TIFS paper presented at WIFS 2021

On Microstructure Estimation Using Flatbed Scanners for Paper Surface-Based Authentication

Runze Liu and Chau-Wai Wong

NC State University, North Carolina, USA

December 10th, 2021

Runze Liu and Chau-Wai Wong, "On Microstructure Estimation Using Flatbed Scanners for Paper Surface-Based Authentication." *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 3039–3053, Apr. 2021.

Outline

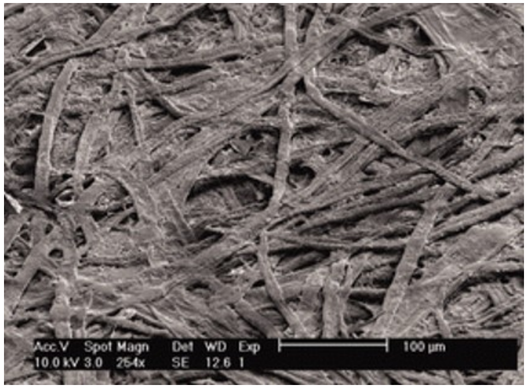
- Background of paper surface-based authentication
- Effect of specular reflection
- Authentication performance using scanners
- Practical questions in deployment:
  - How large should the paper patch size be?
  - How will misalignment affect the performance?

Background of Paper Surface-Based Authentication

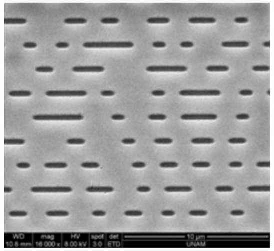
- Background of paper surface-based authentication
- Effect of specular reflection
- Authentication performance using scanners
- Practical questions in deployment:
  - How large should the paper patch size be?
  - How will misalignment affect the performance?

Objects Can Have Fingerprint

- Fingerprint of human beings[1]
  - Identify the person
  - An expression of gene
- Objects can also be considered to have "fingerprints"
  - Identifier for objects
  - Due to intrinsic and extrinsic variations



Paper surface scanned by SEM[2]



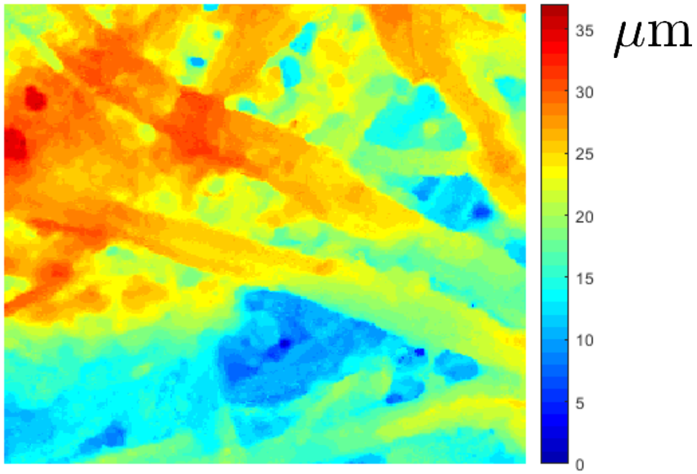
A microscopic view of pits and lands of a CD surface[3]

1 https://en.wikipedia.org/wiki/Fingerprint
2 R. Cowburn, "Laser surface authentication-natural randomness as a fingerprint for document and product authentication," *Proceedings of Optical Document Security*, 2008.
3 Hammouri Ghaith, Dana Aykutlu, and Sunar Berk, "CDs have fingerprints too." In *International Workshop on Cryptographic Hardware and Embedded Systems,* Berlin, Heidelberg, 2009.

Uniqueness of Paper Surface

- Paper surfaces:
  - Inter-twisted wood fibers, unique and physically unclonable
  - Unique randomness, may be regarded as “fingerprint”

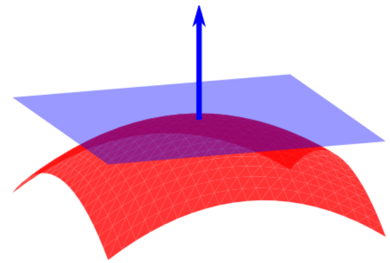
- Authentication applications:
  - Important documents, e.g., IDs, checks
  - label of wine bottles

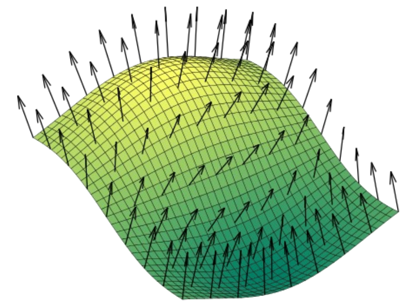


0.2mm by 0.2mm paper under confocal microscope

Norm Map

- Definition: surface normal

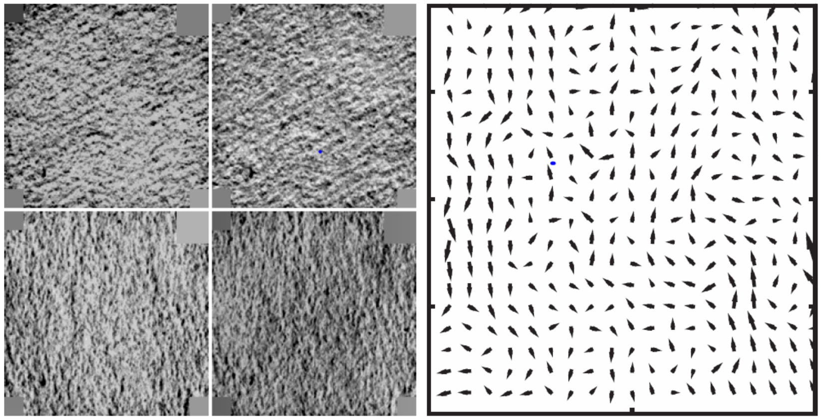




https://en.wikipedia.org/wiki/Normal_(geometry)

- Normal vector field: a collection of 3D normals over a 2D grid

- Norm map: 2D vector field on *x*-*y* plane



Scanned paper surfaces and a norm map [1]

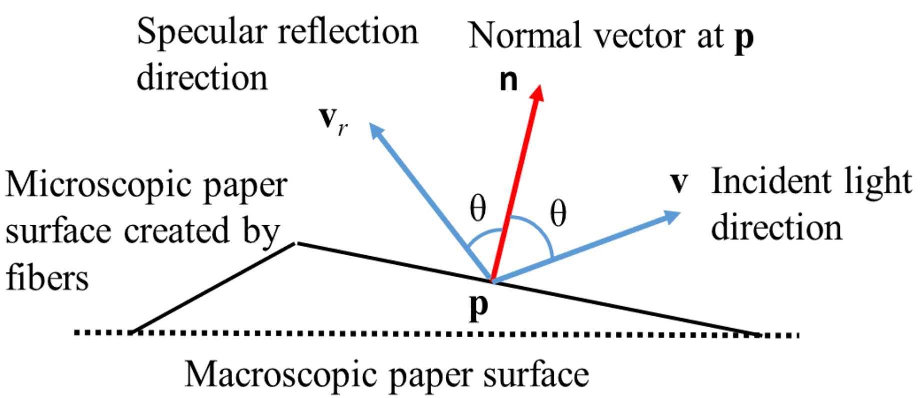
[1] Chau-Wai Wong and Min Wu, "Counterfeit detection based on unclonable feature of paper using mobile camera," *IEEE Transactions on Information Forensics and Security (T-IFS)*, vol.12, no.8, pp.1885–1899, Aug. 2017

