Volume 7, Issue 3, March 2017 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

An Intelligent Approach for Anti-Spoofing in a Multimodal Biometric System

P. Devakumar[*]
M.Tech(Information Security), Dept. of CSE
Pondicherry Engineering College,
Puducherry, India

R. Sarala
Assistant Professor, Dept. of CSE
Pondicherry Engineering College,
Puducherry, India

DOI: 10.23956/ijarcsse/V7I3/0143

Abstract— Biometric systems are vulnerable to certain type of attacks at various points in the biometric model. A spoofing attack which is submitting a stolen, copied biometric trait to the sensor to gain unauthorized access to the biometric system is one among them. Multimodal biometric systems are designed to increase the accuracy of the biometric system, but they are more vulnerable to spoofing attacks than a unimodal biometric system. The existing approaches for anti-spoofing do not consider multiple biometric traits and also have a high false acceptance rate. The proposed method is designed to overcome spoofing in a multimodal biometric system that uses a combination of face, fingerprint and iris images. The extracted biometric features are fused and fed to a convolution neural network that employs deep learning to detect spoofed features from real features. The proposed method gives better results than existing anti-spoofing methods.

Keywords— Multimodal Biometrics, Anti-spoofing, Biometric feature extraction, Biometric feature fusion, Convolution Neural Network.

I. INTRODUCTION

The Multimodal biometric systems use more than one biometric trait. The Multimodal biometric systems use different mechanisms for biometric fusions. Multimodal biometrics are often referred to as multi- biometrics. Unimodal biometric systems often fail to correctly identify and verify an individual with a desired result and accuracy. Multimodal biometric systems are designed for this purpose. There are several kinds of attacks [1] in a Multimodal biometric system as shown in Figure 1 and they are type 1 attack include presenting fake biometrics at the sensor where a fake biometric sample is presented as input to the system. Type 2 attacks include replay attack where a biometric signal is stored and then it is replayed to access the system. Type 3 attacks include overriding the feature extraction where the feature extractor is attacked using a Trojan horse so that it produces feature sets selected by the intruder. Type 4 attacks include replacing features where the features extracted from the biometric input signal are replaced with a different feature set. Type 5 attacks include Corrupting the matcher where the matcher is attacked to produce preselected match scores. Type 6 attacks include tampering with stored templates where the attacker modifies a template in the Database. Type 7 attacks include attacking the channel between the stored templates and the matcher where the data sent to the matcher through a communication channel are modified. Type 8 attacks include overriding the final decision where the attacker is able to override the final match decision.

A spoofing attack is a type 1 attack, where a stolen, copied biometric trait is submitted to the sensor to gain unauthorized access to the biometric system. It is used to defeat the biometric system. This kind of attack is also called as “direct attack” since it is carried out directly on the biometric sensor. The feasibility of a spoof attack is much higher than other types of attacks against biometric systems. Since it does not require any knowledge of the system.

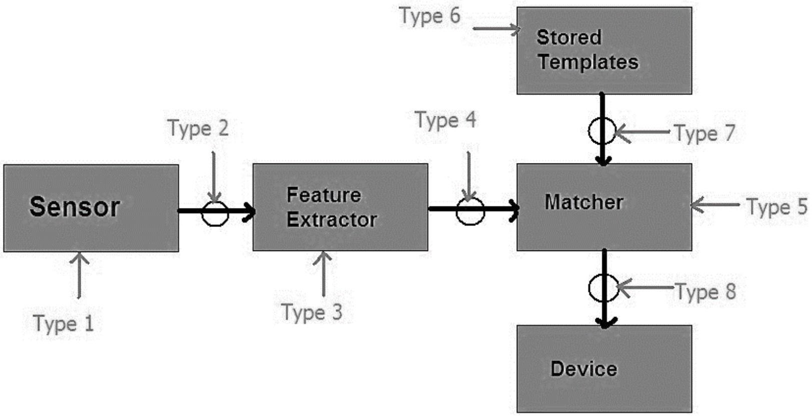

Figure 1. Types of attacks in biometric System

A multimodal biometric system can be defeated easily by an impostor even by spoofing only one biometric trait. Anti-spoofing is a technique to detect spoofing attack in the biometric system. It checks whether the biometric input is real of spoof using image processing techniques. Facial biometrics spoofing techniques involve placing genuine photographs or dummies and playing recorded videos. Artificial fingerprints can be easily created using silicon, wax, gelatine and mouldable plastic or clay. The iris spoofing methods include iris images, photographic surfaces, fake glass or plastic eye and iris texture printed on contact lenses.

