BULGARIAN ACADEMY OF SCIENCES

CYBERNETICS AND INFORMATION TECHNOLOGIES • Volume **20**, No 3
Sofia • 2020 Print ISSN: 1311-9702; Online ISSN: 1314-4081
DOI: 10.2478/cait-2020-0035

A Novel Feature Descriptor for Face Anti-Spoofing Using Texture Based Method

Raghavendra R. J., R. Sanjeev Kunte

Department of Computer Science and Engineering, JNN College of Engineering, Shimoga-577204, Karnataka, India
E-mails: raghavendra.r.j@jnnce.ac.in sanjeevkunte@jnnce.ac.in

***Abstract*:** *In this paper we propose a novel approach for face anti-spoofing called Extended Division Directional Ternary Co-relation Pattern* (*EDDTCP*). *The EDDTCP encodes co-relation of ternary edges based on the centre pixel gray values with its immediate directional neighbour and its next immediate average directional neighbour, which is calculated by using the average of cornered neighbours with directional neighbours. The proposed method is robust against presentation attacks by extracting the spatial information in all directions. Three Experiments were performed by using all the four texture descriptors* (*LBP, LTP, LGS and EDDTCP*) *and the results are compared. The proposed face anti-spoofing method performs better than LBP, LTP and LGS.*

***Keywords*:** *Face Anti-spoofing, Extended Division Directional Ternary Co-relation Pattern* (*EDDCP*), *Texture analysis, Replay-Attack.*

1. Introduction

In recent times, face authentication system has received more and more attention, which is based on the identity of the image/video of face and decides to accept or reject the input based on the matching. Compared with the conventional verification system which makes the user to draw pattern and password in one stroke, the face authentication system has the exclusive benefit to authenticate a person since intruder can easily use the stolen passwords. Furthermore, face recognition is normally non-intrusive and images/videos of face can be easily acquired with various digital devices, hence face authentication system has been used in various capacities such as information security and access control. Many methods have been proposed recently on face recognition due to its popularity in terms of its usage in many security systems. However, the face authentication system can be easily spoofed by fake/spoof image/video [1, 2]. Because of rapid spread of images/videos of face over internet, face spoofing becomes much easier by means of social networking. Therefore, there is a urgent need of filtering off capability of the spoof faces to secure the face recognition system.

The research over face anti-spoofing has been developing in recent time. The spoofing attack is defined as an intruder pretending to be genuine user to gain illegal access and data of a system or person. The most common types of attacks are photo-attack, video-attack and 3D-mask attack. In photo attack, intruder tries to reproduce a face image on paper or exhibit on the display of digital device. Besides the screen and paper, an innovative spoofing method is the disguising attack with cut eyes and mouth presented in [3]. In video attacks, intruder portraying a face video using digital device for face spoofing. Video attacks are more sophisticated compared to photo attacks since they provide the liveness and motion data to enhance the sense of reality. The 3D-attacks are based on the 3D-face model with advancement of 3D-printing technology [4]. However, 3D-attacks are more costly compared to photo and video attacks.

In face anti-spoofing texture based approaches were used. These approaches comprises a technique of face anti-spoofing using Local Ternary Pattern (LTP), Local Binary Pattern (LBP) and Local Graph Structure (LGS) to categorize between genuine and attack faces. LTP uses ternary values, which is an extended version of LBP, and it is not affected by noise. LTP is variant to changes in gray values. However, the LGS uses imbalance graph structure and extracts uneven information compared to left than right side of graph.

The disadvantages of LTP, LBP and LGS feature descriptors inspire us to suggest a new method for face anti-spoofing. In this paper, we propose a novel feature descriptor called an Extended Division Directional Ternary Co-relation Pattern (EDDTCP) for face anti-spoofing system, which is based on extracting features from the face images in order to address problem of spoofing.

The main contributions are listed as follows:

1. To obtain more spatial information, a new descriptor is developed which is expressed as co-relation difference based on center pixel and average of neighbour's pixel.
2. The proposed method is robust in nature compared to (SOTA) state of the art approaches under different lighting settings.
3. The proposed method performance is verified on various anti-spoofing datasets.

The rest of the paper is structured as follows. Section 2 discusses the existing methods in detail. In Section 3, we present the overview of system architecture of our proposed method of face anti-spoofing system. Section 4 presents the experimental results and discussion. Finally, conclusion is presented in Section 5.

2. Literature survey

The existing literature based on various descriptors are reviewed in this section.

A handcrafted method based on Local Binary Pattern (LBP), builds the histogram of values of grayscale of the image. A given set of familiar images and their histograms are used to train classifier such as Support Vector Machine (SVM) to predict test face is real or spoof [5]. In some other works, a given face image is segmented into patches and produce histogram of each and concatenated to produce

a greater number of features of that image [6]. An extension of LBP based method called Multi-scale Local Binary Pattern (MLBP) was proposed [39]. This method produces the histograms on varying number of neighbourhood pixels (P and R values) of the LBP. A different version of LBP was proposed called Dynamic Local Ternary Patterns (DLTP) [7]. This method uses three labels instead of two (by the conventional LBP) by comparing a center pixel with its neighbours to produce LTP code.

The reflectance information of given image used as countermeasure in face anti-spoofing has appealed the attention of many researchers. 2D and 3D face masks were used in face spoofing. In order to tackle this problem, authors in [8] have proposed method based on the reflectance analysis on the image textures. This method proved better results compared to texture analysis based methods for mask detection. Another work [9] uses multispectral lighting to represent multispectral reflectance to differentiate among real, spoof face and different types of masks made of sponge, paper etc. As a result, two different light wavelengths have been selected (850 nm and 1450 nm) to differentiate real/spoof. In similar work [10], two different wavelengths have been chosen (685 nm and 850 nm) after checking the albedo curves existed in the mask materials and face. In single 2D image, method shows higher reflectance contrast compared to images used by photometric stereo method.

In last few years, lot of improvement has occurred in face anti-spoofing techniques. Earlier methods uses Gabor wavelets [11] or blinking of eye in order to find whether the liveness detection existed in the given image or not [12]. These methods had basic detection of liveness and low computational cost. However, detection of eye blinks can be targeted using cut-photo attack and very low accuracy. Another advancement found from LBP uses Three-Orthogonal-Planes (LBP-TOP) to accomplish face anti-spoofing [13]. The advancement increases the accuracy, by maximum advantaging of the dynamic texture power, motion analysis and texture, alongside a fusion-based framework of score level. However, the method shows very little improvement and is unable to cope up with low quality videos presentationss in CASIA-FASD database.

In [14], a score-fusion framework was suggested, giving more awareness on quality of the database. However, in score-fusion framework only such techniques are included which are statistically independent and other techniques such as potential methods are statistically scrutinized before it can be considered. In [15], context-based anti-spoofing technique was proposed. It shows how HOG (Histogram of Oriented Gradients) descriptors are used to detect scenic cues and analysis of the upper part of the body could be used. There is a lot of improvement in results with respect to video attacks. However, this method is restricted to specific attack scenes and is limited to indoor environments.