Fully Diffuse Model

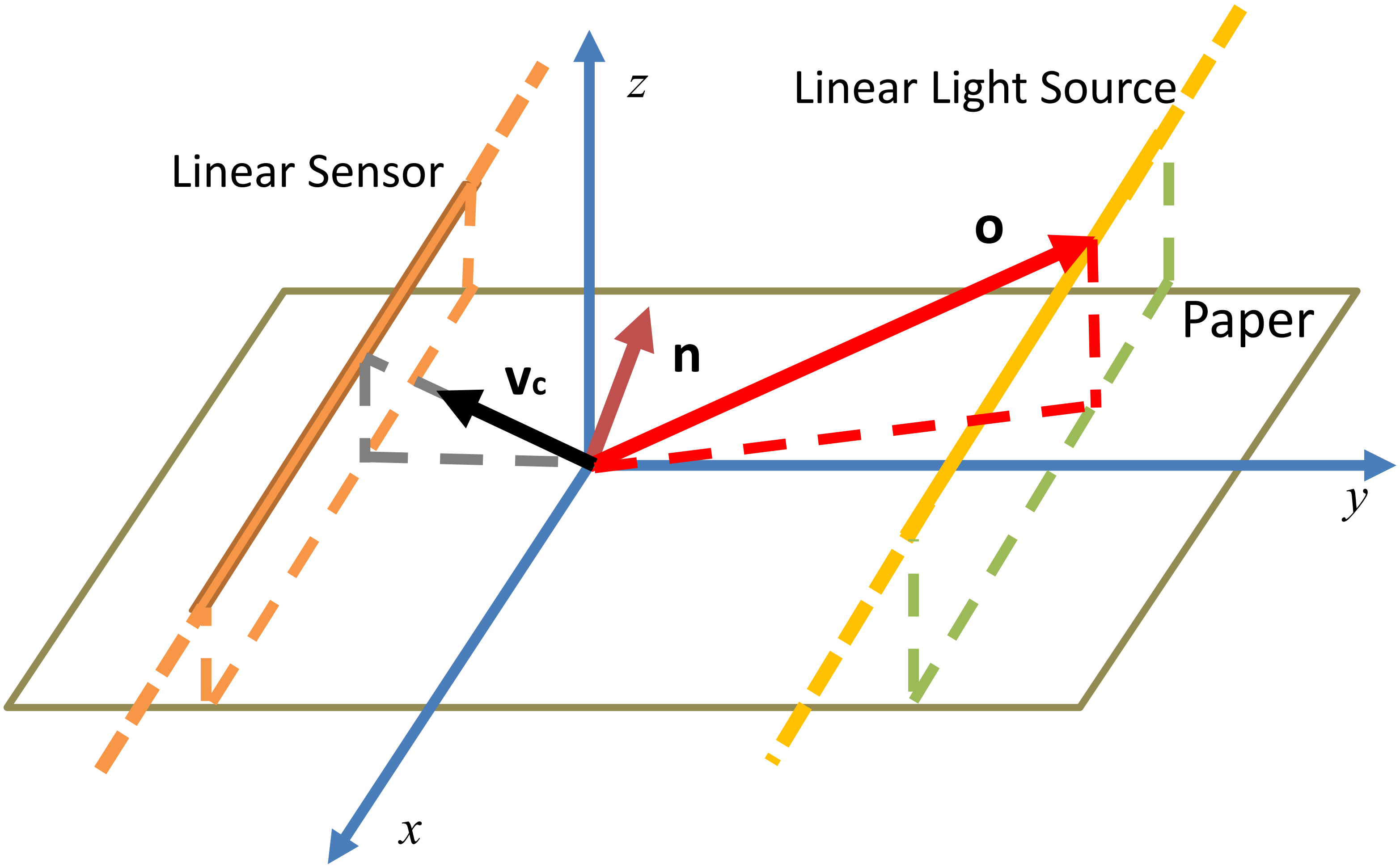
- Fully diffuse light reflection model, do not consider specular (mirror-like) reflection:

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

  - l: Strength of incident light,
  - λ: Capability of surface to reflect light.
- Perceived intensity does not depend on camera location.

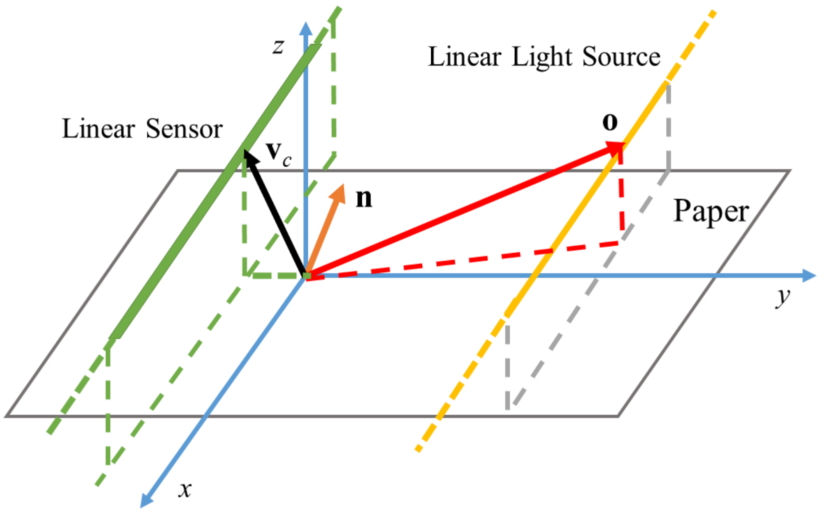


Optical System of a Flatbed Scanner



Use Flatbed Scanners to Derive Norm Map

- A configuration of the optical system of a flatbed scanner



- Intensity of light perceived under fully diffuse model:

$$I = \int_{-a}^{b} l_r \; do_x \approx l \cdot w_d \int_{-a}^{a} \mathbf{n}^T \frac{(o_x, o_y, o_z)^T}{||(o_x, o_y, o_z)||^3} \; do_x$$

- Rotate paper patch 90° and then scan:
  $I_{0^\circ}, I_{90^\circ}, I_{180^\circ}, I_{270^\circ}$.

Clarkson, W., Weyrich, T., Finkelstein, A., Heninger, N., Halderman, J.A. and Felten, E.W., 2009, May. Fingerprinting blank paper using commodity scanners. In *2009 30th IEEE Symposium on Security and Privacy* (pp. 301-314). IEEE.

Use Flatbed Scanners to Derive Norm Map

- Scan the paper in two opposite directions I_{0°, I_{180°;
- Take differences:

$$
\begin{aligned}
d_y &= I_{0^\circ} - I_{180^\circ} \\
&= \rho \int \left\langle \mathbf{n}, \frac{(x, o_y, o_z)^\top}{\|(x, o_y, o_z)^\top\|^3} - \frac{(x, -o_y, o_z)^\top}{\|(x, -o_y, o_z)^\top\|^3} \right\rangle \mathrm{d}x \\
&= \rho \int \left\langle \mathbf{n}, \frac{(0, 2o_y, 0)^\top}{\|(x, o_y, o_z)^\top\|^3} \right\rangle \mathrm{d}x \\
&= n_y \rho \int \frac{2o_y}{\|(x, o_y, o_z)^\top\|^3} \mathrm{d}x \\
&= n_y \rho s \, .
\end{aligned}
$$

- Obtain a scaled version of y-component of norm map.

Clarkson, W., Weyrich, T., Finkelstein, A., Heninger, N., Halderman, J.A. and Felten, E.W., 2009, May. Fingerprinting blank paper using commodity scanners. In *2009 30th IEEE Symposium on Security and Privacy* (pp. 301-314). IEEE.

