Face Anti-Spoofing Architectures

A thesis submitted in partial fulfilment of

requirements for the degree of

Bachelor of Technology

by

Shubham Lohiya (150102064)

Shubham (150102079)

Under the guidance of

Dr. Kannan Karthik

Associate Professor,

Department of EEE, IIT Guwahati

DEPARTMENT OF ELECTRONICS & ELECTRICAL ENGINEERING

INDIAN INSTITUTE OF TECHNOLOGY GUWAHATI

April 2019

CERTIFICATE

This is to certify that the work contained in this thesis entitled

Face Anti-Spoofing Architectures

is the work of

Shubham Lohiya and Shubham

(Roll No. 150102064 and 150102079 respectively)

for the award of the degree of Bachelor of Technology, carried out in the Department of Electronics and Electrical Engineering, Indian Institute of Technology Guwahati under my supervision and that it has not been submitted elsewhere for a degree.

_____

Guide

Date: _____

Place: _____

DECLARATION

The work contained in this thesis is our own work under the supervision of the guides. We have read and understood the “B. Tech./B. Des. Ordinances and Regulations” of IIT Guwahati and the “FAQ Document on Academic Malpractice and Plagiarism” of EEE Department of IIT Guwahati. To the Best of our knowledge, this thesis is an honest representation of our work.

_____

Author

Date: _____

Place: _____

Acknowledgements

We would like to express our deepest and most sincere gratitude to our supervisor, Dr. Kannan Karthik, for his invaluable guidance, support and encouragement. His vast experience and deep understanding of subject proved to be immense help to us, and also his profound viewpoints and extraordinary motivation enlightened us in many ways. The freedom and the relaxed environment that he gave motivated us a lot. We would like to express our sense of gratitude to all the faculty members for their help, encouragement and for the deep insights given through the various courses they had taught.

We would like to express our sincere thanks to our seniors and other research scholars, with whom we had several useful discussions. We have also benefitted a lot from our classmates and friends throughout the entire course of study who helped us in many ways to proceed and whose presence somehow perpetually refreshed and memorable for giving us such a pleasant time in IITG. Their critical feedbacks and healthy discussions encouraged us to think. Our grandparents, parents, brother and sister were always there to support us. Their love and confidence gave us the courage to fight it out.

SHUBHAM (150102079)

SHUBHAM LOHIYA (150102064)

IIT Guwahati

April, 2019

Contents

List of Figures

Nomenclature

SVM	Support Vector Machine
LBP	Local Binary Pattern
t-LBP	Transitional Local Binary Pattern
IQA	Image Quality Assessment
IDA	Image Distortion Analysis
CASIA	Chinese Academy of Sciences Institute of Automation
NR	Non Referential
SVDD	Support Vector Data Description
RBF	Radial Basis Function
RGB	Red Green Blur
HSV	Hue Saturation Value

Abstract

Facial anti-spoofing has been essential in recent times, with the natural integration of biometric-based access control systems, either based on fingerprint or face in smart phones. The same anti-spoofing frame (implemented at a slightly advanced level), is also required in unmanned surveillance stations to detect the presence of disguises or prosthetics deployed by illegal traffickers to avoid being snapped by hidden cameras. In this work, we have modified & integrated existing techniques for face recognition in order to achieve the task of real/spoof image classification. This work consists of three modules namely:

[1] Image Quality Assessment (IQA) exploiting the sharpness profile of the input image consisting of pixel-difference, similarity and edge based measures

[2] Local binary pattern (LBP) and transition-Local binary pattern (t-LBP) histograms (8 bins) exploits the textural features of an input images. We extract the histograms of both the above mentioned patterns and concatenate them to form 16 dimensional feature vector. These features (LBP & t-LBP) complement each other and helps in order to achieve a better classification result.

[3] Image Distortion Analysis (IDA) is based on five different features – specular reflection, blurriness, chromatic moment, colour diversity and the farthest neighbour histogram.

The experimental results, obtained on publicly available CASIA face anti-spoofing dataset showed classification accuracy of 96% for the first module (NR face anti-spoofing approach), an accuracy of 89% for the second module (NR face anti-spoofing approach) and an accuracy of 84% (average accuracy of one-class Linear Kernel SVM for 14 different individuals, referential or person-specific face anti-spoofing approach) for the third module. The results exhibited in this work proves that the examination of the quality of genuine face images uncovers profoundly significant data that might be proficiently used to separate them from spoofed images. Due to the computational simplicity of these modules, makes it appropriate for real-time applications.

Problem Statement

There are two modes in which anti-spoofing can be performed:

1. Identity independent setting in which the anti-spoofing algorithm has no prior idea regarding the subject in the facial snapshot or video presented to the camera.
2. Reference based anti-spoofing wherein a person may claim to be someone else by presenting a prosthetic of that individual's face. Here, the anti-spoofing system has prior information (pre-stored genuine images available) regarding the subject who may have been impersonated.