The rest of the paper is organized as follows: In Section 2, the literature survey on anti-spoofing techniques in a multimodal biometric system are described. The proposed work for anti-spoofing is discussed in Section 3. The experimental results are discussed in Section 4. The conclusion is presented in Section 5.

II. RELATED WORK

A. Face anti-spoofing

In [2] swing Kollreider et.al proposed a facial anti-spoofing technique proposed is based on lip movement. Users are asked to start uttering the specific number sequence prompted randomly from 0 to 9 and each lip movement was recorded sequentially. Using optical flow features, the 10 lip movements of users were categorized into 10 different classes trained by SVM classifier. In [3] Bao et.al designed a technique using optical flow is designed for face spoof detection. The differences and properties of optical flow fields are analysed. These measurements are generated from 3D objects and 2D planes such as translation, rotation, moving in forward or backward and swing. In [4] Kant et.al presented a method based on fusion of thermal imaging and skin elasticity of human face is presented. In this method, the user is asked to chew and move forehead simultaneously. The correlation coefficients are calculated between the images captured by web camera. The facial skin elasticity is measured by using discriminant analysis to differentiate the human skin from other materials such as gelatine, cadaver, rubber, clay, etc.

In [5] Litong Feng et.al proposed image quality cues and motion cues are fused for liveness Detection face biometrics. This work is a combination of shearlet-based image quality feature (SBIQF), Optical flow based face motion feature and optical flow-based scene motion feature. Shearlet is utilized to develop an image quality-based liveness feature. Dense optical flow is utilized to extract motion-based liveness features. In [6] Shervin et al designed a multiscale dynamic texture descriptor based on binarized statistical image features (BSIF) on three orthogonal planes (MBSIF-TOP). The BSIF computes a binary code string for each pixel in an image where each bit is obtained by first convolving the image with a linear filter and then binarizing the filter responses. In [7] Ling Mei et al proposed a robust local descriptor, called WLD-TOP. It combines temporal and spatial information into a single descriptor with a multiresolution strategy. The TOP method extracts descriptor code from XY, XT and YT plane. The WLD-TOP descriptor is obtained by concatenating WLD on three orthogonal planes, namely XY, XT and YT.

B. Fingerprint Anti-spoofing

In [8] Tan et.al developed a new method is developed to quantify the perspiration property in a single image. The ridge signal which represents the gray level values is extracted. Then wavelet transform is used to decompose this signal into multi-scales. On each scale, static features are taken to quantify the perspiration pattern to differentiate between live and non-live fingerprints. In [9] Jia et.al presented an anti-spoofing method based on the analysis of human skin elasticity is presented. Once the fingertip is on the scanner surface, a sequence of fingerprint images are captured which describe the finger deformation process. The correlation coefficient between the fingerprint area, the signal intensity and the standard deviation of the fingerprint area are extracted from the image sequence. The Fisher Linear Discriminant is used to discriminate the real from artificial materials in [10] Tan et.al described a liveness detection method is described based on noise analysis along the valleys of the ridge-valley structure of fingerprint images. Statistical features are extracted in multiresolution scales using the wavelet decomposition technique.

In [11] Abhisheket al proposed a minutiae count method to detect the fake fingerprint. Minutiae represent a ridge end or ridge bifurcation in the fingerprint. The fingerprint image is binarized. Morphological operations are applied for thinning and then the number of minutiae is counted. Zahid et al. [12] proposed to measure correlation to detect spoofing. The correlation between real and fake images are used for classification. The features are extracted from a fingerprint image using texture descriptors. The proposed work uses Partial Learn Square (PLS) to learn the correlation. The classification scheme based on SVM, GMM, Gaussian Copula and Quadratic Discriminant Analysis is used to classify whether the input fingerprint is coming from live person or not. Murilo et al [13] combined fingerprint level3 feature, statistical features and image quality features to detect the spoofing. The pore frequency and number of pores are calculated. The statistical features are energy, entropy, mean, variance, skewness and kurtosis. These features represent the visual differences in the gray level intensities that can be observed between live and fake fingerprints.

