Enabling Paper-Based Surface Authentication via Digital Twin Modeling and Experimental Verification

Prasun Datta,[1] Chau-Wai Wong,[1] Min Wu[2]

[1]NC State University [2]University of Maryland, College Park

August 8, 2024

IEEE MIPR 2024

Outline

- **Introduction and Motivation**
- Proposed Digital Twin
- Digital-Twin Guidance
- Proposed Real-World Authentication Method
- Conclusion and Future Work

Introduction and Motivation

- ❖ Fingerprints are unique and permanent.
- ❖ Used for unique identification, e.g.,
  - suspects in investigations,
  - Apple pay.

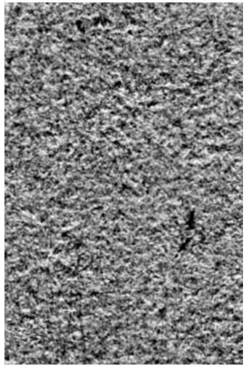
Fingerprint [1]

1. https://en.wikipedia.org/wiki/Fingerprint

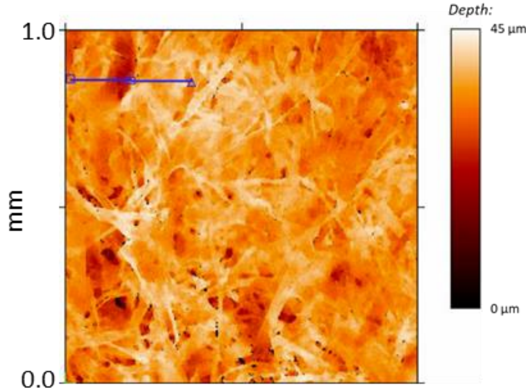
Introduction and Motivation

- ❖ Fingerprints are unique and permanent.
- ❖ Used for unique identification, e.g.,
  - suspects in investigations,
  - Apple pay.
- ❖ Objects/paper surfaces possess unique intermingled microscopic structure.
- ❖ May authenticate using microstructures.

Fingerprint [1]



Paper surface image, acquired using flatbed scanner [2]



Paper surface 3-D structure, acquired using confocal microscope [3, 4]

1. https://en.wikipedia.org/wiki/Fingerprint
2. W. Clarkson, T. Weyrich, A. Finkelstein, N. Heninger, J. A. Halderman, and E. W. Felten, “Fingerprinting blank paper using commodity scanners,” IEEE Symposium on Security and Privacy, 2009.
3. C.-W. Wong and M. Wu, “Counterfeit detection based on unclonable feature of paper using mobile camera,” IEEE Transactions on Information Forensics and Security, 2017.
4. High Resolution Surface Topography FRT MicroProf Chromatic Aberration Sensor, Innventia AB, 2012.

Can Paper Surface be Used as “Fingerprint”?

Clarkson et al. (2009) first introduced a method to authenticate **blank white paper**.

1. W. Clarkson, T. Weyrich, A. Finkelstein, N. Heninger, J. A. Halderman, and E. W. Felten, “Fingerprinting blank paper using commodity scanners,” IEEE Symposium on Security and Privacy, 2009.

Can Paper Surface be Used as "Fingerprint"?

Clarkson et al. (2009) first introduced a method to authenticate **blank white paper**.

- Utilized flatbed scanners to scan paper surface.
- Used surface normals (from photometric stereo) as "fingerprint".

Flatbed scanner [2]

1. W. Clarkson, T. Weyrich, A. Finkelstein, N. Heninger, J. A. Halderman, and E. W. Felten, "Fingerprinting blank paper using commodity scanners," IEEE Symposium on Security and Privacy, 2009.
2. https://www.amazon.com/Canon-CanoScan-Lide-Slim-Scanner/dp/B07G5YBS1W

Can Paper Surface be Used as "Fingerprint"?

Clarkson et al. (2009) first introduced a method to authenticate **blank white paper**.

- Utilized flatbed scanners to scan paper surface.
- Used surface normals (from photometric stereo) as "fingerprint".
- Limitations: lack of portability and need for specialized operating knowledge.

Flatbed scanner [2]

1. W. Clarkson, T. Weyrich, A. Finkelstein, N. Heninger, J. A. Halderman, and E. W. Felten, "Fingerprinting blank paper using commodity scanners," IEEE Symposium on Security and Privacy, 2009.
2. https://www.amazon.com/Canon-CanoScan-Lide-Slim-Scanner/dp/B07G5YBS1W

Can It be More Accessible?

Wong and Wu (2015) authenticate paper surfaces using **cellphone**-captured photos.

- Used **camera flash** to obtain surface normals.

Capturing a photo of a paper with camera flash [1]

1. C.-W. Wong and M. Wu, "Counterfeit detection using paper PUF and mobile cameras," IEEE International Workshop on Information Forensics and Security, 2015.

Can It be More Accessible?

Wong and Wu (2015) authenticate paper surfaces using **cellphone**-captured photos.

- Used **camera flash** to obtain surface normals.
- Pros: easy to use, e.g., in business, govt. agencies.

Capturing a photo of a paper with camera flash [1]

1. C.-W. Wong and M. Wu, “Counterfeit detection using paper PUF and mobile cameras,” IEEE International Workshop on Information Forensics and Security, 2015.

Can It be More Accessible?

Wong and Wu (2015) authenticate paper surfaces using **cellphone**-captured photos.

- Used **camera flash** to obtain surface normals.
- Pros: easy to use, e.g., in business, govt. agencies.
- Cons: prolonged exposure to flash causes eye injuries.

Capturing a photo of a paper with camera flash [1]

1. C.-W. Wong and M. Wu, “Counterfeit detection using paper PUF and mobile cameras,” IEEE International Workshop on Information Forensics and Security, 2015.

Can It be Safer?

- We propose to authenticate paper surfaces using merely **indoor lights** without relying on camera flash.

Structured Indoor Lighting [1]

1. https://www.familyhandyman.com/project/how-to-install-low-profile-led-lights/

Can It be Safer?

- We propose to authenticate paper surfaces using merely **indoor lights** without relying on camera flash.
- **Challenges:**
  - Lowered strength of arriving light at the patch ➔ reduced signal-to-noise ratio.
  - Complicated appearance of paper due to shadows & secondary reflections.

Structured Indoor Lighting [1]

1. https://www.familyhandyman.com/project/how-to-install-low-profile-led-lights/

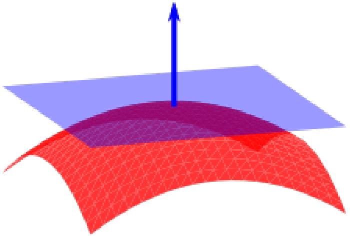
Contributions of Proposed Work

- Built **digital twin to guide** the design of authentication method in the physical world.

