Spoofed Video Detection Using Histogram of Oriented Gradients

Aparna Maurya
Information and Communication Technology
Gautam Buddha University
Greater Noida
14pit076@gbu.ac.in

Sandhya Tarar
Information and Communication Technology
Gautam Buddha University
Greater Noida
sandhya@gbu.ac.in

ABSTRACT
Nowadays face recognition system usage is increasing day by day to provide better security mechanism. But with the face recognition system, there are some spoofing methods also attached using which the system can be befooled easily. These attacks are simple and easy as they cost less and the images can also be easily retrieved from social sites; therefore there are high chances of them to be successful. . Still there is a scarcity of a productive anti-spoofing algorithm to resolve this issue.

The aim of this paper is to present a method which can be used for identification of the spoof. A method is proposed which takes the live video streaming input from the user and perform Liveness detection on the user based on the eye blinking movement and for face feature extraction Histogram of Oriented Gradient (HOG) is used as it proves to be an effective feature descriptor in the face recognition. Two classifiers k Nearest Neighbour (kNN) and Neural Network (NN) are used for the classification purpose. The work is performed on the self created Database and implementation is performed in MATLAB for better understanding, visualization and programming. The performance results of the kNN and NN classifier are compared and finally it is concluded that which classifier outperforms the other one.

Keywords
face recognition; spoofing; liveness detection; HOG; kNN classifier; NN classifier

1. INTRODUCTION
Face recognition is the fastest and least encroaching biometric technology. It uses the human face for identification, as human face plays a key role in our social interaction. Face recognition is better than fingerprint, palm print and iris recognition as the person does not have direct contact in the process and no additional sensor is required in the process. The process of identification does not demand the person for his interaction with the recognition system. The vital issues that are recently tackled in the technological development route are the resilience of this quickly rising technology to attacks, mainly like spoofing. In present- day standards, Spoofing is mentioned by the term presentation attack. Spoofing the system means be-fooling the biometric system by pretending to be a genuine user, but actually being an illegitimate user by using certain version of original biological trait [1].

It is comparatively simpler to retrieve an individual's face image or video as it can be simply taken by a digital camera or it can be downloaded and printed from social media than the other biological traits such as fingerprint, palm print, and iris. Additionally, the launching cost of a face spoof attack like print photo attack, display photo attack, or replayed video attack is comparatively lower than the other attacks. Määtta et al. [2] stated that the Windows XP and Vista laptops of Lenovo, Asus and Toshiba can be easily spoofed. These laptops scan the faces of users for authentication. It is demonstrated in [2] how to easily be-fool the systems "Lenovo's Veriface III", "Asus' SmartLogon V1.0.0005", and "Toshiba's Face Recognition 2.0.2.32" by imposturing facial images of the authentic user.

In recent years popularity of spoofing is increasing, but the anti-spoofing methods are limited. Many methods have been formulated to detect the photograph spoofing. The main focus is on the motion analysis [3-5] and liveliness detection for lip movement [6] and for eye blinking [7] in the existing techniques. There are certain techniques for texture analysis, on the basis of frequency spectrum of the live face [8]. When 3D Spoof attacks are introduced i.e. 3D Mask then many techniques of 2D Spoof attack are of no use. Kollreider et al. shows that a face recognition system depending on face liveliness detection i.e. blinking of the eyes and movement of lips can be attacked by the fake user by using photographic masks wrapped on his face and the regions around the eyes and mouth are cutout [9].

2. ISSUES IN FACE RECOGNITION SYSTEM
There are various issues that are faced in the face recognition system. Some of the issues are discussed are discussed below:

2.1 Security
One of the major problems that are identified from the past years is the problem of Security. For security reasons there are various solutions that are provided from the ID type passwords; which sometimes become too long and complicated to be remembered to the security access control systems based on the biometric modalities like fingerprint, iris, face, palm-print, voice recognition, digital signature etc.
Face Recognition Systems are threatened by the face spoofing attacks with include print attack, display attack or video attack

VisionNet'16, September21-24,2016,Jaipur,India
©2016ACM.ISBN978-1-4503-4301-5/16/09$15.00
DOI: http://dx.doi.org/10.1145/2983402.2983408

also known as replay attack. This draws our concern towards the Security of the system from the possible face spoof attacks.