Motivations

- Fully diffuse model does not consider the specular reflection;
- Does the estimated norm map resemble the real quantity with physical interpretations?
- Can feature engineering on the estimated norm maps yield higher authentication performance?
- Other practical concerns to be addressed, such as the effect of paper patch size and misalignment.

Outline

- Background of paper surface-based authentication
- Effect of specular reflection
- Authentication performance using scanners
- Practical questions in deployment:
  - How large should the paper patch size be?
  - How will misalignment affect the performance?

Effect of Specular Reflection

- Background of paper surface-based authentication
- Effect of specular reflection
- Authentication performance using scanners
- Practical questions in deployment:
  - How large should the paper patch size be?
  - How will misalignment affect the performance?

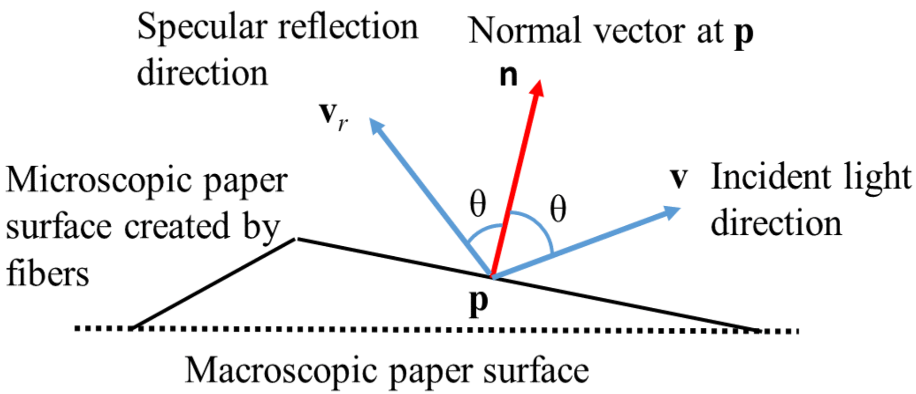
Generalized Light Reflection Model

- Will specular reflection affect the norm map estimation?
- Generalized light reflection model:

$$l_r = \frac{l}{\|\mathbf{o}-\mathbf{p}\|^2}\left\{w_d \cdot \left(\mathbf{n}^T\mathbf{v}\right)^+ + \boxed{w_s \cdot \left(\mathbf{v}_c^T\mathbf{v}_r\right)^{k_e}}\right\}$$

$\mathbf{o}$ is the the light source position, $\mathbf{v}_c$ is camera direction, $k_e > 0$ controls the gloss level of the surface.

- Ignoring specular reflection may lead to inaccurate estimation of norm map.



Specular Reflection in Scanners

- Intensity of light perceived under fully diffuse model:

$$I = \int_{-a}^{b} l_r \, do_x \approx l \cdot w_d \int_{-a}^{a} \mathbf{n}^T \frac{(o_x, o_y, o_z)^T}{||(o_x, o_y, o_z)||^3} \, do_x$$

- Intensity of light perceived under generalized model:

$$\begin{aligned} I &= \int_{-a}^{a} l_r do_x = l \int_{-a}^{a} \left(w_d \mathbf{n}^T \mathbf{v} + \boxed{w_s \mathbf{v}_c^T \mathbf{v}_r} \right) \frac{1}{||\mathbf{o}||^2} do_x \\ &= l \int_{-a}^{a} \left(w_d \mathbf{n}^T \mathbf{v} + \boxed{w_s \mathbf{v}_c^T (2\mathbf{n}\mathbf{n}^T - \mathbf{I})\mathbf{v}} \right) \frac{1}{||\mathbf{o}||^2} do_x . \end{aligned}$$

- Take differences: $I_{0^\circ} - I_{180^\circ} \approx n_y \left[s + 2(2o_y + v_{cy})s' \right]$
- **Specular** reflection **does not play a role** in norm map estimation with flatbed **scanner**. Specular reflection cancels out in the optical system of a flatbed scanner.

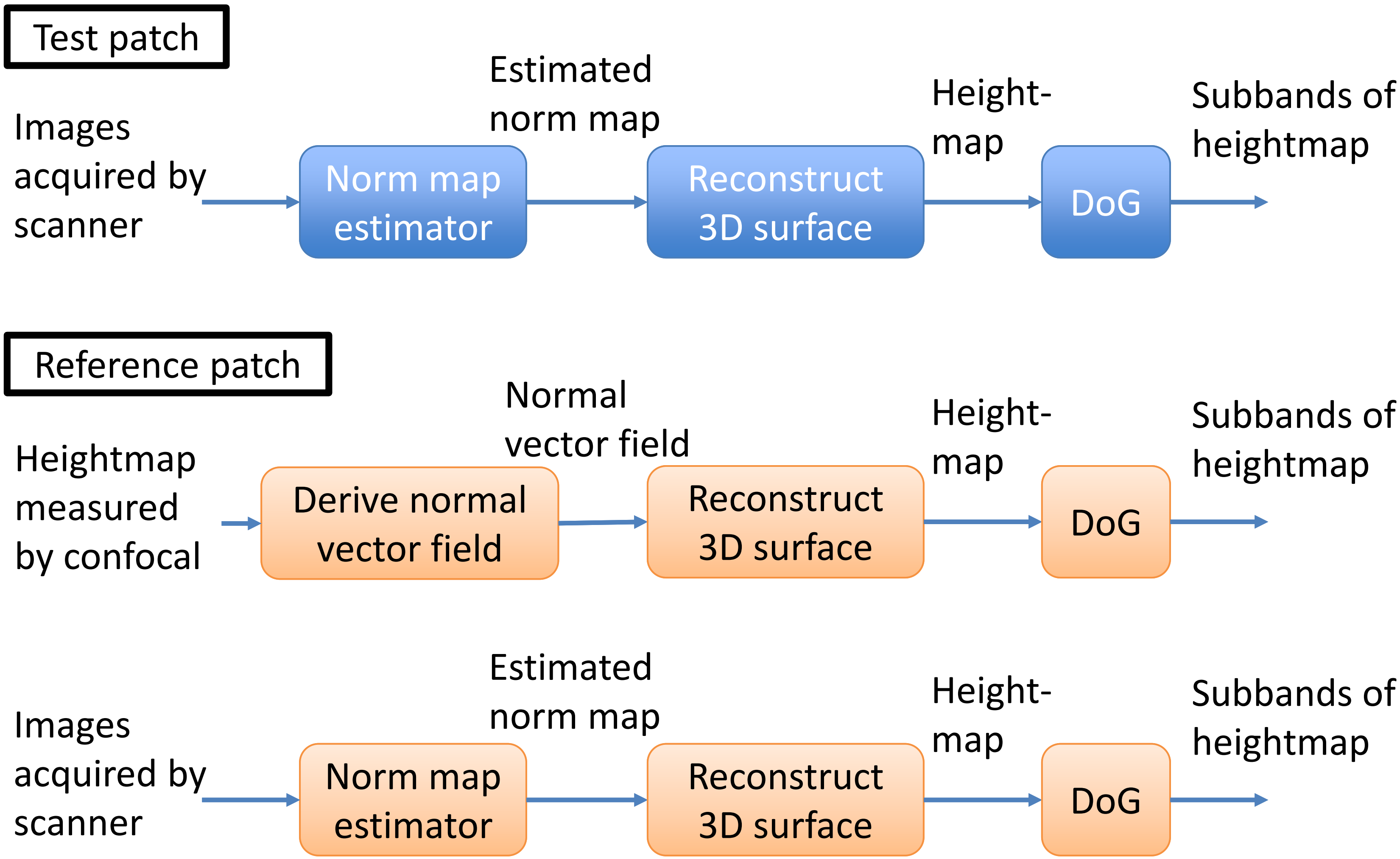
Outline

- Background of paper surface-based authentication
- Effect of specular reflection
- Authentication performance using scanners
- Practical questions in deployment:
  - How large should the paper patch size be?
  - How will misalignment affect the performance?

