THE UNIVERSITY OF WINNIPEG

Secure Multimedia Processing over Cloud

Pradeep K. Atrey
University of Winnipeg, Canada
p.atrey@uwinnipeg.ca
www.acs.uwinnipeg.ca/pkatrey/

Winnipeg


UWINNIPEG
THE HEART OF THE CITY,
the heart of the continent
THE UNIVERSITY OF WINNIPEG


Fort McMurray
Manitoba
Saskatchewan
Grande Prairie
Thompson
Edmonton
Flin Flon
Prince Albert
Saskatoon
Calgary
Swift Current
Regina
Brandon
Winnipeg
Ontario
Timmins
Amos
Quebec
Ottawa
Montreal
Fredericton
Halifax
Charlotte
Augusta
Concord
Boston
Providence
Hartford
Rochester
Buffalo
Toronto
Detroit
Cleveland
Pittsburgh
New York
Philadelphia
Baltimore
Washington D. C.
Norfolk
Richmond
Louisville
Nashville
Charlotte
Columbia
Atlanta
Jacksonville
Tallahassee
Jackson
Baton Rouge
Austin
Dallas
Little Rock
Birmingham
Memphis
Oklahoma City
Kansas City
St. Louis
Cincinnati
Indianapolis
Dayton
Chicago
Milwaukee
Minneapolis
St. Paul
Duluth
Omaha
Cheyenne
Denver
Boulder
Salt Lake City
Provo
Las Vegas
Reno
Oakland
Los Angeles
San Diego
Phoenix
Albuquerque
Santa Fe
Tucson
Hermosillo
Mexicali
Williston
Grand Forks
Bismarck
Helena
Butte
Boise
Twin Falls
Portland
Vancouver
Seattle
Spokane
Victoria
Prince George
Kamloops
Red Deer
Scottsbluff
U. S. A.
ATLANTIC
OCEAN

Winnipeg Summer

Winnipeg Winter

THE UNIVERSITY OF WINNIPEG

Acknowledgement

- This research is partly supported by

Natural Sciences and Engineering Research Council of Canada

Conseil de recherches en sciences naturelles et en génie du Canada

THE UNIVERSITY OF WINNIPEG

Other Contributors

Manoranjan Mohanty

Wei Tsang Ooi

NUS National University of Singapore

Ankita Lathey

Nishant Joshi

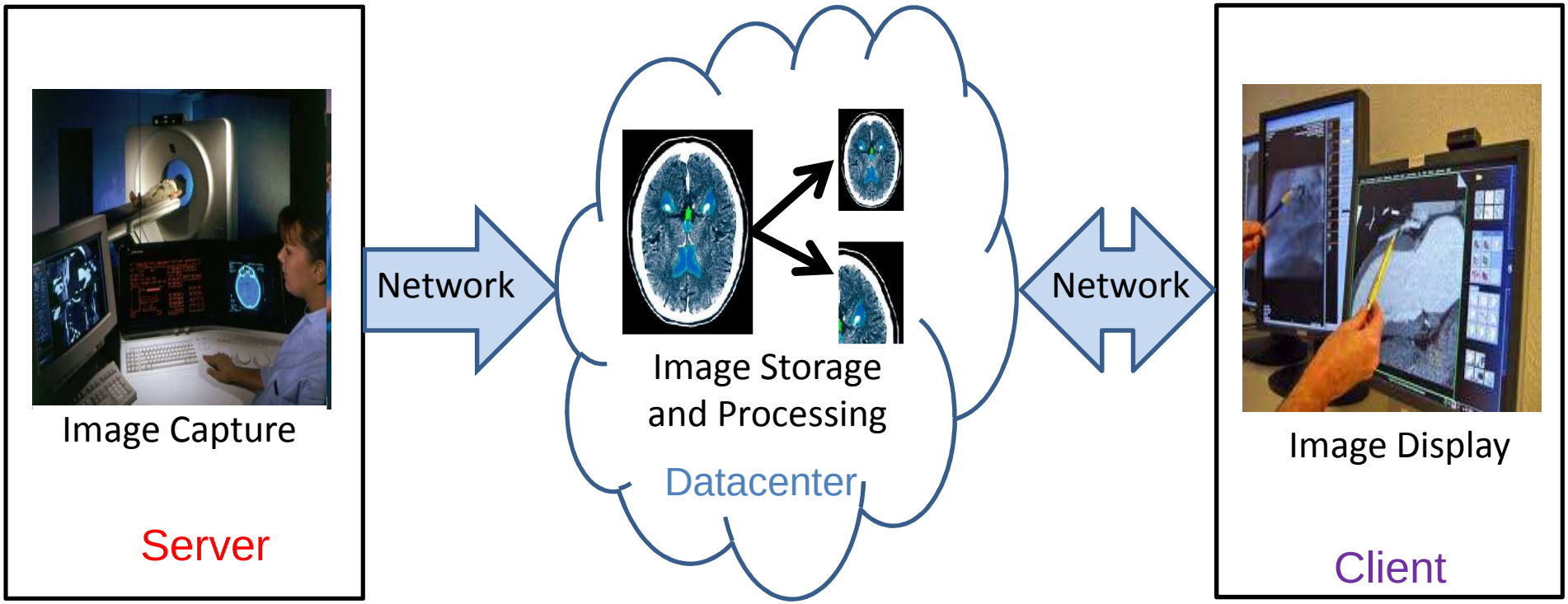
THE UNIVERSITY OF WINNIPEG

Cloud-based Multimedia Computing

- Very popular these days
- Companies Offering 2D Imaging
  - AT&T, Dell, Intel etc.
- Companies Offering 3D Imaging
  - Microsoft, KDDI, Sinha Systems etc.

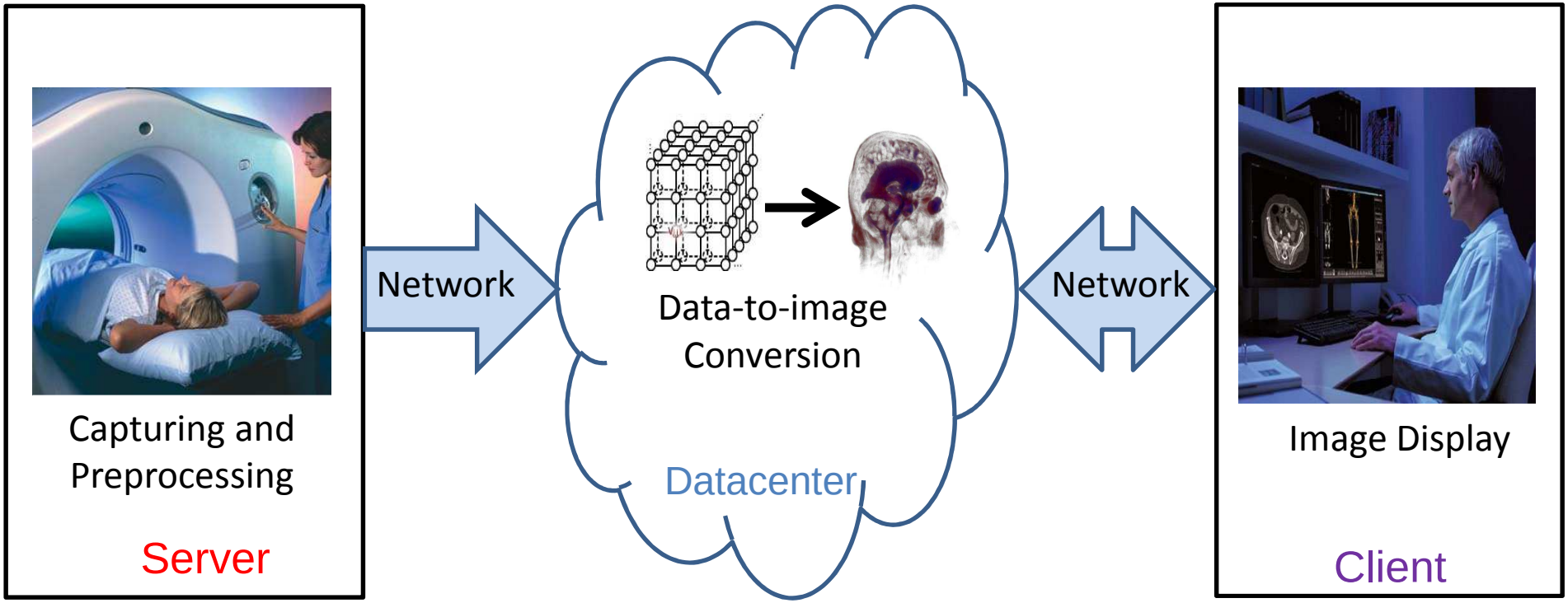
Image source: http://www.msimaging.com/Content/themes/MSI/images/cloud-based-software-image-silo-cloud-file.jpg

