electronics

MDPI

Article

FASS: Face Anti-Spoofing System Using Image Quality Features and Deep Learning

Enoch Solomon [1,*] and Krzysztof J. Cios [1,2]

[1] Department of Computer Science, Virginia Commonwealth University, Richmond, VA 23284 , USA
[2] University of Information Technology and Management, 35-225 Rzeszow, Poland
* Correspondence: solomone@vcu.edu

Abstract: Face recognition technology has been widely used due to the convenience it provides. However, face recognition is vulnerable to spoofing attacks which limits its usage in sensitive application areas. This work introduces a novel face anti-spoofing system, FASS, that fuses results of two classifiers. One, random forest, uses the identified by us seven no-reference image quality features derived from face images and its results are fused with a deep learning classifier results that uses entire face images as input. Extensive experiments were performed to compare FASS with state-of-the-art anti-spoofing systems on five benchmark datasets: Replay-Attack, CASIA-MFSD, MSU-MFSD, OULU-NPU and SiW. The results show that FASS outperforms all face anti-spoofing systems based on image quality features and is also more accurate than many of the state-of-the-art systems based on deep learning.

Keywords: anti-spoofing system; biometrics security; deep learning; face image quality features; ensemble learning; random forest

check for updates

Citation: Solomon, E.; Cios, K.J. FASS: Face Anti-Spoofing System Using Image Quality Features and Deep Learning. *Electronics* **2023**, *12*, 2199. https://doi.org/10.3390/electronics12102199

Academic Editor: Gwanggil Jeon

Received: 14 April 2023
Revised: 8 May 2023
Accepted: 8 May 2023
Published: 12 May 2023

Copyright: © 2023 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

Face recognition is used in a range of applications which require robustness to changes in the environment and resilience to circumvention, which is known as spoofing. Spoofing is defined as an attack where a fraudster tries to gain access to the system by masquerading as a valid user/employee [1]. Its goal is to fool biometric measures by presenting to the sensor (most often a camera) a manufactured artifact, such as a photograph or video to impersonate a valid user. Since such attacks are very frequent, they became a major concern for the designers and users of face recognition systems. As a consequence, spoofing is an active field of research as measured by a multitude of publications [2–6]; dissertations [7–10]; books [11–13] and standards [14]. There are also international competitions that seek to evaluate performance of the developed countermeasures [15–17].

Even when there are identity verification mechanisms in place, fraudsters always find a way to get around them. One such method is face spoofing, in which a fraudster attempts to deceive a facial recognition system by displaying a spoof face to the camera.

The most popular means of spoofing is to put on a valid user's mask and present it to the biometric verification system, which is referred to as a mask attack. Another method is to get hold of and print a photo of a user and present it to the camera, which is known as print attack. Another type of spoofing is a replay attack, when the system is presented with the screen of a device on which a recorded video of a valid user is played.

One approach to detect a spoofing attack is to analyze the presented spoofing image and identify in it the key features, called image quality (IQ) features, and use them to determine whether the presented image is genuine or spoofed; as there is a voice quality measurements [18]. Ref. [19] used 25 such IQ features to distinguish between genuine and spoofed images of a user. In [20] 18 IQ features were used for detecting a spoofing attack and achieved better performance than the one reported in [19]. In [21] an image distortion

method (IDA) was used for detecting a spoofing attack, which is based on four face IQ features, namely, blurriness, color diversity, specular reflection, and chromatic moments.

A very different approach to detect spoofing attack is to use deep learning on the presented images instead of manually extracted image quality features and then using some classifier, like those used in [19–21]. A knowledge discover approaches could also be applied to detect spoofing attacks [22,23]. Convolutional neural networks (CNN) that are able to automatically find the best features present in the images (for labeled data) were successfully used for detecting spoofing face images, as well as for fingerprint, and iris [24–26]. In [27], a semi-supervised learning was used for detecting a spoofing attack using a few labeled data points. Spatiotemporal anti-spoof network (STASN) was proposed in [28] to detect spoofing attacks. In [29] the authors used a bipartite auxiliary supervision network (BASN) for detecting spoofing attacks. In [30] an approach called bi-directional feature pyramid network was proposed for detecting spoofing attacks. In [31] authors proposed a method based on stimulating eye movements using visual stimuli with randomized trajectories. In [32] a head-detection algorithm and deep neural network were used for detecting a spoofing attack. In [33] a hybrid unsupervised and semi-supervised domain adaptation network for cross-scenario face spoofing attack was used. Ref. [34] introduced a CNN based framework with a densely connected network trained using both binary and pixelwise binary supervision (DeepPixBiS) for detecting spoofing attacks. Ref. [35] proposed a method for face anti-spoofing that estimates depth information from multiple RGB frames and proposed a supervised method to efficiently encode spatiotemporal information in a spoofing attack. It included two modules: optical flow-guided feature block and convolutional-gated recurrent unit modules, designed to extract short-term and long-term motion to discriminate between living and spoofing faces. Ref. [28] proposed a face anti-spoofing model with a spatiotemporal attention mechanism fusing global temporal and local spatial information. Ref. [36] proposed Bilateral Convolutional Networks (BCN) that was able to capture intrinsic material-based patterns via aggregating multi-level bilateral macro- and micro- information. Ref. [37] proposed a patch-wise motion parameterization method, which explores the underlying motion difference between the facial movements re-captured from a planar screen and those from a real face.

Indeed, recent studies have revealed that the performance of the state-of-the-art face anti-spoofing methods degrades under the real-world variations (e.g., illumination and camera device variations) [13,38–41], which indicates that more robust face anti-spoofing methods are needed to reach the deployment levels of the face biometric systems. In this paper, we propose a hybrid face spoofing detection system, called Face Anti-Spoofing System Using Image Quality Features and Deep Learning (FASS), that combines a spoofing detection method based on a small number of image quality features with a spoofing detection method based on deep learning at the confidence score level.

2. The Proposed Approach

The proposed approach consists of several parts and is depicted in Figure 1:

1. Extraction of image quality features from the face images.
2. Using these features as input to an SVM and Random Forest (RF) classifiers to determine if a face image is a genuine or a spoofed face.
3. Using ResNet50 deep neural network to do the similar classification.
4. Merging classification confidence scores of both classifiers to make a final determination whether the presented face is genuine or spoofed.
5. If it is a genuine face, it proceeds into the next part of the face verification system [42].

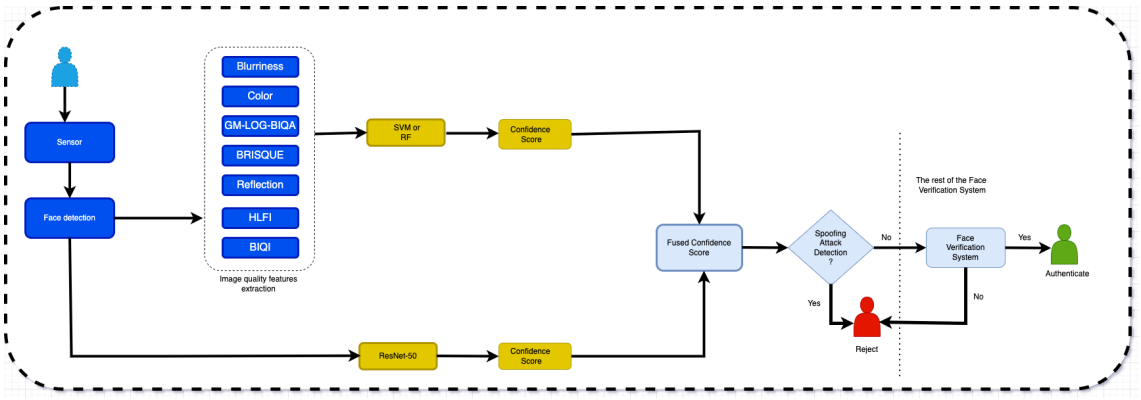

Figure 1. Face Anti-Spoofing System Using Image Quality Features and Deep Learning (FASS) architecture.