Authentication Performance Using Scanners

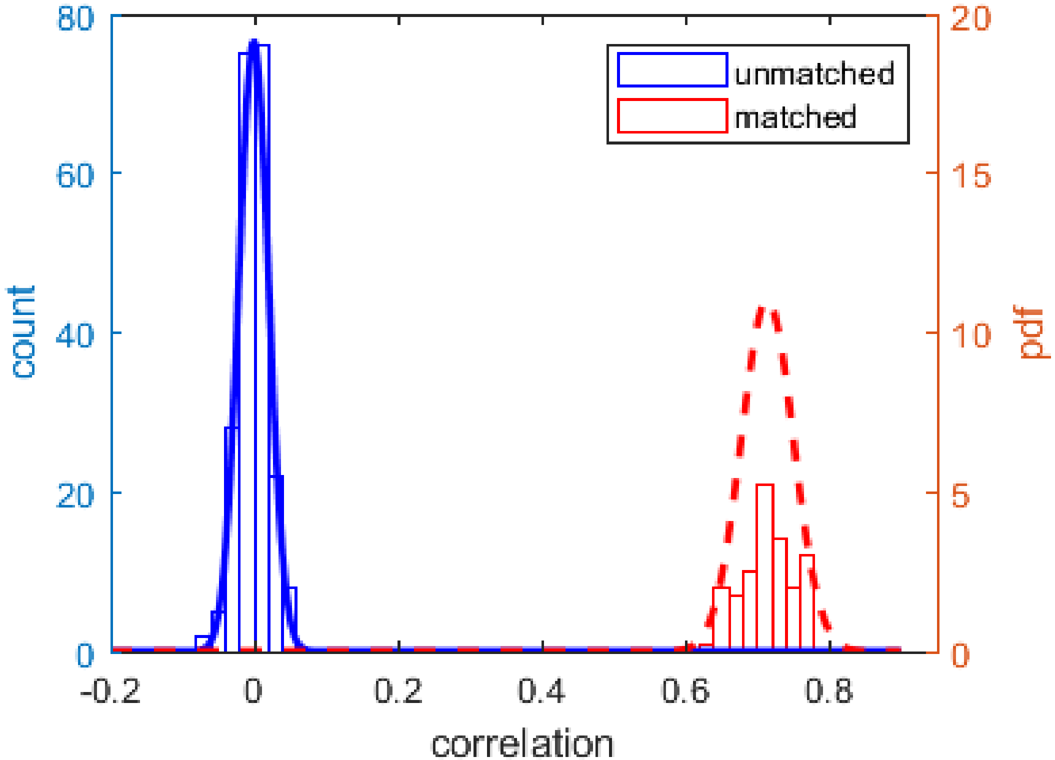
- Background of paper surface-based authentication
- Effect of specular reflection
- Authentication performance using scanners
- Practical questions in deployment:
  - How large should the paper patch size be?
  - How will misalignment affect the performance?

Authentication Pipeline



Authentication Results

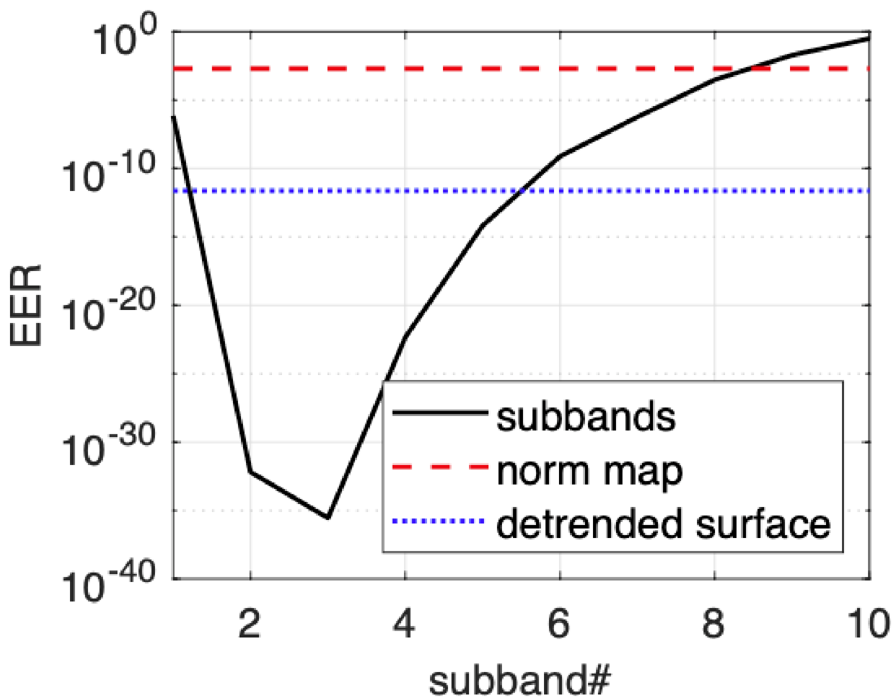
- Unmatched: test and reference patches are different; Matched: test patch is the same as the reference patch.
- Assume correlations to be Gaussian (or Laplacian) distributed to extrapolate the tails of the correlations.



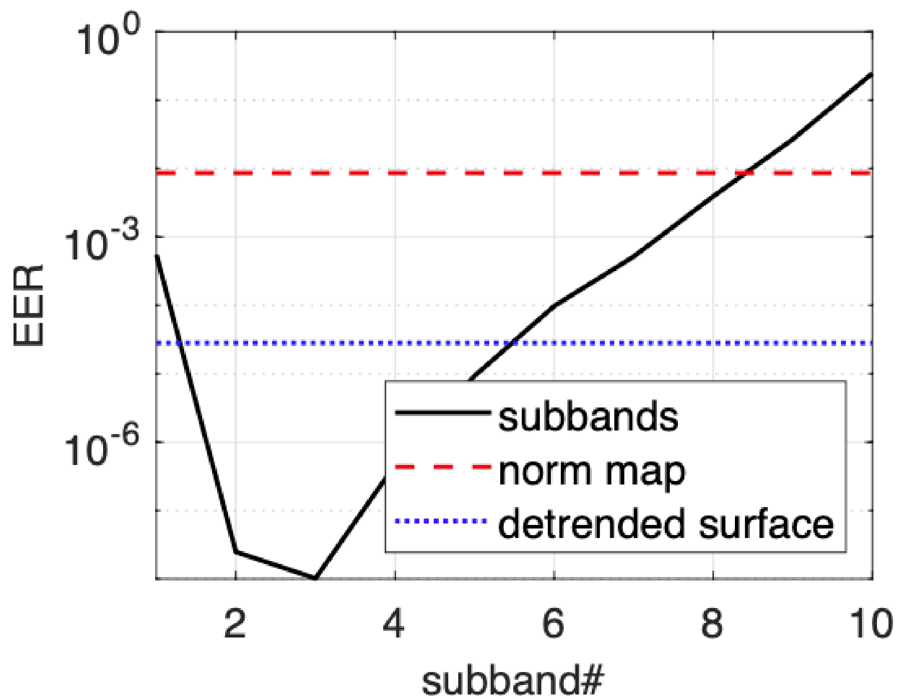
Authentication Results

- Reference is from **confocal microscope** (ground truth);
- The scanners can capture meaningful physical features.

