# Liveness Detection Using Face Detection

Prakash Rajagopal and Vishesh Tanksale

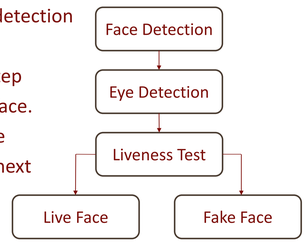
School of Informatics and Computing, Indiana University, Bloomington

## INTRODUCTION / MOTIVATION

- Biometrics are actively being used for authentication on various system
- Used because of high accuracy, ease of use and more secure
- Use of human physiological characteristics that are distinct for each human being like fingerprints, iris scans, voice, face.
- Some human physiological characteristics like face are highly prone to spoofing attack
- Availability of high resolution and cheap cameras makes it easy to spoof faces using videos or photos
- Numerous highly accurate face recognition approaches are available
- Aim is to develop an anti spoofing face recognition system using physiological characteristics of human face
- The anti spoofing system will work without use of any special hardware

## WORKFLOW

The workflow of our liveness detection is as mentioned below




- Face Detection : The first step eye detection is to detect face. The algorithm used for face detection is mentioned in next section
- Eye Detection : We are trying to locate the eyes in the face region detected.
- Liveness Test : Based on the eye region we perform liveness test. We tried two different methods for eye detection. Mentioned them in detail in next section

## FACE & EYE DETECTION

**Initial Face Detection**

• Viola jones algorithm with the Haar classifiers for face detection is used to detect the actual face

**Gotcha for Eye detection using Haar classifiers**

• Eye detection using Haar classifiers fails for closed eyes since the default classifier is trained only for open eyes

• Any classifier based on closed eyes lead to a lot of false positives.

**Eye detection using Landmark detection**

• Feature detection of face using Landmark detection where Hog is used along with provided data file to detect face regions.

**SVM based classification into open , closed or ambiguous**

• The isolated eye region is scaled and passed through an SVM classifier where we compare with the closed eye and open eye database. The eyes are scored accordingly and are classified as open, ambiguous and closed.

• The classifiers will be use the following database for training

- ZJU Eyelink database - http://www.cs.zju.edu.cn/gpan or http://www.stat.ucla.edu/gpan [Doesn't work]
- Closed Eye database

http://parnec.nuaa.edu.cn/xtan/data/ClosedEyeDatabases.html

Eye Detection Results

## EYE NORMALIZATION

**Image Normalization [2]**

- The eye images can have different orientations and sizes
- To compare images normalization is necessary
- Image is reduced to fixed dimension and then Self Quotient Image (SQI) is applied for normalization
- SQI can be thought of as a high pass filter.

Where Q is given by

$$Q = \frac{I}{I'} = \frac{I}{F * I} \quad \text{[ From Ref 2]}$$

Where, I' is low frequency image of the original image, F is the Gaussian Kernel.

$$G = \frac{1}{2\pi\sigma^2} e^{\frac{i^2+j^2}{2\sigma}} \quad \text{[ From Ref 2]}$$

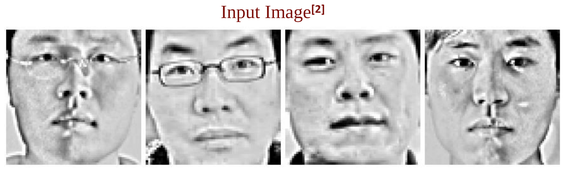
$$\tau = Mean\ (I)$$

W(i,j) = 0 I(I,j) <$\tau$ or 1 otherwise

F(i,j) = W(i,j) G(i,j)

where I is the kernel size, I(i, j) is the intensity, F(i, j) is the Gaussian kernel, and W(i, j) is the weight in (i, j).

