ISSN No:-2456-2165

Innovative Face Detection using Artificial Intelligence

Hira Khalid
Department of Software Engineering
HITEC University
Taxila, Pakistan

Abstract:- With the growing technology, various kinds of frauds are becoming so common, especially in the domain like face detection and other biometric systems. Additionally, it is hard for the service providers to keep data's privacy. Moreover, it is required to protect the system from spoofing. Hackers could use fake-eyes, snaps for face identification to get themselves authenticated. These face recognitions could also be done by face detection by video streaming and by capturing specific moments of any individual. Also, these types of frauds could be done easily as our systems are unable to detect the real-life face and face extracted from photos and videos. Additionally, these photos and videos would be freely available by Internet and other sources. Now-a-days, many ideas are implemented for the detection of face liveness for the purpose of authentication. The paper will represent innovative detection of faces by the use of features' fusion by using machine learning classifiers.

Keywords:- *Face Detection, Artificial Intelligence, Classification, Feature Extraction.*

I. INTRODUCTION

Biometrics technologies is commonly used term referred where technology is used for the identification of a person, which is relied upon the characteristics of an individual. The initial biometric technology was fingerprint identification. Furthermore, with the vast number of technologies, more classifications came into picture, i.e., palm print identification, iris recognition, speech recognition, face recognition, DNA, and gesture recognition. So, performance of identification relies on security, accuracy, and robustness of the technology. Initially, in every biometric system, features of an individual must be saved in a database. Moreover, every time an individual comes for identification, the freshly captured features would be matched with the saved features of an individual and if both features matched, it would be accepted as approved individual.

Biometric technologies are widely used for the purpose of authentication, with the technology advancement. Additionally, it has taken many applications, which are unable to maintain security of the information saved in the databases (DBs). These DBs would be effortlessly available and copied through the Internet because of no security of information. As, nobody has the power to stop the distribution of the information, which is stolen, the benefits of biometric technology are becoming disadvantages. On of the technology is "Face Detection", widely used for the purpose to identify the legitimate individual, which is relied on his physical and behavioral characteristics. In this technology of identifying individual would be done by the comparison of an existing pictures of individual in the DB with live features of an individual [1].

However, these images could be fooled effortlessly through identifying system using some saved images without notifying to the legitimate individual. Images, videos of identified individual or pictures taken from his/her social media accounts could do spoofing, easily. Thus, for maintaining privacy of these pictures, also, to check pictures' liveness for the purpose of identification, many investigators are applying various techniques.

In suggested work, the features, like, LuminanceR, Luminance are extracted are taken from the image dataset of 12146 pictures. Mean values of the recorded frames are transmitted for the purpose of classification by various classifier algorithms and in result, we will get trained model of dataset. Moreover, for video, live face will be detected for the purpose of preprocessing. Moreover, features would be extracted and then trained model will be used for prediction.

II. LITERATURE SURVEY

Biometric identification has acquired much significance now-a-days. This biometric authorization could be done through face recognition, palm-print recognition, fingerprint recognition, iris recognition etc. Face recognition is the mostly used biometric application. As, it takes fewer human being involvement. However, precision is utmost significant factor for face recognition. Additionally, this type of application needs least time to recognize identified individual. There are different techniques applied by researchers to recognize face is through Multi-level Block Truncation Coding [1].

This experiment is implemented by using 4 levels of Block truncation coding. It is done to extract feature vector for DB of 100 pictures. Algorithm performance is determined by noticing the ratio of Genuine Acceptance and False Acceptance. In conclusion, it is noticed that the result precision increases with the increasing level of Block Truncation Coding.

ISSN No:-2456-2165

Similarly, the security of DB is significant as the face recognition is increasing, generally. These days, the DB can be seen and spoofed, easily. Dynamic texture can be used to avoid spoofing in face detection [2]. In this research, 1st grey scaled frame, occurred from original frame would be transmitted by modified census transform. By considering 50 pixels of height and width of already detected faces were normalized to matrix of 64 x 64 and lessened noise using LBP-TOP computations. LBP operators were employed on every plane and used for the calculation of histogram and concatenation. After feature extraction step, next step is Binary Classification, to differentiate real person from spoofing attack to access pictures from DBs. By doing this procedure, best outputs are attained using non-linear Support Vector Machine classifier.

