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

hologram [1]

UV ink [2]

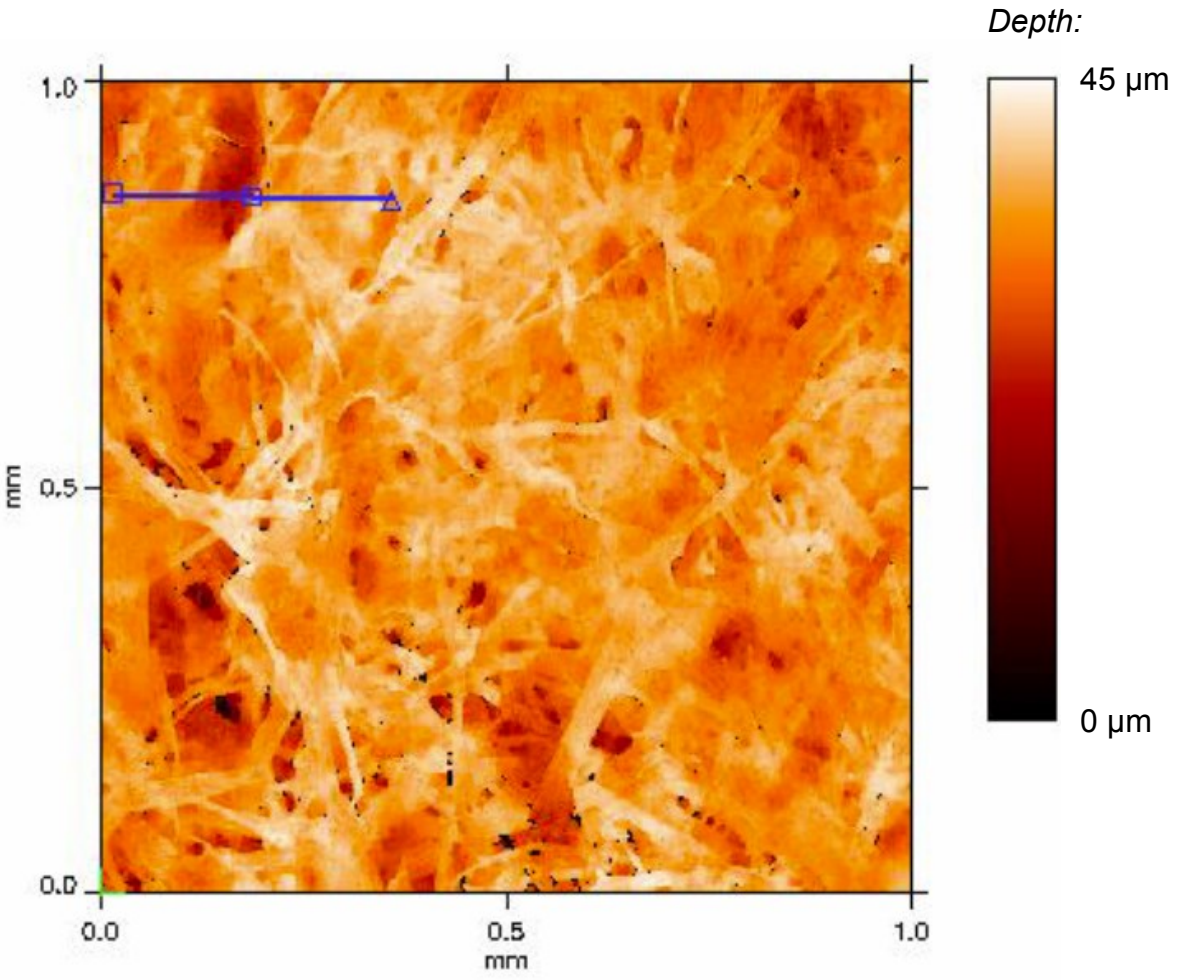
random fibers

- *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

[1] http://www.imagehologram.com/Laser-sticker-anti-counterfeiting-sticker-laser-label-633.html
[2] http://www.prlog.org/10652246-keep-counterfeit-money-out-of-register-with-new-pen-and-uv-light-detector-system.html

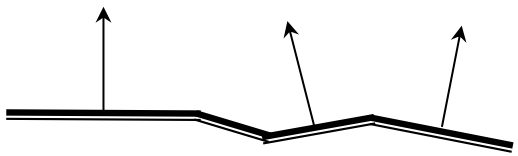
Physical Features of Paper: Unique 3-D Surfaces



3-D Structure of a 1 mm-by-1 mm Paper Patch

(reconstructed by scans of confocal microscope)

Normal vectors of a microscopic surface:

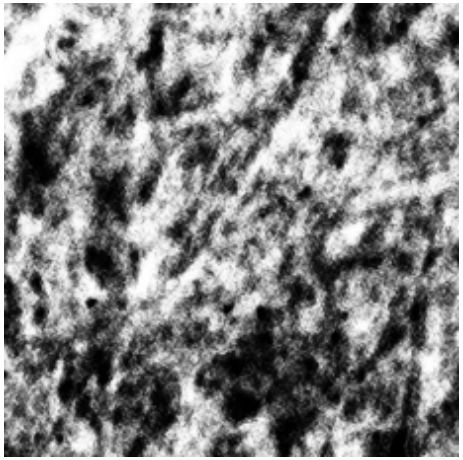


Topography map of copy paper, reproduced from "High resolution surface topography FRT MicroProf chromatic aberration sensor," in a product sheet by Innventia, Aug. 2012.