The identity independent problem is less challenging from a technical viewpoint as compared to the reference based anti-spoofing problem. In the case of the latter, one has to deliberately ignore recognition based features and focus on "condition/acquisition-specific features" to detect some form of spoofing.

In our problem, we propose to develop a reference based anti-spoofing system for a closed unmanned authentication system, implemented for an organization. Natural full frontal poses under different lighting conditions will be stored in the database for different subjects. When a person presents his face (natural or disguised as someone else) to the camera, claiming to be subject-X, multiple snapshots will be taken and then a naturalness check will be done by comparing the test-snapshots with the pre-stored natural facial images of that specific subject-X.

Once the base-feature set for anti-spoofing is designed and calibrated, the problem becomes tantamount to an outlier detection algorithm, assuming that there is sufficient information in the database to learn the statistical model for subject-specific naturalness (from the point of view of the face). 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 one-class SVM and other anomaly detection algorithms will be explored.

Introduction

Spoofing attack is the act of outwitting a biometric sensor by presenting a counterfeit biometric evidence of a valid user. Face spoofing attacks are attempted in 3 major ways:

1. Print/Photo Attack: The attacker uses the victim's photo and display it using digital device or in printed form to outwit the biometric sensor.
2. Replay/Video Attack: The attacker uses a looped video of the victim's face and display it using digital device to outwit the biometric sensor.
3. 3-D Mask/Prosthetic Attack: The attacker uses a mask of the victim's face to outwit the biometric sensor.

These attacks have been mentioned in increasing order of their sophistication.

Attacks that involve showing of a image on a 2D device or a planar surface can easily be learned by classifier as these type of spoofs boils down to image manipulation.

We proposed face anti-spoofing architectures for both non-referential and referential i.e. person-specific face anti-spoofing approach. Previously, we have worked on image quality assessment and textural features such as LBP and its variant for the purpose of non-referential face anti-spoofing architecture. In this case, we used publicly available face spoof database CASIA, we divided the whole database into two class of genuine and spoof images and performed binary classification using above mentioned anti-spoofing techniques as features for Linear SVM.

In this work, we have built a referential i.e. person-specific face anti-spoofing architecture. We studied various image distortion analysis algorithms which is useful in catching the intrinsic distortions in print attacks with respect to genuine facial images. We have used the same CASIA database containing genuine and spoof images for 14 different individuals. We assumed to have only the genuine facial images at the time of training. Hence, problem becomes an anomaly detection problem. We used one-class Linear SVM in order to tackle this problem.

Literature Survey

Methodology - 1 (Involving Image Quality Assessment)

In our solution, the original image is compared with an image processed with Gaussian filter having certain variance. Further, image quality measures are extracted from the given image that form the feature vector for the corresponding image. SVM classifier is trained using the computed feature vector and the label provided to the training example. Now given a query image, image quality measures are used to generate feature vector which is used against the trained SVM model. The trained SVM will classify the given query image as either a real face or a spoof i.e. binary classification.

The chosen image quality measures/features intent to estimate the appearance of the image in an objective and reliable way.

The deployed method operates on the complete image without searching for any specific characteristics and hence it doesn't require any pre-processing steps such as eye detection, face detection, etc. prior to the calculation of proposed features.

The image quality measures that have been considered in the work can be categorized into 3 disjoint groups based on the image information measured.

1. Pixel Difference Measures: These measures captures the distortion between two images based on their pixel-wise differences.
2. Correlation Based Measures: These measures captures the similarity between the two images using different variants of the correlation function.
3. Edge Based Measures: These measures are used to capture the 2 most important visual features of the image, namely corners and edges that play a key role for identification & characterization in human visual system.

The full-reference image quality measures used can be found in [7].

Methodology - 2 (Involving Linear Binary Patterns)

Visual inspection of the image of a real user and spoofed image of the user look very similar but if we translate the given image to proper feature space then some disparities many become evident. We have tried to capture the texture properties of the image with features based on Local Binary Patterns (LBP).The simplest Local Binary Pattern for a particular pixel is usually denoted as LBP^{3X3} and is formed by comparing the intensity values of that pixel with the intensity values of the pixels in its 3x3 neighbourhood. In this way, each pixel is assigned a label with value from 0 to 2^8-1. In the case of uniform Local Binary Pattern (LBP^{u2}), only the labels which contain at most two 0-1 or 1-0 transitions are considered. The

feature vector of an image or a region/section of the image is formed by calculating a histogram of the pixel labels. One other strong motivation for using LBP is it's illumination invariant property i.e. robustness of LBP to monotonic grey-scale changes.

There are two ways in which we can capture the texture feature for an image. These are as follows:

1. The first option would be to compute the LBP feature for all the pixels in the image and put them in one histogram where bins in histograms would be equal value ranges between 0 to 2^8-1. The votes for different ranges in the histogram formed will be denoting our final feature vector.
2. The second option would be to divide the image into K*K blocks and computing the LBP feature for each of the blocks separately. Finally, concatenating the per block computed features to obtain our final feature vector.

