computers

MDPI

Article

Face Liveness Detection Using Dynamic Local Ternary Pattern (DLTP)

Sajida Parveen [1,3,*], Sharifah Mumtazah Syed Ahmad [1,2], Nidaa Hasan Abbas [1], Wan Azizun Wan Adnan [1], Marsyita Hanafi [1,2] and Nadeem Naeem [1,3]

1 Department of Computer and Communication Systems Engineering, Faculty of Engineering, Universiti Putra Malaysia, 43400 UPM Serdang, Selangor, Malaysia; s_mumtazah@upm.edu.my (S.M.S.A.); nidaahasan71@gmail.com (N.H.A.); wawa@upm.edu.my (W.A.W.A.); marsyita@upm.edu.my (M.H.); nadeemnaeem@yahoo.com (N.N.)

2 Research Center of Excellence for Wireless and Photonic Network, Serdang 43400, Malaysia

3 Faculty of Electrical, Electronics and Computer Systems Engineering, Quaid-e-Awam University of Engineering Science and Technology, Nawabshah 67450, Pakistan

* Correspondence: sajidaparveen@quest.edu.pk; Tel.: +60-16-926-4104

Academic Editor: René Mayrhofer

Received: 23 February 2016; Accepted: 20 May 2016; Published: 24 May 2016

Abstract: Face spoofing is considered to be one of the prominent threats to face recognition systems. However, in order to improve the security measures of such biometric systems against deliberate spoof attacks, liveness detection has received significant recent attention from researchers. For this purpose, analysis of facial skin texture properties becomes more popular because of its limited resource requirement and lower processing cost. The traditional method of skin analysis for liveness detection was to use Local Binary Pattern (LBP) and its variants. LBP descriptors are effective, but they may exhibit certain limitations in near uniform patterns. Thus, in this paper, we demonstrate the effectiveness of Local Ternary Pattern (LTP) as an alternative to LBP. In addition, we adopted Dynamic Local Ternary Pattern (DLTP), which eliminates the manual threshold setting in LTP by using Weber's law. The proposed method was tested rigorously on four facial spoof databases: three are public domain databases and the other is the Universiti Putra Malaysia (UPM) face spoof database, which was compiled through this study. The results obtained from the proposed DLTP texture descriptor attained optimum accuracy and clearly outperformed the reported LBP and LTP texture descriptors.

Keywords: face liveness detection; dynamic local ternary pattern (DLTP); skin texture analysis

1. Introduction

Spoofing attacks upon face recognition systems involve presenting artificial facial replicas of authorized users to falsely infer their presence in order to bypass the biometric security measures. Such attacks can be carried out easily by means of printed photographs or digital images displayed on tablet, smart phones, *etc*. In order to distinguish real face features from fake faces, face liveness detection is a commonly used countermeasure approach. It is aimed at detecting physiological life signs in an identity [1].

Face liveness detection algorithms can be classified into two methods: intrusive and non-intrusive [2]. In intrusive methods, the involvement of the user is required to exhibit certain response to the system such as rotating head, performing few actions or mouth movement by uttering some words according to the system's instructions. While in non-intrusive methods, the system does not require any user involvement nor are users required to give any performance in any manner for liveness detection.

Furthermore, these two methods are subdivided into three categories. The first category includes analysis of skin properties and frequency reflectance from the texture of the presented face in front of the sensor. In other words, for this approach, face liveness detection is carried out via analyzing and differentiating textural properties of real skin from spoof counterparts. The second category involves the use of dedicated sensors that can detect the evidence of liveness such as infrared or thermal cameras are deployed. However, such devices are expensive and thus the approach is often limited to highly secure applications. The third category of face liveness detection schemes is based on challenging response methods or motion analysis. For this approach, the liveness detection techniques are based on actions that are deliberately performed by the user in front of the cameras according to the system's instructions, such as head and lip movement. This approach may be viewed as intrusive to the users as they are required to be cooperative with the system. It also involves complicated liveness detection algorithms that would exhume the computing resources [3–5].

In recent research, non-intrusive analysis that falls under the category of skin texture analysis has been shown to be very effective for face liveness detection. For extraction of texture features, a number of algorithms have been proposed to achieve a good classification rate.

Local binary pattern is one of the most popular, simple and efficient texture operators among various texture operators [6]. The code of the Local Binary Pattern (LBP) algorithm is grounded on binary number operation by specifying the center pixel grayscale value as a threshold for comparing the 3×3 neighborhood of each pixel with the value of central pixel value. The use of the center pixel as threshold causes the LBP descriptor to be more sensitive to noise, especially for smooth regions of the images. To overcome this noise sensitivity problem, an abstraction of LBP is proposed by Tan *et al.* [7] known as Local Ternary Pattern (LTP). In LTP, the difference between the central pixel and its neighbor is encoded by three values e.g., 1, 0 and -1 within the zone of user-specified threshold around the central pixel value. Usually, this threshold value is set manually in order to attain the best performance in specific problems and applications. In the LTP texture descriptor, the selection of threshold values in ternary quantization for a particular application is a critical task to minimize the sensitivity of noise with central pixel value.

In this paper, we present a new modified LTP based texture descriptor [8,9] against face spoofing. This approach relies on Weber's law which states that change of a stimulus (e.g., lighting or sound) that will be just noticeable is a constant ratio of the original stimulus. Dynamic Local Ternary Pattern (DLTP) is motivated by this point and compute relative intensity difference of a given pixels against its neighbors by dynamic process of threshold calculation. This threshold is obtained on the assumption of Weber's law. We also collected a face spoof database, Universiti Putra Malaysia (UPM) Face Spoof Database, using verity of textures for spoof attacks. Experiments conducted on UPM Face Spoof Database, Replay-Attack, Chinese Academy of Sciences (CASIA) and Nanjing University of Aeronautics and Astronautics (NUAA) databases. The proposed method is economical and practical as it does not require any expensive capture devices, complicated algorithms or cooperative subjects.

The organization of rest of the paper is as follows: Section 2 describes related research work in detail. Proposed countermeasures along with details of dynamic threshold setting are employed in Section 3. Section 4 presents the experimental results and discussions. Last but not least, Section 5 concludes the paper.

2. Related Work

This section presents related work on liveness detection that is based on the analysis of surface properties of the presented facial samples (*i.e.*, the first category as described in the introduction).

Fourier spectra have been used to differentiate fake faces from real faces based on the assumption that real skin has a high frequency component, which is greater than printed photos [10]. The method was based on the structure and movement information of a face, and analyzed by using high frequency descriptors and frequency dynamic descriptors, respectively, of face images. The experiments were carried out on a self-collected database which was not made available to the public. However, at

the same time, this technique was found to be sensitive to various lighting effects and vulnerable to spoofing attacks by using high quality photographs.