For avoiding spoofing attack, recaptured pictures are used for the real face detection [3]. Researchers considered the differentiation of spoofed and real pictures from NUAA DB. Moreover, Hue Channel Distribution, blurriness and specular ratio are used for checking the originality of an image [3]. Finally, it is considered the effective technique to recognize originality of images. Furthermore, detection rate could be accomplished 20 fps on personal computer.

Live face detection can also be done by 3D face shape analysis [4]. In this technique, 3D data is captured to simulate spoof attack. Experiment is done by real face in front of camera and already taken picture or snap. Further, they have taken 3D features by 2D photographic source [4]. Due to lack of variation of surface, it makes it straight that the scanned picture is originated from 2D image, and it is not original person's face.

Tracking of pupil could also be considered for the detection of spoofing attack [5]. Eye area would be extracted through HAAR-CASCADE classifier [5]. Portion of eye is cropped from the camera frame and then it would be rotated in constant eye area. After that, pupil is extracted from that specific eye area.

After some frames, algorithm will select any of the direction, it sends signal to Arduino for activation of chosen direction of eight LED's. Direction of eye would be noticed that Pupil direction and LED match. It results in live-face detection if it matches.

III. PROPOSED METHOD

In face liveness detection, this method will extract features i.e., Luminance, RGB-Grey and LuminanceR. Fig 1 will show each step:

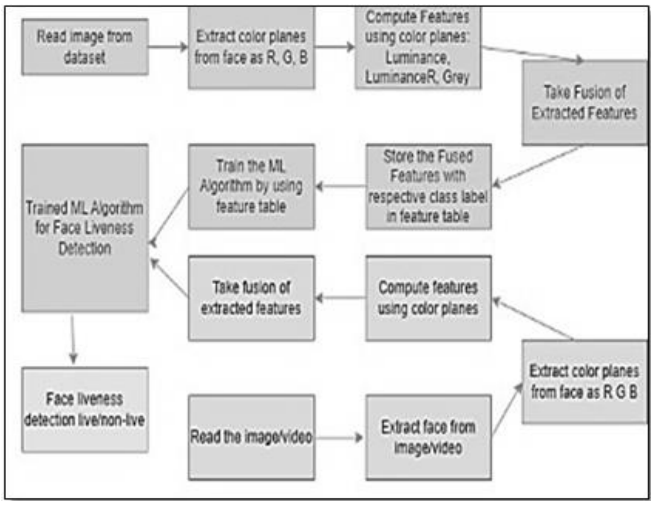

Fig 1 ML Model for Face Detection

The proposed method is categorized in two phases. In 1st phase, 1st pictures from the database of NUAA would be traversed incrementally. After traversing, red, blue, and green planes would be extracted from each image. After that, Luminance, LuminanceR and Grey features will be calculated and saved in a feature-table with their class. After completion, training of the system will be start by using Machine Learning algorithms.

To calculate Luminance, LuminanceR and Grey features, we will use following formulas:

Grey = Average ($Images_{a,b}$)a,b: Rows and Columns

Now,

Rows = Rows from images in DB

Columns = Columns from images in DB

Luminance = {(0.299 x Red) + (0.587 x Green) + (0.114 x Blue)}

Now,

Red = Red plane values in the image

Green = Green plane values in the image

Blue = Blue plane values in the image

LuminanceR = {(0.2126 x Red) + (0.7152 x Green) + (0.0722 x Blue)}

So,

LuminanceR means Luminance Relative

After that, system would fetch videos and images. Then, extract face frames. System will extract red, blue, and green planes from each face frame. Then, features will be computed using above mentioned color planes, Luminance and Luminance Relative. Further, it will make fusion of the features which are similar. Moreover, all these calculated values would be used as an input in trained Machine Learning model for face detection. Finally, the specific face would be detected as live or not.

