Secure Cloud-Based Volume Ray-Casting

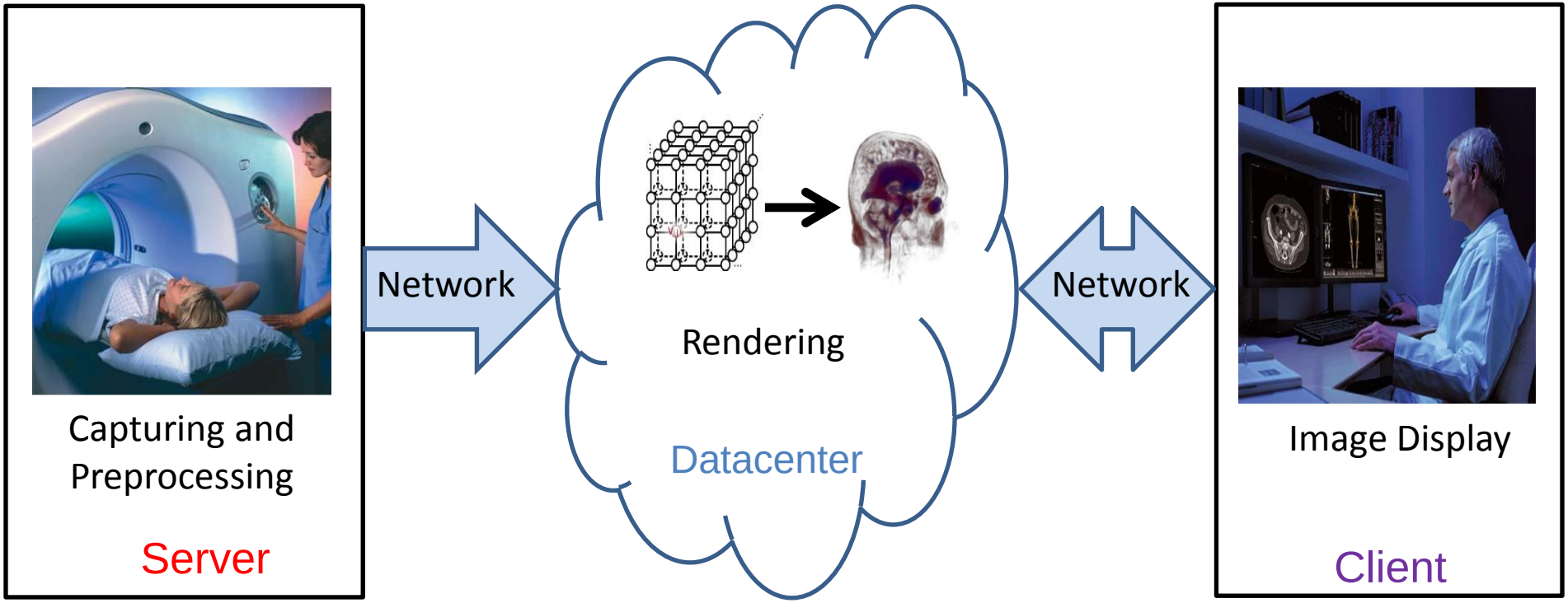
Manoranjan Mohanty
Wei Tsang Ooi
National University of Singapore

Pradeep K. Atrey
University of Winnipeg

Cloud-Based Volume Rendering is Becoming Popular

- Research
  - ✓Dorn et al. 2011.
  - ✓Philbin et al. 2011.
  - ✓Vazhenin. 2012.
- Companies Offering Cloud-based Rendering
  - ✓Microsoft, KDDI, Sinha Systems etc.

Cloud-Based Volume Ray-Casting



Security and Privacy are the Main Challenges

- How many of you mind if your medical image is available to an adversary?
- What can an adversary do with an image?

http://greenberg-art.com/.Toons/Toons,%20social/ qqxsgMedical%20privacy.gif

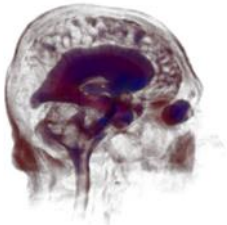
Addressing Security and Privacy Challenges

- Little Explored Area

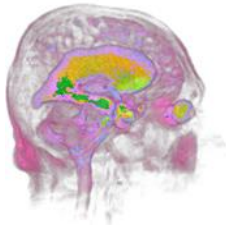
Addressing Security and Privacy Challenges

- Little Explored Area

- Secure Pre-Classification Volume Ray-Casting



Original



Color Hidden

Manoranjan Mohanty, Pradeep K. Atrey, and Wei Tsang Ooi. **Secure cloud-based medical data visualization**. 2012.

