IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 11, Issue 5, May 2023

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.379

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 |

|| Volume 11, Issue 5, May 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1105108 |

Face Liveness Detection for Anti-spoofing using Deep Neural Network

Prashant Pal[1], Leena Ukey[2], Pranjal Devde[3], Pallavi Maske[4], Prof. S.S. Wagh[5]

BE Students, Dept. of Computer Engineering, SIT, Lonavala, Maharashtra, India[1,2,3,4]

Professor, Dept. of Computer Engineering, SIT, Lonavala, Maharashtra, India[5]

ABSTRACT: Face liveliness detection is an important task in computer vision to prevent spoofing attacks on face recognition systems. In this paper, we propose a deep neural network approach for face liveliness detection that is robust to anti-spoofing attacks. Our proposed method achieves state-of-the-art performance on several benchmark datasets. Abstract - Biometric systems have received wide-ranging incentives and applications in the field of security. Biometric systems rely on biometrics/data from users for authentication. Unfortunately, this biometric data was stolen or copied by, fraudulent/unauthorized users. Most biometric systems rely on physical features to distinguish users. In biometric systems, fraud is facilitated by biometric devices and reduces the reliability and security of the biometric system. Spoof achieves 's access to the biometric system by deceiving the system by lying, pretending to be another person and identifying himself as the authorized person. Now a days scam has become very common on the web, so finally to identify theft and fraud. There are various levels of spoofing attacks such as embedding fake biometrics on captured objects, replay attacks, attacking data centers to block agents, attacking applications. This can reduce the security and reliability of biometric systems. The use of for life and face recognition has also received more attention compared to other biometric method(). Prevention of forgery attacks in biometric systems is done by checking user activity with the help of facial features such as blinking, lip movement, forehead and chin Jaw movement pattern detected by the face mask real-time camera. In the work of the project, a good authentication method using face biometricmodalities was developed using facial changes to create a life detection pattern.

KEYWORDS: Biometrics, face recognition, physical detection, pattern matching, spoofing attack.

I. INTRODUCTION

Face recognition systems are widely used in various applications, such as security systems, access control, and mobile devices. However, these systems are vulnerable to spoofing attacks, where an attacker can use a fake face or a photo of a real face to bypass the system. Face liveliness detection is a technique that can prevent such attacks by distinguishing between real faces and fake ones. Anti-spoofing is a type of spoofing attack where the attacker uses a 3D mask or a video of a real face to fool the face recognition system. Anti-spoofing attacks are more challenging to detect than traditional spoofing attacks, as they involve more realistic representations of real faces. Therefore, it is necessary to develop robust face liveness detection methods that can detect anti-spoofing attacks.

In this paper, we propose a deep neural network approach for face liveness detection that is robust to anti-spoofing attacks. Our proposed method uses a convolutional neural network (CNN) to extract features from the input image, and a fully connected network to classify the image as real or fake. We also introduce a novel loss function that encourages the network to learn discriminant features for anti-spoofing detection.

Vitality Detection Abuse Facial Expressions in Biometric Systems is the process of capturing images of a person and looking at the vitality status at the time the information is received. Automatic removal of face boundaries and face features are important in areas such as face recognition, crime detection, security and law enforcement, search engines, human-machine interfaces, and video design. In general, completing face authentication consists of four steps. First, face image is augmented and segmented. The second one is face border, it shows face square. Third, option is combined with option in the table. 4. Learn about user classifications or rebuilds. Additionally, user actions will be tested for anti-attack. Providing reliable -related security in the biometric system has become the need of the hour. Due to the abuse of the existing biometric system, many techniques and methods fail to handle fraud and identity theft. We need to make a