2.1. Extracting Image Quality Features

There are two main methods for assessing the quality of a presented image features. One uses the so-called full-reference (FR) and the other uses No-Reference (NR). FR method requires access to the genuine, called reference, image of a valid user and also access to the presented, possibly spoofed, image. Thus, it compares the genuine image with the presented (spoofed) image. In contrast, the NR method is based on using only the presented images. In this work, we only focus on selecting NR image quality features as quite often the reference images are not available.

The authors in [19] proposed a binary classification system to detect spoofing attacks for three biometric modalities (Iris, Fingerprint, and Face), using 25 IQ features. Among them only BIQI, NIQE, JQI and HLFI features are the NR features. In [20] the authors used 18 IQ features for face anti-spoofing, with HLFI being the only NR feature. Ref. [21] proposed a face spoof detection method using four quality features, all of them were NR features.

In Table 1, we have selected and listed 12 NR quality features. To check if these 12 features can be further be reduced, we use the min-Redundancy max-Relevance (mRmR) [43] measure, see Equation (1). It uses mutual information to define relevance and redundancy of features as it seeks to find a set of features that jointly have the maximal statistical dependency on the classification label and minimum redundancy with respect to the selected features. Equation (1) shows how its values are computed for each feature. The best feature is the one with the highest score, second best with the second highest score, etc. The output is a vector of scores for all 12 features. Importantly, we need to take into account that mRmR scoring heavily depends on the data used. Thus, to get a more reliable assessment of the goodness of the features we decided to calculate the mRmR on three datasets, namely, Reply-Attack, CASIA-MFSD and MSU-MFSD to determine the overall importance of features for detecting a spoofing attack.

Next, for the same datasets, in order to determine their best combinations (i.e., the first best feature, the first two best together, the first three best together, etc.) we use a measure called ACER, defined in Equation (4). It is used to evaluate results of the SVM classifier when increasing the number of input features, according to their mRmR order.

$$score_i(f) = \frac{relevance(f|target)}{redundancy(f|features\ selected\ until\ i-1)} \quad (1)$$

$$APCER = \frac{FP}{(TN+FP)} \quad (2)$$

$$BPCER = \frac{FN}{(FN+TP)} \quad (3)$$

where *FP* is false positive, *TN* is true negative, *TP* is true positive and *FN* is false negative.

$$ACER = \frac{(APCER + BPCER)}{2} \quad (4)$$

Table 1. List of the twelve no-reference (NR) image quality (IQ) features.

NR IQ Features Name	Reference
Blind Image Quality Index (BIQI)	[44]
Naturalness Image Quality Estimator (NIQE)	[45]
High-Low Frequency Index (HLFI)	[46]
Reflection	[47]
Blurriness	[48,49]
Chromatic Moment	[50]
Color	[50,51]
Blind/Referenceless Image Spatial QUality Evaluator (BRISQUE)	[52]
Gradient-Magnitude map and Laplacian-of-Gaussian based Blind Image Quality Assessment (GM-LOG-BIQA)	[53]
HDR Image GRADient based Evaluator-1 (HIGRADE-1)	[54]
Robust BRISQUE index (Robustbrisque)	[45]
Distortion Identification-based Image Verity and INtegrity Evaluation (DIIVINE)	[55]

2.2. Selecting the Best Image Quality Features

For the Replay-Attack dataset, the order of best features, according to mRmR, is: Blurriness, Color, GM-LOG-BIQA, BRISQUE, Reflection, HLFI, BIQI, Robustbrisque, Chromatic Moment, DIIVINE, HIGRADE-1, and NIQE, which is shown in Figure 2.

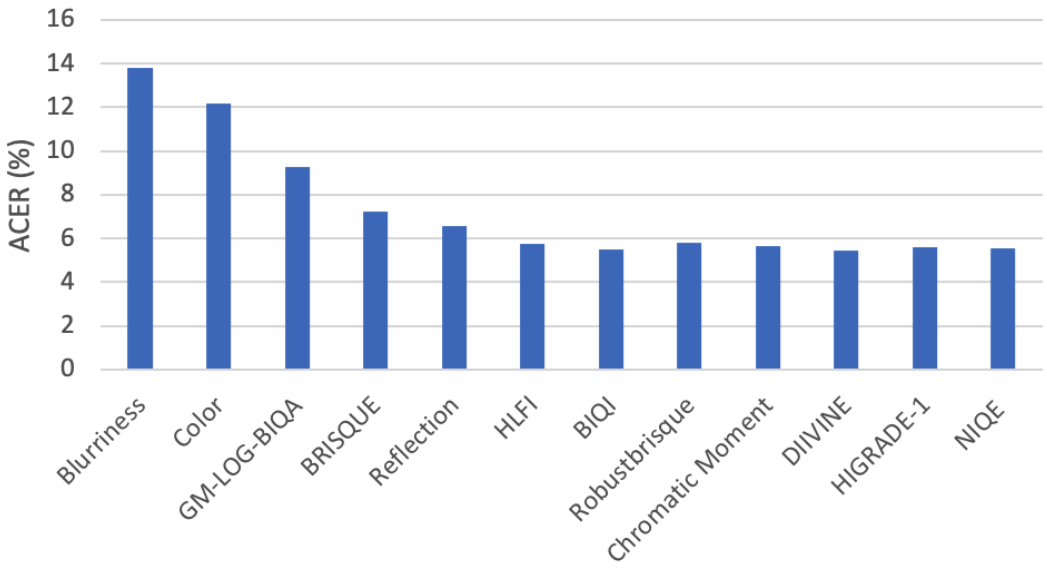

Figure 2. ACER value as it changes with adding additional features for the Replay-Attack dataset.

Notice that after the seventh feature, the error rate goes slightly up before slightly going down when 10 features are used. We thus choose the first seven features, namely, Blurriness, Color, GM-LOG-BIQA, BRISQUE, Reflection, HLFI and BIQI.

For the CASIA-MFSD dataset, the mRmR order of feature is: Blurriness, Color, HLFI, BRISQUE, GM-LOG-BIQA, Reflection, BIQI, Chromatic Moment, Robustbrisque, HIGRADE-1, NIQE and DIIVINE, shown in Figure 3.

