Image Quality Improvement based on Face Spoofing Detection using Optimized QDA Method

Mandeep Kaur
Research scholar
Department of IT
GNDEC, Ludhiana

Hanit Karwal
Assistant Professor
Department of IT
GNDEC, Ludhiana

Kulvinder Singh Mann, PhD
Professor
Department of IT
GNDEC, Ludhiana

ABSTRACT
In the last years, the biometric organization like developers, retailers, and researchers have worked on challenging tasks to implement more accurate protection approach against spoofing issues. Spoofing attacks disturb high-security area in the government sectors, IT companies, and communication system. Various faces liveness and anti-spoofing detection methods have proposed, the primary issue still unresolved due to difficulties in searching the features and techniques for spoof intruders. Surveyed the various spoof detection methods to find a forgery face in biometric systems. The existing process has developed to detect the duplicate faces from photos which have been shared through OSM (Online Social Media). In existing color space methods used to extract image contrast and illumination map of the region. It measures the image quality parameter and compared with the background region of the color image. Quadratic Discriminant analysis methods used to detect the spoof image and results achieved 96.5%. Implement novel classification technique to improve the accuracy rate, specificity and sensitivity rate. HOG method is used to extract the feature in the unique format. Feature Selection of the extracted features using PSO and QDA method. In the Optimized QDA method, reasonable feature has been selected with the help of best solution and background region detect. The proposed method is tested with DSO -1 and DSI-1 face photo dataset and achieve the accuracy rate 98.3% and Specificity rate value is 0.9% and compared with the QDA method.

Keywords
Face Spoofing Detection, Particle Swarm Optimization (PSO), OQDA (Optimized Quadratic Discriminant Analysis), Online Social Media, DSO-1 and DSI-1 Dataset.

1. INTRODUCTION
For the recognition and identification of an individual, biometrics play a pivotal role.Biometric process is a trait to detect biometric information of the person. The identification is done by using different traits of an individual. Biometric traits of an individual are the behavioral, physical and biological characteristics carried uniquely by that individual. Biometric systems solely concentrating on human identification have gained significant importance in the present epoch[1]. As it's possible to create an identify one's personality with the help of biometric traits, biometric systems have installed in various fields for security purposes like financial transactions, airport, checking, security services, accessing personal computer and authentication systems [2].

Face recognition systems have been widely utilized in the executive as well as corporate sector for the authentication and identification of an individual. Due to increase in popularity of face recognition systems, there is a high probability of breach allowing an illegitimate user to pretend as an authorized user to gain access and privileges of the authorized person. Face spoofing is usually done by using 2D photographs, moving objects or by some other methods [3].

The biometric traits are presented by a live person or some other source by yielding false proof to gain access to authorized user's privileges, known as spoof detection. Recognition of a live person from non-live traits presented by an intruder is a challenging task. The judgement of the live from the non-live revelation has turned into an issue. Though, face spoofing is a main challenging issue, so it becomes necessary to develop a robust and an efficient method for the detection of the face spoofing [4] [5].

Spoofing attack is a method of the fake approval in which intruders yield a false proof to biometric scheme to achieve identification of any other authorized user.

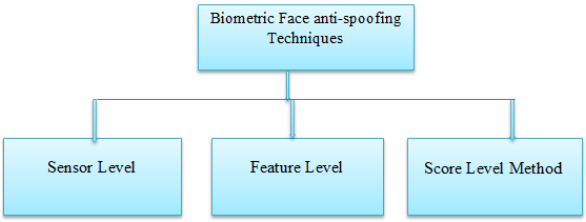

Fig 1. Biometric Face Anti-spoofing techniques

Sensor level based Method is also Known as hardware-based method that includes a specific sensor to detect the features of the face trait. The features are related to the instincts properties of social such as living individuals,signal of the body and nervous system. For instance, blood pressure, pulse rate and brain signal. Feature level Method is also called as software based technique. In this method, extraction of the features from the biometric model where fake and real face traits are distinguished. An interesting feature of the this technique is to perform the functioning of the attained model,but not on biometric trait [10]. This technique is based on the software and hardware approach. Biometric Character tics are detected at the score level to implement fusion synthesis that obstructs the spoofing threats.