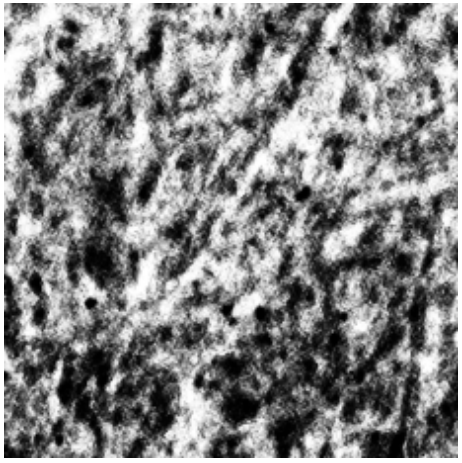
High-End Camera Captured Patch (1 mm^2)

RGB Combined

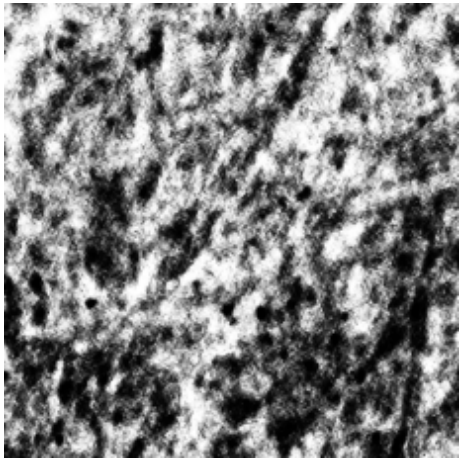
Red



Green



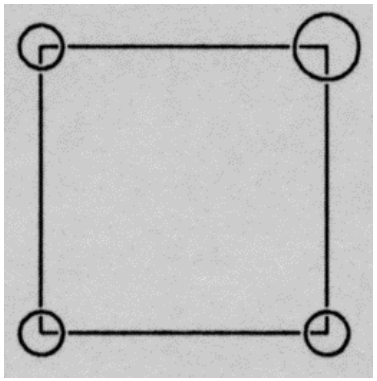
Blue



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

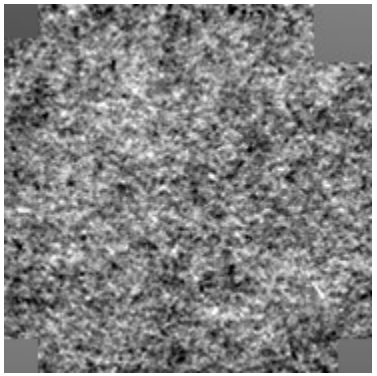
Image of scanner captured patch with registration pattern:



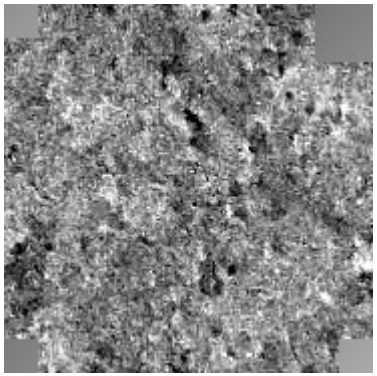
Registration container (600 pixels per inch):

- Square box: 400-by-400 pixels
- Line width: 5 pixels
- 4 circles at corners
- Alignment: Hough transform, perspective transform, and correlation refinement

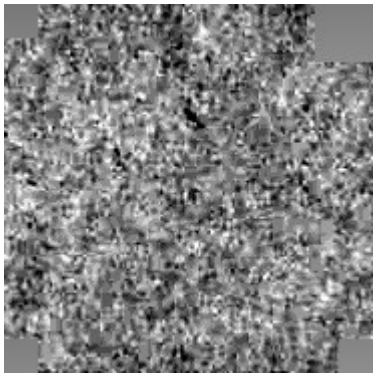
Contrast enhanced patches:



Scanner



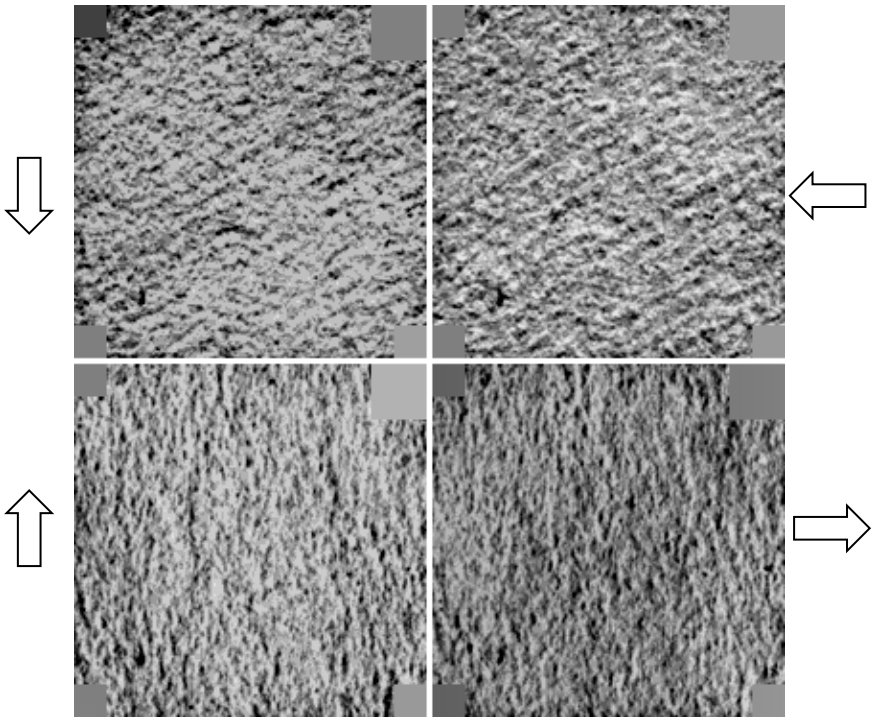
iPhone 6



Pantech Tablet

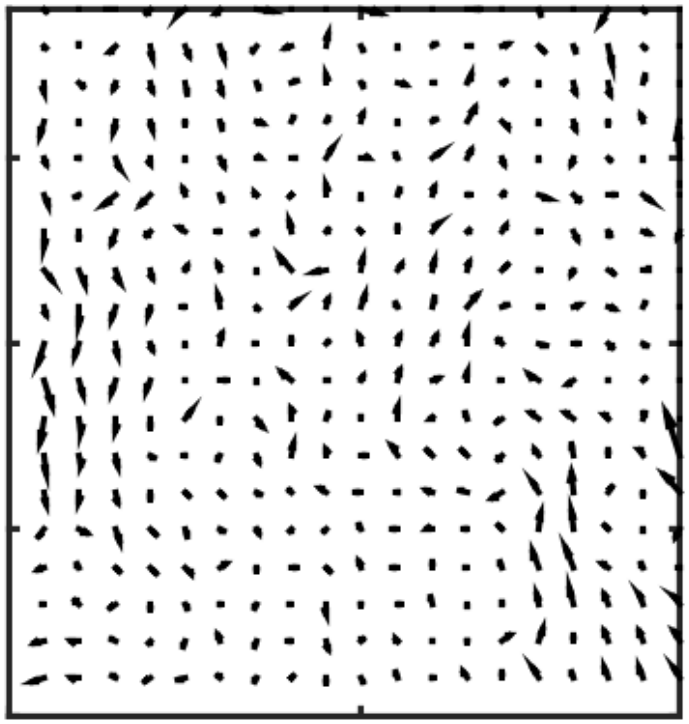
Extracted Norm Map [1] From 4 Scans

appearance images from 4 scan directions



patch size: ⅔ in-by-⅔ in, 600 ppi,
scanned by Epson 2450

estimated norm map

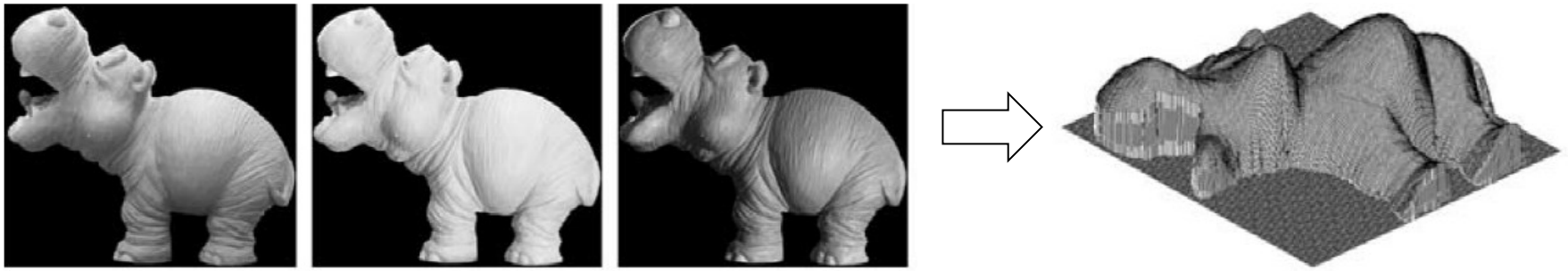


What about using **mobile cameras** for norm map estimation?

[1] W. Clarkson, T. Weyrich, A. Finkelstein, N. Heninger, J. Halderman, and E. Felten, "Fingerprinting blank paper using commodity scanners," in *Proc. IEEE Symposium on Security and Privacy*, Berkeley, CA, May 2009, pp. 301-314.

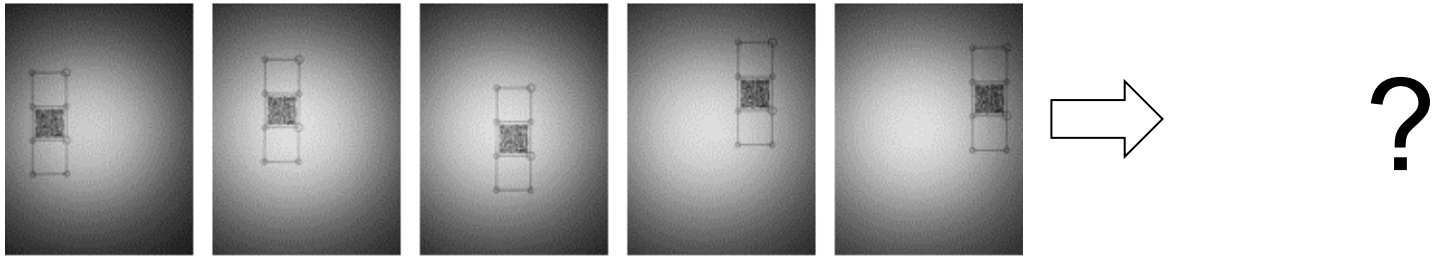
Challenge to Estimate Norm Map of Paper

- Shape/structure from photometric stereo:



R. Basri, D. Jacobs, I. Kemelmacher, "Photometric stereo with general, unknown lighting," *Int'l J. Computer Vision*, May 2007.