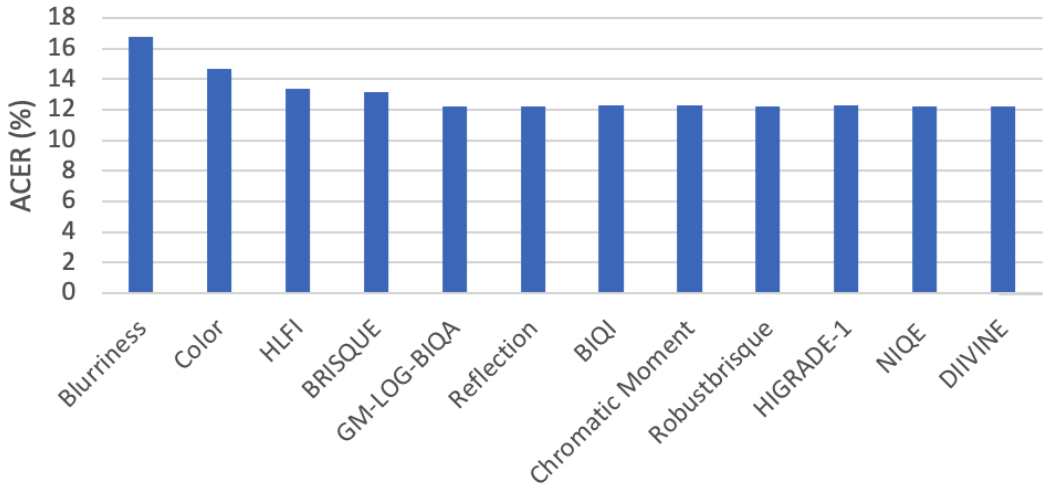

Figure 3. ACER value as it changes with adding additional features for the CASIA-MFSD dataset.

We see that after the first 5 features are combined, namely, Blurriness, Color, HLFI, BRISQUE, and GM-LOG-BIQA, ACER value remains the same, thus we chose these five features.

For the MSU-MFSD dataset, the mRmR order of features is: Blurriness, Color, BRISQUE, GM-LOG-BIQA, BIQI, Reflection, HLFI, Chromatic Moment, HIGRADE-1, Robustbrisque, NIQE and DIIVINE, shown in Figure 4.

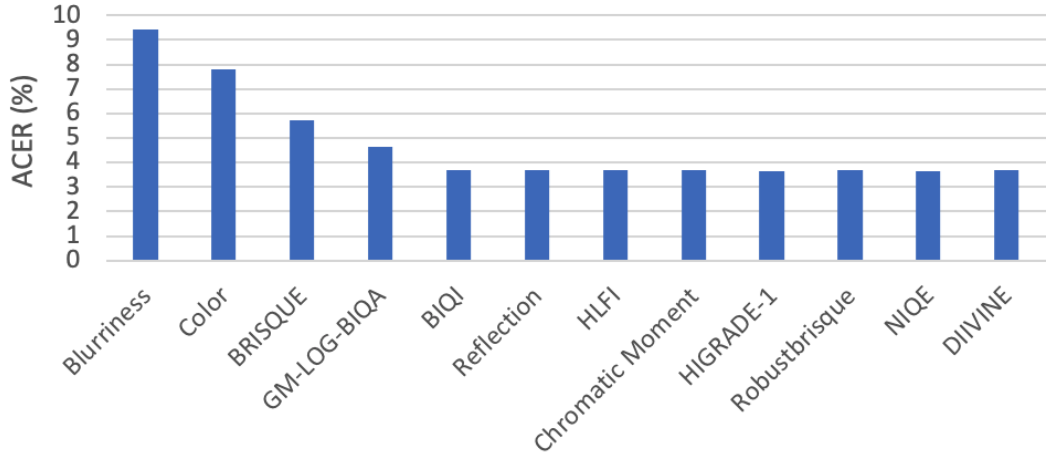

Figure 4. ACER value as it changes with adding additional features for the MSU-MFSD dataset.

We see that the ACER remains about the same after using the first six features: Blurriness, Color, BRISQUE, GM-LOG-BIQA, BIQI and Reflection.

The combined list of best features from the above experiments is Blurriness, Color, GM-LOG-BIQA, BRISQUE, Reflection, HLFI, and BIQI. These seven features are described below.

Blurriness for short distance spoof attacks, spoof faces are often defocused in mobile phone cameras. The reason is that the spoofing medium (printed paper and screen) usually is of limited size, and the attacker must place them close to the camera to obscure the boundaries of the attack medium. As a result, spoof faces are defocused, and the resulting image blur can be used as indication for anti-spoofing [48,49].

Color is an important difference between genuine and spoof faces is the color diversity, as genuine faces have richer colors. This diversity fades out in spoof faces due to the color reproduction loss during image/video recapture [50].

GM-LOG-BIQA defines local spatial contrast features that characterize various perceptual image structures related to luminance discontinuities. The Gradient Magnitude (GM) captures the local changes of luminance, while the Laplacian of Gaussian (LOG) is sensitive to local intensity contrast and BIQA is blind image quality assessment which means it doesn't require a reference image to measure the quality of the image [53].

BRISQUE is a Blind/Referenceless Image Spatial Quality Estimator. Its features are derived from the empirical distribution of locally normalized luminance values and their products under a spatial natural scene statistic and they follow a Gaussian-like distribution. These features are then used in support vector regression to map image features to an image quality score [45].

Reflection degrade the quality of face images/videos by obstructing the background scenes.The existence of a reflection component in an image will not only change the color of the object surface but also destroy its edge contour, but the saturated reflection will also lead to the complete loss of image texture information, which provides a good clue for anti-spoofing tasks [56].

HLFI is a High-Low Frequency Index, which uses local gradients as a blind metric to detect blur and noise. It is sensitive to the sharpness of the image, which is done by computing the difference between the power in the lower and upper frequencies of the Fourier Spectrum [46].

BIQI is Blind Image Quality Indices which is a two-step no-reference image quality measurement. Given a distorted image, the first step performs the wavelet transform and extracts features for estimation of the presence of image distortions and it evaluates the quality of the image across these distortions by applying support vector regression on the wavelet coefficients [44].

2.3. Fusing the Classifiers Results

The FASS system (see Figure 1) fuses the results of the SVM and random forest (RF) classifiers (separately) that uses the selected above seven NR quality features with the result of the ResNet50 algorithm that operates directly on raw input images for detecting a face spoofing attack.

The confidence scores of two classifiers are combined in a weighted fashion according to Equation (5).

The fused confidence score is calculated as follows:

$$FS = (\alpha * \Theta_x\ ) + ((1 - \alpha) * \Theta_y\ ) \tag{5}$$

where FS is the fused confidence score, Θ_x is ResNet-50 confidence score, Θ_y is SVM or Random Forest (RF) confidence score and α is the weight parameter.

To find the best weight values for ResNet-50 and image quality features, we experimented with different values for the weight on the validation part of replay-attack dataset as it is shown in Figure 5. The figure shows that the fusion of image quality features with ResNet-50 using different weight values provides better EER. Since the best EER value is found when the weight is 0.75, we have used weight of 0.75 for the results reported in all experimental tables.