Photo Attack is a type of spoofing attacks, intruder yields 2D photographs of the authorized user. These photographs can be taken by intruder using digital camera, mobile phones, tablets or they can be hacked through some social networking sites like Facebook, Twitter, etc [6].

Mask Attack: In three dimensional attacks, intruders create a three-dimensional mask of the actual person which may comprised of silicon, plastic or paper. A 3D mask is created

by using the profundity details of the face to create a replicated version of the face. These profundity details of the face are generally missing in 2D photo attacks [7] [8].

Video attacker takes video of the genuine individual using mobile, tablet or digital cameras.

It has complexity distinguishing color distortions, due to undefined image illumination variations and recapturing process. In this process, main issues or drawback can be avoided in certain cases like as Indoor Access Control Systems as Lighting is always the same at the Biometric Access Point and Enrolment Samples can be image acquired in the same conditions such as authentication[9][10].

In this research proposal, develop an algorithm to detect spoofed face images using HOG feature extraction. Implement Optimized QDA classifier on the proposed technique to classify real or fake images.

Section I define the main overview of face spoofing detection and face spoofing attacks. Section II describes the existing work with the techniques mentioned. III and IV sections elaborate the research proposal and result discussion with comparative analysis. Section V elaborates the conclusion and future work.

2. RELATED WORK

Face spoofing is an attempt to access rights to someone privileges by using photo, videos or a different alternative for an authorized face of a person. Face Spoofing is a fake biometric that is used in an attempt of a biometric sensor. The biometric traits are presented from a live person or some other source is called as the spoof detection. **Jayan, T. J. et al., 2018 [11]** proposed a research on the fast and robust algorithm for the detection of the fake faces from the images taken from the cameras that was also shared with the social media. The face segments were extracted through different color spaces and estimates the map of the region. Moreover, the image quality parameters of the segments and background regions were compared in this paper. The feature vectors were generated using the image quality parameters. In this research, Quadratic Discriminant Analyser (QDA) classifier was used for the detection of the fake images.**Patel, K., Han, H and Jain, A. K. et al., 2016[12]** addressed on the issue of the face spoofing recognition in contract to picture and moving object on the basis of the threats, image noises, pattern recognition. They established the spoof attack dataset that consists more than 1000 classes. Published and repetition threat that was caught using far and nearer cameras. They analyzed the inference of the noise and threats, utilizing strength models which are RGB and grayscale image, an area of the face, descriptive features. They developed a reliable spoof detective scheme using machine devices. Experimental approach was done on dataset such as CASIA and MSU-MFSD dataset through which spoof detection was reliable for test approaches. **Fourati, E. et al., 2017[13]** demonstrates the anti-spoofing solution for the image quality assessment to discriminate the real and the fake images. The image quality assessment was based on the extraction of the frames and low complexity classifiers. The image quality countermeasures are the face spoofing attacks. In this research, the main focus on the face spoofing attacks using photos, videos and 3d masks images. The liveness face was detected using the presentation attack detection based on the image quality assessment. **Li, H., Wang et al., 2016[14]** proposed research on the image quality regression framework to overcome the issues of face spoofing detection. Firstly, the clusters of the same (camera model feature) and different quality classifiers based were extracted through the image quality assessment. The regression function maps from the features of the image quality assessment. The classification was used the classifiers and, the prediction was done for the verification of the face. In this research, the experiments were done using single class classifiers. **Galbally, J et al., 2014[15]** presented a novel face detection method and various fraud attempts used in multi-biometric biometric systems. The main goal of this research was to increase the security of the biometric system by adding the live-ness image assessment. The main problems may be attacks or error metrics due to the mismatch of the images. The real time applications use the 25 general images features for the extraction of an image and comparing that with other samples. In this research, the experimental results were compared using state of the art approach and real quality biometric systems. In this research, the software based method was utilized for the detection of the fraud attempts to images and various types of the attacks.