Our Objective

- Secure Post-Classification Volume Ray-Casting
  - ✓Confidentiality: Hide both color and shape
  - ✓Integrity
  - ✓Privacy
  - ✓Low Overheads

Technical Challenges

- Finding a Cryptosystem
  - ✓ Fully homomorphic cryptosystem is not practical
  - ✓ Somewhat homomorphic cryptosystem cannot hide all information

Technical Challenges

- Finding a Cryptosystem
  - ✓ Fully homomorphic cryptosystem is not practical
  - ✓ Somewhat homomorphic cryptosystem cannot hide all information
- Using Floating Point Numbers with a Cryptosystem
  - ✓ Modular prime operation of a cryptosystem is incompatible with floating point operations of ray-casting

Addressing Technical Challenges

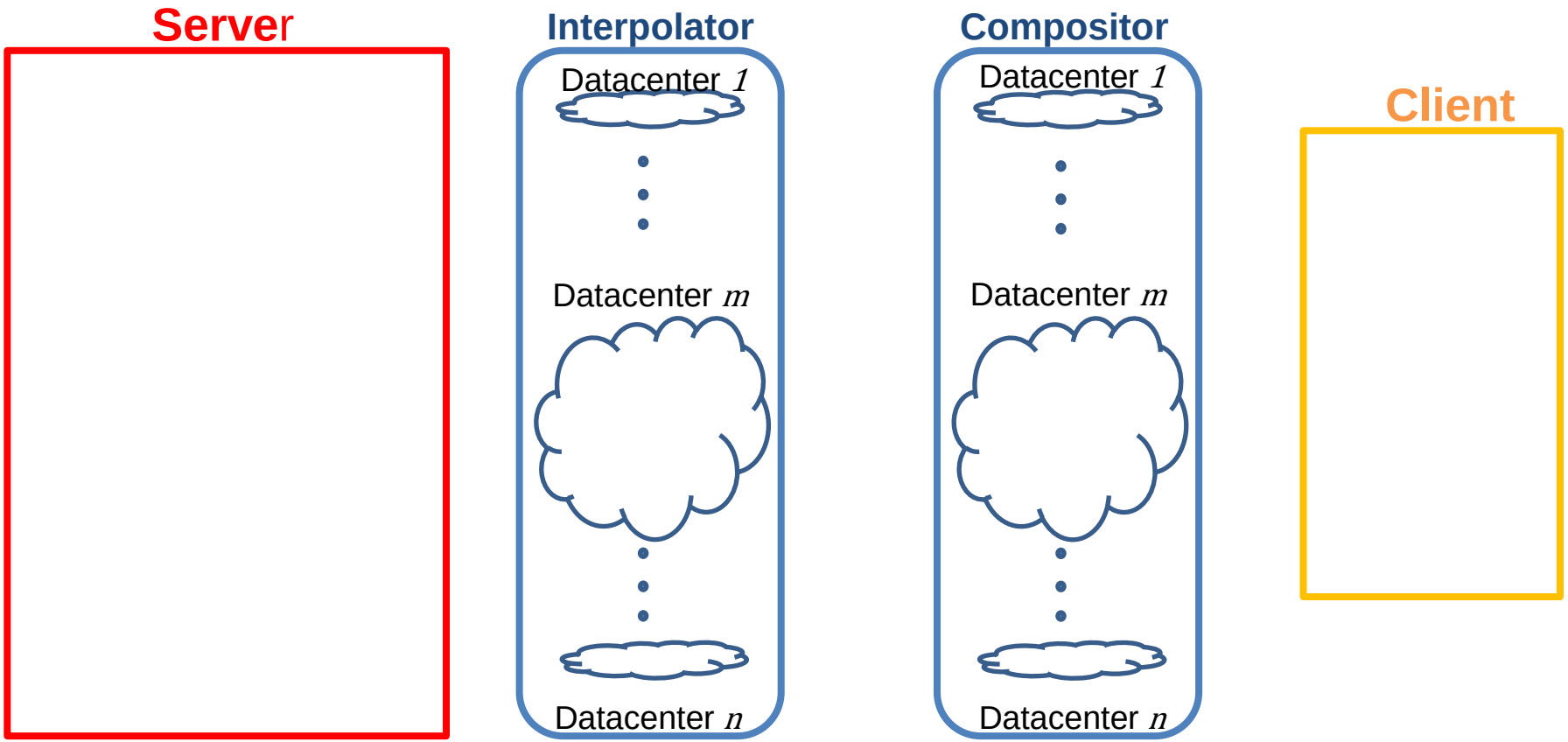
- Finding a Cryptosystem
  - ✓ Shamir's secret sharing-based secure multi-party computation

Addressing Technical Challenges

- Finding a Cryptosystem
  - ✓Shamir's secret sharing-based secure multi-party computation
- Using Floating Point Numbers with Shamir's Secret Sharing
  - ✓Convert floating point number to fixed point number

