Face Anti-Spoofing Architectures

DEPARTMENT OF ELECTRONICS & ELECTRICAL ENGINEERING

INDIAN INSTITUTE OF TECHNOLOGY GUWAHATI

April 2019

Introduction

► Biometrics utilize characteristics, such as **fingerprint**, **face**, and **iris** to uniquely authenticate an individual.

► Face is the most accessible biometric modality. A face anti-spoofing framework is required to detect the presence of disguises deployed by illegal traffickers.

► The attacks can be made in 3 major ways: **print/photo** attacks, **replay/video** attacks, **3-D mask/prosthetic** attacks.

► In this work, we focused on **print attacks** that involves showing victim's photo using printed form to outwit biometric sensors. Such scenarios can easily be learned by classifier, such spoofs boils down to **image manipulation**.

► We studied, modified and demonstrated various face anti-spoofing techniques namely Image Quality Assessment **(IQA)**, Textural features Local Binary Patterns **(LBP)** & its variants, and Image Distortion Analysis **(IDA)**.

Problem Statement

► Face anti-spoofing can be performed in 2 modes:

- ■ **Identity independent anti-spoofing** in which algorithm has no prior idea regarding the subject in the facial snapshot to the camera.
- ■ **Reference based anti-spoofing** wherein a person may claim to be someone else by presenting a prosthetic of that individual's face.

► The identity independent problem is less challenging from a technical viewpoint as compared to the reference based anti-spoofing problem.

► In our solution, we developed a **reference based anti-spoofing system** for a closed unmanned authentication system, implemented for an organization.

► **Natural full frontal poses** under different lighting conditions are stored in database for different subjects.

► Once the base-feature set for anti-spoofing is designed and calibrated, any attempt to produce a spoofed version of the face should be detected by this anti-spoofing algorithm by treating this test-query set as an outlier. Ideas involving **anomaly detection algorithms** namely **1-class SVM** are explored [6].

