ISSN: 0976-9102 (ONLINE)
DOI: 10.21917/ijivp.2020.0311

FACE-SPOOF DETECTION USING RADON TRANSFORM BASED STATISTICAL MEASURES

Akhilesh Kumar Pandey and Rajoo Pandey
Department of Electronics and Communication, National Institute of Technology, Kurukshetra, India

Abstract

With the rising popularity of biometric traits-based authentication systems, their weaknesses are also grabbing attention of the research communities. This paper introduces a new anti-spoofing scheme for face recognition systems which exploits different measures based on the radon transform. The feature set used in the proposed method consists of five popularly known statistical moments, and uses support vector machine for classification. Extensive simulations are carried out using two different databases to assess the performance of the proposed method. It is found that the proposed method achieves a true recognition rate (TRR) of around 97%, yet maintaining the false acceptance rate (FAR) at around 1%.

Keywords:

Image Quality Measures, Radon Transform, Face-Antispoofing

1. INTRODUCTION

The tremendous growth of consumer devices and high speed communication systems witnessed in recent time has led the society to usher into a new electronic era where the identity and personal data of the individuals are often required to be stored in their personal devices, which need to be updated and upgraded from time to time [1]. Therefore, the security of such device is of utmost importance to protect them from possible attacks [2].

It is found through several studies that the biometric traits-based authentication systems are highly reliable in any scenario [1]-[3]. The iris and fingerprint-based recognition systems are widely used but require an intensive care for their satisfactory operation [4]. On the other hand, face recognition-based systems are non-intrusive in nature and require less care and installation cost [5]. Many personal devices have an inbuilt camera these days, therefore, it is easier to implement face recognition systems in them without increasing the device cost significantly. With the availability of enormous computational power, new methods of hacking are being invented by the attackers. Face spoofing is an example of such attacks, where a replica of the biometric trait is presented before the sensor. To overcome this challenge, therefore, it is mandatory to detect the life sign in the captured information, which is accomplished by different levels of the authentication procedure [7]. There are several methods available in the literature to detect face spoofing using different approaches. The techniques used for prevention of spoofing attack can be broadly classified as:

- *Hardware-Based Techniques*: Under this category, some specific device is incorporated in the system to detect the living characteristic e.g., facial thermogram, reflection from the eye. Many-a-time challenge response methods are added, which require the cooperation from the user. Fingerprint and iris recognition-based methods inherently detect the life sign by employing additional sensors, whereas the face recognition-based systems usually rely on challenge-response technique [8]-[12].
- *Software-Based Techniques*: Recently the focus has shifted to software-based techniques as they do not require additional sensors to detect spoofing. In this class, a qualitative evaluation of the captured image is done to classify the input. The technique is referred to as either static or dynamic depending upon whether single instance of the input or a sequence is used for evaluation. The dynamic techniques have been conventionally used for anti-spoofing but require user cooperation and are complex and expensive. This has led the research community to focus on static techniques, which have the advantage of being relatively user friendly, less costly and less complex [13]-[17].

The detection of motion is one of the most commonly employed approach for anti-spoofing. In this approach, eye blinking, mouth movement, and head rotations are detected to differentiate real and fake faces. In [18], eye blinking is detected by using graphical similarities, whereas in [19], authors use optical flow line to detect the motion in the mouth region. Strategy of Anjos et al. [20] for anti-spoofing is about finding the correlation between foreground and background regions of the captured images and hence noticing the head rotations for the classification [20]. Despite the success rate of such techniques, these are not generally employed in face recognition (FR) systems as they need to process a video, which makes them time consuming and computationally expensive.

Kim et al. [21] detected the reflectance dissimilarity by observing the spectrum and noticed the difference between low and high frequency components of the real and fake faces. Zhang et al. [22] proposed to use the difference between the reflectance of skin and non-skin material by employing an additional sensor. Marcel et al. [23] introduced another approach and established that image-quality plays an important role in this scenario. The basic idea behind this approach is the fact that real and fake face always have different qualities. Due to its computational efficiency, it is an attractive option but the error rate needs to be reduced.