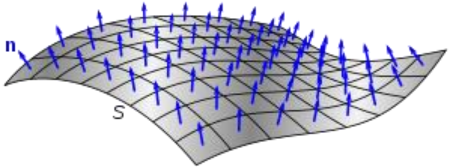
- Verified our authentication method’s effectiveness on both simulated and real-world paper patches.

- Utilized **“negative” light source** trick to increase effective light strength.

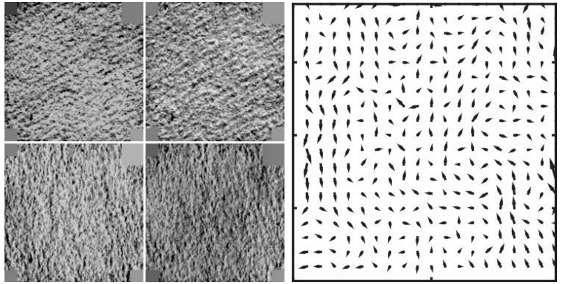
Preliminaries: Definitions



Surface Normal [1]



Normal vector field [1]



Scanned paper surface and norm map [2]

Surface Normal: vector perpendicular to tangent plane.

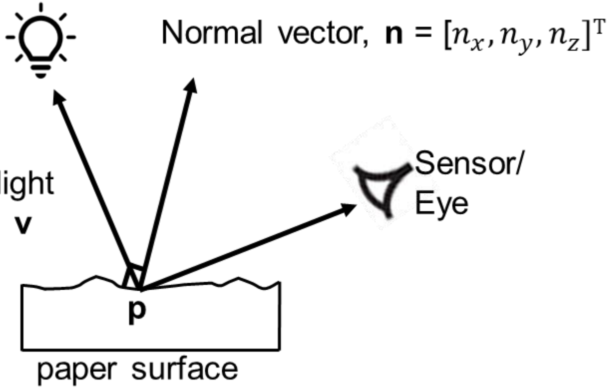
Normal vector field: collection of 3-D surface normals over 2-D grid.

Norm map: normal vector field projected onto x-y plane.

Can be unique discriminative feature.

1. https://en.wikipedia.org/wiki/Normal_%28geometry%29
2. C.-W. Wong and M. Wu, "Counterfeit detection based on unclonable feature of paper using mobile camera," IEEE Transactions on Information Forensics and Security, 2017.

Preliminaries: Fully Diffuse Reflection Model



Treating paper as fully diffuse surface.

$$l_{\mathrm{r}} = \lambda \cdot l_0 \cdot \mathbf{n}^{\top}\mathbf{v} / \|\mathbf{v}\|_2^3$$

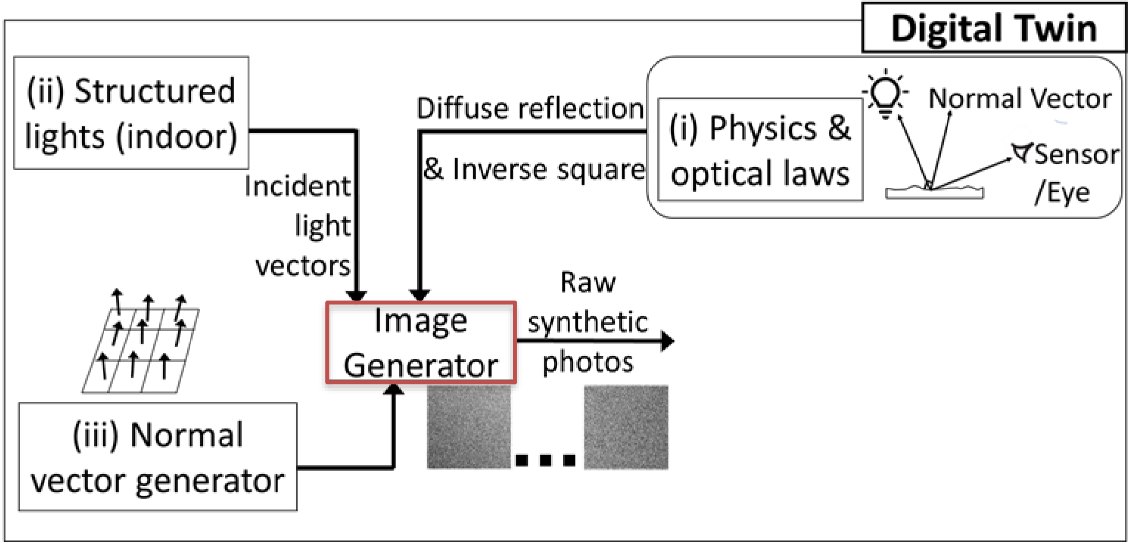
- λ — albedo, ability of a surface to reflect light.
- l_0— light source intensity.

Outline

- ❖ Introduction and Motivation
- ❖ **Proposed Digital Twin**
- ❖ Digital-Twin Guidance
- ❖ Proposed Real-World Authentication Method
- ❖ Conclusion and Future Work

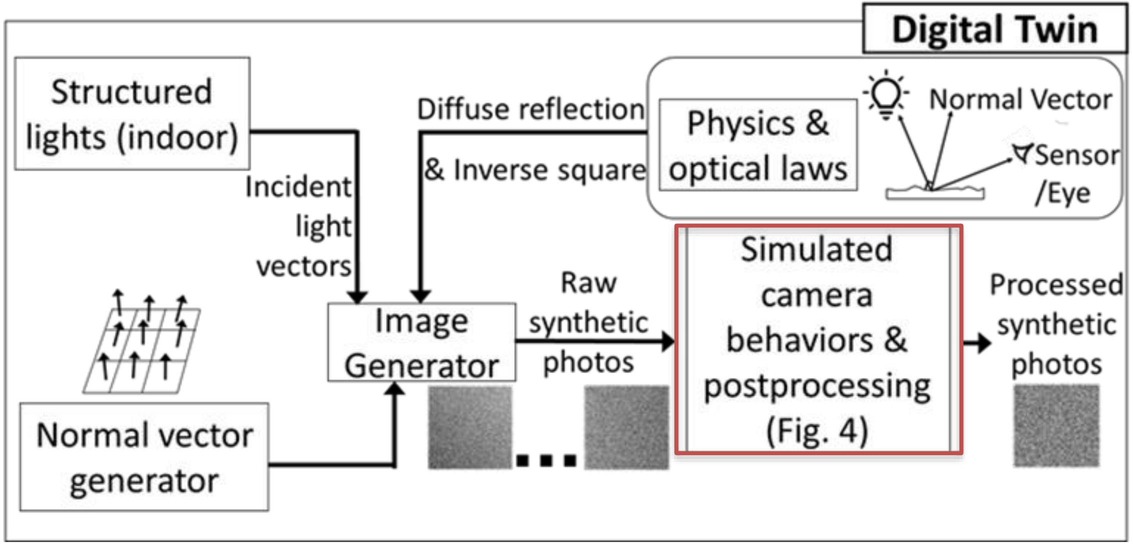
Proposed Digital Twin (DT)