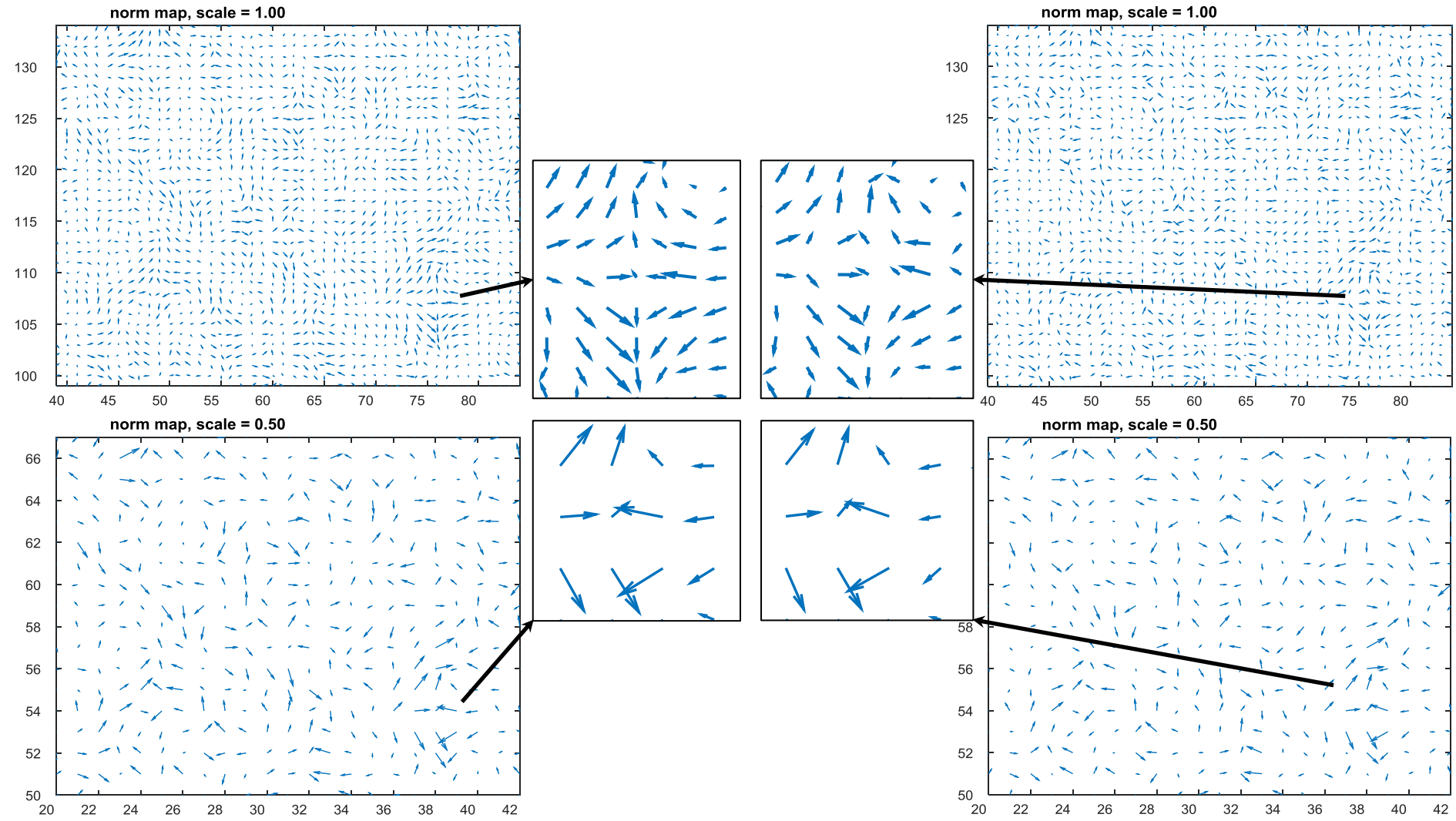
- In our problem, structure exists at a much smaller scale:



Norm Maps: Scales & Scanner Models

scanner 2450

scanner GT2500



Performance of Norm Maps

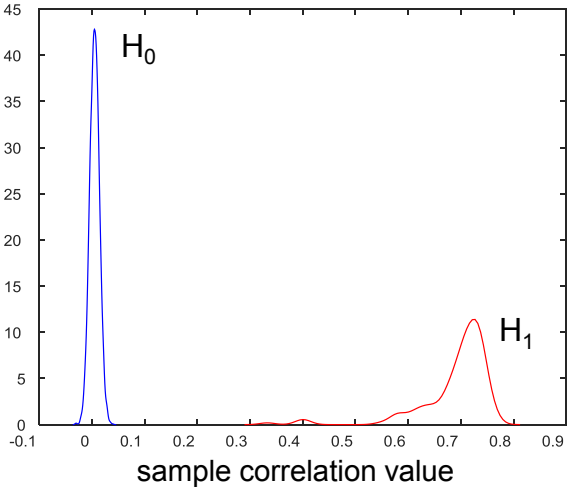
Very good performance!

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

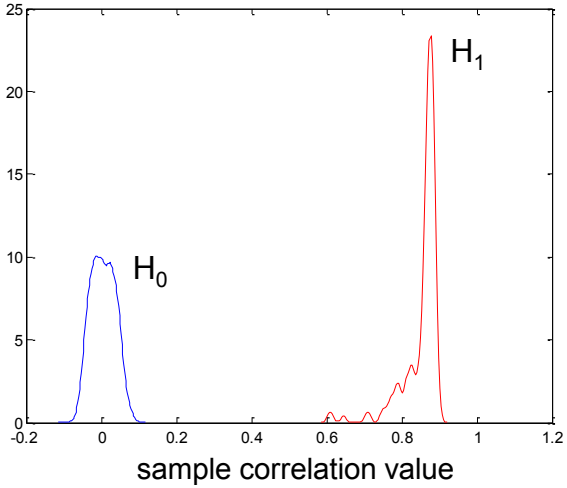
PDFs for correlation:

- **H_0**: test and ref images are from different patches
- **H_1**: test and ref images are from the same patch