The surface properties of live human or imitated faces have been analyzed by using the Lambertian model [11]. The authors developed two extensions of the sparse logistic regression model for classification. The first extension was based on sparse low rank logistic regression, and the second extension was based on nonlinear models via empirical mapping. These derived models estimate the latent reflectance information from the imitated faces. The authors introduced the NUAA face imposter database, which is publicly available. The proposed method was suitable for real time application and did not consume any extra hardware, while, in real-time, the illumination conditions may greatly affect the face presentation, which may influence the performance of the spoof detection method. Furthermore, the method was proposed to restrict only photo based attacks. Moreover, to deal with un-control illumination changes, a method was proposed to identify the liveness of the user by using the properties of recaptured images from the LCD display and its illumination changes [12]. The authors used a Difference of Gaussian (DoG) filter for display images, and, to overcome lighting effects, a contrast-limited adaptive histogram equalization (CLAHE) approach was used on the NUAA and Yale Face Database B and reduced the error rate in more than 50% for spoofs (NUAA Imposter Database) and more than 65% for the case of recaptured LCD images (Yale Recaptured Database).

In a real world scenario, a face of a live person that is biometrically presented to the system has some characteristics, e.g., it may be possible to observe a slight movement of the face or an eye blinking. However, in cases of deceit, even a slight movement of the head is not independent from its background. Schwartz *et al.* [13] took advantage of this valuable information and proposed an approach based on spatial and temporal information of the face. The authors utilized a low level feature descriptor and partial least squares regression. The feature descriptor considered information regarding color, shape and texture. The calculated feature vectors of three parameters of the face was based on the histogram of oriented gradients (HOG), color frequency (CF), gray level co-occurrence matrix (GLCM), and histograms of shearlet coefficients (HSC). The performance of the proposed scheme was evaluated on the FSA and NUAA database by partial least squares (PLS) based weighting. The limitation of this approach emerges in the form of different behaviors of feature descriptors in two datasets. For example, HSC performs better on the FSA dataset; however, GLCM provides better results on the NUAA dataset.

A very well-known and effective texture operator called Local Binary Pattern (LBP) and its modified versions are widely used in face anti-spoofing schemes. The LBP operator can be defined as a rotation invariant grayscale measure. The LBP is a two-step calculation, involving a thresholding step and an encoding step. In the first step, all the neighborhood pixels are converting their values into the binary 0 or 1 by compared with the value of their center pixel of the pattern. Then, in the next step, the obtained binary numbers are encoded and converted into decimal numbers [14]. In [15], micro texture patterns for printed artifacts are analyzed by using a multi-scale LBP method. The experiment was conducted on an NUAA dataset. To discriminate between the live and the non live face, a Support Vector Machine (SVM) was utilized. The calculated LBP features in this were found to be useful for spoof detection and can also be utilized for recognition algorithm. The strength of LBP texture descriptor was analyzed for discriminating the skin texture of a real face image and various spoof attack in [16]. The results are compiled on the REPLAY ATTACK database that was introduced and made publicly available by the authors. By using the same database, Tiago *et al.* [17] presented the approach to analyze the textural properties by extending the LBP texture descriptor. The proposed method employed a multi-resolution strategy in a single descriptor from three orthogonal planes of the local binary pattern (LBP-TOP) that combines the space and time information. The system was designed to detect both photo and video attacks in face liveness detection and was found to be more effective in time domain multi-resolution.

Another skin texture analysis based method known as a Local Binary Pattern Variance (LBPV) descriptor was proposed for liveness detection [18]. The proposed method analyzed the textural

properties of captured and recaptured images. To enhance the discriminate power of the scheme, the Difference of Gaussian (DoG) filter was used at the preprocessing step to obtain the special frequency band, and LBPV was deployed to calculate the feature that carried the information of contrast and texture characteristics. Evaluations were carried out on NUAA datasets, and the method was proved to be invariant to variance of illuminations and rotation of photographs at different angles.

The extension of LBP known as Local Graph Structure (LGS), and its extended version was introduced in face liveness detection by Housam *et al.* [19,20]. LGS has a slightly different method compared to the other LBP extensions. In LGS, six pixels are utilized to form the neighbors of the target pixel. The calculation of the pattern starts from the target pixel to the left region of the graph in an anti-clockwise direction and then the right region in a clockwise direction. In this process, the edges of two pixels are connected through vertices and assigned a binary number 1 if a neighboring pixel gray value is greater than or equal to the target pixel; otherwise, binary 0 is assigned. The authors divided the face image region into numbers of blocks and then LGS was applied on each block and the local feature descriptors were calculated. After that, the histograms of local features were concatenated into a global descriptor. The evaluation of the spoofing rate was conducted on the NUAA database. Different training sizes were adopted in this research work to measure the robustness of LGS. Moreover, the structure and dynamics of micro textures were analyzed to extract the feature based on LBP-TOP [21] for liveness identification. The experiments of the proposed approach were carried out on two publicly available databases: the CASIA Face Anti-Spoofing and Print-Attack Database. The obtained results indicate the improvement in EER from 16 to 10 percent. The better performance of countermeasure was observed on the Replay-Attack database as compared to the CASIA database.

Recently, LBP based image distortion analysis (IDA) [22] for face spoof detection has been proposed in which they analyzed the reflection of light, blurriness, the quality of image and color diversity distortion in printed photo or LCD screen images. For feature extraction, LBP was used to calculate four different features, namely: specular reflection, blurriness, chromatic moment and color diversity to create the IDA feature vector. The experiment was conducted on three databases: the first was the author's collected Mobile Face Spoofing Database (MSU MFSD), and the other two were public-domain face spoof databases (Idiap REPLAY-ATTACK and CASIA). The results were calculated on multiple SVM classifiers. The proposed method of spoof detection was evaluated on cross-databases, which means trained on one dataset and tested on other datasets. The results showed better performance [22] on intra-database and cross-database as compared to the state-of-the art. Similarly, the strength of dynamic texture for face liveness detection in a video sequence was proposed in [23]. The method based on kernel discriminant analysis and utilized a multi dynamic texture descriptor based on binarized statistical image features of three orthogonal planes (MBSIF-TOP) to detect the face spoof attacks.