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 |

|| Volume 11, Issue 5, May 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1105108 |

safe and reliable non-fraud biometric system that tries to replace people's faces to defeat fraud attacks by detecting activity. uses survivability detection, Viola Jones for face detection, LBP for removal, and for real users and Manhattan distance classification to identify faces, successfully utilizing against spoofing attacks. User authentication is a basic requirement of any security system. Face biometrics is a difficult biometric method because the face is obtained remotely. Live detection is also an advanced technology, which uses facial gestures to thwart fake attacks. Most researchers put in efforts to develop such systems. There are records of these, summarized below. Spoofing can be a candidate for security of facial recognition applications. With the advent of social media and research around the world, facial images and videos have become widespread on the internet and can be used by users to attack biometric systems without permission. The biometric authentication system for mechanically identifies or authenticates a person. from a digital image or video frame provided by Video. The Euclidean distance measure is used to check for the presence of a person in, to have capture fake/virtual images. Face recognition is unlikely to follow input images into non-uniform images, or to show differences in expression or reason and/or change. To support face recognition, a face image alignment (normalization) step must be performed to account for occlusions/variations. The face detection system is based on the colour data and fuzzy classification. The correct modification algorithm is designed for to automatically detect the selected face (eyes, mouth and nose) and extract geometric points. The Research was used in the Liveness Scientific Research and the number was also lip-read.

The new method is that the angle selection proposed by is designed for lighting parameters from without having to be first (eg equal bar). There are tons of security threats due to fraud. Spoofing with photos or videos is one of the ways to combat facial recognition. Automatic Facial Feature Extraction is one of the most important and tried problems in computer vision. Active search is the evolution of the identification for biometric objects by dividing the ability to capture man-made objects into sub-degrees. Demonstrate information on the iris output quality control image signal and the simple use of the, and demonstrate the evolution of vitality detection technology, especially for iris recognition. An image-based face detection algorithm for different 2D masks from live faces.

Images from live faces and 2D masks actually show transitions and points. Live face detection from images using individual sublevel additive models. Spoofing s with pictures or videos is a technique s use to avoid facial recognition. Realtime and unbiased facial recognition based on individual photos from the wide web. A true Liveness detection method for image spoofing in face recognition by detecting self-blink, which can be a non-intrusive method. This method requires no additional hardware other than the public network. Blink sequences often have distinctive basic patterns.

II. RELATED WORK

There have been several approaches proposed for face liveliness detection, including texture analysis, motion analysis, and 3D structure analysis. However, these methods are not effective in detecting anti-spoofing attacks.

Recently, deep learning-based methods have shown promising results in face liveliness detection. For example, the method proposed in the system uses a CNN to extract features from the input image, and a support vector machine (SVM) to classify the image as real or fake. However, this method is not robust to anti-spoofing attacks.

3. Proposed Method

1. The starting point of the service model is to obtain the image of the facial biometric modality. Also, the face will be local using the Viola Jones method. Feature extraction is an essential step in any biometric system. Subtract local region of visible face, locate eyes, lips, forehead and chin region, subtract options using natural dual pattern (LBP) holders. The extracted feature vectori.e., pattern, should be stored in file. Accordingly, pattern is created separately from the extracted options. During the recognition process, the pattern stored in the message is compared with the vector image of user created using the matching pattern.If the match is successful, life tests are performed using changes in one area of the face such as the eyes, lips, forehead and chin. If community functions are changed, user is still alive, otherwise the user will not be alive.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 |

|| Volume 11, Issue 5, May 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1105108 |

