Occlusion and spoof attack detection using Haar Cascade classifier and local binary pattern for human face detection for ATM

Cite as: AIP Conference Proceedings **2494**, 050004 (2022); https://doi.org/10.1063/5.0107262
Published Online: 31 October 2022

Nandkumar Kulkarni, Dnyaneshwar Mantri, Pranav Pawar, et al.

Occlusion and Spoof Attack Detection using Haar Cascade Classifier and Local Binary Pattern for Human Face Detection for ATM

Nandkumar Kulkarni[1, a)], Dnyaneshwar Mantri[2, b)], Pranav Pawar[3, c)], Madhukar Deshmukh[4, d)], Neeli Prasad[5, e)]

[1]Smt. Kashibai Navale College of Engineering, Pune, India
[2]Sinhgad Institute of Technology, Lonavala, India
[3]Birla Institute of Technology & Science, Pilani - Dubai Campus, United Arab Emirates
[4]K L University, Guntur, Andhra Pradesh, India
[5]TrustedMobi, VehicleAvatar Inc., USA

[a)]Corresponding author: npkulkarni.skncoe@sinhgad.edu
[b)]dsmantri.sit@sinhgad.edu
[c)]pranav@dubai.bits-pilani.ac.in
[d)]madhukar_aau@kluniversity.in
[e)]neeli.prasad@vehicleavatar.com

Abstract. The crime rate has been rising at an unprecedented rate, and security has become a big concern in ATM machines. Face detection is the most common biometric technique due to its non-invasive nature. It's been used in a variety of fields, including camera auto focus, attendance, crowd monitoring, object tracking, security, system, etc. Face detection systems uses image processing techniques that are being learned to operate reliably in a variety of conditions, including changes in posture, lighting, skin color, occlusion, and face spoofing. The face detection system has become increasingly vulnerable to occlusion. Occlusion refers to the deliberate shielding of one's face with a helmet, sunglasses, scarves, or other items in order to avoid being caught. These issues have a significant impact on the development of image processing techniques and system's performance. In this paper the Haar Cascade Classifier (HCC) scheme is projected for face detection where precision as well as minimal processing time are important factors for ATM. The proposed scheme uses deep learning models such as Convolutional Neural Networks to enhance the reliability in feature extraction plus classification of images. Face biometric access control devices are becoming more common in everyday lives, but they remain vulnerable to spoofing attacks. This paper also proposes face spoofing identification using Local Binary Pattern (LBP) that has useful features for face detection. The proposed spoofing attack detection technique has yielded encouraging results.

Keywords— Face Detection, Haar Cascade classifier, Face Spoof Detection, Local Binary Patterns.

INTRODUCTION

Face detection is a computer technique that recognizes human faces in digital imagery and is used in a number of applications such as law enforcement, security measure, phone unlock, biometrics etc. The face detection will be a focused research topic because of its efficiency and transparency where the human does not need to cooperate much and the detection systems are being trained to work accurately under variations in pose, illumination, skin color, occlusion, face spoofing etc [1-3]. This, results in generation of various false positives, acceptable yet rejected detects, false negatives which make face detection system vulnerable. Out all the bio metric systems face detection is the most preferred system for the reason that it's non- invasive in type and also it does not take much time of the people to pass through the security system. Some of the problems faced by face detection system is face spooking where the system is fooled using a fake photo instead of a live one. Illumination variation causes errors in results. Face occlusion (Ref. Fig.1) detection where the face is covered by a scarf, glasses, helmet, etc. is a necessary security measure to tackle crime rate. Occlusion detection pinpoints the disguised individuals and then sends real time alarms when a suspicious person has been detected [4]**.** Various methods have been proposed to detect face occlusions. and to allow individuals access to ATM based on the outcome of occlusion detection. A picture of the individual will be captured by a camera on the machine which will be stored in the memory with a timestamp. If any illegal activity is reported related to that ATM center at a specific time, it would be much easier for the crime department officials to trace the culprit. The increasing no of ATM robbery is the main motivation for the problem under consideration. Each ATM is equipped with a surveillance system that records customer face details. When offenders use the ATM to withdraw illicit funds, they normally conceal their faces with something so that the security device does not capture their facial details. A human security can be breached by threatening, bribing, influencing, etc. So that’s why there is a need of new and advance security solutions.

