Biometric Systems
Lesson 8: Face recognition –Spoofing

Maria De Marsico
demarsico@di.uniroma1.it

SAPIENZA
UNIVERSITÀ DI ROMA

Dipartimento di Informatica

Outline

- Introduction: spoofing in biometrics
- Face spoofing
- Face antispoofing - Liveness Detection
- Face antispoofing at BIPlab

Outline

- **Introduction: spoofing in biometrics**
- Face spoofing
- Face antispoofing - Liveness Detection
- Face antispoofing at BIPlab

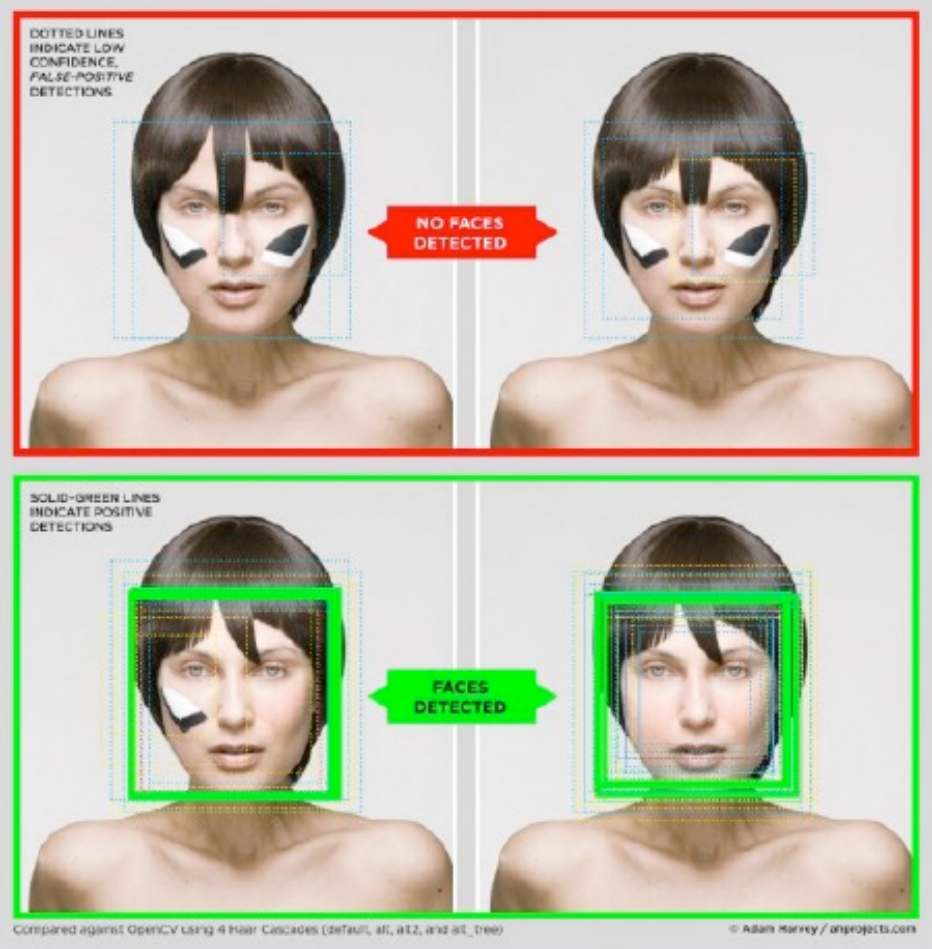
Spoofing

- In the context of **network security**, a **spoofing attack** is a situation in which one person or program successfully masquerades **as another** by falsifying data (IP address, e-mail address, etc.) thereby gaining an illegitimate advantage.

Biometric Spoofing

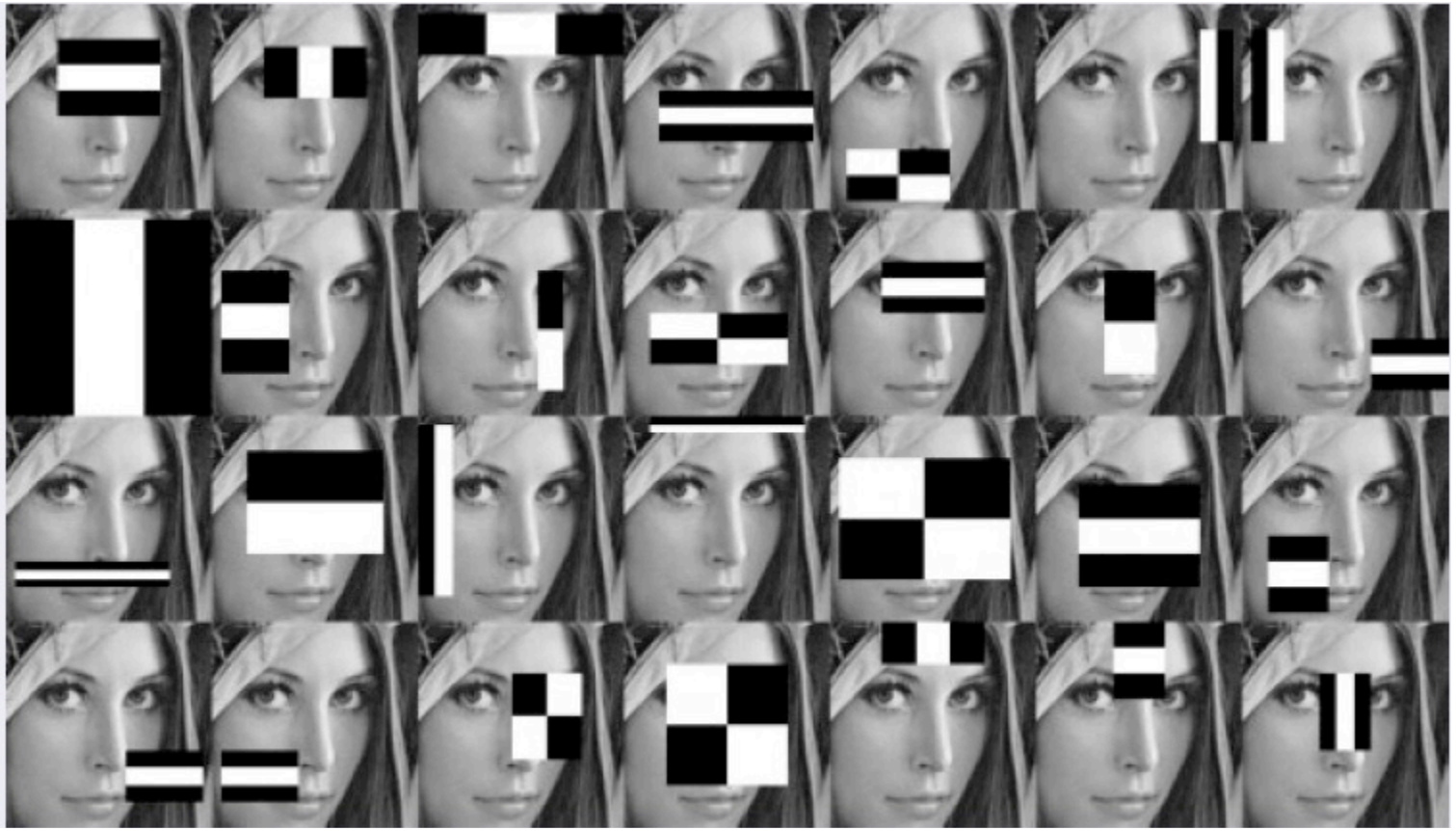
- **Biometric spoofing** is the act of fooling a biometric application, by using a copy or performing an imitation of the biometric factor identifying the legitimate subject.
- **Biometric spoofing** attack is carried out by presenting an artifact **biometric** trait to the system to fool it pretending **to be** a genuine user.
- **Camouflage** or **disguise** is a different problem: the attack is carried out presenting an artifact **biometric** trait to the system to fool it pretending **not to be** oneself.

Spoofing vs. Camouflage



CVDazzle. https://ahprojects.com/projects/cv-dazzle/

Spoofing vs. Camouflage



Viola-Jones popular face detector is especially affected, but it is not the only one …

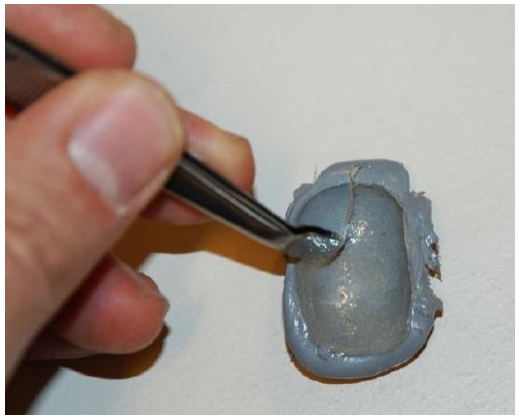
Spoofing vs. Camouflage

CV Dazzle Look

Spoofing vs. Camouflage

IIIT-Delhi Disguise Version 1 face database: http://www.iab-rubric.org/resources/facedisguise.html

Spoofing vs. Camouflage



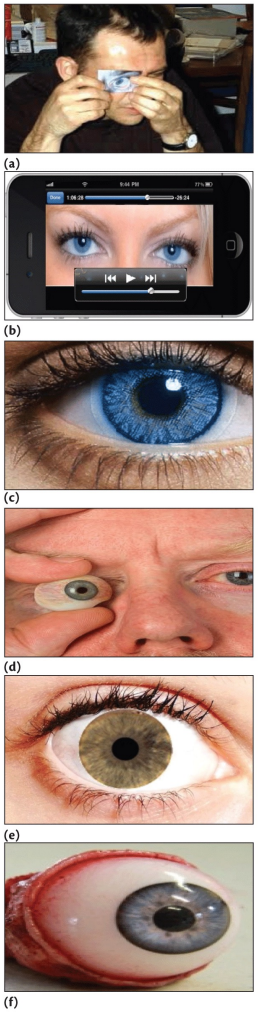
Spoofing

Camouflage

Spoofing vs. Camouflage

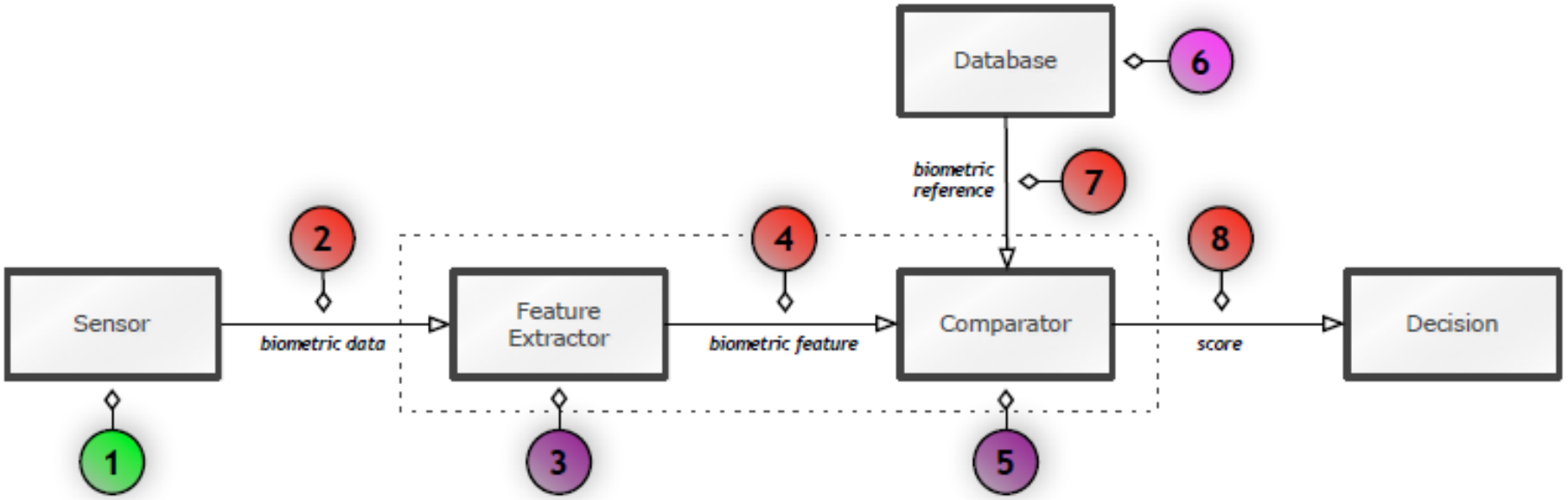
Spoofing

(a) a photograph, (b) a video,
(c) A printed contact lens,
(d) An artificial eyeball,
(e) a reverse-engineered iris image,
(f) a real eye removed from the genuine user'sbody.



Camouflage

Spoofing Attacks: where



Attacks can be:

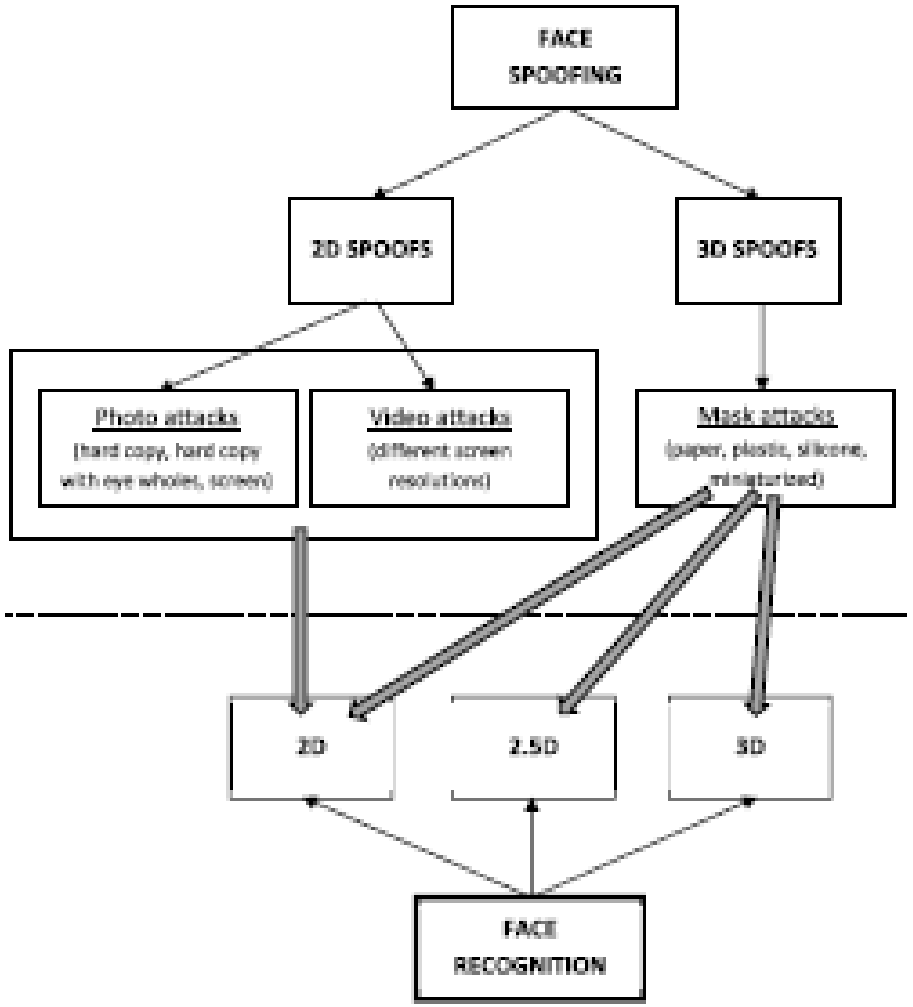
- **Indirect** (2-8): bypassing the feature extractor or the comparator (3, 5), manipulating the biometric references in the biometric reference database (6), exploiting possible weak points in communication channels (2, 4, 7, 8).
- **Direct** (1) - **spoofing attacks** also popular as **presentation attacks**