In [16], Holistic face (H-face) is created by using different feature vectors of 12 different components. The performance of H-face is very good but limited to use in real time applications due to its high computations. The method proposed in [17] uses extension of conventional LBP methods by performing motion enlargement using vectors of optical flow before LBP histograms. However, it gives small improvement over performance but it lacks in the same issues suffered by other LBP type

descriptors. In another method [18], image quality assessment is used in face anti-spoofing. The assessment may contain combination of different measures such as difference of pixels, edges and co-relation. The features like Total Edge Difference (TED), Average Distance (AD) and Signal to Noise Ratio (SNR) that use very low computation could be used in real time applications. However, performance of this approach is very minimal compared to other approaches.

Anti-spoofing approach based on colour images is proposed in [19] by using LBP in different color space, such as RGB, HSV and YC_bC_r. This approach shows very encouraging results but lacks of variation of light and environment. The existence of Moir'e pattern in the videos [20] can be used to differentiate the real and spoof videos. This method shows better performance on videos but fails on photo. Agarwal also suggests Haralick features [21] can be used in face anti-spoofing with very good results. But this approach requires more space to represent features and computation cost is also very high.

Recently combinations of different methods are used to differentiate spoof and real faces [22]. The combined features [23] of face and scene joined with features of image quality measures are used. An artificial neural network classifier is trained to differentiate real/spoof images. It shows very good results, but computational cost and memory usage are very high. Usage of Convolution Neural Network (CNN) [24] shows excellent results for face anti-spoofing. In spite of very good results, it consumes more memory and more computational overheads than other methods.

Face anti-spoofing approaches have improved, but still there is no robust solution for various environment changes, which occur consequently, such as change in resolution or lighting, camera without cost of substantial time and space overhead. Small attention is paid to methods in usage of resources, in real-time applications and how they perform under different conditions of varying environment. The method being discussed in the next coming sections tries to address suitably the above requirements.

3. Overview of the Face Anti-spoofing architecture

In this section, insight of the proposed method of face anti-spoofing system that uses various descriptors such as LTP, LBP, LGS and EDDTCP is presented. The system architecture, which identifies specific attributes of living trait is shown in Fig. 1.

In the beginning, input face images are loaded from the dataset. From the face image, texture features are extracted using LTP, LBP, LGS and EDDTCP descriptors. These descriptors represent spatial information of face image. These features are used to train classifiers. With the help of the pre-trained classifier the system verifies whether a given test face image is genuine or spoofed. In our proposed method we first test the system using the existing descriptors such as LTP, LBP and LGS. Later we introduced a novel descriptor called EDDTCP in which the average of cornered neighbours are calculated and stored. The performance of the new descriptor against SOTA approaches are compared. The details of the proposed method is given in Section 3.4.

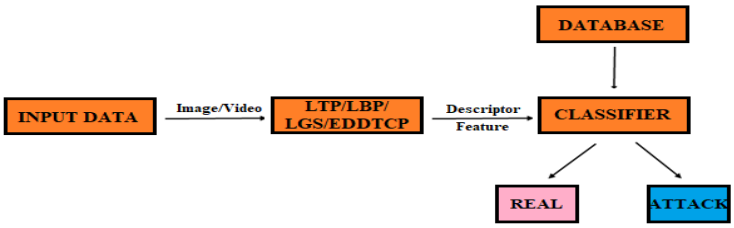

Fig. 1. Face Anti-spoofing architecture

3.1. Local Binary Pattern (LBP)

LBP is a descriptor used for analysis of texture. This descriptor uses the pixels of an image, denoted in terms of 0's and 1's using equations:

(1) $$\mathrm{LBP}_{P,R} = \sum_{m=0}^{m-1} d(B_i - B_c)2^m,$$

(2) $$d(X) = \begin{cases} 1 & \text{if } X \geq 0, \\ 0 & \text{otherwise.} \end{cases}$$

Details about LBP can be found in reference [25].

The disadvantages of LBP are that, variations of images due to the noises, illumination and partial occlusions are not handled.

3.2. Local Ternary Pattern (LTP)

LTP is a descriptor used for analysis of texture. This ternary pattern is introduced by Tan and Triggs [26]. This descriptor uses the pixels of an imagep denoted in terms of –1, 0 and 1's using equations:

(3) $$\mathrm{LTP}_{P,R} = \sum_{m=0}^{m-1} 2^m d'(B_i - B_c),$$

(4) $$(X) = \begin{cases} +1 & \text{if } X \geq t, \\ 0 & \text{if } -t < X < t, \\ -1 & \text{if } X < -t. \end{cases}$$

The disadvantage of LTP is difficulty to set the right threshold for a specific application. Also, when the threshold value is same as the difference of neighbours and center pixels, in such cases LTP generated code turns-out to zero.

3.3. Local Graph Structure (LGS)

Yet another texture descriptor is LGS presented by Eimad and Bashir [27]. This texture descriptor uses the concept of graph to represent pixels, denoted in terms of 0's and 1's using equations:

(5) $$\mathrm{LGS}_{P,R} = \sum_{k=0}^{7} d''(B_d - B_n)2^p, \; p = 7, 6, \ldots,$$

(6) $$d''(x) = \begin{cases} 1 & \text{if } x \geq 0, \\ 0 & \text{if } x < 0, \end{cases}$$

where, B_d and B_n represents the neighbours in traversal.

However, the LGS uses imbalanced graph structure and extracts uneven information compared to left than right side or vice versa.

3.4. Extended Divisional Directional Ternary Co-relation Pattern (EDDTCP)

The disadvantages of LBP, LTP and LGS have encouraged us to develop a novel texture descriptor EDDTCP for face anti-spoofing application. The EDDTCP is calculated based on averages of neighbour pixels of a given image (5×5 pixels) from

center pixel. The EDDTCP values are computed using center pixel's first order derivatives and co-relation values in all 8 directions.

In the EDDTCP, the first order derivatives (at R and R+1) for a given centre pixel (B_C) is calculated as follows:

In the beginning, the average of neighbour pixels are calculated using the equations:

$$C_{P,R}(\mathrm{Avg}_j) = \sum_{i=1}^{3} C_{P,R}(B_i),\ \ j = 1, 2, \ldots, 8, \tag{7}$$

$$C_{P,R}(B_i) \ = C_{P,R}(B_i) * \ C_{P,R}(B_c),\ \ i = 1, 2, \ldots, P, \tag{8}$$

$$C_{P,R+1}(B_{i+1}) = C_{P,R}(\mathrm{Avg}_j) * \ C_{P,R}(B_c),\qquad i = 1, 2, \ldots, P, \tag{9}$$

$$C'_{P,R}(B_i) = \ C_{P,R}(B_i) \ - \ C_{P,R+1}(B_{i+1}),\qquad i = 1, 2, \ldots, P. \tag{10}$$

Once we have calculated first order derivatives, now based on the sign of derivatives code them as follows:

$$C''_{P,R}(B_i) = \ g_1\left(C_{P,R}(B_i)\right), \tag{11}$$

$$C''_{P,R+1}(B_{i+1}) = \ g_1\left(C_{P,R+1}(B_{i+1})\right), \tag{12}$$

$C''_{P,R}(B_i)$ and $C''_{P,R+1}(B_{i+1})$ are the co-related ternary values from a centre pixel, denoted by naming function called g_1.