❖ Image Generator



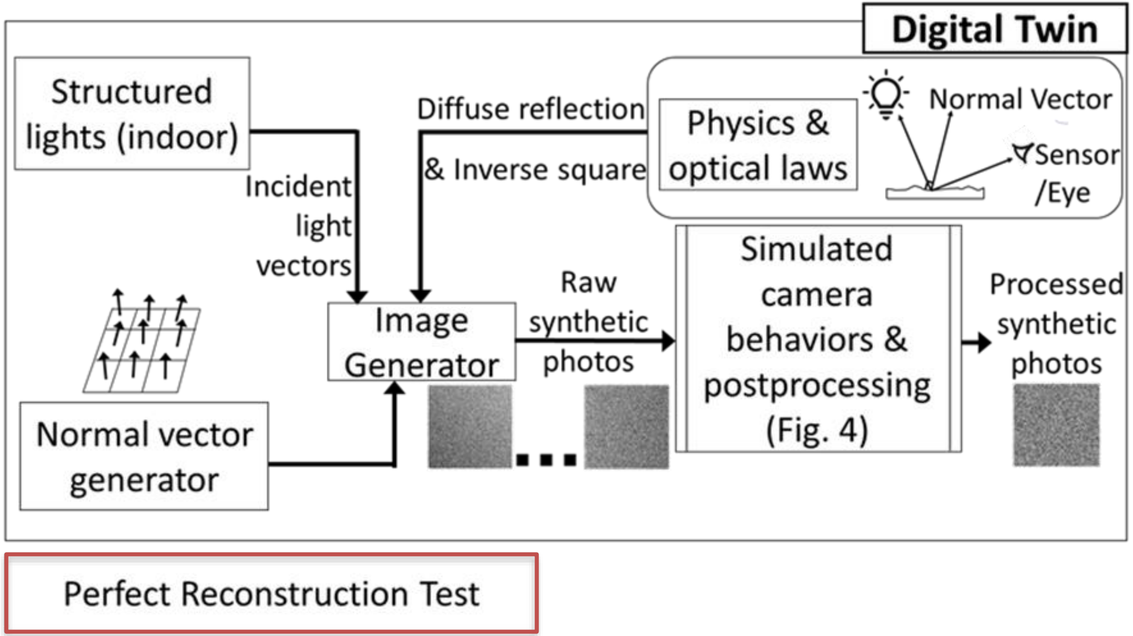
Proposed Digital Twin (DT)

- ❖ Image Generator
- ❖ Postprocessing



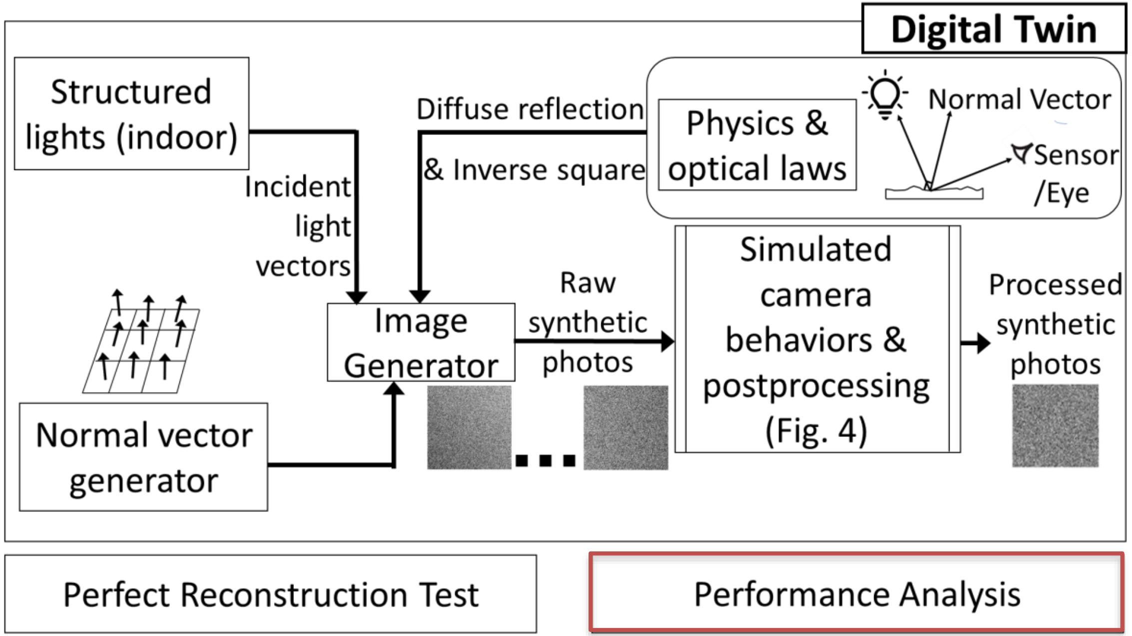
Proposed Digital Twin (DT)

- ❖ Image Generator
- ❖ Postprocessing
- ❖ Perfect Reconstruction Test



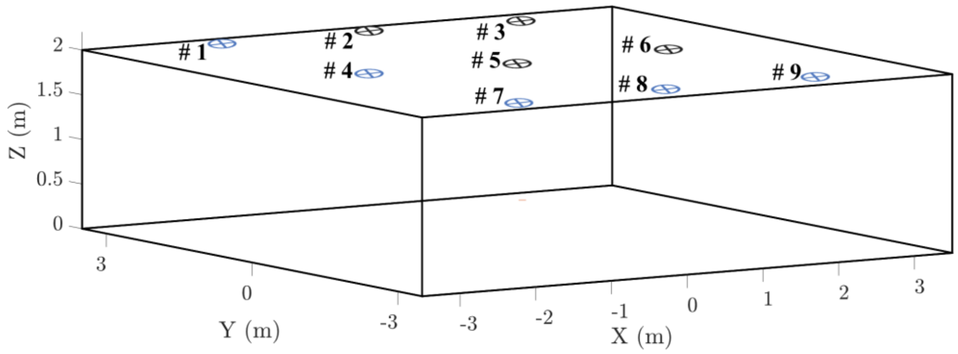
Proposed Digital Twin (DT)

- ❖ Image Generator
- ❖ Postprocessing
- ❖ Perfect Reconstruction Test
- ❖ Performance Analysis



Proposed DT: Lighting in Simulated Room

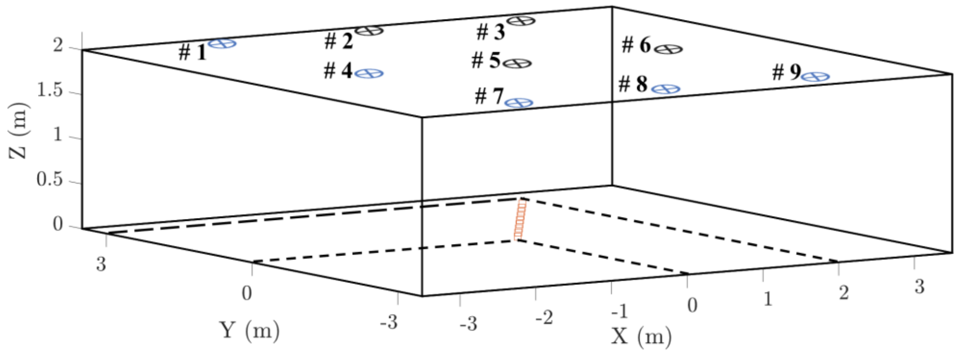
- "⨂": matrix of nine equally spaced point light sources.
- Lights #2, #3, #5, and #6 used for DT's validation and testing.
- Remaining lights used for studying impact of increased light sources.



