Idiap database has been extensively used by researchers and has been utilized for spoofing detection performance evaluation in many studies. Figure 14 shows ten examples of correctly classified face images. As shown in the figure, the surface reflection and color distortion that appear in the spoofing face images were adequately captured by the proposed method. Figure 15 shows ten examples of misclassified face images in Idiap database, which were incorrectly assessed due to dim lighting, skin color, face position, or colored light source. In particular, a live face image in which the person is not looking directly at the camera (i.e., the fourth image of the first row in Figure 15) was misclassified by the proposed method. Both live and spoofing face images that portray a person with dark skin were also often misclassified. One possible reason for this misclassification is the imbalance of images of individuals of various races in the training set, which was discussed in [16].

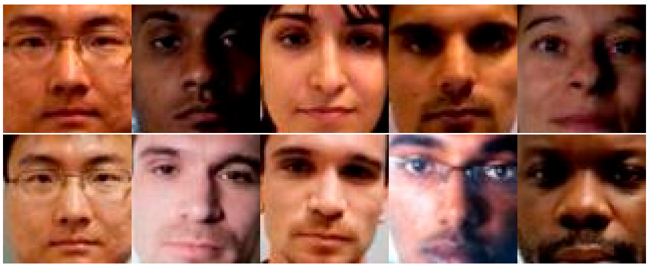


**Figure 14.** Ten examples of correctly classified images in Idiap database by using the proposed method. (**top row**) live face images; (**bottom row**) spoofing face images.

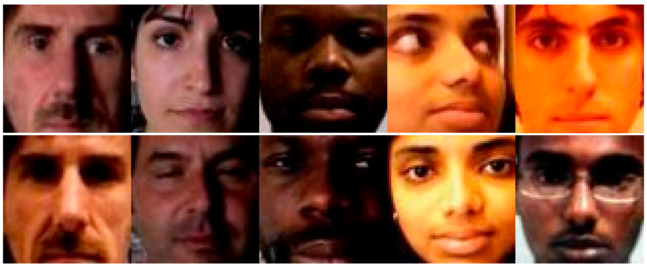


**Figure 15.** Ten examples of misclassified images in Idiap database by using the proposed method. (**top row**) live face images; (**bottom row**) spoofing face images.

### *5.5. Comparison with Other Methods in MSU Database*

For the MSU database, the proposed method achieved an EER of 10.20%, which is higher than that in [16] (8.58%). However, the EER achieved by the proposed method was improved from 10.20% to 7.23% when a nonlinear SVM with the radial basis function kernel was utilized. The parameters used in the nonlinear SVM were obtained through cross-validation, and the attributes were scaled to avoid numerical difficulties [33]. Following this addition, the proposed method achieved better performance than did the method developed by Wen et al. [16], and the proposed method effectively discriminated live and spoofing face images in the MSU database. Figure 16 shows ten examples of correctly classified images in the MSU database. Most of the live face images were captured under appropriate illumination conditions, whereas the spoofing face images possessed imperfect color and texture reproduction properties caused by the printing and display devices. In other words, the proposed method successfully extracted color- and texture-based features to differentiate between the live and spoofing face images. Figure 17 shows ten examples of misclassified images in the MSU database. Some potential reasons for the false rejection of the live face images are the inclusion of an accessory (e.g., cap), poor illumination, low resolution, and non-neutral facial expression. These factors can lead to poor facial texture and thus affect the performance of texture-based features in a detection system. Some potential reasons for the false acceptance of spoofing face images are overexposure, an external light source from above the subject, specular reflection on the bilateral forehead, and imperfect face alignment. These region-related factors can affect the performance of the block-based color moment due to the use of information from local areas of the image. Several of the misclassified spoofing face images were captured in high resolution and thus provided facial textures similar to the live face images.

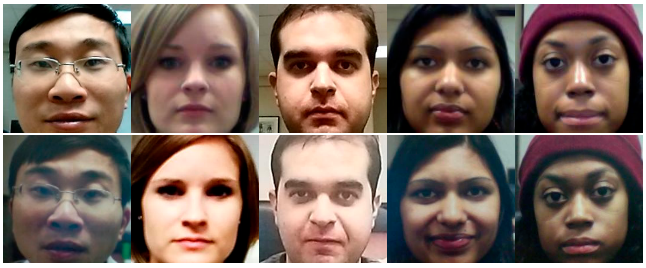


**Figure 16.** Ten examples of correctly classified images in the MSU database by using the proposed method. (**top row**) live face images; (**bottom row**) spoofing face images.