Further, above values are used for computation of EDDTCP as follows:

$$C'''_{P,R}(B_i) = \ g_2\left(\left(C'_{P,R}(B_i)\right)\right). \tag{13}$$

Equation (13) denotes the co-relation between immediate directional neighbour, its next right-angled neighbour and center pixel:

$$\mathrm{EDDTCP} = \begin{pmatrix} C'''_{P,R}(B_1), & C'''_{P,R}(B_2), \\ , & C'''_{P,R}(B_c), \\ , & C'''_{P,R}(B_P). \end{pmatrix}. \tag{14}$$

The EDDTCP comprises values of directional co-relation sign of derivative and center pixel in Equation (14). The EDDTCP is the 3-valued pattern denoted by –1, 0, 1, which is further transformed into 2-valued pattern by using the ELTP (extended local ternary pattern) [27] as follows:

$$g_3(X) = \begin{cases} 1 \text{ if } X > \ B_c + t, \\ 0 \text{ if } X \geq B_c - t \text{ and } X \leq B_C + t, \\ -1 \text{ if } X < \ B_c + t, \end{cases} \tag{15}$$

where, B_c is a centre pixel, t is a threshold.

The threshold is calculated using Median Absolute Deviation (MAD) of all pixels in G:

$$t = \mathrm{MAD}(G),\ G = \{g_i,\ i = 0, 1, \ldots, 8\}.$$

For simplicity, each ternary pattern of EDDTCP is divided into Upper half (EDDTCP_U) and Lower half (EDDTCP_L) as follows:

$$\mathrm{EDDTCP\_U}_{P,R}(i,j) = \sum_{m=0}^{m-1} 2^m \left(D_1(g_3(X), 1)\right), \tag{16}$$

$$\mathrm{EDDTCP\_L}_{P,R}(i,j) = \sum_{m=0}^{m-1} 2^m \left(D_2(g_3(X), -1)\right), \tag{17}$$

$$D_1(X,Y) = \begin{cases} 1 \text{ if } X = Y = 1, \\ 0 \quad \text{otherwise}, \end{cases} \tag{18}$$

$$D_2(X,Y) = \begin{cases} 1 \text{ if } X = Y = \ -1, \\ 0 \quad \text{otherwise}. \end{cases} \tag{19}$$

Equations (20) and (22) are used to build histogram of upper pattern EDDTCP_U and lower pattern EDDTCP_L, respectively. Later, it is used for EDDTCP pattern calculations of given image:

(20) $\mathrm{HG}_{\mathrm{EDDTCP_U}}[L] = \sum_{i=1}^{N1}\sum_{j=1}^{N2} g_4\left(\mathrm{EDDTCP_U}_{P,R}(i,j), S\right),\ S \in (0, 2^{p-1}-1),$

(21) $$g_4(X,Y) = \begin{cases} 1 & \text{if } X = Y, \\ 0 & \text{else,} \end{cases}$$

where, $N_1 \times N_2$ is the size of output of upper pattern image EDDTCP_U;

(22) $\mathrm{HG}_{\mathrm{EDDTCP\_U}}[K] = \sum_{i=1}^{N1}\sum_{j=1}^{N2} f_5\left(\mathrm{EDDTCP\_L}_{P,R}(i,j), T\right),\ T \in (0, 2^{p-1}-1),$

(23) $$g_5(X,Y) = \begin{cases} 1 & \text{if } X = Y, \\ 0 & \text{else,} \end{cases}$$

where, $N_1 \times N_2$ is the size of output of lower pattern image EDDTCP_L.

The final histogram for whole image is computed by combining upper and lower ternary pattern histograms by using the equation

(24) $$\mathrm{HG}_{\mathrm{EDDTCP}} = \mathrm{HG}_{\mathrm{EDDTCP\_U}}[L] + \mathrm{HG}_{\mathrm{EDDTCP\_L}}[K].$$

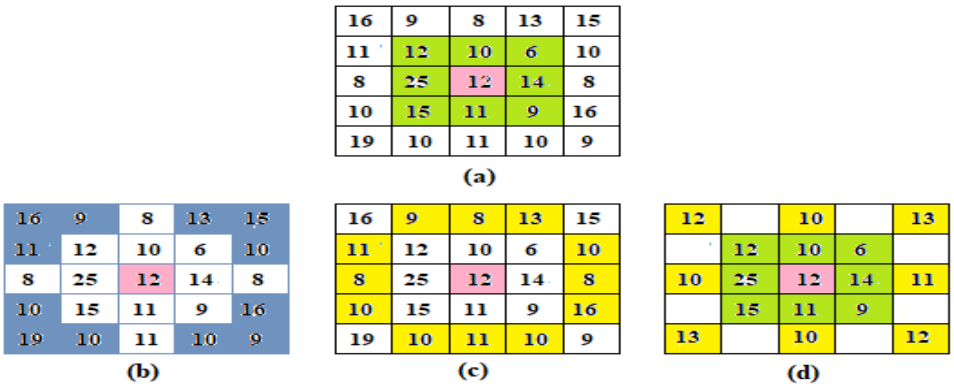

Fig. 2. Sample Image (a), Marked corner neighbours (b), Marked directional neighbours (c), Average of neighbours (d)

The EDDTCP computation is as follows: Consider 5×5 pixels of given sample image as shown in Fig. 2a and center pixel and neighbours are marked with pink and green colour respectively. The given image is divided into cornered neighbours and directional neighbours marked with blue and yellow colour respectively as shown in Figs 2b and 2c. The average of cornered neighbours and average of directional neighbours are calculated and stored as shown in Fig. 2d. The EDDTCP values are computed by using the co-relation difference between product of center pixel with its immediate directional neighbour and its directional neighbour as shown in Fig. 3.

The EDDTCP computation process is explained by an example as follows: Consider a sample image and its center pixel marked with pink color "12" and its immediate neighbour (at an angle of 135° to center pixel) marked with no color as shown in Fig. 2b. In order to calculate next immediate directional neighbour by using average of cornered neighbours they are marked with blue colour, "11", "16" and "9" as shown in Fig. 2b. Once the average of cornered neighbour is calculated and stored as next immediate directional neighbour (at an angle of 135° to center pixel) and is marked with yellow colour "12" as shown in the Fig. 2d.