Cloud-based Multimedia Storage and Processing



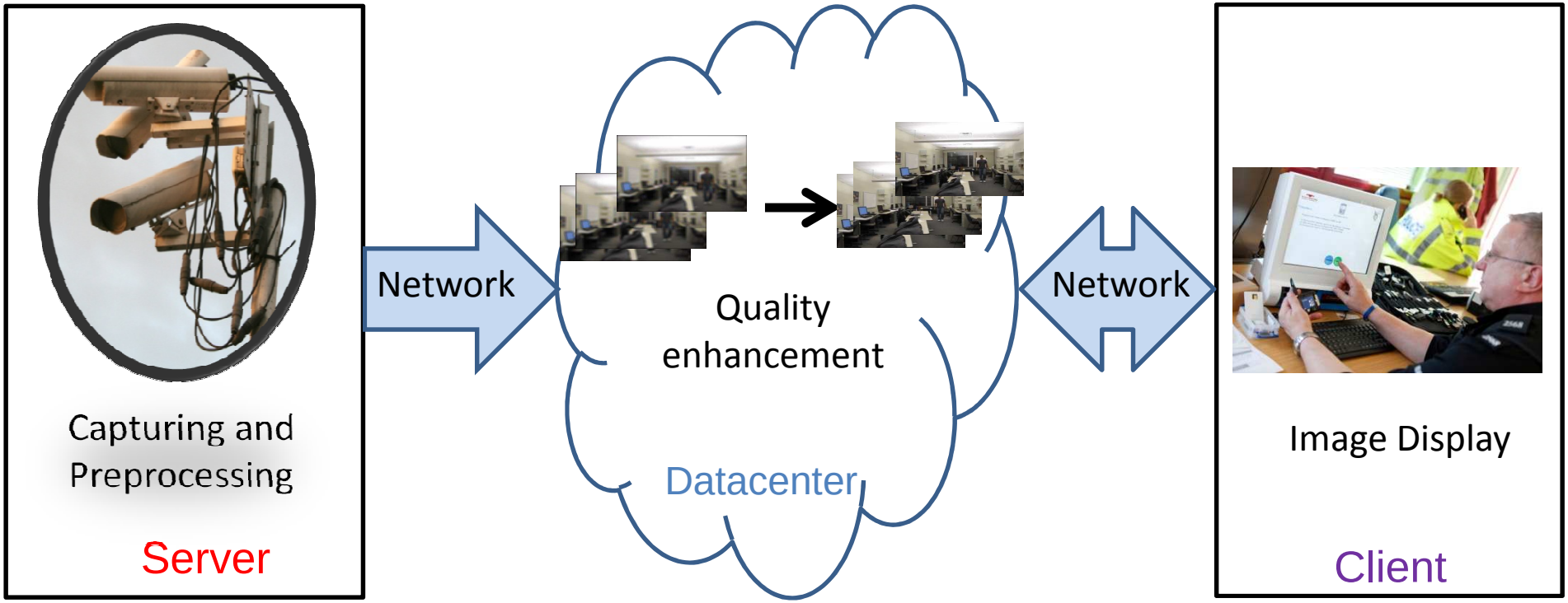
2D Image Visualization

Cloud-based Multimedia Storage and Processing



3D Image Visualization

Cloud-based Multimedia Storage and Processing



Surveillance Video Quality Enhancement

Cloud-based Multimedia Storage and Processing

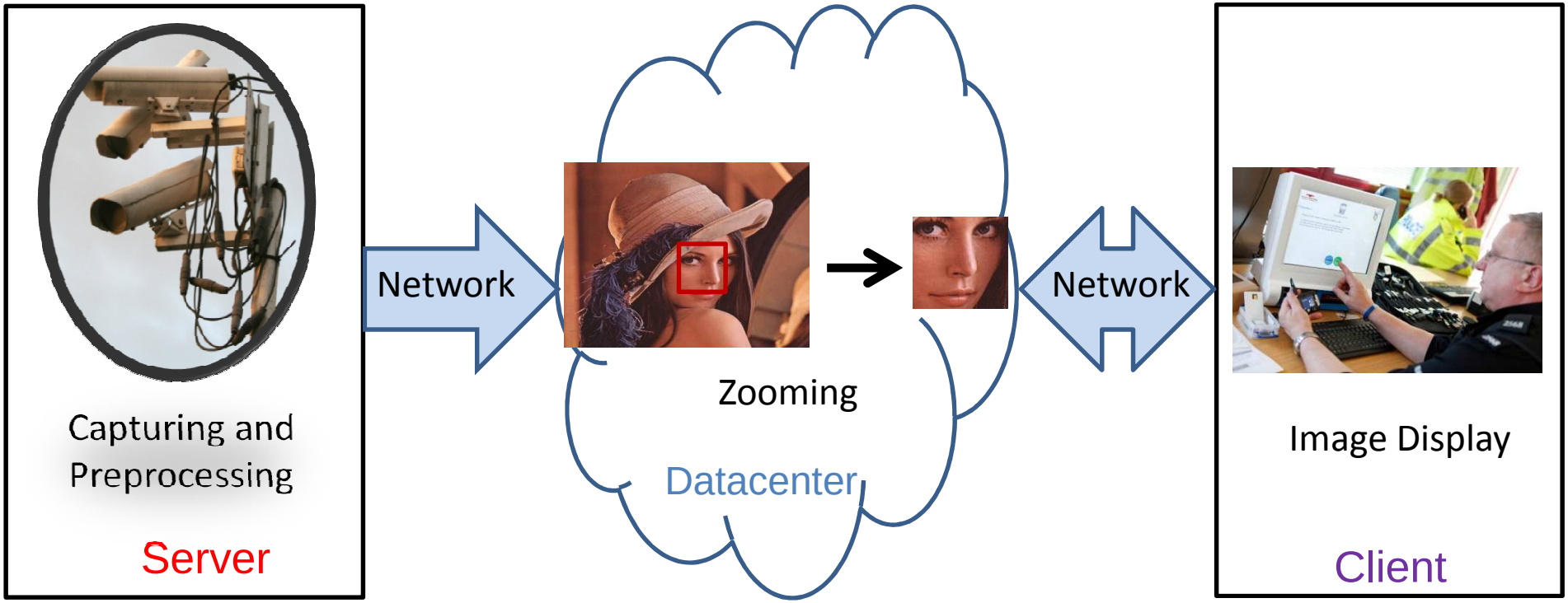


Image Zooming and Cropping

Security and Privacy Challenges in Cloud-based Storage and Processing

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

- What can an adversary do with an image?

