Spoofing Face Recognition Using Neural Network with 3D Mask

REKHA P.S
M.E Department of Computer Science and Engineering, Gnanamani College of Technology, Pachal, Namakkal-637018.
rekhaps06@gmail.com

MRS.R.SUMATHI M.E. Assistant Professor,
Department of Computer Science and Engineering, Gnanamani College of Technology, Pachal, Namakkal-637018.
sumathikavi@ymail.com

ABSTRACT
Spoofing refers tricking or deceiving computer systems or other computer users. This is typically done by hiding one's identity or faking the identity of another user on the Internet. Widespread acceptability and use of biometrics for person authentication has instigated several techniques for evading identification. One such technique is altering facial appearance using surgical procedures that has raised a challenge for face recognition algorithms. Mainly focusing on 2D attacks forged by displaying printed photos or replaying recorded videos on mobile devices can no longer be maintained. We aim to inspect the spoofing potential of subject-specific 3D facial masks for different recognition systems and address the detection problem of this more complex attack type & also a multi objective evolutionary granular algorithm is proposed to match face images before and after plastic surgery. The algorithm first generates non-disjoint face granules at multiple levels of granularity. Finally the performance of this recognition is given by ANN classifier. It gives higher accuracy as compared to existing algorithms and a commercial face recognition system.

INTRODUCTION
The most commonly used biometric trait by humans, face recognition has become an active research topic for many decades now and it has found great application in consumer electronics and software. Face easily accessible compare to other biometric content like finger print or iris. Spoofing attack create fake evidence .It is relatively simple to attack for facial recognition system due to the fact that the photograph or videos of a user can easily accessed from a distance .Valid user as a person that are enrolled in a face recognition system .An attacker can gain to access by showing their photos.

Antispoofing classified into three groups:
- Texture Analysis
- Motion Analysis
- Liveness Detection

Texture Analysis
This technique check the texture of the captured face image. It depends on the quality of the image or video quality.

Motion Analysis
This method analyzing the motions in the scene.

Liveness Detection
Liveness of the face is determined based on live face specific gestures such as eye-blinking or lip movement.

RELATED WORK
The previous work in mask detection aim to difference between facial skin and mask materials. The authors conducting more experiments on different material such as silicon, latex or skin-jell which show different reflectance compared to facial skin.

SVM classifier is used to split up between genuine and fake samples on a database of 20 masks of different materials: plastic, silica gel. The
advantage of their work to identify on real facial mask.

Morpho database is constructed by using 3D laser scanner. The client picture is captured by 3D laser scanner. In Morpho database available in the texture image. Face recognition system oppose 3D mask attacks and a micro texture analysis based counter measure applied separately on color image and depth maps.

In base line face recognition algorithms samples are compared with the gallery. This comparison produce two types of result first is real genuine and real impostor. Other result is mask genuine and mask impostor.

MASK ATTACK DATABASES

There are two types of spoofing database for 3D mask.

A. Morpho Database

Morpho database is a non public database. Morpho database consist of real access and mask attack samples.

B. 3D Mask Attack database

3D Mask Attack Database is a face Spoofing database. It consist of 17 users.

PROPOSED SYSTEM

The methodology carried out in the proposed work is artificial neural network technique. These techniques we can use more than one input check the problem. We used feed forward A single stage feed forward neural network classifier containing one input, one hidden and one output layer was predominantly used for face classification. The extraction of face features in the detected by using Local Binary Pattern(LPB). These features are given as the input to the Artificial Neural Network and Back Propagation Network Classifier.

OBJECTIVES

A. Face Detection.

B. Feature Extraction

C. Back Propagation Neural Network

FACE DETECTION

Face Detection is one of the most important tasks of any facial classification system. The faces are detected by using Viola Jones Algorithm. In Viola-Jones algorithm, first to scan a sub-window capable of detecting faces from a given input image. And then to rescale the input image to different sizes and at last to run the fixed size detector through these images.

FEATURE EXTRACTION

Viola Jones Algorithm is used for the feature extraction. This principal is used for determining the geometry of the faces. The distance between eyebrow to eye, eyebrow to nose top, nose top to mouth, eye to mouth, left eye to right eye, width of nose, width of mouth, these features are selected from the images.

CLASSIFICATION USING ANNS

1. Back propagation network (BPNs) is used to classify the images.
2. The neural network used to hidden layer, input layer , output layer.

**Fig 2: Artificial Neural network**

**ARTIFICIAL NEURAL NETWORK (ANN)**

An artificial neural network (ANN), generally called neural network (NN), is a mathematical model or computational model that is inspired by the structure and/or functional aspects of biological neural networks. A neural network contains of an interconnected group of artificial neurons (processing element), working in unison to solve specific problems. ANNs, like people, learn by example. The neuron has two modes of operations. The training/learning mode and the using/testing mode. In mainly cases an ANN is an adaptive system that converts its structure based on external or internal information that flows through the network in the learning phase. Recent neural networks are non-linear statistical data modeling tools. They are generally used to model complex relationships between inputs and outputs or to find patterns in data.

An ANN is created by combining artificial neurons into a structure containing three layers.

1. The first layer consists of neurons that are responsible for a face image sample.

2. The second layer is a hidden layer which allows an ANN to perform the error reduction necessary to successfully achieve the desired output.

3. The final layer is the output layer wherein the number of neurons in this layer is determined by the size of the set of desired outputs, with each possible output being represented by a separate neuron.

**BACK PROPAGATION NETWORKS (BPN)**

Back propagation neural networks are the most common neural network structures, as they are simple, effective and useful in a variety of applications. Back propagation neural network is a network of nodes arranged in layers. First layer of network is input layer, last layer of the network is output layer and remaining all intermediate layers are hidden layers. Three layered back propagation neural network having input, output and hidden layer, has been used for classification. All nodes from one layer are connected to all nodes in next layer. Each connection is associated with its weight which represents strength of the particular connection. Before the training process, the weight for the nodes are considered as random.

**SIMULATION RESULT**

**Fig 3: Input Image**

**Fig 4: Antispoofing Technique**
ADVANTAGE OF PROPOSED SYSTEM

The results of the artificial neural network techniques were promising as we got 97.5% for accuracy.

CONCLUSION

Utilization of 3D masks in spoofing attacks becomes easier cheaper each day with the advancements in 3D printing technology. The experimental results generally suggest that for both data types, ANN classification of block-based extracted uniform LBP features is more accurate in mask detection. For the sake of reproducible research, the source code is made publicly available, together with the database and its protocols. A possible extension to this work is to explore the spoofing performances in 3D face recognition systems and to devise methods to detect attacks using pure 3D data, instead of 2.5D. Additionally, further investigation can be done on spoofing the spoofing potential of each mask separately.

ACKNOWLEDGEMENT

I would like to thank all the faculties and students of Computer Science and Engineering Department, Gnanamani College of Technology management for their guidance and support and facilities extended to us.

REFERENCE PAPER


[7] Nesli Erdogmus and Sébastien Marcel “ Spoofing Face Recognition With 3D Masks”

Fig 5: Output