C. Iris Anti-spoofing

In [14] Daugman et.al presented an anti-spoofing technique based on multispectral illumination to find the difference in the reflectance properties between the iris and the sclera at different wavelengths. In [15] spoof detection based on behavioural eye features like the eye hippos is presented. Eye hippos are a permanent oscillation by the eye pupil even under uniform lighting. In [16] an iris anti-spoofing technique is presented based on the specific characteristics of conjunctival vessels and iris textures that can be extracted from multispectral images.

Diego et al. [17] proposed Local Binary Pattern. LBP for spoof detection LBP encodes the intensity variations between a pixel and its neighbouring pixels. For each pixel, the surrounding pixels and sampled. The result of LBP is a binary code. Oleg el al. [18] proposed Liveness detection techniques in the area of eye movement biometrics. Two attack scenarios were considered, in which the imposter does and does not have direct access to the biometric database. Liveness detection was performed on the feature-level and match score-level for several existing eye movement biometric techniques. The results suggest that eye movement biometrics are highly resistant to circumvent by artificial recordings when liveness detection is performed at the feature-level. Mohit et al. [19] proposed to spoof an iris recognition system by synthesizing a semi-transparent contact lens. The Response of Gaussian derivative filters with multiple scales and orientations at each pixel location is clustered using K-means to certain regions with different textures.

D. Fingerprint Anti-spoofing

In [20] PeterWild et al presented a robust multimodal anti-spoofing technique by combining face and fingerprint biometrics. In this method median filtering concept is used to extract features from input data. An analysis of median filter for filter radius is presented. The bootstrap aggregating classifier is used for anti-spoofing. In [21] the various local descriptors for face, fingerprint and iris biometric traits are analyzed. The analyzed features are LBP, LPQ, WLD, BSIF, SIFT, DAISY, LCPD and SID. In [22] the issues in multimodal anti-spoofing are presented. The various measures involved in multimodal spoofing are given.

III. PROPOSED WORK

The proposed system extracts different type of feature from each biometric trait. The overall architecture of the proposed system is given in Figure 2. The modules in the system are feature Extraction, Feature Fusion, and Classification. In Feature Extraction the ridgelets are used to extract features from the face biometric input. The level1 and level2 features are extracted from the fingerprint. From the Iris image, the Local Ternary Pattern is calculated. In Feature Fusion, the extracted outputs will be fused and then it will be sent to the classification. In Classification, the convolution neural network classifies the output as real or spoof.