NK Ratha et al. Enhancing security and privacy in biometrics-based authentication systems, IBM Systems Journal, 40(3):614634, 2001

Outline

- Introduction: spoofing in biometrics
- **Face spoofing**
- Face antispoofing - Liveness Detection
- Face antispoofing at BIPlab

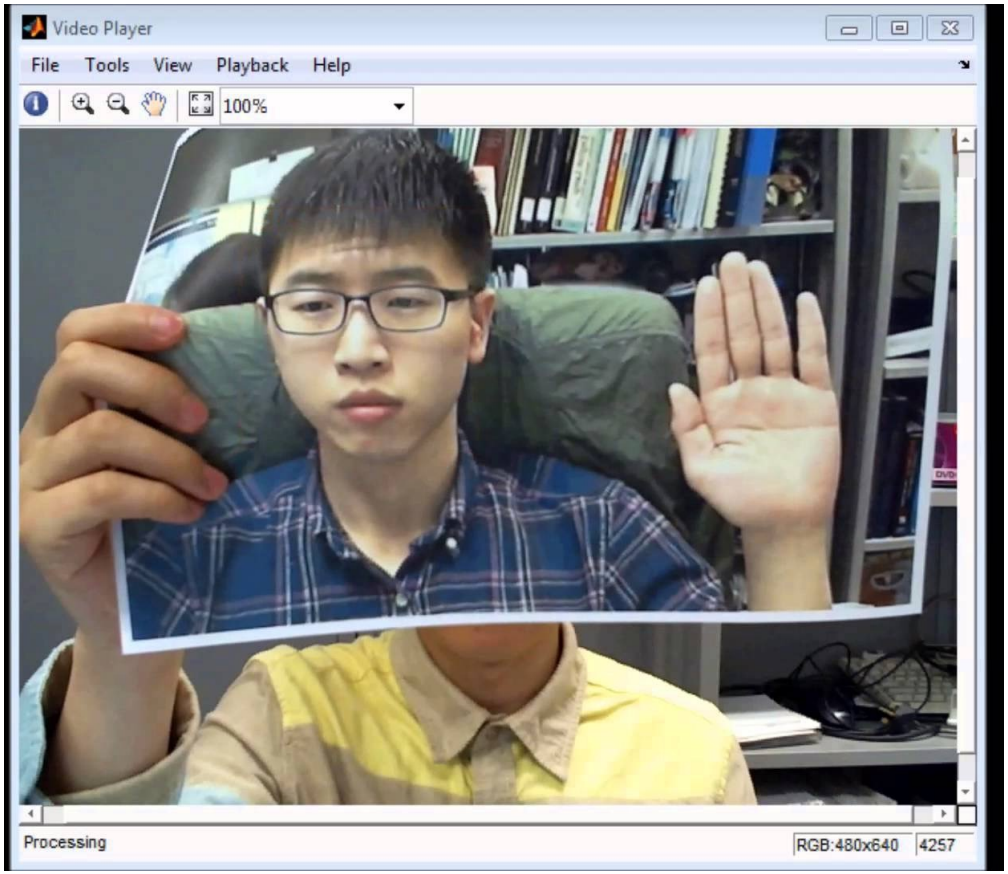
Spoofing classification



From: Galbally, J., Marcel, S., & Fierrez, J. (2014). Biometric antispoofing methods: A survey in face recognition. *IEEE Access*, *2*, 1530-1552.

Spoofing Attacks: how Biometric trait -dependent

2D face spoofing: print attack same with photo and video



2D face spoofing: reply attack

A video captured from the Internet and possibly used for a reply attack

Spoofing Attacks: how Biometric trait -dependent

NIR face spoofing print attack: camera with NIR illuminator and NIR sensor

row 1: NIR camera - row 2: VIS camera
real (left), print VIS (middle), print NIR (right)

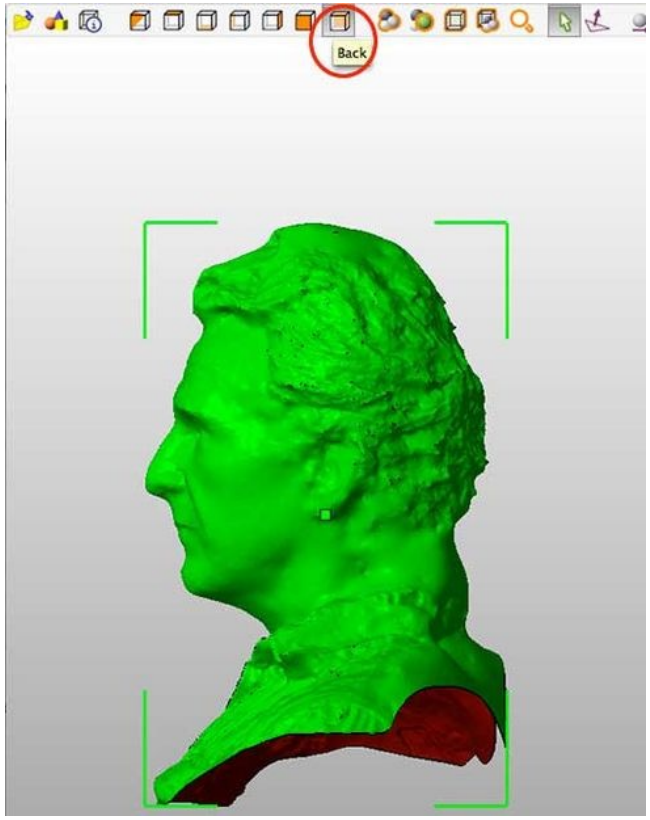
Spoofing Attacks: how Biometric trait -dependent

3D mask attack:
from laser scan (expensive) or from … photos
(http://www.instructables.com/id/Make-a-3D-Printed-Mask-from-Photos/)

Source photos
processed with **123D Catch online**
produces an exportable mesh

Spoofing Attacks: how Biometric trait -dependent

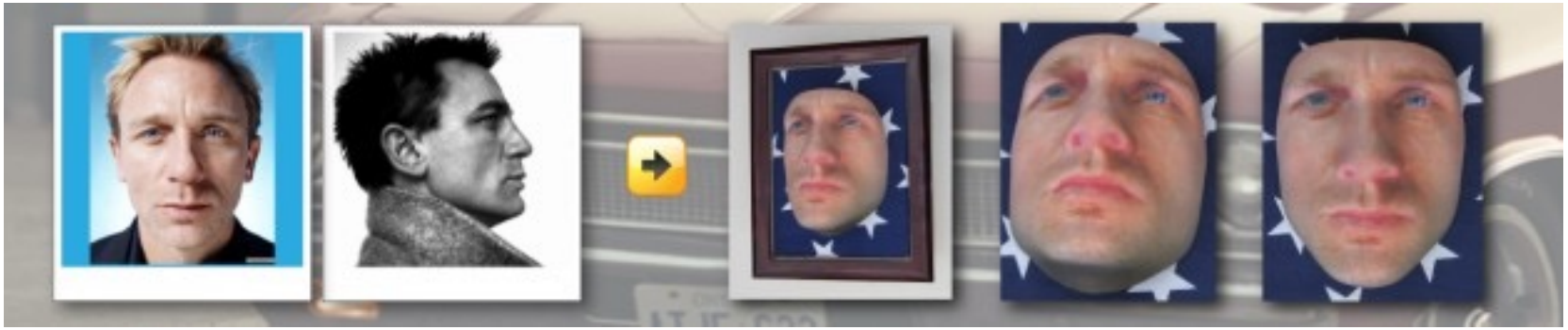
3D mask attack:
from laser scan (expensive) or from … photos
(http://www.instructables.com/id/Make-a-3D-Printed-Mask-from-Photos/)

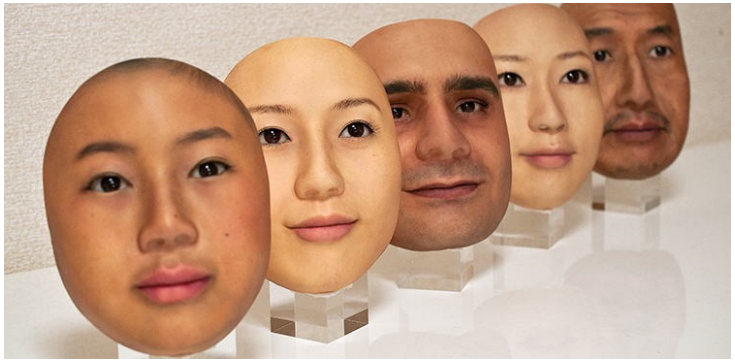


Export the editable mesh into **Netfabb Studio Basic** and after editing export to 3D printer

Spoofing Attacks: how Biometric trait -dependent

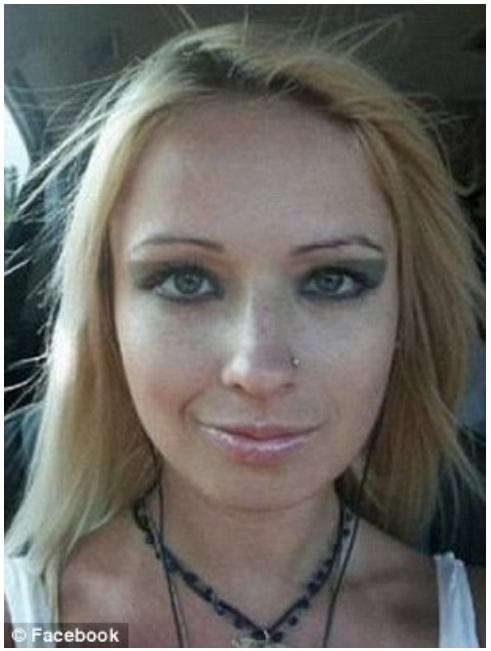
3D mask attack: easy to get a mask
Web service at http://www.thatsmyface.com/(one or two photos needed!) and
http://real-f.jp/en_news.html (photos front, left and right oblique at least; possible with face impression or 3D scan too for better results)





Spoofing Attacks: how Biometric trait -dependent

The last border: plastic surgery and/or make-up



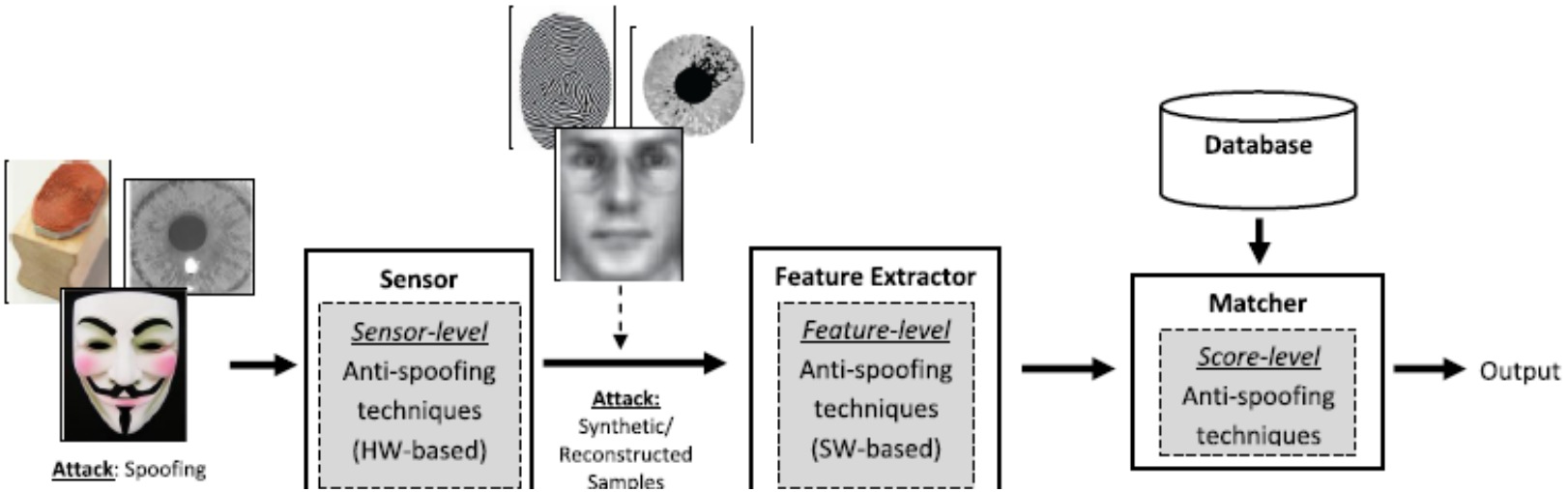
Daily Mail 13 November 2012
Valeria Lukyanova

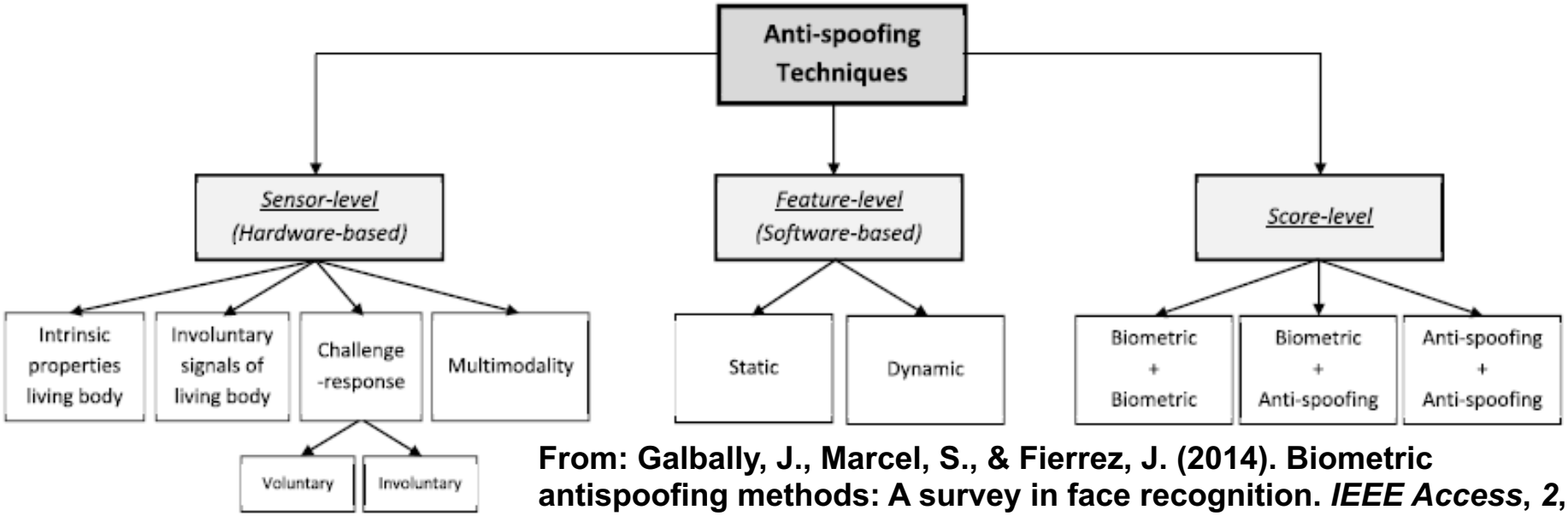
http://www.dailymail.co.uk/femail/article-2232466/Human-Barbie-Model-excessive-plastic-surgery-doll-like-shows-proportions-fashion-shoot.html

Outline

- Introduction: spoofing in biometrics
- Face spoofing
- **Face antispoofing - Liveness Detection**
- Face antispoofing at BIPlab

Antispoofing classification





From: Galbally, J., Marcel, S., & Fierrez, J. (2014). Biometric antispoofing methods: A survey in face recognition. *IEEE Access*, *2*, 1530-1552.