Feature: length of norm vector



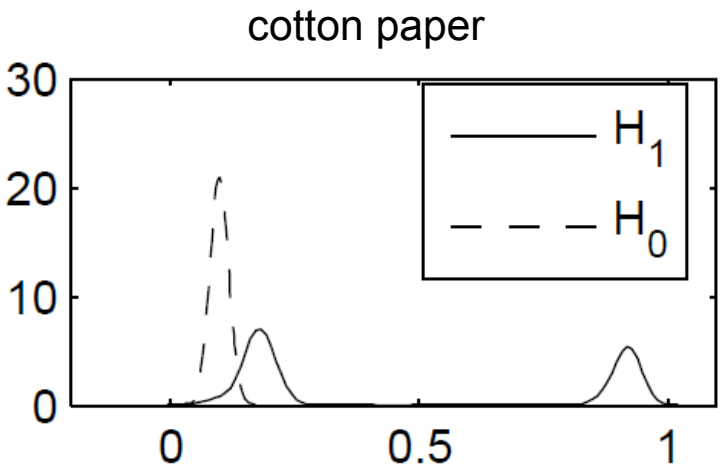
Feature: *x*-component of norm vector

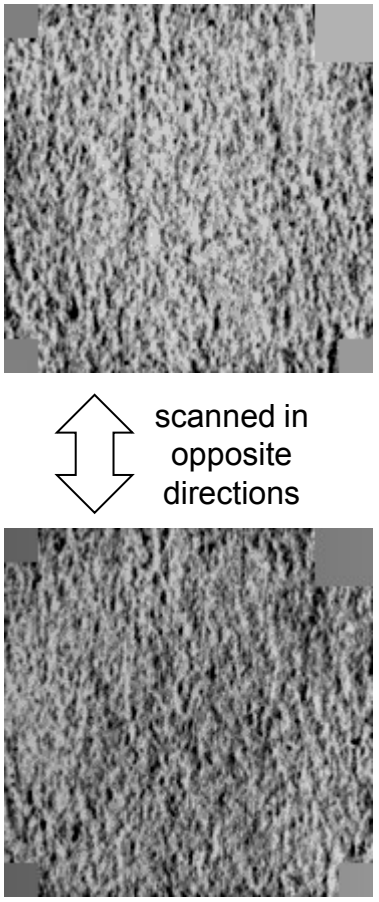


What about directly using *scanned images* for authentication?

Performance of Scanned Images

Won't work if scan dir. are not identical





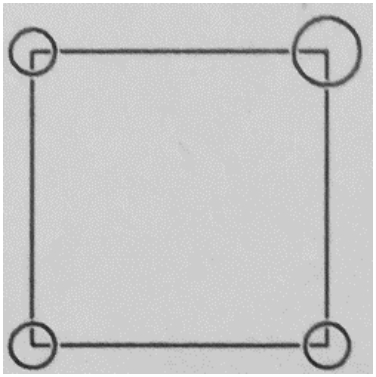
Appearances differ in small details

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

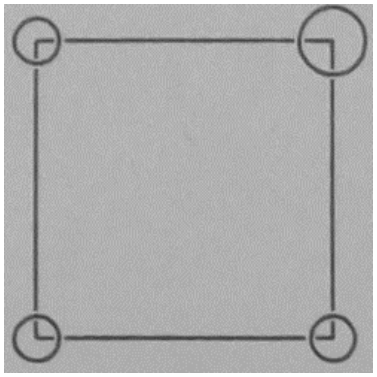
Performance of Mobile Images

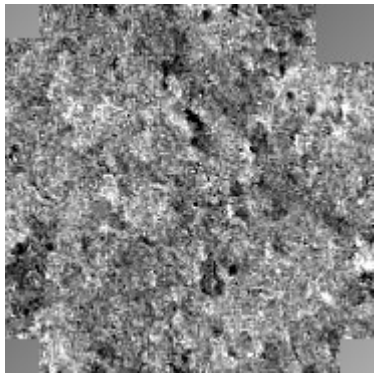
Limited performance!

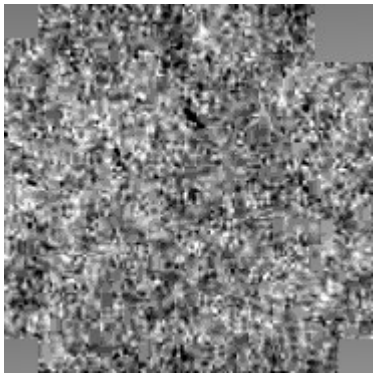
iPhone 6



Pantech Tablet

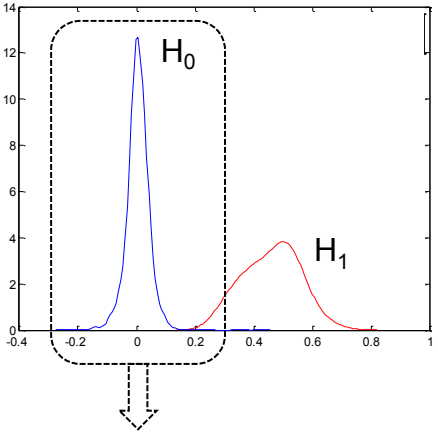




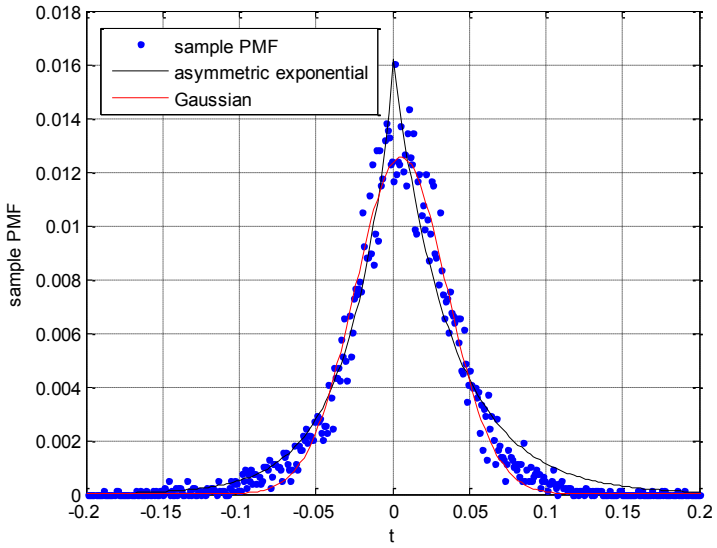


Captured images looks similar in high-level but details are quite different.