FIGURE 1. Face Occlusion Examples

LITERATURE SURVEY

By looking at a person's face, one can learn about their speech, gender, age, and ethnicity [4-7]. Appearance-based approaches and feature-based approaches are two broad types of face recognition methods. In the appearance-based technique, the face detector receives the entire image as input. Face identification based on characteristics like shape of the face, eyes, hair, and mouth extracted from a picture is known as a feature-driven method. Focused on corners, lines, and curves (generic), template-based, and Structural matching are the three different kinds of attribute extraction methods [8]. Geometric and Appearance based techniques are preferred for facial extraction. In ATMs only the surveillance cameras cannot stop anyone from accessing the machine if their face is obstructed. CNN is a deep learning architecture that combines feature extraction and classification for face occlusion detection [9]. The head position is first observed in a test picture, followed by the presence of eyes and mouth. A cascaded CNN followed by two cascaded CNN is used to detect head, eyes and mouth respectively in the proposed system [2]. There are seven CNNs in cascade for the face occlusion detection system-3 for head detection (head-16-net, head-32-net, and head-48-net), 2 in lieu of eye revealing (eye-net), and 2 in lieu of mouth revealing (mouth-net). YOLO (You Only Look Once) improves detection accuracy by training on complete photographs. In this strategy, object recognition is interpreted as a single regression problem. Item detection's various components are merged into a single neural network. YOLO is highly quick (basic network – 45 frames per second, fast version – 150 frames per second). YOLO views the full image during training and testing, unlike region proposal-based approaches, therefore it indirectly stores contextual facts about classes in addition to their presence [10].

The Fast Regional Convolutional Neural Network (R-CNN) is a variant of the Spatial Pyramid Pooling Network (SPPnet) which employs a single SPP layer, as well as the RoI layer to fine-tune a pre-qualified ImageNet prototype from start to finish. It is made up of dual module termed as Regional-Proposal-Network (RPN), that is an entirely convolutional network that generates item suggestions for the next module [11]. Many face spoofing detection algorithms such as Texture evaluation, Analysis of motion, Evaluation of image quality, and Methods based on hardware have been presented since the early 2000 [12-13]. To explain the distinctions between actual and synthetic faces, the authors in retrieved multi-scale LBP features and SVM like classifiers [14-17, 22]. In [18] the authors retrieved Haralick characteristics commencing from video frames. An approach based on color-textures to record color changes in brightness and chrominance is available in [23]. In [19] the authors employed Gaussian pyramids to extract multi-scale textural characteristics and utilized them to detect fraudulent faces in another study. For spoof detection, authors in [20, 24] suggested an endwise CNN mechanism. Instead of employing fully connected layers, [4] uses convolutional feature maps to extract hand-crafted features and shown good results. A LSTM to identify face spoofing is presented in [21]. Table 1 shows a comparison of the key occlusion and spoof detection approaches.