Liveness Detection

Main approaches for face

- Print attack (lower effort)
  - Texture
  - Shape
  - Movement
  - Sensor fingerprint
- Video (medium)
- 3D mask (highest … ?)

Note- 0-effort attack: the impostor presents his/her biometric trait without any attempt to couterfait it

Liveness Detection

2D Print Attack

- The essential difference between the live face and photograph is that a live face is a fully **three dimensional object** while a photograph could be considered as a **two dimensional planar structure**.

- Structure from motion can yield the depth information to distinguish a live person from a still photo.

- The disadvantages of depth information are that , it is hard to estimate depth information when **head is still**, and the estimate is very sensitive to **noise** and **lighting**.

- Optical flow can be computed on the input video to obtain the information of face motion for liveness judgment, but it is vulnerable to **photo motion** in depth and photo **bending**.

- A possible multimodal approach fuses face-voice against spoofing exploiting the lip movement during speech. This kind of method needs voice recorder

Liveness Detection - 2D Print Attack

Eye Blink

- Among the earliest approaches, it is possible to consider those relying on eye blinking analysis.
- Eyeblink is a physiological activity of rapid closing and opening of the eyelid.
- Blink speed can vary with fatigue, emotional stress, amount of sleep, eye injury, medication, or disease, but the spontaneous resting blink rate of a human being is nearly from 15 to 30 eyeblinks per minute (a blink every 2 to 4 seconds) and the average blink lasts about 250 milliseconds.
- A current generic camera can easily capture the face video with not less than 15 fps, i.e. the frame interval is not more than 70 milliseconds, therefore it can capture two or more frames for each blink when the face looks into the camera.

Liveness Detection - 2D Print Attack

Eye Blink

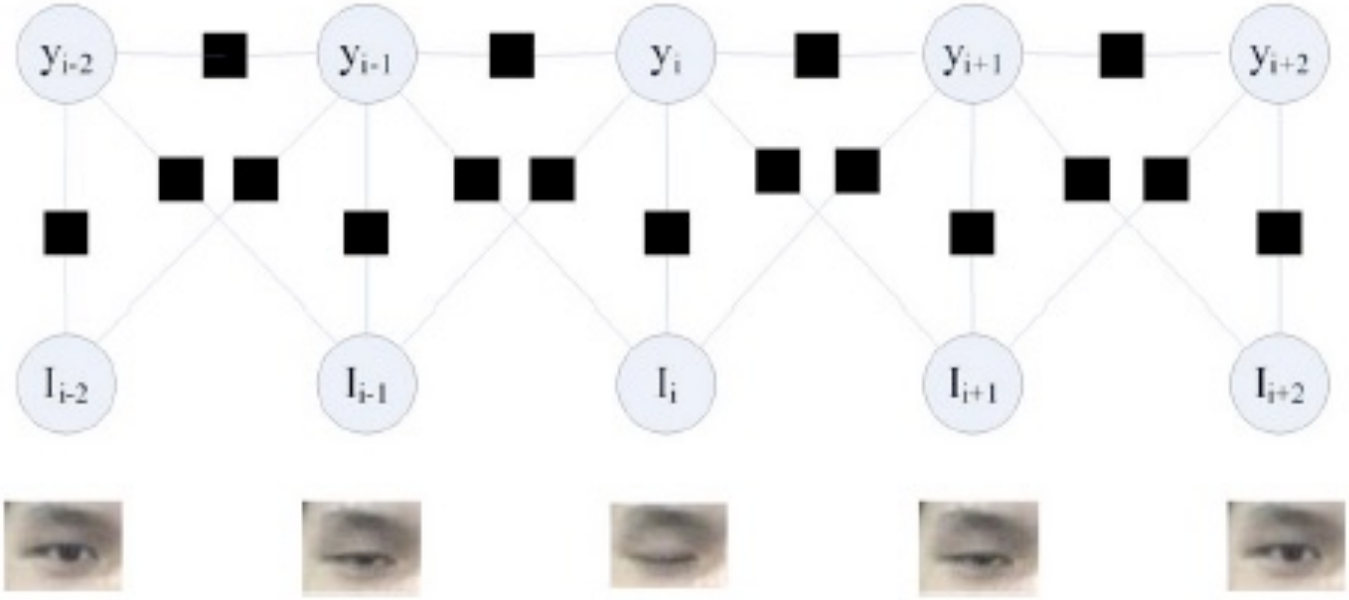
- The work by Pan et al. models eyeblink behaviors by an undirected Conditional Random Field framework, incorporated with a discriminative measure of eye states.
- An eyeblink activity can be represented by an image sequence S consisting of T images, where S = $\{I_i, i = 1, \ldots, T\}$.
- The typical eye states are *opening* and *closing*. In addition, there is an ambiguous state when blinking from open state to close or from close state to open.
- It is possible to define a three-state set for eyes, $Q = \{\alpha : open, \gamma : close, \beta : ambiguous\}$
- A typical blink activity can be described as a state change pattern of $\alpha \rightarrow \beta \rightarrow \gamma \rightarrow \beta \rightarrow \alpha$.
- Suppose that S is a random variable over observation sequences to be labeled, and Y is a random variable over the corresponding label sequences to be predicted, all of components yi of Y are assumed to range over a finite label set Q.
- Let $G = (V,E)$ be a graph and Y is indexed by the vertices of G. Then (Y, S) is called a *conditional random field (CRF)*, when conditioned on S, the random variables Y and S obey the Markov property w.r.t. the graph:

$$p(y_v|\mathrm{S}, y_u, u = v) = p(y_v|\mathrm{S}, y_u, u \sim v)$$

where $u \sim v$ means that u and v are neighbors in G.

Liveness Detection - 2D Print Attack

Eye Blink



An Adaboost training is used to characterize *eye closity*

Pan, G., Sun, L., Wu, Z., & Lao, S. (2007, October). Eyeblink-based anti-spoofing in face recognition from a generic webcamera. In *Computer Vision, 2007. ICCV 2007. IEEE 11th International Conference on* (pp. 1-8). IEEE

Liveness Detection - 2D Print Attack

Micro-texture

- The work by Määttä et al. Exploits LBP for micro-texture analysis.
- The proposal assumes that face prints usually contain **printing quality defects** that can be well detected using texture features.
- Human faces and prints **reflect light in different ways** because a human face is a complex non rigid 3D object whereas a photograph is a planar rigid object (different specular reflections and shades).
- The surface properties of real faces and prints, e.g. **pigments**, are also different.
- The work exploits **multi-scale local binary patterns** (**LBP**).
- As a further advantage, the texture features that are used for spoofing detection can also be used for face recognition.
- The vectors in the feature space are then fed to an **SVM classifier** which determines whether the micro-texture patterns characterize a live person or a fake image.

Määttä, J., Hadid, A., & Pietikäinen, M. (2011, October). Face spoofing detection from single images using micro-texture analysis. In *Biometrics (IJCB), 2011 international joint conference on* (pp. 1-7). IEEE.

Liveness Detection - 2D Print Attack

Micro-texture

- A live face and a face print in the original space and the corresponding LBP images (basic LBP).
- We can notice that the printed photo looks quite similar to the image of the live face whereas the LBP images depict some differences.
- Uniform LBP is used at different scales (different values of P=number of neighbours and R= window radius)

Määttä, J., Hadid, A., & Pietikäinen, M. (2011, October). Face spoofing detection from single images using micro-texture analysis. In *Biometrics (IJCB), 2011 international joint conference on* (pp. 1-7). IEEE.

Liveness Detection - 2D Print Attack

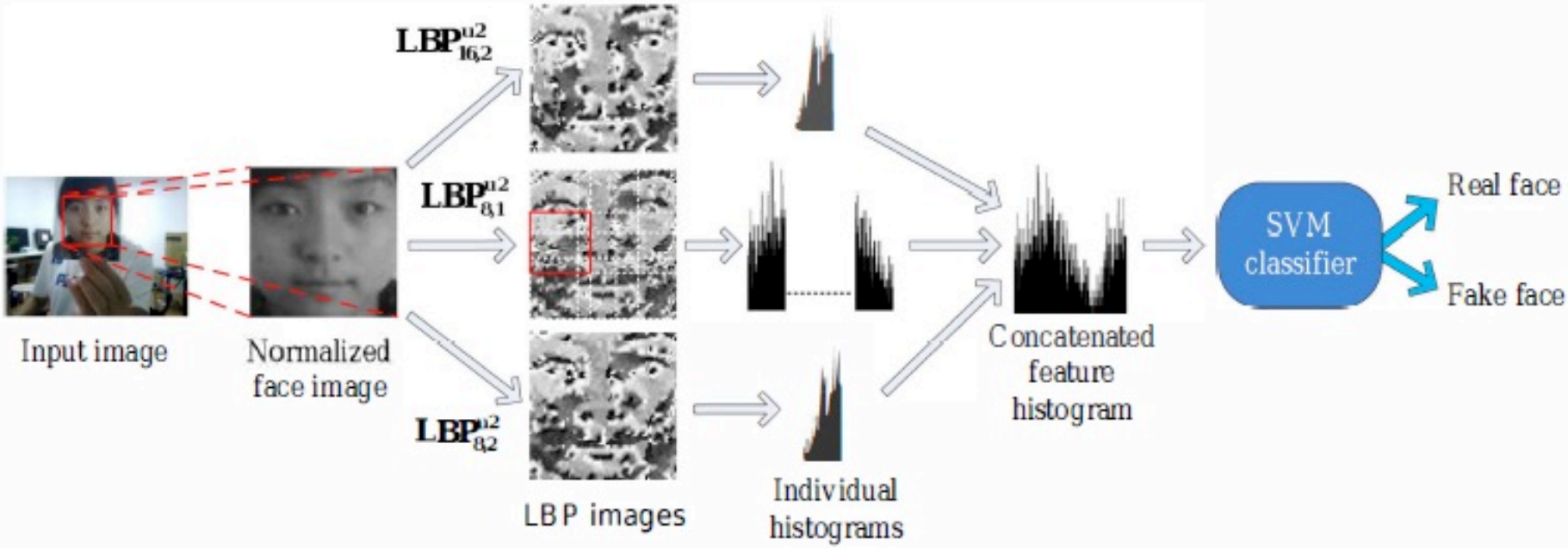
Micro-texture

- The face is first detected, cropped and normalized into a 64 x 64 pixel image.
- $LBP^{u2}_{8,1}$ operator is applied on the normalized face image and the resulting LBP face image is divided into 3 x 3 overlapping regions (with an overlapping size of 14 pixels).
- The local 59-bin histograms from each region are computed and collected into a single 531-bin histogram.
- Two other histograms from the whole face image are computed using $LBP^{u2}_{8,2}$ and $LBP^{u2}_{16,2}$ operators, yielding 59-bin and 243-bin histograms that are added to the 531-bin histogram previously computed.
- The length of the final enhanced feature histogram is 833 (i.e. 531 +59+243).
- An SVM classifier with radial basis function kernel is trained using a set of positive (real faces) and negative (fake faces) samples.

Määttä, J., Hadid, A., & Pietikäinen, M. (2011, October). Face spoofing detection from single images using micro-texture analysis. In *Biometrics (IJCB), 2011 international joint conference on* (pp. 1-7). IEEE.

Liveness Detection - 2D Print Attack

Micro-texture



Määttä, J., Hadid, A., & Pietikäinen, M. (2011, October). Face spoofing detection from single images using micro-texture analysis. In *Biometrics (IJCB), 2011 international joint conference on* (pp. 1-7). IEEE.

Liveness Detection - 2D Print Attack

Captured-Recaptured

- The work by Kose and Dugelay exploits a rotation invariant LBP variance (LBPV) based method together with a pre-processing step of Difference of Gaussian (DoG) filtering.
- The image of a photo is an image of a real face which passes through the camera system twice and the printing system once, it is in fact a recaptured image which has lower image quality compared to a real face image taken under same imaging conditions.
- DoG filter is used in a pre-processing step to obtain a special frequency band which gives considerable information to discriminate between real and photo images.
- A recaptured face image has less sharpness (lower image quality) when compared to captured face image; therefore recaptured image contains less high frequency components. This fact can be observed by analysing the 2D Fourier spectra of real face and photo face images.

Kose N. and Dugelay J.-L., “Countermeasure for the protection of face recognition systems against mask attacks,” in *Proc. IEEE Int. Conf. Autom. Face Gesture Recognit.*, Apr. 2013, pp. 1–6.

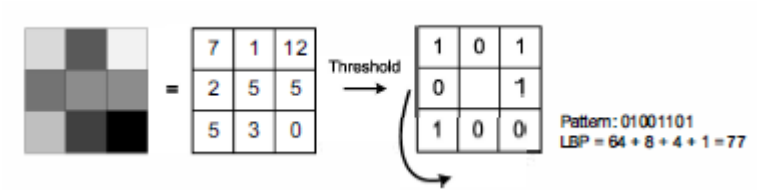
Liveness Detection - 2D Print Attack

Captured-Recaptured

$$LBP_{P,R} = \sum_{p=0}^{P-1} s(g_p - g_c)2^p,$$

$$s(x) = \begin{cases} 1 & x \geq 0 \\ 0 & x < 0 \end{cases}$$

LBP codes



$$H(k) = \sum_{i=1}^{X} \sum_{j=1}^{Y} f(LBP_{P,R}(i,j), k), \quad k = [0\ K]$$

$$f(x,y) = \begin{cases} 1 & x = y \\ 0 & else \end{cases}$$

LBP histogram

Kose N. and Dugelay J.-L., “Countermeasure for the protection of face recognition systems against mask attacks,” in *Proc. IEEE Int. Conf. Autom. Face Gesture Recognit.*, Apr. 2013, pp. 1–6.

