Pupil dynamics for presentation attack detection in iris recognition

Adam Czajka

Biometric Laboratories
NASK & Warsaw University of Technology

International Biometric Performance Conference
Gaithersburg, April 1-3, 2014
Static eye imitations

Eye models

Biometric image of the authentic iris

Foil and paper printouts

Biometric images of the artefacts

Paper printout

Printed contact lens

Prosthetic eye
1. Static 2D images
   - paper and foil printouts
   - images displayed on a screen (hypothetical)
   - simple but alarming: possible impersonation of a given eye

2. Static 3D objects
   - authentic eye + printed contact lens
   - prosthetic eyes
   - impersonation difficult or impossible; typical aim: disturbing an iris pattern to cause a false rejection
Countermeasures for static eye imitations

1. Passive measurement
   • 2D liveness features: frequency analysis, use of local binary patterns, use of thermal data
   • 3D liveness features: eyeball shape, iris tissue structure, Purkinje reflections

2. Active measurement
   • positions of stimulated NIR reflections
   • tissue absorption for different NIR wavelengths

Example thermal image of the eyes (left) and 3D structure of the iris (right)
Dynamic eye imitations

1. Deformable objects with printed iris patterns
2. Movies displayed on a screen, off-line or on-line (hypothetical)
3. Image capture under coercion

Countermeasures for dynamic eye imitations

1. Passive measurement:
   analysis of involuntary activities of the eye
   • spontaneous oscillations of the pupil size
   • detection of spontaneous blinks

2. Active measurement:
   use of voluntary activities of the eye
   • gaze detection when following moving objects
   • eyeball dynamics (analysis of fixations and saccades)
   • pupil dynamics (modeling of pupil size variations when stimulated by visible light)
Liveness features: channel gains \((K_i, K_r)\),
time constants \((T_1, T_2, T_3)\) and delays \((\tau_1, \tau_2)\)

\[ x \quad \frac{-K_r s}{(1 + sT_1)(1 + sT_2)} \quad e^{-\tau_1 s} \quad y \]

\[ \frac{-K_i}{(1 + sT_3)} \quad e^{-\tau_2 s} \quad + \]

\(x\) - visible light intensity
\(y\) - pupil size
**Modeling of pupil dynamics**

Clynes Kohn nonlinear model

**Liveness features:** channel gains ($K_i$, $K_r$),
time constants ($T_1$, $T_2$, $T_3$) and delays ($\tau_1$, $\tau_2$)

\[ x \xrightarrow{\frac{-K_r s}{(1+sT_1)(1+sT_2)}} e^{-\tau_1 s} \xrightarrow{-K_i}{(1+sT_3)} e^{-\tau_2 s} \xrightarrow{\text{+}} y \]

$x$ - visible light intensity

$y$ - pupil size
Liveness features: channel gains ($K_i$, $K_r$),
time constants ($T_1$, $T_2$, $T_3$) and delays ($\tau_1$, $\tau_2$)

$x$ - visible light intensity
$y$ - pupil size
Liveness features: channel gains ($K_i$, $K_r$),
time constants ($T_1$, $T_2$, $T_3$) and delays ($\tau_1$, $\tau_2$)
Modeling of pupil dynamics
Model identification (finding a best fit)

\[
\hat{\phi} = \arg\min_{\phi \in \Phi} \sum_{i=1}^{N} (\hat{y}_{i;\phi} - y_i)^2
\]

where:

\(\phi = [K_r, K_i, T_1, T_2, T_3, \tau_1, \tau_2]^T\) – liveness features
\(\Phi\) – set of possible values of \(\phi\)
\(\hat{\phi}\) – identified liveness features
\(\hat{y}_{i;\phi}\) – model output given the liveness features \(\phi\)
\(y_i\) – actual (observed) change of the pupil size
\(N\) – length of the observed sequence
1. Classification

- use of Support Vector Machine to classify samples in $\phi$-space
- SVM maximizes the gap between samples of different classes
- SVM may solve linear and non-linear problems (use of ‘kernel trick’)

2. Goodness of fit

- use of normalized root mean square error

\[
\text{GoF} = 1 - \frac{\| \hat{y}_\phi - y \|}{\| \hat{y}_\phi - \bar{y} \|}
\]

where $\bar{y}$ is an average of $y$. 
Question 1: How to simulate odd reactions of the eye?

- using static objects $\rightarrow$ we’re doomed to succeed
- simulation of the coerced use $\rightarrow$ not really feasible
Questions

Question 1: How to simulate odd reactions of the eye?
- using static objects → we’re doomed to succeed
- simulation of the coerced use → not really feasible

Question 2: Should we uncritically rely on classifier output?
- misclassifications always happen, so what about other metrics, e.g. goodness of fit?
Question 1: How to simulate odd reactions of the eye?
  • using static objects → we’re doomed to succeed
  • simulation of the coerced use → not really feasible

Question 2: Should we uncritically rely on classifier output?
  • misclassifications always happen, so what about other metrics, e.g. goodness of fit?