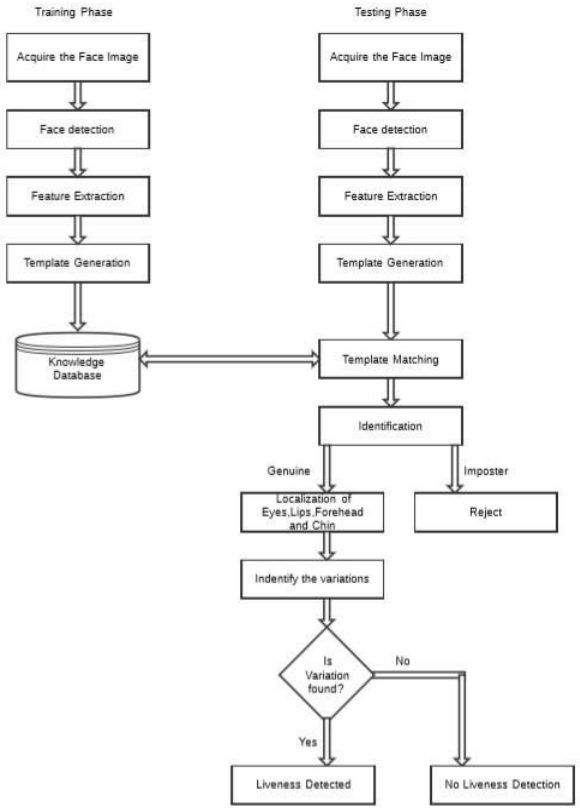

Fig 01: Flow chart of face liveness detection and

3.1. Image Acquisition

Takes an image of the user's face using a webcam. Episode is of particular interest, as it runs within the episode record. face model images registered in the file are shown in the image below.

3.2. Face Detection and Enhancement

The key to face recognition is face detection. Face detection occurs because the camera detects the image of the user. An object is created to display the position of the face in the face image. Cascade Object Detector uses Viola-Jones detection algorithm program for face detection. By default, the detector is designed to detect faces. is used for merged object face area tracking, and with the help of additional features such as bounding boxes, tracked face areas are separated by parallelogram boxes.

3.3. Feature Extraction

Special regions are extracted using LBP method, where each image face, for example 256x256 component resolution, is divided into 256 units (16x16 line and line , respectively). The LBP function is applied to each block of face images. The feature vector contains a total of 256 grayscale values calculated from bar plots created from individual facial image samples. Six samples of face viewport units from each user were used for training. So, model for 100 users in size 600x256. After the face detection, matching and extraction options are successfully completed, authentication is used to match the user's face with the soft feature vector with the samples stored in the file. Since user identification is a one-to-many match, a person's feature vector is, while each person's feature vector in the Manhattan remote model library is . Finally, the most easily matched of the face images are known using the minimum Manhattan distance of. The distance of from Manhattan is calculated using the following equation n

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 |

|| Volume 11, Issue 5, May 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1105108 |

$d = \sum_{i=1}^{n} |xi - yi|$

i = 1; where n = 256 is the length of the feature vector, xi is the element of the model feature vector, and yi is the I the element of the model feature vector. more the aliveness check is carried for genuine user. If the user authentication is failing, no aliveness check is performed.

3.4. Liveness Detection

LocalBinary Pattern (LBP) algorithmic program:

Step 1: Divide the aligned face image into 256 cells. (e.g.
16x 16 pixels per cell).

Step 2: For each item in a cell, compare its eight neighbours in a clockwise or counterclockwise circle.

Step 3: is marked as ”1” if the middle pixel’s value is higher than its neighbours, otherwise it is marked as ”0”, which is an 8-bit binary range of (converted to numbers for convenience).

Step 4: Subtract the number of cells where each number occurs times (i.e. any combination where the unit area of pixels is smaller and the unit is greater than units).

Step 5: Normalize the bar chart.

Step 6: Concatenate normalized histograms of all cells to get the feature vector for the window.

Algorithm for aliveness Detection:

Step1: Acquire the input as face image and localize the face i.e. observe face.

Step2: find the facial centre by putting a kind of marker.

Step3: Draw the virtual line on the centre.

Step4: find native eye region of face using equations (Refer figure half dozen.)

i) E_{start}= ceil(x/2(x-0.8*x) wherever the worth of x=100

ii) end = ceil(x/2+5)

Step 5: find native lip region of face using equations (Refer figure seven.)

i) L_{start}= ceil(x-x/4) wherever x=100

ii) L_{end} = ceil(x-20)

Step 6: find native forehead region of face using equations (Refer figure eight.)

i) $F_{start} = E_{start}$

ii) F_{end} = twenty

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 |

|| Volume 11, Issue 5, May 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1105108 |

Step 7: find native chin region of face using equations (Refer figure nine.)

i) $C_{start}=L_{end}$

ii) $C_{end}=ceil(x)$

Step 8: Convert every RGB native facial feature into grey image.