Liveness Detection - 2D Print Attack

Captured-Recaptured

- LBPV is used to add contrast information to the LBP histogram.

$$Var_{P,R} = \frac{1}{P}\sum_{p=0}^{P-1}(g_p - u)^2 \qquad u = 1/P\sum_{p=0}^{P-1} g_p$$

- The LBPV computes the variance from a local region and accumulates it into the LBP bin as the weighting factors

$$LBPV_{P,R}(k) = \sum_{i=1}^{X}\sum_{j=1}^{Y} w(LBP_{P,R}(i,j),k), \quad k = [0\ K]$$

$$w(LBP_{P,R}(i,j),k) = \begin{cases} \mathrm{var}_{P,R}(i,j) & LBP_{P,R}(i,j) = k \\ 0 & else \end{cases}$$

- The quadratic means of histogram distances (chi-square) between a new probe and genuine and fake model sets of histograms are computed and compared to classify the new probe.

Kose N. and Dugelay J.-L., “Countermeasure for the protection of face recognition systems against mask attacks,” in *Proc. IEEE Int. Conf. Autom. Face Gesture Recognit.*, Apr. 2013, pp. 1–6.

Liveness Detection - 2D Print Attack

Gaze Stability

- The algorithms proposed by Ali et al. are based on the assumption that the spatial and temporal coordination of the movements of eye, head and (possibly) hand involved in the task of following of a visual stimulus is significantly different when a genuine attempt is made compared with certain types of spoof attempts.
- The task requires head/eye fixations on a simple target that appears on a screen in front of the user.
- In the case of a photograph spoofing attack, visually guided hand movements are needed to orientate the photographic artefact to point in the correct direction towards the challenge ite
- The stimulus appears in a random sequence to prevent predictive video attacks.
- Face images are then captured at each presentation of the stimulus on the screen and STASM is used to extract relevant landmarks.

Ali, A., Hoque, S., & Deravi, F. (2016). Gaze stability for liveness detection. *Pattern Analysis and Applications*, 1-13

Liveness Detection - 2D Print Attack

Gaze Stability

Ali, A., Hoque, S., & Deravi, F. (2016). Gaze stability for liveness detection. *Pattern Analysis and Applications*, 1-13

Liveness Detection - 2D Print Attack

Gaze Stability

- Collinearity features are computed by the Mean Square Error between the expected positions of landmark points (given the trajectory of stimuli) and the detected ones computed.
- As there are multiple face landmarks as well as several stimulus challenge trajectories, a feature vector F_{colin} can be constructed from the concatenation of these MSE values (and optionally other feature values) and used for liveness detection.
- Colocation features rather take into account the difference in landmark positions when the stimulus is presented in the same location. Even in this case a F_{coloc} vector can be computed.
- One movement threshold is used to check if the attacker is trying to subvert the liveness detection system by minimizing movements of the artefact in response to the stimulus.
- A second threshold is used to detect if the movements of the artefact are resulting in repeatable positioning of the eyes in response to the stimulus.

Ali, A., Hoque, S., & Deravi, F. (2016). Gaze stability for liveness detection. *Pattern Analysis and Applications*, 1-13

Liveness Detection - 2D Print Attack

Optical Flow

- The paper by Anjos et al. exploits the Optical Flow Correlation (motion correlation) between the head of the user trying to authenticate and the background of the scene, which indicates the presence of a spoofing attack.
- The direction of objects in the scene is estimated using OF techniques.
- The use of OF is expected to grant more precise estimation of motion parameters between the regions of interest in the scene, assuring that motion cues are related in direction and do not come from unrelated phenomena.
- OFC quantizes, histograms, normalizes and directly compares motion direction vectors from the two regions of interest in order to provide a correlation score, for every analysed frame.
- In practice, face and background **should not move together.**
- **Does not work with 2D masks**

Anjos, A., Chakka, M. M., & Marcel, S. (2013). Motion-based counter-measures to photo attacks in face recognition. *IET biometrics*, *3*(3), 147-158.

Liveness Detection - 2D Print Attack

Image Distortion Analysis

Wen et al. Exploit a set of image distortion features for spoofing detection:

(1) specular reflection from the printed paper surface or LCD screen;

(2) image blurriness due to camera defocus;

(3) image chromaticity and contrast distortion due to imperfect color rendering of printer or LCD screen;

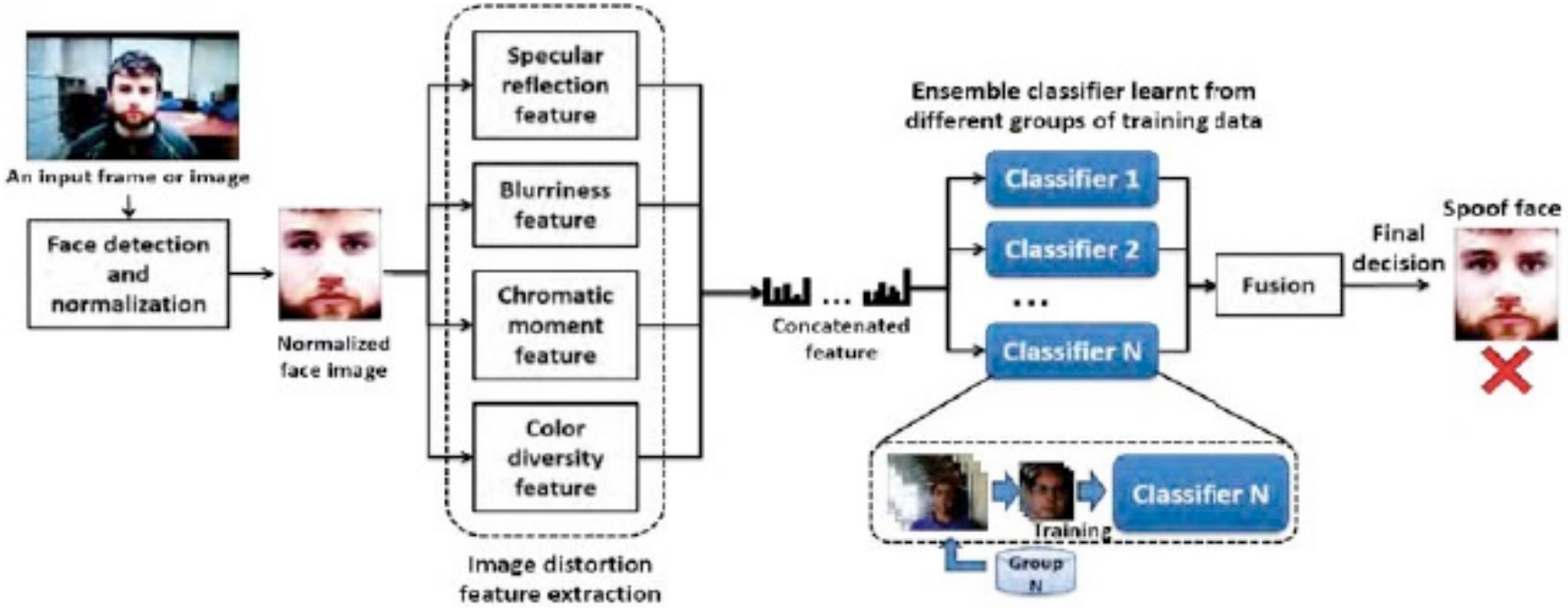
(4) color diversity distortion due to limited color resolution of printer or LCD screen.

Wen, D., Han, H., & Jain, A. K. (2015). Face spoof detection with image distortion analysis. *IEEE Transactions on Information Forensics and Security*, *10*(4), 746-761.

Liveness Detection - 2D Print Attack

Image Distortion Analysis

Wen et al. Exploit a set of image distortion features for spoofing detection



Wen, D., Han, H., & Jain, A. K. (2015). Face spoof detection with image distortion analysis. *IEEE Transactions on Information Forensics and Security*, *10*(4), 746-761.

Liveness Detection - 2D Print Attack

Image Distortion Analysis

According to the Dichromatic Reflection Model light reflectance I of an object at a specific location x can be decomposed into diffuse reflection (Id) and specular reflection (Is) components:

$$I(x) = Id + Is = wd(x)S(x)E(x) + ws(x)E(x)$$

where $E(x)$ is the incident light intensity, $wd(x)$ and $ws(x)$ are the geometric factors for the diffuse and specular reflections, respectively, and $S(x)$ is the local diffuse reflectance ratio.

Since 2D spoof faces are recaptured from original genuine face images, the formation of spoof face image intensity $I(x)$ can be modeled as follows:

$$I'(x) = I'd + I's = F(I(x)) + ws'(x)E'(x)$$

In the second equation the diffuse reflection of spoof face image Id is substituted by $F(I(x))$ because the diffuse reflection is determined by the distorted transformation of the original face image $I(x)$.

$F(\cdot)$ is a distortion function that depends on the spoofing medium.

Wen, D., Han, H., & Jain, A. K. (2015). Face spoof detection with image distortion analysis. *IEEE Transactions on Information Forensics and Security*, *10*(4), 746-761.

Liveness Detection - 2D Print Attack

Image Distortion Analysis

- The total distortion in $I'(x)$ compared to $I(x)$ consists of two parts: i) distortion in the diffuse reflection component ($I'd$), and ii) distortion in the specular reflection component ($I's$), both of which are related to the spoofing medium.
- $I'd$ is correlated with the original face image $I(x)$, while $I's$ is independent of $I(x)$.
- Due to the glassy surface of tablet/mobile phone and the glossy ink layer on the printed paper, there is usually a specular reflection around the spoof face image. While for a genuine 3D face, specular reflection is only located in specific fiducial locations (such as nose tip, glasses, forehead, cheeks, etc.).

Wen, D., Han, H., & Jain, A. K. (2015). Face spoof detection with image distortion analysis. *IEEE Transactions on Information Forensics and Security*, *10*(4), 746-761.

Liveness Detection - 2D Print Attack

Image Distortion Analysis

- After calculating the specular reflection component image *Is*, the specularity intensity distribution is represented with three dimensional features: i) specular pixel percentage r, ii) mean intensity of specular pixels μ, and iii) variance of specular pixel intensities σ.
- Blurriness is represented by two values, bot in the range 0,1:
  - the difference between the original input image and its blurred version - the larger the difference, the lower the blurriness in the original image.
  - average edge width in the input image.
- Chromatic features - the normalized facial image is converted from the RGB space into the HSV (Hue, Saturation, and Value) space to compute the chromatic features:
  - the mean, deviation, and skewness of each channel
  - the percentages of pixels in the minimal and maximal histogram bins of each channel
- Color diversity features (genuine faces tend to have richer colors) - color quantization (with 32 steps in the red, green and blue channels, respectively) is performed on the normalized face image to compute two measures:
  - the histogram bin counts of the top 100 most frequently appearing colors,
  - the number of distinct colors appearing in the normalized face image.

Wen, D., Han, H., & Jain, A. K. (2015). Face spoof detection with image distortion analysis. *IEEE Transactions on Information Forensics and Security*, *10*(4), 746-761.

Liveness Detection - 2D Print Attack

Image Distortion Analysis

- Different spoof attacks will have different sample distributions in the IDA feature space.
- For example, while the printed attack samples tend to have lower contrast than the genuine samples, the replay attack samples tend to have higher contrast.
- Different types of attacks might also have different chromatic distortion characteristics.
- Instead of training a single binary classifier, an ensemble classifier is more appropriate to cover various spoof attacks.
- An ensemble classifier scheme is set up by training multiple constituent spoof classifiers in different groups of spoof attack samples.

Wen, D., Han, H., & Jain, A. K. (2015). Face spoof detection with image distortion analysis. *IEEE Transactions on Information Forensics and Security*, *10*(4), 746-761.

Liveness Detection – Replay Video Attack

- The paper by Patel et al. addresses the problem of facial spoofing detection against replay attacks based on the analysis of aliasing in spoof face videos.
- They analyze the **moiré pattern aliasing** that commonly appears during the recapture of video or photo replays on a screen in different channels (R, G, B and grayscale) and regions (the whole frame, detected face, and facial component between the nose and chin).
- Multi-scale LBP and DSIFT features are used to represent the characteristics of moiré patterns that differentiate a replayed spoof face from a live face (face present).

(a) Overlay of two patterns (b) Printing (c) Screen shooting

Patel, K., Han, H., Jain, A. K., & Ott, G. (2015, May). Live face video vs. spoof face video: Use of moiré patterns to detect replay video attacks. In *Biometrics (ICB), 2015 International Conference on* (pp. 98-105). IEEE.

Liveness Detection – Replay Video Attack

- By comparing the spoof face videos and the live face videos, it is possible to observe that moiré patterns often exist in the entire spoof video frame, which appear as **a distinct texture pattern** overlaid on a live video frame.
- This inspired the authors to capture moiré patterns using a number of well known texture descriptors.
- The authors use MLBP and SIFT for spoof detection, either individually or combined.
- Each video is decoded into individual frames.
- Given an input frame or a detected face or a face region, it is first divided into 32×32 patches with an overlap of 16 pixels between every two successive patches.

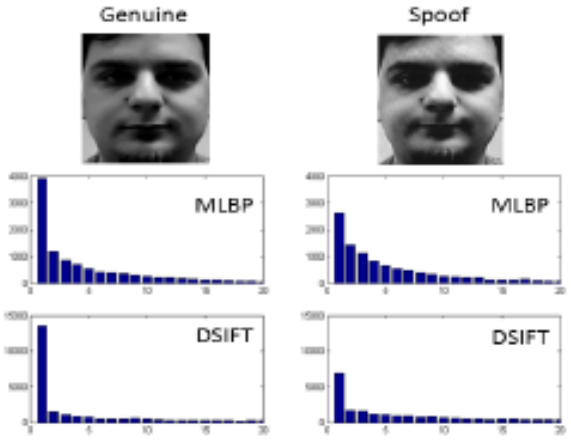
Patel, K., Han, H., Jain, A. K., & Ott, G. (2015, May). Live face video vs. spoof face video: Use of moiré patterns to detect replay video attacks. In *Biometrics (ICB), 2015 International Conference on* (pp. 98-105). IEEE.