3. RESEARCH METHODOLOGY

In this section, described about the problem which is found in the existing work. Research objective descriptions about the research work with proposed methods and parameters. Research Methodology described about the proposal in stepwise. All steps are elaborate in section 2.

Face identification System is secure spoofing attacker which is verified as an original limitation. FSA (Face Spoofing Attacks) is considered by screening a DI (Digital Image) acquisition of measuring subject in front of the sensor devices. Extra re-production stages design, color interference between real and fake facial image. The advance method in face verification use to un-lock smart mobile phone, but the attackers can easily attack earlier networks through replay attack, Photo Display, 3D-Mask etc. It is essential to carry out a new technique for FSD to give more security.

In Proposed research work, search the dataset from the UCI Machine Learning Repository site. Download and Train the dataset according to the category Real and Fake Facial Images. Create a knowledge based dataset with the help of Optimized Quadratic Discriminant Analysis. Upload the image from the Training folder. In Pre-processing phase has applied the rgb2 grayscale command to convert the color image to grayscale format. Gray Scale Conversion used to reduce the dimensionality of the uploaded image.Apply the color space technique which is HSV and lab methods. HSV method is a representation of the RGB color model. In this model describes the different color mix together with saturation dimensional approaching the mixture of those paints with changing amounts of white and black color. The YCBCR color structure is worldwide used for digital images. In this image pattern, Luminance data are stored as a single (Y) and chromatic data is stored as 2 color difference components, Cb defines the difference between the blue and reference value, cr defines the difference between the R-component and a ref value. Smooth phase has checked the noise in the uploading image. Noise attack means to degrade the input image. Then noise level verification has implemented a smooth or filtration method to calculate the smooth image. Implement a HOG method which is a feature extraction method.

Hybrid method has implemented using Particle Swarm Optimization and Quadratic Discriminant Analyser. In the optimization phase, select the features based on the extracted features and classify the spoofing face images. It classifies the feature set based on discriminant analysis and calculates the

near distance,identifies the real and fake face images.

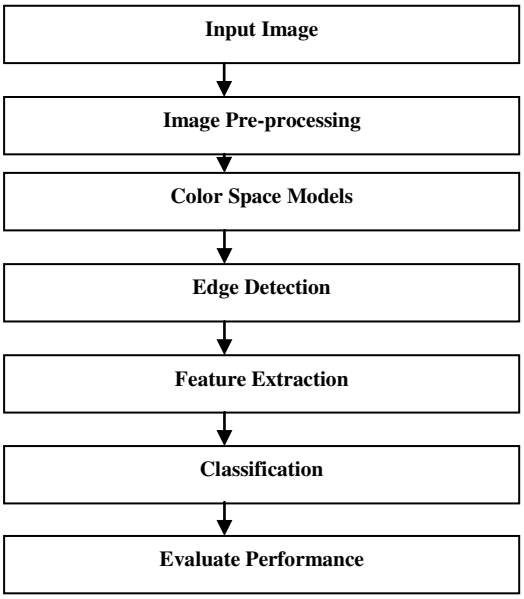

Fig 2. Proposed Flow Chart

It evaluates the performance analysis with the help of accuracy rate, error rate and compared with the existing methods.

4. RESULT ANALYSIS

In this section, described that the dataset description in face spoofing images in DSO-1 and DSI – 1 dataset.

4.1 DSO-1 Dataset

DSO- 1 is a collection of 200 indoor and outdoor facial images with an image resolution of 2048 * 1536 image pixels. In this set of facial images, 100 is real face that has no-adjustments and 100 are fake facial image. Fake images were created by adding 1or more individual in a source image. [16].