In this work, we have considered the first method to generate the LBP histogram for the entire input images. In addition to LBP, we have also adopted another modification to LBP i.e. transition LBP (t-LBP), which acts as a complementary feature to the computed LBP feature. It can be viewed as a data about the partial ordering of border pixels. Additionally, t-LBP too enjoys the benefit of being illumination invariant.

The various formulations of LBP used can be found in [8].

Methodology - 3 (Involving Image Distortion Analysis)

In this method, we have explored features 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. As the colour reproduction process is not exact, so we can exploit this cause to our case.

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 ($\mathbf{I_d}$) and specular reflection ($\mathbf{I_s}$) components. The specular reflection component of the image is separated. Then the specular intensity distribution is portrayed in terms of three dimensional vector with the first component being specular pixel percentage, the second component being mean intensity of specular pixels and the third component being variance of specular pixel intensities. More is the specular component in a given query image, more are the chances of the image being the spoofed one. This can be stated as the specular component of a recaptured image during print attacks and screen in screen attacks is result of superposition of the specular component from the first capture and that from the recaptured image. Hence, this may result in differentiating spatial distribution as stated in [2].

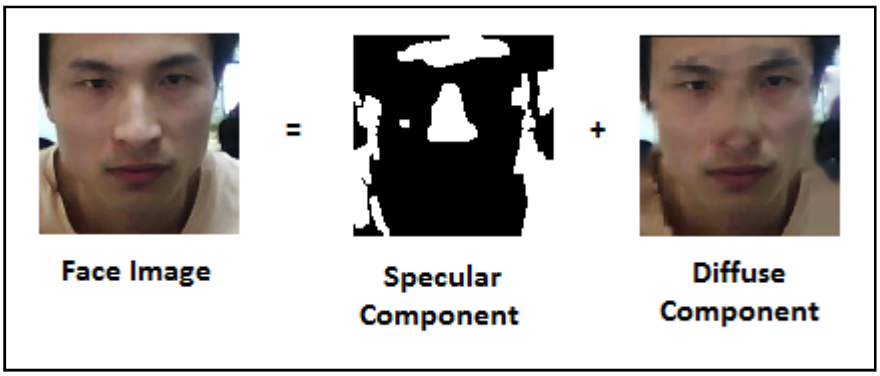

Figure 1: Decomposition of face image into its specular and diffuse components

Blurriness: Image appears blurry when the values of its high special frequency components are attenuated. Various types of blurs occur due to different reasons:

1.Motion blur – Blur due to relative motion between the scene and camera.

2.Blur due to image processing operations – Blur may find its way into image while performing compression operation.

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]. Any component of this spread can be measured i.e. either the horizontal or vertical component.

The spoofed faces are mostly defocused because of the recapturing process via mobile cameras. The prominent reason being the finite size of spoofing medium (screen attack, printed attack), hence the attacker has to place the camera near the spoofing medium to hide the boundaries of the same. So, the image blur due to defocus can be used as a key characteristic of a spoofed image.

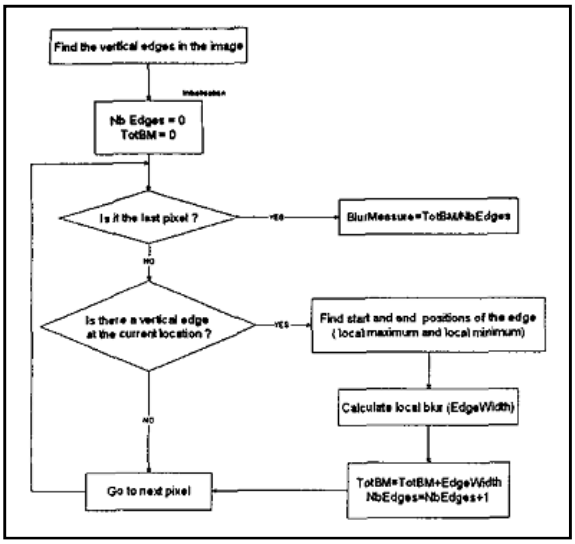

Figure 2: Blurriness measure algorithm

Firstly, an edge detection algorithm is deployed to find (let's say the horizontal) edges in the image. Then each column of the image is scanned for the pixels corresponding to the edge location. The starting and ending points of the edge is defined as the local minima and maxima locations in the vicinity of the edge. The difference between the starting location and the ending location of the edge is taken as the local blur measure for the given edge location. To obtain the overall blur measure of the image, we average the local blur values at all the edge locations.

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 convert the standard image in RGB (Red, Green, Blue) space into HSV (Hue, Saturation, Value) space. And then the first order moment i.e. mean, the second order central moment i.e. variance and the third order central moment i.e. skewness of each of the channel is calculated. We are also using the percentage of pixels in minimum and maximum histogram bins. These 5 values for each of the three channels is used as a 3*5=15 dimensional feature vector. We expect that these statistical measures of all the 3 channels i.e. Hue, Saturation and Value will be able to capture the disparity between spoof and genuine images because of the richer colour profile of genuine images.