TABLE 1. Literature Survey

Ref. No	Method	Metrics and Findings	Advantages	Disadvantages	Usage
[1]	Deep CNN	Detection accuracy of 98%, 86% and 100% on the AR face db, face occlusion db and LFW dataset	Uses RCNN with Deep Networks	Person wearing clothing complex textures leads to generation of negative data	Used for Occlusion detection
[2]	Head, eye and mouth recognition.	AR dataset 92.7%, FO dataset 93.1%	7-layer Cascaded CNN model.	Computationally complex	Grey scale image, Face Occlusion detection, histogram equalization
[3]	Uses Haar classifier	A Histogram is produced of the normalize-d image	Better performance in case of the dim lit conditions of the images.	Normalization of the image required to overcome cons of dim lit images.	Gary processing of the image, histogram normalization for face detection.
[4]	Local Binary Pattern (LBP)	Equal error rates reduce from 7% to 0.6%	Outperforms the state of art methods	Detection fails for particular attack.	Spoof detection with less complex network's layers
[5]	Face spoofing identification utilizing deep learning as well as domain generalization	Lesser error rate	More prejudicial and generic knowledge can be learned by the classifier.	Collecting a huge database covering all camera models, lighting situations, and facial traits is complicated.	Anti-spoofing and Face recognition.
[6]	Haar Cascade Classifier used with Open CV	Simple background = 0% False detection rate and with complex background = 6.76% false detection rate	Speed and reliability. Works very well for simple ackgrounds No restriction on wearing glasses	Gives high performance for simple background.	Used for detection of face.
[7]	Methods like Gabor filters, LBP, PCA etc.	Accuracy from 95-100% obtained using these techniques	Extracts prominent features efficiently.	Need large no of features	Used in face recognition
[8]	Single regression problem.	YOLO scores 57.9% mAP (mean Average Precision)	Fast real-time processing.	YOLO has a lower score than R-CNN by 8-10%	Real time object Detection
[9]	Selective Search Algorithm, Region proposals	Approximately takes 0.4 secs to detect the face	Less false positives than MTCNN.	Computationally complex than haar classifier	Face Detection.
[10]	Support Vector Machine (SVM)	TPR around 80%	Fake-face images taken from a Samsung Galaxy Alpha and an iPhone 5Sas well	Prior understanding of the processing system, as well as some command over it, is essential.	Face Detection.
[11]	Non-linear diffusion	No of Iteration, accuracy	Prevention against face-spoofing	Increasing iterations reduces the accuracy and requires more computational time	Anti-spoofing, and detection of replay attacks

EXISTING SYSTEM

A cascaded CNN is utilized for head detection, with dual cascaded CNNs for eye and mouth occlusion detection. In CNN model the captured color image is transformed to greyscale. These greyscale images undergo histogram equalization before being scanned using the sliding window method. The three cascaded head detection nets (head-16-net, head-32-net, and head-48net) are used to determine head position. The head-16-net scans the whole image at several scales to eliminate over 90% of the exposure windows in a test image. The remaining exposure windows are cut out and reduced to 32 x 32 pixels as input images for head-32-net to remove them completely. To assess the exposure window, final 48-net admits the discovery windows as 48 x 48 pictures [2]. Then eye-net and a mouth-net procedure is applied to check for occlusion. Two CNNs are utilized in eye-net.

The first level CNN quickly rejects the majority of detection windows. The second level of CNN decides whether the exceptional windows are eye-catching or not. The mouth-net is built similarly to the eye-net, with the difference that the input picture size for the first and second level CNN is 32 * 16 and 64 * 32 respectively. This approach is highly efficient since the model learns hierarchically, so even if it identifies some real-life pictures that aren't in the dataset, it may still generate accurate results to a degree because it learns to identify occlusion based on past patterns. A face spoofing attack happens as soon as someone attempts to impersonate somebody by altering their appearance in order to obtain unauthorized access and benefits. Some of the existing methodologies are: The use of ultra-violet cameras to create a vein map of a person's face [3]. Another method suggested is 2-D Fourier spectra which works on two simple perceptions; the dimensions of a photo must be less than those of a live face and the photo is flat. Second, the standard deviation of frequency components in sequence must be extremely low [3]. Another method is color texture information that progresses the strength of diverse descriptors contrasted to their grey-scale equivalent [5]. It is proposed that a Fourier spectrum of sensor pattern noise (FS-SPN) be used [6].

