A STUDY ON PUF CHARACTERISTICS FOR COUNTERFEIT DETECTION

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

Media & Security Team at UMD
MAST

Introduction

➢ **Anti-counterfeiting**: safeguard consumer goods, documents, money

➢ **Existing mechanisms**

hologram [1]   UV ink [2]   random fibers

Rely on visual examination & decision

➢ **Investigate optical features of surfaces**

- Physical Unclonable Features (**PUFs**): **intrinsic** *vs.* **extrinsic**
- Automation: pre-stored references; use **mobile imaging** to verify
- Relatively low-cost

Alignment of Surfaces

➢ **Designed an alignment pattern**

registration & extraction
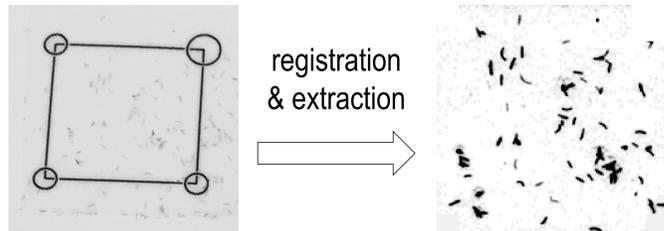
➢ **Algorithm** (⅓-pixel accuracy): Hough transform, perspective transform, *etc.*

References

[1] Laser sticker, *Suzhou Image Laser Tech Co., Ltd.*
[2] DriMark Counterfeit Detector Pen, *DriMark Products, Inc.*
[3] Topography map of a copy paper, *Innventia*
[4] Ramdot™, *ProofTag SAS*
[5] Commercial sticker, *Kinde Tech. Co., Ltd.*

Intrinsic Surface PUFs

➢ **Intrinsic features:**
microscopic **roughness** of paper surface due to inter-twisted fibers

45 μm
0 μm
3-D structure of 1x1 mm² paper [3]
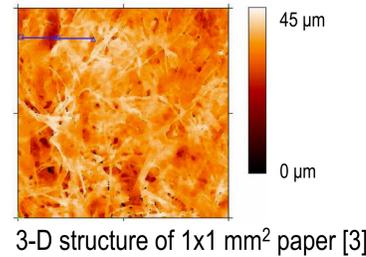
➢ **Norm map** (by scanners)

- Estimable by using 4 scans from different directions
- Clear separation of PDFs of H_1 (test and ref images are from **identical** patch), and H_0 (test and ref images are from **different** patches)

images of 4 scans   estimated norm map   PDFs of $\hat{\rho}$ for H_0 & H_1

Feature: x-component of norm vector
H_1
H_0
sample correlation value $\hat{\rho}$
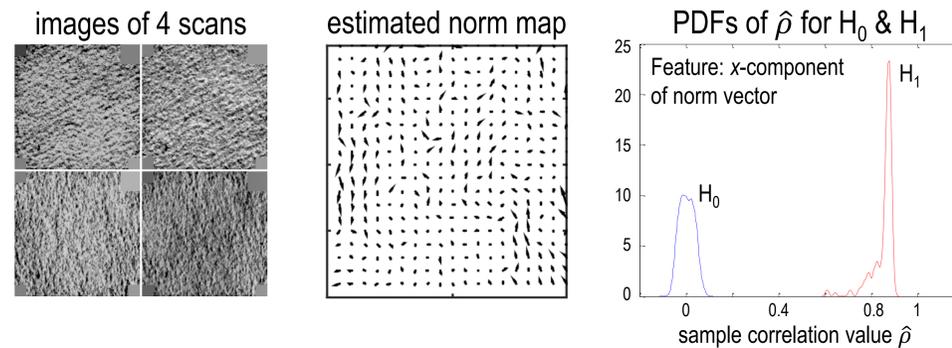
➢ **Appearance image** (by mobile cameras): PDFs overlap → low authentication performance