The potential use of joint quantization of local feature texture descriptors for face liveness detection has been provided in [24]. Various biometric traits such as iris, fingerprint and face are utilized to evaluate the performances of these texture descriptors. Moreover, a new robust and powerful local descriptor, called Weber's Local Descriptor-Three Orthogonal Planes (WLD-TOP) has been proposed in [25], which combined the temporal and spatial information into a single descriptor with a multi-resolution strategy. Extensive experiments were reported on CASIA and the self-collected Sun Yat-Sen University–Mobile Face Spoof Database (SYSU-MFSD). The state-of-the-art study shows that development of facial surface analysis based anti-spoofing systems are reasonable in cost, no user involvement is required and they are easy to implement.

3. Method and Evaluation

In this paper, we proposed a Dynamic Local Ternary Pattern (DLTP) [8,9] for face liveness detection. Weber's law is adopted for tuning the threshold value dynamically for every image pattern in the Local Ternary Pattern (LTP). The threshold equation for ternary quantization in LTP is given below:

$$a_i = \begin{cases} 1 & if \quad p_i > c + \tau \\ 0 & if \quad c - \tau \leqslant p_i \leqslant c + \tau \\ -1 & if \quad p_i < c - \tau \end{cases} . \tag{1}$$

c is the intensity value of the center pixel, p_i (i = 0, 1, ... , p−1) is the intensity value of the neighborhood pixels and τ is a threshold value. Furthermore, the ternary pattern is split into two binary codes named upper and lower pattern. For this purpose, the binary threshold function h_i for the upper pattern is computed as:

$$h_i = \begin{cases} 1 & if \quad a_i = 1 \\ 0 & otherwise \end{cases} . \tag{2}$$

The binary threshold function l_i for the lower pattern is calculated:

$$l_i = \begin{cases} 1 & if \quad a_i = -1 \\ 0 & otherwise \end{cases} . \tag{3}$$

The weighted sum function for upper pattern can be expressed as:

$$LTPh_{P,R} = \sum_{i=1}^{P} h_i \times 2^{i-1}, (h_i \in \{0, 1\}). \tag{4}$$

The weighted sum function for lower pattern can be expressed as:

$$LTPl_{P,R} = \sum_{i=1}^{P} l_i \times 2^{i-1}, (l_i \in \{0, 1\}). \tag{5}$$

The $LTP_{8,2}$ operator and its computational process on image patches is represented in Figure 1.

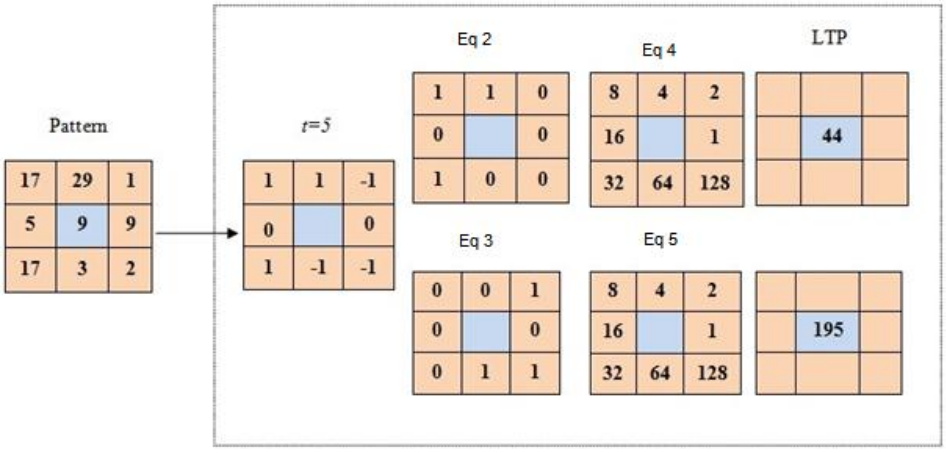

Figure 1. Calculation of Local Ternary Pattern (LTP) operators. The obtained ternary pattern is further coded into upper and lower binary in the LTP.

In DLTP, an equation for threshold is introduced, which is based on Weber's law, instead of choosing a direct fix value of threshold in LTP. The Weber's law expressed as:

$$\frac{\Delta I}{I} = k. \tag{6}$$

ΔI represents the increment threshold of the initial stimulus intensity I and k signifies the proportion of (6) which remains constant. According to the Weber's law in DLTP, ΔI is generalized as $|p_i - c|$ when I is considered as c. In order to calculate the difference in texture characteristics, a dynamic process of threshold calculation is adopted on the assumption that $\Delta I = |p_i - c|$ is noticeably different for discrimination. By the local statistics of the pattern, the threshold equation according to Weber's law can be expressed as:

$$\frac{|p_i - c|}{c} = \gamma = \tau. \tag{7}$$

For the constant factor, γ is used in (7) that is threshold value (τ), and c is the center pixel of the patch in an image. The (7) is used to generate the DLTP code, in which the threshold value is dynamically generated and assigned the code 1, 0, and -1 within the zone of $\pm$ threshold (τ) value around the central pixel value. The value of τ supports the setting of different threshold values dynamically for every patch of the image automatically. Equation (7) of threshold value (τ) is used to generate DLTP code as shown below:

$$DLTP(a_i) = \begin{cases} 1 & if \quad p_i > c + \tau \\ -1 & if \quad p_i \leqslant c - \tau \\ 0 & otherwise \end{cases} \tag{8}$$

Here, p_i and c is defined in Equation (1); τ is the dynamic threshold for the center pixel x_c.

In this research work, LTP and DLTP are employed for feature extraction and explore the textural properties of facial skin to identify the difference between a live face and a spoofed face. The calculation process of DLTP is similar to that of LTP, which is shown in Figure 2. In the proposed framework of DLTP, it is shown that ternary code e.g., +1, 0, and -1 is generated in DLTP that is further divided into its corresponding positive and negative parts, and treated as two separate binary patterns. This reduces the feature size from 3^n to 2×2^n. Furthermore, the histograms are computed separately and the result is combined only at the end of computation. The threshold value in DLTP does not set manually but will set dynamically on the basis of Weber's law. In this paper, the spatial area is selected by using the value of p (e.g., number of neighborhood pixels) and R (radius of the circle) and combining the information provided N DLTP operators from the whole image. The selected value of p and R for our experiment is defined in the next section.