4.2 DSI-1 Dataset

DSI-1 defined 50 face images (25 real face image and 25 fake face images) downloaded from different websites on the internet with dissimilar resolutions. Real Images downloaded from FLICKR and DOCTORED facial images were collected from different websites like as 1000 WORTH, BENETTON group 2011 and PLANET HILTRON etc. [16]

Proposed Method has described the result analysis with optimized quadratic discriminant analysis. It trains the multiple data sets from the data set folder. Upload the images from the training folder. It applied the pre-processing image phase, feature extraction method to extract the unique properties and classify the optimized QDA method analysis and spoof the facial images and detect the real and fake image. Testing Section is basically analyzing of the test image as compared with the training section or a database.

It figure 3 shows the upload test image from the test image. It converts the color image to a grayscale image. It reduces the dimensions of the uploaded image. Upload the 3D image and rgb2gray command implemented and extract the image Black and white format and 2D format.

(i) (ii)

Fig 3. (i) Real Image and (ii) Grayscale Image

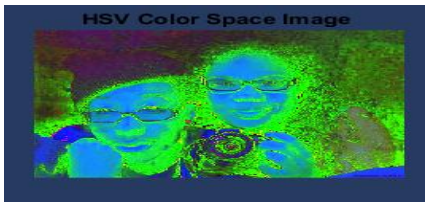

Fig 4 HSV Color Space Image

The above figure 4 shows the HSV color space image model, when color selection is based on the paint HSV model represents a red, green and blue components.It color contributes to high configuration and quality graphics. The Selection HSV color model starts with preference one of the available hues and then modifying shade and color or brightness values.

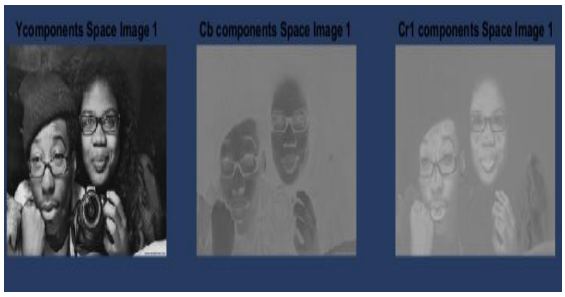

Fig 5. Color Space Model (Ycbcr) Image

Above figure showed that the Ycbr color model is based on color components. It is widely used for digital video. This color model format (Luminance) is saved as a single color (Red) component and chromatic information is saved as two-different components CB and CR. Cb that defines the difference between the blue color component and a reference value. Cr defines the difference between the red color component and a ref value.

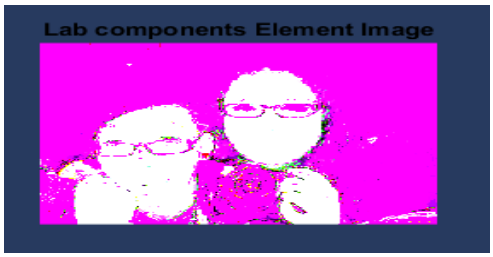

Fig 6. Lab Components Element Image

The above figure shows that the lab model which implements to fetch the image color components red, green and blue one at a time. It is the most representative of color components not normally used. It is normally converted to minimum accuracy color spaces like as RGB (Red,Green and Blue) and CYMK is a process of four color components.

Fig 7. Noisy and Smooth Image

The above figure shows the distorted images using Salt and Pepper Noise and Filter the distorted data with median two-dimensional transformation methods.

Fig 8. Edge Image

Above figure defined that the edge detection use Sobel operator. It generates a picture emphasizing edges,calculating an approx... of image gradient and integer-valued filters.

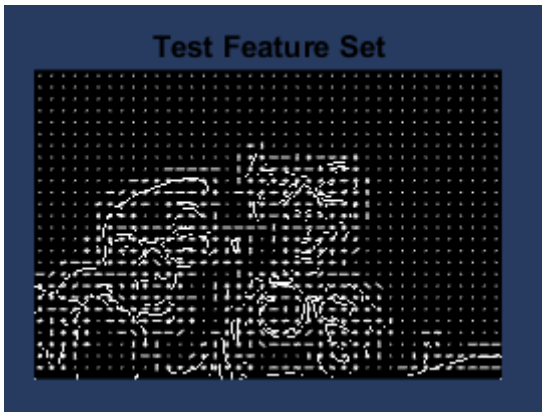

Fig. 9 Feature Set (HoG)

Above figure shows the feature extracted image using HOG (Histogram Oriented Gradient) method. It is calculated for an entire picture by separating the image into small cells and summing up the gradients over every image pixel within cell in an image. It's used to verify the image features.