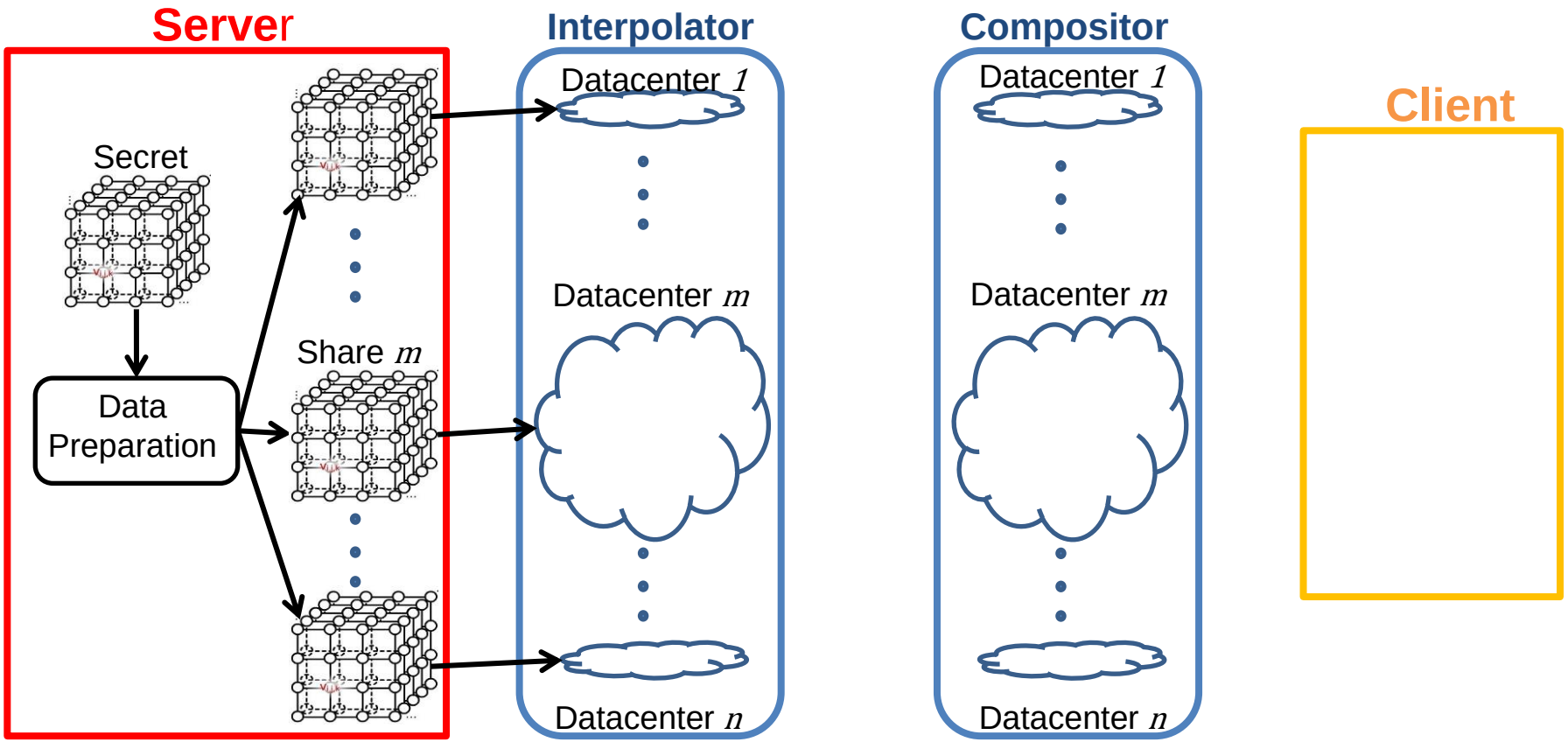
Secure Cloud-Based Volume Ray-casting Framework