Different machine learning classifiers i.e., Support Vector Machine, Random Forest Algorithm, Random Tree, Decision Table, Naïve Bayes, MLP, J48. Moreover, Accuracy is calculated in percentage for every feature by using these machine learning algorithms. Out of all the images in the database, 50 percent images are used in training and rest for testing and accuracy calculation. This 50 – 50 percentage is changed to 60 – 40 and 80 – 20 for testing and training to observe the features after fusion i.e., Grey, Luminance and Luminance Relative.

IV. EXPERIMENTATION ENVIRONMENT

For this research, Webcam of 2 Megapixel from the company of Logitech is utilized. Open CV library and Python language is used on Windows 8. NUAA dataset is used for the collection of images. Total images are 12146.

V. PERFORMANCE MEASURES

Generally, execution of features, like, Luminace, Luminace Relative and Grey are calculated by using Average Classification Accuracy, as:

$$\text{Accuracy} = \frac{\text{TP} + \text{TN}}{\text{TP} + \text{TN} + \text{FP} + \text{FN}}$$

TP = True Positive, TN=True Negative

VI. RESULTS & COMPARISON

Below are the obtained results by the algorithm proposed for face liveness detection. When NUAA DB is divided 50-50 i.e., 50 percent images for training and rest for testing,

Table 1 Accuracy for Face Detection for 50-50 percent training & testing image dataset

Classifier	Grey	Luminance	LuminaceR	Fusion, Grey+, Luminance+, LuminanceR
Naive-Bayes	68.7469	68.7469	68.681	69.208
Support Vector Machine	68.5658	68.5658	67.8083	68.6481
MLP	69.0927	69.0927	68.8128	77.8363
j48	71.151	71.151	72.2707	74.9547
Random-Forest	63.9058	63.4118	63.6588	77.3094
Decision Tree	63.8893	63.3954	63.6588	73.8679

It is noticed from the results that performance is far better after the fusion of all the Features by using machine learning algorithms in comparison to consider all the features, separately.

Table 2 Accuracy for Face Detection for 60% Train & 40% test Image Dataset

Classifier	Grey	Luminance	LuminanceR	Fusion, Grey+, Luminance, LuminanceR
Naive-Bayes	67.6616	67.6616	68.5056	69.0202
Support Vector Machine	68.4232	68.4232	67.5793	68.5056
MLP	67.7645	67.7645	67.7028	77.2334
j48	71.2021	71.1816	71.3462	71.3462
Random Forest	71.2021	71.1816	72.3755	75.8954
Decision Tree	64.4504	64.0181	63.3594	77.2334

It is again noticed that performance is better when working by the fusion of all the features, using machine learning algorithms as compared to take features separately.

Table 3 Accuracy for Face Detection for 80% train & 20% test image dataset

Classifier	Grey	Luminance	LuminanceR	Fusion, Grey+, Luminance, LuminanceR
Naive-Bayes	66.9	66.9	67.641	68.6702
Support Vector Machine	67.4763	67.4763	66.2413	67.8469
MLP	67.394	67.3528	67.7645	75.2573
j48	71.9638	71.9638	71.7579	72.499
Random Forest	71.9638	71.9638	71.7579	76.7806
Decision Tree	63.5241	63.0712	63.3594	78.1392

VII. CONCLUSION

Face detection becomes very important now-a-days because number of biometric devices are working which takes face for the detection. When there are many images saved in the database, chances of hacking and spoofing increase. All the saved images can be stolen from the database for future authentication. Many systems, now-a-days, grant access to the users from images and these machines are not able to detect liveness of human being. In this method, NUAA database is used to train and test images by using several machine learning algorithms i.e., Naïve Bayes, Support Vector Machine, MLP, Decision table, Decision trees, Random Forest, and j48. In proposed method, Luminance, Luminance Relative and Grey features are extracted from the images of NUAA database. After that, processing is done for videos and extracted features separately and fusion of all the features. Moreover, it is taken as an input for model training. After all the procedure, it is deduced that performance is better with fusion of features i.e., grey, luminance and luminanceR. Number of images in observations are also varied for further performance testing. 50-50%, 60-40% and 80-20% images are taken for training and testing purposes. Moreover, the system developed could be used to detect face liveness for avoiding attacks by spoofing through fusion of features.