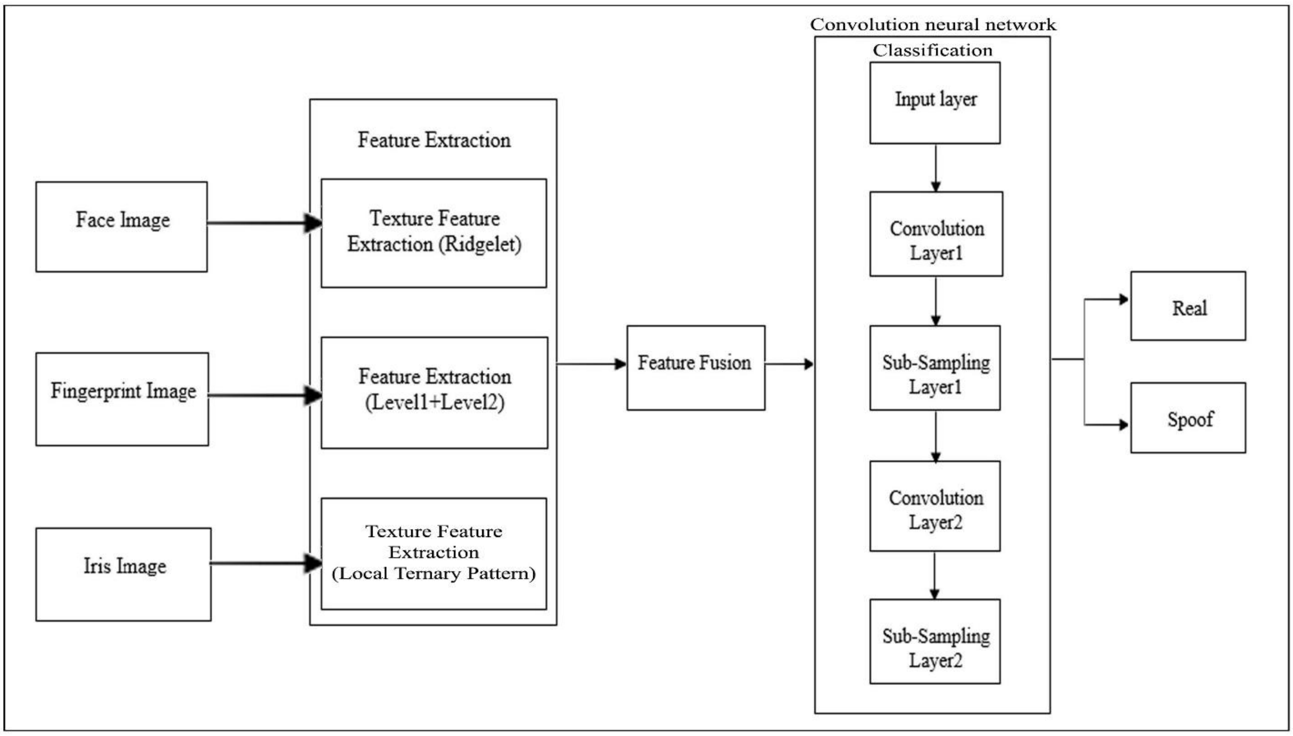

Figure 2. Overall architecture diagram of the proposed anti-spoofing approach

A. Feature Extraction

1) Face Feature Extraction: Ridgelets are effective to represent objects with singularities along lines. The ridgelet transform [23] maps line singularity into point singularity using radon transform. The ridgelets are a way of concatenating 1-D wavelets along lines. The image is decomposed into blocks. The ridgelet transform is applied to each block.

```
Algorithm: Ridgelet-Transform
Step1.  Compute the 2-D Fast Fourier Transform of the Face biometric image.
Step2.  Perform Cartesian to Polar Conversion.
Step3.  Compute the 1-D Inverse Fourier Transform (IFFT) on each line of the digital polar grid.
Step4.  Apply wavelet transform along the radial variable in the Radon space.
```

2) Fingerprint Feature Extraction: The block orientation map [24] is estimated from the given fingerprint image. Then orientation coherence is calculated. The Gradient based method is used for calculating orientation map. The minutiae count [11] is calculated for the fingerprint.

```
Algorithm: Orientation-map
Step1.  Compute the gradients in the x direction and y direction using a Sobel operator.
Step2.  Calculate Gradient angle.
Step3.  Create a Block orientation map.
Step4.  Calculate Orientation coherence from orientation map.
```

```
Algorithm: Minutiae-Count
Step1.  Adjust image intensities to enhance contrast.
Step2.  Convert the gray scale image to a binary image.
Step3.  Find the ridges of one pixel length.
Step4.  Detect Minutiae points using 3X3 pattern masks
```

*3) Iris Feature Extraction:*The Local Ternary Pattern [25] is a ternary or 3-valued code. In LTP the neighbourhood pixel values are compared with the central pixel using a lag limit value ‘l’. Based on this comparison the neighbourhood values will be assigned one of the three values +1 or 0 or -1.

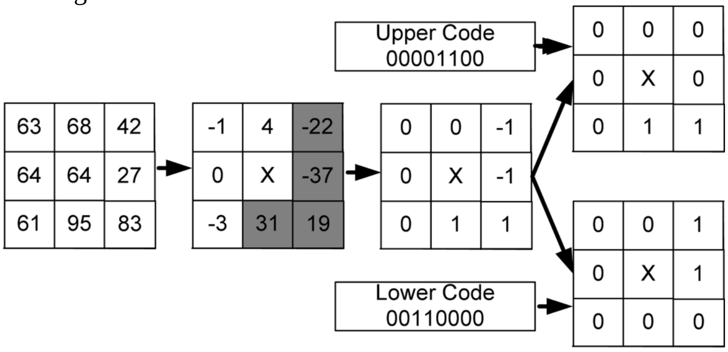

Figure 3. Local Ternary Pattern

```
Algorithm: LTP
Step1.  Assume C as center pixel and p as neighboring pixel
Step2.  The threshold is calculated as
        If p>c+k then the value will be 1,
        If p>c-k and p<c+k then the value will be 0,
        If p<c-k then the value will be -1.
Step3.  Combine neighboring pixels.
Step4.  Compute histogram for these values
```