PROPOSED SYSTEM

Most ATMs now have cameras embedded in to capture evidence in the event of a mugging or other crime. Software could detect the face of the user, and if no occlusion or obstruction found then it will let the user proceed with the card. It would store the image of the detected face with timestamp into the database. If there is any mask, helmet, cap, scarf etc. kind of occlusion on the face due to which the face is not detected properly then it will simply halt the machine and not proceed until a proper face detected. For detecting the occlusion, Haar Cascade Classifier (HCC) mechanism is utilized and additional layer for detecting the spoof attack have also been added, it uses LBP for the same. Haar characteristics are the most important aspect of the HCC for face detection. HCC is finest detectors in lieu of face detection from a picture with reference to speediness as well as trustworthiness. The Haar traits begins scanning the picture in order to distinguish face commencing the top left corner in addition terminates the process in the bottom right corner. To recognize the face inside image, the image is scanned numerous times via the haar-like characteristics [7]. To begin analyzing these attributes in any given picture, the Voila Jones method employs a 2424 window as the foundation window size. If all of the harr feature's that are available such as position, type, and scale, are considered then 160, 000 features in the timeframe need to be calculated, which is nearly impossible. The Adaboost algorithm is used to solve this issue.

Adaboost is a machine learning technique which aids in identification of the prominent traits amongst the 160,000. Adaboost builds a robust classifier as a linear grouping of several fragile classifiers. The HCC is used to detect whether a face is present or not. The cascade uses Haar-like features and is a tree-based technology [7]. The model need not be trained with haar features; instead, a classifier with a tiny dataset is built and trained. The weighting for each feature is utilized to educate the classifier successfully without a large quantity of training photos. Figure 2 depicts the overall basic system architecture diagram for occlusion detection. The camera/webcam captures the users face, and gives to the other module for pre-processing, where the image is turned grey from rgb and then prominent features of the face such as eyes, face, and mouth are enhanced and passed onto next layer where CNN are used to identify which all features have been enhanced and if they detect any prominent face like features, wherein it classifies if it’s a face or no, if not then there is an occlusion and the machine is halted, else the machine grants access for further use.

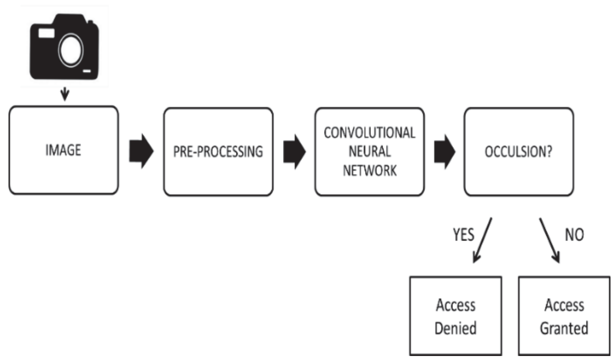

FIGURE 2. Architecture diagram

METHODOLOGY USED FOR IMPLEMENTATION

Algorithm

The ALGORITHM 1 is utilized for face and Occlusion detection.

ALGORITHM 1: Face Detection, Occlusion Detection

```
face_occlusion_detect(image)
{   flag = 0
    grey = convert image from BGR to grey
    face = detect face boundary coordinates from grey
    if (face detected)
    {       draw boundary around the face
            crop_face = crop the face from the grey
            roi_mouth = restrict the region of interest to lower half of crop_face
            mouth = detect face boundary coordinates from roi_mouth
            if (mouth detected)
            {       draw boundary around the mouth
                    nose = detect nose boundary coordinates from crop_face
                    if (nose detected)
                    {      draw boundary around the nose
                           roi_eye = restrict the region of interest to upper half of crop_face
                           eye = detect eye boundary coordinates from roi_eye
                             if (eye detected)
                             {       draw boundary around the eyes
                                     return crop_face
                             }
                    }
            }
    }
}
face_spoof_detection(image)
{   hist = generate histogram of image using local binary patterns
    prediction = predict whether the face is a spoof or not using trained model
    return prediction
}
```

The HCC consists of four stages:

1. **Haar Feature Selection:** A pre-processed image is passed and haar feature selection takes place on it. Edge, line and four rectangle features are selected using the haar like features, shown in Fig. 3. It calculates the average of the pixel intensities of a region (black and white) and takes the difference to search for a feature.