❖Architecture



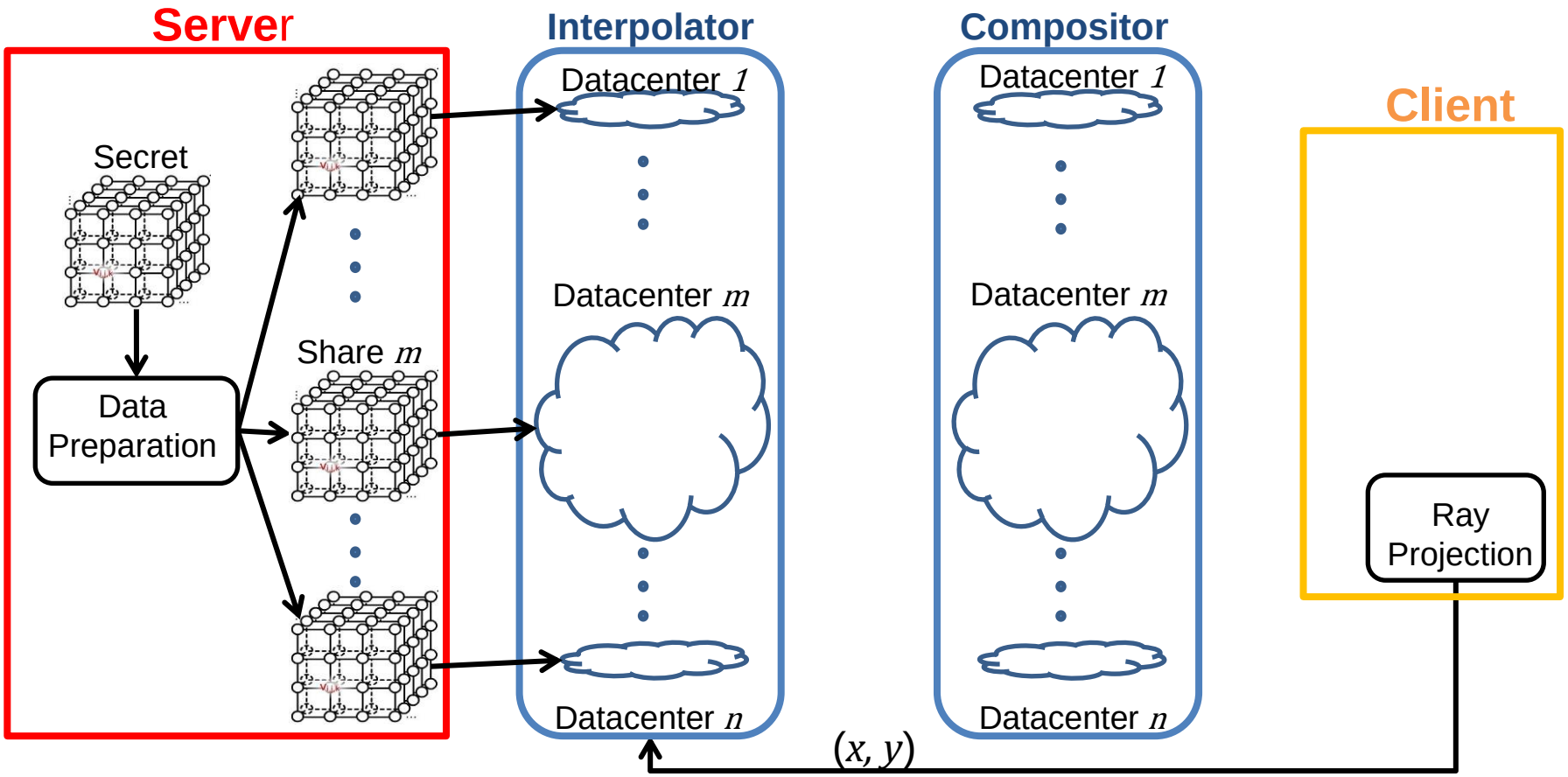
Secure Cloud-Based Volume Ray-casting Framework

❖Workflow: Data Preparation



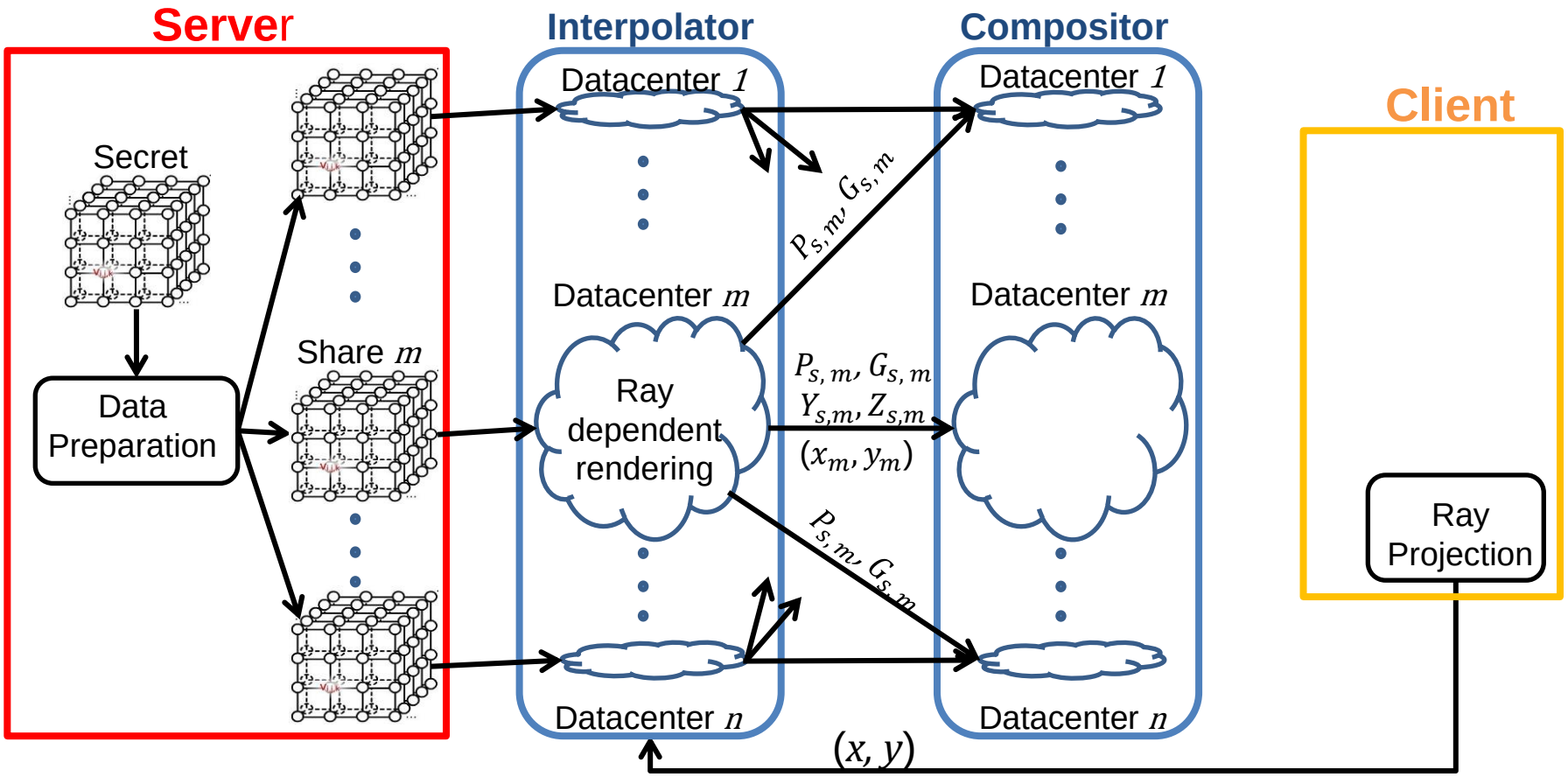
Secure Cloud-Based Volume Ray-casting Framework