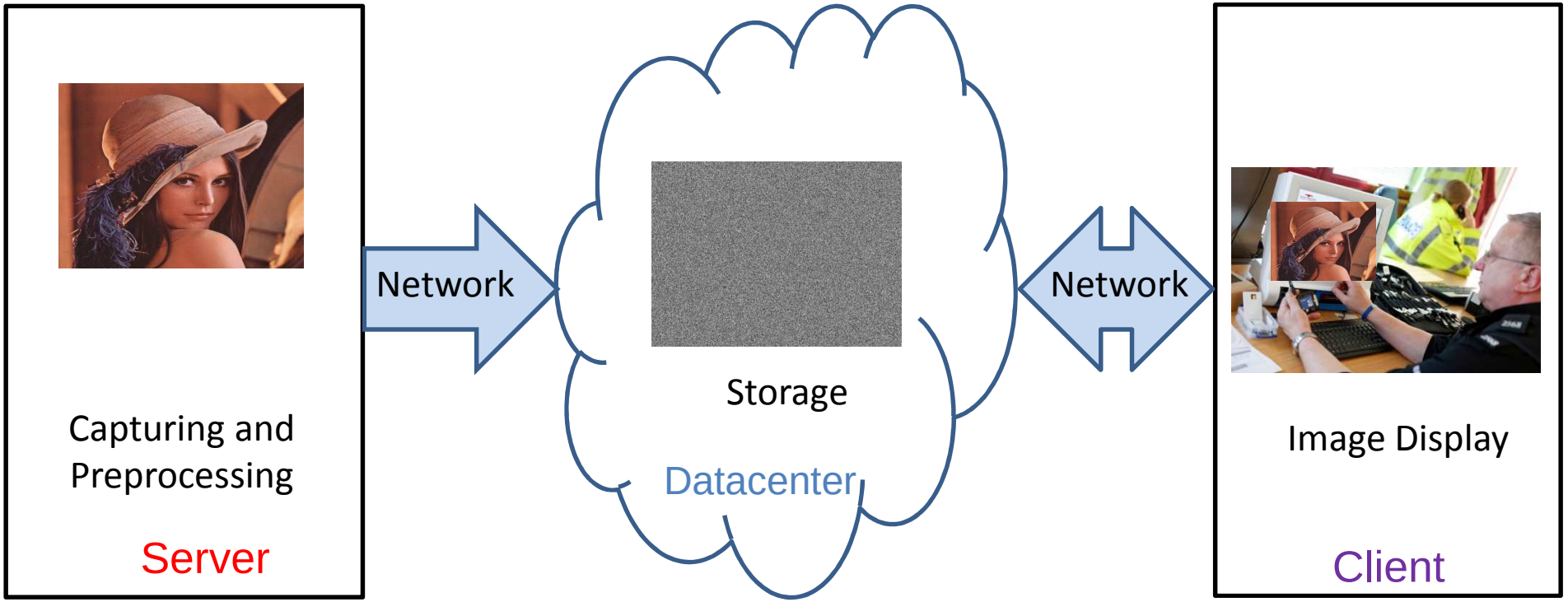
Image source: http://greenberg-art.com/.Toons/Toons,%20social/ qqxsgMedical%20privacy.gif

Rest of the talk

- Introduction and Motivation
- **Addressing the Challenges**
  - Finding a Cryptosystem
  - Using Real Numbers in a Cryptosystem
- Three Frameworks
  - Secure Cloud-based Image Scaling/Cropping
  - Secure Cloud-based Pre-classification Volume Ray-casting
  - Secure Cloud-based Surveillance Video Enhancement
- Conclusions