B. Feature Fusion

The features extracted from the face image, fingerprint image and iris image are combined to form a feature vector for classification. In feature-level fusion, the feature sets originating from multiple biometric algorithms are consolidated into a single biometric feature set by using appropriate techniques like feature normalization, feature selection and transformation. In the feature-level fusion the detection of correlated feature values are generated by different biometric algorithms and to identifying a salient set of features that can improve recognition accuracy. In feature normalization, individual feature values of vectors X and Y may exhibit significant variations both in their range and distribution. The goal of feature normalization is used to modify the location and scale of the feature values in order to ensure that the contribution of each component to the final match score is comparable. The technique used for feature normalization is Min-Max. The feature selection process selects a minimal set of relevant features that contains maximum discriminatory information while discarding many redundant or irrelevant features. It can be performed either prior or after the fusion to extract useful features from the larger set of features. The techniques used for feature selection is sequential forward selection (SFS), the feature transformation transforms the existing fuse features into a lower dimensional space, where the classification task is made easier. This may include linear techniques like Principal Component Analysis (PCA) or Linear Discriminant Analysis(LDA) or non-linear techniques like Subclass Discriminant Analysis(SDA). The technique used for feature transformation is Principal Component Analysis(PCA).

C. Classification

The Convolution neural network (CNN) is used for classification [26]. It contains sampling layer and convolution layer. The architecture of a typical CNN is composed of multiple layers where each layer performs a specific function to get the useful representation from the input. The convolution layer forms the basis of the CNN and performs the core operations of training. Convolutional layers consist of a rectangular grid of neurons that perform the convolution operation over the input. The sub-sampling layeris placed after the convolutional layer. It will alsoreduce the spatial dimensions of the input volume for the next convolutional Layer.

There are three types of layers in a Convolutional Neural Network which includes convolutional layers, pooling layers and fully connected layers.

Convolutional Layers: The convolutional layer is a building block of a CNN. The layer's parameters consist of a set of learnable filters, which will have a smaller receptive field, but extend through the full depth of the input volume. During the forward process, each filter is convolved across the width and height of the input volume, then it will compute the dot product between the entries of the filter and the input to produce a 2-dimensional activation map of that filter. As a result, the network learns filters that activate when it detects some specific type of feature at any spatial position in the input.

*Pooling Layer:*These layers follow a sequence of one or more convolutional layer and are intended to Consolidate the features learned and expressed in the previous layers feature map. The function of the pooling layer is to progressively reduce the spatial size of the representation to reduce the amount of parameters and compute in the network, and hence to also control the overfitting. It is common to periodically insert a pooling layer in-between successive layer.

Fully Connected Layers: These layers are the normal flat feed-forward network layer. These layers may have a non-linear activation function or softmax activation in the output layer of class predictions. After feature extraction and consolidation the fully connected layers are used in the performance of convolutional and pooling layers. They are used to create final non-linear combinations of features and for making predictions by the network.

IV. EXPERIMENTAL RESULTS

The multimodal database used for anti-spoofing is BiosecurID[27] database. This database consists of 20 real face samples, 128 real fingerprint samples and 32 real iris samples. The description about BiosecurID database is given in Table 1. The performance of the proposed anti-spoofing method is measured in terms of false acceptance rate and false rejection rate. The False Acceptance Rate(FAR) is the rate of spoof images that are accepted by the system. The False Rejection Rate(FRR) is the rate of real images that are rejected by the system. The Half Total Error Rate (HTER)denotes the average of FAR and FRR The proposed method is compared with the existing techniques in Table II. The proposed method is compared with the following existing methods: Local Binary Pattern (LBP), Weber Local Descriptor (WLD), Local Phase Quantization (LPQ), Binarized Statistical Image Feature (BSIF) and Local Contrast Phase Descriptor (LCPD). The proposed method gives better result than existing methods.

