The Improved Complete Dynamic Local Ternary Pattern Texture Descriptor for Face Spoof Attacks

Sajida Parveen[1,2*], Sharifah Mumtazah Syed Ahmad Abdul Rehman[1], Nadeem Naeem[2], Jherna Devi[3,4], Mukhtiar Ahmed[4]

[1]Department of Computer & Communication Engineering, UPM Serdang, Selangor D.A 43400, Malaysia;
[2] Faculty of Electrical, Electronic & Computer Systems Engineering, QUEST Nawabshah 67480, Pakistan;
[3]Institute of Technology for Nanostructures (NST) & Centre for Nanointegration Duisburg-Essen (CENIDE), University Duisburg-Essen, Duisburg, D-47057, Germany.
[4]Department of Information Technology, QUEST Nawabshah, Sindh, pakistan

Summary
Texture analysis is widely used in the field of face liveness detection system because of its discriminant properties in differentiating between live and spoof facial samples. Most popular texture descriptor known as LBP and its extended versions had often been used to calculate the texture features for verifying the spoof attacks. However, there are several limitations with LBP and the corresponding extended descriptors. In this paper, we filled the research gap and proposed a new robust texture descriptor, which include local features by Sign, Magnitude and Center complementary components. The threshold value was dynamically set by implementing Weber's Law for threshold setting. The proposed texture descriptor was used for face liveness detection and through experimental analysis on available face spoof databases it is proved that it outperformed as compare to the stat-of-art texture descriptors.

Key words:
Liveness Detection- texture descriptor-facial biometrics- weber's law.

1. Introduction

Conventional authentication systems were often employed in the form of passwords verification or token based systems such as via smartcards validation. Such authentication systems have security limitations, such as password can be cracked and smartcards cab be stolen. Hence, biometrics authentication has been introduced in order to provide additional security to authentication system with the notion that biometrics traits belong to individual user that cannot be easily stolen. However, nowadays, the open availability of biometric traits on the printed and electronic media actually made them easier to be duplicated and spoofed. Thus, biometric based authentication systems are vulnerable to direct and indirect attacks [1,2].The direct attack is defined as, the claim identity of an individual's is changed at the time of presentation to the sensors. This research work focuses on one kind of a direct attack known as spoofing. A fake biometric is used for authentication as a legitimate user in spoofing attack.

Numerous biometric traits have been researched and implemented for identification and authentication applications such as voice, fingerprints, iris, face, ear, gait, facial thermo-grams, order, DNA, retina, hand and finger geometry. According to the International Biometric Group (IBG), face is the second most largely deployed biometric at world level in terms of market quota right after fingerprints [3]. In order to falsely gain the authentication to a system, the attacker can try to present a mask, photograph, or a video recording, showing the facial image of a legitimate client to the camera as that authorized client. From the state-of-art, texture based face liveness detection gets more attention for the researchers. Face texture based analysis methods exploit the texture patterns of real and fake faces that provide detectable information to identify the attacks. In this class, extracted feature descriptor shows certain spatial structure properties that differentiate the real skin from fake face skin surface. Unfortunately, in the face liveness detection systems, still the research continues to find the best texture descriptor for texture analysis. Moreover, most of the research work in this field has only reported the results for face liveness detection but none of them have mentioned the causes and analyzed the level of difficulty for spoof attacks with different mediums.

A novel texture descriptor is proposed in this research paper for identification of the face spoof attacks. The new descriptor also demonstrates the level of difficulty for every attack. The comparative analysis with state-of-art texture descriptor is performed on three available face spoof databases.

The rest of the research paper is organized as follows. A comprehensive literature on texture based face liveness detection and different texture descriptors is reviewed in Section 2. The proposed novel Texture descriptor is described in Section 3. The obtained experimental results

Manuscript received December 5, 2018
Manuscript revised December 20, 2018

discussed in Section 4. Finally, the conclusion is made in Section 5.

2. Related work

In the literature, various methods have been proposed to protect authentication systems from spoofing attacks such as liveness detection, multiple biometric features and the combination of biometric traits with smart cards, passwords or tokens. This paper mainly focuses on the face liveness detection method.

According to the international standards organization (ISO) under the subcommittee on biometrics [3], liveness is the quality of state of being alive, which is the evidenced by means of anatomical, physiological or behaviors characteristics. According to nature of life sign clues the categorization of face liveness detection schemes mainly based on four classes: Motion analysis, Life sign detection, hardware based analysis and texture analysis [4].

Being evidently non-intrusive, the analysis of skin texture has attracted immense amount of research interest for developing face liveness detection systems. Normally, the users are unaware of the clues, used to detect the liveness in non-intrusive face anti-spoofing systems. As such, texture based face liveness detection systems are independent of the user's response and also has the advantage of cheap hardware requirement. In other words, the data acquisition process does not require any additional expensive hardware such as thermal camera and 3D scanner, which makes them easier to implement.