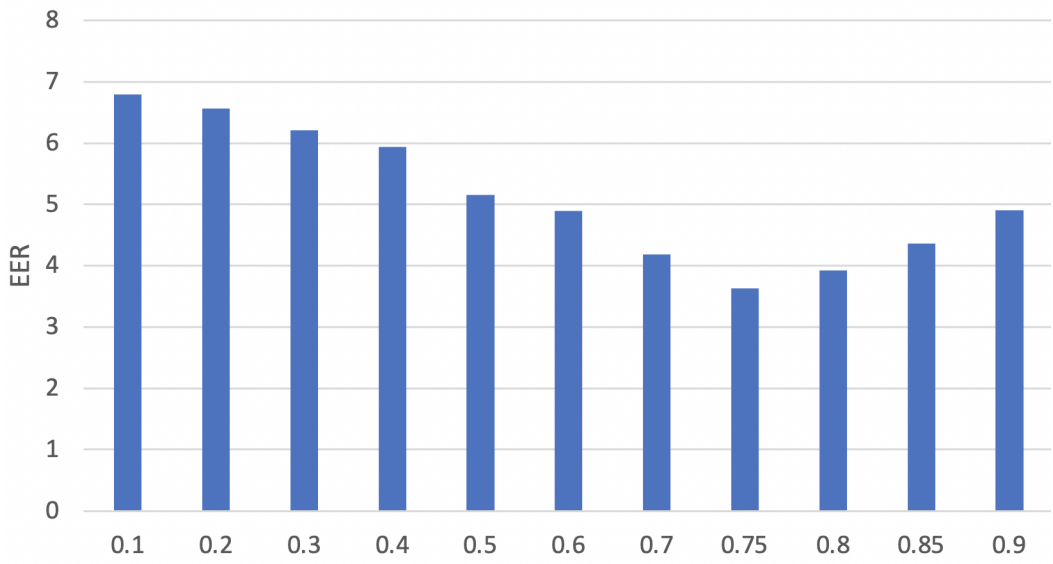

Figure 5. EER value as the weight changes for the replay-attack dataset.

3. Experiments

3.1. Experimental Setup

The Pytorch library [57] was used for implementing the FASS system. All experiments were run for 100 epochs or until the validation error stopped decreasing, whichever was sooner, and using a batch size of 64. Stochastic gradient descent with momentum (0.9), weight decay (5×10^{-4}) and a logarithmically decaying learning rate (initialized to 10^{-2} and decaying to 10^{-8}) were used.

Five face spoofing datasets, namely, Replay-Attack [58], CASIA-FASD [59], MSU-MFSD [21], Oulu-NPU [60] and SiW [61] were used to evaluate FASS and compare its results with the state-of-the-art results. Multi-Task Cascaded Convolutional Neural Network [62] was used to detect faces from the video frames. The face images of all five datasets were resized to the size 224 × 224 px for computational efficiency. We used data partitions into the train-validate-test as detailed in the data descriptions below.

3.2. Datasets

Five face anti-spoofing benchmark datasets, namely, Replay-Attack [58], CASIA-FASD [59], MSU-MFSD [21], Oulu-NPU [60] and SiW [61], were used.

Replay-Attack dataset consists of 1200 video clips of photo and video spoof attempts of 50 users, under different lighting conditions. Training set has 60 genuine and 300 spoof users. Validation set has 60 genuine and 300 spoof images. Test set has 80 genuine and 400 spoof images.

CASIA-MFSD contains 50 users video clips under different resolutions and light conditions. Three spoof face attacks are implemented, which include warped photo attack, cut photo attack and video attack. The dataset contains 600 video clips, in which 120 videos for training, 120 videos for validation and 360 videos for testing are used.

MSU-MFSD dataset has 280 video clips of genuine and spoof faces from 35 users. Two cameras with different resolutions (720 × 480 and 640 × 480) were used to record the videos from the 35 users. The 280 videos were divided into training (60 videos), validation (60 videos) and testing (160 videos) datasets, respectively.

Oulu-NPU dataset consists of 4950 video clips and has four testing protocols: Protocol 1 evaluates the effect of the illumination variations; Protocol 2 evaluates the effect of spoofing attack instrument variations; Protocol 3 evaluates the effect of camera device variations; and Protocol 4 is a combination of the three protocols. For all protocols, the 4950 video clips were divided into three disjoint subsets for training, validation and testing, namely, 1800, 1350 and 1800, respectively.

SiW dataset has genuine and spoof videos from 165 users. It has three protocols. The first protocol evaluates the generalization of the face attack detection under different face poses and expressions. The second protocol evaluates the generalization capability on cross-medium of the same spoof type. The third protocol evaluates the performance on an unknown attack. We used 45, 45 and 75 users for training, validation and testing, respectively.

3.3. Evaluation Metrics

Performance of biometric verification systems depends on accuracy of acceptance/rejection of the analyzed image [63,64]. The measures used are false acceptance rate (FAR), Equation (6), and false rejection rate (FRR), Equation (7). FAR is the ratio of incorrectly accepted spoofing attack faces, whereas FRR is the ratio of incorrectly rejected genuine faces. The commonly used metric in anti-spoofing literature is Half Total Error Rate (HTER), Equation (8), while Equal Error Rate (EER) is a value of HTER at which FAR and FRR have the same values.

The other metrics used in ISO standard [65] are: Attack Presentation Classification Error Rate (APCER), Equation (2), Bona fide Presentation Classification Error Rate (BPCER), Equation (3) and Average Classification Error Rate (ACER) Equation (4). BPCER (Equation (3)) and APCER (Equation (2)) measure genuine and spoof classification error rates, respectively. ACER (Equation (4)) summarizes the two measures.

$$FAR = \frac{FP}{Spoof\ Samples} \tag{6}$$

$$FRR = \frac{FN}{Genuine\ Samples} \tag{7}$$

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

where FP is false positive and FN is false negative.

3.4. Results of Using the Quality Features on the Replay-Attack, CASIA-MFSD and MSU-MFSD Datasets

Table 2 compares FASS results with other algorithms that use different numbers of image quality features, namely, 4, 25 and 18 features.

Table 2. The results of using image quality features (Reference (R) and No-Reference (RN)) on Replay-Attack, CASIA-MFSD and MSU-MFSD datasets.

Methods	No. of R + NR Quality Features	HTER (%) on Replay Attack	EER (%) on CASIA-MFSD	EER (%) on MSU-MFSD
IDA [21]	4 NR	7.41	13.3	8.58
Galbally et al. [19]	21 R + 4 NR	15.2	-	-
Costa-Pazo et al. [20]	17 R + 1 NR	5.28	-	-
FASS with RF	7 NR	**4.3**	**7.02**	6.51
FASS with SVM	7 NR	5.02	7.17	**6.48**

As it is shown in the table, we compare our two proposed methods (i.e., FASS with Random Forest (RF) and FASS with SVM) with the other three algorithms in order to see the classification accuracy of RF and SVM methods.

We notice in Table 2 that FASS performs better results than the other systems on three datasets. FASS with RF and FASS with SVM result in 18.18% and 4.9% HTER relative improvement when compared with [20], respectively. Comparison with the CASA-MFSD dataset, FASS with RF and FASS with SVM provide 47.2% and 46% relative EER improvement over [21], respectively. Compared with [21], FASS with RF and FASS with SVM gave 24.1% and 24.5% relative EER improvement on the MSU-MFSD dataset, respectively.

These results show that the selected seven no-reference image quality features are good for detecting face spoofing attacks. Both RF and SVM classification methods provide more or less similar results. While RF classification has the best results on Replay Attack and CASIA-MFSD dataset, SVM classification has the best result on MSU-MFSD.

For the Replay-Attack dataset, only HTER results are reported in the literature and, for CASIA-MFSD and MSU-MFSD datasets only EER results are reported, thus we used them in our comparisons.

3.5. Results on OULU-NPU Dataset

Table 3 shows the results of the FASS and other state-of-the-art systems for anti-spoofing, for four different protocols on the OULU-NPU dataset.