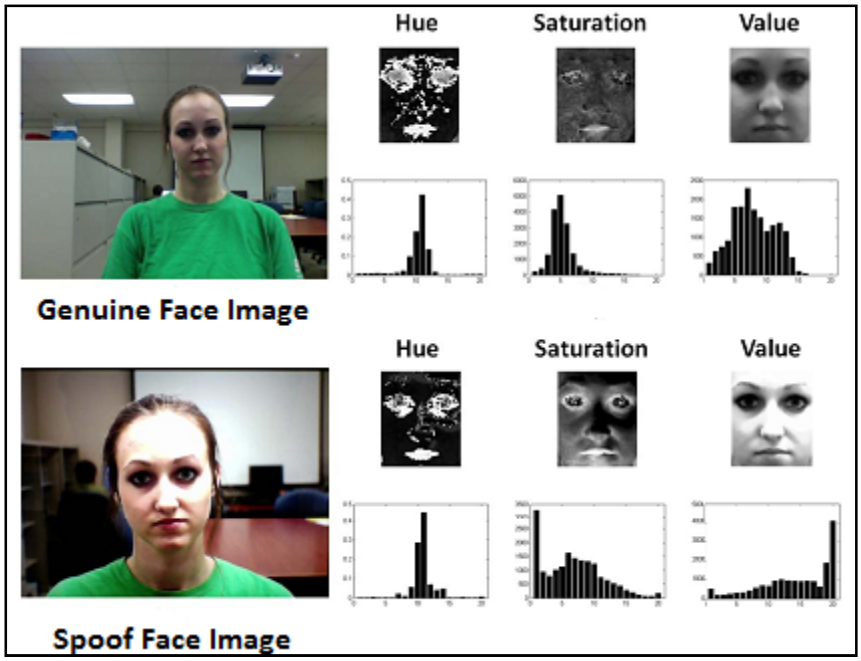

Figure 3: Histograms of HSV components of genuine and spoof face images

Colour Diversity: Genuine image have a richer colour profile as compared to spoofed images. Again the reason of fading colour in spoofed images is because of colour reproduction loss during recapture process as stated in [4]. We construct the histogram of all the colours involved in the image and pick the occurrence frequency of top N (here 100) colours. Also number of colours participating in the histogram is also considered. Here we

make use of the concept of 3-D histogram where each of the 3 channel is quantized by a fixed constant length. Let's say we take a bin length of 8 then this will imply 256/8=32 bins in each dimension. Hence, we will have a 32^3 bins in total. This bin length can be changed and therefore number of bins will also change. If we take bin length to be very small then this may lead to capturing of noise and unwanted information whereas if increase bin length to be very large then we lose a lot of minor information and are left with just coarse features. This implies a trade off between the bin size and the complexity of the feature.

Farthest Neighbour Histogram: Farthest neighbour of a given pixel is calculated out of the 4 adjacent neighbours of a given pixel and an appropriate distance metric which in our case is the L1 colour distance between pixels as stated in [5]. Notice that maximum L1 colour distance between 2 pixels can be 255*3 = 765. We calculate a 765-dimensional histogram where i'th entry will indicate the fraction of pixels having farthest neighbour distance equal to i in the given image. Since we cannot use a 765-dimensional histogram as whole for classification task due to computational inefficiency, hence we have computed statistical measures of colour histogram such as mean, standard deviation, skewness, kurtosis. Hence, this feature will in turn help us to encapsulate the idea of colour aberration. For spoofed images, we expect that the variance of the colour distance histogram will have a greater value than the variance of colour distance histogram for genuine images due to the incorporation of noise during recapture process. Mean, skewness and kurtosis captures information from the histogram which complements the variance measure.

Support Vector Machine

Support Vector Machine (SVM) is a discriminative classifier. The hyper-plane is drawn such that the distance between the support vectors and the hyper-plane is as maximum as possible. This means the drawn hyper-plane best splits the data. It draws a optimal hyper-plane i.e. a hyper-plane with maximum margin. This built hyper-plane is used to classify new points that are queried against the learned SVM model.

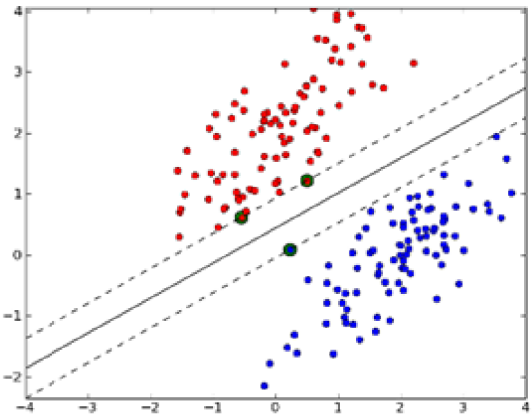

Figure 4: Example of Binary Classification using SVM

Points marked from red ink belong to class A and the points marked with blue ink belong to class B. The green points shown in the figure are the support vectors for the drawn optimal hyper-plane separating class A from class B. Perpendicular distance of the dotted line from the bold black line, i.e. the hyper-plane is called margin.