Correlations assumed to be Gaussian



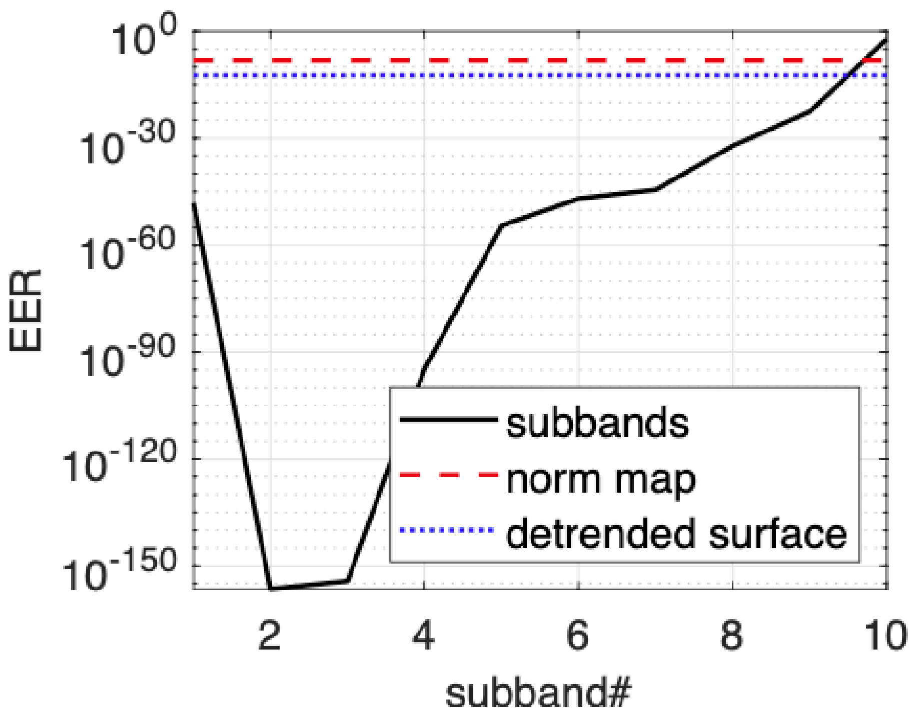
Correlations assumed to be Laplacian



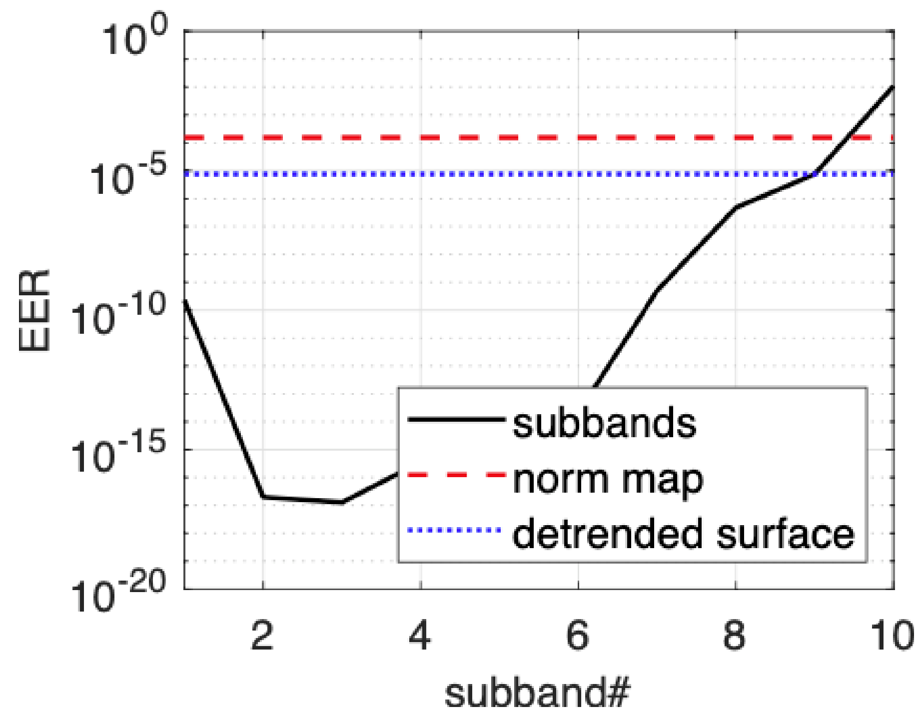
Authentication Results

- Reference is **scanner** (practical; confocal is expensive)
- Spatial-frequency Subbands #2 and #3 are more discriminative features.

Correlations assumed to be Gaussian



Correlations assumed to be Laplacian



Outline

- Background of paper surface-based authentication
- Effect of specular reflection
- Authentication performance using scanners
- Practical questions in deployment:
  - How large should the paper patch size be?
  - How will misalignment affect the performance?

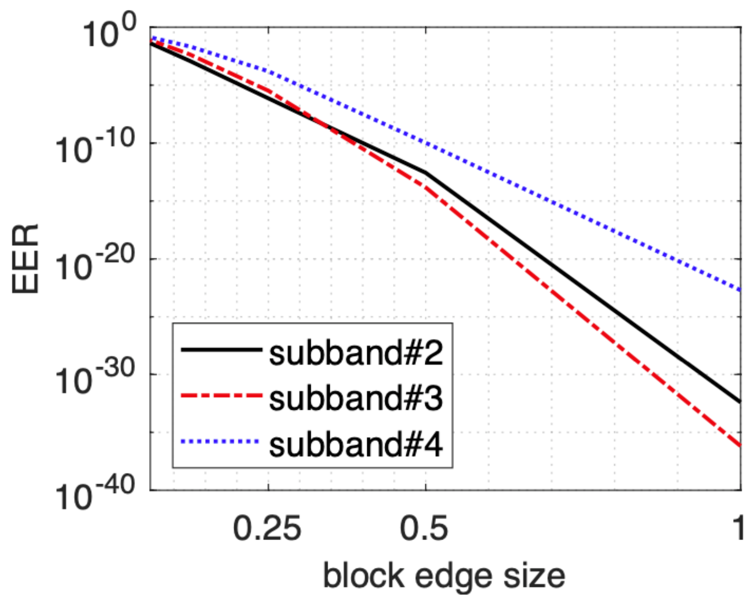
Practical Questions in Deployment

- Background of paper surface-based authentication
- Effect of specular reflection
- Authentication performance using scanners
- Practical questions in deployment:
  - How large should the paper patch size be?
  - How will misalignment affect the performance?