Table 3. The results using four protocols on the OULU-NPU dataset.

Protocol	Method	APCER (%)	BPCER (%)	ACER (%)
1	GRADIANT [66]	1.3	12.5	6.9
	DeepPixBiS [34]	0.8	**0.0**	**0.4**
	STASN [28]	1.2	2.5	1.9
	Auxiliary [61]	1.6	1.6	1.6
	CPqD [66]	2.9	10.8	6.9
	FaceDs [67]	1.2	1.7	1.5
	MILHP [37]	8.3	0.8	4.6
	BASN [29]	1.5	5.8	3.6
	FAS-TD [35]	2.5	**0.0**	1.3
	FASS with RF	**0.3**	0.5	0.6
	FASS with SVM	**0.3**	1.5	0.9
2	DeepPixBiS [34]	11.4	0.6	6.0
	Auxiliary [61]	2.7	2.7	2.7
	GRADIANT [66]	3.1	1.9	2.5
	STASN [28]	4.2	**0.3**	2.2
	FAS-TD [35]	**1.7**	2.0	1.9
	FaceDs [67]	4.2	4.4	4.3
	MILHP [37]	5.6	5.3	5.4
	BASN [29]	2.4	3.1	2.7
	FASS with RF	2.1	0.7	1.7
	FASS with SVM	1.8	1.3	**1.6**
3	DeepPixBiS [34]	11.7 ± 19.6	10.6 ± 14.1	11.1 ± 9.4
	FAS-TD [35]	5.9 ± 1.9	5.9 ± 3.0	5.9 ± 1.0
	GRADIANT[66]	2.6 ± 3.9	5.0 ± 5.3	3.8 ± 2.4
	FaceDs [67]	4.0 ± 1.8	3.8 ± 1.2	3.6 ± 1.6
	Auxiliary [61]	2.7 ± 1.3	3.1 ± 1.7	2.9 ± 1.5
	MILHP [37]	**1.5 ± 1.2**	6.4 ± 6.6	4.0 ± 2.9
	BASN [29]	1.8 ± 1.1	3.6 ± 3.5	2.7 ± 1.6
	STASN [28]	4.7 ± 3.9	**0.9 ± 1.2**	2.8 ± 1.6
	FASS with RF	1.9 ± 1.7	1.2 ± 1.2	**1.7 ± 0.3**
	FASS with SVM	2.0 ± 1.4	1.8 ± 1.3	1.9 ± 0.6
4	DeepPixBiS [34]	36.7 ± 29.7	13.3 ± 14.1	25.0 ± 12.7
	GRADIANT [66]	5.0 ± 4.5	15.0 ± 7.1	10.0 ± 5.0
	Auxiliary [61]	9.3 ± 5.6	10.4 ± 6.0	9.5 ± 6.0
	FAS-TD [35]	14.2 ± 8.7	**4.2 ± 3.8**	9.2 ± 3.4
	STASN [28]	6.7 ± 10.6	8.3 ± 8.4	7.5 ± 4.7
	MILHP [37]	15.8 ± 12.8	8.3 ± 15.7	12.0 ± 6.2
	FaceDs [67]	5.1 ± 6.3	6.1 ± 5.1	5.6 ± 5.7
	FASS with RF	**4.0 ± 3.6**	5.6 ± 3.5	**5.2 ± 1.9**
	FASS with SVM	4.3 ± 4.5	6.4 ± 5.7	5.4 ± 3.2

Similarly to Table 2, our two methods (i.e., FASS with RF and FASS with SVM) are compared with other reported results in terms of accuracy.

From Table 3, we see that FASS gave the best APCER (Equation (2)) value of all anti-spoofing systems on protocol 1. Compared with DeepPixBiS, FASS shows 62.5% relative improvement. However, FASS is not as good using BPCER (Equation (3)) and ACER (Equation (4)) measures as DeepPixBiS.

FASS with SVM gives the best ACER (Equation (4)) value on protocol 2. Compared with FAS-TD, FASS with SVM shows 15.8% relative ACER (Equation (4)) improvement. It

has almost the same APCER (Equation (2)) value as FAS-TD. However, it lags behind the STASN on BPCER (Equation (3)).

Using protocol 3, Table 3 shows that the FASS with RF system gives the best ACER (Equation (4)) value, however, it does not have the best APCER (Equation (2)) and BPCER (Equation (3)) values.

On protocol 4, FASS with RF gives the best APCER (Equation (2)) and ACER (Equation (4)) values. However, FASS is not as good as the FAS-TD system using BPCER (Equation (3)) measure.

3.6. Results on SiW Dataset

Similarly, we compared (Table 4) the FASS system on SiW dataset on its 3 different protocols using two classifications (i.e., FASS with RF and FASS with SVM).

Table 4. The results using three protocols on the SiW dataset.

Protocol	Method	APCER (%)	BPCER (%)	ACER (%)
1	Auxiliary [61]	3.58	3.58	3.58
	STASN [28]	–	–	1.00
	FAS-TD [35]	0.96	0.50	0.73
	BASN [29]	-	-	0.37
	BCN [36]	0.55	**0.17**	0.36
	FASS with RF	**0.46**	0.18	**0.31**
	FASS with SVM	0.49	0.19	0.34
2	Auxiliary [61]	0.57 ± 0.69	0.57 ± 0.69	0.57 ± 0.69
	STASN [28]	–	–	0.28 ± 0.05
	FAS-TD [35]	**0.08 ± 0.14**	0.21 ± 0.14	0.15 ± 0.14
	BASN [29]	-	-	0.12 ± 0.03
	BCN [36]	**0.08 ± 0.17**	0.15 ± 0.00	**0.11 ± 0.08**
	FASS with RF	0.11 ± 0.31	0.14 ± 0.10	0.12 ± 0.02
	FASS with SVM	0.15 ± 0.10	**0.13 ± 0.10**	0.14 ± 0.03
3	STASN [28]	–	–	12.10 ± 1.50
	Auxiliary [61]	8.31 ± 3.81	8.31 ± 3.80	8.31 ± 3.81
	FAS-TD [35]	3.10 ± 0.81	3.09 ± 0.81	3.10 ± 0.81
	BASN [29]	-	-	6.45 ± 1.80
	BCN [36]	2.55 ± 0.89	2.34 ± 0.47	2.45 ± 0.68
	FASS with RF	**2.29 ± 0.24**	2.01 ± 0.15	**2.03 ± 0.17**
	FASS with SVM	2.33 ± 0.17	**1.98 ± 0.14**	2.15 ± 0.13

We can see, FASS with RF and FASS with SVM had 18.1% 10.9% relative APCER (Equation (2)) improvement when compared with BCN, respectively. Similarly, FASS with RF had the best ACER (Equation (4)) result on protocol 1. FASS with SVM provided the second best ACER (Equation (4)) value on protocol 1.

On protocol 2, both of FASS's performance using RF and SVM classification methods was not good in terms of APCER (Equation (2)) when compared with FAS-TD and BCN, however, FASS with SVM was the best performing and FASS with RF is the second best performing in terms of BPCER (Equation (3)).

As it is shown in Table 4, FASS with RF gives us the best APCER value (i.e., 2.29%) and the best ACER value (i.e., 2.03%). Similarly, FASS with SVM had the best result on BPCER (1.98%).