SVM is constrained optimization problem which in one way can be solved by Lagrange Multipliers technique.

$$\text{minimize:} \quad W(\alpha) = -\sum_{i=1}^{\ell} \alpha_i + \frac{1}{2} \sum_{i=1}^{\ell} \sum_{j=1}^{\ell} y_i y_j \alpha_i \alpha_j \mathbf{x}_i \mathbf{x}_j$$

$$\text{subject to:} \quad \sum_{\substack{i=1 \\ 0 \le \alpha_i \le C}}^{\ell} y_i \alpha_i = 0 \qquad (4)$$

SVM can easily be used for 2 class classification. Also, it can be extended for multi- class classification by using one vs rest classification scheme.

If we can transform our given set of data points to higher dimension the there is a chance that we can separate different classes in our data in higher dimension which in lower dimension was non-separable. For SVM to be trained for that higher dimension, we don't need the exact transformation of our data but we just need the inner product of our data in that higher dimensional space. It is quite tough to get the exact transformation of our data as compared to just the inner product of our data in higher dimension. This process of using the inner products of our data points and surpassing the process of exact transformation of data in higher dimension is termed as the 'Kernel trick'.

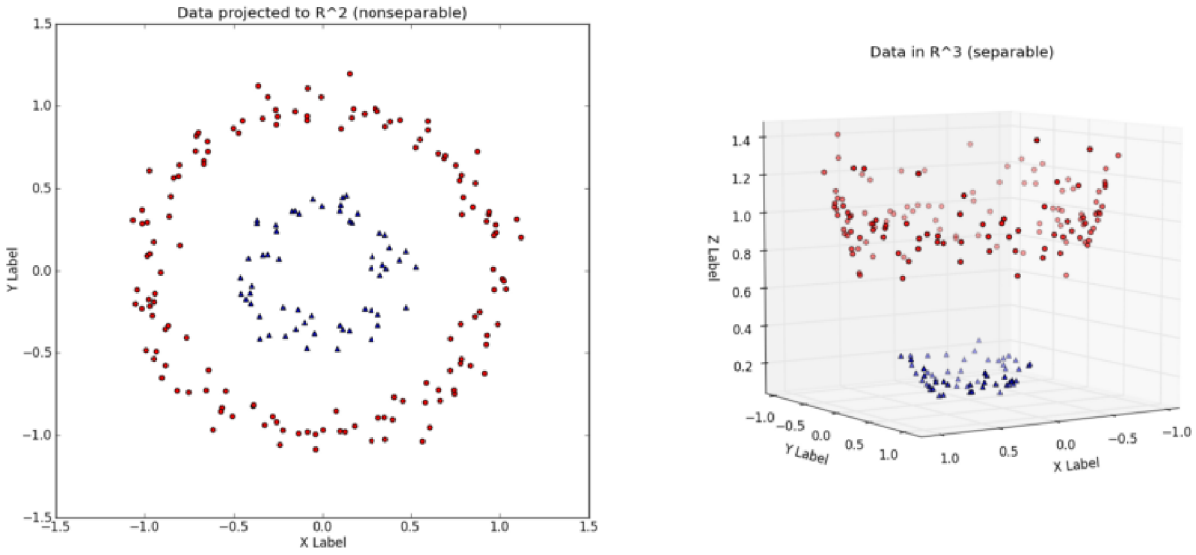

Figure 5: 2D linearly inseparable data points projected to 3D space using kernel

Various types of kernels are available for SVM. For example:

1. Polynomial Kernel
2. Gaussian Kernel
3. Laplace RBF Kernel
4. Sigmoid Kernel

One-class SVM (SVDD - Support Vector Data Description)

The method of support vector data description tries to obtain a spherical boundary in feature space around the training data.

Support vector data description can be used for outlier detection - to detect unobvious behaviour from certain points in dataset. Outlier show unacceptable large or low values in comparison to other data points.

Support vector data description can also be used for classification where one of the two classes is under-sampled. Just for example, the unusual low and high current values shown by a machine just before and during faulty behaviour. As this faulty behaviour simulation may become too expensive in some scenarios and may be unsimulatable in other. Hence we will have very less samples for time just before and during faulty behaviour. SVDD can be put to use in these cases.

Support vector data description can also be used for comparison of datasets. When a classier is very expensive to train and we have multiple options of datasets to train it further then a quality assessment can be done using SVDD for choosing a better dataset.

We have one-class SVM of two types mainly:

1. Linear Case (LOC-SVM): In this classification scheme, we assume that the positive class forms a cluster, hence the algorithm tries to fit a hyper-sphere to include the training data points with outlier detection. For example, it tries to fit a circle in 2D dimension to include most positive data points while leaving few as outliers.