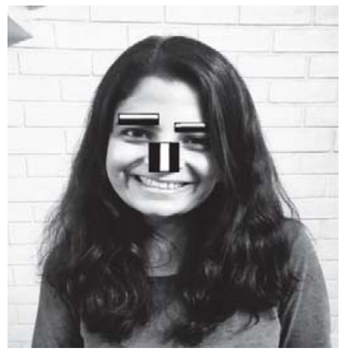

FIGURE 3. Haar like features

2. **Integral Image:** It aids in the computation of haar-like characteristics such as rectangle corner points and the coordinates of the point dividing white and black regions are referred rather than calculating the average a difference of all the pixel intensities in a particular region.
3. **Adaboost:** It is also called as a rejection cascade. More than 1,60,000+ features are created. Adaboost is used to reject the redundant and unnecessary features. It creates a powerful classifier by combining weak classifiers in a linear fashion (Ref. Equation 1).

$$f(x)=a_1f_1(x)+a_2f_2(x)+\ldots \tag{1}$$

Here, F(x) is robust classifier and f(x) are feeble classifiers. The weak classifiers help in detecting the occlusion on the mouth, nose or eyes if any.

4. **Cascading:** It is divided into phases, each of which having a set of characteristics. Each face's role is to assess whether or not a quantified sub-window is, in fact, a face, if not instantly discards it. The Fig. 4. (a) shows that the face is detected by the Haar classifier and the eyes, nose and mouth are identified by means of weak haar classifiers indicating that there is no occlusion detected on the face. In such a case ATM machine would proceed further. Whereas in the Fig. 4. (b), the face is detected but the mouth and nose are not detected as they are obstructed by the mask, in such a case the ATM machine would get a signal that it couldn't detect a proper face and hence it would either ask the user to retry or come to a halt.

Face Spoof Detection

To address the issues related to inadequate training data besides too much of network data, the authors present a unique end-to-end learnable LBP mechanism for face spoofing discovery (Ref. ALGORITHM 2). The proposed network has three different benefits due to the integration of set sparse binary filters with derivable statistical histogram procedures, the proposed network has three different benefits:

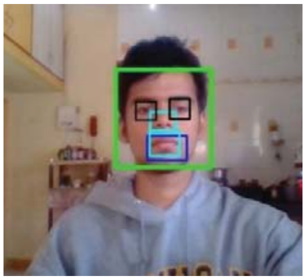

FIGURE 4. (a) Face detected and no occlusion by HCC

FIGURE 4. (b) Face detected and no occlusion by HCC

- significantly decreasing parameters in convolutional as well as fully connected layers
- efficiently educating the model with minimal input
- fully accomplishing the core LBP extraction procedure

The proposed network is made up of four modules: CLs, LBP layers, loss function, and classification layers. The network comprises of CL along with LBP layers in order to extract implemented LBP traits. A loss function module is utilized to educate the model and CL finds whether the input face is a spoofing attack.

ALGORITHM 2: Face Spoof Detection and Storing of Images

1. The input video is divided into continuous frames
2. These frames are feed into the LBP model to extract LBP features
3. The middle pixel is matched with surrounding eight pixels.
4. If the values of the surrounded pixel are larger or identical then 1 is inserted else 0.
5. Then an eight-bit binary number is obtained which is later converted to a decimal number and stored.
6. Decimal number can vary up to 256 different values that can be used to make a histogram and analyzing the variation in the grey-scale.
7. This gives an idea about the sharp features, if the values change from 0 to 1 or vice versa it means that an edge is been detected. Average is taken of these features.
8. This is then fed into the SVM classifier to get the classification results.
9. Once the face is detected, it scans for any occlusion on the face. If there is any occlusion detected, then stored in the SQLite database.