2.2 Face Detection

As there are millions of faces present in this world, so it becomes tough for the machine to detect the face correctly every time. Face detection is the first step to be followed in face recognition. It is most important that this step should be properly executed, so that the subject is correctly recognized and accurately classified. For this purpose there are various techniques which are based on the features or based on the appearance.

2.3 Liveness Detection

Another problem identified is the liveness detection of the subject who is present in front of the camera. Liveness means that the subject is in motion or not. It checks whether the person have blinking eyes or not or they have movement or not. Basically, it checks the blinking eye, lip movement, heartbeat etc. If liveness of the subject is well identified then there are fewer chances of the photo attacks on the Face Recognition System.

3. ATTACKS ON FACE RECOGNITION SYSTEM

Some of the spoofing attacks that are possible on the system are as follows:

- Photo Attack
- Video Attack
- Mask Attack

In the above discussed spoofing attacks can be again classified into two categories 2D Spoofing Attack and 3D Spoofing Attack. Attacks which are performed using the photograph and videos are the 2D spoofing attacks and the attacks performed using the masks comes under the 3D Spoofing Attack. The Spoofing Attacks have been discussed below:

3.1 Photo Attack

It is a 2D Spoofing Attack which can also called as the photograph or print attack. In this type of attack the illegitimate user presents the face image or we can say a photograph of the authentic user is presented infront of the recognition system to be-fool it. The genuine user's photograph may have been retrieved from some social networking site where he has uploaded the photographs and can also take the photograph using digital camera.

3.2 Video Attack

Sometimes video attacks are also names as replay attacks. This is more critical type of attack than the photo attacks as it becomes more difficult to differentiate between the genuine and the fake user as dynamics is also traced with the texture of face. In this type, the video of the authentic user is replayed using a digital device instead of using the static image [10].

3.3 Mask Attack

3D Spoofing Attack is considerably new as compared to the above mentioned 2D Spoofing Attacks that are photograph and video In this type of attack the spoofing medium is the three dimensional mask of the authentic user which increases the difficulty to detect the attack. Nowadays it is becoming easier and possible to self manufacture a mask with the new generation of low cost three-dimensional capturing sensors, etc and the decrease in price of three dimensional printing devices [11].

4. LITERATURE REVIEW

There is a lot of work done in the area of face recognition in the past years. There are various face recognition techniques which work on the different features of the face. Some of the techniques like Eigenface [12], Independent Component Analysis (ICA) [13], Linear Discriminant Analysis (LDA) [14], Evolutionary Pursuit (EP) [15], etc have been discussed in the paper by *Maurya and Tarar*. The paper consists of the various techniques which are used for face detection and work on different features of the face [16].

The work of automatically distinguishing whether the given biometric trait arises from the authorized user or is from another source is referred to as various terms by *Marcel et al* like spoof detection, anti- spoofing and presentation attack detection [17]. Liveliness detection is also act as a synonym of the Spoof detection in many areas, but generally it can be referred to some more constricted problems of sensing vitality signs such as heartbeat or eye blinking. In this work the term used is anti-spoofing method.

Jain et al have proposed an anti-spoofing algorithm which uses Image Distortion Analysis (IDA). IDA consists of features which are separated from the image to create the 121-dimensional feature vector; these features are blurriness, chromatic moment, specular reflection and color diversity and fed to a form of SVM classifier which consists of multiple SVM classifiers [18]. The algorithm supported the image quality analysis based methods [19]. SVM is a two class classifier which distinguishes the class of the image. Experimental results are performed on the two freely available face spoof databases which are Idiap REPLAY-ATTACK and CASIA FASD and on the collected database by author which is MSU MFSD to prove that the approach proposed performs better over the other methods in anti-spoof detection [18]. Because of the increasing popularity and increasing use of face recognition for authentication purpose, it has drawn in a remarkable curiosity from the last few years. TABULA RASA which is a major focuses of the FP7 EU funded project [20], is "trusted biometrics under spoofing attacks".