This paper attempts to improve the performance of the IQM-based approach of [24] for spoof detection by using the radon transform of the captured image. The feature set in the proposed method uses various statistical moments instead of just a single feature based on maxima in [24]. These features are further used for classification of the image under consideration as real or fake by using SVM. The overall study presented in this paper can be summarized as:

- Feature extraction by using the Radon transform of the image to make the decision about the liveness of the face image captured from the camera.

- Analysis of different statistical measures in the radon transform domain to distinguish the real faces from the recaptured ones.
- Discussion on the necessary length of the feature vector created by statistical measures of the radon transform.

The organization of the paper is as follows. In section 2, preliminaries of radon transform are discussed, and different statistical moments are stated. In section 3, proposed methodology is described. Section 4 provides the results obtained by extensive experimentation. Conclusion and future directions are provided in section 5.

2. BACKGROUND

As the proposed work involves different statistical moments along with the radon transform, in this section, their basics are briefly explained.

2.1 THE RADON TRANSFORM

The Radon transform of an image *f*(*x*,*y*), for a certain set of angles, can be interpreted as the projection of the image along the given angles. The resulting projection is the sum of the pixel intensities in a certain direction as illustrated in Fig.1.

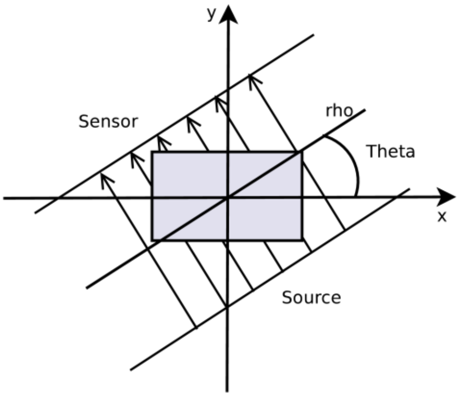

Fig.1. The sensor and source arrangement are rotated around the center of the image. For every given angle 'Theta', the sum of the pixel intensities is computed which falls in a ray perpendicular to the line ρ. The process is repeated for all the angles that are given

The radon transform is widely used in tomography, where an image is created from the projection data associated with cross-sectional scans of an object. The radon transform of *f*(*x*,*y*) is denoted by *RT*(*ρ*,*θ*) and can be expressed as:

$$RT(\rho,\theta)=\int_{-\infty}^{\infty}\int_{-\infty}^{\infty}\left(f(x,y)\delta(\rho-x\cos\theta-y\sin\theta)\right)dxdy \quad (1)$$

2.2 FIRST ORDER MOMENTS

There are several types of moments that exist in the literature of statistics to describe any distribution. The most commonly used first order moments are mean, median and mode. In the present study moments of vectors obtained from the radon transformed image are used to form the feature vectors which are then applied to SVM classifier to identify face spoofing. Moments up to third order are considered here. For a vector $\vec{x}$ having *N* elements, the mean, median and mode are denoted as $\bar{x}$, $\hat{x}$, and $\breve{x}$ are defined respectively by:

$$\bar{x}=E[\vec{x}]=\frac{1}{N}\sum_{i=1}^{N}x_i \quad (2)$$

$$\hat{x}=\begin{cases} sort(\vec{x})|_{(N+1)/2} & N\in odd(I) \\ \dfrac{sort(\vec{x})|_{(N)/2}+sort(\vec{x})|_{(N+2)/2}}{2} & N\in even(I)\end{cases} \quad (3)$$

$$\breve{x}=\arg\max\left(freq(\vec{x})\right) \quad (4)$$

where,

$sort(\vec{x})|_k$ is the *k*th element of the vector $\vec{x}$ after sorting it in any ascending or descending order.

$freq(\vec{x})$ is a function which returns the frequency of the elements in the vector.