Overall, FASS with RF compared with five state-of-the-art methods on this dataset performed almost the best in terms of ACER (Equation (4)) on all three protocols (0.31%, 0.12%, and 2.03% respectively). These results show good generalization of FASS for variations of face pose and expression, and for different spoof mediums.

3.7. Results of Cross-Dataset Testing between CASIA-MFSD and Replay-Attack Datasets

Table 5 shows the results of testing using HTER measure for cross-dataset testing (trained on CASIA-MFSD but tested on Replay-Attack dataset), and vice versa. We see that FASS with RF gives us the best result when trained on CASIA-MFSD data and tested on Replay-Attack data. FASS with RF provides us a 45.18% HTER relative improvement

compared to BCN system. However, both FASS with RF and FASS with SVM did not give the best results when trained on Replay-Attack but evaluated on CASIA-MFSD dataset. On average, however, they gave better results compared to the other state-of-art system results. The results of Table 5 indicate that FASS generalizes well, different from a different distribution.

Table 5. Comparison of cross-dataset testing between CASIA-MFSD and Replay-Attack datasets.

Method	Train: CASIA-MFSD Test: Replay-Attack	Train: Replay-Attack Test: CASIA-MFSD
Motion-Mag [68]	50.1	47.0
LBP-TOP [69]	49.7	60.6
STASN [28]	31.5	30.9
Auxiliary [61]	27.6	28.4
FAS-TD [35]	17.5	**24.0**
LBP [51]	47.0	39.6
Spectral cubes [70]	34.4	50.0
BCN [36]	16.6	36.4
BASN [29]	23.6	29.9
FaceDs [67]	28.5	41.1
FASS with RF	**9.1**	24.5
FASS with SVM	9.7	25.6

While a number of face spoof detection techniques have been proposed, their generalization abilities are still to be improved. We propose an efficient face spoof detection system called FASS which is based on fusing the scores of the two classifiers such as SVM/RF and ResNet50.

4. Conclusions

Genuine face image and a spoof face image are very similar although careful visual inspection can find small differences between the two. It is thus reasonable to assume that the image quality features can be identified and used to automatically distinguish between genuine and spoof images.

Following this assumption, we identified seven no-reference face image quality features to be used in spoof detection systems. These features are Blurriness, Color, GM-LOG-BIQA, BRISQUE, Reflection, HLFI, and BIQI. We then introduced a novel face anti-spoofing system, FASS, that uses these no-reference image quality features as an input to the SVM and RF classifiers. It also uses the original images as input to the deep learning ResNet50 classifier and then combines their results. While deep learning classifiers in general perform better than classifiers that use image quality features extracted from images, the results of FASS show that by fusing the outputs of different classifiers that use different feature inputs improves the overall accuracy.

FASS was evaluated on the Replay-Attack, CASIA-MFSD, MSU-MFSD, OULU-NPU and SiW face anti-spoof benchmark datasets and it was demonstrated that the fusion of ResNet50 and SVM/RF results improved detection of face spoofing attacks. FASS performed better than several of the state-of-the-art systems during both intra-datasets and extra-datasets testing. These results confirm the usefulness of the identified seven no-reference image quality features, which can be used by others in their anti-spoofing research.

Author Contributions: Conceptualization, E.S. and K.J.C.; methodology, E.S. and K.J.C.; software, E.S.; validation, E.S. and K.J.C.; formal analysis, E.S. and K.J.C.; investigation, E.S.; resources, E.S. and K.J.C.; data curation, E.S.; writing—original draft preparation, E.S. and K.J.C.; writing—review and editing, E.S. and K.J.C.; visualization, E.S.; supervision, K.J.C.; project administration, K.J.C. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: Replay-Attack (https://www.idiap.ch/en/dataset/replayattack), CASIA-FASD (https://www.idiap.ch/software/bob/docs/bob/bob.db.casia_fasd/v2.0.5/py_api.html), MSU-MFSD (https://www.v7labs.com/open-datasets/msu-mfsd), Oulu-NPU (https://www.idiap.ch/software/

bob/docs/bob/bob.db.oulunpu/master/index.html), SiW (http://cvlab.cse.msu.edu/siw-spoof-in-the-wild-database.html).