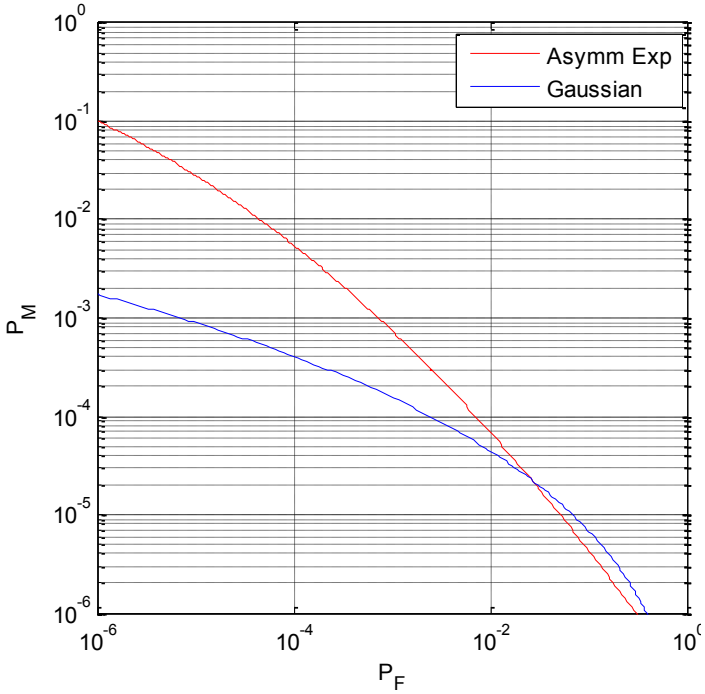
Performance of Mobile Images



iPhone 6 (test)
vs iPhone 6 (ref)