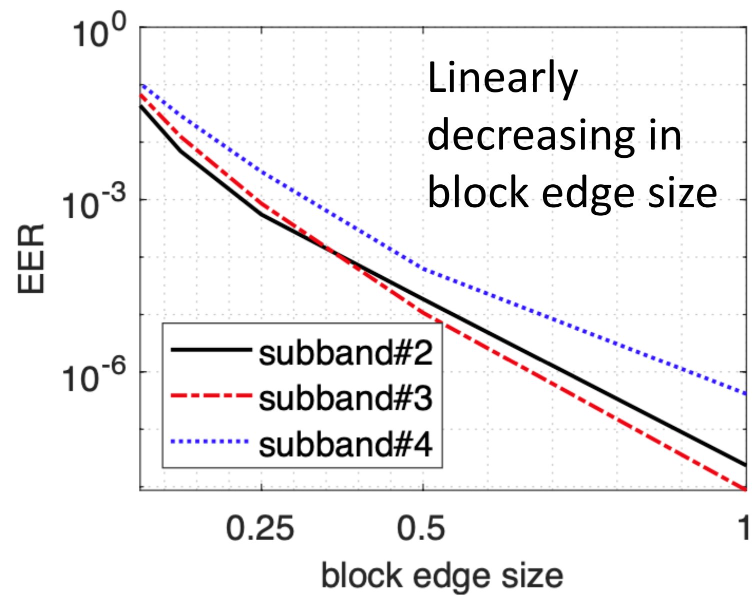
Paper Patch Size

- How large should the paper patch size be?
- After a cut, a paper patch is divided into **four** blocks of the same size, block edge size decreasing to half;

Correlations assumed to be Gaussian



Correlations assumed to be Laplacian



- Larger patches are desired for authentication.

Paper Patch Size

- Under Laplacian assumption: $\mathrm{EER} = \frac{1}{2}\exp\left[\frac{\sqrt{2}}{\sigma_0+\sigma_1}(\mu_0-\mu_1)\right]$ μ_i, σ_i are mean and standard deviation for i^{th} hypothesis;
- After n cuts:

$$\mathrm{EER}(n) = \frac{1}{2}\exp\left[\frac{\sqrt{2}}{2^n\sigma_0 + 1.5^n\sigma_1}(\mu_0-\mu_1)\right]$$
$$\approx \frac{1}{2}\exp\left[\sqrt{2}\cdot 2^{-n}(\mu_0-\mu_1)/\sigma_0\right],$$

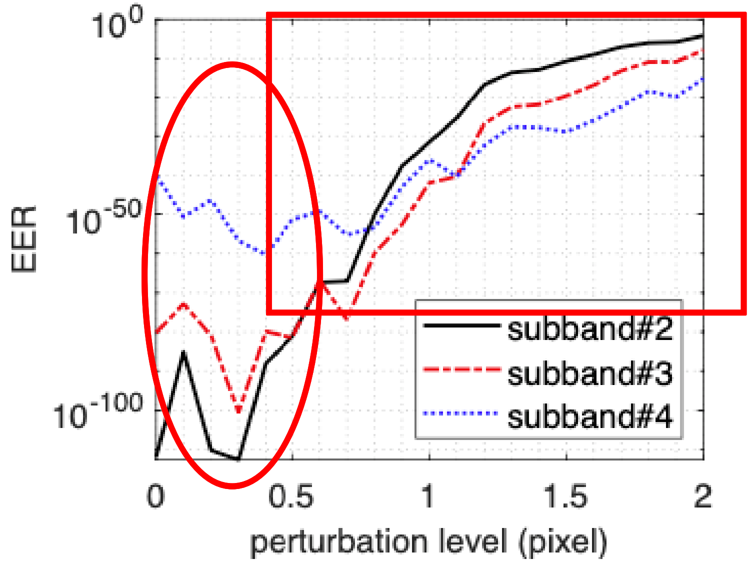
Standard deviations will increase by 2 times. For positively correlated sub-patches, the std increases less than 2.

- 2^{-n} is the block edge size after n cuts; $\log(\mathrm{EER}(n))$ is linearly decreasing in block edge size.

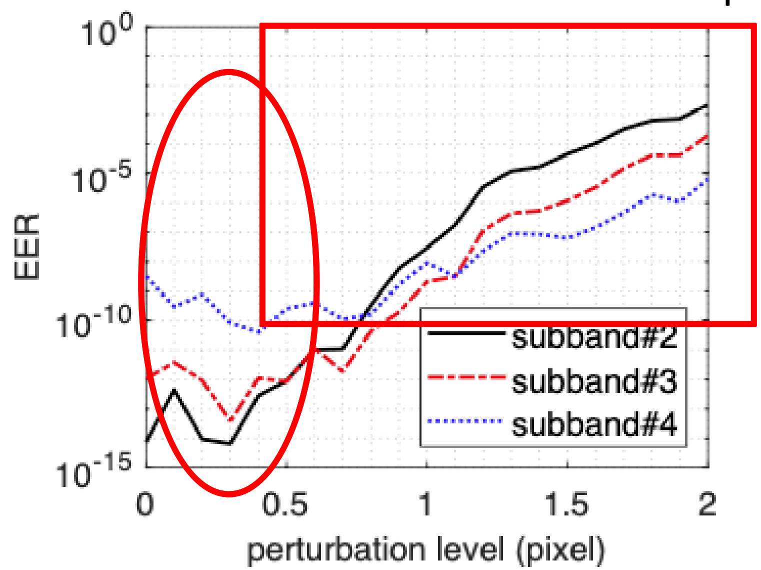
Effect of Registration Errors

- How will misalignment affect the performance?
- Perturb the estimated location (x, y) of paper patches; $x' = x + e_1, y' = y + e_2,$ where $e_1, e_2 \sim N(0, L^2)$;
- Large EER when $L > 0.4$ pixels;
- Precise alignment is important.

Correlations assumed to be Gaussian



Correlations assumed to be Laplacian



Conclusions and Future Work

- Specular reflection does not play a role in norm map estimation in the optical setup of **scanner**;
- High spatial-frequency subbands of the heightmap are more powerful than the norm map;
- Studied the effects of paper patch size and misalignment for practical application scenarios.
- *Future work*:

  Investigate key research questions using mobile cameras to acquire the microstructure, such as the how to build resilience to specular reflection.

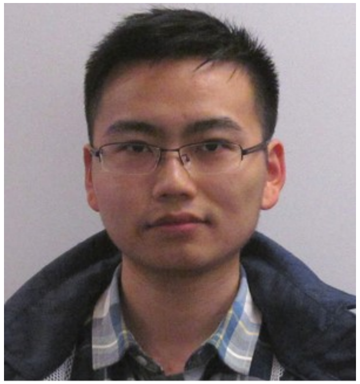
Dataset

- The dataset is available by request;
- Will appear on IEEE Dataport[1] in a month;
- We invite you to join the competition contest to improve the estimation accuracy and authentication performance.

1 https://ieee-dataport.org/

TIFS paper presented at WIFS 2021

On Microstructure Estimation Using Flatbed Scanners for Paper Surface-Based Authentication