2. Non-linear Case Using Kernel (KOC-SVM): In feature space, we cannot always assume the training data points to form a cluster, they can have complicated non-linear distributions. Kernel-based one-class SVM can be used to tackle such cases.

Further information regarding one-class SVM can be found in [6].

Experimental Setup

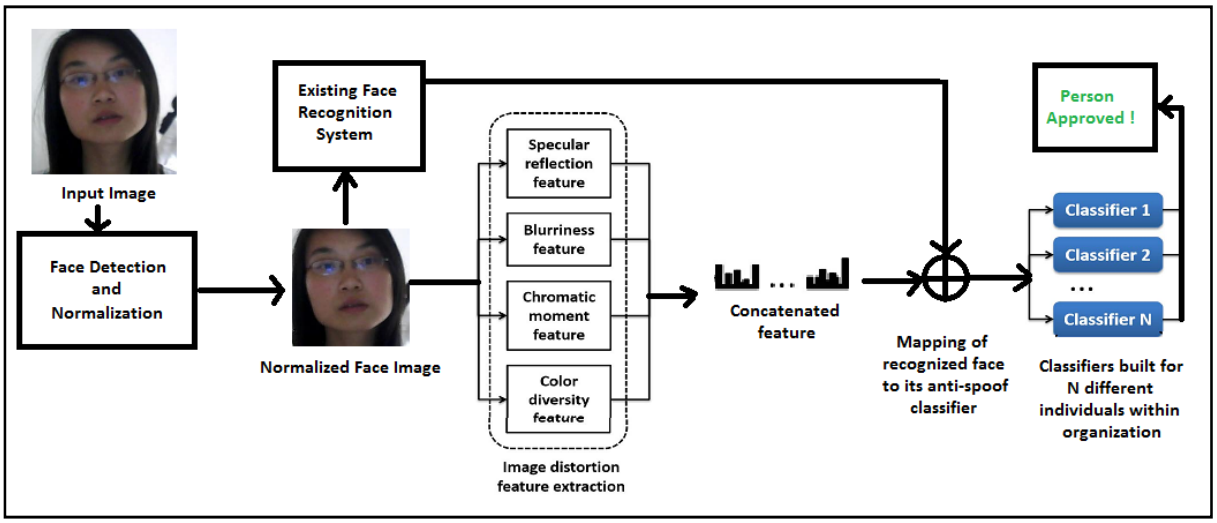

Figure 6: Person-Specific Face Anti-Spoofing Architecture using IDA features

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. At first, a 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 the organization and the 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 the organization, a separate face anti-spoofing classifier will be built. During training phase, it is assumed that only the genuine face images are available to us. Genuine face images for each individual is divided into 80:20 train-test split. Image distortion analysis features are computed for genuine face images and concatenated to form a 124-dimensional feature vector for each train image. 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). For the classification task, one class Linear SVM classifier is used. (Refer Literature Survey)

For each of the 14 individuals, classification report is prepared consisting of number of genuine and spoof facial images, number of train and test images, classification score of one-class Linear SVM classifier for each of the five IDA features separately, and for concatenated IDA feature.

In addition to this, confusion matrix is also added of one-class Linear SVM for concatenated IDA feature. Finally, an overall (average) classification report is stated for anti-spoofing framework.

CASIA Spoof Database

Figure 7: Genuine face images of 14 different individuals of CASIA database

Figure 8: Spoof face images of 14 different individuals of CASIA database

The results mentioned in the following pages for each person is in order as per above database face images, first from left to right (1st row), i.e. Person 1-7, then from left to right (2nd row), i.e. Person 8-14. Refer the results accordingly.

Results

Person 1

- Number of Train samples: 199 genuine samples (80:20 train-test split)
- Number of Test samples: 50 genuine samples + 614 spoof samples

Feature Type (One-Class Linear SVM)	Specular Reflection	Blurriness Measure	Chromatic Moment	Colour Diversity	Farthest Neighbour Histogram	Concatenated IDA features 124-dimension
Accuracy (%age)	93.82	90.21	65.81	36.44	7.07	73.94

Confusion Matrix (One-class Linear SVM for 124-dimension concatenated IDA feature)		
Classified as:	**Genuine Images**	**Spoof Images**
Genuine Images	**48**	**2**
Spoof Images	**171**	**443**

Person 2

- Number of Train samples: 45 genuine samples (80:20 train-test split)
- Number of Test samples: 12 genuine samples + 609 spoof samples

Feature Type (One-Class Linear SVM)	Specular Reflection	Blurriness Measure	Chromatic Moment	Colour Diversity	Farthest Neighbour Histogram	Concatenated IDA features 124-dimension
Accuracy (%age)	94.04	98.06	71.17	6.92	2.41	87.92

Confusion Matrix (One-class Linear SVM for 124-dimension concatenated IDA feature)		
Classified as:	**Genuine Images**	**Spoof Images**
Genuine Images	**10**	**2**
Spoof Images	**73**	**536**