REFERENCES

[1]. Dr. H. B. Kekre,Dr. Sudeep Thepade, Sanchit Khandelwal, "Face Recognition using Multilevel Block Truncation Coding", *International Journal of Computer Applications (0975 – 8887) ,Volume 36– No.11, December 2011*.

[2]. Tiago de Freitas Pereira, Jukka Komulainen, Andre Anjos, Jose Mario De Martino, Abdenour Hadid, Matti Pietikainen & Sebastien Marcel., "Face liveness using dynamic texure" *EURASIP Journal on Image & Video Processing*, Article No. 2(2014).

[3]. Xiao Luan, Huamming Wang, Weihua Ou, Linghui Liu, " Face Liveness Detection with Recaptured Feature Extraction", *IEEE,International Conference on Security, Pattern Analysis & Cybermetics, 2019.*

[4]. Andrea Lagorio, Massimo Tistarelli, Marinella Cadoni, Clinton Fookes, Sridha Sridharan,"Liveness Detection Based on 3D Face Shape Anyalasis", *International Workshop on Biometrics & Forensics*. IEEE, 2013.

[5]. Galbally, Javier, et al. "Iris liveness detection based on quality related features." *Biometrics (ICB), 2012 5th IAPR International Conference on*. IEEE, 2012.

[6]. Rehman, Y.A., Po, L.M. and Liu, M. (2018) 'LiveNet: Improving features generalization for face liveness detection using convolution neural networks', *Expert Systems with Applications*, 108, pp. 159–169. doi:10.1016/j.eswa.2018.05.004.

[7]. Rehman, Y.A., Po, L.M. and Liu, M. (2018) 'LiveNet: Improving features generalization for face liveness detection using convolution neural networks', *Expert Systems with Applications*, 108, pp. 159–169. doi:10.1016/j.eswa.2018.05.004.

[8]. Seo, J. and Chung, I.-J. (2019) 'Face liveness detection using thermal face-CNN with External Knowledge', *Symmetry*, 11(3), p. 360. doi:10.3390/sym11030360.

[9]. Mohamed, A.A. *et al.* (2021) 'Face liveness detection using a sequential CNN technique', *2021 IEEE 11th Annual Computing and Communication Workshop and Conference (CCWC)* [Preprint]. doi:10.1109/ccwc51732.2021.9376030.

[10]. Policepatil, S. and Hatture, S.M. (2021) 'Face liveness detection : An overview', *International Journal of Scientific Research in Science and Technology*, pp. 22–29. doi:10.32628/ijsrst21843.

[11]. Sengur, A. *et al.* (2018) 'Deep feature extraction for face liveness detection', *2018 International Conference on Artificial Intelligence and Data Processing (IDAP)* [Preprint]. doi:10.1109/idap.2018.8620804.

[12]. Khairnar, S. *et al.* (2023a) 'Face liveness detection using artificial intelligence techniques: A systematic literature review and Future Directions', *Big Data and Cognitive Computing*, 7(1), p. 37. doi:10.3390/bdcc7010037.

[13]. Farrukh, H. *et al.* (2020) 'Facerevelio', *Proceedings of the 26th Annual International Conference on Mobile Computing and Networking* [Preprint]. doi:10.1145/3372224.3419206.

[14]. Fourati, E., Elloumi, W. and Chetouani, A. (2019) 'Anti-spoofing in face recognition-based biometric authentication using image quality assessment', *Multimedia Tools and Applications*, 79(1–2), pp. 865–889. doi:10.1007/s11042-019-08115-w.