Local Binary Pattern (LBP) has widely been used for face liveness detection [5, 6 and 7]. The texture features of the face were analyzed with LBP and its variants (such as multi-scale LBP) for photo and video based spoof attacks.

Also the LBP descriptor extracted from Three Orthogonal Planes (LBP–TOP) [8], where time and space information were combined into a single descriptor with multi-resolution strategy composing of the structural and dynamic texture properties of the image. The experiments were conducted on two publicly available databases: CASIA face Anti-Spoofing and Print-Attack Database. The system was designed to detect photo and video based spoofing attacks. The texture analysis of captured (live) and re-captured (spoof) facial images was investigated by using local binary pattern variance (LBPV) [9] and DoG filter to characterize the contrast between live face and photo images. Though, this method is simple to implement, illumination invariant and robust to change in image orientation, it effectiveness was only demonstrated on photo based spoofing attacks.

Housam et al. [10] proposed an extension of LBP known as Local Graph Structure (LGS) for face liveness detection. LGS used six pixels to generate the binary code and the calculation of the pattern starts from the target pixel to the left region of the graph in anti-clockwise direction and then to right region in a clockwise direction. In this process, the edges of two pixels are connected through vertices with a binary number 1 assigned if the gray value of the neighbor pixel is greater than or equal to the target pixel, otherwise binary 0 is assigned. The spoofing rate of LGS was evaluated on NUAA imposter database.

A general image quality assessment based method was proposed in [11] to extract 14 image quality features. The extracted features of such quality measures were combined via LDA classifier to separate the real and fake access attempts. Two publicly available databases: REPLAY-ATTACK and CASIA-FAS were considered for evaluation of the anti-spoofing method. The system achieved more promising results to protect the face recognition system.

Recently, LBP based Image Distortion Analysis (IDA) for face spoof detection was presented in [12]. The technique examines the reflection of light, blurriness, the quality of image and color diversity distortion in printed photo or LCD screen image. For IDA feature extraction, four different features i.e. spectular reflection, blurriness, chromatic moment and color diversity were extracted using LBP operator and multiple Support Vector Machine (SVM) were used for classification. The experiments were conducted on three databases: Mobile face spoofing database (MSU MFSD) and two public-domain face spoof databases (Idiap REPLAY- ATTACK and CASIA FASD).

Another new method based on kernel discriminant analysis was proposed for analyzing the dynamic texture in video sequences [13]. The method utilized multi dynamic texture descriptor based on binarized statistical image features of three orthogonal planes (MBSIF-TOP) to detect the face spoof attacks. The authors also performed the fusion of two texture descriptor i.e. MBSIF-TOP and multi-scale local phase quantization (MLPQ-TOP) for face liveness detection. For classification kernel discriminant analysis (KDA) was adopted to classify the fused texture pattern. The performance of the system showed the effectiveness of statistical independence of texture analysis, while, synthesis attack was discovered as the limitation of this approach.

The detailed study and potential use of joint quantization of local feature texture descriptors is provided [14] for face liveness detection. Various biometric traits such as iris, fingerprint and face were utilized to evaluate the performances of these texture descriptors. In this literature review and for comparison analysis, only the results on face trait are considered. The experimental analysis was carried out on REPLAY-ATTACK DB.

By utilizing the three orthogonal planes, an extended WLD called as WLD-TOP local descriptor, has been proposed in [15]. The WLD-TOP was the combination of temporal and spatial information into a single descriptor with a multi-resolution strategy. Numerous experiments were conducted on two databases (CASIA and self collected SYSU-MFSD) by generating intra and cross-datasets. WLD-TOP descriptor has achieved a better liveness detection performance in both intra and cross-databases.

Despite their effectiveness, the previously proposed texture descriptors e.g. LBP, LBP-TOP, LVP, GLBP are unable to cope with issues in the analysis related to illumination, blur, rotation and scaling. LBP texture descriptor and its variants utilize two values in each pattern. One is the center pixel, which is used normally as a threshold value and the other is neighboring pixels. These neighboring pixels are the gray values around the center pixel value in each patch of the pattern. As the LBP code is based on the threshold value that is generally considered as a center pixel of the pattern, it is obvious that LBP is very sensitive to the noise effect on the central pixel. This limitation of LBP is observable when two different codes are generated by LBP for two similar patterns in an image. Therefore, it can be considered that all the other extensions of LBP also face the same limitation.