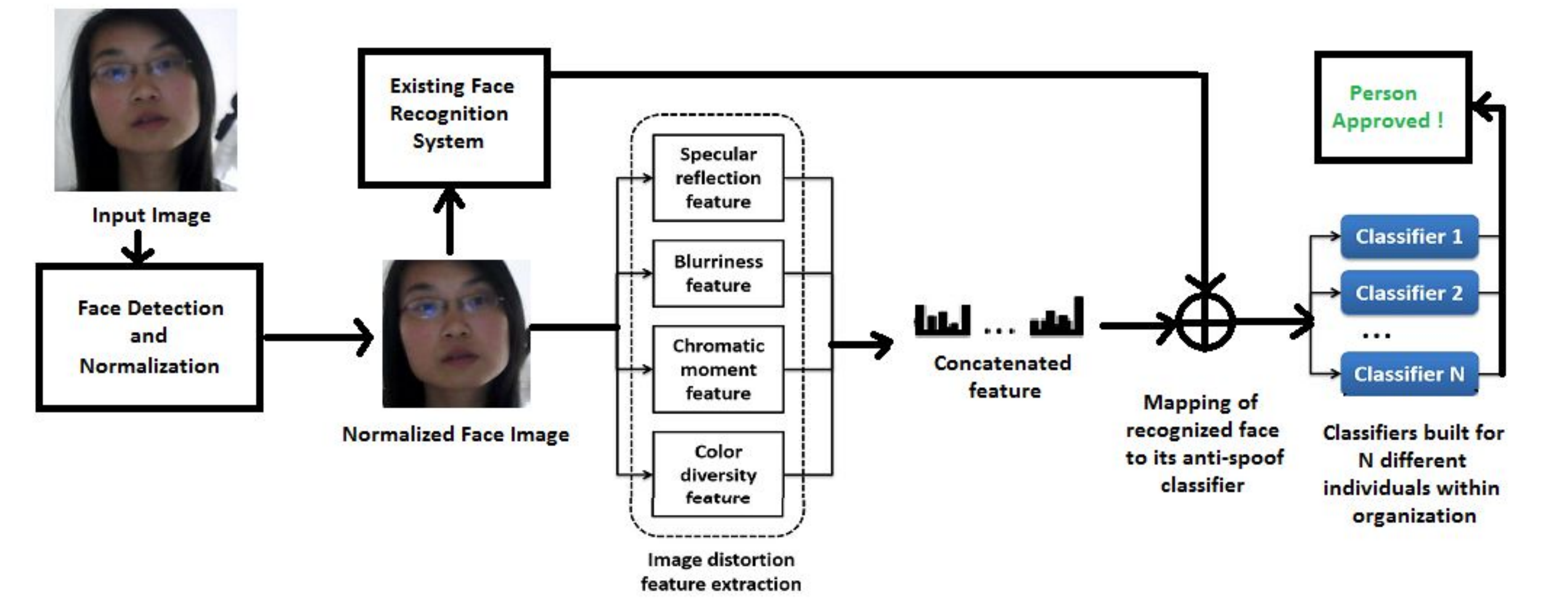
Methodology

► For identity independent problem, we used **image quality assessment** measures having **pixel difference**, **correlation based**, and **edge based** measures [7] and textural features namely **local binary pattern** (LBP) and its variant transitional-LBP [8].

► For **reference based anti-spoofing** we explored image distortion analysis features [1], that have their motivation stemming from the various **noise and distortion components** that enter into the spoofed images because of both the **spoofing medium** and the **recapture process**.

1. Blurriness: Blur is most noticeable in textured areas and along the edges. The feature that we are using attempts to calculate the spread of edges as mentioned in [3]. Spoofed faces are mostly defocused because of the recapturing process via mobile cameras.So, image blur due to defocus can be used as a key characteristic of a spoofed image.

Experimental Setup



► In this work, we have used publicly available **CASIA spoof database** as out base database. It consists of genuine and spoof images of 14 different individuals. We have built a person-specific face anti-spoofing architecture.

► Person provides the system with a face image and claims to be person X within organization. A person is authorized only if he/she is the person whom he/she claims to be within organization and face image presented to the system is **genuine**.

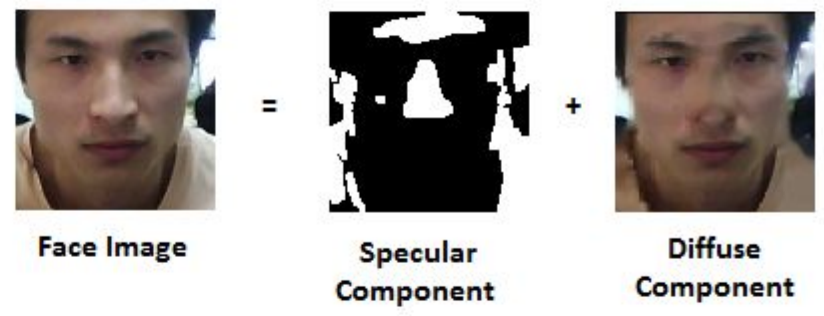
► In order to recognize the identity of input face, we can use an existing state-of-art face recognizer. It can noted that this **work does not focuses on face recognition**, hence the identity of an individual can be submitted manually to the system.

► For each individual within organization, a separate outlier detection classifier is **trained using genuine images** (50 images per person) stored in database. Spoof classification is dealt as an **outlier detection task**, for which **1-class linear SVM** is used.

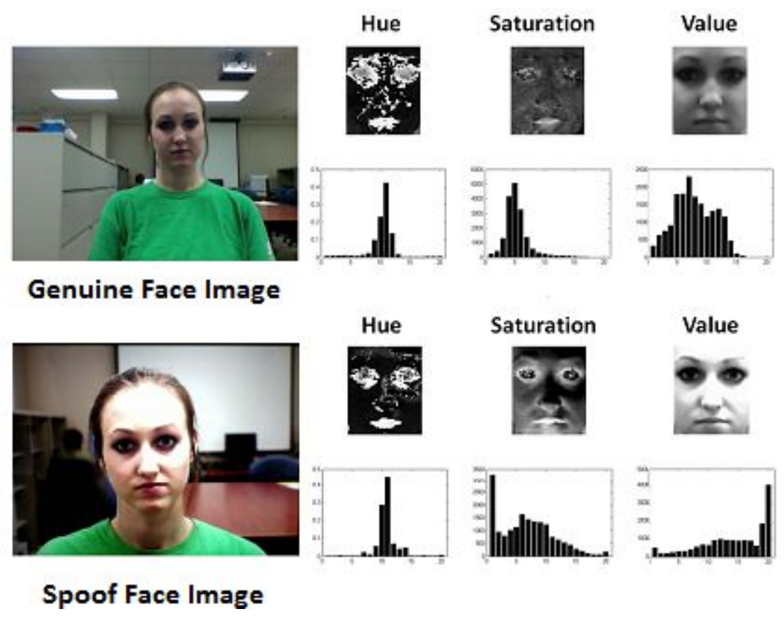
► **IDA feature vector** consists of **specular reflection** measures (3-dimension), **blurriness** measure (1-dimension), **chromatic moment** feature (15-dimension), **colour diversity** feature (101-dimension) and **farthest neighbour histogram** feature (4-dimension) which is concatenated to form a **124-dimensional feature vector** for each train and test image.