Liveness Detection – Replay Video Attack

- The MLBP features are calculated as

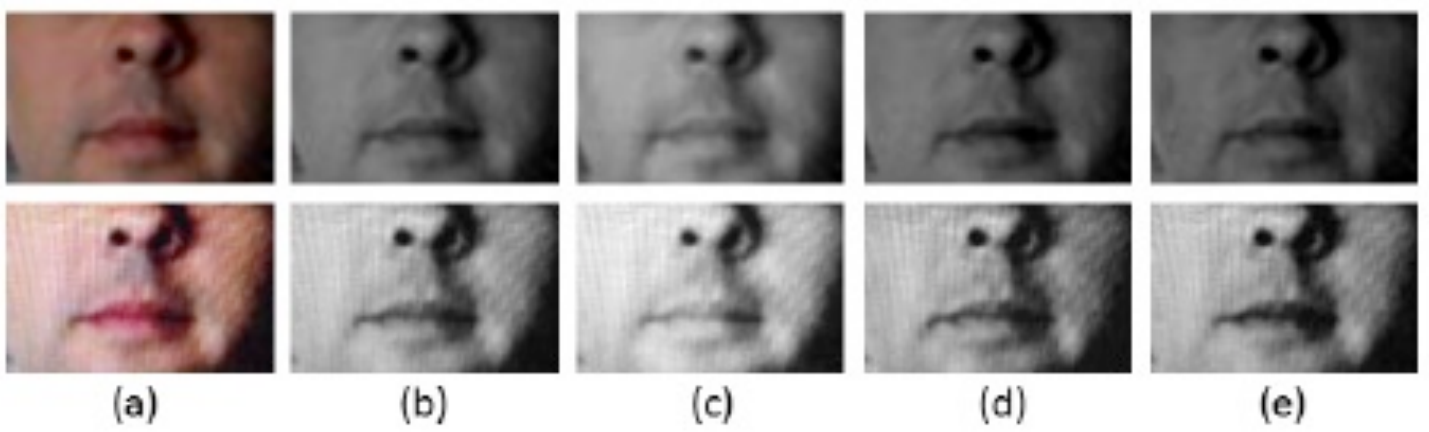
$$f_{MLBP}(I) = \{LBP_{P,R}\}_{(P,R)\in\{(8,1),(24,3),(40,5)}$$

- The DSIFT features from each image patch are calculated using 8 orientation bins and 16 segments.



Patel, K., Han, H., Jain, A. K., & Ott, G. (2015, May). Live face video vs. spoof face video: Use of moiré patterns to detect replay video attacks. In *Biometrics (ICB), 2015 International Conference on* (pp. 98-105). IEEE.

Liveness Detection – Replay Video Attack



Live video frames (top row) and spoof video frames we collected (bottom row) for one subject Video frames are shown using the (a) RGB image, (b) grayscale image, (c) red channel, (d) green channel, and (e) blue channel.

The moir´e patterns in one of the channels (red, green and blue) of an input image can be more discriminative than the other two channels or the intensity image.

Patel, K., Han, H., Jain, A. K., & Ott, G. (2015, May). Live face video vs. spoof face video: Use of moiré patterns to detect replay video attacks. In *Biometrics (ICB), 2015 International Conference on* (pp. 98-105). IEEE.

Liveness Detection

3D Mask Attack

- Methods that depend on the assumption of a planar surface for a fake face are rendered futile in case of 3D facial mask attacks
- The earliest studies in mask detection aim to distinguish between facial skin and mask materials by exploiting the difference in their **reflectance** characteristics.
- Different materials have to be taken into account (e.g., plastic, silica gel, paper pulp, plaster, sponge) and different wavelenghts.
- Wavelenghts are chosen after inspecting the albedo curves of facial skin and mask materials with varying distances.
- In some cases the distance from the sensor affects the accuracy of spoofing recognition.
- An alternative proposal entails using a micro-texture analysis based counter measure applied separately on color images and depth maps captured from the probe sample.
  - In fact, most 3D scanners provide both texture images and depth maps

Liveness Detection

3D Mask Attack

- A close look at the differences between masks and real faces reveals that they have different **texture** and **smoothness** characteristics.
- Based on these observations, the LBP based approach can be used in order to detect mask attacks.
- The work by Kose and Dugelay exploits exactly the same approach described for photo attack, using it both on the texture image and on the depth map.

Kose N. and Dugelay J.-L., “Countermeasure for the protection of face recognition systems against mask attacks,” in *Proc. IEEE Int. Conf. Autom. Face Gesture Recognit.*, Apr. 2013, pp. 1–6

Liveness Detection

3D Mask Attack

- Texture-based approaches show powerful abilities and achieve encouraging results on 3D mask face anti-spoofing. → the method to adopt may depend on the material (as for fingerprints) and could fail to detect imposters with hyper-real masks.
- The work by Liu et al. proposes as possible solution the analysis of heartbeat signal through remote Photoplethysmography (rPPG).
  - A **photoplethysmogram** (**PPG**) is an optically obtained plethysmogram, i.e., a volumetric measurement of an organ.
  - A PPG is often obtained by using a **pulse oximeter** which illuminates the skin and measures changes in light absorption.
  - A conventional pulse oximeter monitors the perfusion of blood to the dermis and subcutaneous tissue of the skin to indirectly monitor the oxygen saturation of a patient's blood (as opposed to measuring oxygen saturation directly through a blood sample) and changes in blood volume in the skin, producing a **photoplethysmogram**.

Liu, S., Yuen, P. C., Zhang, S., & Zhao, G. (2016, October). 3D Mask Face Anti-spoofing with Remote Photoplethysmography. In *European Conference on Computer Vision* (pp. 85-100). Springer International Publishing.

Liveness Detection

3D Mask Attack

- **Remote PPG** is a non-invasive technique which measures the small changes in color under the skin epidermis, caused by variations in volume and oxygen saturation of the blood in the vessels, due to heart beats.
- FaceReader by Noldus: each cardiac cycle as a peak in the data.
- A local rPPG correlation model allows to extract discriminative local heartbeat signal patterns so that an imposter can better be detected regardless of the material and quality of the mask.
- It is possible to learn a confidence map through heartbeat signal strength to weight local rPPG correlation pattern for classification, to further exploit the characteristic of rPPG distribution on real faces.

http://www.noldus.com/facereader/remote-photoplethysmography-facereader

Liu, S., Yuen, P. C., Zhang, S., & Zhao, G. (2016, October). 3D Mask Face Anti-spoofing with Remote Photoplethysmography. In *European Conference on Computer Vision* (pp. 85-100). Springer International Publishing.

Spoofing Attacks: research datasets

2D VIS face spoofing: NUAA Photograph Imposter Database

Different photo-attacks (from left to right) : (1) move the photo horizontally, vertically, back and front; (2) rotate the photo in depth along the vertical axis; (3) the same as (2) but along the horizontal axis; (4) bend the photo inward and outward along the vertical axis; (5) the same as (4) but along the horizontal axis.

Available at http://parnec.nuaa.edu.cn/xtan/data/nuaaimposterdb.html

Spoofing Attacks: research datasets

2D MultiSpectral (VIS+NIR) face spoofing: CASIA database

Available on request at http://www.cbsr.ia.ac.cn/english/FaceAntiSpoofDatabases.asp

Spoofing Attacks: research datasets

3D face spoofing: The **HKBU** 3D **M**ask **A**ttack with **R**eal World Variation**s** Database (**HKBU MARs**) **database**

Sample mask images in the proposed new 3D mask face anti-spoofing database. (a)-(f) are ThatsMyFace masks and (g)-(l) are Real-F masks (http://real-f.jp/en_news.html)

Publicly available http://rds.comp.hkbu.edu.hk/mars/#

Spoofing Attacks: research datasets

Datasets from European project Tabula Rasa

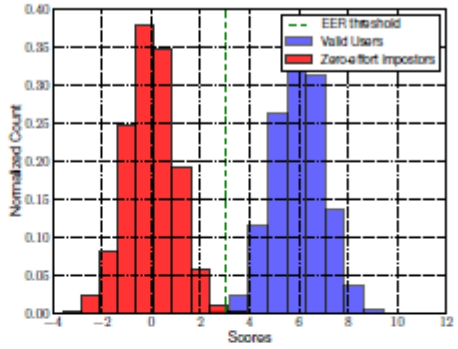
- **The Idiap Research Institute PRINT-ATTACK Database:** www.idiap.ch/dataset/printattack
- **The Replay-Attack Database:** www.idiap.ch/dataset/replayattack
- **3DMAD database :** www.idiap.ch/dataset/3dmad
- **CASIA Face Anti-Spoofing Database:** http://www.cbsr.ia.ac.cn/english/FaceAntiSpoofDatabases.asp

Antispoofing evaluation

- Spoof False Acceptance Rate (SFAR): % of spoofing attacks falsely accepted

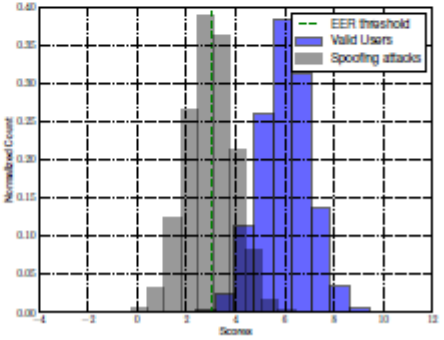
Licit scenario

- False Rejection Rate (FRR)
- False Acceptance Rate (FAR)
- Half Total Error Rate (HTER)



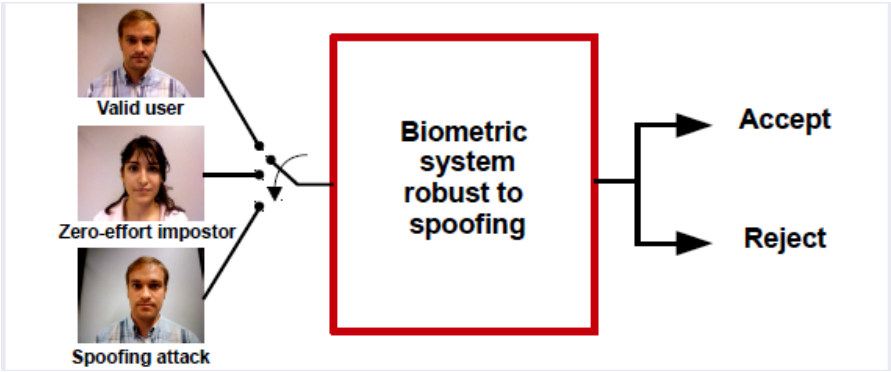
Spoof scenario

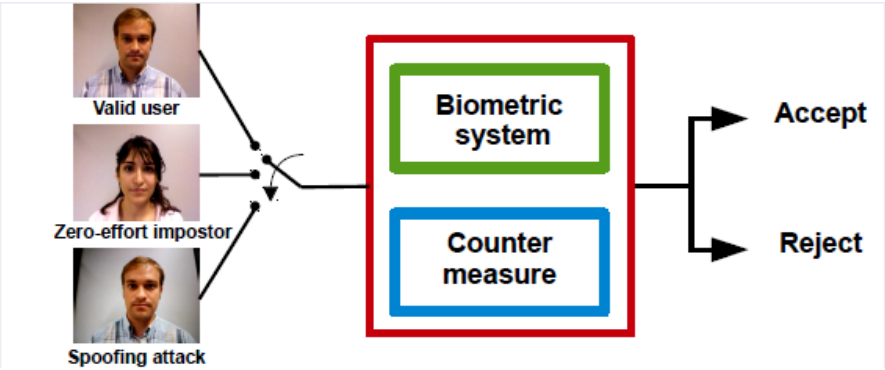
- False Rejection Rate (FRR)
- Spoof False Acceptance Rate (SFAR)

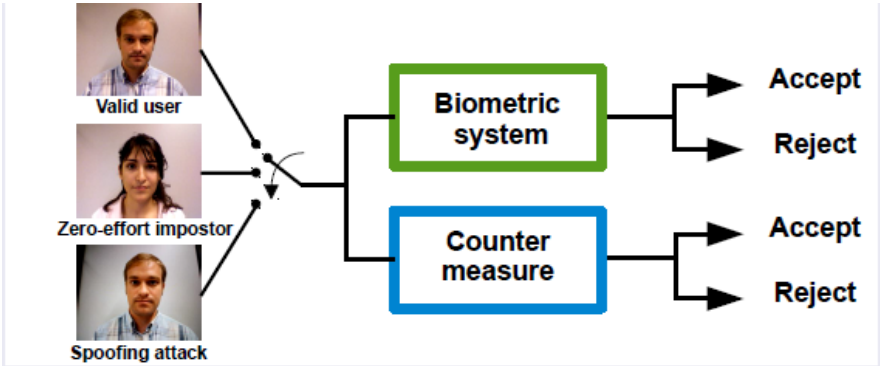


From the turorial on **Tutorial Biometric Spoofing (ICB'15) - Idiap Research Institu**
www.idiap.ch/~marcel/professional/ICB_2015.html

Antispoofing evaluation



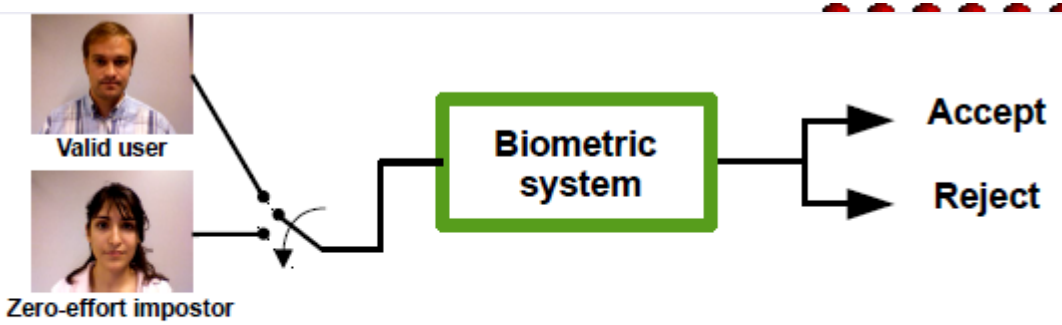




From the turorial on **Tutorial Biometric Spoofing (ICB'15) - Idiap Research Institute**
www.idiap.ch/~marcel/professional/ICB_2015.html

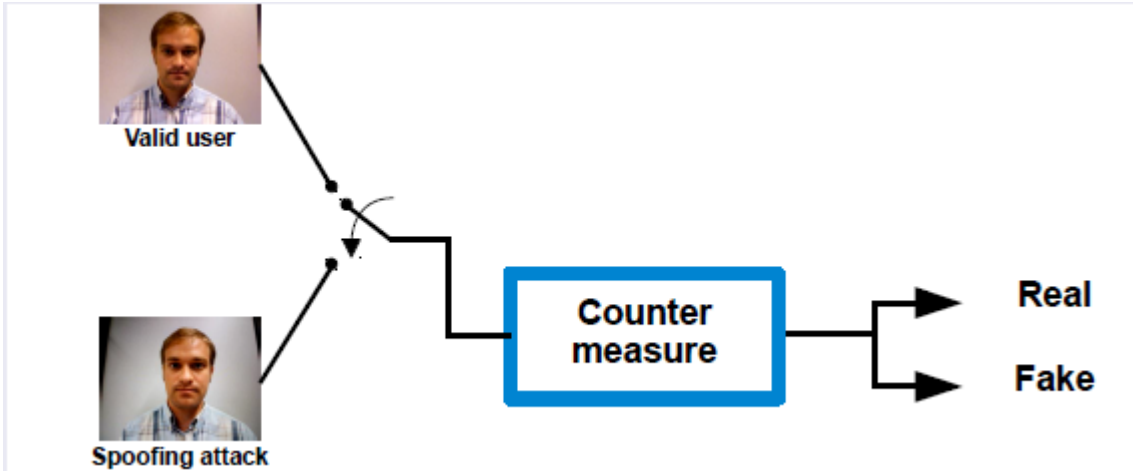
Antispoofing evaluation

False Rejection Rate (FRR): % of genuine users falsely rejected
False Acceptance Rate (FAR): % of zero-effort impostors falsely accepted