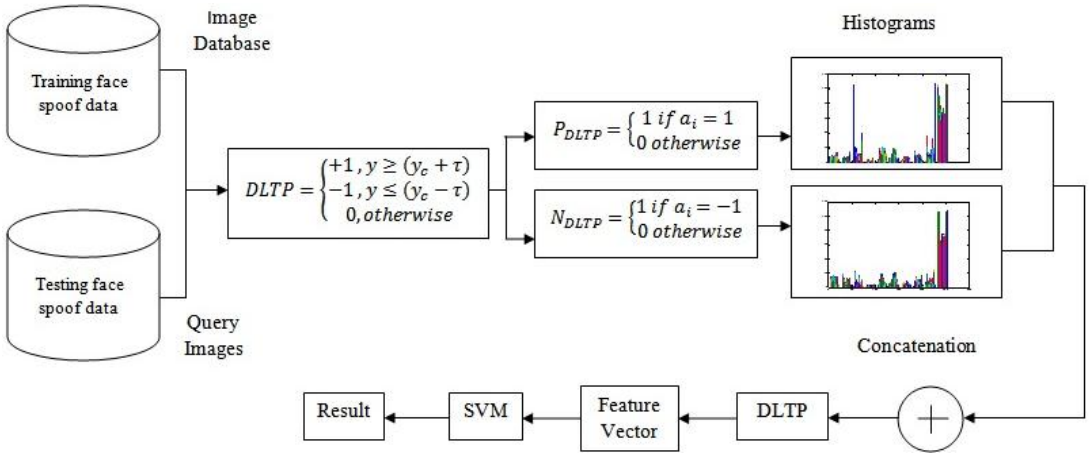

Figure 2. Block diagram of the face liveness detection system by using the Dynamic Local Ternary Pattern (DLTP) feature descriptor.

3.1. Experimental Setup

In this subsection, we evaluate the performance of the proposed method on our collected UPM face spoof database [26] and, for comparison, we adopt three publicly available databases: CASIA Face Anti-Spoofing Database [27], the Replay-Attack database [28] and the NUAA database [11] face spoof database. The details of the all the databases are discussed below.

Face liveness detection is a binary classification problem, in which the result must be either positive (genuine face) or negative (spoof face). The Support Vector Machine (SVM) with liner kernel was chosen to separate positive and negative face spoofing samples. The SVM classifier with linear kernel is used for each training dataset of all the databases with parameters optimized by cross-validation. The tenfold cross validation is used in every experimental setup with a fixed value of optimal cost (C = 10) and applied on UPM face spoof, CASIA, Replay-Attack and NUAA databases. Furthermore, the proposed method is compared to a single scale technique, namely LTP [29]. The value of patch size P, and radius R for $\mathrm{LTP}_{P,R}$ and $\mathrm{DLTP}_{P,R}$ were set as eight and two, respectively, for each pattern window. Through both techniques, we computed a 59-bin histogram for normalizing the values of the image.

For evaluating and obtaining high performance from both feature descriptors, we applied six different threshold values for LTP for evaluating the developing dataset and obtaining the best threshold value for calculating the difference in patterns between live face and spoof face image. The histograms are computed from the feature extraction stage and then passed to an SVM for classification into the fake and real faces. In all experiments, the performance is measured in accuracy of system, Half Total Error Rate (HTER), False Acceptance Rate (FAR) and False Rejection Rate (FRR) in percentage.

3.1.1. UPM Face Spoof Dataset

The UPM face spoof database is collected and compiled during this research work. In our experiment, we follow the standard of data gallery independence in which the first 10 subjects are utilized for training dataset and the images of the remaining 20 subjects are utilized for testing the model. The training and developing set consists of 4500 genuine sample images, and 18,000 sample images are utilized to develop the testing dataset. For spoof attacks, 1500 sample images from all type attacks are designed per subjects. In this manner, 7500 samples images are utilized for training and developing datasets, while the remaining 30,000 fake sample images of 20 subjects are used for testing protocol. These 30 participants are from different ethnicities, between the ages of 20 and 50. Facial images were frontal shots captured using a single view camera, with spatial resolution of 1440 $\times$ 1080 pixels. The imaging and recording conditions was an indoor environment under uncontrolled illumination. During each session, several variables were considered such as facial expressions, eye blinks, and wearing a scarf. The high resolution image consumes more memory with high computation and time. Therefore, we cropped the region around the frontal faces to 345 $\times$ 400 resolution, while retaining the maximum quality for printing photographs. Fake faces played a very important role in enhancing the challenges for face anti-spoofing algorithms. For this purpose, the spoof database is compiled based on variations in terms of textures. We have introduced four different types of paper material in photo attacks: common A4, matt, laminated, and without lamination paper. Furthermore, this study utilized different digital screens such as iPhones, laptops, and tablet PCs for different resolution quality attacks. To make the collected database more challenging in terms of attacks, the images are captured from different distances. Tilted and bended images are also captured in order to increase the level of difficulty. The sample images of face spoof datasets are shown in Figure 3.

Figure 3. Face sample images with different variations of self-collected database.

3.1.2. NUAA Dataset

The publicly available NUAA Photograph Imposter Database contains images of both real client access and photo attacks. The face image of each individual is collected in three different sessions, with an interval of approximately two weeks, whereby in each session, the environmental and illumination conditions are varied. There are 500 images for each subjects' recording. The images in the database are captured using conventional webcams, with resolution of 640 × 480 for 15 subjects. Even subjects that appeared in test and training sets are quite different. As it is explained in [11], six out of nine subjects do not appear in the training set for live human case and six out of 15 subjects do not appear in the training set for photo case.

3.1.3. CASIA Face Anti-Spoofing Database (CASIA FASD)

The CASIA FASD contained training and testing data set of 50 subjects. The training data set comprised of 20 subjects and test dataset contained 30 subjects. For both the training and testing dataset, seven test scenarios are setup, e.g., wrapped photo attack, cut photo attack, video, image quality test attacks and overall test. This database also follows the standard of gallery independence, and the subjects are not overlapped in any dataset. We utilized the corresponding overall training and test sets for model training and performance for our experiment. In this scenario, all the data are combined to be used for a general and overall evaluation.

3.1.4. Replay-Attack Database

The Replay-Attack database consists of real access and spoof attacks of 50 subjects. The database was comprised of a total of 1200 video recordings. These included real attempts, print attacks, phone attacks and tablet attacks of 200, 200, 400 and 400 videos, respectively. The dataset is subdivided into three sets named the training, development and testing set. Identities for each subset were chosen randomly, but do not overlap, *i.e.*, people that are on one of the subsets do not appear in any other set. The training subset contains 360 videos of 60 real access and 300 videos of attacks. The development (validation) set was comprised of 360 videos of 60 real and 300 attack attempts. The testing group consist of 480 videos of 80 real-access and 400 attack videos. For performance evaluation, the train set

utilized to train the classifier and typically the usage of the development set was used to adjust the parameters of classifier for good performance. For evaluating the performance of a model, the test set is intended to be used.

For evaluating the performance of LTP and DLTP, we follow the protocols specified by Replay-Attack database. We utilized the training dataset and developing set for training and parameter tuning, respectively, to optimize the classifier. Finally, the test set is used to evaluate the performance of proposed method for face liveness detection.