3-D view of the capturing setup in DT

Proposed DT: Lighting in Simulated Room

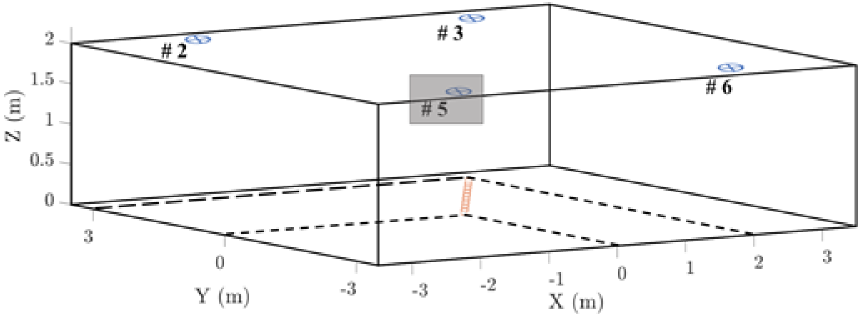
- "⊗": matrix of nine equally spaced point light sources.
- Lights #2, #3, #5, and #6 used for DT's validation and testing.
- Remaining lights used for studying impact of increased light sources.
- "□": patch locations used for authentication experiments.



3-D view of the capturing setup in DT

Proposed DT: Patch Photos Generation

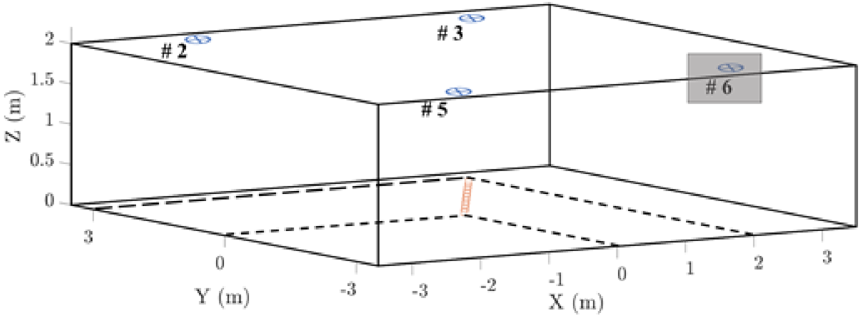
- Generate raw synthetic photos using diffuse reflection model.
- Sequentially turn off lights #5, #6, #3, and #2, while keeping rest 3 lights on.
- 3 lights superimposed ➔ one equivalent stronger light source.

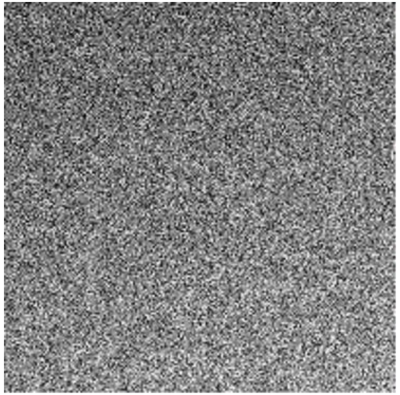


light #5 off
Raw synthetic photos of a paper patch

Proposed DT: Patch Photos Generation

- Generate raw synthetic photos using diffuse reflection model.
- Sequentially turn off lights #5, #6, #3, and #2, while keeping rest 3 lights on.
- 3 lights superimposed ➔ one equivalent stronger light source.



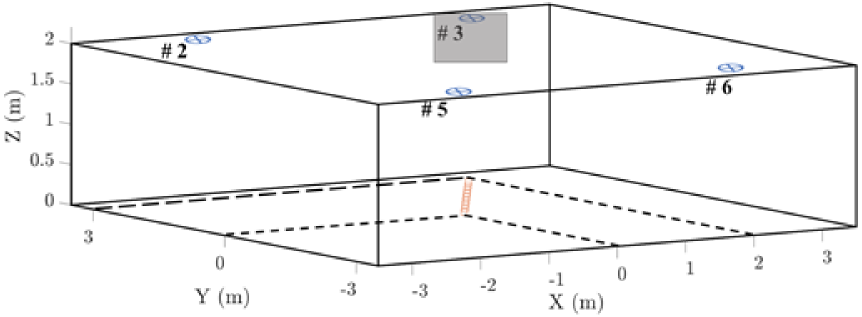


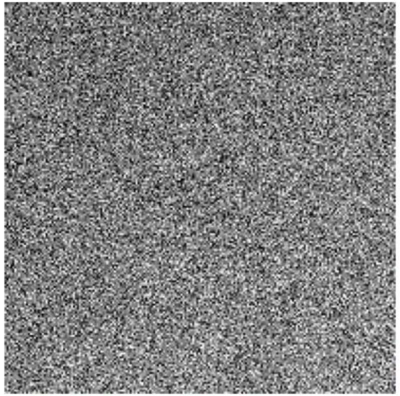
light #6 off

Raw synthetic photos of a paper patch

Proposed DT: Patch Photos Generation

- Generate raw synthetic photos using diffuse reflection model.
- Sequentially turn off lights #5, #6, #3, and #2, while keeping rest 3 lights on.
- 3 lights superimposed ➔ one equivalent stronger light source.