Smoking is not good for health

Security and Privacy Challenges: Secure Storage over Cloud



Encryption techniques – Watermarking – Secret sharing

Smoking is not good for health

Security and Privacy Challenges: Insecure Processing over Cloud

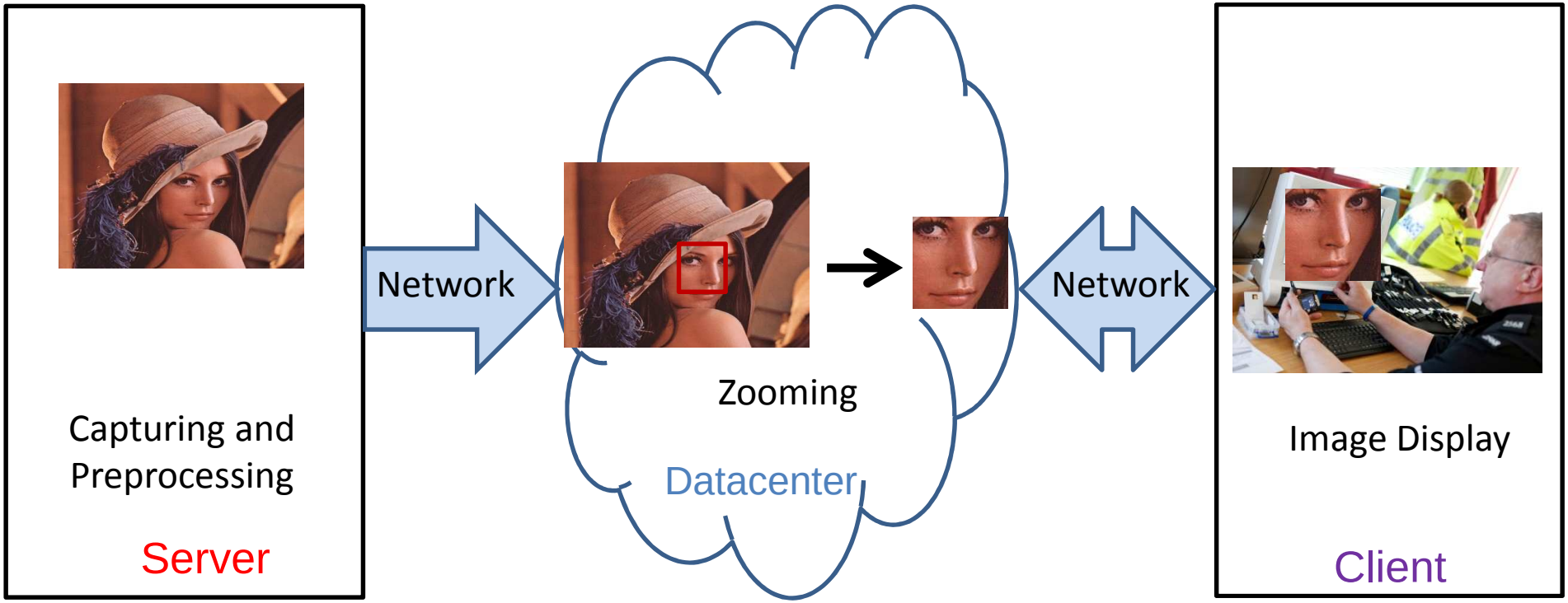


Image Zooming and Cropping on Original Data

Smoking is not good for health

Security and Privacy Challenges: Secure Processing over Cloud

Still to be addressed

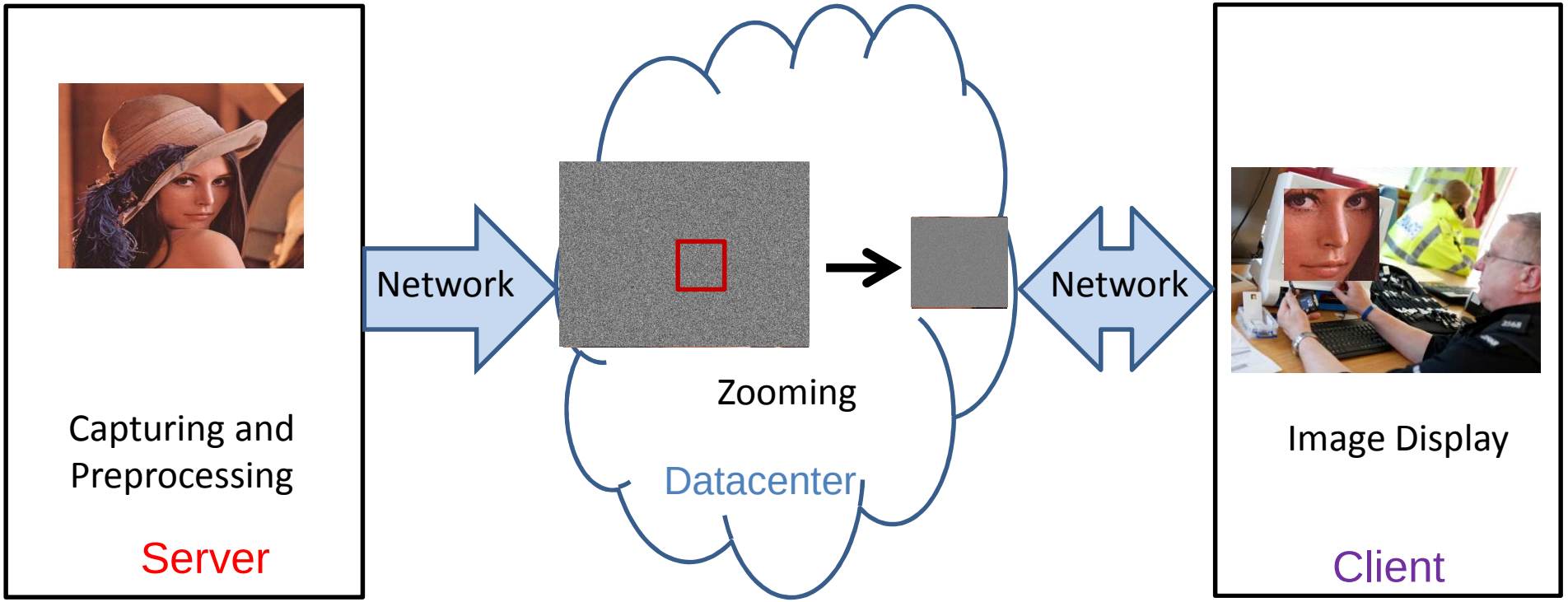


Image Zooming and Cropping on Encrypted Data

Our Objective: Secure Cloud-based Multimedia Processing

- Confidentiality
- Integrity
- Availability
- Privacy

Smoking is not good for health

Our Objective: Secure Cloud-based Multimedia Processing

- Confidentiality
- Integrity
- Availability
- Privacy
- Computational Efficiency
- Bandwidth Efficiency
- High Quality Image

Smoking is not good for health

Technical Challenges

- Finding a Cryptosystem
  - Fully homomorphic cryptosystem is not practical

    E(A) + E(B) = E(A+B)
  - Somewhat homomorphic cryptosystem cannot hide all information

Technical Challenges

- Finding a Cryptosystem
  - Fully homomorphic cryptosystem is not practical

    E(A) + E(B) = E(A+B)
  - Somewhat homomorphic cryptosystem cannot hide all information

- Using Real Numbers in a Cryptosystem
  - Modular prime operation of a cryptosystem is not compatible with real number operations of a data/image processing algorithm

Rest of the talk

- Introduction
- Addressing the Challenges
  - **Finding a Cryptosystem**
  - Using Real Numbers in a Cryptosystem
- Three Frameworks
  - Secure Cloud-based Image Scaling/Cropping
  - Secure Cloud-based Pre-classification Volume Ray-casting
  - Secure Cloud-based Surveillance Video Quality Enhancement
- Conclusions

Finding a Cryptosystem

- Key Observations
  - Shamir's (*k*,*n*) Secret Sharing (SSS) or (*l*,*k*,*n*) Multi-Secret Sharing (MSS) can be used as principal cryptosystem
  - Other cryptosystems can be used to support operations that are not supported by SSS and MSS

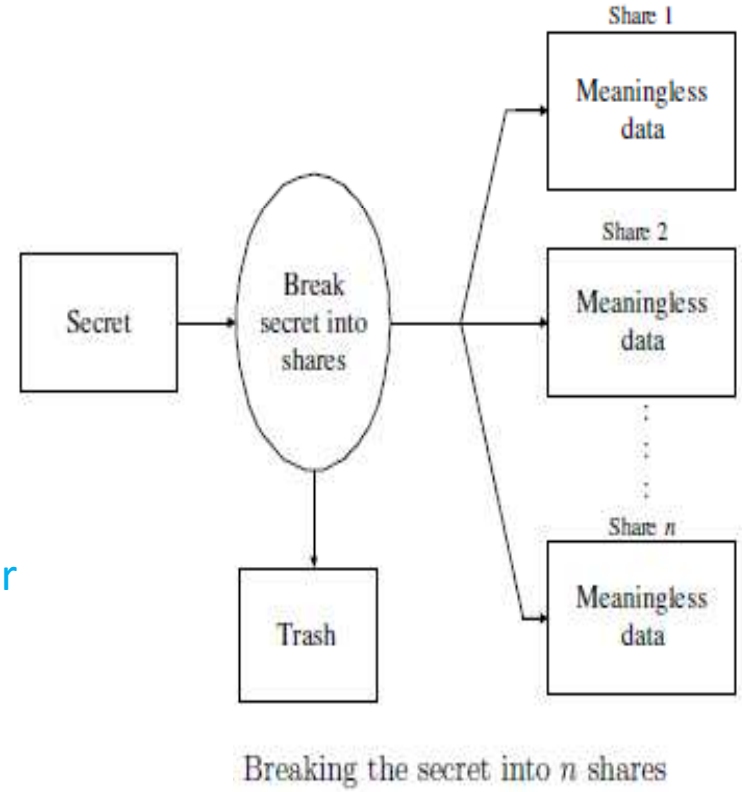
Finding a Cryptosystem

- Review of (k, n) SSS

Sharing a Secret

$$F(x) = \left(S + \sum_{i=1}^{k-1} a_i x^i\right) mod\ q$$

Secret — Random Number — Prime Number



Breaking the secret into n shares

Finding a Cryptosystem

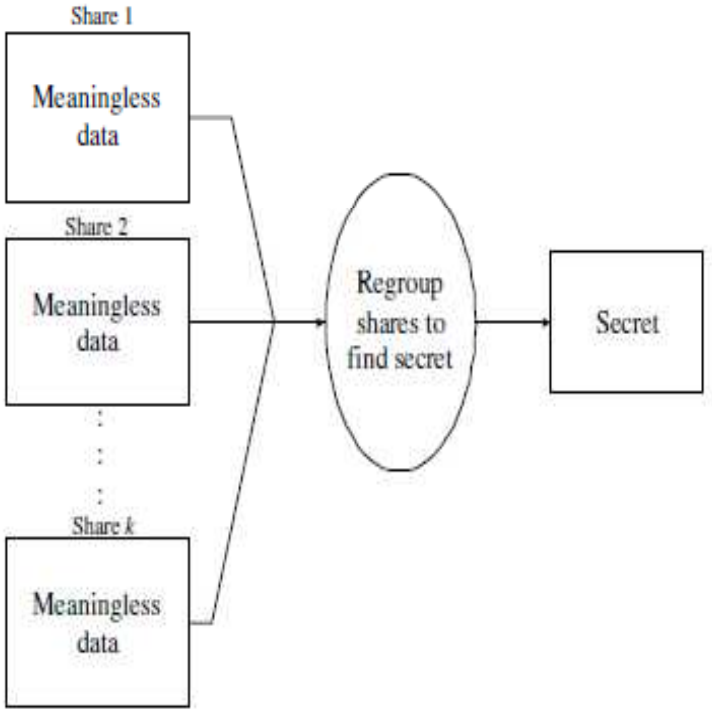
- Review of (k, n) SSS

Reconstructing a Secret

$$L(x) = \left(\sum_{i=0}^{k-1} F(i)\, t_i(x)\right) mod\ q$$

$F(i)$: i^{th} Share

$t_i(x)$: $\prod_{j=0, j\neq i}^{k-1} \frac{x - x_j}{x_i - x_j}$



Reconstructing the secret using $k \leq n$ shares

Finding a Cryptosystem

- Review of (*l*, *k*, *n*) MSS

Sharing a Secret

$$F(x) = \left(\sum_{i=0}^{l-1} s_i x^i + \sum_{i=l}^{k-1} a_i x^i\right) mod\ q$$

s_i : i^{th} Secret

Rest of the talk

- Introduction
- Addressing the Challenges
  - Finding a Cryptosystem
  - **Using Real Numbers in a Cryptosystem**
- Three Frameworks
  - Secure Cloud-based Image Scaling/Cropping
  - Secure Cloud-based Pre-classification Volume Ray-casting
  - Secure Cloud-based Surveillance Video Quality Enhancement
- Conclusions