CASIA and NUAA spoof database do not have dedicated samples for developing sets like the Replay-Attack database. For this purpose, we split the training dataset into two equal subsets in which one is used for training, and the other is used as a developing (validation) dataset for tuning the classifier. The details about the data partitioning and number of sample images are given in Table 1.

Table 1. Details about the data partitioning (Genuine + Spoof).

Database	Training Set	Validation/Developing Set	Testing Set
NUAA	871 + 874	872 + 874	3362 + 5761
CASIA	2289 + 5929	2290 + 5929	5603 + 16958
Replay-Attack	22,497 + 69,686	22,498 + 70,246	29,791 + 93,686
UPM FSD	4500 + 7500	4500 + 7500	30,000

4. Results and Discussion

The analyzed score distribution of live and spoofed faces of NUAA, CASIA, Replay-Attack and UPM Face Spoof datasets for face liveness detection are shown in Figure 4. It can be observed that for NUAA, CASIA, Replay-Attack and UPM datasets, most of the scores for live faces come under the value of 0 to 0.6, −2 to 2, −2.8 to 1.9 and −3 to 2, respectively, and no live face scores are shown above these ranges. In contrast, most of the non-live faces achieved a score between 0.3 and 1 for NUAA, −0.1 and 5 for CASIA, −0.7 and 6.7 for Replay-Attack, and −2 and 6.6 for UPM face spoof datasets.

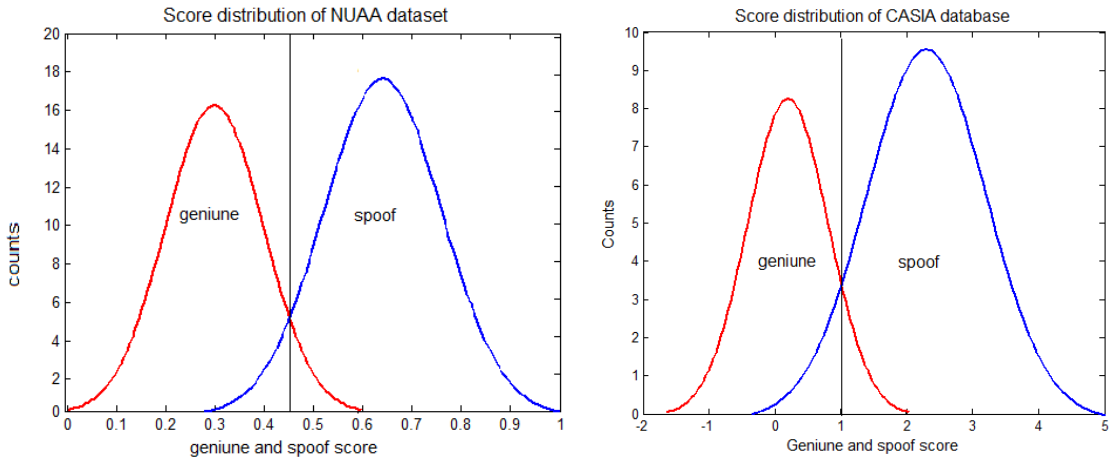

Figure 4. *Cont.*

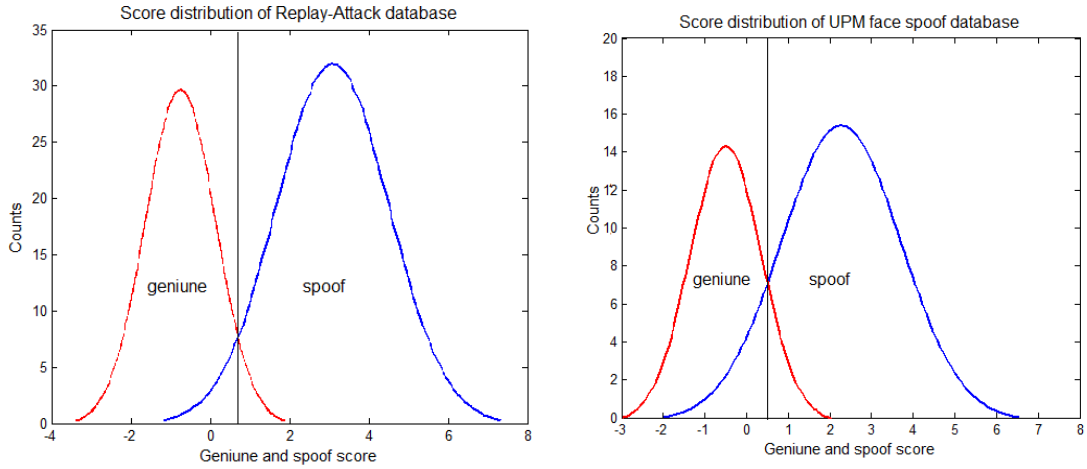

Figure 4. Genuine and spoof score distribution. (**a**) NUAA dataset; (**b**) CASIA dataset; (**c**) Replay-Attack and (**d**) UPM face spoof dataset.

Firstly, we performed the validation by utilizing the developing dataset for tuning the classifier and selecting the best threshold value for the LTP texture descriptor in the application of face liveness detection. The rate of face liveness detection with LTP on development sets in all four face spoof databases are shown in Table 2 in terms of accuracy, Half Total Error Rate (HTER) and Area Under the Curve (AUC) along with False Acceptance Rate (FAR) and False Rejection Rate (FRR) at different threshold values. From the obtained results, it can be seen that LTP achieved a higher accuracy at threshold value 5 for all of the databases.

Table 2. Performance of Local Ternary Pattern (LTP) (P = 8, R = 2) with different threshold values (τ) on development (validation) dataset.

Database	τ	Accuracy	HTER	FAR	FRR	AUC
NUAA	2	87	12.1	10	14.2	0.898
	5	**89.88**	**8.4**	**5**	**11.8**	**0.886**
	8	81.4	17.2	15.3	19.1	0.788
	10	**90.48**	**8.2**	**7**	**9.4**	**0.9278**
	12	88.78	11.6	9	14.2	0.8312
	15	87.23	12.3	8	16.6	0.828
UPM	2	81.34	17.8	16.7	18.9	0.7876
	5	**86.13**	**12**	**11**	**13**	**0.814**
	8	81.9	18.5	17	20	0.79
	10	82.54	18.29	17	19.58	80.1
	12	82.92	16.66	13.2	20.12	80
	15	81.9	17.9	16	19.8	79.2
Replay-attack	2	88.4	10	7	13	83.3
	5	**92.87**	**6.2**	**6.1**	**6.3**	**0.912**
	8	91.42	7.54	5	10.08	0.899
	10	86.57	16.12	15	17.24	0.812
	12	87.32	12.2	9.8	14.6	0.822
	15	84.8	13.6	12.5	14.7	0.810
CASIA	2	88.02	9.67	6.3	13.04	0.829
	5	**92.98**	**5.43**	**4.8**	**6.06**	**0.91**
	8	79.67	20.56	17.23	23.89	0.687
	10	90	7.89	8.9	6.88	0.878
	12	86.23	18.3	13	23.6	0.822
	15	88.6	14	13	15	0.836

In the NUAA database, threshold 5 and 10 achieved very close values in HTER and accuracy results for face liveness detection. From the calculated results, we select the stable threshold value (*i.e.*, five in the case of face liveness detection) for LTP texture descriptor to perform the testing step against DLTP texture descriptor.