Fig. 3 depicts the calculation of co-relation matrix in which immediate neighbour (in 135° angle to center pixel) marked with green colour "12" and center pixel marked with pink colour "12" and their product is named as product-1. The product of local co-relation between next immediate directional neighbour is marked with yellow colour "12" and center pixel which is named as product-2. Later, the co-relation difference between product-1 and product-2 is found that gives the first value for EDDTCP image pattern. Similarly, remaining EDDTCP values are computed from seven directions.

Fig. 3. Co-relation matrix calculation

Further, EDDTCP image patterns is computed using these EDDTCP values as shown in Fig. 4. The EDDTCP image pattern is converted into ternary pattern by calculating dynamic threshold (t) by using Median Absolute Deviation (MAD) [28, 37, 38] of neighbours (i.e., t = 42.37). The ternary value is denoted by –1, if neighbour pixel value is less than difference of center pixel and threshold. Ternary value is denoted by 1, if neighbour pixel value is greater than sum of center pixel and threshold. Ternary value is denoted by 0, if neighbour pixel value is within a range from difference of center pixel and threshold to sum of center pixel and threshold. Further, these values are transformed into two 2-valued pattern called Binary pattern-1 (all positive values are 1's and remaining are 0's) and Binary pattern-2 (all negative values are 1 and remaining are 0's). Next, applied binary weights on Binary pattern-1 and calculated EDDTCP High Value as "8" are used. Similarly, Binary pattern-2 is used for calculation of EDDTCP Low Value as "65".

The proposed method EDDTCP is quite dissimilar from the renowned LBP, LTP and LGS. The EDDTCP encodes the spatial co-relation between centre pixel, immediate neighbour and its next immediate directional neighbour in all directions. Whereas LBP, LTP and LGS descriptors encodes relation between the centre pixel and its neighbours only. Consequently, EDDTCP descriptor extracts more spatial information than SOTA approaches (LGS, LBP and LTP). It has been already proved that directional features are very valuable [29-31] in many applications of image processing.

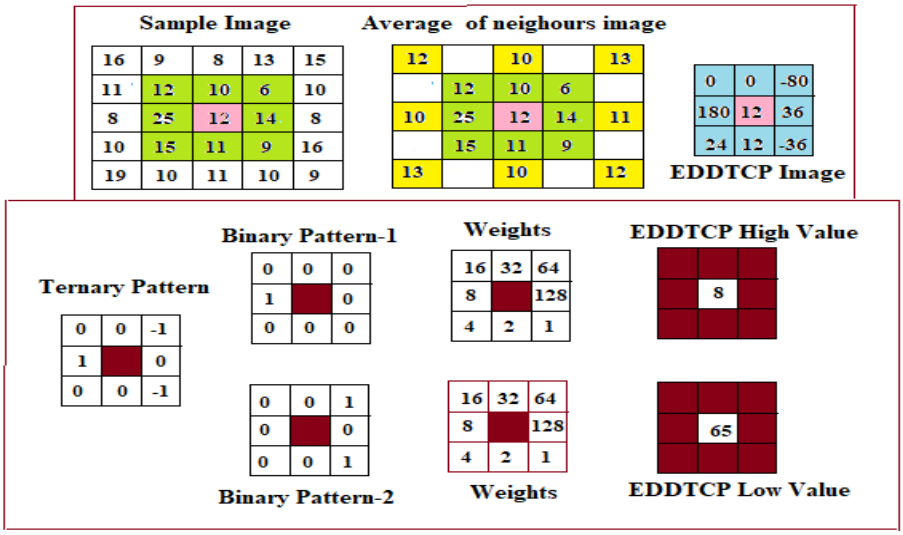

Fig. 4. Example for EDDTCP calculation

3.4.1. Proposed system framework

The system framework of proposed method as shown in the Fig. 5. In the beginning input is loaded with face images from the dataset. The average of cornered neighbours are calculated and stored. The first order derivatives are computed using co-relation difference. The EDDTCP comprises the 3-valued patterns, which are computed using ELTP. Transform the 3-valued pattern of the EDDTCP into 2-valued patterns and compute the histogram of it. The EDDTCP feature vector is calculated by combining the histogram of each. The training set of dataset is used to train SVM classifier. The classifier will categorize the given test image as genuine/spoof.

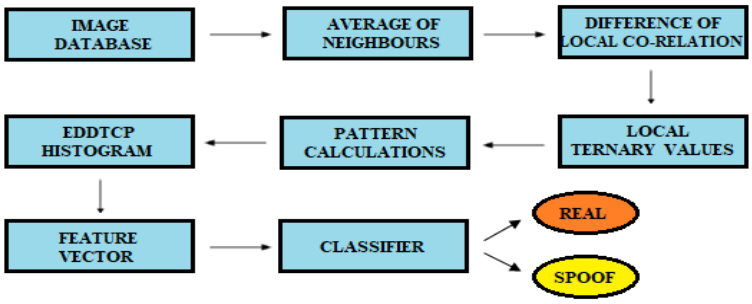

Fig. 5. System framework of the proposed method for face anti-spoofing

3.4.2. The proposed method algorithm

Algorithm

Input: Image; *Output:* Spoofing results.

Input: Face image; *Output:* Genuine/Spoof.

Step 1. Load input images from the dataset and convert it into grey-scale images.

Step 2. Consider the 5×5 matrix of a grey-scale image; identify the cornered neighbours and directional neighbours.

Step 3. Calculate the average of cornered neighbours with directional neighbours.

Step 4. Calculate the first-order derivatives (at R and R+1) with respect to the center pixel.

Step 5. Calculate the local difference between center pixel and its immediate neighbour and its average directional neighbour.

Step 6. Compute the 3-valued pattern using ELTP.

Step 7. Constitute the EDDTCP image ternary pattern.

Step 8. The EDDTCP image ternary pattern is transformed into 2-valued patterns.

Step 9. Calculate the histogram of the binary patterns separately and combine them.

Step 10. Compute the histograms of 2-valued patterns.

Step 11. Compute the EDDTCP feature vector by combining the histogram of each.

Step 12. Use the training set of dataset to train SVM classifier.

Step 13. Categorize the test image as genuine/spoof.

4. Experimental results and discussions

The performance of the developed method is evaluated by conducting different experiments over face anti-spoofing datasets such as Replay-Attack [34], NUAA [32], MSU-MFSD [33]. In following subsections, obtained results are discussed.

The SVM/KNN/LDA classifiers are used in all the experiments for training and testing of the images. During testing, the system extracts feature vector for each test image using given descriptor and the trained classifier categorizes the given test image as genuine/spoof.