Local Ternary Pattern (LTP) [16] was introduced to overcome noise sensitivity with central pixel in LBP. In LTP, the descriptor is quantized into three levels (-1, 0, and 1) and decomposed into two higher and lower descriptors by assigning the threshold value with respect to the center pixel. However, one of the main challenges of LTP is the difficulty to set the right threshold value for a particular application in order to increase the performance. Besides that, another prominent issue with LTP is when the threshold value becomes exactly the same as the difference of central and neighbor hood pixels. In such case the generated code of LTP turns out to be zero. To deal with these issues of threshold in LTP descriptor, recently noticeable extensions of LTP known as Improved Local Ternary Pattern (ILTP) [17], Local Adaptive Ternary Pattern (LATP) [18], Dynamic Local Ternary Pattern (DLTP) [19] and Enhanced Local Ternary Pattern (ELTP) [20] have been proposed, which are based on some automatic strategy to adaptively set the threshold value in each local region.

Basic operation of LBP descriptor is based on the sign of the patch derived from calculating the difference between the central and neighboring pixels while the original value (magnitude) is neglected. All the state-of-the-art texture descriptors follow similar approach for deriving the representations. Nevertheless, there are some cases where the information generated from the local features is not sufficient for classifying the patterns. Moreover, the neighborhoods with different visual perceptions may have the same binary code by the LBP-based. Therefore, the counter measures were proposed in Complete Local binary Pattern (CLBP) [21] and Complete Local Ternary Pattern (CLTP) [22] in which the extracted information is considered by joining the sign and magnitude component of the pixels and also considered the global intensity value for getting more accurate information about the patterns. Based on the review of previous work, it can be concluded that, none of the currently existing texture descriptors covers all the aforementioned limitations.

2.1 Main Contributions

- The main contribution of this paper is to propose a novel texture descriptor Complete Dynamic Local Ternary Pattern (CDLTP) that overcome the limitations of LBP and its extended operators by extracting three types of feature (CDLTP_S, CDLTP_M and CDLTP_C) for more accurate coding and solve the problem of specific threshold value in LTP operator for particular application via Weber’s law. The proposed descriptor shares similar representation as presented in [22 and 23]. However, the threshold value is adopted by reformulating the Weber’s law for image analysis.
- The proposed texture descriptor CDLTP utilized for face liveness detection to calculate more discriminative information for texture patterns of original skin and spoof attacks in terms of sign, magnitude, center grey value and dynamically adoption of threshold value in ternary quantization for local region of image.
- Furthermore, the comparison has been performed on five state-of-art texture descriptors and three publicly available face spoof database. According to that the proposed CDLTP outperformed in terms of detection rate and ROC.

3. Proposed Method

In an image patch, it is plausible that the contrast locations contain highly valuable information which can be comprehensively described by a feature descriptor. However, a minor variation in contrast may have a very deterring effect on detection performance. The contrast of an image can be affected by the type of sensors, in addition to acquisition factors such as image resolution, ambient lighting, and flash of the acquisition sensor. In theory, a precise interpretation of these observations can be derived using the Weber’s law, which states that the just noticeable difference (jnd) between two stimuli is directly proportional to the magnitude of the stimuli [23]. In other words, the ratio of the increment threshold to the background intensity is constant. This relation known as Weber's Law, can be formally expressed as:

$$k = \Delta I / I \,, \tag{1}$$

where ΔI represents the increment threshold (just noticeable difference for discrimination); I represents the initial stimulus intensity, and k signifies that the proportion on the right side of the equation remains constant despite variation in the term I . Following this assumption, we therefore adopt Weber's law in this paper to set the threshold value of Complete model of Local Ternary Pattern (CLTP).

However, it is worth noting that in order to make the Weber's law meaningful in terms of 2D image representation, we replaced the original terms in Eq.1 as follow:

$$|w_p - w_c| = \Delta I; \quad w_c = I; \quad \varepsilon = k \tag{2}$$

Where $|w_p - w_c|$ which is equivalent to the jnd represents the difference between a centre pixel w_c and the neighboring pixel w_p and ε is the Weber's law constant. Thus, we reformulate Eq.1 as:

$$\varepsilon = \frac{|w_p - w_c|}{w_c} \,, \tag{3}$$

Consequently, the threshold value can be derived by applying Eq.3 as:

$$\tau = w_c \times \varepsilon \,, \tag{4}$$

where τ is the threshold value, w_c is the center pixel and ε is the constant or scaling factor. Furthermore, the value of the threshold τ in Eq.4 is utilized to generate ternary quantization codes:

$$\alpha = \mathrm{w_c} + \tau \,, \tag{5}$$

$$\beta = \mathrm{w_c} - \tau \,, \tag{6}$$

In a local neighborhood, the texture pattern depending on the values of quantization codes can be computed as:

$$s(x) = \begin{cases} 1 & if \quad w_p \geq \alpha \\ -1 & if \quad w_p \leq \beta \\ 0 & otherwise \end{cases} . \tag{7}$$

We use the threshold value τ from intensity differences between its neighbors and a current pixel as the changes of the current pixel. By means of Weber's law, we are able to find the salient variations within an image. Specifically, in ternary quantization we attempt to preserve more discriminating information in comparison to using the absolute fix value of threshold τ for whole image.