In another work Bharadwaj et al presents a new approach which uses Euclerian motion magnification for the enhancement of facial features usually shown by the subjects in face videos for spoofing detection [21]. Two kinds of the feature extraction algorithms; a form of LBP and HOOF descriptor are used for improved performance and for motion estimation respectively are proposed by the authors. Experiment is performed on the Print Attack and Replay Attack Spoofing databases. A near perfect half total error is provided by the HOOF descriptor of 0% and 1.25% respective databases.

New challenges are encountered in video surveillance (unconstrained scenarios) and in driver's license and passport photos (constrained scenarios) because of the variations in image resolution, facial pose, occlusion, ambient illumination, expression and background clutter. Rowden et al [22] formed a single candidate list for the subject by using the whole range of media as a research. Rowden et al have shown that approach proposed rises the likelihood of properly distinguishing the subject by using of many fusion schemes, 3-D face models, and

quality measures integration for fusion and video frame selection [22].

Erdogmus and Marcel inspect the spoofing likely of subjectspecific 3D facial masks for 2D face recognition. In addition [23] analyze Local Binary Patterns based countermeasures acquired by Kinect using both color and depth data. First publically available 3D Mask Attack Database (3DMAD) is used for this purpose, taped with a low-cost depth camera. Experiments on 3DMAD prove that easily possible facial masks can pose a dangerous threat to 2D face recognition systems and LBP is a strong weapon to get rid of it [23].

It is broadly acknowledged that biometric systems are unprotected to spoofing, also known as imposture. While vulnerabilities and countermeasures for other biometric modalities have been widely studied, e.g. face verification, speaker verification systems remain vulnerable. Evans et al have represented some proper vulnerabilities deliberated in the literature and a precise survey of recent work to build up spoofing countermeasures [24].

Kollreider et al have presented a face detection technique which includes mouth localization and each frame is processed in proper duration. To confirm liveness, motion analysis is exploited [25]. Quangles are designed for illumination invariance excluding the condition of preprocessing by utilizing both the gradient and double angle direction and by ignoring the magnitude of the gradient. In a quantized feature space boosting techniques are applied. Scale invariance is implemented through the use of an image scale pyramid. Kollreider et al discussed that when calculating motion, the liveness verification mechanism as postulations for which an evidential measure of calculation is forbidden. Databases used are the YALE database and the CMU-MIT frontal face database and the results are witnessed on the same and also on liveness verification mechanism [25].

Face biometrics is essential in the areas where user authentication is a very essential measure to protect the information from the attackers. It is simple to use, natural, and little human encroaching. Freitas Pereira et al have discussed in their work that how good the face anti-spoofing measures which already exists can perform in a more real time environment. Experiments are performed on the two publically present video databases which are Idiap Replay Attack Database and CASIA Face Anti-Spoofing Database. They exhibit low-level generalization and possible database convergent in the calculated measures. To spread and trade with the variety of attacks in a real world scenario [26] two strategies are introduces (inter-test and intra-test protocol) that show promising results.

5. PROPOSED METHOD

A solution for the listed problems in this paper previously which are faced in the face recognition system is given in this section. The attack which is focused is the 2D attack which is photo attack. It does not work for the 3D attack which is mask attack. Live video streaming input is taken from the user and further analysis is performed on the images taken during the live video streaming.

Liveness detection is performed by analyzing the eye blinking movement of the user. Mapping is performed using the standard information provided in the OpenCV library. HOG is used for feature extraction as it proves to be an effective feature descriptor in face recognition [27].

5.1 Algorithm

Step 1*:* Input file: Video
Live video streaming input is taken directly from the subject using the webcam.

Step 2: Liveness Detection: using the eye blinking movement.
Liveness detection is performed to check whether the subject is live or some kind of spoof is performed.

Step 3: Preprocessing the data i.e. changing to gray scale, cropping, dynamic threshold, magnitude, resize, Haar face features extraction and mapping.
a) Changed from RBG to gray scale using MATLAB function.
b) Cropping and Mapping of the images are performed based on the standards set in OpenCV and Haar face features are also extracted.
c) Image magnitude is saved in preprocessing and based on this magnitude a dynamic threshold is set automatically.