Support Vector Machine (SVM). A supervised learning algorithm called Support Vector Machine (SVM) was used in all experiments for binary classification. A SVM creates an ideal hyper-plane as decision surface such that the boundary of separation between real and spoof data is maximized. As we know, any supervised learning model (SVM) needs to be trained then tested. The following parameters are used in training.

- Observed_matrix – A matrix of predictor data, where each row represents the feature vector of an image.
- Label – collection of class labels with each row represents to corresponding to the observed_matrix row. Label can be “1” for real and “0” for spoof data respectively.
- KernelFunction – The “linear” KernelFunction type was used for 2-class learning of SVM classifier.
- ClassNames – Discriminates between the genuine and spoof classes. The genuine class is the first element and the spoof class is the second element.

The tuning of SVM classifier is done by using the following parameters as follows:

- **Kernel:** This parameter is used to select the type of hyper-plane used to separate the data. "*linear*" type of hyper-plane was used to separate the data.
- ***C*:** This is the penalty parameter of the error and controls the balance between smooth decision boundary and differentiating the training points accurately. *C*=0.1 was used as error penalty parameter.
- **Degree:** It is a parameter used when set a kernel as polynomial. It represents basically the degree of the polynomial used to find the hyper-plane to split the data. Degree=1 was used as degree of polynomial.

K-Nearest Neighbours (KNN). KNN is simplest classifier, which uses Euclidean distance between its neighbours to decide the nearest neighbour. Each feature of given image is treated as equally important in Euclidean distance. Conversely, some features (genuine face image) are more discriminative than other features (spoof face image). In Euclidean distance, noise is dominated when the noisy features are more than useful features. The computational overhead is very high for a large number of samples.

Linear Discriminate Analysis (LDA). LDA is a classification method. It uses different Gaussian distributions on different classes. During training of LDA, the fitting function calculates the attributes of Gaussian distribution for each class. To classify, trained LDA finds the class with least misclassification cost.

The performance of the developed method is measured using some metrics as parameters: Average Recognition Rate (ARR), Precision (P), Recall (R), and Half Total Error Rate (HTER) which are given in Eqations (25)-(28), respectively:

(25) Average Recognition Rate: $\text{ARR} = \frac{1}{S}\sum_{i=1}^{s} \text{RR}\,(K_i),\ s = 1, \ldots, 3,$

(26) Precision: $P(T_q) = \frac{\text{Number of real images identified}}{\text{Total number of real images}},$

(27) Recall: $R(T_q) = \frac{\text{Number of real images recogized}}{\text{Number of real images recogized+Number of false negative attack images}},$

(28) $\text{HTER} = \frac{\text{FAR+FRR}}{2}.$

4.1. Experiment 1

In this experiment, three face anti-spoofing dataset such as Replay-Attack, NUAA and MSU-MFSD datasets were used. The three different sizes of real and spoof images were used for training. The original image of size 160×160 pixels, further segmented into 80×80 pixels of four non-overlapping sub-images and finally, segmented into 40×40 pixels of 16 non-overlapping sub-images. We have used three classifiers SVM, KNN and LDA in order to compare the performance of EDDTCP on all three datasets.

During training of different classifiers using NUAA dataset, it is totally divided into 10 categories. Each category comprises different number of images from each subject. In category-1, ten images were considered in each subject of real with spoof then tested. Next, category-2 to category-10, number of images were augmented from twenty to hundred in each subject of real with spoof respectively for training. For other datasets also same type of training was followed. The testing set contains the

combination of both genuine and attack images of total 3099 images (1150 real images and 1949 spoof images).

MSU-MFSD dataset comprises 15 subjects of real and spoof images. During training of different classifiers, three different sizes were used as discussed earlier. During testing, a set containing the combination of both genuine and attack images of total 1855 images of 20 different subjects (1000 real images and 855 spoof images) were used.

Replay-Attack dataset comprises 15 subjects of real and spoof images. During training of different classifiers, three different sizes were used as discussed earlier. During testing, a set containing the combination of both genuine and attack images of total 1600 images of 20 different subjects (800 real images and 800 spoof images) were used.

Table 1. ARR of SOTA approaches on different datasets using various classifiers

Descriptor	Category	SVM			KNN			LDA		
		NUAA (%)	MSU-MFSD (%)	Replay-Attack (%)	NUAA (%)	MSU-MFSD (%)	Replay-Attack (%)	NUAA (%)	MSU-MFSD (%)	Replay-Attack (%)
LBP	10	88.17	86.70	87.60	86.67	83.97	83.74	84.51	86.46	85.43
LTP	10	89.67	85.74	78.67	87.87	83.07	80.60	86.15	84.51	86.15
LGS	10	89.37	85.94	83.41	88.87	87.37	82.97	87.32	86.29	86.29
EDDTCP	**7**	**93.04**	**91.23**	**89.90**	**89.83**	**88.73**	**86.80**	**92.22**	**90.87**	**88.86**

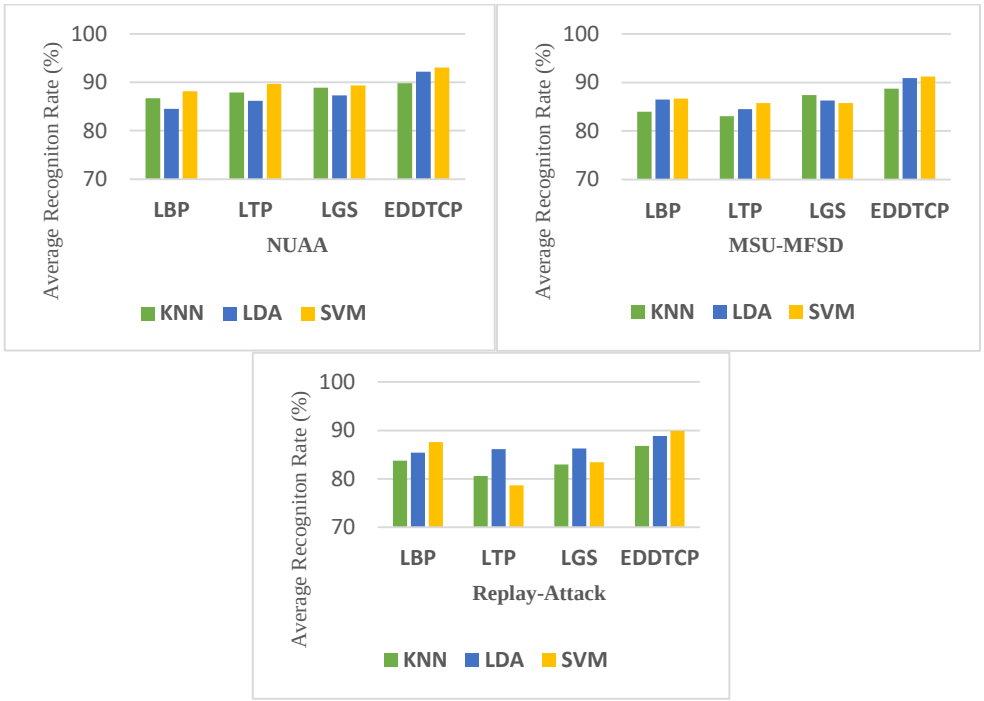

Fig. 6. Comparison of EDDTCP with SOTA approaches using different classifiers on various datasets

It was witnessed from the Fig. 6 at category-7, the EDDTCP shows best Average Recognition Rate (ARR) and further increase (of number of images) will not improve the recognition rate. This shows that EDDTCP outperforms compared to other

methods (LBP, LTP, LGS) which take more number of training images (category-10). Also it is observed from Fig. 6 that the recognition rate is at its peak for category-7 and further increase in training images will not improve the recognition rate.