In addition to the proposed CDLTP, we proceed further to enhance the discriminating property of texture descriptor by introducing three types of texture features: global intensity, sign and magnitude components. Typically, there are two decompositions of CDLTP: (1) sign complementary components and (2) magnitude complementary components. These two components can be expressed as:

$$\mathrm{s_p^{high}} = \mathrm{s(w_p} - \alpha) \,, \tag{8}$$

$$\mathrm{s_p^{low}} = \mathrm{s(w_p} - \beta) \,, \tag{9}$$

$$\mathrm{m_p^{high}} = \mathrm{s(w_p} - \alpha) \,, \tag{10}$$

$$\mathrm{m_p^{low}} = \mathrm{s(w_p} - \beta) \,, \tag{11}$$

where w_p is the gray value of the neighboring pixel, s_p^{high}, s_p^{low}, m_p^{high} and m_p^{low} are the sign and magnitude complementary components of the lower and higher patterns for ternary quantization. The complete model of the higher pattern with a sign complementary component can be derived from Eq.8 as:

$$\mathrm{CDLTP\_S_{(P,R)}^{high}} = \sum_{\mathrm{p=0}}^{\mathrm{p\text{-}1}} 2^{\mathrm{p}} \mathrm{s(w_p} - \alpha) \,, \tag{12}$$

$$s_p^{high} = \begin{cases} 1, & w_p \geq \alpha \\ 0 & otherwise \end{cases} \,, \tag{13}$$

where P is the numbers of neighboring pixels used for each patch and R is the radius of the patch. Likewise, the complete model of the lower pattern of sign complementary component is built using Eq.9.

$$\mathrm{CDLTP\_S_{(P,R)}^{low}} = \sum_{\mathrm{p=0}}^{\mathrm{p\text{-}1}} 2^{\mathrm{p}} \mathrm{s(w_p} - \beta) \,, \tag{14}$$

$$s_p^{low} = \begin{cases} 1, & w_p < \beta \\ 0 & otherwise \end{cases} , \quad (15)$$

The final descriptor of sign component can be expressed in compact form using Eq.12 and Eq.14.

$$CDLTP\_S_{P,R} = [CDLTP\_S_{P,R}^{high} \quad CDLTP\_S_{P,R}^{low}] \quad (16)$$

Looking at Eq.12 and 14 independently, it can be observed that the higher and lower sign components are equivalent to LBP, thus it was noted that most of the information of the local differences are encoded in the sign component but with more comprehensive and discriminative representation by combining the higher and lower feature vectors in Eq.16.

Similarly, the magnitude complementary component of the higher pattern is computed by using Eq.10 as follows:

$$\mathrm{CDLTP\_M}_{(P,R)}^{high} = \sum_{p=0}^{p-1} 2^p \, t(m_p^{high}, v) , \quad (17)$$

$$t(m_p^{high}, \gamma) = \begin{cases} 1, & |w_p - \alpha| \geq v \\ 0, & |w_p - \alpha| < v \end{cases} , \quad (18)$$

Where v is the mean value of mp in the whole image. The lower pattern of the magnitude complementary component is also expressed by using Eq.11 as:

$$\mathrm{CDLTP\_M}_{(P,R)}^{low} = \sum_{p=0}^{p-1} 2^p \, t(m_p^{low}, v) , \quad (19)$$

$$t(m_p^{low}, \gamma) = \begin{cases} 1, & |w_p - \beta| \geq v \\ 0, & |w_p - \beta| < v \end{cases} , \quad (20)$$

Eventually, the complete magnitude component for CDLTP is generated from Eq.17 and 19 as follows:

$$CDLTP\_M_{P,R} = [CDLTP\_M_{P,R}^{high} \quad CDLTP\_M_{P,R}^{low}] . \quad (21)$$

According to the Eq.21 the CDLTP_M also produces binary strings so that it can be conveniently used together with rest of the CDLTP operator for skin texture pattern classification. The magnitude component contributes as additional discriminative information, which is beneficial for accurately classifying spoof attacks from high quality face samples.

Moreover, to further enhance the discriminative property of the proposed descriptor, the center operator is computed in similar fashion to the sign and magnitude complementary components.

$$CDLTP\_C_{P,R}^{high} = t(\alpha, v_i) , \quad (22)$$

$$CDLTP\_C_{P,R}^{low} = t(\beta, v_i) , \quad (23)$$

Where vi is the average gray level of the whole image. $CDLTP\_C_{P,R}^{high}$ and $CDLTP\_C_{P,R}^{low}$ are then combined to build the central operator.

$$CDLTP\_C_{P,R} = [CDLTP\_C_{P,R}^{high} \quad CDLTP\_C_{P,R}^{low}] \quad (24)$$

The center pixel, which expresses the local gray level of the image, also has discriminative information. To make it consistent with CDLTP_S and CDLTP_M, it is calculated as expressed in Eq.24 from higher and lower levels.