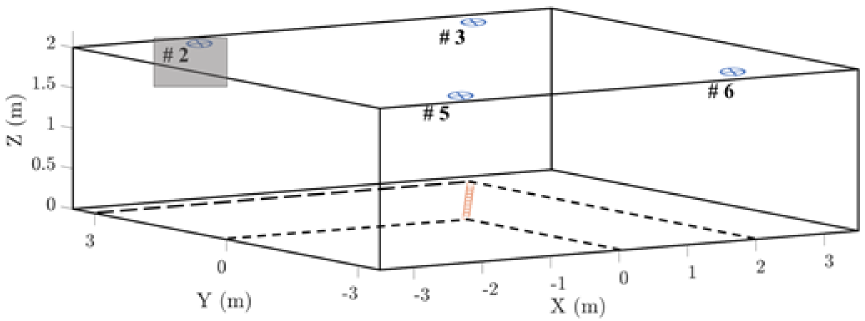


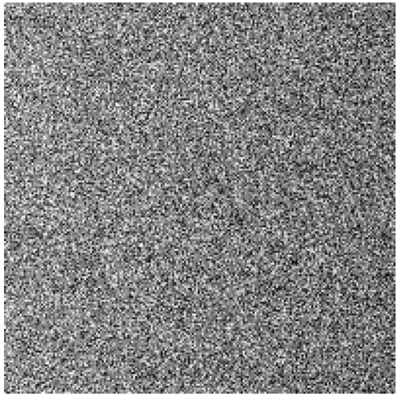
light #3 off

Raw synthetic photos of a paper patch

Proposed DT: Patch Photos Generation

- Generate raw synthetic photos using diffuse reflection model.
- Sequentially turn off lights #5, #6, #3, and #2, while keeping rest 3 lights on.
- 3 lights superimposed ➔ one equivalent stronger light source.



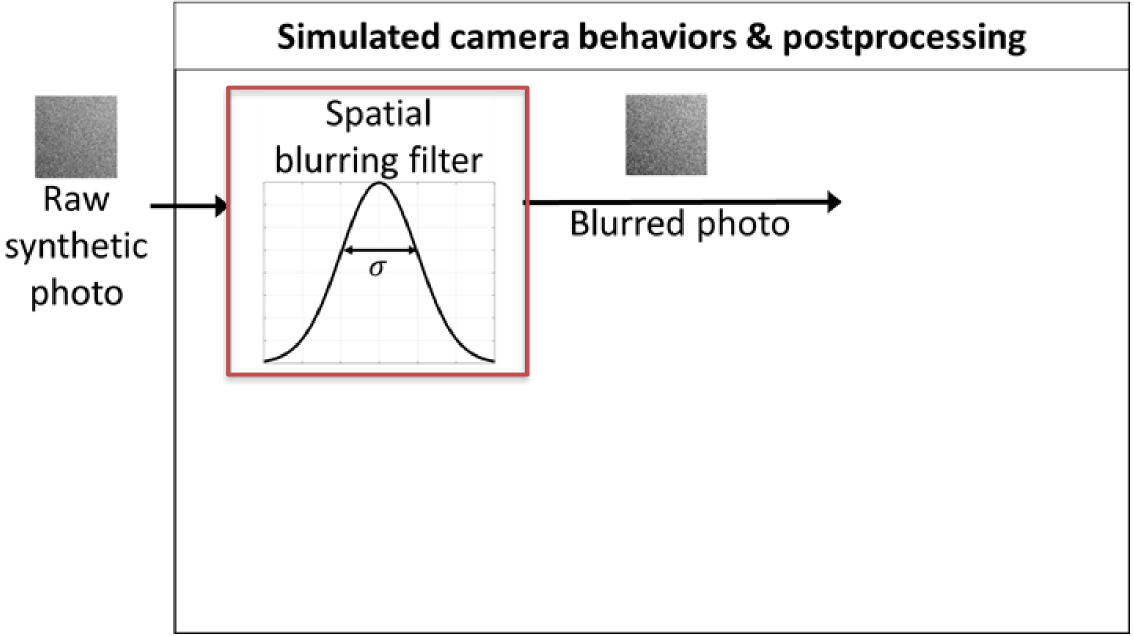


light #2 off

Raw synthetic photos of a paper patch

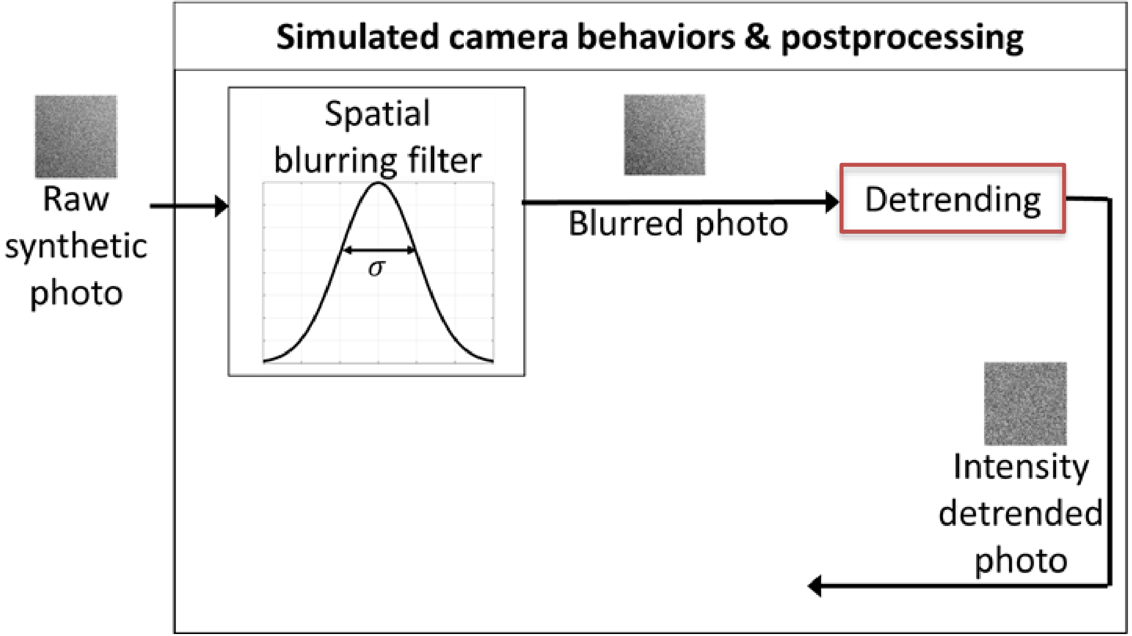
Proposed DT: Simulated Camera & Postprocessing

- Generate synthetic patches that resemble real patch's appearance.
- Spatial blurring filter