Secondly, for dealing with different characteristics of textures [30] for spoof attacks, this experiment is conducted to compare the performance of the DLTP method with the LTP on four spoof databases: NUAA, Replay-Attack, CASIA and the UPM spoof database. The corresponding results of LTP and DLTP presented in Table 3 by utilizing the test dataset that is already mentioned in Table 1 for all the databases.

According to the results, our proposed method has higher accuracy results and lower error rate for all of the databases. All results indicate that our proposed texture descriptor outperforms compared to the traditional LTP descriptor. It can be observed that the proposed method of DLTP is more robust to noise with uniform pattern because of ternary quantization. In addition, DLTP has the ability to select the threshold value dynamically by following Weber's law. Compared with LTP, DLTP has the ability to set the threshold automatically according to the ratio of difference in patterns. DLTP can find the minor difference between the faces of genuine and spoof.

The receiver operating characteristic (ROC) curves are presented in Figure 5 that show the error graph of False Positive Rate against True Positive Rates. ROC curves are best for comparing the performance analysis of any two systems. The generated ROC curves of DLTP compared with LTP tested on four databases: NUAA, CASIA, Replay-Attack and the UPM face spoof database are presented in Figure 5a–d, respectively.

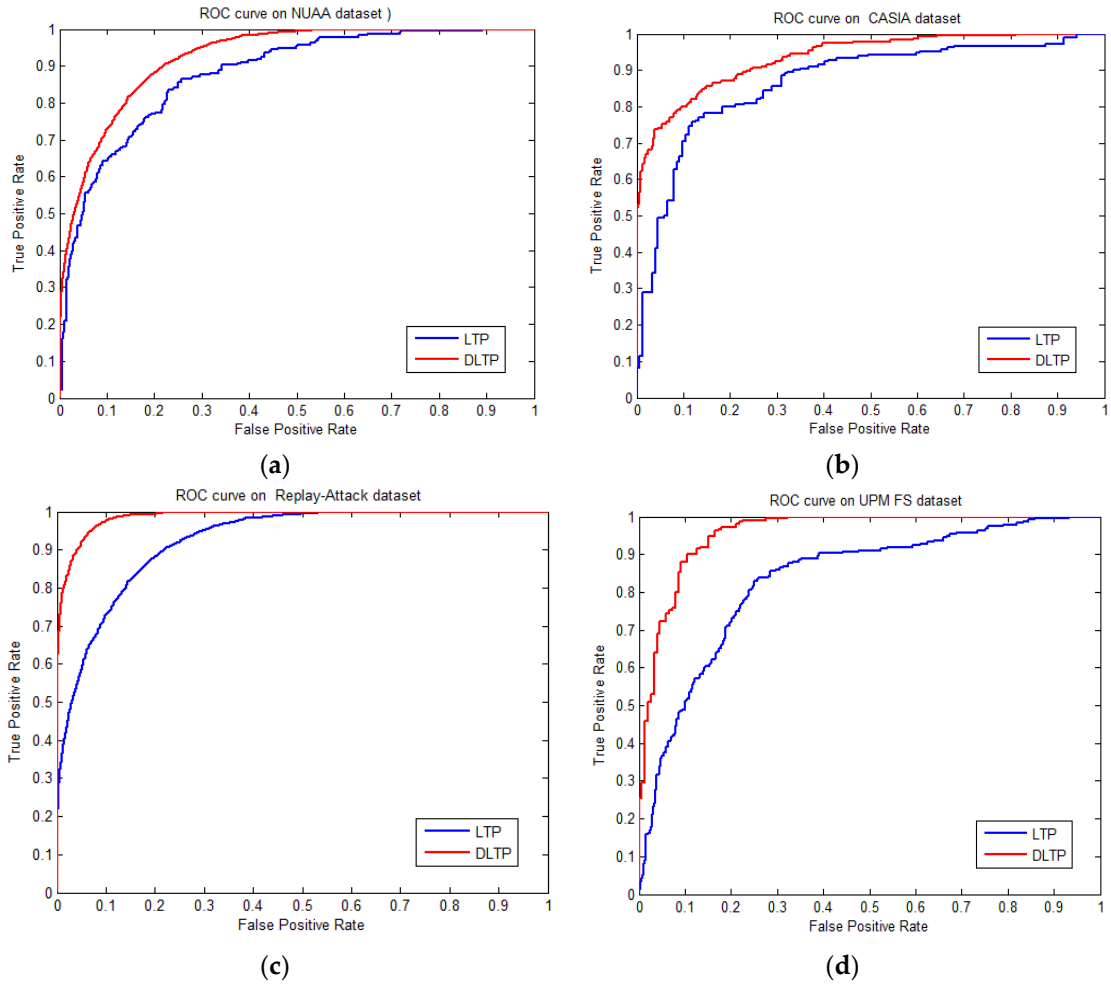

Figure 5. Receiver Operating Characteristic (ROC) curve of LTP and DLTP. (**a**) NUAA; (**b**) CASIA; (**c**) Replay-Attack and (**d**) UPM face spoof databases.

Table 3. Performance of LTP at threshold value (τ = 5) and Dynamic Local Ternary Pattern (DLTP) (P = 8, R = 2) on four databases.

Database	Method	Accuracy	HTER	FAR	FRR	AUC
NUAA	LTP	91.1	7.4	5.1	9.7	0.886
	DLTP	94.5	3.5	3.2	3.8	0.952
CASIA	LTP	93.02	6.1	5	7.2	0.934
	DLTP	94.4	5.4	4.8	6	0.958
Replay-Attack	LTP	91.93	6.4	5.9	6.9	0.923
	DLTP	97.2	4.8	4.7	4.9	0.987
UPM FSD	LTP	86.95	12.2	11.1	13.3	0.898
	DLTP	92.8	7.3	5.2	9.4	0.956

The ROC curves showed consistent higher performance in all the database tests, which indicate that DLTP features are more robust across different illumination, scenarios, and various textures than LTP features. In addition, DLTP obtained more dynamic threshold values that traditional methods lacked, which depicts the higher performance of the face liveness detection method.