Person 3

- Number of Train samples: 90 genuine samples (80:20 train-test split)
- Number of Test samples: 23 genuine samples + 603 spoof samples

Feature Type (One-Class Linear SVM)	Specular Reflection	Blurriness Measure	Chromatic Moment	Colour Diversity	Farthest Neighbour Histogram	Concatenated IDA features 124-dimension
Accuracy (%age)	88.66	89.13	93.13	67.41	98.88	80.19

Confusion Matrix (One-class Linear SVM for 124-dimension concatenated IDA feature)		
Classified as:	**Genuine Images**	**Spoof Images**
Genuine Images	**20**	**3**
Spoof Images	**121**	**482**

Person 4

- Number of Train samples: 544 genuine samples (80:20 train-test split)
- Number of Test samples: 137 genuine samples + 608 spoof samples

Feature Type (One-Class Linear SVM)	Specular Reflection	Blurriness Measure	Chromatic Moment	Colour Diversity	Farthest Neighbour Histogram	Concatenated IDA features 124-dimension
Accuracy (%age)	48.05	73.02	67.78	62.55	16.91	74.76

Confusion Matrix (One-class Linear SVM for 124-dimension concatenated IDA feature)		
Classified as:	Genuine Images	Spoof Images
Genuine Images	123	14
Spoof Images	174	434

Person 5

- Number of Train samples: 152 genuine samples (80:20 train-test split)
- Number of Test samples: 38 genuine samples + 595 spoof samples

Feature Type (One-Class Linear SVM)	Specular Reflection	Blurriness Measure	Chromatic Moment	Colour Diversity	Farthest Neighbour Histogram	Concatenated IDA features 124-dimension
Accuracy (%age)	98.42	38.39	99.36	26.54	5.68	92.25

Confusion Matrix (One-class Linear SVM for 124-dimension concatenated IDA feature)		
Classified as:	Genuine Images	Spoof Images
Genuine Images	34	4
Spoof Images	45	550

Person 6

- Number of Train samples: 584 genuine samples (80:20 train-test split)
- Number of Test samples: 146 genuine samples + 458 spoof samples

Feature Type (One-Class Linear SVM)	Specular Reflection	Blurriness Measure	Chromatic Moment	Colour Diversity	Farthest Neighbour Histogram	Concatenated IDA features 124-dimension
Accuracy (%age)	48.67	64.07	95.69	80.79	22.01	93.37

Confusion Matrix (One-class Linear SVM for 124-dimension concatenated IDA feature)		
Classified as:	Genuine Images	Spoof Images
Genuine Images	129	17
Spoof Images	23	435

Person 7

- Number of Train samples: 609 genuine samples (80:20 train-test split)
- Number of Test samples: 153 genuine samples + 605 spoof samples

Feature Type (One-Class Linear SVM)	Specular Reflection	Blurriness Measure	Chromatic Moment	Colour Diversity	Farthest Neighbour Histogram	Concatenated IDA features 124-dimension
Accuracy (%age)	77.17	72.69	78.23	48.81	19.12	94.72

Confusion Matrix (One-class Linear SVM for 124-dimension concatenated IDA feature)		
Classified as:	Genuine Images	Spoof Images
Genuine Images	141	12
Spoof Images	28	577

Person 8

- Number of Train samples: 98 genuine samples (80:20 train-test split)
- Number of Test samples: 25 genuine samples + 599 spoof samples

Feature Type (One-Class Linear SVM)	Specular Reflection	Blurriness Measure	Chromatic Moment	Colour Diversity	Farthest Neighbour Histogram	Concatenated IDA features 124-dimension
Accuracy (%age)	98.39	56.25	81.41	62.17	4.01	94.39

Confusion Matrix (One-class Linear SVM for 124-dimension concatenated IDA feature)		
Classified as:	Genuine Images	Spoof Images
Genuine Images	23	2
Spoof Images	33	566

Person 9

- Number of Train samples: 381 genuine samples (80:20 train-test split)
- Number of Test samples: 96 genuine samples + 439 spoof samples

Feature Type (One-Class Linear SVM)	Specular Reflection	Blurriness Measure	Chromatic Moment	Colour Diversity	Farthest Neighbour Histogram	Concatenated IDA features 124-dimension
Accuracy (%age)	25.23	89.71	96.44	97.38	39.43	98.31

Confusion Matrix (One-class Linear SVM for 124-dimension concatenated IDA feature)		
Classified as:	Genuine Images	Spoof Images
Genuine Images	88	8
Spoof Images	1	438

Person 10

- Number of Train samples: 60 genuine samples (80:20 train-test split)
- Number of Test samples: 16 genuine samples + 242 spoof samples

Feature Type (One-Class Linear SVM)	Specular Reflection	Blurriness Measure	Chromatic Moment	Colour Diversity	Farthest Neighbour Histogram	Concatenated IDA features 124-dimension
Accuracy (%age)	52.32	94.57	71.71	50.0	86.04	58.13