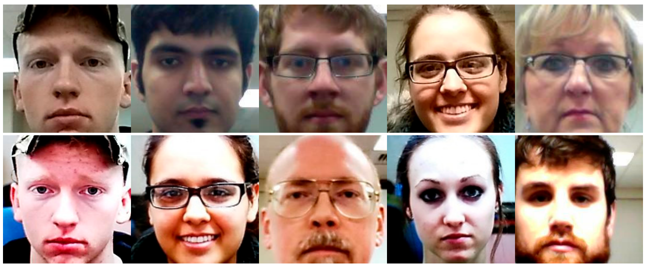


**Figure 17.** Ten examples of misclassified images in the MSU database by using the proposed method. (**top row**) live face images; (**bottom row**) spoofing face images.

According to the experimental results, previously published methods and the proposed method performed better or worse than each other depending on the database utilized. In particular, various illumination conditions rendered the identification of face spoofing images difficult. Moreover, the lack of images containing diverse facial expressions, face positions, and skin color in the training sample led to failures in the proper classification of live and spoofing face images. Although the proposed method did not consistently achieve the best performance for each database in the present study, it performed excellently in terms of the accuracy rate (96.69%), EER (7.01%), HTER (4.92%), and EER (7.23%) under the original testing protocols for the NUAA, CASIA, Idiap, and MSU databases.

### *5.6. Computational Complexity Analysis*

The computational complexity of the proposed face liveness detection system is theoretically analyzed as follows. The proposed system consists of feature extraction and classification. The first two features, MLBP and R–G deviated texture, rely on the LBP operator. The computational complexity of the LBP operator is $O(PN) + O\left(P2^P\right)$ where $P$ is the number of neighborhood pixels, $N$ is the total number of pixels, and O() is big O notation [36]. Because $P$ is a user-specified parameter and can be considered as a constant in the experiments, the computational complexity of the LBP operator is a linear-time process. For the block-based color moment, the computational complexity of computing the mean, standard deviation, and skewness of the color distribution of all blocks is $O(mN_m)$, where $m$ is the number of blocks and $N_m$ is the total number of pixels in one block. Because the image is divided into blocks without overlapping, the computational complexity of the block-based color moment is $O(N)$.

For the classification, the computational complexity of the SVM classifier is $O\left(N_{TS}^3\right)$ in the training phase where $N_{TS}$ is the number of training samples, and $O(DN_{SV})$ is in testing phase where $D$ is the dimension of the input vector and $N_{SV}$ is the number of support vectors [37]. Note that the computational complexity of the SVM classifier in testing phase is only considered for real-time implementation. All experiments were performed on a personal computer (3.2 GHz CPU and 16 GB RAM), and the proposed method was implemented in MATLAB. The average processing time for one single image is 54.6 ms, which makes the proposed system feasible for real-time applications.

## 6. Conclusions

This study proposed a face liveness detection system that could identify printed photo attacks and replayed attacks through a single face image. The proposed system adopted the MLBP, R–G deviated texture, and block-based color moment as key features. The MLBP-extracted texture features were collected from the red channel in the images to capture the specular and diffusion components caused by distinct surface reflection and shape deformation properties in 3D and 2D planar objects. The R–G deviated texture was extracted to determine the texture differences between the red and green channels due to skin blood flow. Finally, the block-based color moment was extracted from each image block to identify color distribution differences between live and spoofing face images caused by the imperfect color reproduction property of spoofing mediums. An SVM was trained to discriminate between live and spoofing face images by using the concatenation of the three features. The experimental results showed that the proposed system showed promising performance for face spoof detection on images in four public domain databases (the NUAA, CASIA, Idiap, and MSU databases). Moreover, this system can actually be performed in real time due to shorter computational time. Future research should focus on collecting more images that portray various races, ages, and facial expressions and on developing effective features that can address a wide range of spoofing scenarios.

**Acknowledgments:** This work was financially supported by the Ministry of Science and Technology of the Republic of China, Taiwan, under Contract numbers MOST 106-2221-E-035-092, MOST 105-2221-E-035-014, and NSC 102-2511-S-009-011-MY3.

**Author Contributions:** Shun-Yi Wang designed the algorithm, conducted all experiments, analyzed the results, wrote the manuscript, and conducted the literature review. Yon-Ping Chen conceived the algorithm and wrote the manuscript. Jyun-We Huang partially conducted experiments. Shih-Hung Yang conceived and designed the algorithm, guided all experiments, analyzed the results, wrote the manuscript, conducted the literature review, and guided the direction and all details of this work.