Step 4: Feature extraction and selection: HOG features
Feature extraction and selection is performed using HOG algorithm.

Step 5: Classifier used: kNN Classifier and NN Classifier.

5.2 Methodology

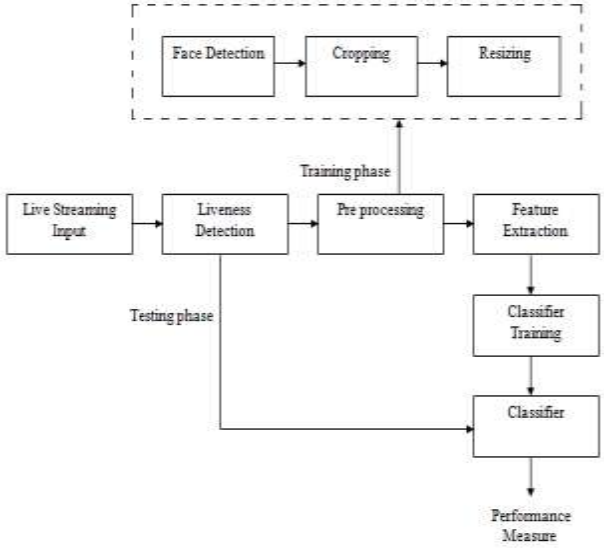

Figure 1: Architecture of the Anti-spoofing system.

The above Figure 1 components have been elaborated in the previous section. This flow of the system is followed by both the classifiers.

6. IMPLEMENTATION

The implementation of this research is performed in the MATLAB R2015a and OpenCV library is also used. The dataset used here is the Self created Database which consists of 4 groups and each group contain 50 samples of frontal face images which are captured through webcam of the laptop. A feature matrix of 200X4356 is created after the training of the images.

Figure 2 shows the samples from the different group of images. Each group is having a name Deeksha, Archie, Aparna and Ankita

respectively. The implementation is shown on one of the subject in the database.

Figure 2: Sample from each group of images.

Firstly the code is executed and the GUI appears on the screen having a button "Start Camera". When the button is clicked a popup message comes "Show your face and click OK". After clicking on Ok button a video preview appear on screen which takes the live video streaming input from the user. Figure 3, Figure 4 and Figure 5 shows the step of live video streaming input taken from user. The face is detected from the preview and the Liveness detection on the basis of the eye blinking movement is performed. Eyes open means 1 and eyes closed means 0. Twenty images are clicked and saved and the absolute difference is calculated. If the unique values in the images is either 0 or 1 then the spoof is detected else if the unique value is {0, 1} means there is eye blinking movement and flow of control moves forward to the next step. Figure 6 and Figure 7 shows the steps in liveness detection.

After liveness detection, preprocessing takes place where the face is detected from the original image and then face is cropped, image is resized, dynamic threshold allocation is done, RBG to gray scale conversion of image is performed, magnitude and Haar features are collected from the image. Figure 8 shows the image after the preprocessing step. Then the features extraction is performed on the image and HOG features are extracted from the cropped image. Then this feature vector is fed to the classifiers for the classification. Figure 9 shows that the feature value is saved in a variable c1 which is a 1X1 matrix. Then the comparison of features is performed and on the basis of that classification is done. If the feature matches with any of the feature group then the user with the group name pops up which shows the name of the user. Figure 10 shows the output after the comparison of the features. If the user is not present in the database then a popup comes which says that the "Unknown Subject Detected". Figure 11 shows the unknown user who is detected.

Figure 3: Figure showing the initial GUI of the system.

Figure 4: Popup that appears on the screen.

Figure 5: Live video streaming of the user.

(a) (b)

Figure 6: Two random images from live streaming (a) with eyes closed and (b) with open eyes.

Figure 7: Figure shows the Spoof detection in the system.