2.3 HIGHER ORDER MOMENTS

In the present study, three popular higher order moments are considered namely variance, skewness and kurtosis. The second order moment is referred to as variance of any distribution, whose higher value can be perceived as greater spread in the distribution. The skewness or third order moment of a random variate can be interpreted as the inclination of the probability distribution. Therefore, a symmetric distribution will always have zero skewness. The fourth order moment of a data set is called kurtosis and can be interpreted as parameter describing the shape of the distribution. The kurtosis of a normal distributed random variate is 3. It is to be compared with the kurtosis of any distribution, e.g., if kurtosis is less than 3, the distribution will produce fewer and lesser extreme outliers than a normal distribution does. These moments are defined by the following equations.

$$Variance=\sigma^2=\frac{1}{N}\sum_{i=1}^{N}(\bar{x}-x_i)^2 \quad (5)$$

$$Skewness=\gamma=E\left[\left(\frac{\bar{x}-\vec{x}}{\sigma}\right)^3\right] \quad (6)$$

$$Kurtosis=\kappa=\frac{E\left[(\bar{x}-\vec{x})^4\right]}{\left(E\left[(\bar{x}-\vec{x})^2\right]\right)^2} \quad (7)$$

3. METHODOLOGY

In this paper, radon transform is used in three different ways, and for every vector that corresponds to an angle, feature(s) are obtained, which are used to enhance the accuracy of the system. Here, the commonly used terminology is first discussed which is further followed by the discussion about formation of the features sets. Let *I* be an 8-bit gray level image of the size $M\times N$, which is first normalized by the highest value (i.e., 255), to produce the image in the range [0,1]. Thereafter, the radon transform is applied for the predefined set of angles in the interval [0, 179]. The transform is denoted by *RT* with the size of $P\times Q$, which indicates that *RT* has *Q* vectors with the length *P* for each vector.

It can be interpreted also as $RT_q = R(I,q)$, where $R(I,q)$ is the radon transform of two-dimensional data *I* computed at an angle of *q* from the positive direction of the X-axis. Using the radon transform matrix *RT*, three feature sets A, B, and C are formed with different strategy to exploit every corner of this transform.

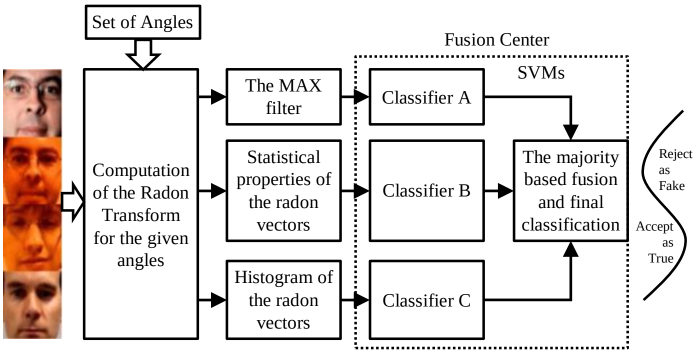
Set of Angles
Fusion Center
SVMs
Computation of the Radon Transform for the given angles
The MAX filter
Statistical properties of the radon vectors
Histogram of the radon vectors
Classifier A
Classifier B
Classifier C
The majority based fusion and final classification
Reject as Fake
Accept as True

Fig.2. Model of the proposed work that uses three classifiers

The Fig.2 shows the model of the proposed work. Here, three different feature sets are formed, which are applied to separate SVM classifiers, namely, classifier A, classifier B, and classifier C, whose outputs are fused to make the final decision about the liveness of the acquired face image. The fusion is based on the majority of the outputs obtained from different classifiers. It can also be noted that the majority-based decision has been widely used in the literature for its simplicity.