Using Real Numbers in a Cryptosystem

- Excluding Modular Prime Operation from the Cryptosystem
  - Example: Shamir's secret sharing $F(x) = S + \sum_{i=1}^{k-1} a_i x^i$

  - Side Effect: Degradation of Security
    - ✓ For $(2, n)$ Shamir's secret sharing, the probability of finding the secret from $F(x_i)$ is:
      With mod q: $1/q$
      Without mod q: $INT(x_i / F(x_i))$

Using Real Numbers in a Cryptosystem

- Modifying Real number to an Integer
  - $R(S,d) = \text{round}(S,d) \times 10^d$

Integer Representative

Obtained by rounding off S by d decimal places

Using Real Numbers in a Cryptosystem

- Modifying Real number to an Integer
  - $R(S,d) = round(S,d) \times 10^d$

Integer Representative

Obtained by rounding off S by d decimal places

  - Side Effect: Roundoff Error
    - ✓Is bounded by $\pm (5 \times 10^{-(d+1)})$
    - ✓Expands with addition and scalar multiplication

Rest of the talk

- Introduction and Motivation
- Addressing the Challenges
  - Finding a Cryptosystem
  - Using Real Numbers in a Cryptosystem
- **Three Frameworks**
  - **Secure Cloud-based Image Scaling/Cropping**
  - Secure Cloud-based Pre-classification Volume Ray-casting
  - Secure Cloud-based Surveillance Video Enhancement
- Conclusions

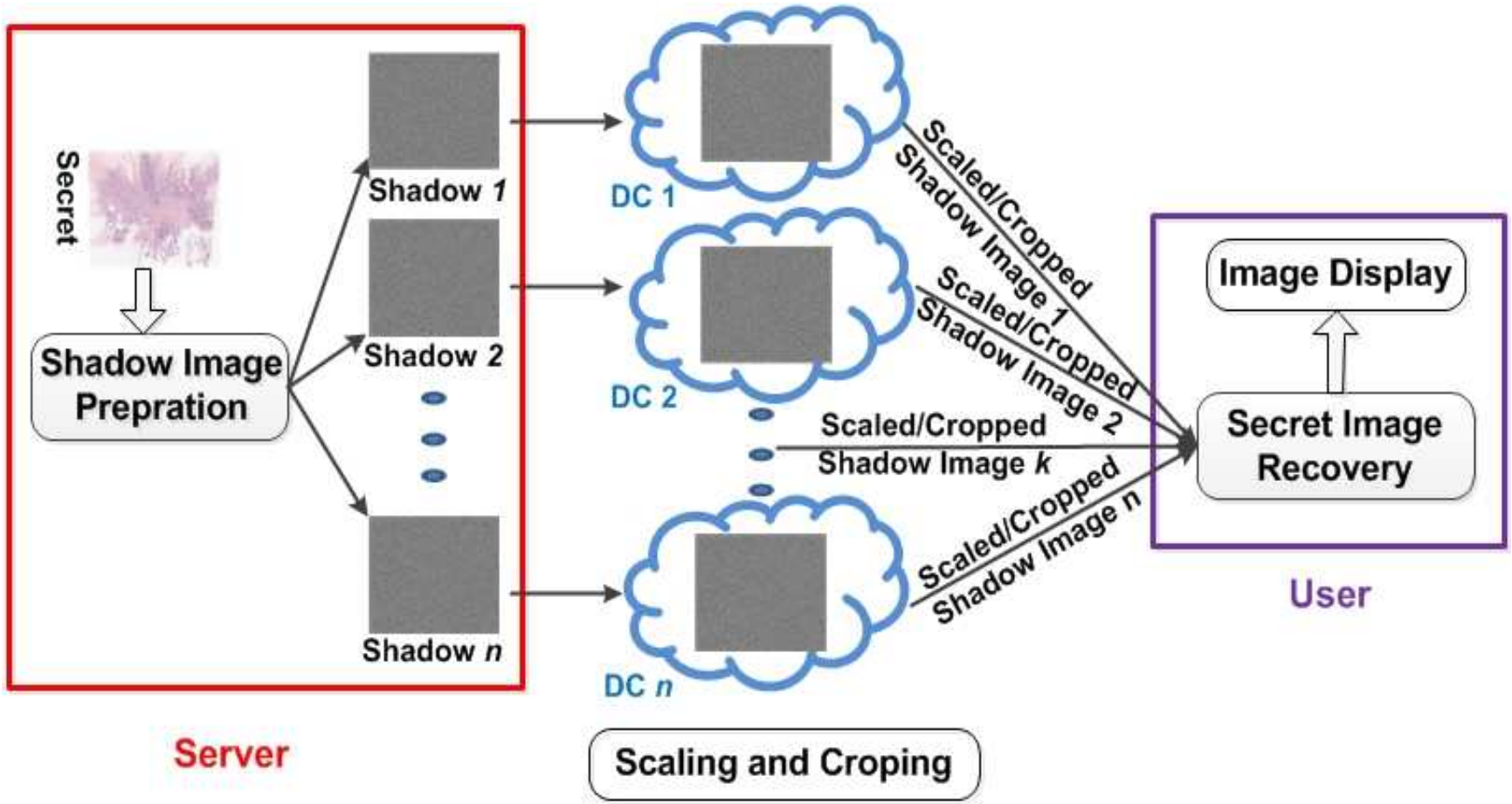
Secure Cloud-based Image Scaling/Cropping

- Why scaling/cropping in data centers?
  - Streaming a large image
    - Downloading a large image (e.g. histopathology image that can be 40 GB in size 80000 × 80000 in dimension) is not feasible
  - Previewing an image before viewing
- Why dynamic scaling/cropping on shadow (or hidden) images?
  - Pre-cropping required additional data to be sent
  - Pre-scaling cannot ensure step-less zooming

M. Mohanty, W.-T. Ooi and P. K. Atrey. **Scale me, crop me, know me not: Supporting scaling and cropping in secret image sharing**. *IEEE International Conference on Multimedia and Expo (ICME'2013)*, July 15-19, 2013, San Jose, CA, USA.

Secure Cloud-based Image Scaling/Cropping

- Architecture and Workflow



Secure Cloud-based Image Scaling/Cropping

- Proposed Secret Image Sharing Scheme
  - Inter-pixel correlation is hidden by using a set of random numbers as coefficient in the secret sharing polynomial
  - (3,*k*,*n*) MSS

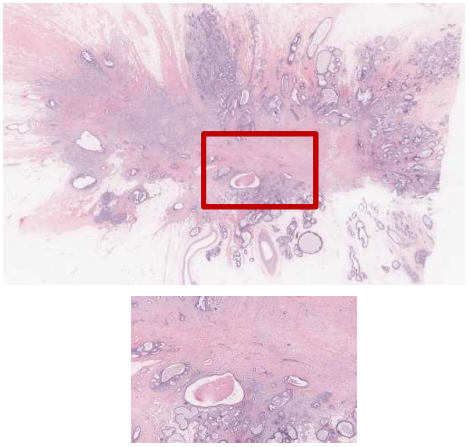
$$H(x) = \left(R + Gx + Bx^2 + \sum_{i=3}^{k-1} a_i x^i \right) \bmod q$$

Secure Cloud-based Image Scaling/Cropping

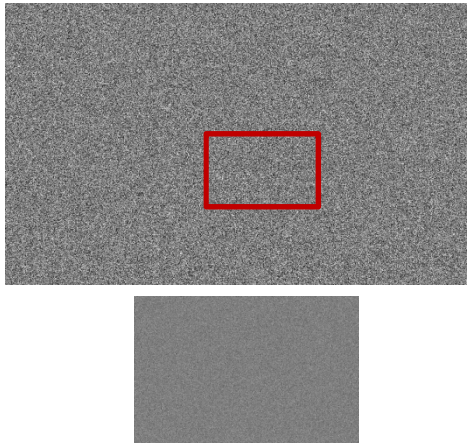
- Experiments
  - Server, datacenters, and user are simulated in a PC
  - Two test images
    - ✓A histopathology image (size 5.2 MB, dimension: 2756 × 3663)
    - ✓The *Lena* Image (size 205.5 KB, dimension: 512 × 512)