From the turorial on **Tutorial Biometric Spoofing (ICB'15) - Idiap Research Institute**
www.idiap.ch/~marcel/professional/ICB_2015.html

We measure 2 errors:
False Living Rate (FLR): % of spoong attacks misclassified as real
False Fake Rate (FFR): % of real access misclassified as fake



Recent standardized evaluation metrics

- For the performance evaluation, it is suitable to use the recently standardized ISO/IEC 30107-3 metrics: **Attack Presentation Classification Error Rate (APCER), Bona Fide Presentation Classification Error Rate (BPCER)** and **Average Classification Error Rate (ACER)** as the evaluation metric, in which APCER and BPECER are used to measure the error rate of fake or live samples, respectively.
- Inspired by face recognition, the **Receiver Operating Characteristic (ROC)** curve is introduced for large-scale face Anti-spoofing, which can be used to select a suitable threshold to trade off the false positive rate (**FPR**) and true positive rate (**TPR**) according to the requirement of real applications.
- **POSITIVE = Bona Fide**
- **NEGATIVE = Attack**

Recent standardized evaluation metrics

- Attack Presentation Classification Error Rate (APCER):

APCER = FP / (TN + FP)

- Bona Fide Presentation Classification Error Rate (NPCER):

BPCER = FN/(FN + TP)

- Average Classification Error Rate (ACER):

ACER = (APCER + NPCER) / 2

- False Positive Rate (FPR):

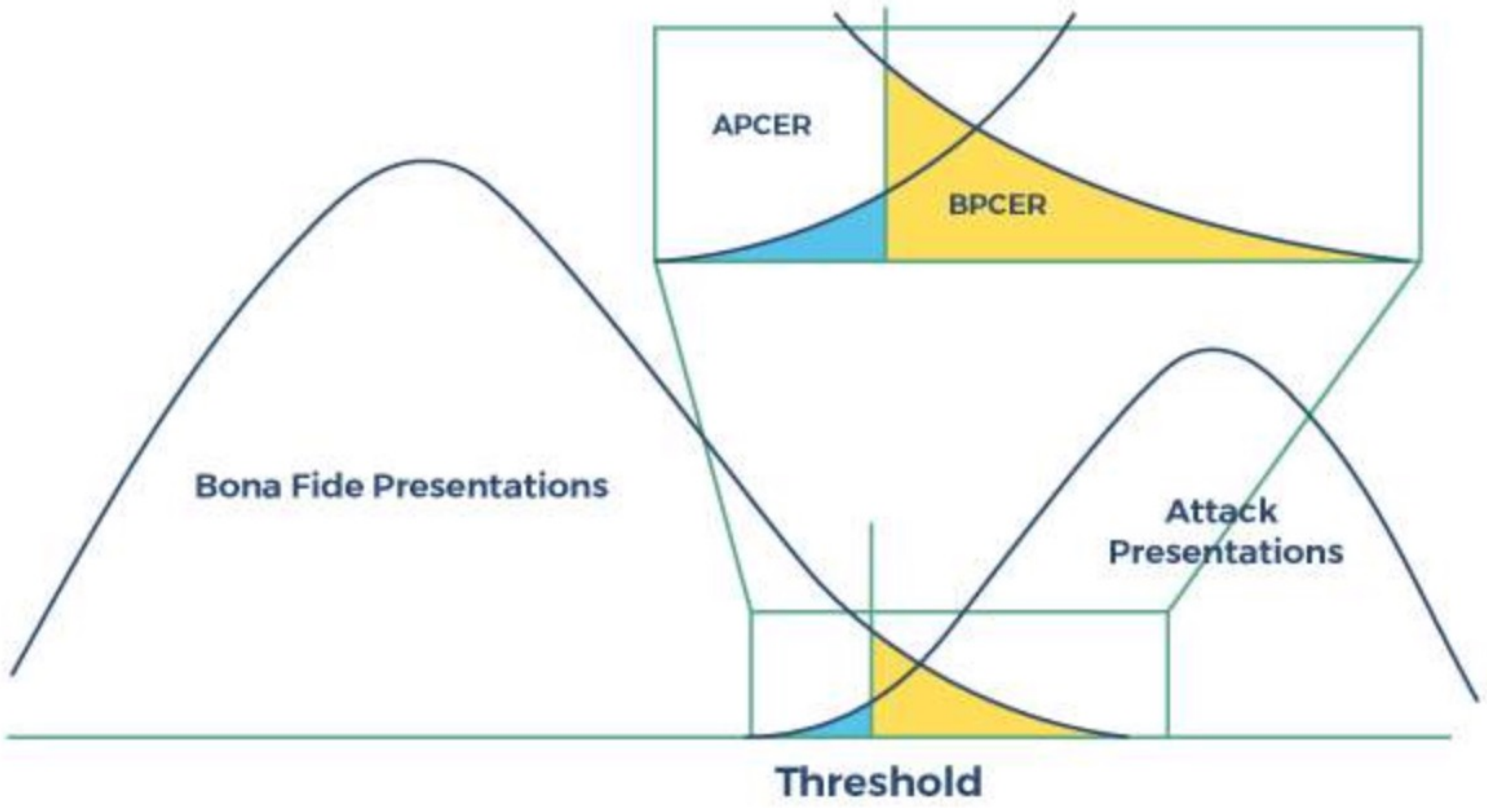
FPR = FP / (FP + TN)

- True Positive Rate (TPR):

TPR = TP / (TP + FN)

- For instance, the FINAL evaluation metric can be the value of TPR @FPR=10E-4, or TPR@FPR=10E-2 or10E-3, and ACER.

Similar to verification



Outline

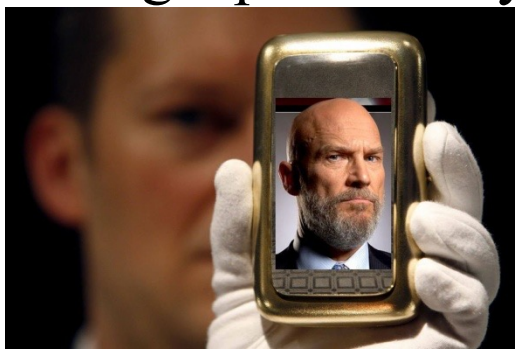
- Introduction: spoofing in biometrics
- Face spoofing
- Face antispoofing - Liveness Detection
- **Face antispoofing at BIPlab**

Face antispoofing at BIPlab

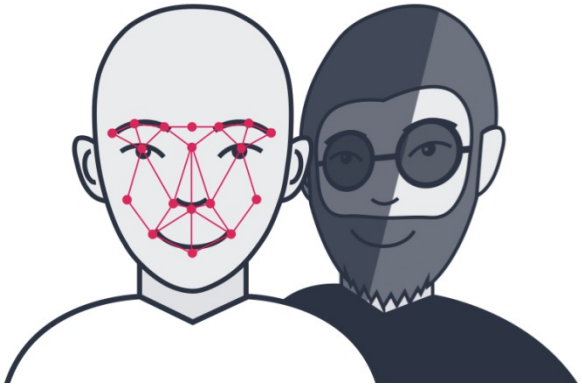
- The most robust spoofing detection systems in the field of face recognition rely on two main activities: 1) verification of **face three-dimensionality**, 2) **interaction** with the user.
- **Face three-dimensionality** verification may require very sophisticated techniques
- **Interaction**, in most cases, involves additional hardware and software.
- **Interaction** may be modelled according to two parameters: **time** and **content**, e.g. motion type.
- Requiring motion at a **random time** is sufficient to avoid an attack through a pre-recorded video (e.g., replay-attacks).
- Challenge-response may be spoofed by video, if the system would always ask a basic and always the same head motion, e.g. turn your head from left to right.
- This latter attack can be successfully addressed by requiring a **specific motion type at random times**, but this asks for a 3D model to track such motion and distinguish it from an appropriately presented photo.
- Spoofing defence is enhanced at the expense of a significant increase of system complexity.

Moving Face Spoofing Detection Via 3D Projective Invariants

- Poor or absent spoofing detection implies that a system can be cheated by simply showing a photo or by a video clip of a registered user.

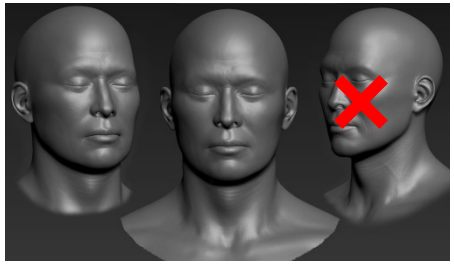


- A possible robust anti-spoofing technique relies on verifying face three-dimensionality, and on a specific user interaction.



Antispoofing for moving faces

- This method has the advantage to exploit face 3D information starting from 2D images, at a much lower computational cost than traditional techniques.



- It is uniquely based on measures from a set of easy-to-detect facial points → it can also process low quality inputs.
- Though the user is randomly requested to move the head, it is not necessary to perform a specific motion, so that also the amount of necessary user accuracy is somehow limited.

- It does not require the user to stay always in a perfect frontal pose and looking towards the capture device, as it is often the case in eyeblink-based techniques.
- The method provides a sufficient tolerance to user's position, given that face rotation is not excessive (e.g., profile pose).

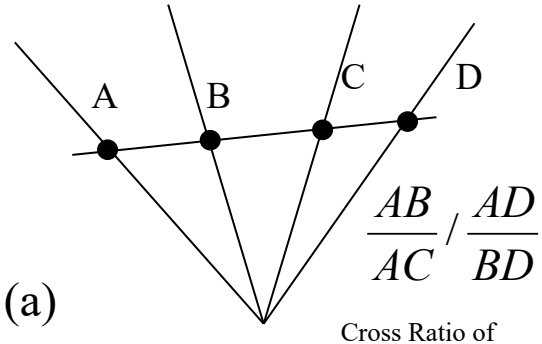
Antispoofing for moving faces

- The user can move more freely, and therefore feel more comfortable.
- We do not have to check the exactness of the taken pose. We rather exploit it to check three-dimensionality of the face.
- When the user is in front of the system, this requires to perform a generic and continuous face motion.
- The request is issued at random times.

Antispoofing for moving faces

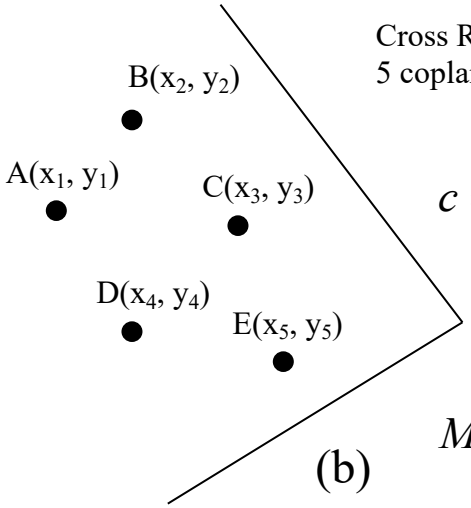
Geometric Invariants

Geometric Invariants are shape descriptors, that are not affected by object pose and scale, by perspective projection and intrinsic parameters of the camera. They are expressed as Ratios of distances/measures or as a combination of 3D/2D coordinates of the points of the object



(a)

Cross Ratio of
4 collinear points

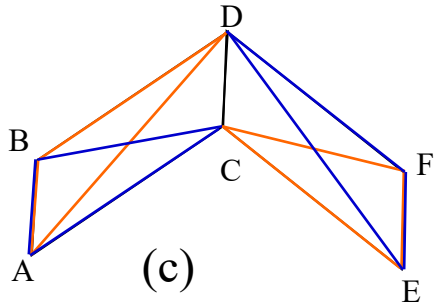


(b)

Cross Ratio of
5 coplanar points

$$c = \frac{M(1,2,4)M(1,3,5)}{M(1,2,5)M(1,3,4)}$$

$$M(j,k,l) = \begin{pmatrix} x_j & x_k & x_l \\ y_j & y_k & y_l \\ 1 & 1 & 1 \end{pmatrix}$$



(c)

$$c = \frac{P_{\overset{\Delta}{ABD}} \cdot P_{\overset{\Delta}{FEC}}}{P_{\overset{\Delta}{ABC}} \cdot P_{\overset{\Delta}{FED}}}$$

All these invriants can be calculated from a single view of the object, then we can refer to them as 2D/3D invariants.

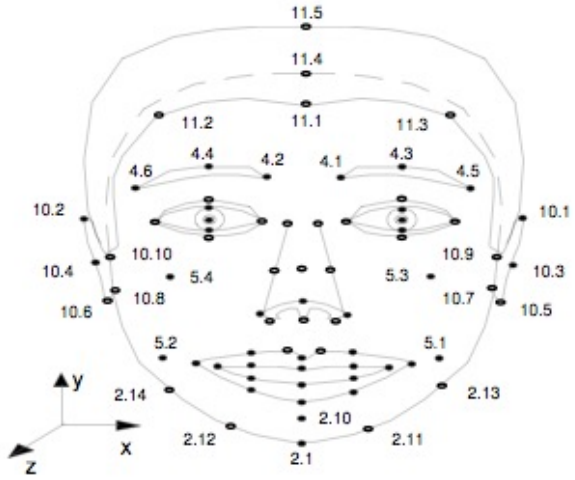
They can be used as a preliminary coarse grain description of the object shape (face).

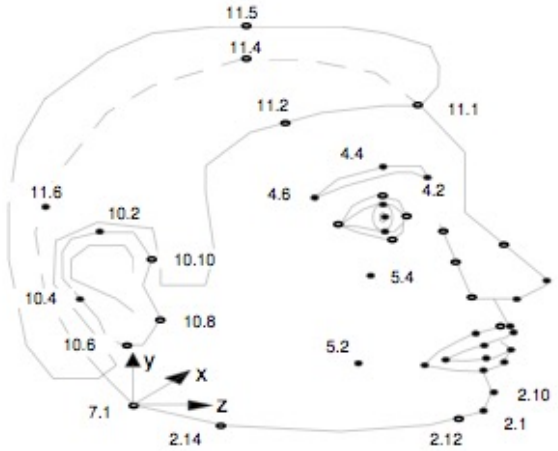
Antispoofing for moving faces

Geometric Invariants

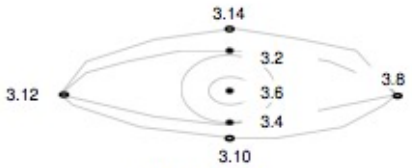
- In this work, the same mathematical definition of geometric invariants is exploited, but these are used according to **reverse** considerations.
- Given a configuration of points on an object, which are **known as not coplanar**, a geometric invariant which would instead **require coplanarity** is computed from them, on **more consecutive** images.
- If the **pose** of the subject in front of the capture device changes, but the computed **cross ratio stays constant**, the points from which it is computed **must** be **coplanar**
- This would **not be possible assuming a 3D face**, and therefore the object is not 3D.
- By applying this argument to face recognition, we can distinguish a real face in front of a capture device from a picture.
- To add a spoofing detection-oriented interaction, the system requires to move the face, and only in those well-defined time intervals the cross ratio will be verified.