Input Image[2]

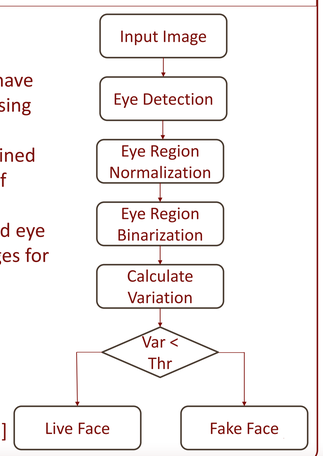


Self Quotient Image[2]

## LIVENESS DETECTION USING BINARIZATION

**Eye Region Binarization [2]**

- Eye region is normalized to have the pixel value of 0 or 1 by using a threshold
- Threshold is adaptively obtained from the mean pixel value of each eye region
- Figure below shows binarized eye regions extracted from images for fake and live face




Ref from [1]

Fake Face [2]

Live Face [2]

- Liveness score is calculated as the hamming distance between two binarized images of eyes
- If average liveness score is less than threshold then its fake face

## METHOD – LIVENESS DETECTION USING CRF

**Detection using eye blinking and CRF [From Ref 1]**

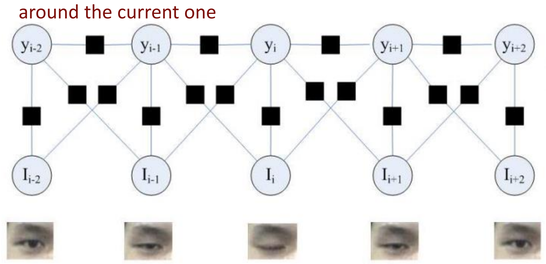
- Conditional modeling of blinking behaviors can be used for liveness detection.
- An eyeblink activity can be represented by an image sequence S consisting of T images, where

$$S=\{ I_i , i=1,\ldots,T\}$$

- The typical eye states in the images are open, close and ambiguous. This can be modeled as a linear chain CRF (conditional random field)[1]

**HMM features**

- Observations : All the images are modeled as observations
- States : Resulting state is the hidden state
- In this graphical model, a parameter of observation window size W is introduced to describe the conditional relationship between the current state and (2W+1) temporal observations around the current one




**Model of linear chain CRF , Window size is 1 here**
**Circles are variable nodes and black boxes are factor nodes**
**[Figure reprinted from Liveness detection Book [1] ]**

**Eye Closity**

- We can compute a value known as the eye closity using the SVM classification score. This score is fed into the initial training of the CRF
- The potential function is the sum of the CRF features at time t. The various parameters are calculated in the training phase with set of images from the Replay attack database (https://www.idiap.ch/dataset/replayattack) and the NUAA Photograph Imposter Database.

**Measurement Techniques**

Eye blinking observations can be measured in three ways :

- One-eye detection rate : Left and Right eye blinks are calculated independently and threshold is set for live and fake images.
- Two-eye detection rate : In it each simultaneous blink activity is accounted for one blink activity.
- Clip detection rate : Any blink of single eye in a small part of the face is considered a liveness indicator

## RESULT

- We have studied and implemented techniques for face detection and eye detection
- Implemented two methods for liveness detection 1) Eye Binarization 2) Hidden Markov Model
- This implementation in combination with face matching can be used for better face recognition with greater security.
- While these techniques certainly improve the anti-spoofing capabilities of the system with respect to static photo based spoofing, We have not been able to touch on counter measures for video based spoofing. For further study, you can refer to "Motion-Based Counter-Measures to Photo Attacks in Face Recognition" paper [6]

## REFERENCES

1. Liveness Detection for Face Recognition : Gang Pan, Zhaohui Wu and Lin Sun , Department of Computer Science, Zhejiang University
2. Liveness Detection for Embedded Face Recognition System : Hyung-Keun Jee, Sung-Uk Jung, and Jang-Hee Yoo
3. Automatic Recognition of Eye Blinking in Spontaneously Occurring Behavior: T Moriyama, T Kanade, JF Cohn, J Xiao, Zara Ambadar, Jiang Gao, Hiroki Imamura
4. Face feature detection tutorial : http://www.learnopencv.com/facial-landmark-detection/
5. OpenCV docs for face detection http://docs.opencv.org/3.1.0/d7/d8b/tutorial_py_face_detection.html#gsc.tab=0
6. Motion-Based Counter-Measures to Photo Attacks in Face Recognition : Andre Anjos, Murali Mohan Chakka and Sebastien Marcel