3.1 MAXIMUM DETECTOR

In the present work to form the first feature set, the maximum of every vector of the *RT*, as discussed in [24], is considered. Thus, different vectors are applied to the maximum detector and their maxima are recorded for the training and testing of the classifier A. The maximum of the vector is described by Eq. (8), and used to form a feature set of dimensions 180 for the angles from 0° to 179° with separation of 1°. It is also seen empirically that as the separation between two angles decreases, the recognition accuracy increases.

$$F_i = \max\left(RT_i\right) \forall i \in 1,...,180 \tag{8}$$

3.2 STATISTICAL PARAMETERS

As studied earlier in [24], the maximum of the vector obtained by radon transform yields a reasonably good fake identification rate, but when it is applied with other statistical properties of the same vector, it enhances the performance significantly. The objective of this section is to exploit the statistical properties of the vectors obtained through radon transform. In this scheme, for every vector, five measures are used to describe the feature set. In order to keep the feature vector length same as that for classifier A, the length of the angle vector is reduced to one fifth i.e., the angles are taken with the separation of 5° instead of 1°. The five features, maximum, mean, median, variance and, skewness, are selected on the basis of their performance separately. The selection of the parameters and their overall effect on the system performance is further discussed in section 4. The statistical properties-based feature vector is applied to classifier B and its decision about the liveness is combined with the decisions of other classifiers to take the final decision.

3.3 HISTOGRAM OF RADON TRANSFORM

The important statistics of an image can also be captured through the histogram. Therefore, in the present work the Histogram of Radon Transform (HRT) is also employed to form the feature vector. To keep the length of this feature vector same as other two feature vectors, 180 bins are considered. For each bin the frequency is computed, and the vector is normalized by the maximum value present in the vector. The normalized vector is considered as the feature set which is applied to classifier C for training and testing.

4. EXPERIMENTAL RESULTS AND DISCUSSIONS

4.1 SIMULATION PREREQUISITES

For the simulation of the present scheme and other existing techniques in Matlab, Ubuntu based core i5 system, with 8GB RAM, is used. The results of the proposed methodology are verified with the help of well-known face anti-spoofing databases, REPLAY-ATTACK [25], and SMU-MFSD [6]. With the face locations given along with the databases, the face from every frame is cropped and resized for further processing. The range of the histogram is predefined with min = 0 and max = 1.5×10^3, with equally spaced bins in the histogram for both real and fake face images. The value of RT falling outside this interval is discarded. A minimum of 500 random samples are taken for the training, and for the testing purpose 20,000 random samples are considered. All the results are computed by averaging 10 different runs in which the SVM is trained. The results are reported in terms of True Recognition Rate (TRR) and False Acceptance Rate (FAR). The TRR is the measure that shows the accuracy of the system to accept the real samples as real ones, while FAR is the acceptance rate of the fake samples as true ones by the same system.

4.2 CLASSIFIER A

As mentioned in section 3.1, this classifier A is employed to detect the real/fake by using the maxima of the radon vectors. From Fig.3, it is clearly observed that as the length of the feature vector increases, the recognition becomes more reliable irrespective of the inherent characteristics of the database.

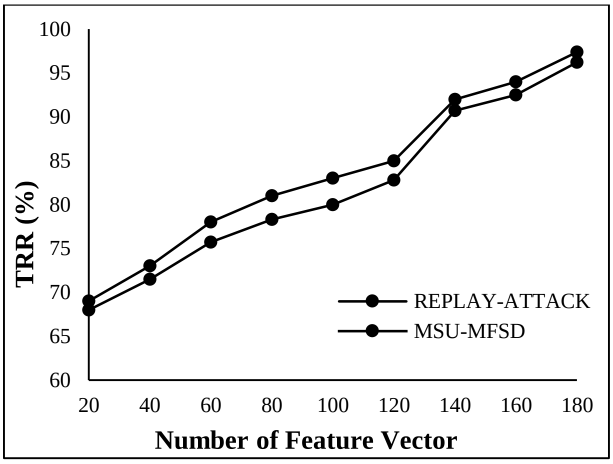

Fig.3. Effect of length of the feature vector on TRR for both databases

The Fig.3 is plotted for the test sets of both databases. As the number of the vectors present in the RT equals the number of angles for which RT is computed, the length of the feature vector directly depends on the separation between two adjacent angles. Therefore, for the length of 20 features, the separation should be 180°/9 = 20°. The other two feature sets used in the study also have dimension of 180.