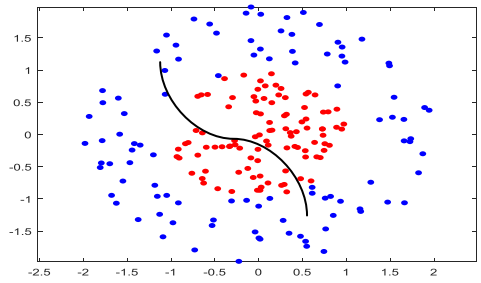

Fig. 10 Classification With OQDA

The above figure shows the Optimization phase with the QDA classification method. It is initialized with a collection of random features and then finds for the best optimal by updating generations. The individual round feature is updated by following 2 best values. Initial is the best fitness solution, it has attained so far. Fitness values is stored public best fit value. Particle Swarm Optimizer is the best value attained so far by any feature in the population set. Best Value is a Global best and called Gbest. The QDA classifier method are attractive because they have nearest solutions that can be identified the fake and real image.

Fig. 11 Spoof Image Detection

Above message box shows that the spoof detects face based on training and testing features. If testing feature set compared with the existing training feature set nearest value considered Then, calculate the distance and detect the spoof image or not.

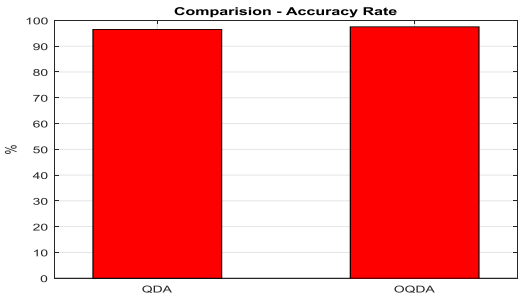

Fig 12. Comparison – Accuracy Rate (%)

The above figure demonstrates the comparison among OQDA and QDA. Both the algorithms are compared that determines OQDA with maximum accuracy rate as compared with the existing QDA algorithm.

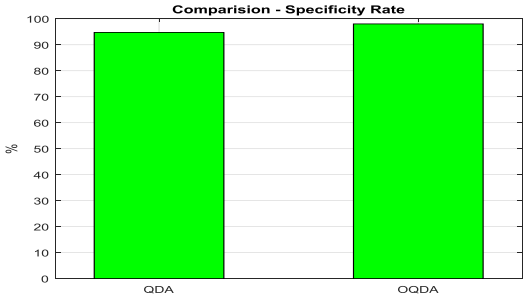

Fig 13. Comparison- Specificity Rate(%)

The above figure demonstrates the comparison between OQDA and QDA. Both the algorithms are compared that determines OQDA with maximum specificity rate.

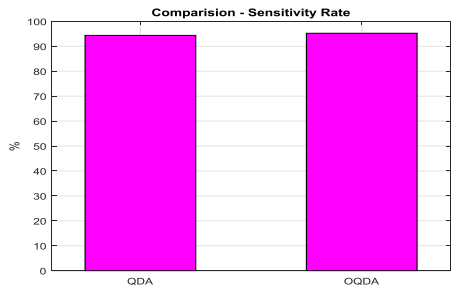

Fig 14. Comparison- Sensitivity Rate (%)

The above figure demonstrates the comparison between OQDA and QDA. Both the algorithms are compared that determines OQDA with improved sensitivity rate.