bounds for H_0



bounds for ROC

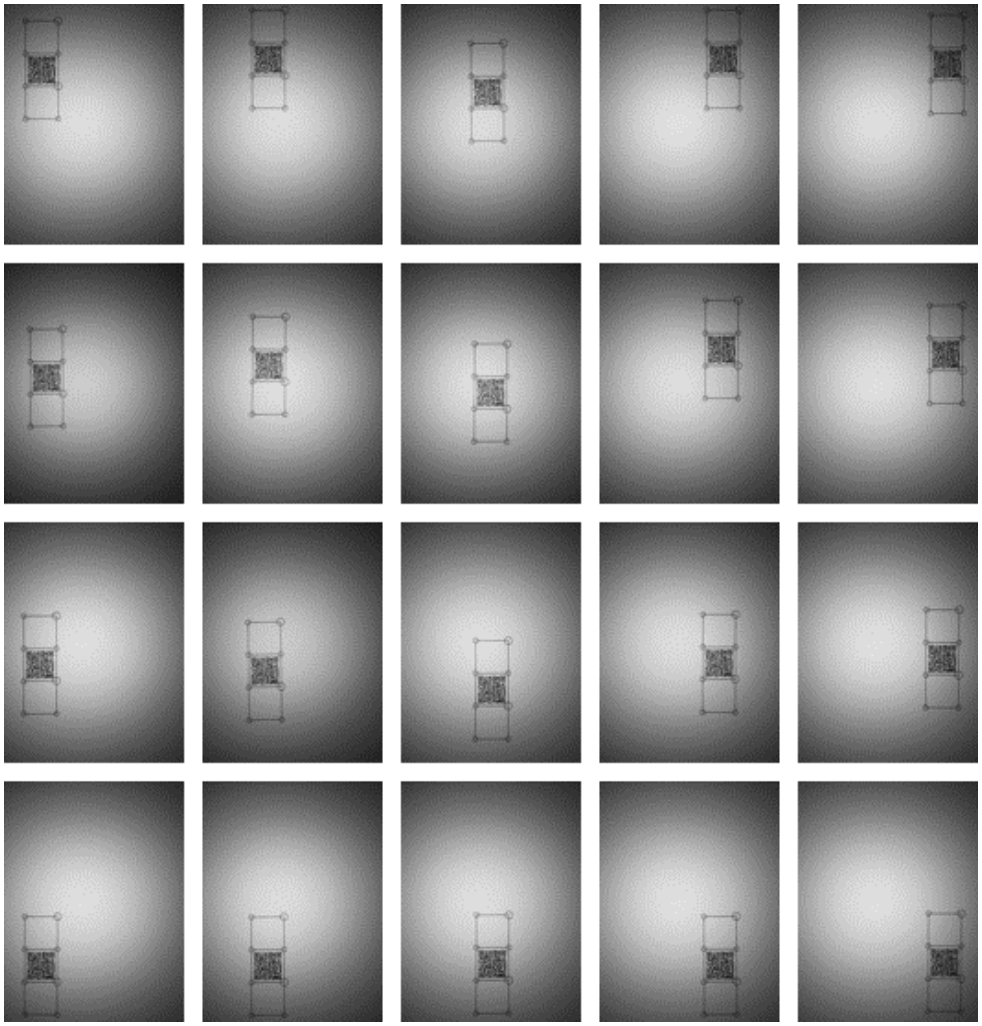
Performances of Different Schemes

Feature / Device	Intensity	Norm map
Scanner	△	☆
Mobile camera	×	–

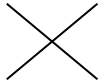
Exploiting Lighting: Mobile Images

Camera position and image index

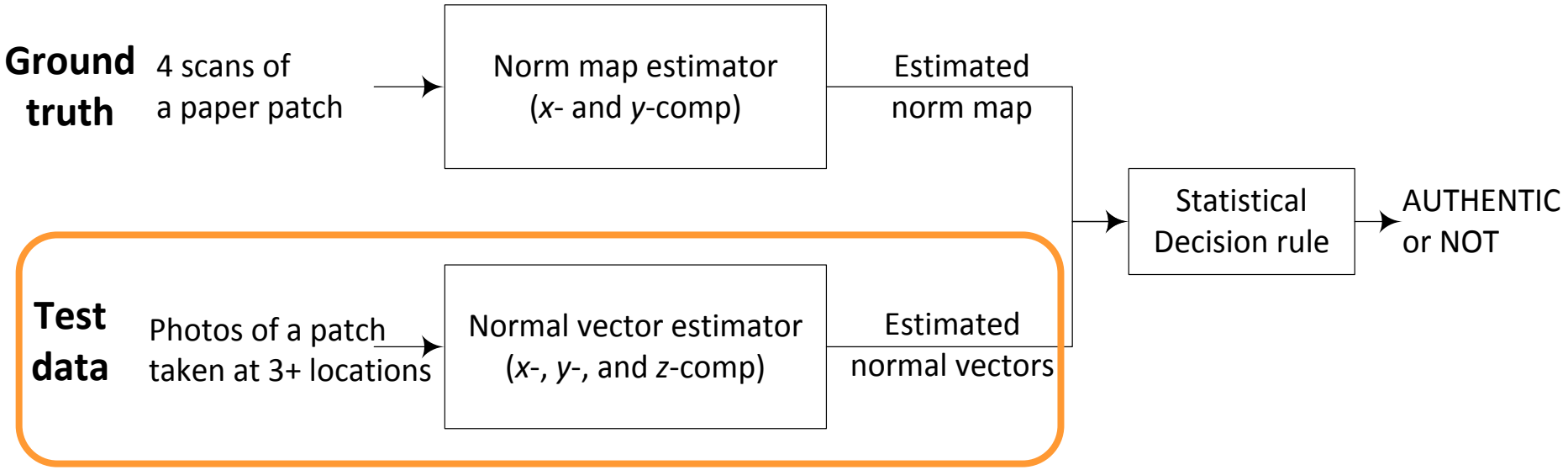
1	5	9	13	17
2	6	10	14	18
3	7	11	15	19
4	8	12	16	20



Performances of Different Schemes

Feature / Device	Intensity	Norm map
Scanner		
Mobile camera (no flash)		–
Mobile camera (with flash)		

Authentication Using Camera & Norm Map



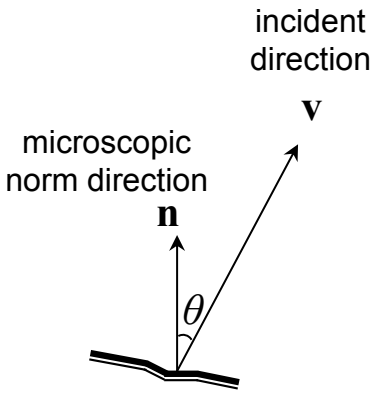
Reflection Model Used – Fully Diffuse

- Perceived intensity unaffected by eye/sensor position.

Diffuse
Specular (mirror-like)

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

$$l_r(\mathbf{v}) = \lambda \cdot \underbrace{l}_{\propto \cos^{\kappa}\theta} \cdot \underbrace{\mathbf{n}^T\mathbf{v}}_{\cos\theta}$$



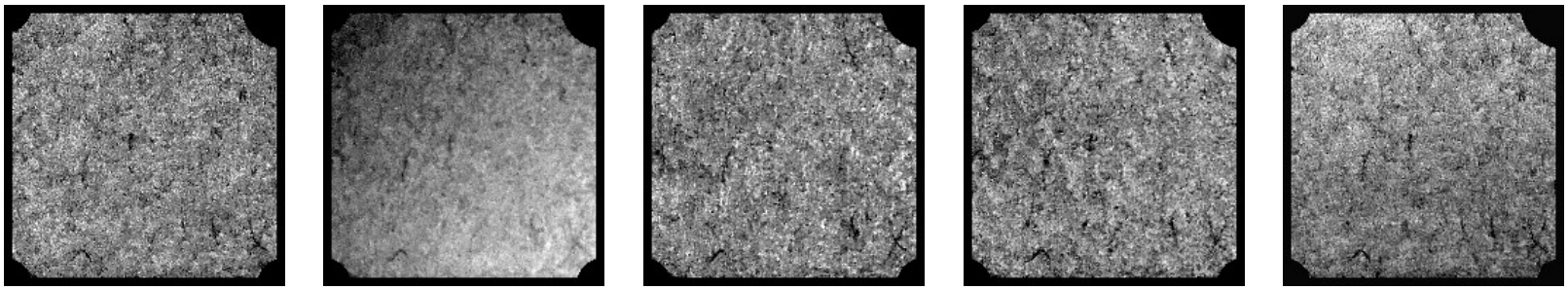
  - l is the strength of the light, and κ accounts for energy fall-off.
  - $(\lambda \cdot l)$ as a whole can be compensated to obtain normalized intensity y with only the effect of $\mathbf{n}^T\mathbf{v}$, *i.e.*,