The framework of Complete Dynamic Local Ternary Pattern (CDLTP) is presented in Fig.1 where we explore all three types of features for analyzing the texture pattern in real and spoof faces. In the first stage, the original image is input to the CDLTP texture descriptor which calculates its center gray level C and the local difference. In the second step, the local difference is then decomposed into the sign S and magnitude M components.

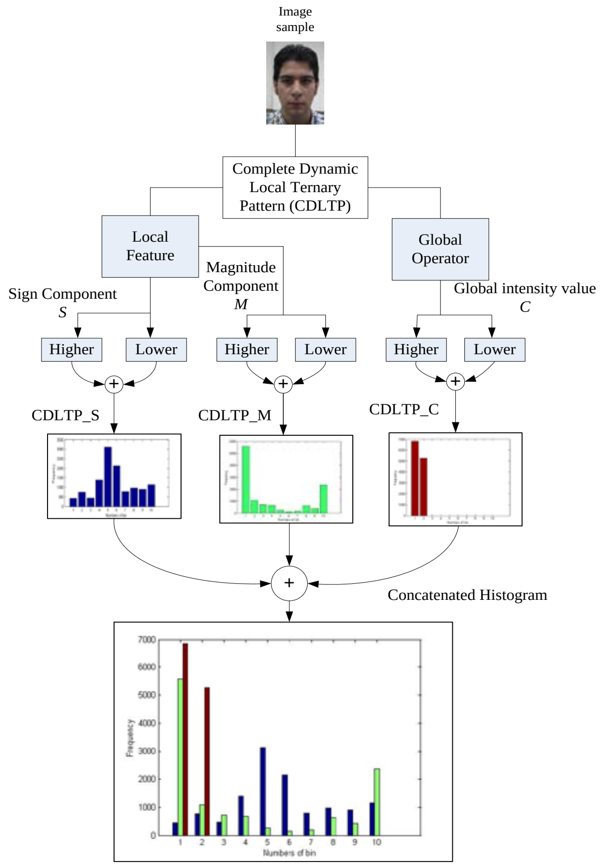

Fig. 1 Framework of the proposed Complete Dynamic Local Ternary Pattern (CDLTP).

Furthermore, each sign and magnitude component is also decomposed into Higher (h) and Lower (l) level for calculating the ternary code. Similarly, global intensity operator C is also decomposed into higher (h) and lower (l) levels. Consequently, three operators, namely global intensity (CDLTP_C), sign operator (CDLTP_S) and magnitude operator (CDLTP_M) are proposed to code the C, S, and M features, respectively. Then, the CDLTP_C, CDLTP_S, and CDLTP_M codes are combined to form the CDLTP feature map of the original image. Finally, a CDLTP histogram to be used as feature vector for a classifier which is used to classify the texture of spoof attacks. To combine the codes of CDLTP_S, CDLTP_M and CDLTP_C, the combination method of histograms reported in [22] is adopted. The three CDLTP_S, CDLTP_M and CDLTP_C codes calculates the histograms separately and then concatenated together.

4. Experimental setup and Datasets

In this paper, we have evaluate the performance of the proposed method on three publicly available databases: CASIA Face Anti-Spoofing Database [24], the Replay-Attack database [25] and the NUAA database [26]. The details of the three databases are discussed below in subsection and presented in Table 1.

4.1. 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 by using conventional camera in three different sessions under varying environmental and illumination conditions. There are 500 images for each subjects' recording. The resolution of the images is 640 × 480 for 15 subjects. The subjects that appeared in testing and training sets are quite different, as six out of the 15 subjects do not appear in the training set for live human case and six out of the 15 subjects do not appear in the training set for photo case.

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

The CASIA FASD contains training and testing data set of 50 subjects. The training data set comprised of 20 subjects and test dataset contains 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 standards 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 evaluation of our experiment. In this scenario, all the data are combined to be used for a general and overall evaluation.

4.3. Replay-Attack Database

The Replay-Attack database consists of real access and spoof attacks of 50 subjects. The database is comprised of a total of 1200 video recordings which include 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 in 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 is comprised of 360 videos of 60 real and 300 attack attempts. The testing set consists of 480 videos of 80 real-access and 400 attack videos. In this experiment, the training set is utilized to train the classifier, the development set to adjust the parameters of the classifier, and the testing set to evaluate the performance of the model.