❖Workflow: Ray Projection



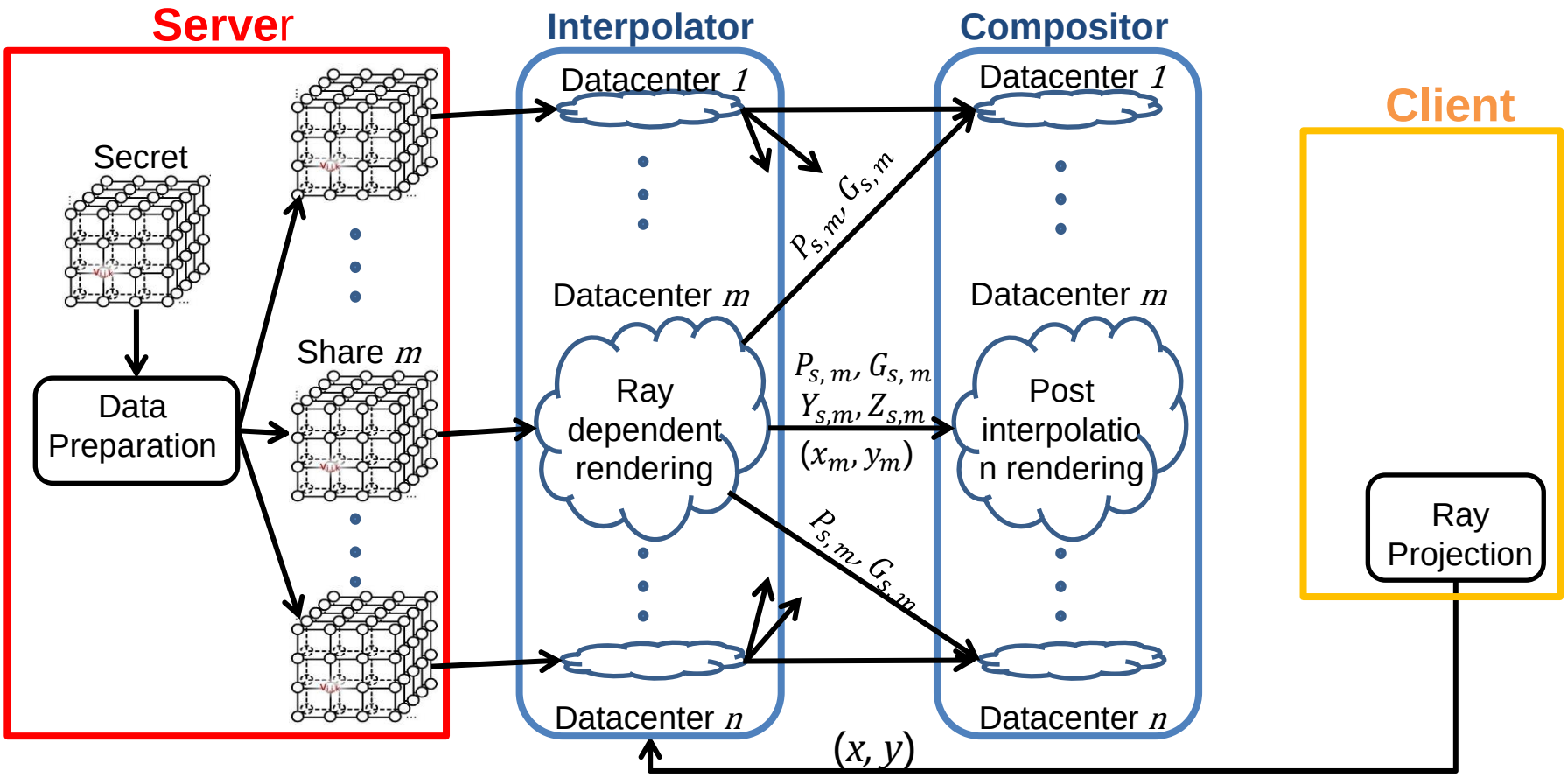
Secure Cloud-Based Volume Ray-casting Framework