Runze Liu and Chau-Wai Wong

NC State University, North Carolina, USA

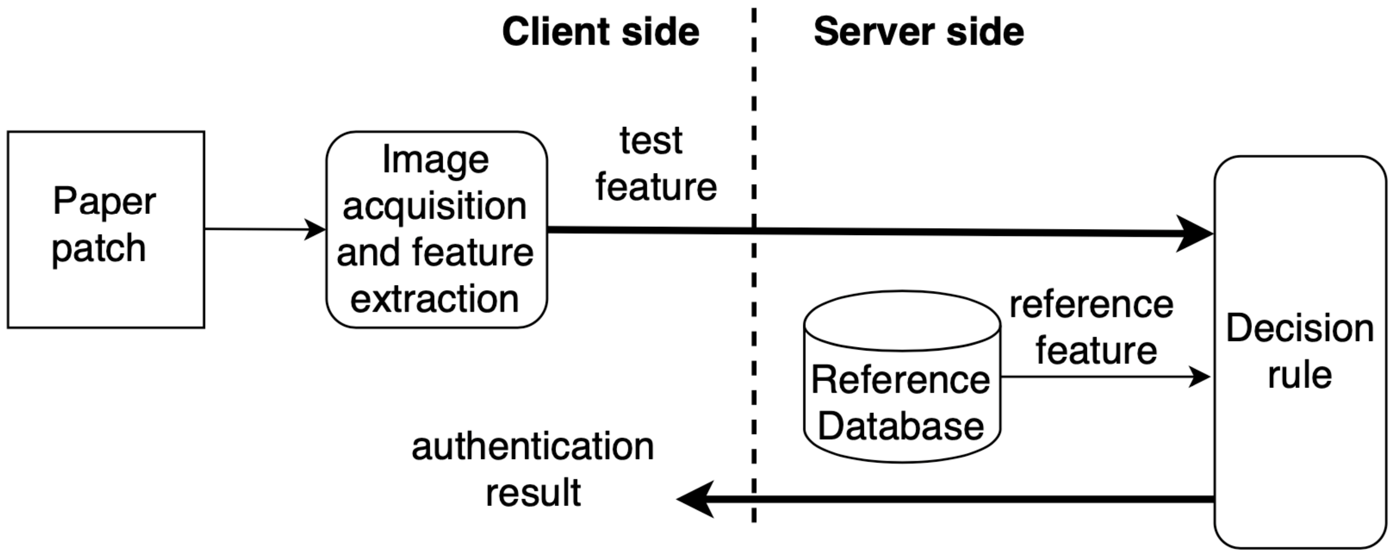
December 10th, 2021

Runze Liu and Chau-Wai Wong, "On Microstructure Estimation Using Flatbed Scanners for Paper Surface-Based Authentication." *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 3039–3053, Apr. 2021.

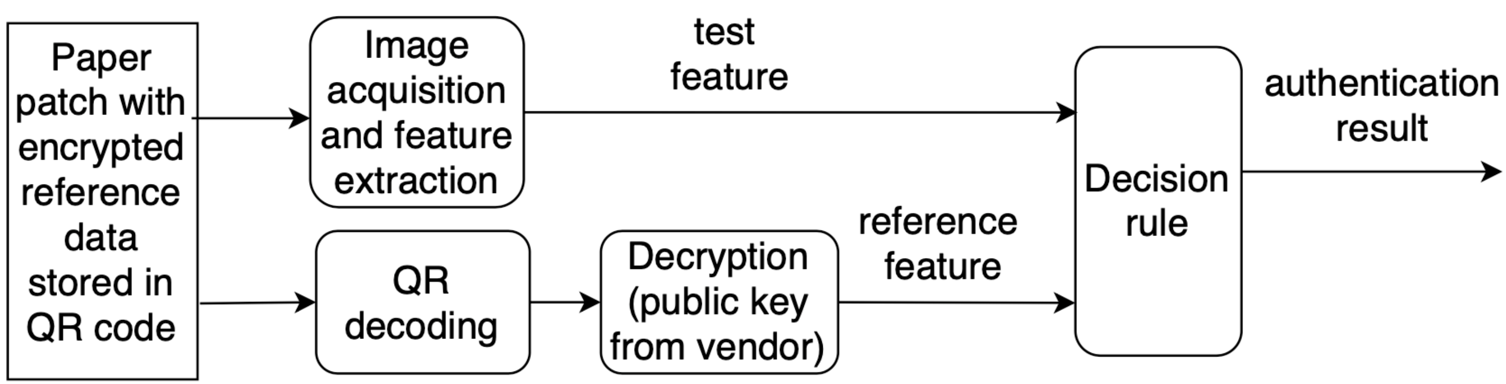
Back up slides

Paper Surface-based Authentication Systems

A client-server model

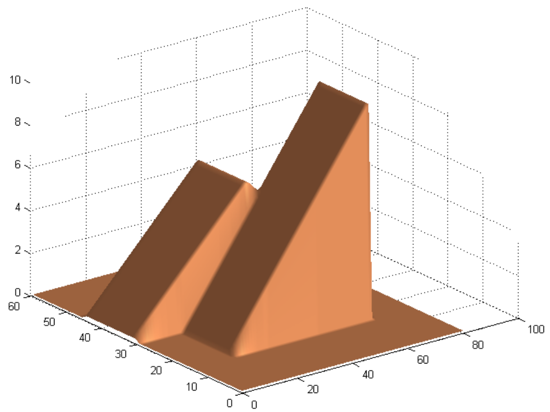


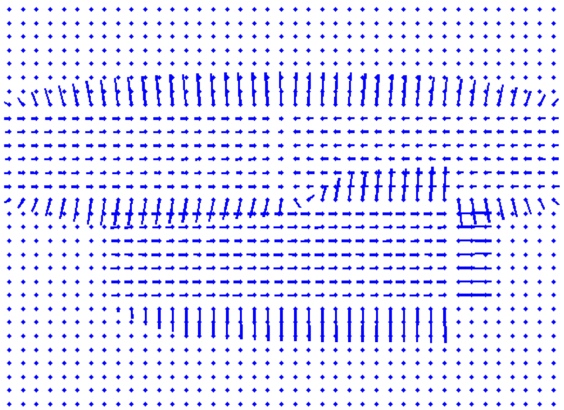
A local model

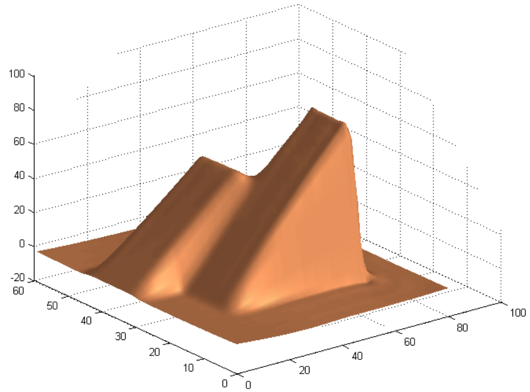


Surface Reconstruction from Normal Vector Field

- Norm map [1]: difficult to visualize; limited discriminative power
- 3D surface:
  - more appealing to human eyes
  - use off-the-shelf image/surface analysis tools
- Ex: Reconstruction of surface from normal vector field