4.4. Classification

For classification of the positive (genuine face) and negative (spoof face) samples for face liveness detection, we used Support Vector Machine (SVM) with linear kernel. In all experiments on UPM face spoof, CASIA, Replay-Attack and NUAA databases, we used C=100 as the regularization parameter for linear SVM. The patch size value (P), and radius (R) for CDLTPP, R and other texture descriptors were set as eight and two respectively, for each pattern in a local region.

Table 1: Details about the data partitioning (Geniune+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	22497+69686	22498+70246	29791+93686

5. Results and Discussions

Various experiments are conducted to examine the robustness and performance of the proposed CDLTP texture descriptor for face spoof attacks as compared to other state-of-the-art texture descriptors.

a. Compared with other texture descriptors

Numerous texture descriptors have been reported in the literature, however we compared the proposed CDLTP with LBP, LTP, DLTP, CLBP and CLTP in Table 2, because they are commonly used texture classification. Moreover, the performance comparison is also illustrated in Fig.4 in terms of Receiver Operating Characteristic (ROC) curve.

Table 2: Performance comparison of face liveness detection using different texture descriptors (%)

Technique	HTER	Rate	AUC
Complete Dynamic Local Ternary Pattern (CDLTP)	**3.4**	**96.547**	**0.987**
Complete Local Binary Pattern (CLBP)	**10.12**	**89.87**	**0.924**
Complete Local Ternary Pattern (CLTP)	**8.547**	**91.45**	**0.9247**
Local Binary Pattern (LBP)	**15.41**	**84.59**	**0.76**
Local Ternary Pattern (LTP)	**15.81**	**84.18**	**0.785**
Dynamic Local Ternary Pattern (DLTP)	**8.762**	**91.23**	**0.91**

From the obtained results in Table 2, it can be notice that, all the Complete models i.e. CLBP, CLTP and CDLTP outperformed other related techniques. This is because the calculated features from the complete model contain more information about the texture patterns in terms of its local and global feature information of the image.

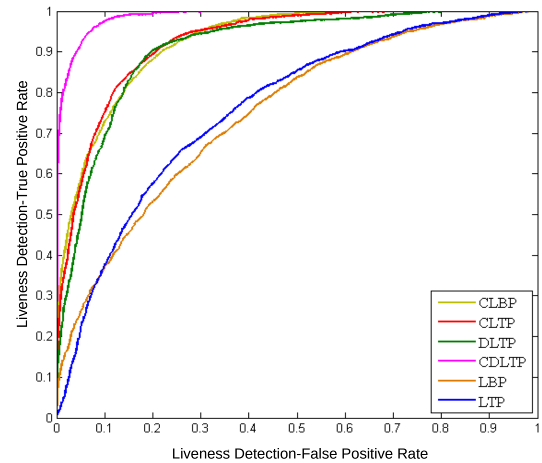

Fig. 4 ROC curve of face liveness detection by using different texture descriptors.

Amongst all texture descriptors, the proposed CDLTP descriptor attained the highest accuracy of 96 % with smallest error rate HTER of 3.4 % for face liveness detection. The result shows that CDLTP texture descriptor improves the robustness for face liveness detection system and calculates more informative features that help to improve the quality of texture analysis.
For visual comparison, it can be noticed in Fig 4 that Complete Dynamic Local Ternary Pattern (CDLTP) outperformed the other 5 state-of-the-art texture representation methods with an AUC of 0.98.

b. Performance evaluation on public datasets

To evaluate the performance of proposed Complete Dynamic Local Ternary Pattern (CDLTP) texture descriptor, different public domain face spoof databases such as NUAA, REPLAY Attack and CASIA are utilized to compare the achieved result of CDLTP with reported results on these databases.
The performance of proposed Complete Dynamic Local Ternary Pattern (CDLTP) texture descriptor in Table 3 is compared three publicly available databases i.e. NUAA, REPLAY-ATTACK and CASIA face spoof databases for face liveness detection. The generated result from calculated features of CDLTP is presented in Table 2 along with other reported results from state-of-the-art and with the published literature from the competition of Tabula RASA with 2D facial spoofing attacks. The HTER was adopted for the comparison analysis, because mostly results are reported in HTER in literature.
The evaluation shows that the proposed calculated features with CDLTP have more ability to discriminate the fake faces as compare to the LBP and other variants of LBP

based features. This is important to note that overall performance of CDLTP on all three public domain database for face liveness detection in texture analysis was outperformed as compared with other reported results in the literature.

Table 3: Comparison of CDLTP with state-of-the-art for face liveness detection on REPLAY-ATTACK, NUAA, CASIA face spoof databases (*[7]; **[14]).