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

References

1. Hadid, A.; Evans, N.; Marcel, S.; Fierrez, J. Biometrics systems under spoofing attack: An evaluation methodology and lessons learned. *IEEE Signal Process. Mag.* **2015**, *32*, 20–30. [CrossRef]
2. Woubie, A.; Bäckström, T. Voice Quality Features for Replay Attack Detection. In Proceedings of the 2022 30th European Signal Processing Conference (EUSIPCO), Belgrade, Serbia, 29 August–2 September 2022; pp. 384–388.
3. Rathgeb, C.; Drozdowski, P.; Busch, C. Makeup presentation attacks: Review and detection performance benchmark. *IEEE Access* **2020**, *8*, 224958–224973. [CrossRef]
4. Abdullakutty, F.; Elyan, E.; Johnston, P. A review of state-of-the-art in Face Presentation Attack Detection: From early development to advanced deep learning and multi-modal fusion methods. *Inf. Fusion* **2021**, *75*, 55–69. [CrossRef]
5. Fang, M.; Damer, N.; Kirchbuchner, F.; Kuijper, A. Real masks and spoof faces: On the masked face presentation attack detection. *Pattern Recognit.* **2022**, *123*, 108398. [CrossRef]
6. Muhammad, U.; Yu, Z.; Komulainen, J. Self-supervised 2D face presentation attack detection via temporal sequence sampling. *Pattern Recognit. Lett.* **2022**, *156*, 15–22. [CrossRef]
7. Li, Z. Cross-Domain Face Presentation Attack Detection Techniques with Attention to Genuine Faces. Ph.D. Thesis, Nanyang Technological University, Singapore, 2023.
8. Nóbrega, M. Explainable and Interpretable Face Presentation Attack Detection Methods. Ph.D. Thesis, Faculdade de Engenharia da Universidade do Porto, Porto, Portugal, 2021.
9. Micheletto, M. Fusion of Fingerprint Presentation Attacks Detection and Matching: A Real Approach from the LivDet Perspective. Master's Thesis, Università degli Studi di Cagliari, Cagliari, Italy, 2023.
10. Benlamoudi, A. Multi-Modal and Anti-Spoofing Person Identification. Ph.D. Thesis, University of Kasdi Merbah, Ouargla, Algeria, 2018.
11. Marcel, S.; Nixon, M.; Fierrez, J.; Evans, N. *Handbook of Biometric Anti-Spoofing: Presentation Attack Detection*; Springer: Berlin/Heidelberg, Germany, 2019.
12. Marcel, S.; Nixon, M.; Li, S. *Handbook of Biometric Anti-Spoofing: Trusted Biometrics under Spoofing Attacks*; Springer: Berlin/Heidelberg, Germany, 2014.
13. Liu, S.; Yuen, P. Recent Progress on Face Presentation Attack Detection of 3D Mask Attack. In *Handbook of Biometric Anti-Spoofing: Presentation Attack Detection and Vulnerability Assessment*; Springer: Berlin/Heidelberg, Germany, 2023; pp. 231–259.
14. Busch, C. Related Standards. In *Handbook of Biometric Anti-Spoofing: Trusted Biometrics under Spoofing Attacks*; Springer: Berlin/Heidelberg, Germany, 2014; pp. 205–215.
15. Chingovska, I.; Yang, J.; Lei, Z.; Yi, D.; Li, S.; Kahm, O.; Glaser, C.; Damer, N.; Kuijper, A.; Nouak, A.; et al. The 2nd competition on counter measures to 2D face spoofing attacks. In Proceedings of the 2013 International Conference on Biometrics (ICB), Madrid, Spain, 4–6 June 2013; pp. 1–6.
16. Ghiani, L.; Yambay, D.; Mura, V.; Tocco, S.; Marcialis, G.; Roli, F.; Schuckcrs, S. Livdet 2013 fingerprint liveness detection competition 2013. In Proceedings of the 2013 International Conference on Biometrics (ICB), Madrid, Spain, 4–6 June 2013; pp. 1–6.
17. Czajka, A. Pupil dynamics for iris liveness detection. *IEEE Trans. Inf. Forensics Secur.* **2015**, *10*, 726–735. [CrossRef]
18. Woubie, A.; Luque, J.; Hernando, J. Using voice-quality measurements with prosodic and spectral features for speaker diarization. In Proceedings of the Sixteenth Annual Conference of the International Speech Communication Association, Dresden, Germany, 6–10 September 2015.
19. Galbally, J.; Marcel, S.; Fierrez, J. Image quality assessment for fake biometric detection: Application to iris, fingerprint, and face recognition. *IEEE Trans. Image Process.* **2013**, *23*, 710–724. [CrossRef]
20. Costa-Pazo, A.; Bhattacharjee, S.; Vazquez-Fernandez, E.; Marcel, S. The replay-mobile face presentation-attack database. In Proceedings of the 2016 International Conference of the Biometrics Special Interest Group (BIOSIG), Darmstadt, Germany, 21–23 September 2016; pp. 1–7.
21. Wen, D.; Han, H.; Jain, A. Face spoof detection with image distortion analysis. *IEEE Trans. Inf. Forensics Secur.* **2015**, *10*, 746–761. [CrossRef]
22. Cios, K.J.; Shin, I. Image recognition neural network: IRNN. *Neurocomputing* **1995**, *7*, 159–185. [CrossRef]
23. Cios, K.J.; Swiniarski, R.; Pedrycz, W.; Kurgan, L.; Cios, K.J.; Swiniarski, R.; Pedrycz, W.; Kurgan, L. The knowledge discovery process. In *Data Mining: A Knowledge Discovery Approach*; Springer: Berlin, Germany, 2007; pp. 9–24.
24. Galbally, J.; Marcel, S.; Fierrez, J. Biometric antispoofing methods: A survey in face recognition. *IEEE Access* **2014**, *2*, 1530–1552. [CrossRef]
25. Menotti, D.; Chiachia, G.; Pinto, A.; Schwartz, W.; Pedrini, H.; Falcao, A.; Rocha, A. Deep representations for iris, face, and fingerprint spoofing detection. *IEEE Trans. Inf. Forensics Secur.* **2015**, *10*, 864–879. [CrossRef]
26. Cios, K.J. Deep neural networks—A brief history. In *Advances in Data Analysis with Computational Intelligence Methods: Dedicated to Professor Jacek Żurada*; Springer: Berlin, Germany, 2018; pp. 183–200.

27. Quan, R.; Wu, Y.; Yu, X.; Yang, Y. Progressive transfer learning for face anti-spoofing. *IEEE Trans. Image Process.* **2021**, *30*, 3946–3955. [CrossRef]
28. Yang, X.; Luo, W.; Bao, L.; Gao, Y.; Gong, D.; Zheng, S.; Li, Z.; Liu, W. Face anti-spoofing: Model matters, so does data. In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition 2019, Long Beach, CA, USA, 15–20 June 2019; pp. 3507–3516.
29. Kim, T.; Kim, Y.; Kim, I.; Kim, D. Basn: Enriching feature representation using bipartite auxiliary supervisions for face anti-spoofing. In Proceedings of the IEEE/CVF International Conference on Computer Vision Workshops, Seoul, Republic of Korea, 27–28 October 2019.
30. Roy, K.; Hasan, M.; Rupty, L.; Hossain, M.; Sengupta, S.; Taus, S.; Mohammed, N. Bi-fpnfas: Bi-directional feature pyramid network for pixel-wise face anti-spoofing by leveraging fourier spectra. *Sensors* **2021**, *21*, 2799. [CrossRef]
31. Ali, A.; Hoque, S.; Deravi, F. Directed Gaze Trajectories for biometric presentation attack detection. *Sensors* **2021**, *21*, 1394. [CrossRef]
32. Kowalski, M. A study on presentation attack detection in thermal infrared. *Sensors* **2020**, *20*, 3988. [CrossRef]
33. Jia, Y.; Zhang, J.; Shan, S.; Chen, X. Unified unsupervised and semi-supervised domain adaptation network for cross-scenario face anti-spoofing. *Pattern Recognit.* **2021**, *115*, 107888. [CrossRef]
34. George, A.; Marcel, S. Deep pixel-wise binary supervision for face presentation attack detection. In Proceedings of the 2019 International Conference on Biometrics (ICB), Crete, Greece, 4–7 June 2019; pp. 1–8.
35. Wang, Z.; Zhao, C.; Qin, Y.; Zhou, Q.; Qi, G.; Wan, J.; Lei, Z. Exploiting temporal and depth information for multi-frame face anti-spoofing. *arXiv* **2018**, arXiv:1811.05118.
36. Yu, Z.; Li, X.; Niu, X.; Shi, J.; Zhao, G. Face anti-spoofing with human material perception. In Proceedings of the European Conference on Computer Vision, Online, 23–28 August 2020; pp. 557–575.
37. Lin, C.; Liao, Z.; Zhou, P.; Hu, J.; Ni, B. Live Face Verification with Multiple Instantialized Local Homographic Parameterization. In Proceedings of the 27th International Joint Conference on Artificial Intelligence (IJCAI-18), Stockholm, Sweden, 13–19 July 2018; pp. 814–820.
38. Yu, Z.; Qin, Y.; Li, X.; Zhao, C.; Lei, Z.; Zhao, G. Deep learning for face anti-spoofing: A survey. *IEEE Trans. Pattern Anal. Mach. Intell.* **2022**, *45*, 5609–5631. [CrossRef]
39. Wang, C.; Lu, Y.; Yang, S.; Lai, S. PatchNet: A simple face anti-spoofing framework via fine-grained patch recognition. In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, New Orleans, LA, USA, 18–24 June 2022; pp. 20281–20290.
40. Wang, C.; Yu, B.; Zhou, J. A Learnable Gradient operator for face presentation attack detection. *Pattern Recognit.* **2023**, *135*, 109146. [CrossRef]
41. Wang, Z.; Wang, Z.; Yu, Z.; Deng, W.; Li, J.; Gao, T.; Wang, Z. Domain generalization via shuffled style assembly for face anti-spoofing. In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, New Orleans, LA, USA, 18–24 June 2022; pp. 4123–4133.
42. Solomon, E.; Woubie, A.; Cios, K.J. UFace: An Unsupervised Deep Learning Face Verification System. *Electronics* **2022**, *11*, 3909. [CrossRef]
43. Peng, H.; Long, F.; Ding, C. Feature selection based on mutual information criteria of max-dependency, max-relevance, and min-redundancy. *IEEE Trans. Pattern Anal. Mach. Intell.* **2005**, *27*, 1226–1238. [CrossRef] [PubMed]
44. Moorthy, A.; Bovik, A. A modular framework for constructing blind universal quality indices. *IEEE Signal Process. Lett.* **2009**, *17*, 7.
45. Mittal, A.; Moorthy, A.; Bovik, A. Making image quality assessment robust. In Proceedings of the 2012 Conference Record of the Forty Sixth Asilomar Conference on Signals, Systems and Computers (ASILOMAR), Pacific Grove, CA, USA, 4–7 November 2012; pp. 1718–1722.
46. Zhu, X.; Milanfar, P. A no-reference sharpness metric sensitive to blur and noise. In Proceedings of the 2009 International Workshop on Quality of Multimedia Experience, San Diego, CA, USA, 29–31 July 2009; pp. 64–69.
47. Gao, X.; Ng, T.; Qiu, B.; Chang, S. Single-view recaptured image detection based on physics-based features. In Proceedings of the 2010 IEEE International Conference on Multimedia and Expo, Singapore, 19–23 July 2010; pp. 1469–1474.
48. Crete, F.; Dolmiere, T.; Ladret, P.; Nicolas, M. The blur effect: Perception and estimation with a new no-reference perceptual blur metric. *Hum. Vis. Electron. Imaging XII* **2007**, *6492*, 196–206.
49. Marziliano, P.; Dufaux, F.; Winkler, S.; Ebrahimi, T. A no-reference perceptual blur metric. In Proceedings of the International Conference on Image Processing, Rochester, NY, USA, 22–25 September 2002; Volume 3, p. 3.
50. Chen, Y.; Li, Z.; Li, M.; Ma, W. Automatic classification of photographs and graphics. In Proceedings of the 2006 IEEE International Conference on Multimedia and Expo, Toronto, ON, Canada, 9–12 July 2006; pp. 973–976.
51. Boulkenafet, Z.; Komulainen, J.; Hadid, A. Face anti-spoofing based on color texture analysis. In Proceedings of the 2015 IEEE International Conference on Image Processing (ICIP), Quebec City, QC, Canada, 17–30 September 2015; pp. 2636–2640.
52. Mittal, A.; Moorthy, A.; Bovik, A. No-reference image quality assessment in the spatial domain. *IEEE Trans. Image Process.* **2012**, *21*, 4695–4708. [CrossRef]
53. Xue, W.; Mou, X.; Zhang, L.; Bovik, A.; Feng, X. Blind image quality assessment using joint statistics of gradient magnitude and Laplacian features. *IEEE Trans. Image Process.* **2014**, *23*, 4850–4862. [CrossRef]