Face reference points

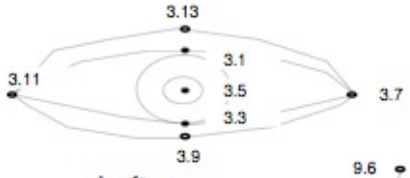




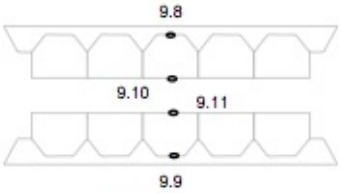
MPEG-4 FEATURE POINTS



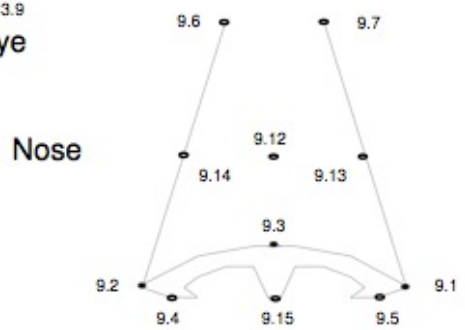
Right eye

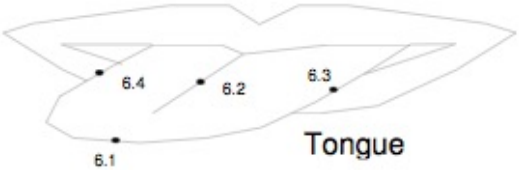


Left eye

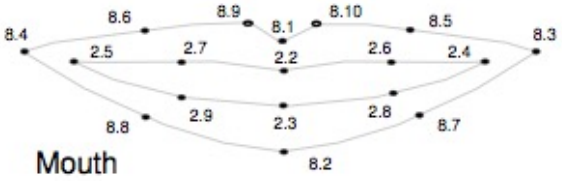


Teeth





Tongue



Mouth

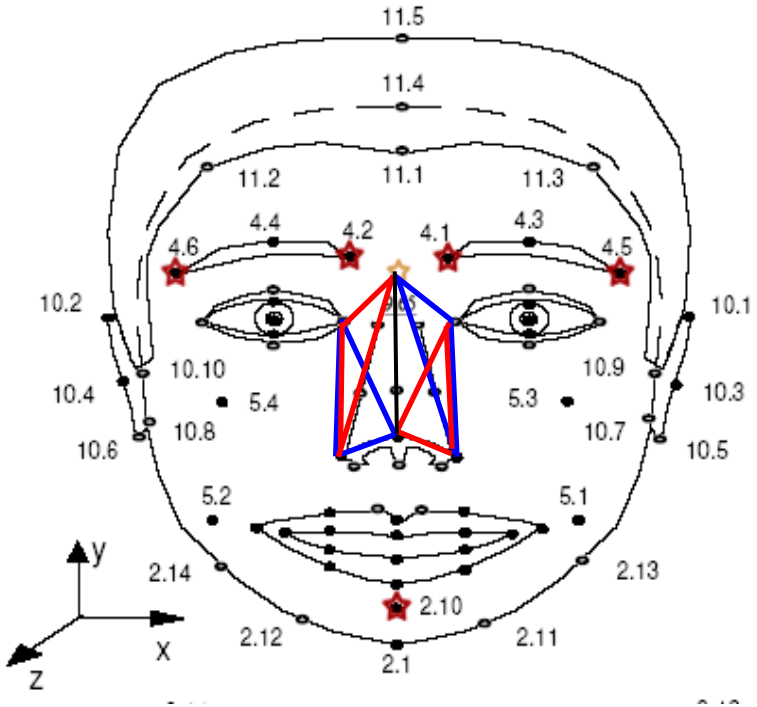
Antispoofing for moving faces

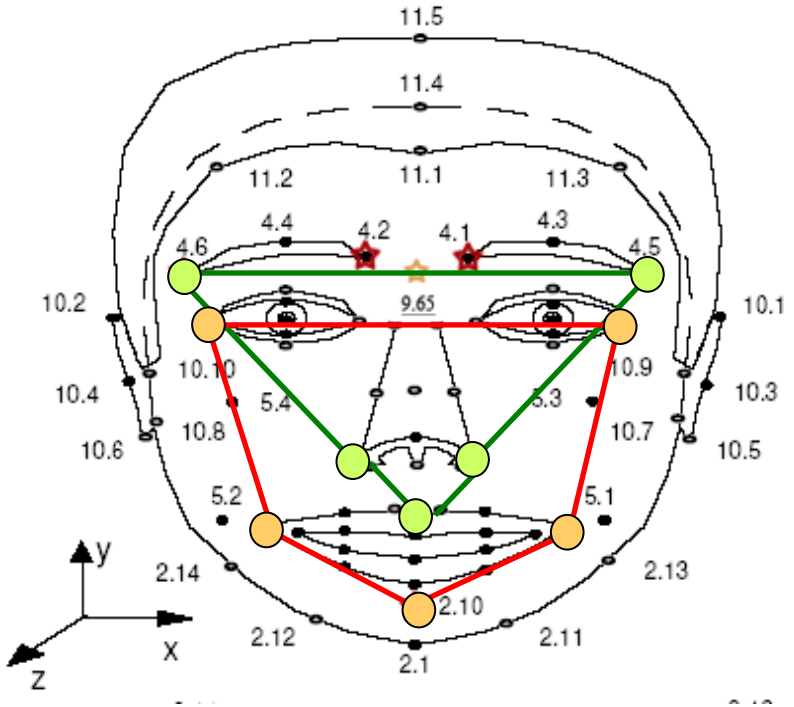
Face Geometric Invariants

Face is not a rigid surface and to find control points which both respect the required hypotheses and that are easy to locate, turns in a difficult task.

Cross Ratio of the area of triangles on adiacent planes

9.65, 3.8, 9.2, 9.3, 9.1 and 3.11





Cross Ratio of 5 coplanar points

4.6, 9.2, 8.1, 9.1 and 4.5

3.12, 8.4, 2.10, 8.3 and 3.7

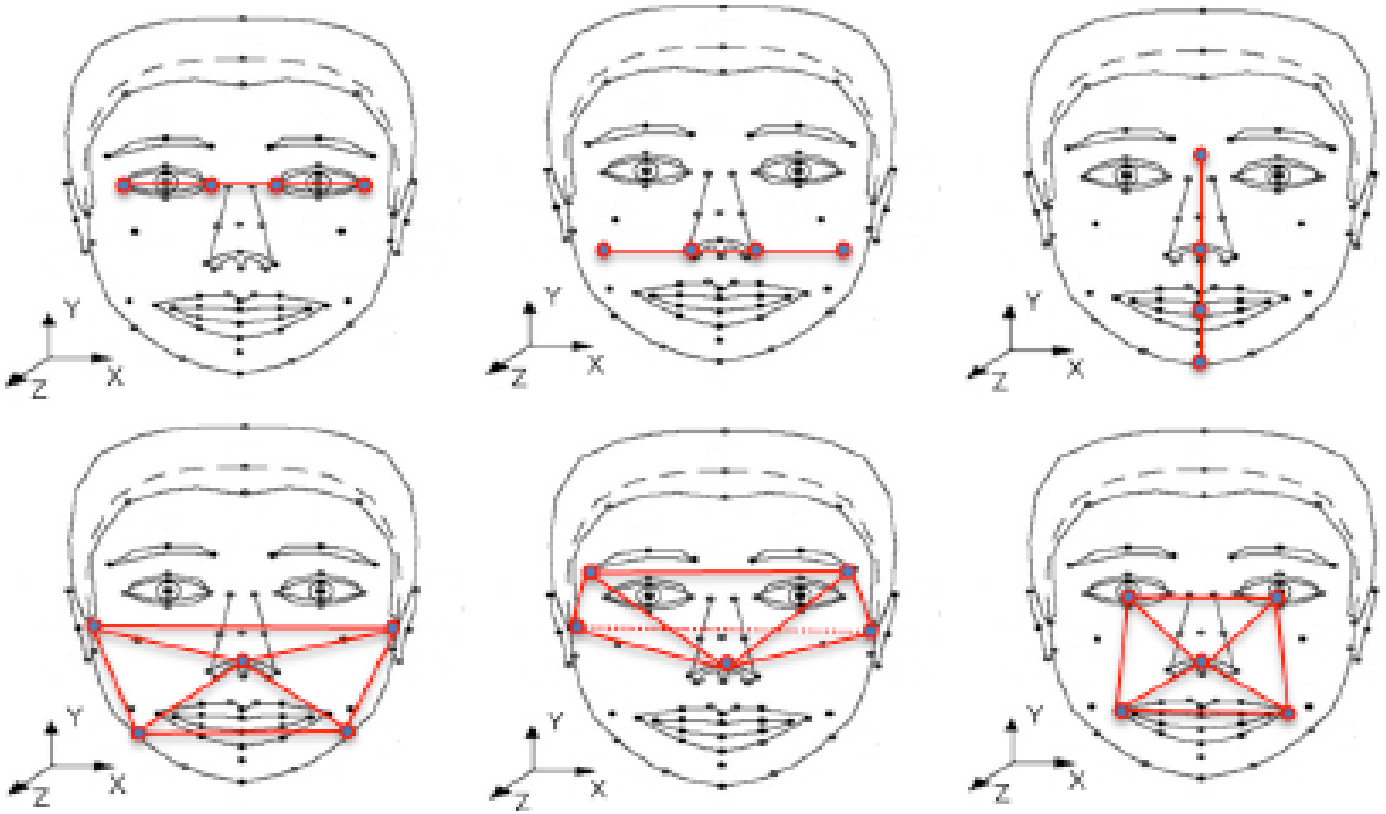
Antispoofing for moving faces

Tested Geometric Invariants

- Intuitively, the best candidates for the specific goal are those points that in a real 3D face model **strongly** violate collinearity/coplanarity constraints, but strictly satisfy them in a possible two-dimensional representation (photo) of the same model.
- For face, good candidates are the centre of eyes, the nose tip, and the chin.

Antispoofing for moving faces

Tested Geometric Invariants



Configurations of points chosen to compute cross ratios *c1*, *c2*, *c3*, *c4*, *c5*, *c6* (from left to right and from top to bottom).
Top: collinear points
Bottom: coplanar points

Antispoofing for moving faces

Tested Geometric Invariants

- The variation *v* of a cross ratio *c* is computed over the last *K* frames (*observation window*) and compared with a predetermined threshold *th*, which is generally different for each cross ratio.
- In addition, the number of frames rated as genuine (that is $v > th$) must be higher than a further predetermined threshold *thv*, which is set also according to the required level of security.
- Frames which present location errors, i.e. no located faces, or incorrectly determined points, are discarded, so that they do not enter the *observation window*.
- The number of considered frames *K* is a crucial parameter in terms of system performances.

Antispoofing for moving faces

Tested Geometric Invariants

- The six cross ratios for the configurations were evaluated on data collected from 10 different users, both through direct capture, and through printed images to simulate spoofing, for a total of 20 acquisitions.
- The aim was to determine which configurations better support discriminating genuine accesses from spoofing attacks.

Antispoofing for moving faces

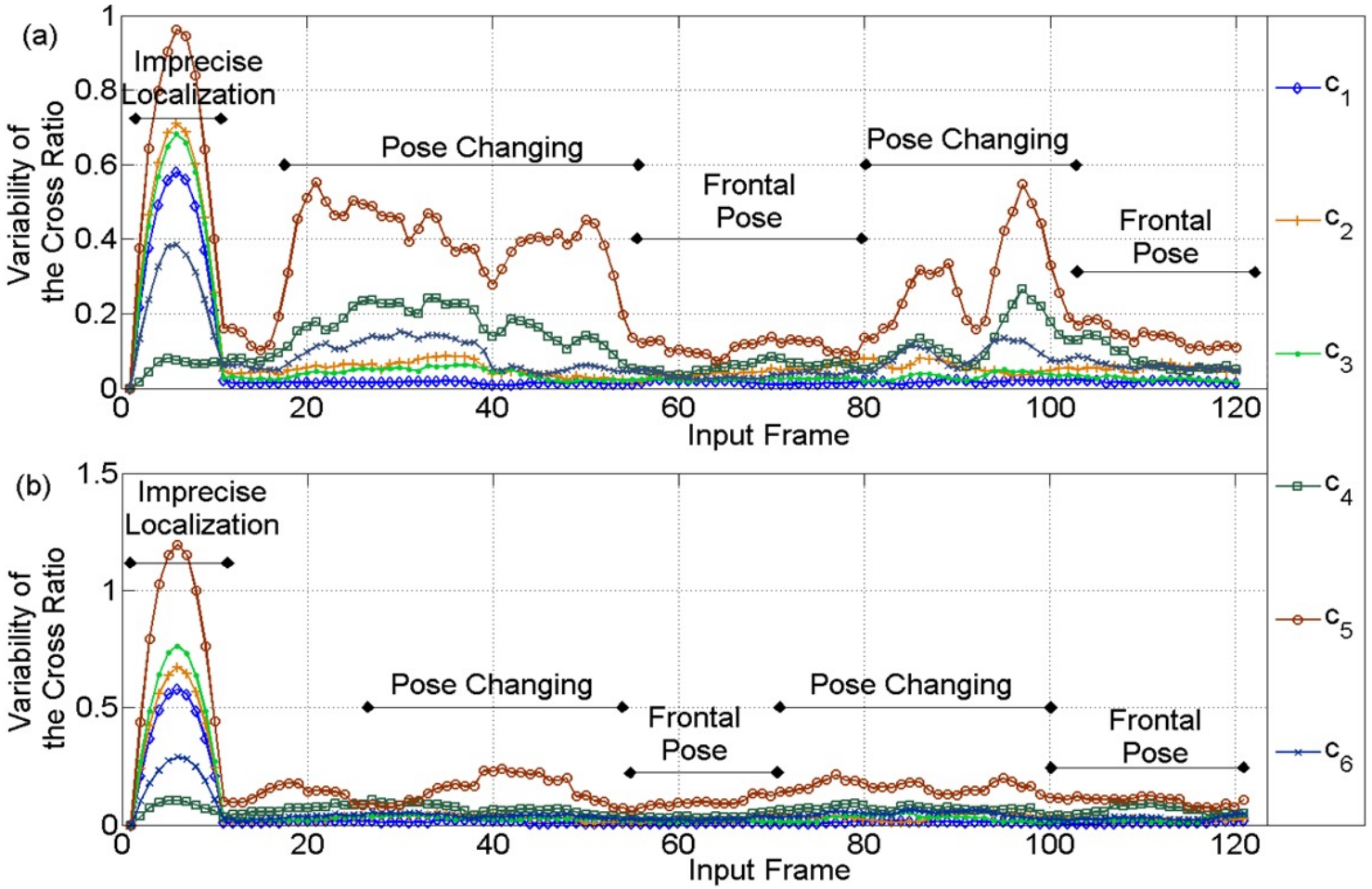
Tested Geometric Invariants

- The six cross ratios for the configurations were evaluated on data collected from 10 different users, both through direct capture, and through printed images to simulate spoofing, for a total of 20 acquisitions.
- The aim was to determine which configurations better support discriminating genuine accesses from spoofing attacks.
- Sequences of genuine attempts: when asked by the system, the subject moves the face.
- Sequences of spoofing attempts: a photo is presented, and, when asked by the system, the impostor varies the photo orientation in front of the capture device.
- Each configuration for cross ratio was separately tested on the two groups of 10 acquisitions (genuine attempts, spoofing attempts).