Secure Cloud-based Image Scaling/Cropping

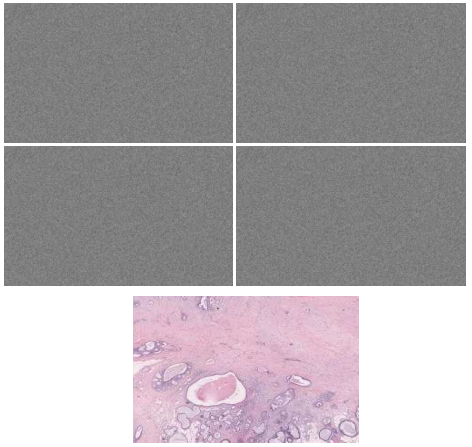
- Results: Scaling



Required



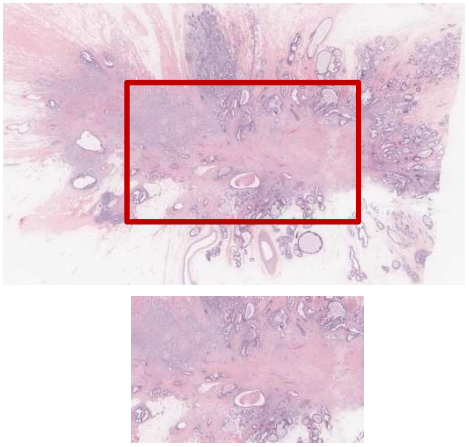
Zoomed Shadow Image



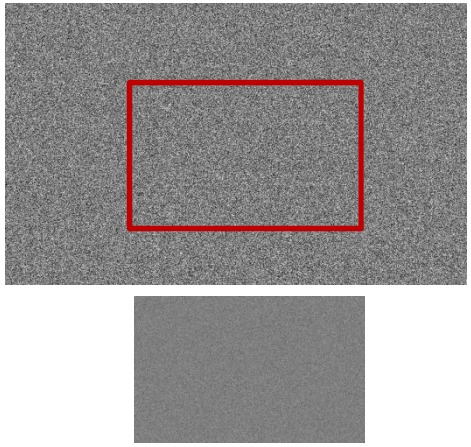
Recovered Zoomed Image

Secure Cloud-based Image Scaling/Cropping

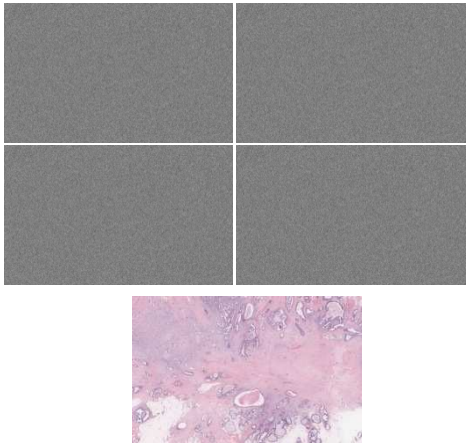
- Results: Cropping



Required



Cropped Shadow Image



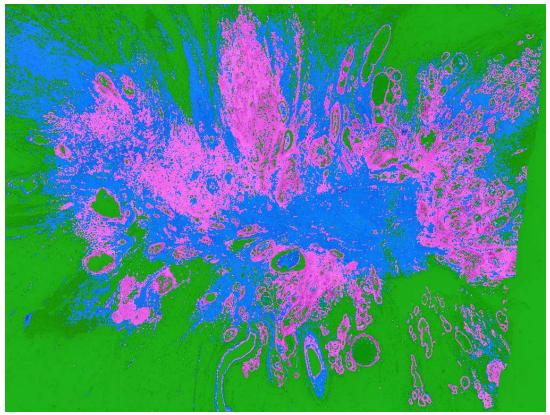
Recovered Cropped Image

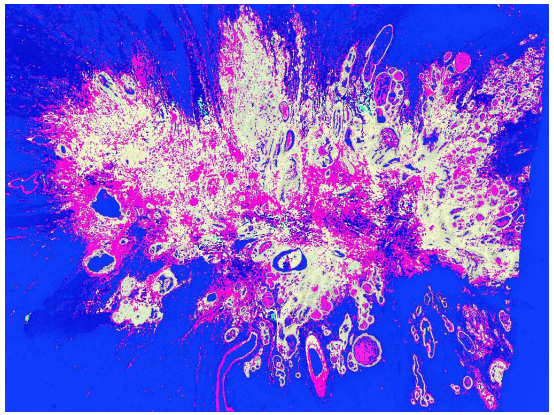
Secure Cloud-based Image Scaling/Cropping

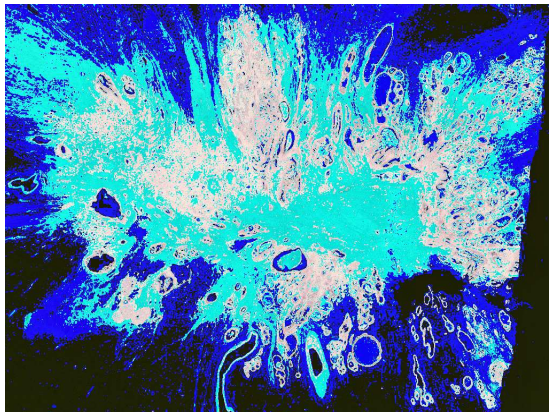
- Security Analysis
  - Confidentiality
    - ✓Perceptual security
    - ✓Multi-secret sharing is not perfectly secure

Secure Cloud-based Image Scaling/Cropping

- Security Analysis
  - Integrity
    - ✓if $n > k$, then ${}^{n}C_{k}$ ways to reconstruct an image