4.3 CLASSIFIER B

As mentioned previously, in this classifier, different statistical moments are used as features to distinguish the real and fake face images. To judge the suitability of various moments, a study is presented in Fig.4. This Fig.4 shows the plot of the test results obtained by employing an SVM based classifier, separately for each statistical moment that forms the input length of 180. It can be noticed from this figure, that increasing the order of the moment does not necessarily improve the performance. When the order of statistical moments is increased up to 4, it is observed that in the set of six moments, the mode and kurtosis is not very effective as the resulting recognition rate is small for those two moments in comparison with other four moments. Therefore, in the present work the remaining four moments are considered along with the maximum as the fifth feature. These five features are computed for different angles by maintaining a separation of 5o between two adjacent angles to form the feature vector of length 180. The feature vector formed in this manner is used to train classifier B. During the experiment, it is noticed that the classifier B outperforms the classifier A by more than 5% in terms of TRR, with lower FAR. The Table.1 shows the TRR and FAR for different classifiers.

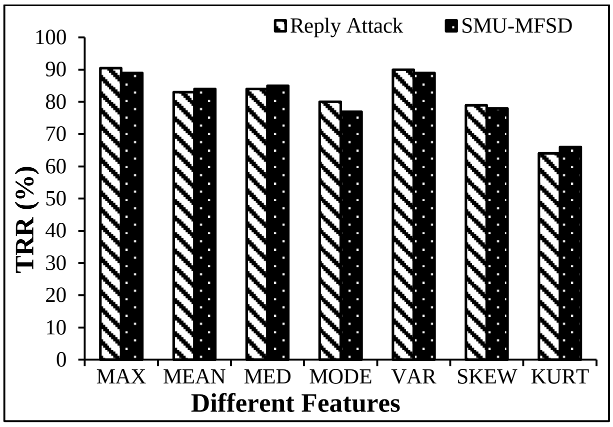

Fig.4. Individual feature analysis taken as all the 180 values of the same feature

Table.1. TRR and FAR for different Classifiers on different sets of the two databases

Attacks	Validation	Classifier A		Classifier B		Classifier C		Final Classification	
		FAR	TRR	FAR	TRR	FAR	TRR	FAR	TRR
Replay-Attack	Train	2.0	96.4	1.7	96.9	1.8	95.8	1.1	97.2
	Enroll	3.1	92.9	1.8	93.5	1.5	93.5	1.0	95.1
	Devel	4.1	90.5	2.1	94.4	3.8	92.1	1.2	95.5
	Test	3.9	91.4	2.4	93.4	3.5	93.8	1.1	95.0
MSU-MFSD	Train	2.2	93.3	3.7	92.7	1.8	96.1	1.0	97.7
	Enroll	2.9	91.4	3.8	90.5	2.7	94.5	1.0	95.5
	Devel	4.8	90.5	3.7	90.1	1.8	95.2	1.2	95.7
	Test	4.8	89.7	4.1	90.5	2.0	95.1	1.2	95.5

4.4 CLASSIFIER C

In the present study, experiments are performed to investigate the usefulness of frequency of the values of the radon transform. For this purpose, the HRT is obtained for predefined, equally spaced bins, which is normalized by maximum value for further processing. It is shown in Fig.5 that as the number of bins increases, the performance also improves. In contrast with classifier A and B, the performance of this classifier is better in MFSD than in replay-attack database. With the help of Table.1, the performance of the individual classifier can be analyzed.

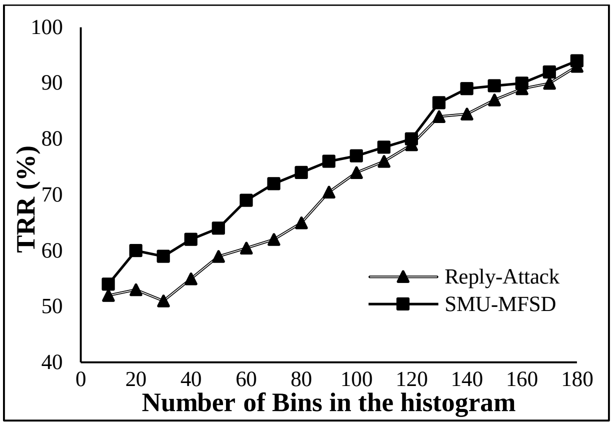

Fig.5. TRR vs. number of bins in the histogram

4.5 COMPARISON WITH EXISTING TECHNIQUES

The proposed work employs different classifiers and their results are combined to obtain the final decision. The Table.1 shows that after fusion the FAR is improved significantly yet maintaining the TRR. In Table.2, it is clearly shown that it outperforms the two popular anti-spoofing techniques, namely, correlation, and $LBP^{u,2}_{8,1}$, described in [20], and [25], respectively.