**Conflicts of Interest:** The authors declare no conflict of interest.

## References

1. Jain, A.K.; Prabhakar, S.; Hong, L.; Pankanti, S. Filterbank-based fingerprint matching. *IEEE Trans. Image Process.* **2000**, *9*, 846–859. [CrossRef] [PubMed]
2. Ramachandra, R.; Busch, C. Presentation attack detection methods for face recognition systems: A comprehensive survey. *ACM Comput. Surv. (CSUR)* **2017**, *50*, 8. [CrossRef]
3. Soldera, J.; Schu, G.; Schardosim, L.R.; Beltrao, E.T. Facial biometrics and applications. *IEEE Instrum. Meas. Mag.* **2017**, *20*, 4–10. [CrossRef]
4. Arashloo, S.R.; Kittler, J.; Christmas, W. An Anomaly Detection Approach to Face Spoofing Detection: A New Formulation and Evaluation Protocol. *IEEE Access* **2017**, *5*, 13868–13882. [CrossRef]

5. Vezzetti, E.; Marcolin, F.; Tornincasa, S.; Ulrich, L.; Dagnes, N. 3D geometry-based automatic landmark localization in presence of facial occlusions. *Multimed. Tools Appl.* **2017**, 1–29. [CrossRef]
6. Marcolin, F.; Vezzetti, E. Novel descriptors for geometrical 3D face analysis. *Multimed. Tools Appl.* **2017**, *76*, 13805–13834. [CrossRef]
7. Huang, K.-K.; Dai, D.-Q.; Ren, C.-X.; Yu, Y.-F.; Lai, Z.-R. Fusing landmark-based features at kernel level for face recognition. *Pattern Recognit.* **2017**, *63*, 406–415. [CrossRef]
8. Smith, D.F.; Wiliem, A.; Lovell, B.C. Face recognition on consumer devices: Reflections on replay attacks. *IEEE Trans. Inf. Forensics Secur.* **2015**, *10*, 736–745. [CrossRef]
9. Chingovska, I.; Anjos, A.; Marcel, S. On the Effectiveness of Local Binary Patterns in Face Anti-Spoofing. In Proceedings of the 2012 BIOSIG International Conference of the Biometrics Special Interest Group (BIOSIG), Darmstadt, Germany, 6–7 September 2012; pp. 1–7.
10. Pan, G.; Sun, L.; Wu, Z.; Lao, S. Eyeblink-Based Anti-Spoofing in Face Recognition from a Generic Webcamera. In Proceedings of the IEEE 11th International Conference on Computer Vision (ICCV 2007), Rio de Janeiro, Brazil, 14–21 October 2007; pp. 1–8.
11. Sun, L.; Pan, G.; Wu, Z.; Lao, S. Blinking-based live face detection using conditional random fields. *Adv. Biom.* **2007**, 252–260.
12. Bao, W.; Li, H.; Li, N.; Jiang, W. A liveness Detection Method for Face Recognition Based on Optical Flow Field. In Proceedings of the International Conference on Image Analysis and Signal Processing (IASP), Taizhou, China, 11–12 April 2009; pp. 233–236.
13. Kollreider, K.; Fronthaler, H.; Faraj, M.I.; Bigun, J. Real-time face detection and motion analysis with application in "liveness" assessment. *IEEE Trans. Inf. Forensics Secur.* **2007**, *2*, 548–558. [CrossRef]
14. Akhtar, Z.; Foresti, G.L. Face spoof attack recognition using discriminative image patches. *J. Electr. Comput. Eng.* **2016**, *2016*. [CrossRef]
15. Galbally, J.; Marcel, S.; Fierrez, J. Image quality assessment for fake biometric detection: Application to iris, fingerprint, and face recognition. *IEEE Trans. Image Process.* **2014**, *23*, 710–724. [CrossRef] [PubMed]
16. Wen, D.; Han, H.; Jain, A.K. Face spoof detection with image distortion analysis. *IEEE Trans. Inf. Forensics Secur.* **2015**, *10*, 746–761. [CrossRef]
17. Lai, C.; Tai, C. A Smart Spoofing Face Detector by Display Features Analysis. *Sensors* **2016**, *16*, 1136. [CrossRef] [PubMed]
18. Määttä, J.; Hadid, A.; Pietikäinen, M. Face Spoofing Detection from Single Images Using Micro-Texture Analysis. In Proceedings of the 2011 International Joint Conference on Biometrics (IJCB), Washington, DC, USA, 12–14 October 2011; pp. 1–7.
19. De Marsico, M.; Nappi, M.; Riccio, D.; Dugelay, J.-L. Moving Face Spoofing Detection via 3D Projective Invariants. In Proceedings of the 5th IAPR International Conference on Biometrics (ICB), New Delhi, India, 29 March–1 April 2012; pp. 73–78.
20. Kim, S.; Ban, Y.; Lee, S. Face Liveness Detection Using Defocus. *Sensors* **2015**, *15*, 1537–1563. [CrossRef] [PubMed]
21. Zhang, Z.; Yi, D.; Lei, Z.; Li, S.Z. Face Liveness Detection by Learning Multispectral Reflectance Distributions. In Proceedings of the IEEE International Conference on Automatic Face & Gesture Recognition and Workshops (FG 2011), Santa Barbara, CA, USA, 21–25 March 2011; pp. 436–441.
22. Kim, S.; Ban, Y.; Lee, S. Face Liveness Detection Using a Light Field Camera. *Sensors* **2014**, *14*, 22471–22499. [CrossRef] [PubMed]
23. Tan, X.; Li, Y.; Liu, J.; Jiang, L. Face liveness detection from a single image with sparse low rank bilinear discriminative model. *Comput. Vis. ECCV* **2010**, *2010*, 504–517.
24. Zhang, Z.; Yan, J.; Liu, S.; Lei, Z.; Yi, D.; Li, S.Z. A Face Antispoofing Database with Diverse Attacks. In Proceedings of the 5th IAPR International Conference on Biometrics (ICB), New Delhi, India, 29 March–1 April 2012; pp. 26–31.
25. Viola, P.; Jones, M.J. Robust real-time face detection. *Int. J. Comput. Vis.* **2004**, *57*, 137–154. [CrossRef]
26. Ojala, T.; Pietikainen, M.; Harwood, D. Performance evaluation of texture measures with classification based on Kullback discrimination of distributions. In Proceedings of the IEEE 12th International Conference on Pattern Recognition, Jerusalem, Israel, 9–13 October 1994; pp. 582–585.
27. Ojala, T.; Pietikainen, M.; Maenpaa, T. Multiresolution gray-scale and rotation invariant texture classification with local binary patterns. *IEEE Trans. Pattern Anal. Mach. Intell.* **2002**, *24*, 971–987. [CrossRef]