Corrupted shadow image(s) implies different reconstructed images

Secure Cloud-based Image Scaling/Cropping

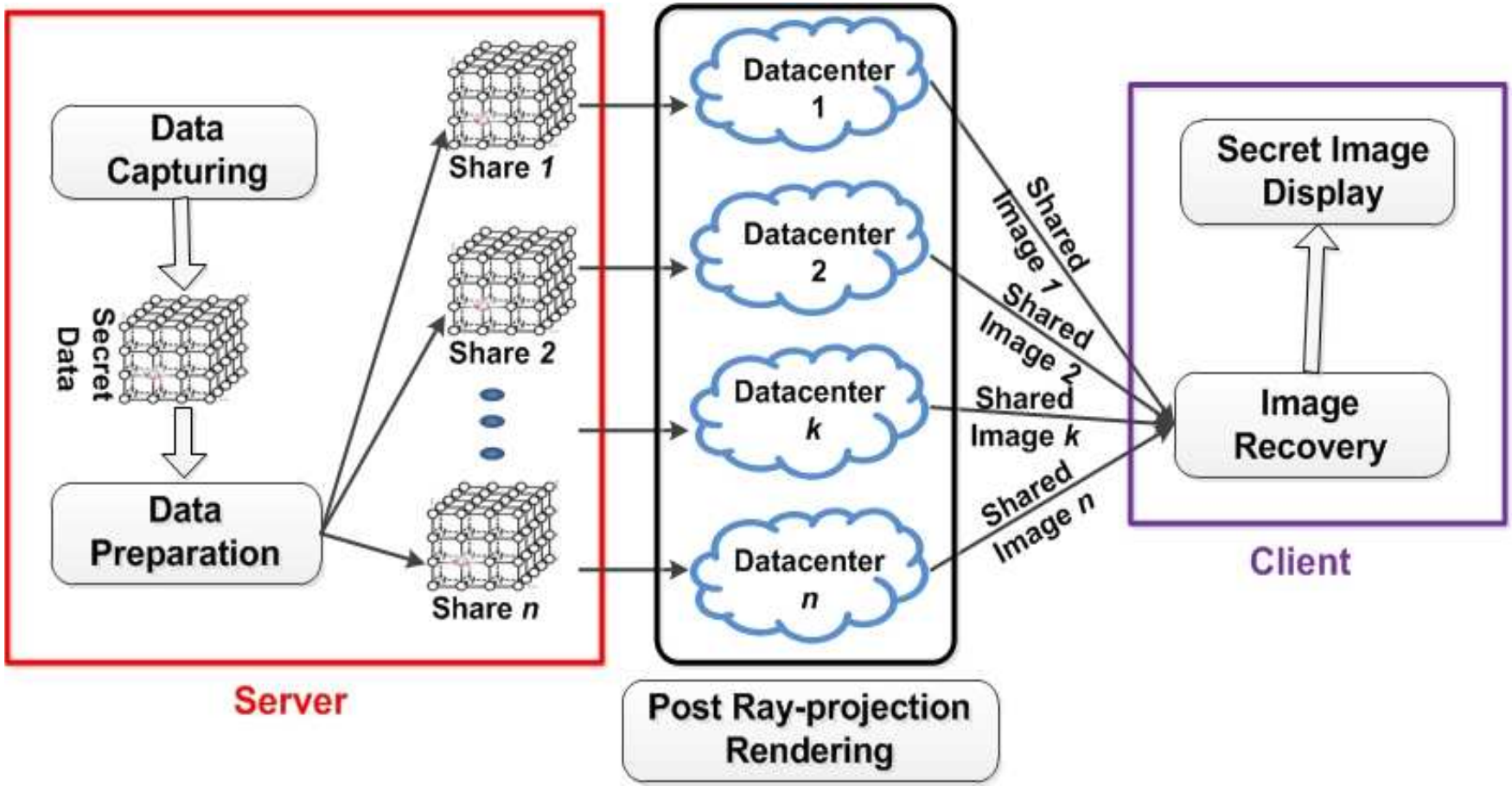
- Performance Analysis
  - Data Overhead
    - ✓ $\frac{bk-24}{24}$ times more than the conventional streaming, where b is the number of bits required to represent q
    - ✓ For $d = 2$ and $k = 4$, 1.5 times more than the conventional
  - Computational Overhead
    - ✓ For a PC with Intel Core 2 Quad 2.83 Ghz processor and 4GB of RAM, approximately 76.35 ms is required to recover a 512 × 512 secret image (0.3 μs per pixel)

Rest of the talk

- Introduction
- Addressing the Challenges
  - Finding a Cryptosystem
  - Using Real Numbers in a Cryptosystem
- Three Frameworks
  - Secure Cloud-based Image Scaling/Cropping
  - **Secure Cloud-based Pre-classification Volume Ray-casting**
  - Secure Cloud-based Surveillance Video Enhancement
- Conclusions

Secure Cloud-based Pre-classification Volume Ray-casting

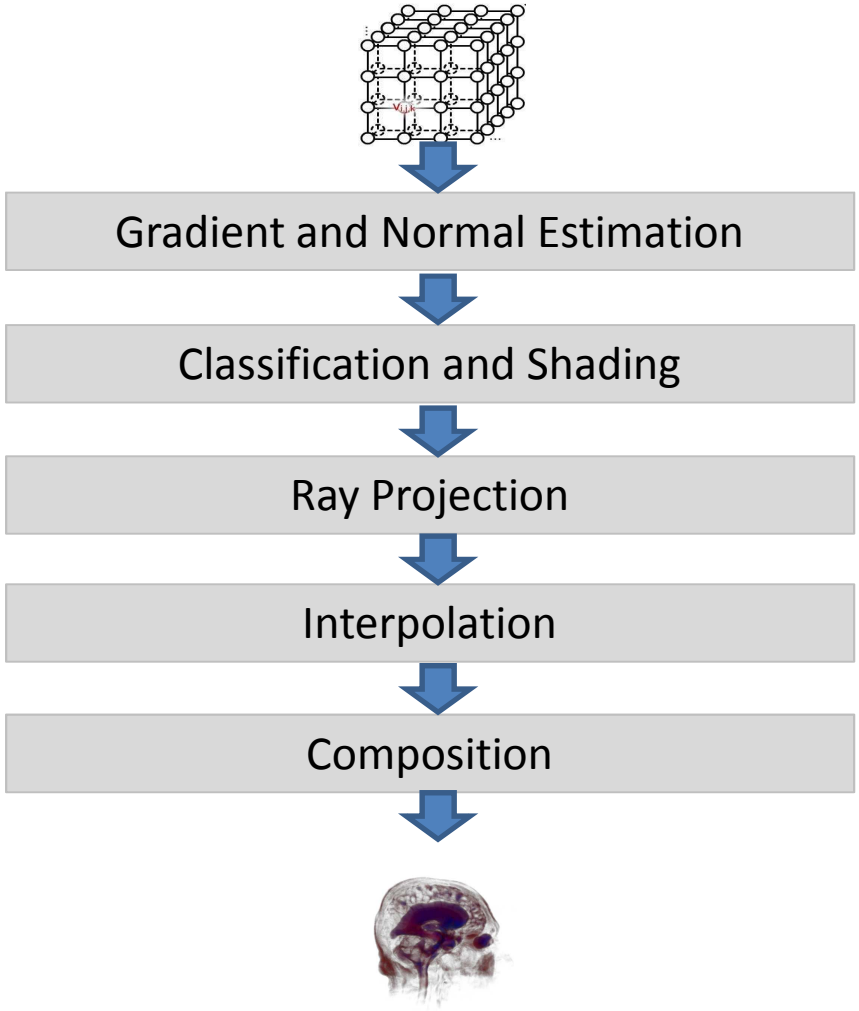
- Architecture and Workflow



M. Mohanty, P. K. Atrey and W.-T. Ooi. **Secure cloud-based medical data visualization**. *The ACM International Conference on Multimedia (ACMMM'12)*, October 29-November 2, 2012, Nara, Japan.

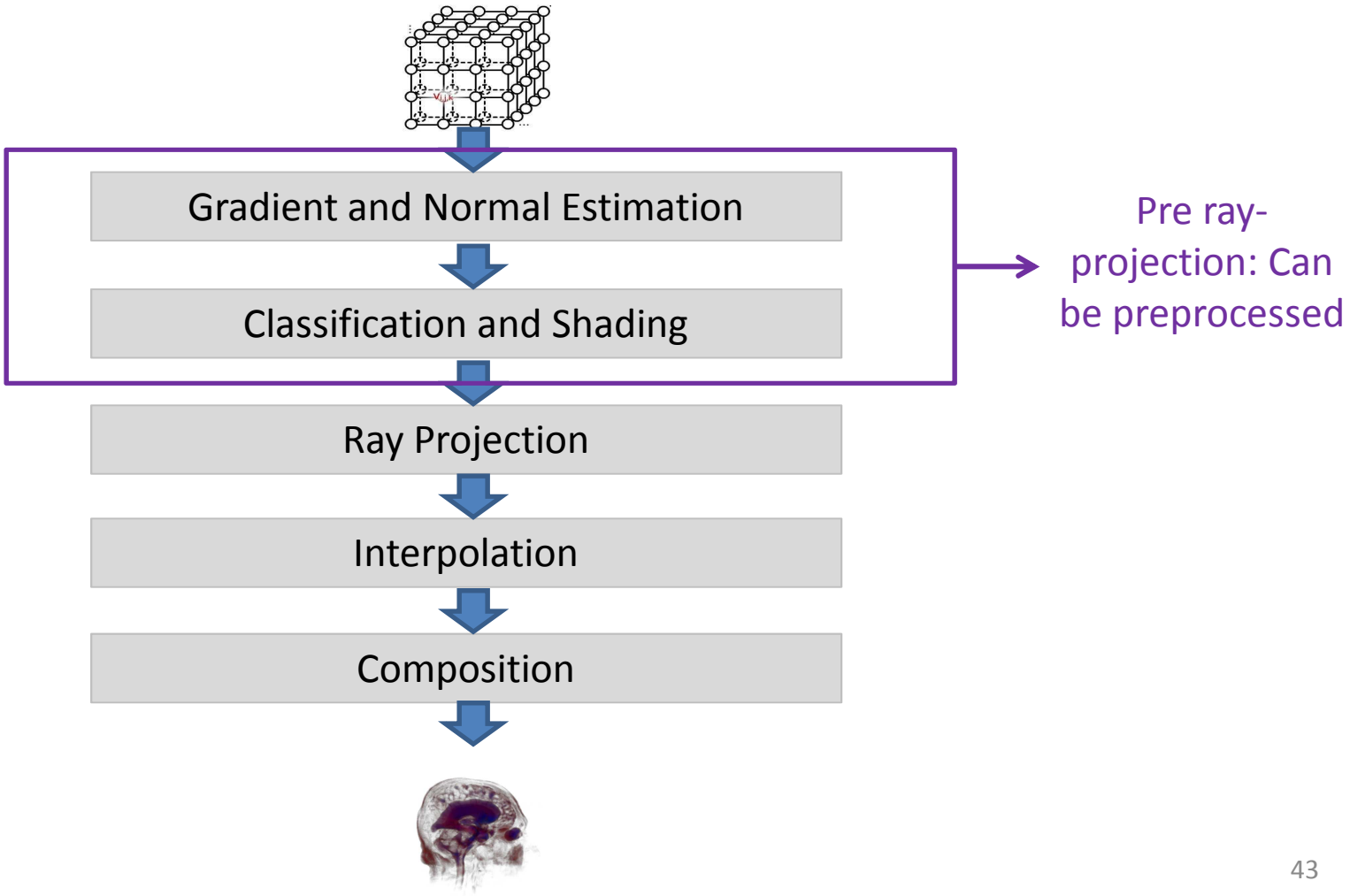
Secure Cloud-based Pre-classification Volume Ray-casting