image (iPhone 6)   PDFs of $\hat{\rho}$ for H_0 & H_1 ROC bounds

H_0
H_1
sample correlation value $\hat{\rho}$

Asymm Exp
Gaussian
P_M
P_F
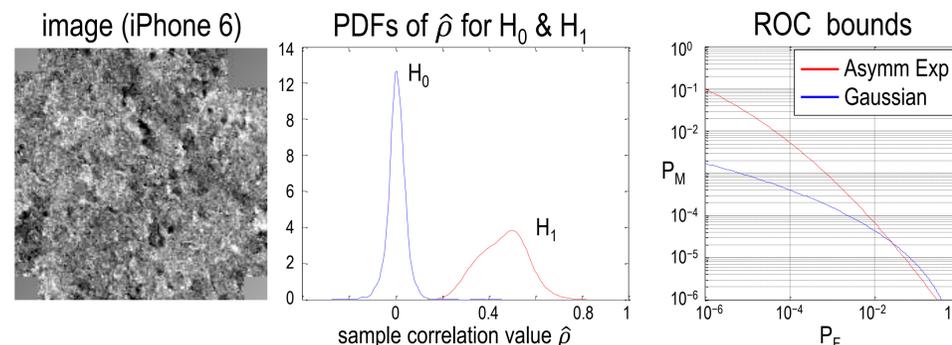
➢ **On-going work**

- Explore using **mobile cameras** for norm map estimation (to appear in WIFS'15)
- Study resilience: folding, water treatment, effect of automatic document feeder, *etc.*

Extrinsic Surface PUFs

➢ **Extrinsic features**

- Foreground objects with random positions, shapes, and orientation
- To understand how authentication performance is controlled by design parameters

randomly positioned color dots [4]   sticker with randomly positioned fibers [5]
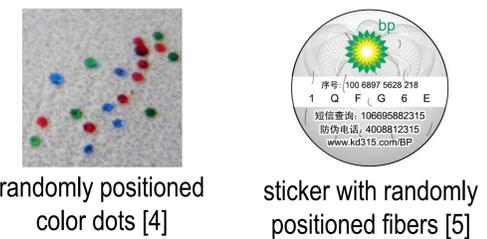
➢ **Lab-produced powder patch**

- Randomly distributed flocking powder, sealed
- High contrast → captured easily; **difficult to clone**
- Clear separation of PDFs of H_0 and H_1
- Denser powder & accurate registration → better

image (iPhone 6)   PDFs of $\hat{\rho}$ for H_0 & H_1

H_0
H_1
sample correlation value $\hat{\rho}$
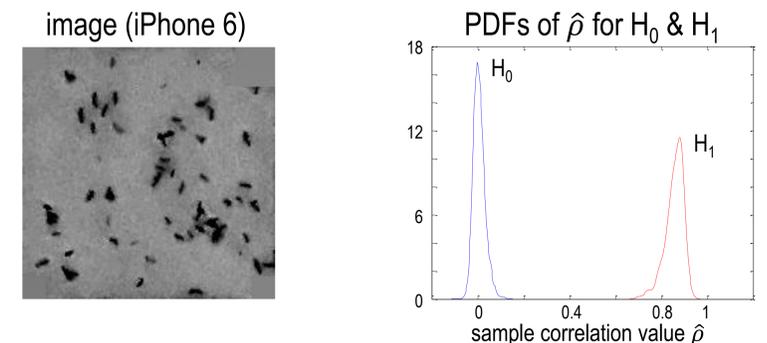
➢ **Simulated isotropic patch**

H_1
disc, r=10
r_{inner}=7 r_{inner}=5
r_{inner}=9
H_0
correlation
constant-value perturbation
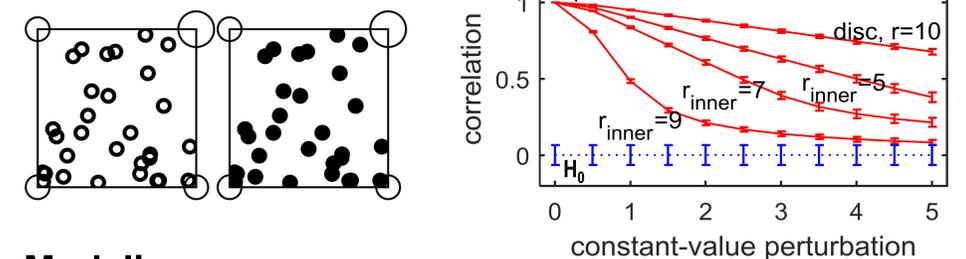
➢ **Modeling**

- Generative model, simplified assumptions
- Find PDFs $f_{\hat{\rho}|H_0}$ and $f_{\hat{\rho}|H_1}$ parameterized by Γ

➢ **On-going work:** better understand the performance impact of patch structures and parameters