COUNTERFEIT DETECTION
USING PAPER PUF AND MOBILE CAMERAS

Chau-Wai Wong* and Min Wu
UNIVERSITY OF MARYLAND, COLLEGE PARK, USA

November 17, 2015
Introduction and Motivation

- Anti-counterfeiting mechanism: techniques to safeguard consumer goods, documents, and money.

- Existing anti-counterfeiting mechanisms
  - Expensive
  - No ground truth
  - Authenticity rely on manual decision

- Investigate optical features of paper surfaces for anti-counterfeiting:
  - Precision: physical unclonable features (PUFs)
  - Automate verification & ease of use: mobile imaging
  - Relatively low-cost

Physical Features of Paper: Unique 3-D Surfaces

3-D Structure of a 1 mm-by-1 mm Paper Patch
(reconstructed by scans of confocal microscope)

Normal vectors of a microscopic surface:

High-End Camera Captured Patch (1 mm²)

RGB Combined

Red

Green

Blue

**Camera**: Cannon EOS REBEL T2i; EF100mm f/2.8L Macro IS USM. **Capturing Condition**: Exposure 0.3 sec, f/2.8, ISO 100, 300 ppi, patch placed at 2f. Camera mounted on a tripod. **Credit**: King Lam Hui. R, G, and B channels are contrast enhanced.
Scanner and Mobile Camera Captured Patches

Image of scanner captured patch with registration pattern:

- **Registration container** (600 pixels per inch):
  - Square box: 400-by-400 pixels
  - Line width: 5 pixels
  - 4 circles at corners
  - Alignment: Hough transform, perspective transform, and correlation refinement

Contrast enhanced patches:

- **Scanner**
- **iPhone 6**
- **Pantech Tablet**


**Extracted Norm Map**\(^1\)** From 4 Scans**

appearance images from 4 scan directions

estimated norm map

patch size: \(\frac{3}{8}\) in-by-\(\frac{3}{8}\) in, 600 ppi, scanned by Epson 2450

What about using **mobile cameras** for norm map estimation?

---

Challenge to Estimate Norm Map of Paper

- Shape/structure from photometric stereo:


- In our problem, structure exists at a much smaller scale:
Norm Maps: Scales & Scanner Models

scanner 2450

norm map, scale = 1.00

norm map, scale = 0.50

scanner GT2500

norm map, scale = 1.00

norm map, scale = 0.50
Performance of Norm Maps

Cross scanner exp.: Epson GT (test) vs. Epson 2450 (ref)

PDFs for correlation:
- $H_0$: test and ref images are from different patches
- $H_1$: test and ref images are from the same patch

Very good performance!

What about directly using scanned images for authentication?
Performance of Scanned Images

Won’t work if scan dir. are not identical

Reason for **two peaks** of $H_1$: Although test and ref images are acquired from the same patch, there are 2 possible scanning directions.

Appearances differ in small details
Performance of Mobile Images

Limited performance!

Captured images looks similar in high-level but details are quite different.
Performance of Mobile Images

iPhone 6 (test) vs iPhone 6 (ref)

bounds for $H_0$

bounds for ROC

Asymm Exp
Gaussian
### Performances of Different Schemes

<table>
<thead>
<tr>
<th>Device</th>
<th>Feature</th>
<th>Intensity</th>
<th>Norm map</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scanner</td>
<td></td>
<td>◢</td>
<td>★</td>
</tr>
<tr>
<td>Mobile camera</td>
<td></td>
<td>×</td>
<td>−</td>
</tr>
</tbody>
</table>
Exploiting Lighting: Mobile Images

Camera position and image index

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>5</td>
<td>6</td>
<td>7</td>
<td>8</td>
</tr>
<tr>
<td>2</td>
<td>9</td>
<td>10</td>
<td>11</td>
<td>12</td>
</tr>
<tr>
<td>3</td>
<td>13</td>
<td>14</td>
<td>15</td>
<td>16</td>
</tr>
<tr>
<td>4</td>
<td>17</td>
<td>18</td>
<td>19</td>
<td>20</td>
</tr>
</tbody>
</table>
## Performances of Different Schemes

<table>
<thead>
<tr>
<th>Device</th>
<th>Feature</th>
<th>Intensity</th>
<th>Norm map</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scanner</td>
<td></td>
<td>![triangle]</td>
<td>![star]</td>
</tr>
<tr>
<td>Mobile camera (no flash)</td>
<td></td>
<td>![x]</td>
<td></td>
</tr>
<tr>
<td>Mobile camera (with flash)</td>
<td></td>
<td>![triangle]</td>
<td>![blue star]</td>
</tr>
</tbody>
</table>

The table above illustrates the performances of different schemes for detecting counterfeit papers using paper PUF and mobile cameras. The intensity and norm map features are compared across scanner and mobile camera devices, with and without flash.
Authentication Using Camera & Norm Map

**Ground truth** 4 scans of a paper patch

Norm map estimator (x- and y-comp)

Estimated norm map

Statistical Decision rule

AUTHENTIC or NOT

**Test data** Photos of a patch taken at 3+ locations

Normal vector estimator (x-, y-, and z-comp)

Estimated normal vectors
Reflection Model Used – Fully Diffuse

- Perceived intensity unaffected by eye/sensor position.

- Intensity depends only on angle $\theta$ between $\mathbf{n}$ and $\mathbf{v}$

$$l_r(\mathbf{v}) = \lambda \cdot l \cdot n^T \mathbf{v}$$

$\alpha \cos^\kappa \theta \cos \theta$

- $l$ is the strength of the light, and $\kappa$ accounts for energy fall-off.

- $(\lambda \cdot l)$ as a whole can be compensated to obtain normalized intensity $y$ with only the effect of $n^T v$, i.e.,

$$y \approx n^T v$$
“Data” for Parameter Estimation

- Normalized intensity values $y_1, \ldots, y_M$:
  - Image #1 to #M
  - Collocated positions

- Incident directions $v_1, \ldots, v_M$:
  - Light of iPhone 6: one centimeter left to the camera
  - Estimating camera position via geometric transform
Estimated norm map consistent with results by high-precision ones by scanners.
Authentication Performances

Flashlight in a dark room

- x-comp (correct)
- y-comp (correct)
- projected length (correct)
- x-comp (simulated incorrect)
- y-comp (simulated incorrect)
- projected length (simu incor)

Flashlight with ambient light

- Same patch ($H_1$)
- Different patches ($H_0$)
Conclusions

- Norm map: promising features to aid counterfeiting detection.

- First work towards using mobile camera to:
  - Successfully estimate the norm map
  - Enable authentication under a ubiquitous setting (ambient lighting)

- On-going & future work on practical issues:
  - Resiliency against physical tampering, etc.
  - General camera position setup