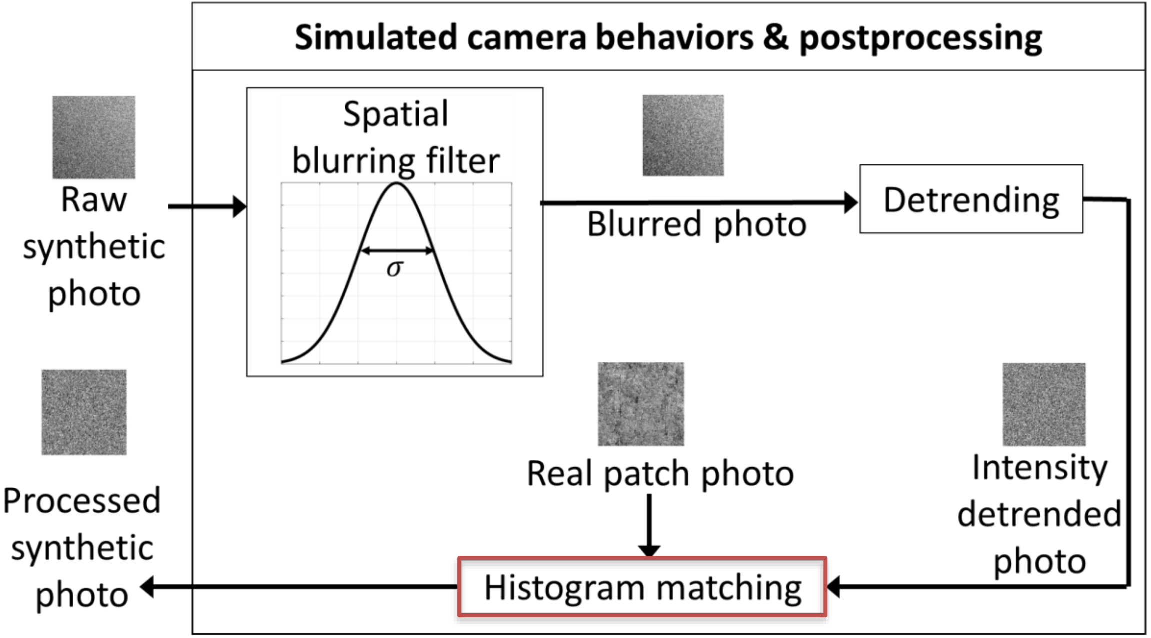
Proposed DT: Simulated Camera & Postprocessing

- Generate synthetic patches that resemble real patch's appearance.
- Spatial blurring filter
- Detrending



Proposed DT: Simulated Camera & Postprocessing

- ❖ Generate synthetic patches that resemble real patch's appearance.
- ❖ Spatial blurring filter
- ❖ Detrending
- ❖ Histogram matching



Outline

- Introduction and Motivation
- Proposed Digital Twin
- **Digital-Twin Guidance**
- Proposed Real-World Authentication Method
- Conclusion and Future Work

Digital-Twin Guidance: Normal Vectors Estimator Design

- Goal: To estimate three unknowns n_x, n_y, and n_z of a normal vector.
- Estimator Inputs: pixel intensity $\zeta^{(1)}$ and incident light vectors $\mathbf{v}^{(-1)}$.
- $\zeta^{(1)}$: aggregated pixel intensity for 3 turned-on lights excluding light #1.

$$\zeta^{(1)} = \sum_{k=2}^{4} l_{\mathrm{r}}^{(k)} / [\lambda l^{(k)}]$$

Digital-Twin Guidance: Normal Vectors Estimator Design

- Goal: To estimate three unknowns $n_x, n_y,$ and n_z of a normal vector.
- Estimator Inputs: pixel intensity $\zeta^{(1)}$ and incident light vectors $\mathbf{v}^{(-1)}$.
- $\zeta^{(1)}$: aggregated pixel intensity for 3 turned-on lights excluding light #1.

$$\zeta^{(1)} = \sum_{k=2}^{4} l_{\mathrm{r}}^{(k)} / [\lambda l^{(k)}]$$
$$= \mathbf{n}^{\top} \left(\sum_{k=2}^{4} \mathbf{v}^{(k)} \right)$$

Digital-Twin Guidance: Normal Vectors Estimator Design

- Goal: To estimate three unknowns n_x, n_y, and n_z of a normal vector.
- Estimator Inputs: pixel intensity $\zeta^{(1)}$ and incident light vectors $\mathbf{v}^{(-1)}$.
- $\zeta^{(1)}$: aggregated pixel intensity for 3 turned-on lights excluding light #1.
- $\mathbf{v}^{(-1)}$: combined incident light vector excluding light #1.

$$\zeta^{(1)} = \sum_{k=2}^{4} l_{\mathrm{r}}^{(k)} / [\lambda l^{(k)}]$$

$$= \mathbf{n}^{\top} \left(\sum_{k=2}^{4} \mathbf{v}^{(k)} \right) \stackrel{\text{def}}{=} \mathbf{n}^{\top} \mathbf{v}^{(-1)},$$

Digital-Twin Guidance: Searching for Best Mode

Config. (A)/Perfect Reconstruction
test to ensure correctness of model.

	Configuration	Cos-sim ↑
(A)	Raw synthetic photo (PR test)	1
(B)	Uniform incident light + (A)	0.90
(C)	Dynamic range expansion + (B)	0.84
(D)	Postprocessing[1] + (C)	0.80
(E)	Dynamic range expansion + (A)	0.63
(F)	Postprocessing[1] + (E)	0.60

Digital-Twin Guidance: Searching for Best Mode

Config. (A)/Perfect Reconstruction test to ensure correctness of model.

	Configuration	Cos-sim ↑
(A)	Raw synthetic photo (PR test)	1
(B)	Uniform incident light + (A)	0.90
(C)	Dynamic range expansion + (B)	0.84
(D)	Postprocessing[1] + (C)	0.80
(E)	Dynamic range expansion + (A)	0.63
(F)	Postprocessing[1] + (E)	0.60

Decreasing trend in cosine similarity as adding more factors.

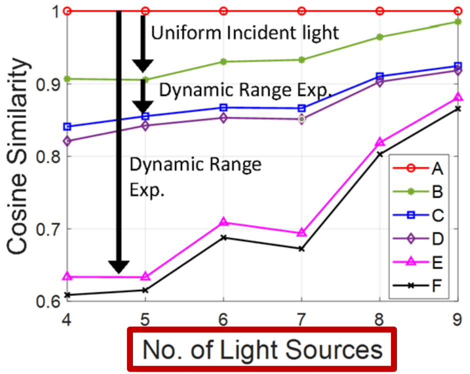
Digital-Twin Guidance: Searching for Best Mode

Config. (A)/Perfect Reconstruction test to ensure correctness of model.

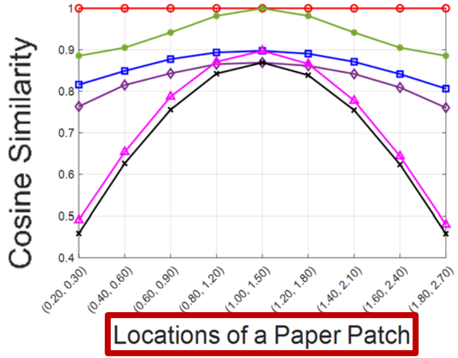
	Configuration	Cos-sim ↑
(A)	Raw synthetic photo (PR test)	1
(B)	Uniform incident light + (A)	0.90
(C)	Dynamic range expansion + (B)	0.84
(D)	Postprocessing[1] + (C)	0.80
(E)	Dynamic range expansion + (A)	0.63
(F)	Postprocessing[1] + (E)	0.60

Decreasing trend in cosine similarity as adding more factors.

Varying 2 Other Factors



More lights ➔ better performance.



Closer to geo-center ➔better performance.