From the Experiment 1, it has been observed that EDDTCP shows superior performance as compared to SOTA approaches.

Fig. 6 shows that the Average Recognition Rate (ARR) of EDDTCP compared with SOTA approaches is higher. It is evident from Fig. 6 and Table 1 that EDDTCP performs superior than other SOTA approaches on three different datasets using SVM, KNN and LDA classifiers.

The performance of EDDTCP with SVM classifier is superior compared to other classifiers such as KNN and LDA over all the three datasets. From Table 1 it is evident that SVM classifier is better than other two classifiers. So, in all further feature experiments we have used SVM classifier.

4.2. Experiment 2

In this experiment, three face anti-spoofing dataset such as Replay-Attack, NUAA and MSU-MFSD datasets were used. The original image is segmented into 40×40 pixels of 16 non-overlapping sub-images. During training of SVM classifier, 100 images in each subject were used and tested.

Table 2. EER and HTER computed for various protocols of the different databases.

Descriptors		LBP		LTP		LGS		EDDTCP	
Error (%)		ERR	HTER	EER	HTER	EER	HTER	EER	HTER
Data bases	NUAA	10.54	12.09	9.70	11.00	9.58	10.83	**5.30**	**5.74**
	MSU-MFSD	3.49	12.54	3.50	12.64	3.65	13.13	**2.37**	**6.56**
	Replay-Attack	1.96	10.72	0.75	19.99	0.35	14.99	**1.26**	**7.86**

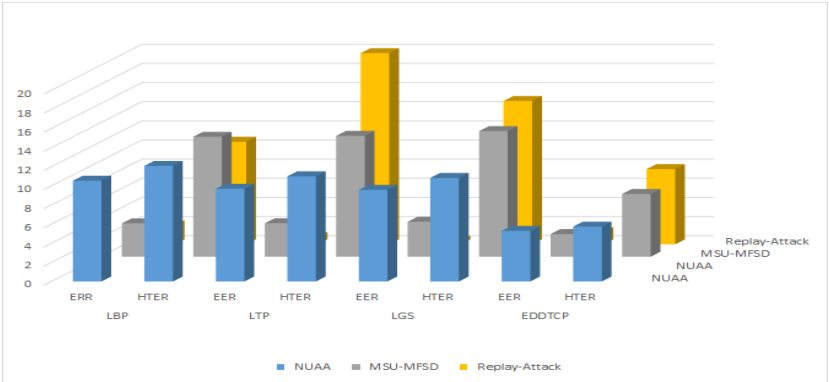

Fig. 7. Performance of EDDTCP with SOTA approaches in terms of EER and HTER on three datasets

The performance of EDDTCP with SOTA approaches on 3 different datasets in terms of metrics HTER and EER is as shown in Fig. 7. This experiment portrays that EDDTCP features have more proficiency to distinguish the genuine/spoof faces as compared to SOTA approaches. The outcome gained on three datasets shows that, EDDTCP performance on face liveness detection is increased over SOTA approaches by lowest 1.26 % EER and 7.86% HTER using SVM. The SOTA approaches

performance is degraded due to heavy illumination changes occurring in the face images of datasets. This issue was addressed by usage of EDDTCP. It is evident from Fig. 7 and Table 2 that EDDTCP performs superior than other SOTA approaches, more robust for discriminating genuine and spoof faces on three different datasets.

4.3. Experiment 3

In this experiment, three face anti-spoofing dataset such as Replay-Attack, NUAA and MSU-MFSD datasets were used. The original image of size 160×160 pixels is segmented into 40×40 pixels of 16 non-overlapping sub-images. During training of SVM classifier, dataset is divided into 10 categories. Each category comprises different number of images from each subject. In category-1, ten images were considered in each subject of real with spoof then tested. Next, category-2 to category-10, number of images were augmented from twenty to hundred in each subject of real with spoof respectively for training. For other datasets also same type of training was followed.

The performance of EDDTCP with SOTA approaches on 3 different datasets in terms of metrics average precision and average recall is as shown in Fig. 7. It is evident from Fig. 8 and Table 3 that EDDTCP performs superior than other SOTA approaches in terms of metrics average precision and average recall on 3 different datasets.

From the Table 3 and Fig. 8, it can be witnessed that EDDTCP outperforms:

1. The LBP by 7.26%, 24.98% and the LGS by 3.09%, 19.67% in terms of average precision and average recall respectively on NUAA database.
2. The LBP by 9.18%, 5.18%, the LTP by 5.41%, 1.51% and the LGS by 5.54%, 1.61% in terms of average precision and average recall respectively on MSU-MFSD database;
3. The LBP by 7.36%, 7.82%, the LTP by 14.13%, 13.81% and the LGS by 9.96%, 10.79% in terms of average precision and average recall respectively on Replay-Attack database.

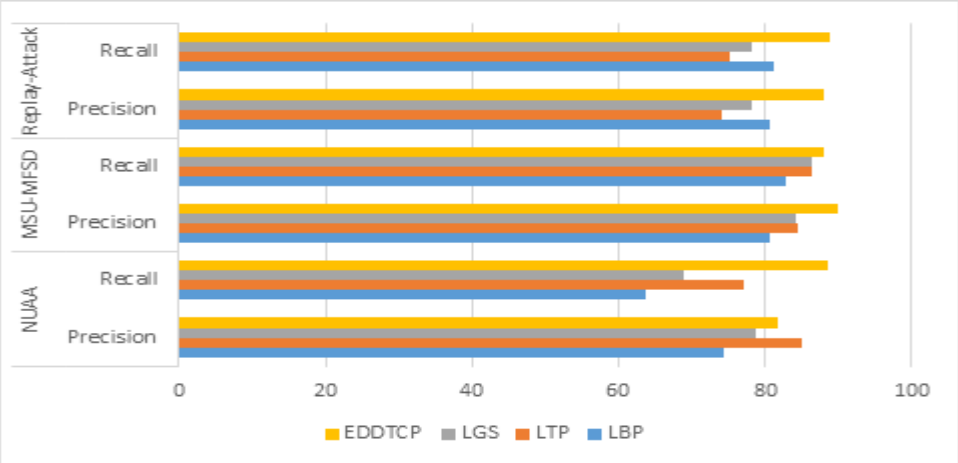

Fig. 8. Performance of EDDTCP with SOTA approaches in terms of Average Precision and Average Recall on different datasets