Table 1:- Proposed Parameters

Param -eters	Accu -racy	Speci ficity	Sensit -ivity	MSE	FAR	FRR
Values	97.5	98	95.2	0.049	0.002	0.0048

Table 2. Comparison Analysis

Parameters	Proposed (OQDA)	Existing (QDA)
Accuracy Rate	97.5	96.5
Specificity	98	94.7
Sensitivity	95.2	94.4

Table 1 and 2 described that the performance analyses with proposed work and existing work. In Table 1 defines the performance metrics like accuracy, specificity, sensitivity, MSE, FAR and FRR. Table 2 defines the comparison between proposed and existing work with Accuracy Rate, Specificity and Sensitivity Rate.

5. CONCLUSION AND FUTURE SCOPE

Conclusion of the proposed method is used to resolve the issues analyse color and texture. Analyse, how well different color model implemented which is HSV, YCBCR and LAB can be used for elaborating the central difference in the color and texture between real and fake faces and if given complementary representations. An efficiency of the various face color, texture representations was analysed by extracting the local and global features from the face image in the different color spaces. In research work , DSO-1 and DSI-1 online social face datasets has been used. In the knowledge-based train the 125 images in real faces and 125 fake images. Overall 250 images used for the training section and 60 images used for the testing section.Proposed method depends on the optimized QDA classifier. Propose method depends on the selected unique properties and extract features from the face images. An edge operator is used to calculate the face regions based on inner and outer area. HOG methods are used for the feature extraction approach to extract the unique features. The particle Swarm Optimization method used to select the feature based on the fitness function. It is fetching the best solution in the extracted feature set (1,0) value. QDA method implemented to detect and classify the training and testing feature set and evaluates the nearest distance. It is compared with nearest feature set and feature comparison true, then evaluate the performance metrics like accuracy rate value is 97.5 %, specificity value is 98 %, and sensitivity value is 95.2% and compared with the existing work accuracy 96.5%.

In future, face spoofing detection can be enhanced with deep learning and ant lion optimization techniques. It will work with HAAR wavelet transformation technique used to filter the image and select the extracted global feature set for spoof attack detection in the online social media face datasets. These methods will improve the processing time, reduce the complexity to enhance the overall performance of the detection system.

6. REFERENCES

[1] Jain, A. K., Hong, L and Kulkarni, Y. (1999, March), "A multimodal biometric system using fingerprint, face and speech", In 2nd Int'l Conf. AVBPA ,Vol. 10.

[2] Gamboa, H and Fred, A. (2004, August), " A behavioral biometric system based on human-computer interaction", In Biometric Technology for Human Identification , International Society for Optics and Photonics , Vol. 5404, pp. 381-392.

[3] Määttä, J., Hadid, A. and Pietikäinen, M. (2011, October), " Face spoofing detection from single images using micro-texture analysis", In 2011 international joint conference on Biometrics (IJCB) ,pp. 1-7, IEEE.

[4] Bharadwaj, S., Dhamecha, T. I., Vatsa, M and Singh, R. (2013), " Computationally efficient face spoofing detection with motion magnification", In Proceedings of the IEEE conference on computer vision and pattern recognition workshops ,vol 2(3), pp. 105-110.

[5] Chingovska, I., Anjos, A and Marcel, S. (2012, September), " On the effectiveness of local binary patterns in face anti-spoofing" In 2012 BIOSIG-proceedings of the international conference of biometrics special interest group (BIOSIG) ,pp. 1-7, IEEE.

[6] Maini, R. and Aggarwal, H. (2008), " Study and comparison of various image edge detection techniques", International journal of image processing (IJIP), vol.3(1).

[7] Han, H., Shan, S., Chen, X. and Gao, W. (2013), " A comparative study on illumination preprocessing in face recognition. Pattern Recognition", vol.46(6), pp. 1691-1699.

[8] Chaves-González, J. M., Vega-Rodríguez, M. A., Gómez-Pulido, J. A and Sánchez-Pérez, J. M. (2010)., " Detecting skin in face recognition systems: A colour spaces study", Digital Signal Processing, vol.20(3), pp. 806-823.

[9] Parveen, S., Ahmad, S. M. S., Hanafi, M., & Adnan, W. A. W. (2015). Face anti-spoofing methods. Current science, 1491-1500.