❖Workflow: Ray Dependent Rendering



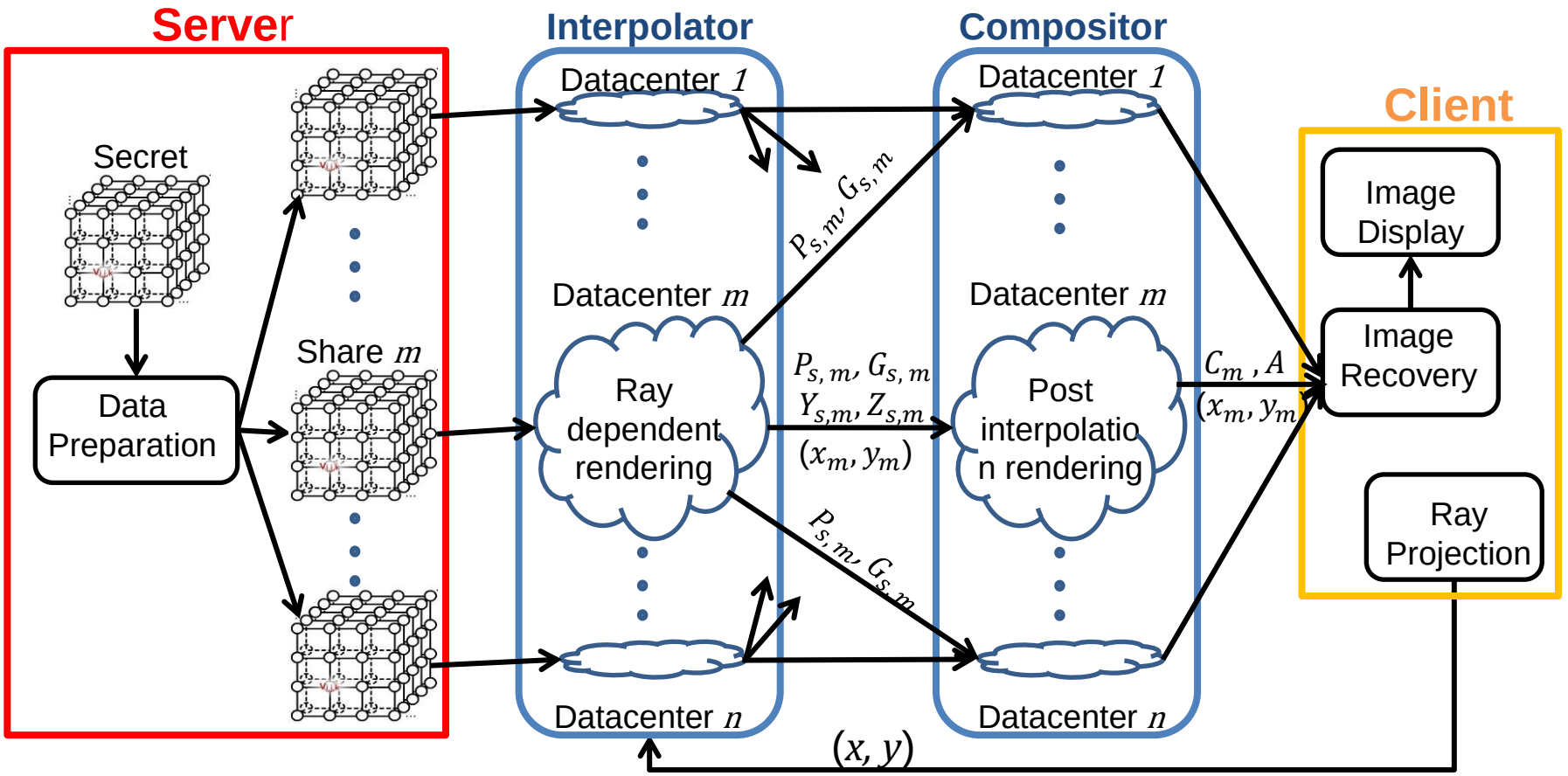
Secure Cloud-Based Volume Ray-casting Framework

❖Workflow: Post Interpolation Rendering



Secure Cloud-Based Volume Ray-casting Framework

❖Workflow: Image Recovery



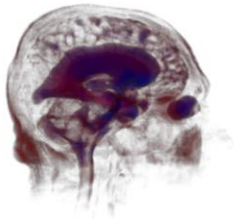
Experiment

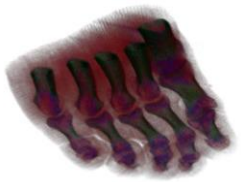
- Server, Datacenters, and Client are simulated in a PC