Methodology

2. Specular Reflection: As indicated by the Dichromatic Reflection Model, light reflectance **I** of an object at a specific location x can be decomposed into diffuse reflection and specular reflection components [2]. The specular reflection component of the image is separated.



3. Chromatic Moment: Spoofed images show a different colour profile in comparison to genuine images. This is because of imperfect colour reproduction property of print or display media as stated in [4].



We explore the **HSV colour space** to quantify this disparity. **Mean**, **variance** and **skewness** of histogram of each channel is calculated along with pixel percentages in bins.

Methodology

4. Colour Diversity: Genuine image have a richer colour profile as compared to spoofed images. We construct the histogram of all the colours involved in the image and pick the occurrence frequency of top N (here 100) colours [4].

5. Farthest Neighbor Histogram: Farthest neighbor of a given pixel is calculated out of the 4 adjacent neighbors and an appropriate distance metric which in our case is L1 color distance between pixels as stated in [5].

Results

	Precision	Recall	F1-Score	Accuracy
IQA	0.96	0.96	0.96	0.96
LBP & t-LBP	0.89	0.89	0.89	0.89
IDA	0.90	0.84	0.85	0.84

1. IQA, LBP & t-LBP: Identity independent anti-spoofing setup, **linear SVM** is used to fit hyperplane between genuine & spoof face image class i.e. **binary classification**. Precision, recall, f1-score, and accuracy is reported on average basis over 2 classes i.e. genuine and spoof class.

2. IDA: Person-specific anti-spoofing architecture, assumed to have only genuine images at time of training. **1-class linear SVM** is used for **outlier or anomaly detection task**. Precision, recall, f1-score, and accuracy is reported on average basis for **14 individuals** of **CASIA spoof database**.

B.Tech. Project Supervisor:

Dr. Kannan Karthik, Associate Professor, Dept. of EEE, Indian Institute of Technology Guwahati

B.Tech. Project Members:

Shubham Lohiya (150102064), ECE, IITG

Shubham (150102079), ECE, IITG

References:

1. Wen, D., Han, H., & Jain, A.K. (2015). Face Spoof Detection With Image Distortion Analysis. IEEE Transactions on Information Forensics and Security, 10, 746-761.
2. X. Gao, T. Ng, B. Qiu and S. Chang, "Single-view recaptured image detection based on physics-based features," 2010 IEEE International Conference on Multimedia and Expo, Suntec City, 2010, pp. 1469-1474.
3. Marziliano, P., Dufaux, F., Winkler, S., & Ebrahimi, T. (2002). A no-reference perceptual blur metric. ICIP.
4. Chen, Y., Li, Z., Li, M., & Ma, W. (2006). Automatic Classification of Photographs and Graphics. 2006 IEEE International Conference on Multimedia and Expo, 973-976.
5. Athitsos, V., Swain, M.J., & Frankel, C. (1997). Distinguishing photographs and graphics on the World Wide Web. 1997 Proceedings IEEE Workshop on Content-Based Access of Image and Video Libraries, 10-17.
6. Yunqiang Chen, Xiang Sean Zhou and T. S. Huang, "One-class SVM for learning in image retrieval," Proceedings 2001 International Conference on Image Processing (Cat. No.01CH37205), Thessaloniki, Greece, 2001, pp. 34-37 vol.1.
7. Galbally, J., & Marcel, S. (2014). Face Anti-spoofing Based on General Image Quality Assessment. 2014 22nd International Conference on Pattern Recognition, 1173-1178.
8. Trefny, J., & Matas, J. (2010). Extended Set of Local Binary Patterns for Rapid Object Detection.