Table I Multimodal Biosecurid Database

Modality	**Model**	**Main Features**	**Number of Samples**
Face	Philips ToUcam Pro II	CCD. Illumin. 1 lux Image size: 640 x 480 pixels	20
Fingerprint	Biometrika FX2000	Optical 569 dpi Capture area: 13.2x24.9 mm Image size: 400x560 pixels	64
	Yubee (Atmel sensor)	Thermal sweeping 500dpi Capture area: 13.9x0.5mm Image size: 280x8 pixels	64
Iris	LG Iris Access EOU 3000	CCD Infrared illumin image size: 640x480 pixels	32

FAR: It represents the percentage of fake images misclassified as real.

$$FAR = \frac{MisclassifiedSpoofRecordings}{TotalSpoofRecordings}$$

FRR: It represents the percentage of Real images misclassified as Fake.

$$FRR = \frac{MisclassifiedLiveRecordings}{Total\ Live\ Recordings}$$

HTER: It denotes the average of FAR and FRR.

$$HTER = \frac{FAR + FRR}{2}$$

Table II Comparison With The Existing Approaches

	HTER		
Methods	**Face**	**Finger print**	**Iris**
LBP	2.8	28.6	6.3
WLD	5.5	1.2	7.1
LPQ	8.5	5.1	5.8
BSIF	2.9	9.0	9.4
LCPD	4.3	1.0	4.5
Proposed Work	2.4	0.89	3.6

V. CONCLUSION

An Intelligent anti spoofing mechanism for a multimodal biometric system is composed of face, fingerprint and iris biometrics is implemented. The technique uses ridgelet for face feature extraction, minutiae count and orientation coherence for fingerprint feature extraction and Local Ternary Pattern for iris feature extraction. The features are combined using feature level fusion and classified using the convolution neural network. The proposed method is evaluated using benchmark dataset BiosecurID multimodal Dataset. The proposed method gives better result than existing methods.

REFERENCES

[1] Ratha, N., Connell, J., Bolle, R. "An analysis of minutiae matching strength". *Proc. AVBPA, International Conference on Audio- and Video-Based Biometric Person Authentication III*, pp. 223-228, 2001.

[2] Kollreider, K., Fronthaler, H., Faraj, M. and Bigun, J., "Real time face detection and motion analysis with application in liveness assessment".*IEEE Trans. Infor. Forensics and Security,* (part 2), pp.548–558, 2007

[3] Bao, W., Li, H., Li, N. and Jiang, W., "A liveness detection method for face recognition based on optical flow field", *Proc. In International Conference on Image Analysis and Signal Processing IASP*, IEEE, 2009, pp. 233–236, 2009.

[4] Kant, C. and Sharma, N., Fake face recognition using fusion of thermal imaging and skin elasticity. *IJCSCIJ*, 4(1), pp. 65–72, 2013.

[5] Litong Feng, Lai-Man Po, Yuming Li, Xuyuan Xu, Fang Yuan, Terence Chun-Ho Cheung, Kwok-Wai Cheung, "Integration of image quality and motion cues for face anti-spoofing: A neural network approach, " *Journal of Visual Communication and Image Representation*,Vol. 38, pp. 451–460, 2016.

[6] ShervinRahimzadehArashloo and Josef Kittler, "Face Spoofing Detection Based on Multiple Descriptor Fusion Using Multiscale Dynamic Binarized Statistical Image Features," *IEEE Transactions on Information Forensics and Security,* Vol.10, No.11, pp. 2396 – 2407, 2015.

[7] Ling Mei1, Dakun Yang, Zhanxiang Feng, and Jianhuang Lai. "WLD-TOP Based Algorithm against Face Spoofing Attacks," *Springer International Publishing, Lecture Notes in Computer Science*, Vol. 9428, pp. 135-142, 2015.

[8] B. Tan and S. Schuckers. "Liveness detection for fingerprint scanners based on the statistics of wavelet signal processing*", In Computer Vision and Pattern Recognition Workshop, 2006. CVPRW'06. Conference on*, pp. 26–26. 2006.

[9] J. Jia, L. Cai, K. Zhang, and D. Chen, " A new approach to fake finger detection based on skin elasticity analysis". *Proc. Lecture Notes in Computer Science*, pp. 309–318, 2007.

[10] B. Tan and S. Schuckers, "New approach for liveness detection in fingerprint scanners based on valley noise analysis",*Journal of Electronic Imaging,* 17(1), pp.011009–011009, 2008.