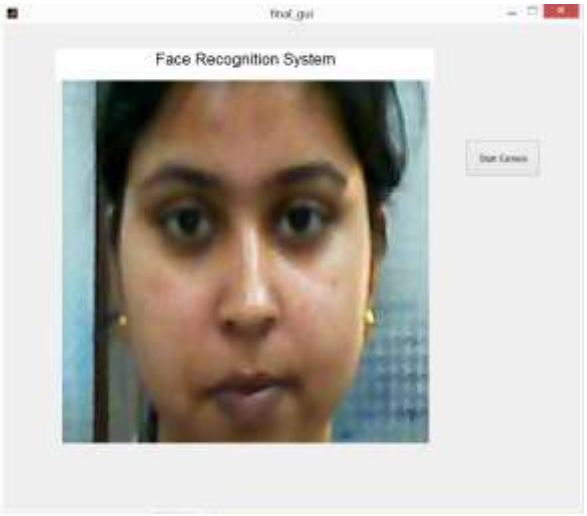

Figure 8: Face image after the preprocessing step.

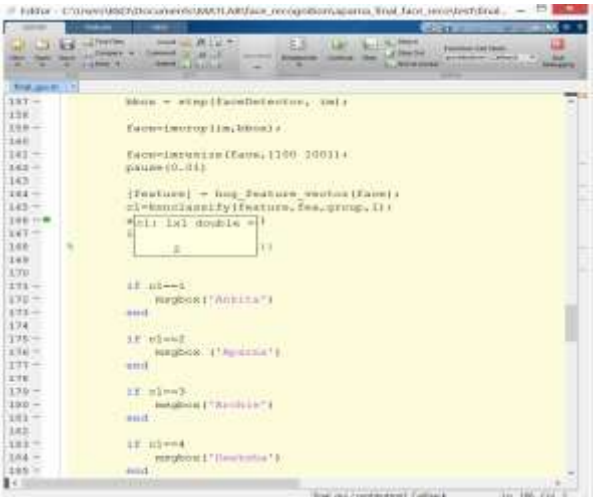

Figure 9: Figure shows the value of the variable c1.

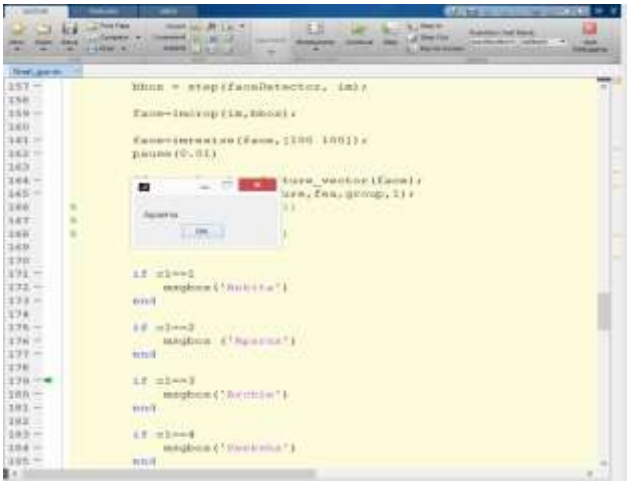

Figure 10: Figure shows the output after the comparison of features.

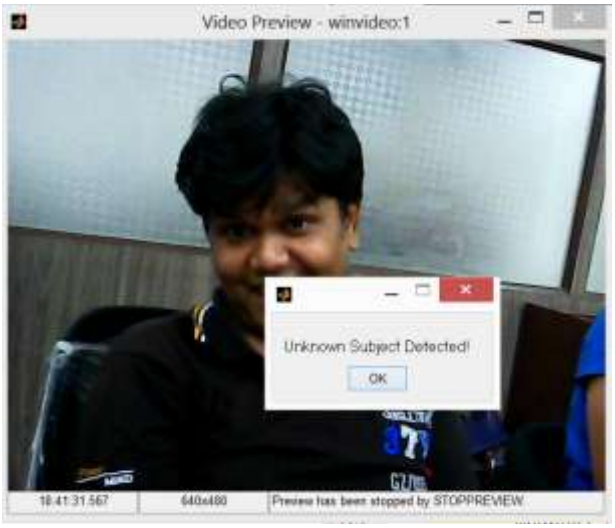

Figure 11: Figure shows the unknown subject is detected.