The obtained results established the conclusion that, due to fixed values of threshold in LTP and dynamic values in DLTP, the DLTP outperforms LTP throughout all the datasets. The result of higher accuracy and lower value of error rates indicates that the DLTP texture descriptor calculates more informative features, has stability in different scenarios and lighting effects, and is found to be more robust for various textures. It is clear from ROC curves and achieved results that DLTP attains better performance and differentiates the live facial skin texture from the spoofed face.

Moreover, in Tables 4–6 we present a comparative evaluation of LTP and DLTP with other existing state-of-the-art approaches to texture based analysis using NUAA, Replay-Attack and CASIA face spoofing databases by adopting similar experimental protocols to benchmark the results. The results indicate that the combination and variations in LBP somehow extends to good performance for face liveness. As compared to the traditional and simple LBP, LTP improves the results in face pattern analysis because of its noise resistance property by quantization of three levels. For making quantization levels more stable and reliable, the dynamic threshold in DLTP is introduced. As per expectations, from the achieved results on all datasets, DLTP provides a better result for face liveness detection in contrast to the state-of-the-art techniques. The improved results are highlighted by the bold font in all of the tables.

Table 4. Performance comparison on NUAA dataset.

Techniques	HTER (%)
Local Binary pattern variance (LBPV) [17]	11.97 and 13.05
Local Binary pattern (LBP) [14]	18.32, 19.03 and 13.17
Local Ternary Pattern (LTP)	7.4
Dynamic Local ternary Pattern (DLTP)	**3.5**

Table 5. Performance comparison on Replay-Attack database.

Approaches	HTER (%)	Approaches	HTER (%)
IQA [30]	15.2	** CoA-LBP	9.4
IDA + SVM [21]	7.4	** Ric-LBP	14.7
LBP-TOP [16]	8.51	** WLD and ** LPQ	17.5 and 21.7
* LBP + SVM	15.16	** BSIF	12.6
DOG + LBP + SVM	11.1	** LCPD	14.0

Table 5. *Cont.*

Approaches	HTER (%)	Approaches	HTER (%)
LLR [20]	5.47	** Keypoint SIFT	25.2
* LBP + LDA	17.17	** Dense SIFT	17.0
LBP + SVM [14]	13.87	** DAISY and ** SID	17.2 and 10.5
MLPQ-TOP + KDA [22]	3.75	LTP	6.4
MBSIF-TOP + KDA [22]	1.38	DLTP	**4.8**

* Chingovska, I., Anjos, A. and Marcel, S., 2012; ** Gragnaniello, D. *et al.*, 2015.

Table 6. Performance comparison on CASIA database.

Approaches	HTER (%)
LBP + LDA [15]	21.01
LBP + SVM [15]	18.17
LBP [14]	18.21
LBP-TOP [16]	10
DoG-based [26]	17.0
IQA [31]	32.4
LTP	6.1
DLTP	**5.4**

5. Conclusions

This paper introduced a new texture descriptor known as Dynamic Local Ternary Pattern (DLTP) in the face liveness detection method. By following Weber's law, in DLTP, the threshold value sets dynamically instead of by a manual setting. Comparison of DLTP is performed with Local Ternary Pattern (LTP) and systematically examined and compared these two techniques in relation to variation of their threshold values. For benchmarking, the performance evaluation is carried out on both publicly available face spoof databases (NUAA, Replay-Attack and CASIA), and our self collected UPM face spoof database. A best threshold value of LTP is utilized to compare the performance of DLTP for face spoof attacks. The comparative analysis of both techniques also shows that DLTP out-performed LTP and other state-of-the-art approaches for face pattern analysis in a face liveness detection method. The dynamic threshold in DLTP was found to be more robust for noise with a central pixel value and invariance with respect to illumination transformation and texture variations as compared to LTP and other texture descriptors.

Acknowledgments: The authors are thankful to the reviewers for their constructive comments which helped to improve the quality of this article.

Author Contributions: Sajida Parveen conceived the idea, designed the framework, performed the experiments, analyzed the data and wrote the paper. Sharifah Mumtazah Syed Ahmad guided this research work to make it a worthy contribution to the scientific community. Nidaa Hasan Abbas and Nadeem Naeem involved in data collection. Sharifah Mumtazah Syed Ahmad, Wan Azizun Wan Adnan and Marsyita Hanafi reviewed the paper contents to improve the manuscript and to make it easier for reader to understand.

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

References

1. Chingovska, I.; Nesli, E.; André, A.; Sébastien, M. Face Recognition Systems under Spoofing Attacks. In *Face Recognition across the Imaging Spectrum*; Bourlai, T., Ed.; Springer: Berlin/Heidelberg, Germany, 2016; pp. 165–194.
2. Parveen, S.; Ahmad, S.M.S.; Hanafi, M.; Azizun, W.A.W. Face anti-spoofing methods. *Curr. Sci.* **2015**, *108*, 1491–1500.
3. Yi, D.; Lei, Z.; Zhang, Z.; Li, S.Z. Face anti-spoofing: Multi-spectral approach. In *Handbook of Biometric Anti-Spoofing*; Marcel, S., Nixon, M.S., Li, S.Z., Eds.; Springer: London, UK, 2014; pp. 83–102.

