FACE FLASHING:
A SECURE LIVENESS DETECTION PROTOCOL BASED ON LIGHT REFLECTIONS

Di Tang\textsuperscript{1}, Zhe Zhou\textsuperscript{2}, Yinqian Zhang\textsuperscript{3}, Kehuan Zhang\textsuperscript{1}

The Chinese University of Hong Kong\textsuperscript{1}
Fudan University\textsuperscript{2}
The Ohio State University\textsuperscript{3}
Face-based Authentication Will Become Popular

Online payment

Door entrance

ATM withdraw

Phone unlock
Face Recognition Is Not Enough

Easy-obtained faces
Face Recognition Is Not Enough

- Easy-obtained faces
- High-resolution printers/screens
- Powerful CPUs/GPUs
- Developed technologies
Liveness Detection Is Necessary

Detect whether the subject under authentication is a real human.
Liveness Detection Is Hard to Be Done Right

Texture extraction methods:

- Local Binary Pattern (LBP)
- 2D Fourier Spectra
- ...

High-resolution screen will fail it.

---- It can outputs any patterns you want
Liveness Detection Is Hard to Be Done Right

Challenge-response protocols:

- Eye blink
- Expression
- Head movement
- Speaking
Human Reaction Time

Machines can do $10^9$ flops, in 260MS

www.humanbenchmark.com
Machines Are Powerful

3D reconstruction

Face morphing
Machines Are Powerful

Expression synthesizing
Fundamental Problem ?
Fundamental Problem?

No strong security guarantee!

Details

Precision

Trembling

Ability
Weakness of Human Reactions

Limited speed

Uncertainty

Smart device + Screen can fail it

2D dynamic attacks (e.g., Media-based Facial Forgery)
What We Want to Do?

Solid stone
to build a secure protocol

Human reaction

Relieve threats
from 2D dynamic attacks
Non-digital
physical

Light reflection
Features of Light Reflection

Fastest in the universe
  -- No computers can generate fake responses at the same speed, no matter how powerful it will be

Without human reaction

Can capture rich information
  -- 3D shape -> eyes, nose
  -- Texture -> skin vs. non-skin
Reflection Model

\[ I_c(x) = \int_\Omega E(x, \lambda)R(x, \lambda)S_c(\lambda)\,d\lambda, c \in \{r, g, b\} \]

E: Illumination  
R: Reflectance  
S: Sensor response function  
\( \lambda \): Wave length  
x: position of a given point

We will separately consider R,G,B channels. There are no inter-effect among them, if we use the raw data (before AWB).
Reflection Model

\[ I_c = E_c \times R_c, c \in \{r, g, b\} \]

E: Incoming light
R: Reflectance

Get reflectance:

To check face

\[ \frac{I_c(x)}{I_c(y)} = \frac{R_c(x)}{R_c(y)}, c \in \{r, g, b\} \]

Get illumination:

To check time

\[ \frac{I_{c1}(x)}{I_{c2}(x)} = \frac{E_{c1}(x)}{E_{c2}(x)}, c1, c2 \in \{r, g, b\} \]

The reflections is determined by incoming light
Without knowing the incoming light, it is impossible to pre-calculate the reflected light.
Design

Things to verify:
1. Response time
2. Face information
3. Expressions
Verifying the Timing is Difficult

Challenging!!

Reflections happen at speed of light

But camera is not

  Limited by the refreshing speed
  \( \Rightarrow \) around 30 fps

Does it mean powerful attackers with high speed camera and displaying devices can bypass?
Working Details of Camera
Anytime, there are always sensors awake
Detecting tiny differences in time is possible
Both camera and LCD monitor work in a scanning pattern. So what will happen?

Assumption:
No modification can be added to the buffer that is being displayed
Partially Captured Images

Screen

camera refresh direction

camera refresh direction

Camera
How to verify?
Challenges

Background challenge

Lighting challenge
Response and Challenge

Get challenges:

\[
\frac{I_{c1}(x)}{I_{c2}(x)} = \frac{E_{c1}(x)}{E_{c2}(x)}, \quad c1, c2 \in \{r, g, b\}
\]
Calculate the Location

The Challenge image (with lighting area)

Camera

Forgery -> Delay -> Wrong location

Accumulation:

\[
d_i = \hat{y}_i - \frac{u_i + d_i}{2}
\]

\[
mean_d = \frac{\sum_{i=1}^{n} d_i}{n}
\]

\[
std_d^2 = \frac{\sum_{i=1}^{n} (d_i - mean_d)^2}{n-1}
\]
Face Feature Verification

Get reflectance:

\[ \frac{I_c(x)}{I_c(y)} = \frac{R_c(x)}{R_c(y)}, c \in \{r, g, b\} \]

Put it into a Neural network for classification
Evaluation
Sensitivity to Forged Responses
Timing: Camera VS. Mirror

(a) scenario

(b) results

Mirror’s

Laptop’s

Device A

Device B
### TABLE II: Four different screens.

<table>
<thead>
<tr>
<th>Screen</th>
<th>Resolution</th>
<th>Pixel Density</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 HUAWEI P10</td>
<td>1920*1080</td>
<td>432 (ppi)</td>
</tr>
<tr>
<td>2 iPhone SE</td>
<td>1136*640</td>
<td>326 (ppi)</td>
</tr>
<tr>
<td>3 AOC Monitor (e2450Swh)</td>
<td>1920*1080</td>
<td>93 (ppi)</td>
</tr>
<tr>
<td>4 EIZO Monitor (ev2455)</td>
<td>1920*1200</td>
<td>95 (ppi)</td>
</tr>
</tbody>
</table>

### TABLE III: Experimental results of face verification.

<table>
<thead>
<tr>
<th></th>
<th>Training Ps</th>
<th>Training Ns</th>
<th>Testing Ps</th>
<th>Testing Ns</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total</td>
<td>20931</td>
<td>20931</td>
<td>3000</td>
<td>3000</td>
</tr>
<tr>
<td>Incorrect</td>
<td>329</td>
<td>0</td>
<td>75</td>
<td>0</td>
</tr>
</tbody>
</table>
Robustness

**TABLE IV: Features of scenes.**

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Scenario 1</th>
<th>Scenario 2</th>
<th>Scenario 3</th>
<th>Scenario 4</th>
<th>Scenario 5</th>
<th>Scenario 6</th>
</tr>
</thead>
<tbody>
<tr>
<td>Illumination</td>
<td>good</td>
<td>varying</td>
<td>intense</td>
<td>normal</td>
<td>normal</td>
<td>dark</td>
</tr>
<tr>
<td>Vibration</td>
<td>no</td>
<td>intermittent</td>
<td>normal</td>
<td>normal</td>
<td>intense</td>
<td>intense</td>
</tr>
</tbody>
</table>

![Accuracy Chart](chart.png)

36
Our method will force adversaries to use “3D Dynamic Attack” which is more expensive.

Our method could not handle 3D dynamic attack twins, silicone masks.
Discussion

Our implementation just used 8 different colors

Our implementation needs several seconds to accomplish once authentication

Using ‘albedo curve’ may handle 3D dynamic attacks

Combine with face recognition algorithm could enhance efficiency and effectiveness
Summary

Face Flashing protocol

Effective and efficient method on timing and face verifications

Prototype and empirical evaluations
Thanks