Confusion Matrix (One-class Linear SVM for 124-dimension concatenated IDA feature)		
Classified as:	Genuine Images	Spoof Images
Genuine Images	14	2
Spoof Images	106	136

Person 11

- Number of Train samples: 327 genuine samples (80:20 train-test split)
- Number of Test samples: 82 genuine samples + 303 spoof samples

Feature Type (One-Class Linear SVM)	Specular Reflection	Blurriness Measure	Chromatic Moment	Colour Diversity	Farthest Neighbour Histogram	Concatenated IDA features 124-dimension
Accuracy (%age)	21.55	89.35	87.01	94.28	20.0	90.9

Confusion Matrix (One-class Linear SVM for 124-dimension concatenated IDA feature)		
Classified as:	Genuine Images	Spoof Images
Genuine Images	73	9
Spoof Images	26	277

Person 12

- Number of Train samples: 348 genuine samples (80:20 train-test split)
- Number of Test samples: 87 genuine samples + 384 spoof samples

Feature Type (One-Class Linear SVM)	Specular Reflection	Blurriness Measure	Chromatic Moment	Colour Diversity	Farthest Neighbour Histogram	Concatenated IDA features 124-dimension
Accuracy (%age)	21.86	89.35	92.35	95.97	17.83	93.84

Confusion Matrix (One-class Linear SVM for 124-dimension concatenated IDA feature)		
Classified as:	Genuine Images	Spoof Images
Genuine Images	73	14
Spoof Images	15	369

Person 13

- Number of Train samples: 94 genuine samples (80:20 train-test split)
- Number of Test samples: 24 genuine samples + 380 spoof samples

Feature Type (One-Class Linear SVM)	Specular Reflection	Blurriness Measure	Chromatic Moment	Colour Diversity	Farthest Neighbour Histogram	Concatenated IDA features 124-dimension
Accuracy (%age)	20.29	99.25	91.33	40.09	62.87	56.68

Confusion Matrix (One-class Linear SVM for 124-dimension concatenated IDA feature)		
Classified as:	**Genuine Images**	**Spoof Images**
Genuine Images	**16**	**8**
Spoof Images	**167**	**213**

Person 14

- Number of Train samples: 170 genuine samples (80:20 train-test split)
- Number of Test samples: 43 genuine samples + 602 spoof samples

Feature Type (One-Class Linear SVM)	Specular Reflection	Blurriness Measure	Chromatic Moment	Colour Diversity	Farthest Neighbour Histogram	Concatenated IDA features 124-dimension
Accuracy (%age)	74.41	95.50	52.71	66.51	8.83	84.80

Confusion Matrix (One-class Linear SVM for 124-dimension concatenated IDA feature)		
Classified as:	**Genuine Images**	**Spoof Images**
Genuine Images	**35**	**8**
Spoof Images	**90**	**512**

Overall Classification Report

- The overall classification score for each classifier is computed as average of accuracy scores of classifiers for all 14 individuals.
- For the concatenated 124-dimension IDA feature, we get an accuracy of 84% on average over 14 individuals using one-class Linear SVM.

Feature Type (One-Class Linear SVM)	Specular Reflection	Blurriness Measure	Chromatic Moment	Colour Diversity	Farthest Neighbour Histogram	Concatenated IDA features 124-dimension
Accuracy (%age)	61.64	81.51	81.73	59.71	29.37	83.87 ≈ **84.0**

Conclusions

In this work, we have proposed a person-specific face anti-spoofing architecture for a closed unmanned authentication system, implemented for an organization. There are various types of face spoofing attacks such as print/photo attack, replay/video attack, 3D mask/prosthetic attack. We have mainly focussed on 2D print attacks as these type of spoofs generally boils down to image manipulation. In this project, we mainly focussed on feature design aspect of face anti-spoofing task in order to achieve a good classification scores. Various deep neural network architectures are published in recent years, in which feature design is an automated task and more emphasis is given to classification task. We studied about various textural features such as IQA (Image Quality Assessment), LBP (Local Binary Patterns) and its variants such as t-LBP for the purpose of binary classification using linear SVM between genuine and spoof face images without any reference. Further, we explored IDA (Image Distortion Analysis) features namely specular reflection, blurriness measure, chromatic moment, colour diversity and farthest neighbour histogram which is useful in catching the intrinsic distortions in print attacks with respect to genuine facial images. These 5 different IDA features are concatenated together to form a 124-dimensional IDA feature vector. At time of training, only genuine face images are available, hence the classification task becomes an anomaly detection problem. We used one-class Linear SVM for the classification task. We used publicly available CASIA spoof database as our base database. The database consists of genuine and spoof facial images of 14 different individuals. The classifier achieved an accuracy of around 84% (with 80:20 train-test split on genuine faces) on average sense. From the results, it can also be concluded that the features that contribute the most in achieving a higher classification score are blurriness measure and chromatic moment. At the time of testing an image presented to the system, it must be noted that 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 and further anti-spoofing task is performed.

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.