7. RESULT ANALYSIS

The results of the two classifiers kNN and NN Classifier are compared and seen that which one of them performs better. Classification accuracy of kNN classifier is 96.77% and classification accuracy of the NN classifier is 99.4%. This means that NN classifier performs better than kNN on the database. Graphs generated from the NN classifiers are shown below:

Figure 12 state that how efficiently the machine is performing on the basis of the training. In this graph we try to find the Best Validation Performance which is 0.06008 at the epoch 30. It is represented by the green dotted line (------).

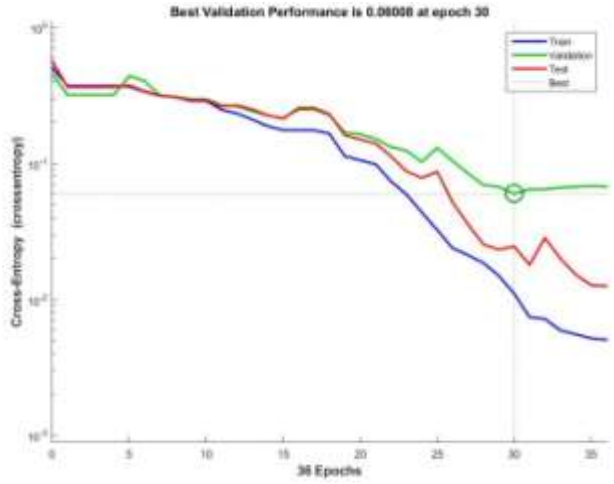

Figure 12: Graph shows the performance of NN classifier.

In Figure 13, gradient function is used to find the gradient with epoch. After the observation it is found that the best value of the gradient is at the epoch 36 which is 0.012232. In Validation fail graph, validation fail is plotted with respect to the number of epoch. By the validation testing the learning efficiency during the training time is identified. In the graph we can see that at epoch 36 the validation check is 6.

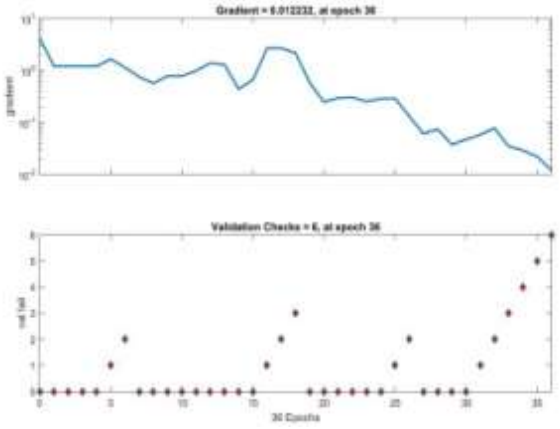

Figure 13: Graphical representation of Gradient and Validation fail.

In Figure 14, ROC (Receiver Operating Characteristic) space, x-axis specifies the False Positive Rate (FPR) and y-axis specifies the True Positive Rate (TPR). The number of negative samples that are uncategorized as positive samples are determined by FPR. The number of positive samples that are labeled right means categorized as positive samples are determined by TPR. The graph shows that the closer the values of the curve follow the left-hand side of the ROC graph, the classification is performed more accurately and the nearer the curve follows to the 45-degree diagonal of the ROC graph, the classification is performed less accurately. In our case the curve is to the left-hand border which means that we have better classification accuracy.

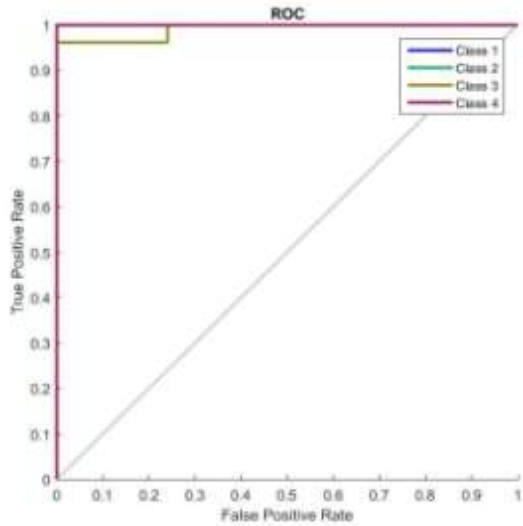

Figure 14: ROC graphical representation of True Positive Rate and False Positive Rate.