[11] Kumar Abhishek, Ashok Yogi, "A Minutiae Count Based Method for Fake Fingerprint Detection," *Procedia Computer Science,*Vol. 58, pp.447-452, 2015.

[12] Zahid Akhtar, Christian Micheloni and Gian Luca Foresti, "Correlation Based Fingerprint Liveness Detection," *in Proc. IEEEInternational Conference on Biometrics (ICB)*, pp. 305-310, 2015.

[13] MuriloVarges da Silva, AparecidoNilceu Marana and Alessandra AparecidaPaulino, " On the Importance of Using High Resolution Images, Third Level Features and Sequence of Images for Fingerprint Spoof Detection," *in Proc. IEEE International Conference on Acoustics, Speech and Signal Processing,* pp. 1807 – 1811, 2015.

[14] J. Daugman, "Iris recognition and anti-spoofing countermeasures," *in Proc. IBC*, 2004.

[15] S. J. Lee et al., "Robust fake iris detection based on variation of the reflectance ratio between the iris and the sclera,"*in Proc. BSym,* pp. 66–71, 2006.

[16] R. Chen, X. Lin, and T. Ding, "Liveness detection for iris recognition using multispectral images," *PRL*, vol. 33, pp. 1513–1519, 2012.

[17] Diego Gragnaniello, Carlo Sanson, Luisa Verdolivaa, "Iris liveness detection for mobile device based on local descriptors*," Pattern Recognition Letters,* Vol. 57, pp.81–87, 2015.

[18] Oleg V. Komogortsev, Alexey Karpov and Corey D. Holland, "Attack of Mechanical Replicas: Liveness Detection with Eye Movements", *IEEE Transactions On Information Forensics And Security*, vol. 10, no. 4, April 2015.

[19] Mohit Kumar and N. B. Puhan, "Iris Liveness Detection Using Texture Segmentation," *in Proc. Fifth National Conference on Computer Vision, Pattern Recognition, Image Processing and Graphics (NCVPRIPG),* pp.1-4, 2015.

[20] Peter wild, petru Radu, Lulu chen and James Ferryman, "Robust multimaodal face and fingerprint fusion in the presence of spoofing attacks", *PatternRecognition*, Vol.50, pp.17–25, 2016.

[21] Diego Gragnaniello, Giovanni Poggi, Carlo Sansone,, and Luisa Verdoliva, "An Investigation of Local Descriptors for Biometric Spoofing Detection", *IEEE Transactions on Information Forensics And Security*, Vol. 10, No. 4, April 2015.

[22] Giorgio Fumera , Gian Luca Marcialis, Battista Biggio, Fabio Roliand Stephanie Caswell Schucker, "Multimodal Anti-spoofing in Biometric Recognition Systems", *Advances in Computer Vision and Pattern Recognition,* pp 165-184, 2014.

[23] Donoho DL, Flesia AG, " Digital ridgelet transform based on true ridge functions", *Academic,* New York, 2001.

[24] KASS M., WITKIN A." Analyzing Orientated Pattern", *Computer Vision, Graphics and Image Processing*, Vol. 37, pp. 362-397, 1987.

[25] Tan, Xiaoyang, and Bill Triggs. "Enhanced local texture feature sets for face recognition under difficult lighting conditions".*Image Processing*, pp.1635-1650, 2010.

[26] Krizhevsky, I. Sutskever, and G. E. Hinton, "ImageNet Classification with Deep Convolutional Neural Networks", *proc. Advances in Neural Information Processing Systems (NIPS)* , 2012.

[27] J. Galbally, J. Fierrez, J. Ortega-Garcia, M. R. Freire ,F. Alonso-Fernandez, J. A. Siguenza, J. Garrido-Salas, E. Anguiano-Rey,G. Gonzalez-de-Rivera, R. Ribalda, M. Faundez-Zanuy, J. A. Ortega,V. Carde˜noso-Payo, A. Viloria, C. E. Vivaracho, Q. I. Moro, J. J. Igarza, J Sanchez, I. Hernaez and C. Orrite-Uru˜nuela, "BiosecurID: a Multimodal Biometric Database", *Journal of Pattern Analysis and Applications*, Vol.12, No.2, 2010.