Question 3: How long shall we observe the eye?
  • larger times give better modeling, but decrease usability
1. **Collection of samples**
   - involuntary pupil oscillations under no light changes
   - pupil reaction to positive and negative jumps in light intensity
   - $N = 25$ volunteers $\times$ 2 eyes $\times$ $K = 4$ samples $= 200$ samples

2. **Representatives of actual and odd reactions**
   - involuntary pupil oscillations as **odd reactions**
   - stimulated changes in pupil size as **actual reactions**
   - pupil modeled as a circle; pupil size $=$ circle radius

3. **Division of dataset into training and testing subsets**
   - leave-one-out cross-validation
   - ‘one’ relates to the person, not a single sequence
   - $N$ divisions; in each division: $2(N − 1)K$ training samples and $2K$ testing samples
Database of eye reactions to light changes
Re: Question 1 (How to simulate odd reactions of the eye?)
Decisions of linear SVM
Observation time: 5 seconds

Classifier: linear SVM. Observation time: 5 sec.

ACCEPT

Correct reaction of the eye
Odd (or no) reaction of the eye

REJECT

SVM decision

Goodness of fit: normalized root mean square error (NRMSE)
Decisions of linear SVM + goodness of fit
Re: Question 2 (Should we uncritically rely on classifier output?)

Classifier: linear SVM. Observation time: 5 sec.

- Correct reaction of the eye
- Odd (or no) reaction of the eye

SVM decision

Goodness of fit: normalized root mean square error (NRMSE)
Modeling horizon (observation time)

Re: Question 3 (How long shall we observe the eye?)

- Modeling horizon: 2 seconds
  - Change in pupil radius (pixels) vs. time (seconds)
  - Time range: 0 to 5 seconds
  - Change range: -100 to 0 pixels

- Modeling horizon: 3 seconds
  - Change in pupil radius (pixels) vs. time (seconds)
  - Time range: 0 to 5 seconds
  - Change range: -100 to 0 pixels

- Modeling horizon: 4 seconds
  - Change in pupil radius (pixels) vs. time (seconds)
  - Time range: 0 to 5 seconds
  - Change range: -100 to 0 pixels

- Modeling horizon: 5 seconds
  - Change in pupil radius (pixels) vs. time (seconds)
  - Time range: 0 to 5 seconds
  - Change range: -100 to 0 pixels

Adam Czajka | IBPC 2014 | 18/24
FerrLive and FerrFake vs. observation time

Linear SVM, goodness of fit not considered

Classifier: linear SVM

- FerrLive
- FerrFake

Regression for FerrLive
Regression for FerrFake

observation time (sec)

error estimator

Adam Czajka | IBPC 2014 | 19/24
FerrLive and FerrFake vs. observation time
Linear SVM, goodness of fit considered

Classifier: linear SVM

-0.005
0
0.005
0.01
0.015
0.02
0.025

error estimator

FerrLive
FerrFake with goodness of fit
Regression for FerrLive
Regression for FerrFake with goodness of fit

observation time (sec)
2 3 4 5

FerrLive and FerrFake vs. observation time
Linear SVM, goodness of fit considered

Classifier: linear SVM

-0.005
0
0.005
0.01
0.015
0.02
0.025

error estimator

FerrLive
FerrFake with goodness of fit
Regression for FerrLive
Regression for FerrFake with goodness of fit

observation time (sec)
2 3 4 5

Adam Czajka | IBPC 2014 | 20/24
FerrLive and FerrFake vs. observation time
SVM with Gaussian kernel, goodness of fit not considered

Classifier: SVM with nonlinear kernel (RBF)
FerrLive and FerrFake vs. observation time
SVM with Gaussian kernel, goodness of fit considered

Classifier: SVM with nonlinear kernel (RBF)

- FerrLive
- FerrFake with goodness of fit
- Regression for FerrLive
- Regression for FerrFake with goodness of fit
Conclusions

1. Dynamics of the pupil delivers interesting liveness features
2. Depending on the assumed dynamics of fake objects, linear classification seems to be sufficient to recognize artefacts
3. Having a few additional seconds (≥ 3) while capturing the iris may provide almost perfect recognition of actual and odd behavior of the pupil
Adam Czajka, Ph.D.
aczajka@elka.pw.edu.pl

Biometrics Laboratory
Research and Academic Computer Network (NASK)
Warsaw, Poland

Biometrics and Machine Learning Laboratory
Warsaw University of Technology
Warsaw, Poland