Figure 15 shows the confusion matrix whose "green" cells represent the correct answers, "red" cells represent the incorrect answers and the "blue" cell represents the sum of all the correct answers. The summation of all the True Positive Rates (TPRs) is written in the blue cell of the confusion matrix which tells about the accuracy of the system.

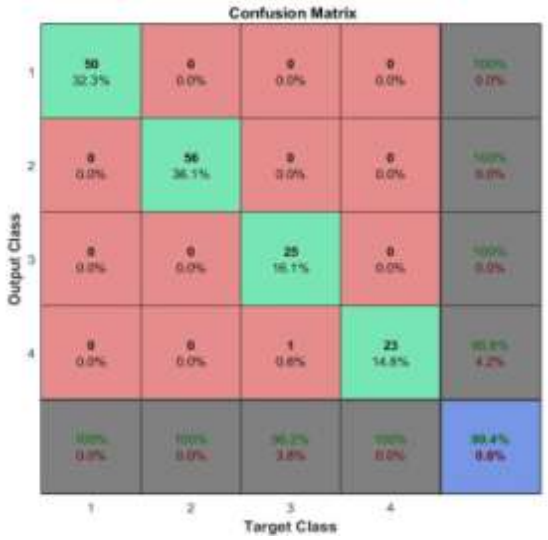

Figure 15: Confusion Matrix of the classes.

Table 1. Classification accuracy of the classifiers.

Classifier	Accuracy (in %)
kNN Classifier	96.77
NN Classifier	99.4

NN Classifier works on the basis of the Deep Pattern Recognition Algorithm. It consist of the Hidden layer which makes it more effective and it also perform well with complex sensory inputs, as in this case it is face images. These are some of the reasons that NN classifier performed better than the kNN classifier. On the other hand kNN classifier is one of the simplest classifier which works on the basis of the distance. In this case the distance is the Euclidean distance.

8. CONCLUSION

To differentiate between various individuals, accurate image classification systems are required as it is very essential part of various industries for access control. Image classification is done by extracting features from the image of the faces and matching the feature vector so formed with a pre formed database. An Anti-Spoofing method based on the liveness detection and HOG algorithm for the identification of spoof is developed and Primary Database is used for implementation. kNN and NN classifiers are used for the classification where NN classifier outperforms the kNN classifier with the 99.4% accuracy while the kNN accuracy is 96.77%.

9. REFERENCES

[1] Galbally, J., Marcel, S. and Fierrez, J., 2014. Biometric antispoofing methods: A survey in face recognition. *Access, IEEE*, 2, pp.1530-1552.

[2] Määttä, J., Hadid, A. and Pietikainen, M., 2011, October. Face spoofing detection from single images using micro-

texture analysis. In *Biometrics (IJCB), 2011 international joint conference on* (pp. 1-7). IEEE.

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

[4] Choudhury, T., Clarkson, B., Jebara, T. and Pentland, A., 1999, March. Multimodal person recognition using unconstrained audio and video. In*Proceedings, International Conference on Audio-and Video-Based Person Authentication* (pp. 176-181).

[5] Kollreider, K., Fronthaler, H. and Bigun, J., 2005, October. Evaluating liveness by face images and the structure tensor. In *Automatic Identification Advanced Technologies, 2005. Fourth IEEE Workshop on* (pp. 75-80). IEEE.

[6] Chetty, G. and Wagner, M., 2006, September. Multi-level liveness verification for face-voice biometric authentication. In *Biometric Consortium Conference, 2006 Biometrics Symposium: Special Session on Research at the* (pp. 1-6). IEEE.

[7] Pan, G., Sun, L., Wu, Z. and Lao, S., 2007, October. Eyeblink-based anti-spoofing in face recognition from a generic webcamera. In *Computer Vision, 2007. ICCV 2007. IEEE 11th International Conference on* (pp. 1-8). IEEE.

[8] Li, J., Wang, Y., Tan, T. and Jain, A.K., 2004, August. Live face detection based on the analysis of fourier spectra. In *Defense and Security* (pp. 296-303). International Society for Optics and Photonics.