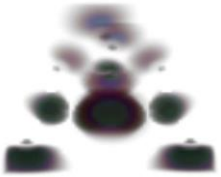
- Customized VTK *5.8.0*
  - ✓Pre-classification volume ray-casting
  - ✓Integrated (3,5) Secret Sharing

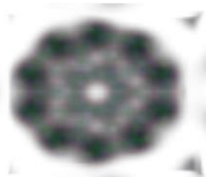
Data Sets

	Dimension	Size
Head	256 X 256 X 124	7.8 MB
Foot	256 X 256 X 256	16 MB
Iron port	68 X 68 X 68	307.3 KB
Bucky	32 x 32 X 32	32.2 KB

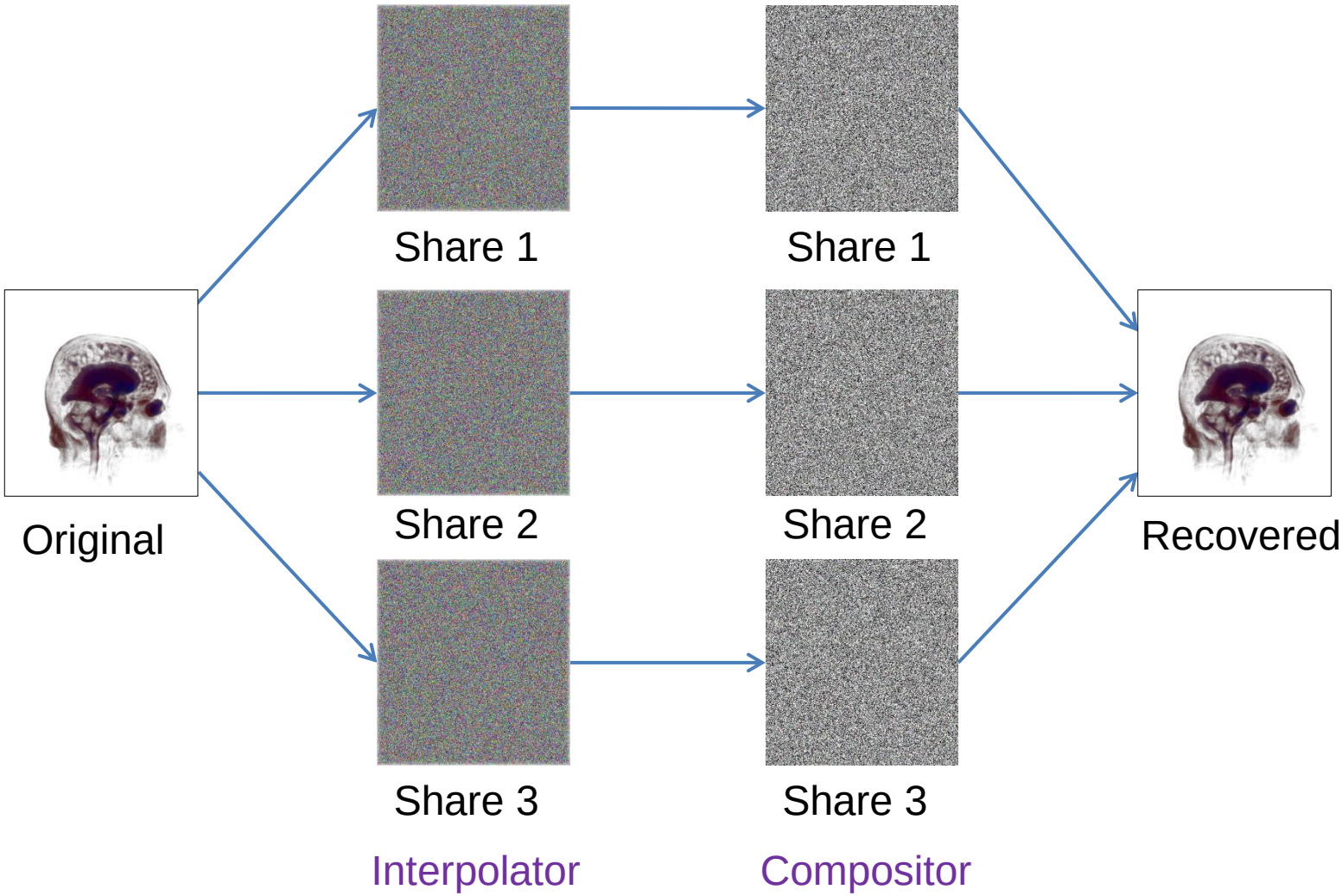




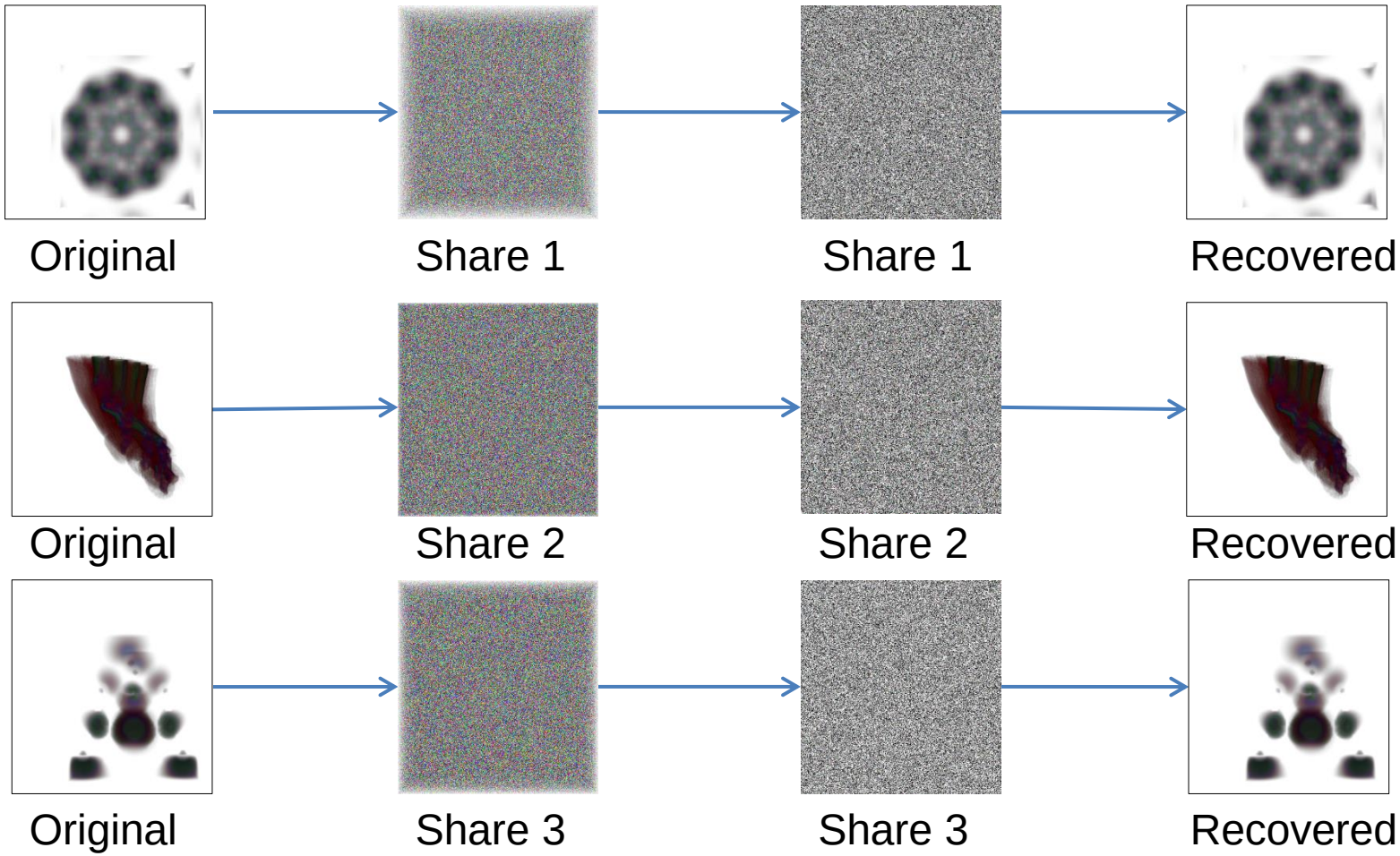




Results

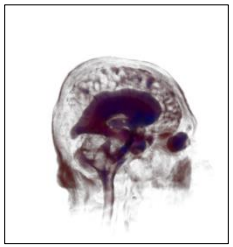

Share 1
Share 1
Original
Share 2
Share 2
Recovered
Share 3
Share 3
Interpolator
Compositor

Results

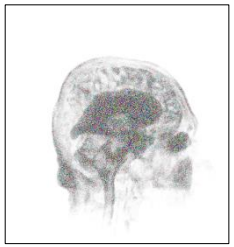

Original
Share 1
Share 1
Recovered
Original
Share 2
Share 2
Recovered
Original
Share 3
Share 3
Recovered
Interpolator
Compositor

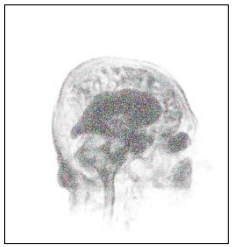
Analysis

- Confidentiality
  - ✓Information theoretically secure
- Integrity



From Untampered Share Images





From Tampered Share Images

Analysis

- Low Computational Overhead
  - ✓$172\ ms$ of more computation for 512×512 image

Analysis

- Low Computational Overhead
  - ✓$172\ ms$ of more computation for 512×512 image
- High Data Overhead
  - ✓19 times more data overhead than conventional rendering

Analysis

- Low Computational Overhead
  - ✓$172\ ms$ of more computation for 512×512 image
- High Data Overhead
  - ✓19 times more data overhead than conventional rendering
  - ✓Low data overhead can be obtained at the cost of security

Thank You !

Q&A