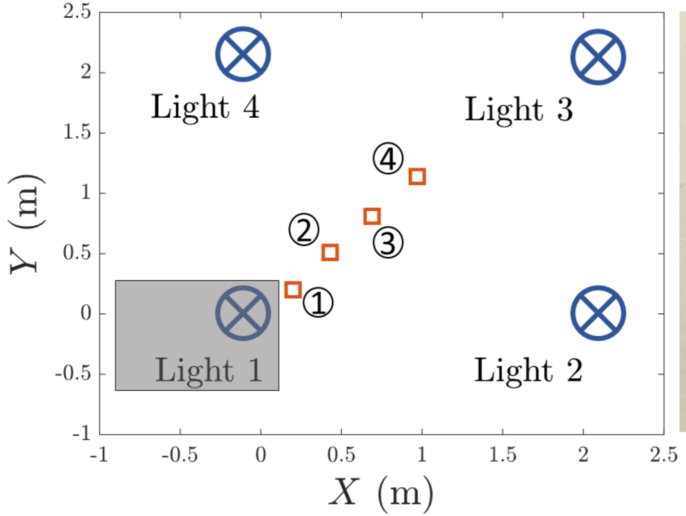
Outline

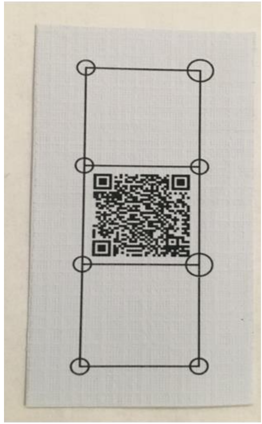
- ❖Introduction and Motivation
- ❖Proposed Digital Twin
- ❖Digital-Twin Guidance
- ❖**Proposed Real-World Authentication Method**
- ❖Conclusion and Future Work

Proposed Real-World Authentication Method

Digital twin guided

- shape & number of light sources.
- placement of paper patch.
- capturing of real-world patches.



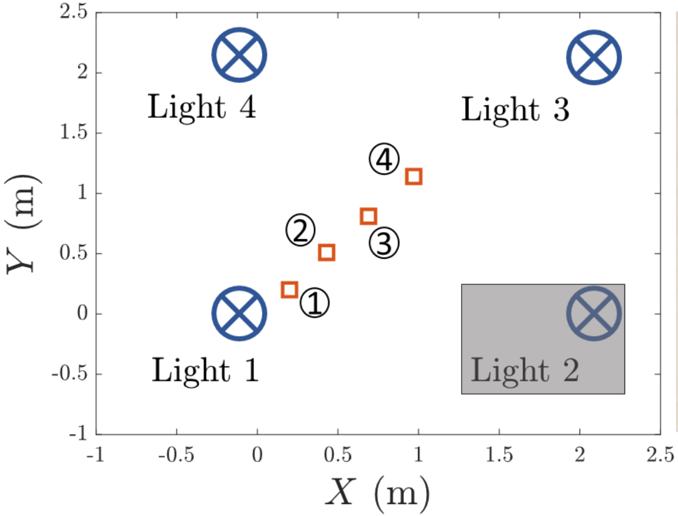


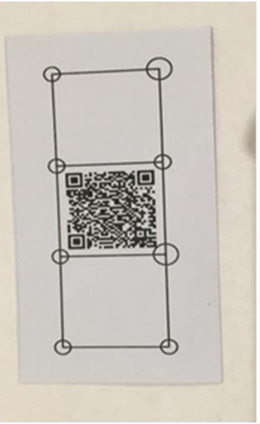
“Negative” Light Source ➔ Blocked one of four lights for each image captured and cast a shadow onto patch.

Proposed Real-World Authentication Method

Digital twin guided

- shape & number of light sources.
- placement of paper patch.
- capturing of real-world patches.



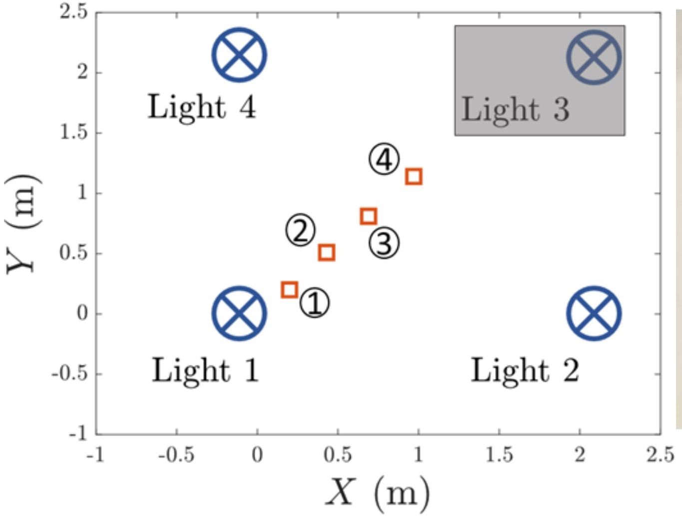


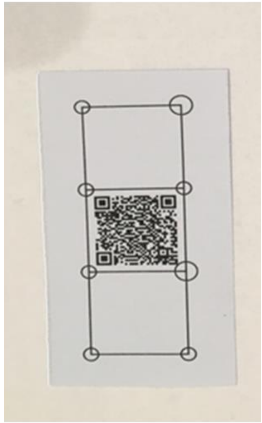
“Negative” Light Source ➔ Blocked one of four lights for each image captured and cast a shadow onto patch.

Proposed Real-World Authentication Method

Digital twin guided

- shape & number of light sources.
- placement of paper patch.
- capturing of real-world patches.



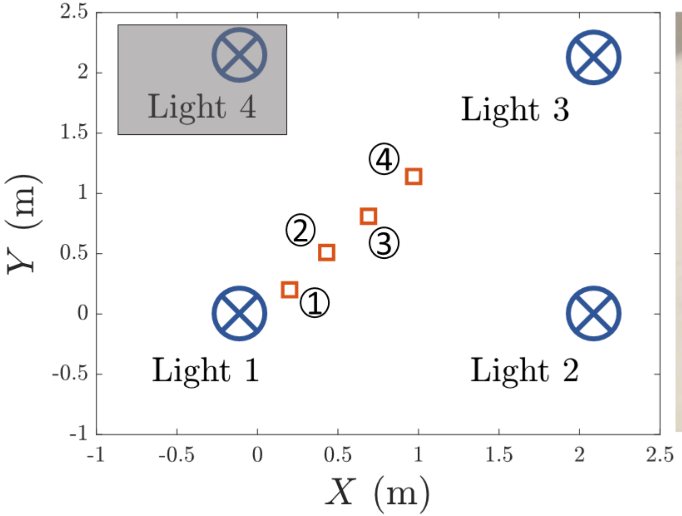


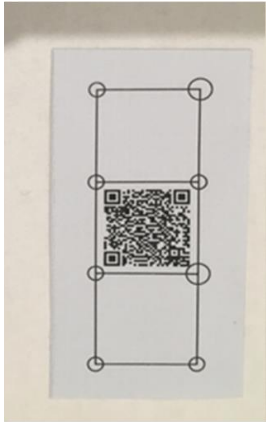
“Negative” Light Source ➔ Blocked one of four lights for each image captured and cast a shadow onto patch.