Dataset	Approaches	HTER (%)
REPLAY-ATTACK	IQA[11]	15.2
	IDA+SVM [12]	7.4
	LBP-TOP [8]	7.60
	*LBP+SVM	15.16
	LLR [9]	5.47
	Fusion [29]	1.76
	*LBP+LDA	17.17
	*LBP	13.87
	MLPQ-TOP+KDA [13]	3.75
	MBSIF-TOP+KDA [13]	1.38
	Kernal Fusion [15]	1.0
	DMD+SVM [30]	7.5
	DMD+LBP+SVM [30]	3.75
	**CoA-LBP	9.4
	**Ric-LBP	14.7
	**WLD and **LPQ	17.5 and 21.7
	**BSIF	12.6
	**LCPD	14.0
	**Keypoint SIFT	25.2
	**Dense SIFT	17.0
	**DAISY	17.2
	**SID	10.5
	CDLTP	**0.68**
NUAA	*LBP+LDA	18.32
	*LBP+SVM	19.03
	*LBP +SVM	13.17
	*(LBP8,1+LBP8,2+LBP16,2) +SVM	2.5
	*LBP+SVM	4.23
	LBPV+DoG [9]	11.97
	LBPV[9]	23.46
	CDLTP	**1.97**
CASIA	*LBP+LDA	21.01
	*LBP+SVM	18.17
	*LBP+SVM	18.21
	LBP-TOP [8]	10
	DoG-based [24]	17
	IQA [11]	32.4
	CDLTP	**6.82**

6. Conclusion

To discover the best texture descriptor for face liveness detection, the expectation is to find unique approach that has the capability to discriminate the medium of fake faces from the original skin. The novel texture descriptor Complete Dynamic Local Ternary Pattern, which is proposed in this paper for face spoof attacks, showed quite promising results in this context. The Weber's law for dynamic setting of threshold value and complete modeling with sign and magnitude components extend the functionality of the descriptor. A comprehensive evaluation of the performance of the descriptor on face liveness detection is conducted on three available facial spoof datasets. Moreover, CDLTP outperformed as compared to the stat-of-the-art techniques on three public domain datasets. This is concluded that proposed texture descriptor CDLTP outperforms in every aspect as compared to the other reported texture descriptors i.e. LBP, LTP, DLTP, CLBP and CLTP.

References

[1]. N. Edrogmus, S. Marcel, Trusted biometrics under spoofing attacks, in: S. Marcel, M. S. Nixon, S. Z. Li, (Eds.), Handbook of biometric anti-spoofing, Springer-Verlag, London, 2014.

[2]. S. Parveen, S. M. S. Ahmad, M. Hanafi, W.A.W. Adnan, " Face anti-spoofing methods", Current Science, 108 (2015) 1491-1500.

[3]. International Biometrics Group, Biometrics market and industry report 2009-2014, IBG, Virginia. USA, 2008.

[4]. A. Adler, S. Schuckers, Biometric Vulnerabilities, Overview. In Encyclopedia of Biometrics, Springer US, 2014, 160-168.

[5]. A. Hadid, The Local Binary Pattern Approach and its Application to Face Analysis, In: Image Processing theory, tools and applications (IPTA), 2008, IEEE, 1-9.

[6]. J. Maatta, A. Hadid, M. Pietikäinen, Face spoofing detection from single images using micro-texture analysis. IEEE, Washington, DC, 2011, 1-7.

[7]. I. Chingovska, A. Anjos, S. Marcel, On the effectiveness of local binary patterns in face anti-spoofing. In Proceedings of International Conference on BIOSIG, IEEE, Darmstadt, 2012, 6–7.

[8]. T. De Freitas Pereira, J. Komulainen, A. Anjos, J. M. De Martino, A. Hadid, M. Pietikäinen, S. Marcel, Face liveness detection using dynamic texture, EURASIP Journal on Image and Video Processing, 2014, 1-15.

[9]. N. Kose, J. L. Dugelay, Classification of captured and recaptured images to detect photograph spoofing. In APR International Conference on Informatics, Electronics & Vision IEEE, Dhaka, 2012, pp. 1027–1032.

[10]. K. B. Housam, S. H. Lau, Y. H. Pang, Y. P. Liew, M. L. Chiang, Face Spoofing Detection Based on Improved Local Graph Structure. International Conference on Information Science and Applications (ICISA), IEEE, 2014, 1-4.

[11]. J. Galbally, S. Marcel, Face anti-spoofing based on general image quality assessment. In Proceedings of the IEEE 22nd International Conference on Pattern Recognition (ICPR), Stockholm, Sweden, 24–28, 2014; 1173-1178.

[12]. D. Wen, H. Han, A. K. Jain, Face spoof detection with image distortion analysis. IEEE Transactions on Information Forensics and Security, 10(4), 2015, 746-76.

[13]. S. R. Arashloo, J. Kittler, W. Christmas, Face spoofing detection based on multiple descriptor fusion using multiscale dynamic binarized statistical image features. IEEE Transactions on Information Forensics and Security, 10, 2015, 2396-2407.