Table 3. Average Precision and Average Recall of SOTA approaches on different datasets

Descriptors	NUAA		MSU-MFSD		Replay-Attack	
	Precision (%)	Recall (%)	Precision (%)	Recall (%)	Precision (%)	Recall (%)
LBP	74.41	63.70	80.64	82.71	80.72	81.12
LTP	84.87	77.20	84.41	86.38	73.95	75.13
LGS	78.62	69.04	84.28	86.28	78.12	78.11
EDDTCP	**81.69**	**88.69**	**89.84**	**87.91**	**88.10**	**88.92**

4.4. Comparisons of the developed method on different datasets

Table 4 reviews the results of the other methods relating to the MSU-MFSD and Replay-Attack database. HTER was used as common metric. In both databases, SVM module is used as classifier. The MSU-MFSD database provides sufficient number of unbalanced real and spoof samples and provides best results using HTER metric. As it can be observed in Table 4, developed method EDDTCP outperforms when compared to [35] and [36]. The metric HTER clearly shows that EDDTCP attained the best performance for the MSU-MFSD database.

From Fig. 9 and Table 4, EDDTCP performs superior than other SOTA approaches on Replay-Attack dataset. This dataset provides an uneven genuine and spoof samples in a percentage of 20:100. The metric clearly shows that EDDTCP achieved the top performance for Replay-Attack dataset. It is evident from Table 4 that EDDTCP performs superior than [35, 36]. The developed method attained top performance on Replay-Attack dataset using HTER metric.

Table 4. Results over MSU-MFSD and Replay-Attack data set

HTER %	MSU-MFSD	Replay-Attack
LBP [35]	21.4	15.6
Motion [36]	17.9	13.2
EDDTCP	**6.56**	**7.86**

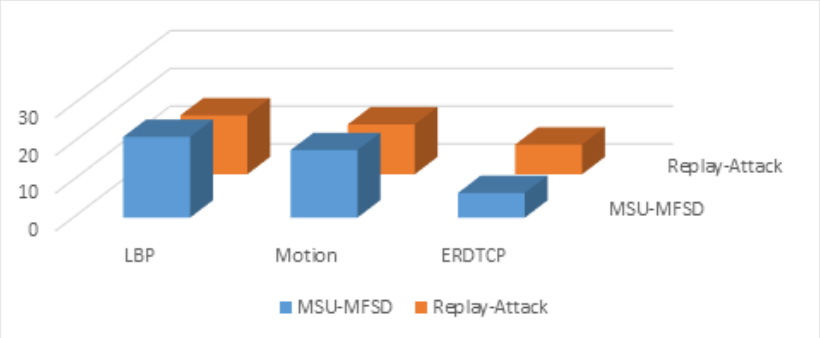

Fig. 9. Results over databases on metric used HTER

5. Conclusions

In this work, an innovative approach for face anti-spoofing is developed using EDDTCP (Extended Division Directional Co-relation Pattern). For a given image EDDTCP transforms the co-relation of 3-valued edges. EDDTCP performance has

been improved sufficiently as compared to State-Of-The-Art (SOTA) approaches. From the results obtained, it is evident that there is significant progress in terms of metrics used. Our proposed method can find real and spoof patterns accurately and efficiently under local co-relation pattern. Extensive experimental results demonstrate the supremacy of our method. Due to the robustness of the developed EDDTCP descriptor, it is not only useful in face biometric applications but it can be as well used in face recognition also.

In the present work, only average of cornered neighbours has been used for local co-relation calculation. This can be further enriched by considering obtuse or acute angle directional neighbours in future, which will enhance the recognition rate.

References

1. D u c, N., B. M i n h. Your Face is Not Your Password. – In: Proc. of Black Hat Conference, Vol. **1**, 2009.
2. A k h t a r, Z., C. M i c h e l o n i, G. L. F o r e s t i. Biometric Liveness Detection: Challenges and Research Opportunities. – Journal of Security & Privacy, IEEE, Vol. **13**, 2015, No 5, pp. 63-72.
3. Z h a n g, Z., J. Y a n, S. L i u, Z. L e i, D. Y i, S. Z. L i. A Face Anti-Spoofing Database with Diverse Attacks. – In: Proc. of International Conference on Biometrics (ICB), IEEE, 2012, pp. 26-31.
4. M a n j a n i, I., S. T a r i y a l, M. V a t s a, R. S i n g h, A. M a j u m d a r. Detecting Silicone Mask Based Presentation Attack via Deep Dictionary Learning. – IEEE Transactions on Information Forensics and Security, Vol. **12**, 2017, No 7, pp. 1713-1723.
5. C o r t e s, C., V. N. V a p n i k. Support-Vector Networks. – Journal of Machine Learning., Vol. **20**, 1995, No 3, pp. 273-297.
6. M a a t t a, J., A. H a d i d, M. P i e t i k a i n e n. Face Spoofing Detection from Single Images Using Micro-Texture Analysis. – In: Proc. of International Joint Conference on Biometrics, 2011, pp. 1-7.
7. P a r v e e n, S., S. M. S. A h m a d, N. H. A b b a s, W. A. W. A d n a n, M. F. H a n a f i, N. N a e e m. Face Liveness Detection Using Dynamic Local Ternary Pattern (DLTP). – Journal of Computers, Vol. **5**, 2016, No 2, p. 10.
8. K o s e, N., J. L. D u g e l a y. Reflectance Analysis Based Countermeasure Technique to Detect Face Mask Attacks. – In: Proc. of International Conference on Digital Signal Processing, IEEE, 2013, pp. 1-6.
9. Z h a n g, Z., D. Y i, Z. L e i, S. Z. L i. Face Liveness Detection by Learning Multispectral Reflectance Distributions. – In: Proc. of International Conference on Automatic Face & Gesture Recognition and Workshops, IEEE, 2011, pp. 436-441.
10. K i m, Y., J. N a, S. Y o o n, J. Y i. Masked Fake Face Detection Using Radiance Measurements. – Journal of Optical Society of America, Vol. **26**, 2009, No 4, pp. 760-766.
11. T a n, X., Y. L i, J. L i u, L. J i a n g. Face Liveness Detection from a Single Image with Sparse Low Rank Bilinear Discriminative Model. – Journal of Computer Vision, 2010, pp. 504-517.
12. P a n, G., L. S u n, Z. W u, S. L a o. Eyeblink-Based Anti-Spoofing in Face Recognition from a Generic Webcamera. – In: Proc. of International Conference on Computer Vision, IEEE, 2007, pp. 1-8.
13. P e r e i r a, T. de F., A. A n j o s, J. M. de M a r t i n o, S. M a r c e l. LBP-TOP Based Countermeasure against Face Spoofing Attacks. – In: Proc. of Asian Conference on Computer Vision, Springer, 2012, pp. 121-132.
14. P e r e i r a, T. de F., A. A n j o s, M. de M a r t i n o, S. M a r c e l. Can Face Anti-Spoofing Countermeasures Work in a Real World Scenario? – In: Proc. of International Conference on Biometrics IEEE, 2013, pp. 1-8.
15. K o m u l a i n e n, J., A. H a d i d, M. P i e t i k a i n e n. Context Based Face Antispoofing. – In: Proc. of International Conference on Biometrics: Theory, Applications and Systems, IEEE, 2013, pp. 1-8.