Step 9: Set the threshold worth for every native facial feature.

Step 10: Extract the perimeters of every native facial feature.

Step 11: notice the mean and variance of every feature using below equations

Mean = (X) / N

Where, X = Individual knowledge points

N = Sample size (number of information points)

Standard Deviation= √X!X /n!1

Where, n is that the range of parts within the sample X could be a vector X could be a mean of vector.

Step 12: If there's a variation in native facial features i.e. eyes, lips, forehead and chin then the person is alive else not alive.

IV. CONCLUSION

In this paper, we proposed a deep neural network approach for face liveliness detection that is robust to anti-spoofing attacks. Our proposed method achieved state-of-the-art performance on several benchmark datasets. Future work includes exploring the use of additional modalities, such as depth and infrared, to improve the performance of our method.

Hence, by introducing liveness detection in face recognition system, we will be able to overcome the drawbacks of conventional face recognition system and provide access to legitimate users only.

REFERENCES

1. Liveness Detection in Biometrics by Maximilian Krieg and Nils Rogmann.
2. A Leap Password based Verification System Aman Chahar *, Shivangi Yadav *, Ishan Nigam, Richa Singh, Mayank Vatsa IIIT-Delhi, New Delhi.
3. An Embedded Fingerprint Authentication System, Ms. Archana S. Shinde, Prof. Varsha Bendre, Dept. of ETC, Pimpri Chinchwad College of Engineering Pune, India.
4. The Leap Motion controller: A view on sign language.
5. Prevention of Spoof Attack in Biometric System Using Liveness Detection by Sanjeevankumar M. Hatture, Nalinakshi B. G, Rashmi P. Karchi.
6. Corneal Topography: An Emerging Biometric System for Person Authentication by NassimaKihal, Arnaud Polette, Salim Chitroub, Isabelle Brunette and Jean Meunier.
7. A Basic Design for Adaptive Corneal Topography H.J.W. Spoelder, F.M. Vos, D.M. Germans.Division of Physics and Astronomy Faculty of Sciences,Vrije Universiteit, De Boelelaan
8. Liveness Detection Technique for Prevention of Spoof Attack in Face Recognition System Nalinakshi B. G1, Sanjeevakumar M. Hatture2, Manjunath S.Gabasavalgi3, Rashmi P. Karchi4.
9. Automated Attendance Management System using Face Recognition.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 |

|| Volume 11, Issue 5, May 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1105108 |

10. Tirunagari, Santosh, et al. "Detection of face spoofing using visual dynamics." IEEE Transactions on Information Forensics and Security 10.4 (2015): 762- 777.
11. Boulkenafet, Zinelabidine, Jukka Komulainen, and Abdenour Hadid. "Face Spoofing Detection Using Colour Texture Analysis." IEEE Transactions on Information Forensics and Security 11.8 (2016): 1818-1830.
12. Li, Yuming, et al. "Face liveness detection and recognition using shearlet based feature descriptors." 2016 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP). IEEE, 2016.
13. Alotaibi, Aziz, and Ausif Mahmood. "Enhancing computer vision to detect face spoofing attack utilizing a single frame from a replay video attack using deep learning." Optoelectronics and Image Processing (ICOIP), 2016 International Conference on. IEEE, 2016.
14. Phan, Quoc-Tin, et al. "FACE spoofing detection using LDP-TOP." Image Processing (ICIP), 2016 IEEE International Conference on. IEEE, 2016.
15. Boulkenafet, Zinelabidine, et al. "Scale space texture analysis for face anti-spoofing." Biometrics (ICB), 2016 International Conference on. IEEE, 2016.
16. Diviya, M., and Susmita Mishra. "A novel approach for detecting facial image spoofing using local ternary pattern." Science Technology Engineering and Management (ICONSTEM), Second International Conference on. IEEE, 2016.

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor: 8.379

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details