[10] Galbally, J., Marcel, S., & Fierrez, J. (2014). Biometric antispoofing methods: A survey in face recognition. IEEE Access, 2, 1530-1552.

[11] Jayan, T. J and Aneesh, R. P. (2018, July), " Image Quality Measures Based Face Spoofing Detection Algorithm for Online Social Media", In 2018 International CET Conference on Control, Communication, and Computing (IC4) , pp. 245-249, IEEE.

[12] Patel, K., Han, H and Jain, A. K. (2016), "Secure face unlock: Spoof detection on smartphones", IEEE Transactions on Information Forensics and Security, vol 11(10),pp. 2268-2283.

[13] Fourati, E., Elloumi, W and Chetouani, A. (2017, August), " Face anti-spoofing with image quality assessment", In 2017 2nd International Conference on Bio-engineering for Smart Technologies (BioSMART) ,pp. 1-4, IEEE.

[14] Li, H., Wang, S and Kot, A. C. (2016, December), " Face spoofing detection with image quality regression",

In 2016 Sixth International Conference on Image Processing Theory, Tools and Applications (IPTA),vol 2(3), pp. 1-6, IEEE.

[15] Galbally, J., Marcel, S. and Fierrez, J. (2014), " Image quality assessment for fake biometric detection: Application to iris, fingerprint, and face recognition", IEEE transactions on image processing, vol 23(2),pp. 710-724.

[16] Dalal, N and Triggs, B. (2005, June). Histograms of oriented gradients for human detection.

[17] Dalal, N., Triggs, B and Schmid, C. (2006, May). Human detection using oriented histograms of flow and appearance. In European conference on computer vision (pp. 428-441). Springer, Berlin, Heidelberg.

[18] Zhu, Q., Yeh, M. C., Cheng, K. T and Avidan, S. (2006, June). Fast human detection using a cascade of histograms of oriented gradients. In 2006 IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR'06) (Vol. 2, pp. 1491-1498). IEEE.

[19] KennedyJ.(2010).Particleswaroptimization. Encyclopedi a of machine learning, pp. 760-766.

[20] Shi, Y and Eberhart, R. C. (1999, July). Empirical study of particle swarm optimization. In Proceedings of the 1999 Congress on Evolutionary Computation-CEC99 (Cat. No. 99TH8406) (Vol. 3, pp. 1945-1950). IEEE.

[21] De Marsico, M., Nappi, M., Riccio, D., & Dugelay, J. L. (2012, March). Moving face spoofing detection via 3D projective invariants. In 2012 5th IAPR International Conference on Biometrics (ICB) (pp. 73-78). IEEE.

[22] Siddiqui, T. A., Bharadwaj, S., Dhamecha, T. I., Agarwal, A., Vatsa, M., Singh, R., & Ratha, N. (2016, December). Face anti-spoofing with multifeature videolet aggregation. In 2016 23rd International Conference on Pattern Recognition (ICPR)(pp. 1035-1040). IEEE.

Hadid, A., Evans, N., Marcel, S., & Fierrez, J. (2015). Biometrics systems under spoofing attack: an evaluation methodology and lessons learned. IEEE Signal Processing Magazine, 32(5), 20-30.

[23] Raval, P., R.R. Sedamkar., & Kulkarni, S. K. (2017). Face Spoofing Detection Using Image Distortion Features. International Journal of Innovative Research in Science,Engineering and Technology, 6(9), 746-761

[24] Zhang, Y., Dubey, R. K., Hua, G., & Thing, V. L. (2018, October). Face Spoofing Video Detection Using Spatio-Temporal Statistical Binary Pattern. In TENCON 2018-2018 IEEE Region 10 Conference (pp. 0309-0314). IEEE.

[25] Aziz, A. Z. A., & Wei, H. (2018, August). Polarization Imaging for Face Spoofing Detection: Identification of Black Ethnical Group. In 2018 International Conference on Computational Approach in Smart Systems Design and Applications (ICASSDA) (pp. 1-6). IEEE.

[26] [https://recodbr.wordpress.com/code-n-data/#dso1_dsi1.