[9] Kollreider, K., Fronthaler, H. and Bigun, J., 2008, June. Verifying liveness by multiple experts in face biometrics. In *Computer Vision and Pattern Recognition Workshops, 2008. CVPRW'08. IEEE Computer Society Conference on* (pp. 1-6). Ieee.

[10] Patel, K., Han, H., Jain, A.K. and Ott, G., 2015, May. Live face video vs. spoof face video: Use of moiré patterns to detect replay video attacks. In*Biometrics (ICB), 2015 International Conference on* (pp. 98-105). IEEE.

[11] Erdogmus, N. and Marcel, S., 2014. Spoofing face recognition with 3D masks. *Information Forensics and Security, IEEE Transactions on*, *9*(7), pp.1084-1097.

[12] Kshirsagar, V.P., Baviskar, M.R. and Gaikwad, M.E., 2011, March. Face recognition using Eigenfaces. In *Computer Research and Development (ICCRD), 2011 3rd International Conference on* (Vol. 2, pp. 302-306). IEEE.

[13] Li, Y. and Fan, C., 2009, August. Face recognition by nonnegative independent component analysis. In *Natural Computation, 2009. ICNC'09. Fifth International Conference on* (Vol. 2, pp. 555-558). IEEE.

[14] Zhao, X., Evans, N. and Dugelay, J.L., 2011, September. Semi-supervised face recognition with LDA self-training. In *Image Processing (ICIP), 2011 18th IEEE International Conference on* (pp. 3041-3044). IEEE.

[15] Liu, C. and Wechsler, H., 2000. Evolutionary pursuit and its application to face recognition. *Pattern Analysis and Machine Intelligence, IEEE Transactions on*, *22*(6), pp.570-582.

[16] Maurya, A. and Tarar S., 2016. Face Recognition techniques: A Survey. *In International Journal of Innovations & Advancement in Computer Science IJIACS on*, 5(2). (pp.2347-8616).

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

[18] Wen, D., Han, H. and Jain, A.K., 2015. Face spoof detection with image distortion analysis. *Information Forensics and Security, IEEE Transactions on*, *10*(4), pp.746-761.

[19] Galbally, J., Marcel, S. and Fierrez, J., 2014. Image quality assessment for fake biometric detection: Application to iris, fingerprint, and face recognition.*Image Processing, IEEE Transactions on*, *23*(2), pp.710-724.

[20] The TABULA RASA project. [Online]. Available: http://www. tabularasa-euproject.org/

[21] Bharadwaj, S., Dhamecha, T., 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* (pp. 105-110).

[22] Best-Rowden, L., Han, H., Otto, C., Klare, B.F. and Jain, A.K., 2014. Unconstrained face recognition: Identifying a person of interest from a media collection. *Information Forensics and Security, IEEE Transactions on*, *9*(12), pp.2144-2157.

[23] Erdogmus, N. and Marcel, S., 2013, September. Spoofing in 2D face recognition with 3D masks and anti-spoofing with kinect. In *Biometrics: Theory, Applications and Systems (BTAS), 2013 IEEE Sixth International Conference on* (pp. 1-6). IEEE.

[24] Evans, N.W., Kinnunen, T. and Yamagishi, J., 2013, August. Spoofing and countermeasures for automatic speaker verification. In *INTERSPEECH* (pp. 925-929).

[25] Kollreider, K., Fronthaler, H., Faraj, M.I. and Bigun, J., 2007. Real-time face detection and motion analysis with application in "liveness" assessment.*Information Forensics and Security, IEEE Transactions on*, *2*(3), pp.548-558.

[26] de Freitas Pereira, T., Anjos, A., De Martino, J.M. and Marcel, S., 2013, June. Can face anti-spoofing countermeasures work in a real world scenario?. In *Biometrics (ICB), 2013 International Conference on* (pp. 1-8). IEEE.

[27] Dalal, N. and Triggs, B., 2005, June. Histograms of oriented gradients for human detection. In *Computer Vision and Pattern Recognition, 2005. CVPR 2005. IEEE Computer Society Conference on* (Vol. 1, pp. 886-893). IEEE.