RESULTS AND DISCUSSION

The following were the results of the implemetation :

- Face detection module gave more than 90% of the accuracy while it is assumed that only one person is accessing the machine and the lighting conditions are up to the mark. The model accurately gives results just within a few seconds.
- With a less dim lit room or poor lighting conditions the accuracy/efficiency of the model would drop to 60%.
- The model detects the occlusion on the face accurately enough. First it detects the mouth and the nose, and then the eyes, if any of the feature is not detected then the it declares that occlusion is detected.
- The occlusion is also detected in almost 90%of the cases.

The HCC gives almost 100% of Face Detection rate, providing the pictures are taken with simple background and 93.24% of Face Detection rate with images having complex background. The experiments are conducted on the databases that is created to assess the efficiency of LBP network. The classifier is tested on two different types of assaults: printed images and replayed attacks. The databases are classified as fake and real (Ref. Table 2).

TABLE 2. Spoof attack Database

Databases	Count of images
Total Real images	3468
Total Fake images	3845

The accuracy is measures as the ratio of TPR (True Positive Rate) and TNR (True Negative Rate) on Total number of samples as shown in equation 2

$$\text{Accuracy} = \frac{TPR+TNR}{Total\ samples} \tag{2}$$

TABLE 3. TPR and TNR

TPR	TNR
0.836	0.858

Calculating from the data mentioned in Table 3 the accuracy of the spoof attack detection module is 0.848 (84.8%).

CONCLUSION AND FUTURE SCOPE

Conclusion

From an experimental standpoint, it is clear that the HCC performs exceptionally well for images with a simple background. The haar cascade method has a number of advantages:

- With reference to speediness and trustworthiness, the HCC is the best detector for large databases.
- Even if the picture is impacted by lighting, the results of face identification using the HCC are more accurate, and using glasses is not a need.

Given the benefits of the HCC, it is appropriate for real-time face identification. The paper proposes unique LBP network to tackle the problem of face spoofing detection. The proposed network blends hand-crafted traits by means of deep learning and uses statistical histograms to decrease network parameters. However, there are significant drawbacks to suggested network. For example, the proposed technique is incapable of detecting a certain type of assault. As a result, future work will focus on how to increase detection performance for a certain type of assault and expand the database to include new invasions.

Future Scope

If this is applied to ATM Security, the frequency of attempts of illegal activities of misusing lost or stolen credit/debit cards can be reduced significantly. As the technology will advance, face detection will be used almost everywhere. Advancement in security and digitalization of the world has made it a worthy topic to work on. Researchers are working in the direction to make it completely secure and reliable.

REFERENCES

1. Y. Xia , B. Zhang, and F. Coenen, *Face Occlusion Detection Using Deep Convolutional Neural Networks* (International Journal of Pattern Recognition and Artificial Intelligence, 2016), pp.1–24.
2. Y. Zhang, Y. Lu, H. Wu, C. Wen and C. Ge, *Face occlusion detection using cascaded convolutional neural network*, (Proc. China Conf. Biometric Recognition., 2016), pp. 720-727.
3. H. Lee, F. Peng, X. Lee, H. Dai and Y. Zhu, *Research on face detection under different lighting*, (IEEE International Conference on Applied System Invention (ICASI), 2018), pp. 1145-1148.