Proposed Real-World Authentication Method

Digital twin guided

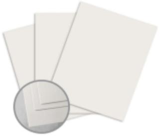
- shape & number of light sources.
- placement of paper patch.
- capturing of real-world patches.





“Negative” Light Source ➔ Blocked one of four lights for each image captured and cast a shadow onto patch.

Proposed Authentication Method: Performance



Location Index	Resume Paper[1]		Copy Paper[2]		Cardstock[3]	
	x	y	x	y	x	y
①	0.26	0.44	0.16	0.14	0.09	0.14
②	0.42	0.53	0.15	0.09	0.07	0.07
③	0.47	0.49	0.23	0.18	0.10	0.04
④	0.56	0.40	0.27	0.11	0.12	0.02
Average	0.43	0.46	0.20	0.13	0.09	0.07

rougher ➔ better authentication

- ❖ Obtained meaningful correlation for most cases.
- ❖ Resume paper (most textured) best, while cardstock (smoothest) worst.

1. https://www.shoplet.com/Southworth-Resume-Envelopes/SOUR1410L/spdv
2. https://fivestarofficesupply.com/neenah-paper-inc/exact-index-copy-paper-white/WAU40311/p
3. https://www.snapncrop.com/85x11-Grey-Cardstock--10-Sheets-_p_5319.html

Outline

- ❖ Introduction and Motivation
- ❖ Proposed Digital Twin
- ❖ Digital-Twin Guidance
- ❖ Proposed Real-World Authentication Method
- ❖ **Conclusion and Future Work**

Conclusion and Future Work

- Proposed a paper-based authentication method using **indoor lights** without the need for active light sources.
- Developed a digital twin to aid the design of a real-world authentication method.
- Simulated synthetic patches to analyze impactful factors.
- Demonstrated feasibility of the proposed method for an office setup.
- **Plan**: To conduct comprehensive real-world verifications with more paper patches and lighting setups.

Enabling Paper-Based Surface Authentication via Digital Twin Modeling and Experimental Verification

Prasun Datta,[1] Chau-Wai Wong,[1] Min Wu[2]

[1]NC State University [2]University of Maryland, College Park

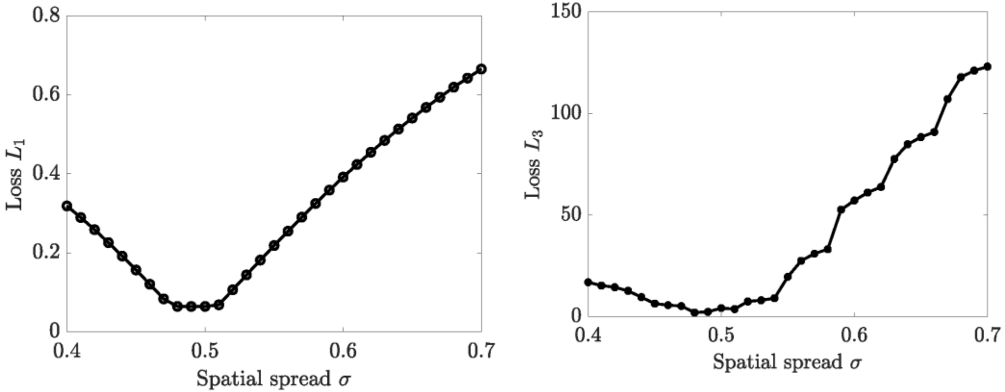
August 8, 2024

IEEE MIPR 2024

Backup Slides

Proposed DT: Tuning Standard Deviation

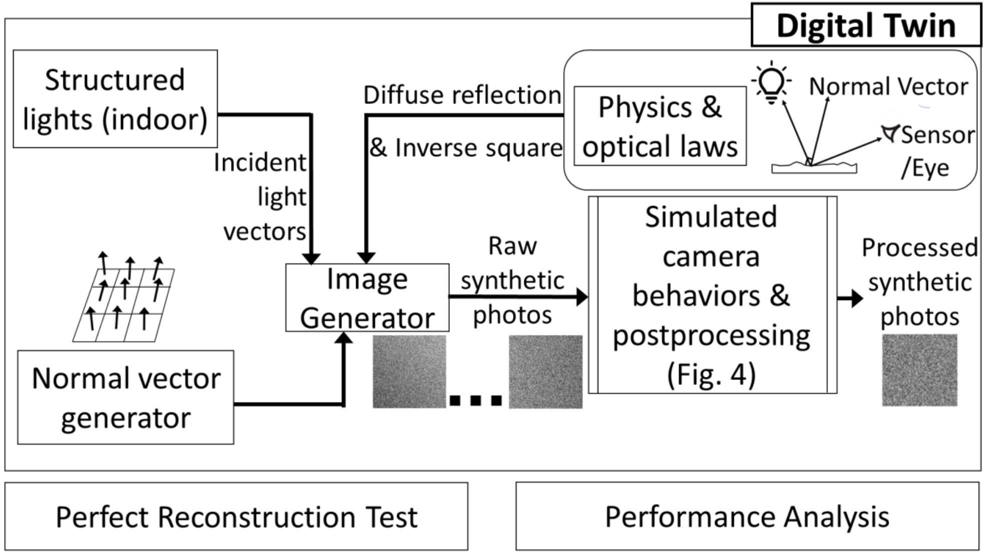
- Three statistical grounded loss functions to characterize difference in distribution of pixel intensity.
- $L_1(\sigma)$: difference of the mean; $L_2(\sigma)$: difference of the median; $L_3(\sigma)$: symmetric Kullback-Leibler (KL) divergence.
- Initial search range of [0.3, 1.30] with 0.1 step size, and then narrowed down to [0.4, 0.7] with 0.01 step size.



$L_1(\sigma)$ and $L_3(\sigma)$ are minimized around $\sigma = 0.5$.

Proposed Digital Twin (DT)

- **Image Generator**: synthesize paper patches using (i) physics and optical laws, (ii) indoor lighting, and (iii) normal vectors.
- **Postprocessing**: spatial blurring, detrending, histogram matching.
- **Perfect Reconstruction Test**: ensure correctness of DT.
- **Performance Analysis**: reveal best mode for designing real-world authentication methods.



Proposed DT: Simulated Camera & Postprocessing

- Generate synthetic patches that resemble real patch's appearance.
- Spatial blurring filter models
  - fiber's diffusion effect of light.
  - point spread function of camera.
- Detrending eliminates spatial trend.
- Histogram matching makes sure the synthetic photo mimics the real patch photo.