4. Anjos, A.; Komulainen, J.; Marcel, S.; Hadid, A.; Pietikäinen, M. Face anti-spoofing: Visual approach. In *Handbook of Biometric Anti-Spoofing*; Marcel, S., Nixon, M.S., Li, S.Z., Eds.; Springer: London, UK, 2014; pp. 65–82.
5. Hadid, A. Face biometrics under spoofing attacks: Vulnerabilities, countermeasures, open issues, and research directions. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops, Columbus, OH, USA, 23–28 June 2014; pp. 113–118.
6. 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]
7. Tan, X.; Triggs, B. Enhanced local texture feature sets for face recognition under difficult lighting conditions. *IEEE Trans. Image Proc.* **2010**, *19*, 1635–1650.
8. Ibrahim, M.; Alam Efat, M.I.; Shamol, H.K.; Khaled, S.M.; Shoyaib, M.; Abdullah-Al-Wadud, M. Dynamic local ternary pattern for face recognition and verification. In Recent Advances In Computer Engineering, Communications and Information Technology, Proceedings of the International Conference on Computer Engineering and Applications, Tenerife, Spain, 10–12 January 2014; pp. 146–151.
9. Liao, W.H. Region description using extended local ternary patterns. In Proceedings of the 20th International Conference on Pattern Recognition (ICPR), Istanbul, Turkey, 23–26 August 2010; pp. 1003–1006.
10. Li, J.; Wang, Y.; Tan, T.; Jain, A.K. Live face detection based on the analysis of Fourier spectra. In Proceedings of the SPIE 5404, Biometric Technology for Human Identification, Orlando, FL, USA, 12 April 2004; pp. 296–303.
11. Tan, X.; Li, Y.; Liu, J.; Jiang, L. Face liveness detection from a single image with sparse low rank bilinear discriminative model. In Computer Vision–ECCV 2010, Proceedings of the 11th European Conference on Computer Vision, Heraklion, Greece, 5–11 September 2010; Daniilidis, K., Maragos, P., Paragios, N., Eds.; Lecture Notes in Computer Science. Springer: Berlin/Heidelberg, Germany, 2010; Volume 6316, pp. 504–517.
12. Peixoto, B.; Michelassi, C.; Rocha, A. Face liveness detection under bad illumination conditions. In Proceedings of the IEEE 18th International Conference on Image Processing (ICIP), Brussels, Belgium, 11–14 September 2011; pp. 3557–3560.
13. Schwartz, W.R.; Rocha, A.; Pedrini, H. Face spoofing detection through partial least squares and low-level descriptors. In Proceedings of the 2011 International Joint Conference on Biometrics (IJCB), Washington, DC, USA, 11–13 October 2011; pp. 1–8.
14. Hadid, A. The local binary pattern approach and its application to face analysis. In Proceedings of the Image processing theory, tools and application, Sousse, Tunisia, 23–26 November 2008; pp. 1–9.
15. Maatta, 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, 11–13 October 2011; pp. 1–7.
16. Chingovska, I.; Anjos, A.; Marcel, S. On the effectiveness of local binary patterns in face Anti-spoofing. In Proceedings of the International Conference of the Biometrics Special Interest Group (BIOSIG), Darmstadt, Germany, 6–7 September 2012; pp. 1–7.
17. De Freitas Pereira, T.; Anjos, A.; De Martino, J.M.; Marcel, S. LBP-TOP based countermeasure against face spoofing attacks. In Computer Vision-ACCV 2012 Workshops, Proceedings of the ACCV 2012 International Workshops, Part I, Daejeon, Korea, 5–6 November 2012; Park, J.I., Kim, J., Eds.; Lecture Notes in Computer Science. Springer: Berlin/Heidelberg, Germany, 2012; Volume 7728, pp. 121–132.
18. Kose, N.; Dugelay, J.L. Classification of captured and recaptured images to detect photograph spoofing. In Proceedings of the 2012 International Conference on Informatics, Electronics and Vision (ICIEV), Dhaka, Bangladesh, 18–19 May 2012; pp. 1027–1032.
19. Housam, K.B.; Lau, S.H.; Pang, Y.H.; Liew, Y.P.; Chiang, M.L. Face spoofing detection based on improved local graph structure. In Proceedings of the 2014 International Conference on Information Science and Applications (ICISA), Seoul, South Korea, 6–9 May 2014; pp. 1–4.
20. Bashier, H.K.; Hoe, L.S.; Hui, L.T.; Azli, M.F.; Han, P.Y.; Kwee, W.K.; Sayeed, M.S. Texture classification via extended local graph structure. *Opt. Inter. J. Light Electron Opt.* **2016**, *127*, 638–643. [CrossRef]
21. Komulainen, J.; Hadid, A.; Matti, P. Face spoofing detection using dynamic texture. In Computer Vision-ACCV 2012 Workshops, Proceedings of the ACCV 2012 International Workshops, Part I, Daejeon, Korea, 5–6 November 2012; Park, J.I., Kim, J., Eds.; Lecture Notes in Computer Science. Springer: Berlin/Heidelberg, Germany, 2012; Volume 7728, pp. 146–157.

22. Wen, D.; Han, H.; Jain, A.K. Face spoof detection with image distortion analysis. *IEEE Trans. Inf. Forensics Secur.* **2015**, *10*, 746–761. [CrossRef]
23. Arashloo, S.R.; Kittler, J.; Christmas, W. Face spoofing detection based on multiple descriptor fusion using multiscale dynamic binarized statistical image features. *IEEE Trans. Inf. Forensics Secur.* **2015**, *10*, 2396–2407. [CrossRef]
24. Gragnaniello, D.; Poggi, G.; Sansone, C.; Verdoliva, L. An investigation of local descriptors for biometric spoofing detection. *IEEE Trans. Inf. Forensics Secur.* **2015**, *10*, 849–863. [CrossRef]
25. Mei, L.; Yang, D.; Feng, Z.; Lai, J. WLD-TOP Based algorithm against face spoofing attacks. In Biometric Recognition, Proceedings of the 10th Chinese Conference on Biometric Recognition, Tianjin, China, 13–15 November 2015; Yang, Ji., Yang, Ju., Sun, Z., Shan, S., Zheng, W., Feng, J., Eds.; Lecture Notes in Computer Science. Springer: Berlin/Heidelberg, Germany, 2015; Volume 9428, pp. 135–142.
26. Parveen, S.; Ahmad, S.M.S.; Hanafi, M.; Adnan, W.A.W. The design and compilation of a facial spoof database on various textures. In Proceedings of the 4th International Conference on Artificial Intelligence and Applications in Engineering and Technology, Kota Kinabalu, Malaysia, 3–5 December 2014; pp. 182–186.
27. Zhang, Z.; Yan, J.; Liu, S.; Lei, Z.; Yi, D.; Li, S.Z. 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.
28. Chingovska, I.; Yang, J.; Lei, Z.; Yi, D.; Li, S.Z.; Kähm, 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 IEEE Biometrics (ICB), Madrid, Spain, 4–7 June 2013; pp. 1–6.
29. Parveen, S.; Ahmed, S.M.S.; Abbas, N.H.; Naeem, N.; Hanafi, M. Texture analysis using local ternary pattern for face anti-spoofing. *Sci. Int.* **2016**, *28*, 965–971.
30. Dey, E.K.; Tawhid, M.N.A.; Shoyaib, M. An Automated System for Garment Texture Design Class Identification. *Computers* **2015**, *4*, 265–282. [CrossRef]
31. Galbally, J.; Marcel, S. Face anti-spoofing based on general image quality assessment. In Proceedings of the IEEE 2014 22nd International Conference on Pattern Recognition (ICPR), Stockholm, Sweden, 24–28 August 2014; pp. 1173–1178.