54. Kundu, D.; Ghadiyaram, D.; Bovik, A.; Evans, B. No-reference image quality assessment for high dynamic range images. In Proceedings of the 2016 50th Asilomar Conference on Signals, Systems and Computers, Pacific Grove, CA, USA, 6–9 November 2016; pp. 1847–1852.
55. Moorthy, A.; Bovik, A. Blind image quality assessment: From natural scene statistics to perceptual quality. *IEEE Trans. Image Process.* **2011**, *20*, 3350–3364. [CrossRef]
56. Tan, R.; Ikeuchi, K. Separating reflection components of textured surfaces using a single image. In *Digitally Archiving Cultural Objects*; Springer: Berlin, Germany, 2008; pp. 353–384.
57. Paszke, A.; Gross, S.; Massa, F.; Lerer, A.; Bradbury, J.; Chanan, G.; Killeen, T.; Lin, Z.; Gimelshein, N.; Antiga, L.; et al. Pytorch: An imperative style, high-performance deep learning library. In Proceedings of the Advances in Neural Information Processing Systems, Vancouver, BC, Canada, 8–14 December 2019; Volume 32.
58. 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 Biometrics Special Interest Group (BIOSIG), Darmstadt, Germany, 6–7 September 2012; pp. 1–7.
59. Zhang, Z.; Yan, J.; Liu, S.; Lei, Z.; Yi, D.; Li, S. A face antispoofing database with diverse attacks. In Proceedings of the 2012 5th IAPR International Conference on Biometrics (ICB), New Delhi, India, 29 March–1 April 2012; pp. 26–31.
60. Boulkenafet, Z.; Komulainen, J.; Li, L.; Feng, X.; Hadid, A. OULU-NPU: A mobile face presentation attack database with real-world variations. In Proceedings of the 2017 12th IEEE International Conference on Automatic Face & Gesture Recognition (FG 2017), Washington, DC, USA, 30 May–3 June 2017; pp. 612–618.
61. Liu, Y.; Jourabloo, A.; Liu, X. Learning deep models for face anti-spoofing: Binary or auxiliary supervision. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, Salt Lake City, UT, USA, 18–23 June 2018; pp. 389–398.
62. Zhang, K.; Zhang, Z.; Li, Z.; Qiao, Y. Joint face detection and alignment using multitask cascaded convolutional networks. *IEEE Signal Process. Lett.* **2016**, *23*, 1499–1503. [CrossRef]
63. Chingovska, I.; Dos Anjos, A.; Marcel, S. Biometrics evaluation under spoofing attacks. *IEEE Trans. Inf. Forensics Secur.* **2014**, *9*, 2264–2276. [CrossRef]
64. Galbally, J.; Alonso-Fernandez, F.; Fierrez, J.; Ortega-Garcia, J. A high performance fingerprint liveness detection method based on quality related features. *Future Gener. Comput. Syst.* **2012**, *28*, 311–321. [CrossRef]
65. Ramachandra, R.; Busch, C. Presentation attack detection methods for face recognition systems: A comprehensive survey. *ACM Comput. Surv. CSUR* **2017**, *50*, 1–37. [CrossRef]
66. Boulkenafet, Z.; Komulainen, J.; Akhtar, Z.; Benlamoudi, A.; Samai, D.; Bekhouche, S.; Ouafi, A.; Dornaika, F.; Taleb-Ahmed, A.; Qin, L.; et al. A competition on generalized software-based face presentation attack detection in mobile scenarios. In Proceedings of the 2017 IEEE International Joint Conference on Biometrics (IJCB), Denver, CO, USA, 1–4 October 2017; pp. 688–696.
67. Jourabloo, A.; Liu, Y.; Liu, X. Face de-spoofing: Anti-spoofing via noise modeling. In Proceedings of the European Conference on Computer Vision (ECCV), Munich, Germany, 8–14 September 2018; pp. 290–306.
68. Bharadwaj, S.; Dhamecha, T.; Vatsa, M.; Singh, R. Computationally efficient face spoofing detection with motion magnification. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops, Portland, OR, USA, 23–28 June 2013; pp. 105–110.
69. Freitas Pereira, T.; Anjos, A.; De Martino, J.; Marcel, S. Can face anti-spoofing countermeasures work in a real world scenario? In Proceedings of the 2013 International Conference on Biometrics (ICB), Madrid, Spain, 4–7 June 2013; pp. 1–8.
70. Pinto, A.; Pedrini, H.; Schwartz, W.; Rocha, A. Face spoofing detection through visual codebooks of spectral temporal cubes. *IEEE Trans. Image Process.* **2015**, *24*, 4726–4740. [CrossRef] [PubMed]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.