$$y \approx \mathbf{n}^T\mathbf{v}$$

"Data" for Parameter Estimation

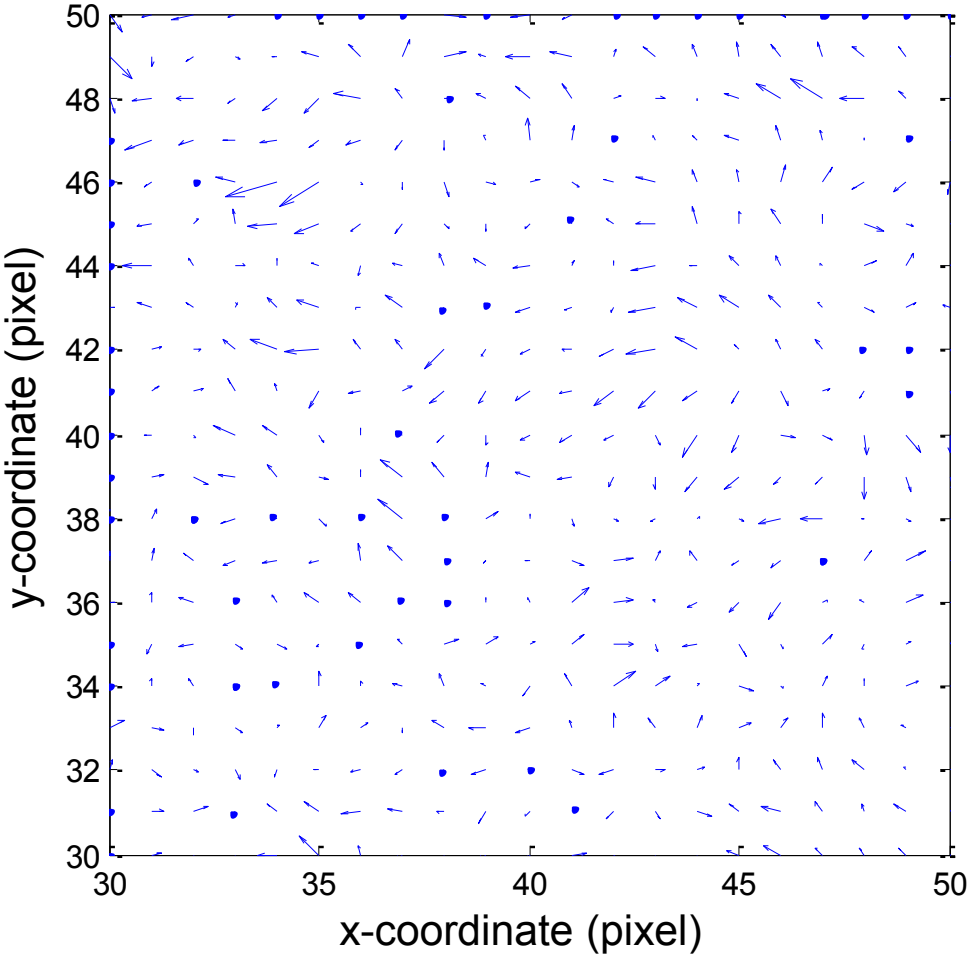
$$y \approx \mathbf{n}^T \mathbf{v}$$

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



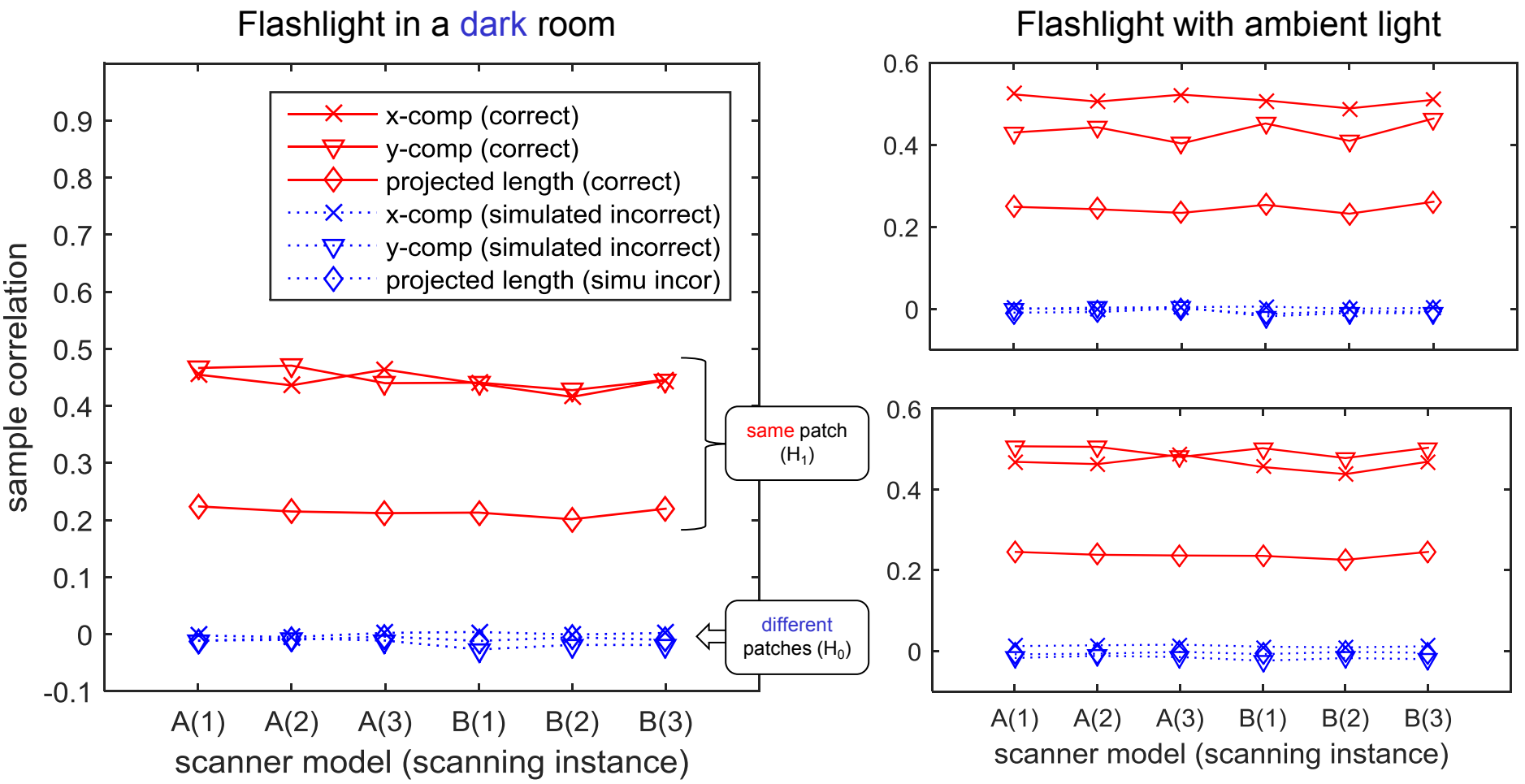
- Incident directions $\mathbf{v}_1, \ldots, \mathbf{v}_M$:
  - Light of iPhone 6: one centimeter left to the camera
  - Estimating camera position via geometric transform

Estimated Norm Map Using iPhone 6



Estimated norm map consistent with results by high-precision ones by scanners.

Authentication Performances



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