[14]. D. Gragnaniello, G. Poggi, C. Sansone, L. Verdoliva, An investigation of local descriptors for biometric spoofing detection. IEEE Transactions on Information Forensics and Security, 2015, 10, 849-863.

[15]. L. Mei, D. Yang, Z. Feng, J. Lai, WLD-TOP Based Algorithm against Face Spoofing Attacks. Biometric Recognition, Springer International Publishing, 2015, 135-142.

[16]. X. Tan, B. Triggs, Enhanced local texture feature sets for face recognition under difficult lighting conditions. IEEE Transactions on Image Processing, 19, 2010, 1635-1650.

[17]. W. Yang, C. Sun, 2011. Face recognition using improved local texture patterns. 9th World Congress on Intelligent Control and Automation (WCICA), IEEE, 2011, 48-51.

[18]. M. Akhloufi, A. Bendada, Locally adaptive texture features for multispectral face recognition. IEEE International Conference on Systems Man and Cybernetics (SMC), 2010. IEEE, 3308-3314.
[19]. M. Ibrahim, M. I. Alam Efat, S. H. Kayesh, S. M. Khaled, M. Shoyaib, M. Abdullah-Al-Wadud, Dynamic Local Ternary Pattern for Face Recognition and Verification. In International Conference on Computer Engineering and Applications, 1012(8), 2014, Tenerife, Spain.
[20]. W. Zhenyu, H. Rong, Y. Wankou, S. Changyin, An enhanced Local Ternary Patterns method for face recognition. 33rd Chinese Control Conference (CCC), IEEE, 2014, Nanjing, China, 4636-4640.
[21]. Z. Guo, L. Zhang, D. Zhang, A completed modeling of local binary pattern operator for texture classification. IEEE Transactions on Image Processing, 19, 2010, 1657-1663.
[22]. T. H. Rassem, B. E. Khoo, Completed local ternary pattern for rotation invariant texture classification. The Scientific World Journal, 2014.
[23]. G. Ekman, Weber's law and related functions. The Journal of Psychology, 1959, 47(2), 343-352.
[24]. Z. Zhang, J. Yan, S. Liu, Z. Lei, D. Yi, S. Z. Li, A face antispoofing database with diverse attacks. In Proceedings of the 5th IAPR International conference on Biometrics (ICB), New Delhi, India, 2012, 26-31.
[25]. I. Chingovska, A. Anjos, S. Marcel, On the effectiveness of local binary patterns in face anti-spoofing, in Biometrics Special Interest Group (BIOSIG), IEEE BIOSIG-Proceedings of the International Conference, 2012, 1-7.
[26]. X. Tan, Y. Li, J. Liu, L. Jiang, 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, K. Daniilidis, P. Maragos, N. Paragios, (Eds.), Lecture Notes in Computer Science. Springer Berlin/Heidelberg, Germany, 2010, Volume 6316, 504–517.
[27]. K. Eismann, S. Duggan, T. Grey. Real world digital photography. Peachpit Press (Pearson Education), Berkeley, CA, 2010, 3rd Edition.
[28]. D. Caetano Garcia, R. L. de Queiroz, Face-Spoofing 2D-detection based on Moiré-Pattern analysis. IEEE Transactions on Information Forensics and Security, 2015, 10(4), 778-86.
[29]. J. Komulainen, A. Hadid, M. Pietikainen, A. Anjos, S. Marcel, Complementary countermeasures for detecting scenic face spoofing attacks. IEEE International Conference on Biometrics (ICB), 2013, 1-7.
[30]. S. Tirunagari, N. Poh, D. Windridge, A. Iorliam, N. Suki, A. T. S. Ho, Detection of face spoofing using visual dynamics. IEEE Transactions on Information Forensics and Security, 2015, 10(4), 762-777.

Sajida Parveen Soomro received her Bachelor of Engineering in Computer Systems from Quaid-e-Awam University of Engineering, Science and Technology Nawabshah, Pakistan in 2006. She completed her Master of Engineering in Communication Systems and Network from Mehran University of Engineering and Technology Jamshoro, Pakistan in 2011. Sajida earned her PhD from Universiti Putra Malaysia in 2016. She joined as a Lecturer in 2007 and currently working as Assistant Professor in the department of Computer Systems Engineering, Quaid-e-Awam University of Engineering, Science and Technology Nawabshah, Pakistan and her field of interest is communication, biometrics, security, image processing and machine learning. Currently engaged with undergraduate and postgraduate research projects in various research areas including finger spoofing, green computing, shape and diseases detection, cultural marks for web designs and etc.

Telecommunications of Japan to study digital beamforming antennas, mobile satellite communication systems, and wireless access network using stratospheric platforms. He now with DDI Tokyo Pocket Telephone, Inc.