16. Y a n g, J., Z. L e i, S. L i a o, S. Z. L i. Face Liveness Detection with Component Dependent Descriptor. – In: Proc. of International Conference on Biometrics, 2013, pp. 1-6.
17. B h a r a d w a j, S., T. I. D h a m e c h a, M. V a t s a, R. S i n g h. Face Antispoofing via Motion Magnification and Multifeature Videolet Aggregation. – In: Proc. of International Conference on Pattern Recogiton, 2014.
18. G a l b a l l y, J., S. M a r c e l. Face Anti-Spoofing Based on General Image Quality Assessment. – In: Proc. of International Conference on Pattern Recognition, IEEE, 2014, pp. 1173-1178.
19. B o u l k e n a f e t, Z., J. K o m u l a i n e n, A. H a d i d. Face Anti-Spoofing Based on Color Texture Analysis. – In: Proc. of International Conference on Image Processing, IEEE, 2015, pp. 2636-2640.
20. P a t e l, K., H. H a n, A. K. J a i n, G. O t t. Live Face Video vs. Spoof Face Video: Use of Moire Patterns to Detect Replay Video Attacks. – In: Proc. of International Conference of Biometrics, IEEE, 2015, pp. 98-105.
21. A g a r w a l, A., R. S i n g h, M. V a t s a. Face Anti-Spoofing Using Haralick Features. – In: Proc. of International Conference on Biometrics Theory, Applications and Systems, IEEE, 2016, pp. 1-6.
22. F e n g, L., L.-M. P o, Y. L i, X. X u, F. Y u a n, T. C.-H. C h e u n g, K.-W. C h e u n g. Integration of Image Quality and Motion Cues for Face Antispoofing: A Neural Network Approach. – Journal of Visual Communication and Image Representation, Vol. **38**, 2016, pp. 451-460.
23. V e n k a t e s h, B., J. A n u r a d h a. A Review of Feature Selection and Its Methods. – Cybernetics and Information Technologies, Vol. **19**, 2019, No 1, pp. 3-26.
24. L u c e n a, O., A. J u n i o r, V. M o i a, R. S o u z a, E. V a l l e, R. L o t u f o. Transfer Learning Using Convolutional Neural Networks for Face Antispoofing. – In: Book of Image Analysis and Recognition. Springer, 2017, pp. 27-34.
25. O j a l a, T., M. P i e t i k a i n e n, D. H a r w o o d. A Comparative Study of Texture Measures with Classification Based on Feature Distributions. – Journal of Pattern Recognition, Vol. **29**, 1996, No 1, pp. 51-59.
26. T a n, X., B. T r i g g s. Enhanced Local Texture Feature Sets for Face Recognition under Difficult Lighting Conditions. – IEEE Transactions on Image Processing, Vol. **19**, 2010, No 6, pp. 1635-1650.
27. E i m a d, E. A. A., H. K. B a s h i r. Face Recognition Using Local Graph Structures. – In: Proc. of International Conference on Human Computer Interaction, 2011, pp. 169-175.
28. Y u a n, J.-H., H.-D. Z h u, Y. G a n, L. S h a n g. Enhanced Local Ternary Pattern for Texture Classification. – In: Proc. of Springer International Publishing Switzerland, 2014, pp. 443-448.
29. K o k a r e, M., P. K. B i s w a s, B. N. C h a t t e r j i. Texture Image Retrieval Using Rotated Wavelet Filters. – Journal of Pattern Recognition Letters, Vol. **28**, 2007, pp. 1240-1249.
30. K o k a r e, M., P. K. B i s w a s, B. N. C h a t t e r j i. Texture Image Retrieval Using New Rotated Complex Wavelet Filters. – IEEE Transactions on System, Man and Cybernetics, Vol. **33**, 2005, No 6, pp. 1168-1178.
31. Md R e z w a n, H., S. M. H. M a h m u d, X. Y. L i. Face Anti-Spoofing Using Texture-Based Techniques and Filtering Methods. – Journal of Physics, Vol. **1229**, 2019, pp. 1-9.
32. K o k a r e, M., P. K. B i s w a s, B. N. C h a t t e r j i. Rotation-Invariant Texture Image Retrieval Using Rotated Complex Wavelet Filters. – IEEE Transactions on System, Man and Cybernetics, Vol. **36**, 2006, No 6, pp. 1273-1282.
33. P a t e l, K., H. H a n, A. K. J a i n. Secure Face Unlock: Spoof Detection on Smartphones. – In: Proc. of IEEE Transactions on Information Forensic and Security, 2016.
34. L i, J., Y. W a n g, T. T a n, A. K. J a i n. Live Face Detection Based on the Analysis of Fourier Spectra. – In: Proc. of the International Society for Optical Engineering, 2004, pp. 296-303.
35. C h i n g o v s k a, A. A., S. M a r c e l. On the Effectiveness of Local Binary Patterns in Face Anti-Spoofing. – In: Proc. of International Conference of the Biometrics Special Interest Group, 2012, pp. 1-7.
36. A n j o s, A., S. M a r c e l. Counter-Measures to Photo Attacks in Face Recognition: A Public Database and a Baseline. – In: Proc. of International Joint Conference on Biometrics, 2011, pp. 1-7.

37. R a g h a v e n d r a, R. J., R. S. K u n t e. Extended Local Ternary Co-Relation Pattern: A Novel Feature Descriptor for Face Anti-Spoofing. – Journal of Information Security and Applications, Elsevier, Vol. **52**, 2020, pp. 1-10.
38. R a g h a v e n d r a, R. J., R. S. K u n t e. Extended Local Ternary Pattern for Face Anti-Spoofing. – In: Proc. of Lecture Notes on Electrical Engineering. Springer, 2020, pp. 221-229.
39. B o u l k e n a f e t, Z., J. K o m u l a i n e n, X. F e n g. Scale-Space Texture Analysis for Face Anti-Spoofing. – In: Proc. of IEEE International Conference on Biometrics, 2016, pp. 1-6.

Received: 05.01.2020; Second Version: 13.07.2020; Accepted: 07.08.2020