28. Lin, K.-Y.; Chen, D.-Y.; Tsai, W.-J. Face-Based Heart Rate Signal Decomposition and Evaluation Using Multiple Linear Regression. *IEEE Sens. J.* **2016**, *16*, 1351–1360. [CrossRef]
29. Barkan, O.; Weill, J.; Wolf, L.; Aronowitz, H. Fast High Dimensional Vector Multiplication Face Recognition. In Proceedings of the IEEE International Conference on Computer Vision, Sydney, Australia, 1–8 December 2013; pp. 1960–1967.
30. Stricker, M.A.; Orengo, M. Similarity of Color Images. In Proceedings of the IS&T/SPIE's Symposium on Electronic Imaging: Science & Technology, San Jose, CA, USA, 5–10 February 1995; pp. 381–392.
31. Cortes, C.; Vapnik, V. Support-vector networks. *Mach. Learn.* **1995**, *20*, 273–297. [CrossRef]
32. Chang, C.-C.; Lin, C.-J. LIBSVM: A library for support vector machines. *ACM Trans. Intell. Syst. Technol. (TIST)* **2011**, *2*, 27. [CrossRef]
33. Hsu, C.-W.; Chang, C.-C.; Lin, C.-J. *A Practical Guide to Support Vector Classification*; National Taiwan University: Taipei, Taiwan, 2003.
34. Menotti, D.; Chiachia, G.; Pinto, A.; Schwartz, W.R.; Pedrini, H.; Falcao, A.X.; Rocha, A. Deep representations for iris, face, and fingerprint spoofing detection. *IEEE Trans. Inf. Forensics Secur.* **2015**, *10*, 864–879. [CrossRef]
35. Kim, W.; Suh, S.; Han, J.-J. Face liveness detection from a single image via diffusion speed model. *IEEE Trans. Image Process.* **2015**, *24*, 2456–2465.
36. Liao, S.; Law, M.W.; Chung, A.C. Dominant local binary patterns for texture classification. *IEEE Trans. Image Process.* **2009**, *18*, 1107–1118. [CrossRef] [PubMed]
37. Burges, C.J. A tutorial on support vector machines for pattern recognition. *Data Min. Knowl. Discov.* **1998**, *2*, 121–167. [CrossRef]