Antispoofing for moving faces

Tested Geometric Invariants

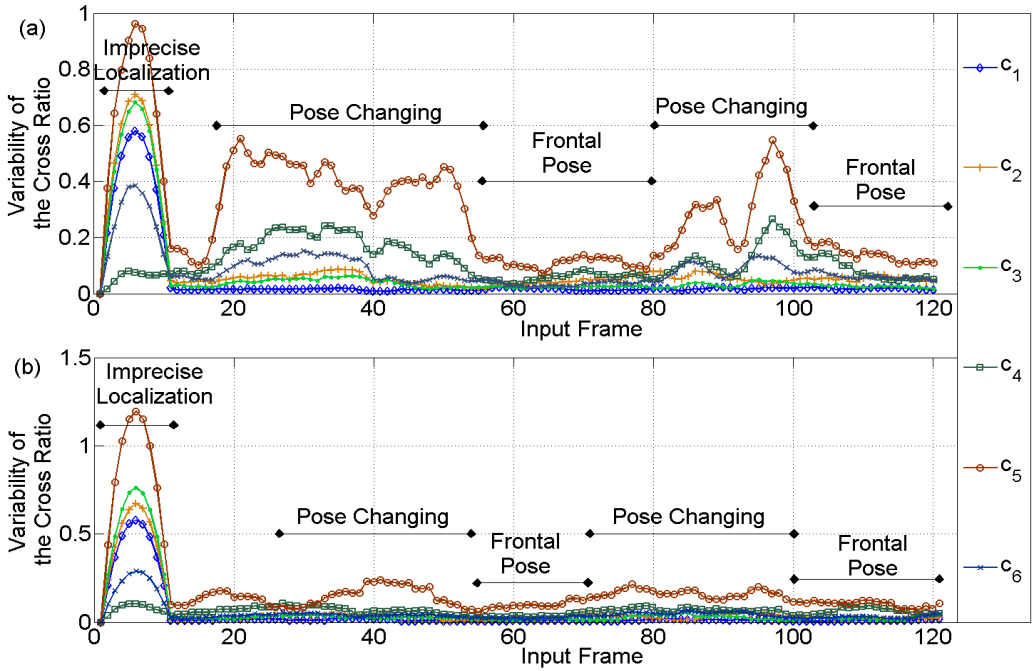
Variability curves produced by cross ratios c1, c2, c3, c4, c5, c6 in one of the experiments (top: genuine access, bottom: spoofing attack)



Antispoofing for moving faces

Geometric Invariants

- For cross ratios computed from four collinear points, constraints are always satisfied, such that the related variation *vi* (i=1,2,3) is always low, both for genuine attempts (a) and for spoofing ones (b).
- The trend of variation *vi* (i=4,5,6) for the cross ratios from coplanar points, undergoes a significant variation for real users (a), which is missing in spoofing attempts (b).



- Notice a high variability of the initial part of all curves, since not all *K* frames (10 here) needed to compute *vi* had been processed yet. This may also happen when location is wrong, so introducing an extra variability which is not due to three-dimensionality.
- How to overcome this limit: these errors contemporarily affect cross ratios of collinear points.
- The system can control at the same time both v1 and v5, and analyze only values of v5 for which v1 has a low value (correctly processed frame).

Antispoofing for moving faces

Tested Geometric Invariants

- Experiments with c_5 tested the best kind of move (better if composed, e.g., yaw + pitch), the best speed (better fast movements) and the number of frames to consider (10 are enough with fast movements).
- Accuracy = the system ability to distinguish genuine subjects from "dummy" ones (photo)
- Measured in terms of Equal Error Rate (EER), by considering as False Acceptance Rate (FAR) the rate of "dummy" subjects classified as genuine, and as False Rejection Rate the rate of genuine users that were rejected as "dummy".
- The system was tested with 20 subjects, each performing 12 attempts: 9 genuine attempts produced by three head motions (yaw, pitch, yaw+pitch) with three different speeds (slow, medium, fast), and 3 spoofing attempts produced by
- the motion of a user photo (shift-rotation, bending, zoom).
- The experiments use specific moves just to have a well-defined test-bed and to better analyze classes of moves (simple, composite), but the system works with any move.

Antispoofing for moving faces

Tested Geometric Invariants

Table 1 EER for varying motion type and speed, when K is 25.

	yaw	pitch	yaw+pitch
Slow	0.35	0.70	0.35
Medium	0.29	0.70	0.00
Fast	0.00	0.29	0.00

Table 2 EER values with varying values of K parameter and of speed, for yaw+pitch motion.

	5 frame	10 frame	15 frame	20 frame	25 frame
Slow	0.70	0.58	0.35	0.35	0.35
Medium	0.64	0.58	0.35	0.29	0.00
Fast	0.06	0.00	0.00	0.00	0.00

FATCHA: Face cAPTCHA

What is a CAPTCHA ?

- *Completely Automated Public Turing test to tell Computers and Humans Apart*
- Prevents bots from using/abusing certain services
- Provides solution by requiring users to do something trivial for
- human but complicated for machine

FATCHA: Face cAPTCHA

CAPTCHA Approaches

- reCAPTCHA (Google)

FATCHA: Face cAPTCHA

CAPTCHA Approaches

- reCAPTCHA (Google)
- Imagination CAPTCHAs (*R.Datta*, *J.Li*, *J.Z.Wang*)

FATCHA: Face cAPTCHA

CAPTCHA Approaches

- reCAPTCHA (Google)
- Imagination CAPTCHAs (*R.Datta*, *J.Li*, *J.Z.Wang*)
- CAPTCHAs based on image orientation (*R.Gossweiler*, *M.Kamvar*, *S.Baluja*)

FATCHA: Face cAPTCHA

CAPTCHA Approaches

- reCAPTCHA (Google)
- Imagination CAPTCHAs (*R.Datta*, *J.Li*, *J.Z.Wang*)
- CAPTCHAs based on image orientation (*R.Gossweiler*, *M.Kamvar*, *S.Baluja*)
- ARTiFACIAL (*Y.Rui*, *Z.Liu*)

FATCHA: Face cAPTCHA

CAPTCHA limitations

Usability

- CAPTCHA based on text is hard for machine but sometimes hard for users too
- If task is too difficult, users are frustrated
- Approaches based on images creates less problems to *most* users

Accessibility

- CAPTCHAs based on reading text or on other visual-perception task:
  - Blind or visually impaired users have problems in access to services protected by both this types of CAPTCHAs
  - Blind users generally use assistive technologies such as screen readers but CAPTCHAs are designed to be unreadable by machines
  - Audio CAPTCHAs are a partial solution but only for blind users, not for those are both visually and hearing impaired

FATCHA: Face cAPTCHA

Security

- EZ-GIMPY and GIMPY CAPTCHAs breaking 92% and 33% of the time respectively *(G.Mori, J.Malik)*
- PWNtcha (*S.Hocevar*) decoder for text based CAPTCHA
- “Simple” audio reCAPTCHA bypassed with Google’s Web Speech API attack
- ARTiFACIAL bypassed using computer vision attack (*Q.Li*)

FATCHA: Face cAPTCHA

FATCHA: Kill two (and more) birds with one stone

(in italian it is more gentle: catch two pigeons with one fava bean)

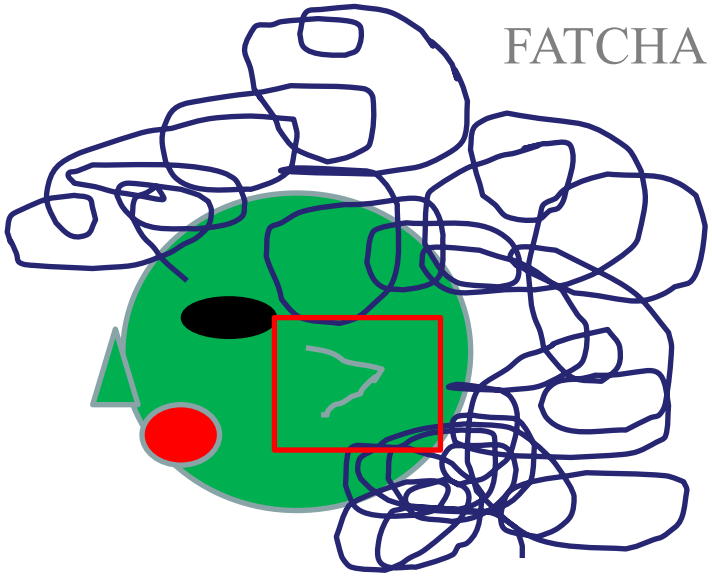
- Reduces the active role of the user to a very easy action: gesture
- Does not involve any perceptual and cognitive task
- Asks the user to produce rather than analyze something
- The user is the CAPTCHA

FATCHA: Face cAPTCHA

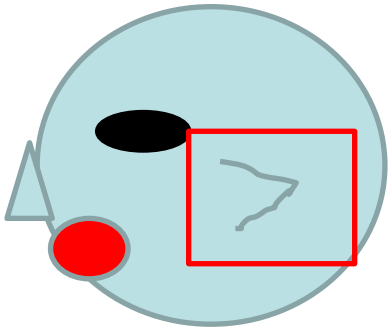
- Asks the user to produce rather than analyze something
- The server chooses **randomly** from a possibly wide yet simple set of gestures and poses (limited to face and may be hand to enforce)
- The server **checks** the user ***action*** and produces a response like in classical CAPTCHAs implementation
- Challenge is in (difficult to automatically recognize) graphical form

FATCHA: Face cAPTCHA

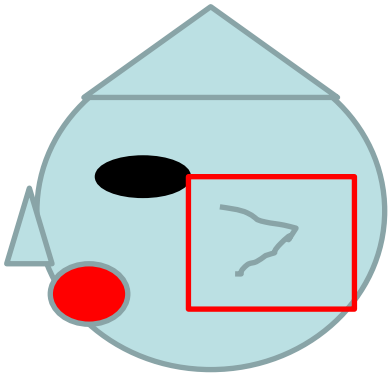
FATCHA challenge



(b)



(a)



(c)

Possible challenges: Show the object in the red square to the camera

Challenge: still to solve the accessibility problem

FATCHA: Face cAPTCHA

FATCHA as antispoofing

- **The server chooses randomly from a possibly wide yet simple set of gestures and poses (limited to face and may be hand to enforce)**
- **The server checks the user *action* and produces a response like in classical CAPTCHAs implementation**
- Interaction-based – more sophisticated than simple eye blinking detection - effective for both photo- (action is requested) and video-based attacks (specific action is requested)

Some references

- Pan, G., Sun, L., Wu, Z., & Lao, S. (2007, October). Eyeblink-based anti-spoofing in face recognition from a generic webcamera. In *Computer Vision, 2007. ICCV 2007. IEEE 11th International Conference on* (pp. 1-8). IEEE.
- Kim Y., Na J., Yoon S., and Yi J., "Masked fake face detection using radiance measurements," *J. Opt. Soc. Amer. A*, vol. 26, no. 4, pp. 760–766, 2009.
- X. Tan, Y. Li, J. Liu and L.Jiang, Face Liveness Detection from A Single Image with Sparse Low Rank Bilinear Discriminative Model, in Proceedings of 11th European Conf. on Computer Vision (ECCV'10), Crete, Greece. September 2010.
- Määttä, J., Hadid, A., & Pietikäinen, M. (2011, October). Face spoofing detection from single images using micro-texture analysis. In *Biometrics (IJCB), 2011 international joint conference on* (pp. 1-7). IEEE.
- Kose, N., & Dugelay, J. L. (2012, May). Classification of captured and recaptured images to detect photograph spoofing. In *Informatics, Electronics & Vision (ICIEV), 2012 International Conference on* (pp. 1027-1032). IEEE.
- Määttä, J., Hadid, A., & Pietikäinen, M. (2012). Face spoofing detection from single images using texture and local shape analysis. *IET biometrics*, *1*(1), 3-10.
- Anjos, A., Chakka, M. M., & Marcel, S. (2013). Motion-based counter-measures to photo attacks in face recognition. *IET biometrics*, *3*(3), 147-158.
- Kose N. and Dugelay J.-L., "Countermeasure for the protection of face recognition systems against mask attacks," in *Proc. IEEE Int. Conf. Autom. Face Gesture Recognit.*, Apr. 2013, pp. 1–6.

Some references

- Erdogmus, N., & Marcel, S. (2014). Spoofing face recognition with 3D masks. *IEEE transactions on information forensics and security*, *9*(7), 1084-1097.
- Hadid, A. (2014). Face biometrics under spoofing attacks: Vulnerabilities, countermeasures, open issues, and research directions. In *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops* (pp. 113-118).
- Galbally, J., Marcel, S., & Fierrez, J. (2014). Biometric antispoofing methods: A survey in face recognition. *IEEE Access*, *2*, 1530-1552.
- Patel, K., Han, H., Jain, A. K., & Ott, G. (2015, May). Live face video vs. spoof face video: Use of moiré patterns to detect replay video attacks. In *Biometrics (ICB), 2015 International Conference on* (pp. 98-105). IEEE.
- Wen, D., Han, H., & Jain, A. K. (2015). Face spoof detection with image distortion analysis. *IEEE Transactions on Information Forensics and Security*, *10*(4), 746-761.
- Galdi, C., Nappi, M., & Dugelay, J. L. (2016). Multimodal authentication on Smartphones: combining iris and sensor recognition for a double check of user identity. *Pattern Recognition Letters*, *82*, 144-153.
- Ali, A., Hoque, S., & Deravi, F. (2016). Gaze stability for liveness detection. *Pattern Analysis and Applications*, 1-13.

Some references

- Liu, S., Yang, B., Yuen, P. C., & Zhao, G. (2016). A 3D Mask Face Anti-spoofing Database with Real World Variations. In *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops* (pp. 100-106).
- Liu, S., Yuen, P. C., Zhang, S., & Zhao, G. (2016, October). 3D Mask Face Anti-spoofing with Remote Photoplethysmography. In *European Conference on Computer Vision* (pp. 85-100). Springer International Publishing.
- Banerjee, S., & Ross, A. (2017, April). From image to sensor: Comparative evaluation of multiple PRNU estimation schemes for identifying sensors from NIR iris images. In *Biometrics and Forensics (IWBF), 2017 5th International Workshop on* (pp. 1-6). IEEE.