Table.2. Comparison of different anti-spoofing methods

Attacks	Validation	$LBP^{u,2}_{8,1}$		Correlation		Proposed Work	
		FAR	TRR	FAR	TRR	FAR	TRR
Replay-Attack	Train	1.1	89.4	1.0	91.1	1.1	97.2
	Test	1.0	87.4	1.0	90.2	1.1	95.0
MSU-MFSD	Train	1.0	90.4	1.1	92.3	1.0	97.7
	Test	1.0	89.2	1.0	89.8	1.2	96.0

5. CONCLUSIONS AND FUTURE DIRECTIONS

In this paper, radon transform is used to detect face-spoofing. The coefficients of radon transformed image are used to form different feature sets. For this purpose, various statistical properties are explored and it is found that maximum, mean, median, variance, and skewness of a vector are potentially effective for detection of face-spoofing. Based on the observations made during experimentation, three different types of feature sets for three separate classifiers are formed and their results are fused to make the final decision on liveness. Among these classifiers, classifier C manifested itself as the best with the highest recognition accuracy on MSU-MFSD database, whereas Classifier B produced better results on Replay-Attack database. It is also found that histogram of radon transformed image is also an attractive option to further increase recognition accuracy.

Other statistical measures of the radon transformed image, such as the ones based on analysis of the cumulative frequency of HRT, can also be explored in future. Also, some other transforms can be utilized in different ways for this purpose and the results may be studied.

REFERENCES

[1] A.K. Jain, A. Ross and S. Pankanti, "Biometrics: A Tool for Information Security", *IEEE Transactions on Information Forensics and Security*, Vol. 1, No. 2, pp. 125-143, 2006.

[2] A.K. Jain, K. Nandakumar and A. Nagar, "Biometric Template Security", *Eurasip Journal on Advances in Signal Processing*, Vol. 2008, pp. 113-121, 2008.

[3] J. Galbally, R. Cappelli, A. Lumini, G. Gonzalez-De Rivera, D. Maltoni, J. Fierrez, J. Ortega-Garcia and D. Maio, "An Evaluation of Direct Attacks using Fake Fingers Generated from Iso Templates", *Pattern Recognition Letters*, Vol. 31, No. 8, pp. 725-732, 2010.

[4] S. Bharadwaj, T. Dhamecha, M. Vatsa and R. Singh, "Computationally Efficient Face Spoofing Detection with Motion Magnification", *Proceedings of IEEE Workshop on Computer Vision and Pattern Recognition*, pp. 105-110, 2013.

[5] J. Galbally, C. McCool, J. Fierrez, S. Marcel and J. Ortega-Garcia, "On the Vulnerability of Face Verification Systems to Hill-Climbing Attacks", *Pattern Recognition*, Vol. 43, No. 3, pp. 1027-1038, 2010.

[6] D. Wen, H. Han and A.K. Jain, "Face Spoof Detection with Image Distortion Analysis", *IEEE Transactions on Information Forensics and Security*, Vol. 10, No. 4, pp. 746-761, 2015.

[7] J. Galbally, J. Fierrez, F. Alonso-Fernandez and M. Martinez Diaz, "Evaluation of Direct Attacks to Fingerprint Verification Systems", *Telecommunication Systems*, Vol. 47, No. 3-4, pp. 243-254, 2011.

[8] S. Memon, N. Manivannan, A. Noor, W. Balachadran and N.V. Boulgouris, "Fingerprint Sensors: Liveness Detection Issue and Hardware Based Solutions", *Sensors and Transducers*, Vol. 136, No. 1, pp. 1-35, 2012.