4. T. B. Patel and J. T. Patel, *Occlusion detection and recognizing human face using neural network*, (International
Conference on Intelligent Computing and Control (I2C2), 2017), pp. 1-4.
5. L. Li, X. Feng, Z. Xia, X. Jiang, and A. Hadid, *Face Spoofing Detection with Local Binary Pattern Network*, (Journal of Visual Communication and Image Representation, 2018), vol. 54, pp. 182-192.
6. H. Li, P. He, S. Wang, A. Rocha, X. Jiang and A. C. Kot, *Learning Generalized Deep Feature Representation for Face Anti-Spoofing*, (IEEE Transactions on Information Forensics and Security, 2018), vol. 13, no. 10, pp. 2639-2652.
7. V. Singh, V. Shokeen, and B. Singh, *Face detection by haar cascade classifier with simple and complex backgrounds images using opencv implementation*, (International Journal of Advance Technology in Engineering and Science, 2013), vol. 1, no. 12, pp. 33-38, 2013.
8. E. Bagherian and R. W. O. K. Rahmat, *Facial feature extraction for face recognition: a review*, (International Symposium on Information Technology, 2008), pp. 1-9.
9. S. Balaban, *Deep Learning and face recognition: the state of the art*, (Proc. SPIE 9457, Biometric and Surveillance Technology for Human and Activity Identification, 2015)
10. J. Redmon, S. Divvala, R. Girshick and A. Farhadi, *You Only Look Once: Unified, Real-Time Object Detection*, (*IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, 2016), pp. 779-788.
11. H. Jiang and E. Learned-Miller, *Face Detection with the Faster R-CNN*, (12th IEEE International Conference on Automatic Face & Gesture Recognition (FG 2017), 2017), pp. 650-657.
12. H. P. Nguyen, F. Retraint, F. Morain-Nicolier and A. Delahaies, *Face spoofing attack detection based on the behavior of noises*, (IEEE Global Conference on Signal and Information Processing (GlobalSIP), 2016), pp. 119-123.
13. A. Alotaibi, and A. Mahmood, *Deep face liveness detection based on nonlinear diffusion using convolution neural network*. (Journal of Signal, Image and Video Processing, 2017), pp. 713–720.
14. Y. Kaya, Ö. Faruk Ertuğrul, and R. Tekin, *Two novel local binary pattern descriptors for texture analysis*, (Applied Soft Computing, 2015), vol. 34, pp. 728-735.
15. J. Lu, V. E. Liong and J. Zhou, *Simultaneous Local Binary Feature Learning and Encoding for Homogeneous and Heterogeneous Face Recognition*, (IEEE Transactions on Pattern Analysis and Machine Intelligence, 2018), vol. 40, no. 8, pp. 1979-1993.
16. I. Karakostas, V. Mygdalis, A. Tefas, I. Pitas, *Occlusion detection and drift-avoidance framework for 2D visual object tracking*, (Signal Processing: Image Communication, 2021), Volume 90, pp. 1-13
17. Z. Xu, S. Li and W. Deng, *Learning temporal features using LSTM-CNN architecture for face anti-spoofing*, (3rd IAPR Asian Conference on Pattern Recognition (ACPR), 2015), pp. 141-145.
18. A. Alotaibi, and A. Mahmood, *Deep face liveness detection based on nonlinear diffusion using convolution neural network*. (Journal of Signal, Image and Video Processing, 2017), pp. 713–720.
19. S. Katsigiannis, E. Keramidas and D. Maroulis, *FLBP: Fuzzy Local Binary Patterns", in Local Binary Patterns: New Variants and Applications*, (Studies in Computational Intelligence, Springer, 2014), pp. 149-175.
20. Y. Yuan, J. Chu, L. Leng, *A scale-adaptive object-tracking algorithm with occlusion detection,* (J. Image Video Proc. 2020)
21. J. Määttä, A. Hadid and M. Pietikäinen, *Face spoofing detection from single images using micro-texture analysis*, (International Joint Conference on Biometrics (IJCB), 2011), pp. 1-7
22. I. Chingovska, A. Anjos and S. Marcel, *On the effectiveness of local binary patterns in face anti-spoofing*, (BIOSIG - Proceedings of the International Conference of Biometrics Special Interest Group (BIOSIG), 2012), pp. 1-7.
23. Z. Boulkenafet, J. Komulainen and A. Hadid, *Face Spoofing Detection Using Colour Texture Analysis*, (IEEE Transactions on Information Forensics and Security, 2016), vol. 11, no. 8, pp. 1818-1830.
24. J. Yang, Z. Lei, and S. Z. Li., *Learn convolutional neural network for face anti-spoofing*, (arXiv preprint arXiv:1408.5601, 2014).