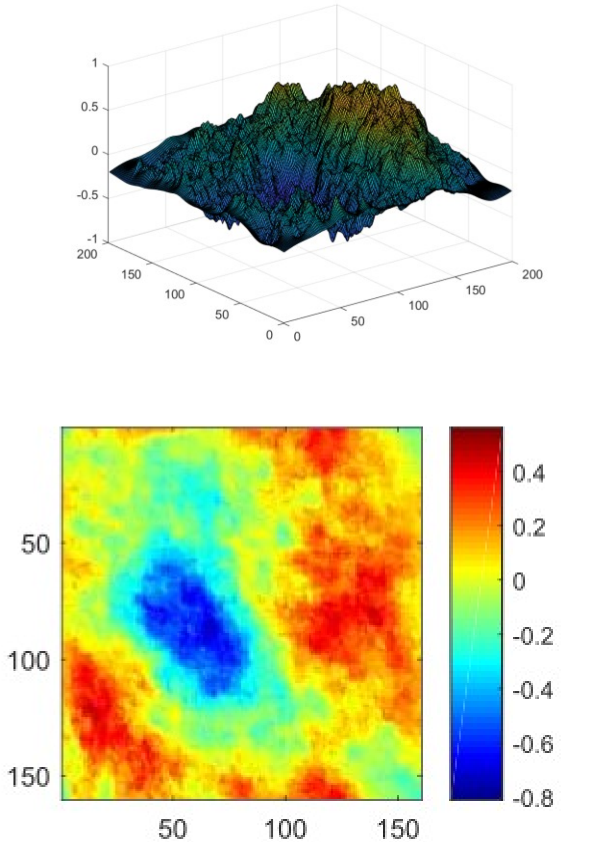




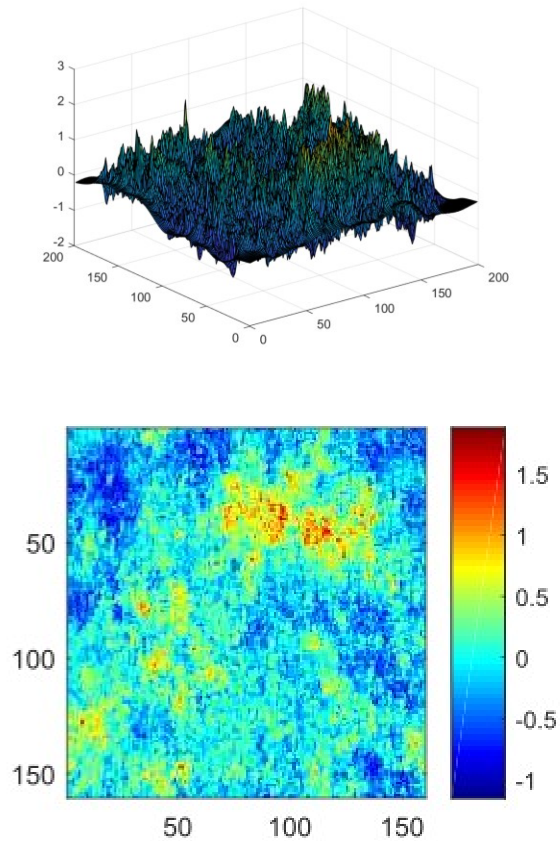
Kovesi, Peter. "Shapelets correlated with surface normals produce surfaces." *IEEE International Conference on Computer Vision*. 2005.

Surfaces From Cameras vs. Confocal Microscope

- Spatial trend in reconstructed surface not similar, but changes in normal direction spatially should be similar.



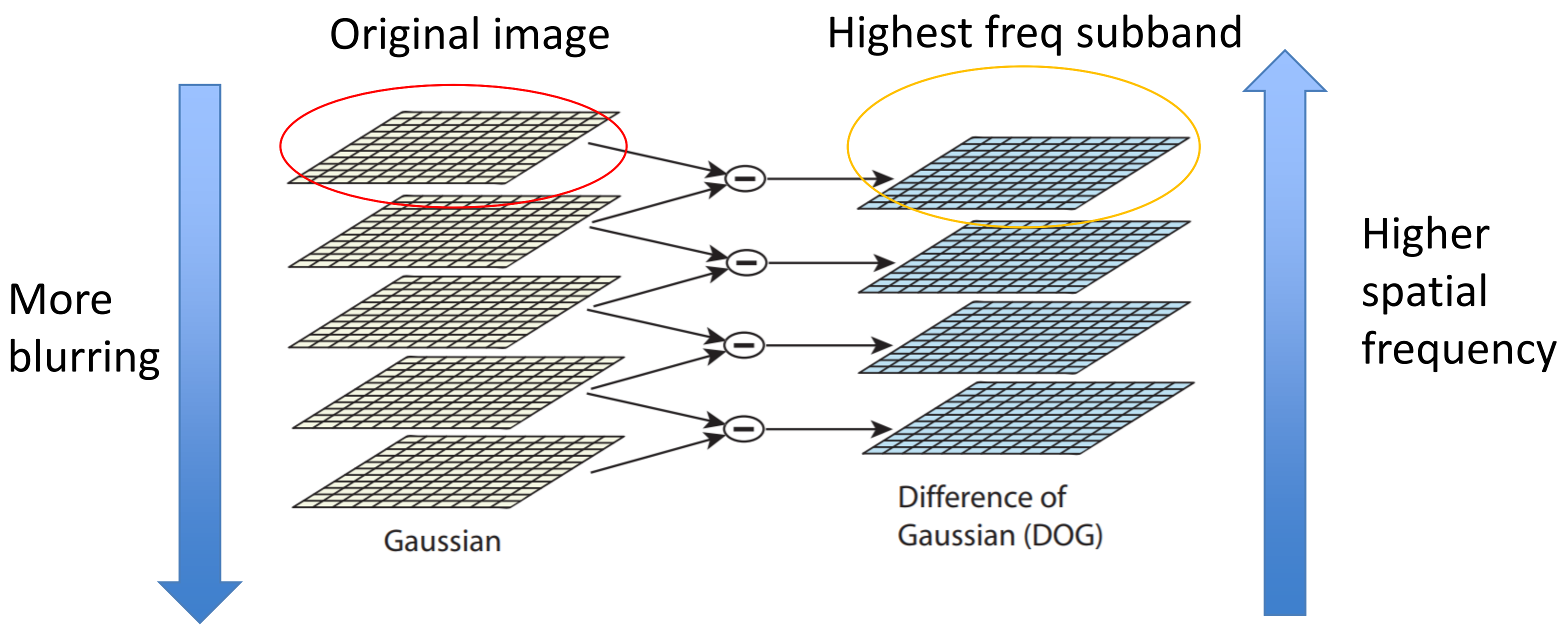
Reconstructed surface from Model 1



Reconstructed surface from confocal

Difference of Gaussian (DoG) Representation

- A DoG representation: take the differences of Gaussian-blurred images. Laplacian pyramids without subsampling.
- Allows separate analysis of the discrimination performance at different spatial frequency subbands.

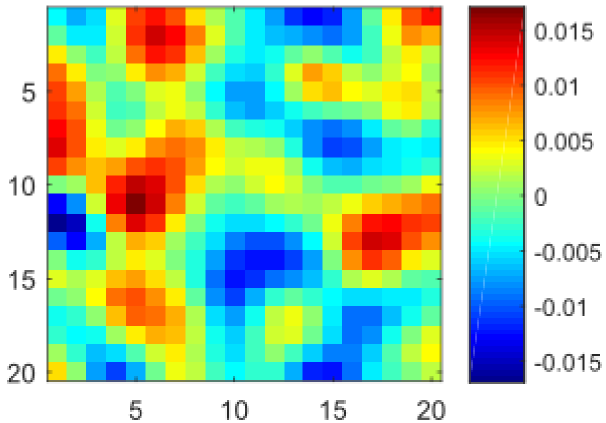


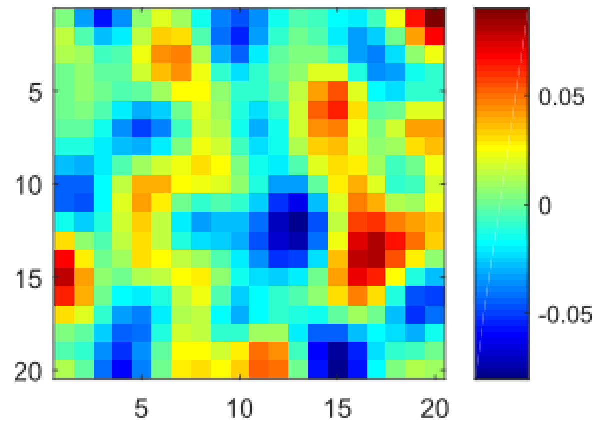
D. G. Lowe. Distinctive image features from scaleinvariant keypoints. International journal of computer vision, 60(2):91–110, 2004

Reconstructed Surfaces at High Spatial Frequency

2nd high frequency subband of:

surface reconstructed from Model 1





surface reconstructed from confocal microscope

Four representative slices from subband image

Normalized height

Normalized height