[9] C. Yuan, X. Sun, and R. Lv, "Fingerprint Liveness Detection based on Multi-Scale LPQ and PCA", *China Communications*, Vol. 13, No. 7, pp. 60-65, 2016.

[10] E.C. Lee, K.R. Park and J. Kim, "Fake Iris Detection by using Purkinje Image", *Proceedings of International Conference on Biometrics*, pp. 397-403, 2006.

[11] A. Pacut and A. Czajka, "Aliveness Detection for Iris Biometrics", *Proceedings of 4th IEEE International Conferences on Security Technology*, pp. 122-129, 2006.

[12] M. Kanematsu, H. Takano and K. Nakamura, "Highly Reliable Liveness Detection Method for Iris Recognition", *Proceedings of International Annual Conferences on Society of Instrument and Control Engineers*, pp. 361-364, 2007.

[13] L. Ghiani, G.L. Marcialis and F. Roli, "Fingerprint Liveness Detection by Local Phase Quantization", *Proceedings of 21st IEEE International Conference on Pattern Recognition*, pp. 537-540, 2012.

[14] C. Gottschlich, E. Marasco, A.Y. Yang and B. Cukic, "Fingerprint Liveness Detection based on Histograms of Invariant Gradients", *Proceedings of International Joint Conference on Biometrics*, pp. 1-7, 2014.

[15] Z. Wei, X. Qiu, Z. Sun and T. Tan, "Counterfeit Iris Detection Based on Texture Analysis", *Proceedings of 19th IEEE International Conference on Pattern Recognition*, pp. 1-4, 2008.

[16] N. Kohli, D. Yadav, M. Vatsa and R. Singh, "Revisiting Iris Recognition with Color Cosmetic Contact Lenses", *Proceedings of IEEE International Conference on Biometrics*, pp. 1-7, 2013.

[17] J.S. Doyle, K.W. Bowyer and P.J. Flynn, "Variation in Accuracy of Textured Contact Lens Detection based on Sensor and Lens Pattern", *Proceedings of 6th IEEE International Conference on Biometrics: Theory, Applications and Systems*, pp. 1-7, 2013.

[18] G. Pan, L. Sun, Z. Wu and S. Lao, "Eyeblink-based Anti-Spoofing in Face Recognition from a Generic Webcamera", *Proceedings of 11th IEEE International Conference on Computer Vision*, pp. 1-8, 2007.

[19] K. Kollreider, H. Fronthaler and J. Bigun, "Non-Intrusive Liveness Detection by Face Images", *Image and Vision Computing*, Vol. 27, No. 3, pp. 233-244, 2009.

[20] A. Anjos and S. Marcel, "Counter-Measures to Photo Attacks in Face Recognition: A Public Database and a Baseline", *Proceedings of IEEE International Joint Conference on Biometrics*, pp. 1-7, 2011.

[21] J. Kim, H. Choi and W. Lee, "Spoof Detection Method for Touchless Fingerprint Acquisition Apparatus", Korea Patent, Vol. 1, No. 54, pp. 314, 2011.

[22] Z. Zhang, D. Yi, Z. Lei and S.Z. Li, "Face Liveness Detection by Learning Multispectral Reflectance Distributions", *Proceedings of IEEE International Conference and Workshop on Automatic Face and Gesture Recognition*, pp. 436-441, 2011.

[23] S. Marcel, M.S. Nixon and S.Z. Li, "*Handbook of Biometric Anti-Spoofing*", Springer, 2014.

[24] R.D. Albu, "Face Anti-Spoofing based on Radon Transform", *Proceedings of 13th IEEE International Conference on Engineering of Modern Electric Systems*, pp. 1-4, 2015.

[25] I. Chingovska, A. Anjos and S. Marcel, "On the Effectiveness of Local Binary Patterns in Face Anti-Spoofing", *Proceedings of International Conference of Biometrics Special Interest Group*, pp. 1-7, 2012.