- Review: Pre-classification Volume Ray-casting



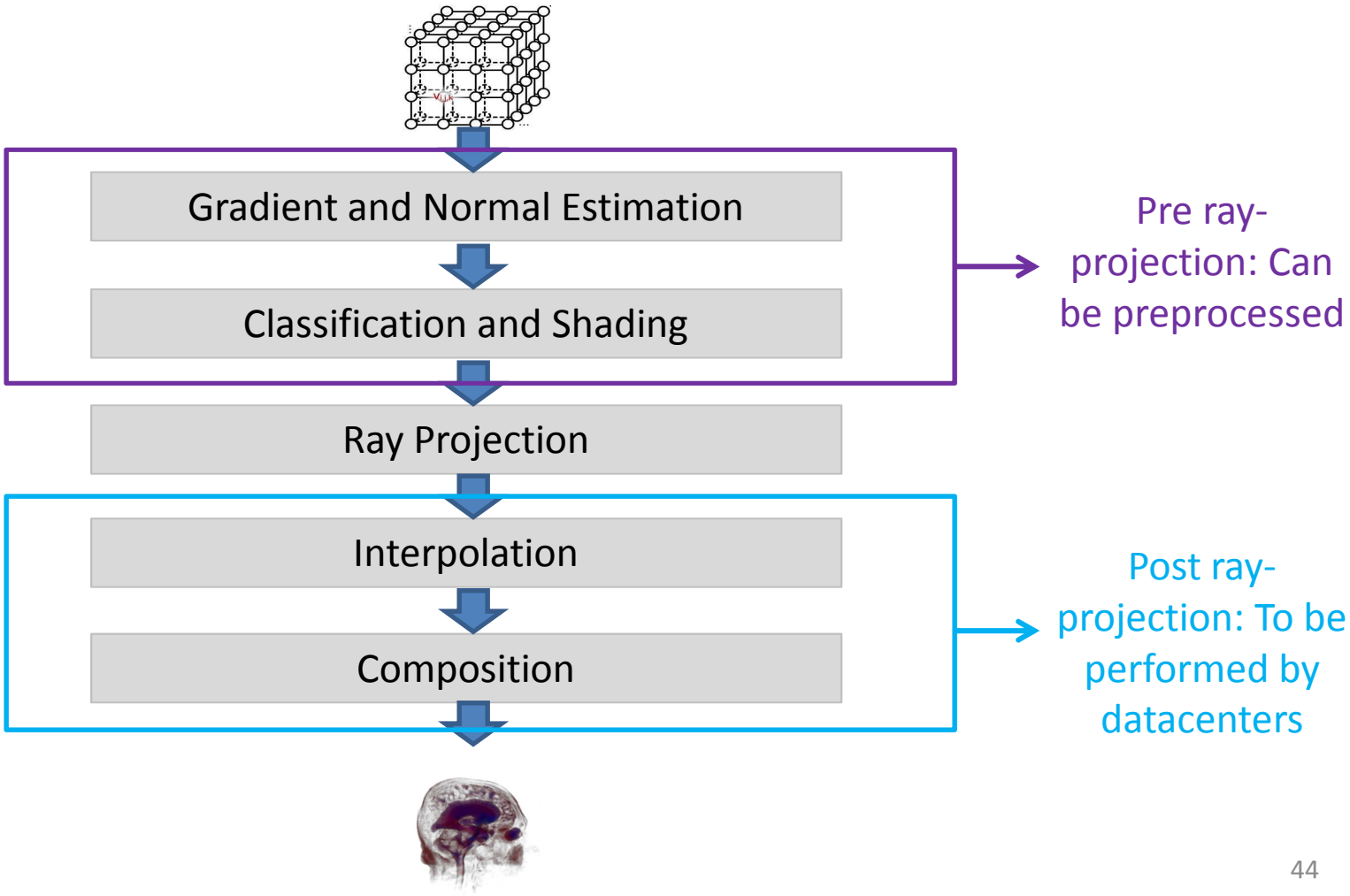
Secure Cloud-based Pre-classification Volume Ray-casting

- Review: Pre-classification Volume Ray-casting



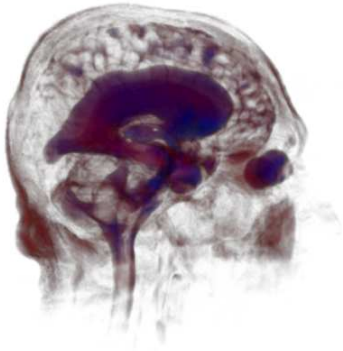
Secure Cloud-based Pre-classification Volume Ray-casting

- Review: Pre-classification Volume Ray-casting

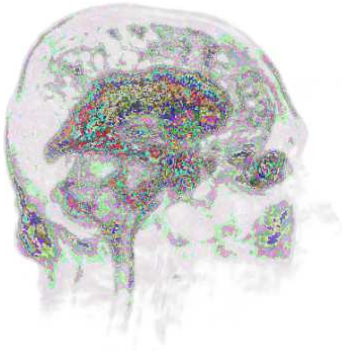


Secure Cloud-based Pre-classification Volume Ray-casting

- Securing Post Ray-projection
  - Hiding computation on colors



Original



Hidden Color

Not hiding computation on opacities

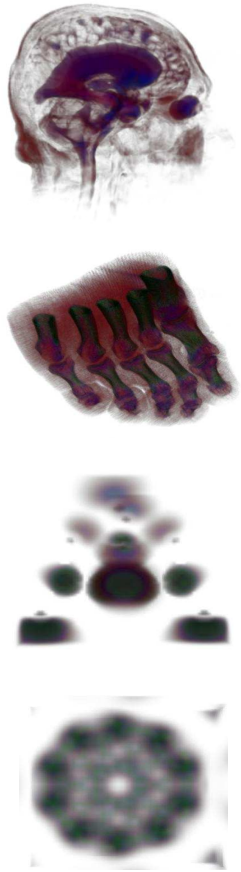
Secure Cloud-based Pre-classification Volume Ray-casting

- 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

Secure Cloud-based Pre-classification Volume Ray-casting

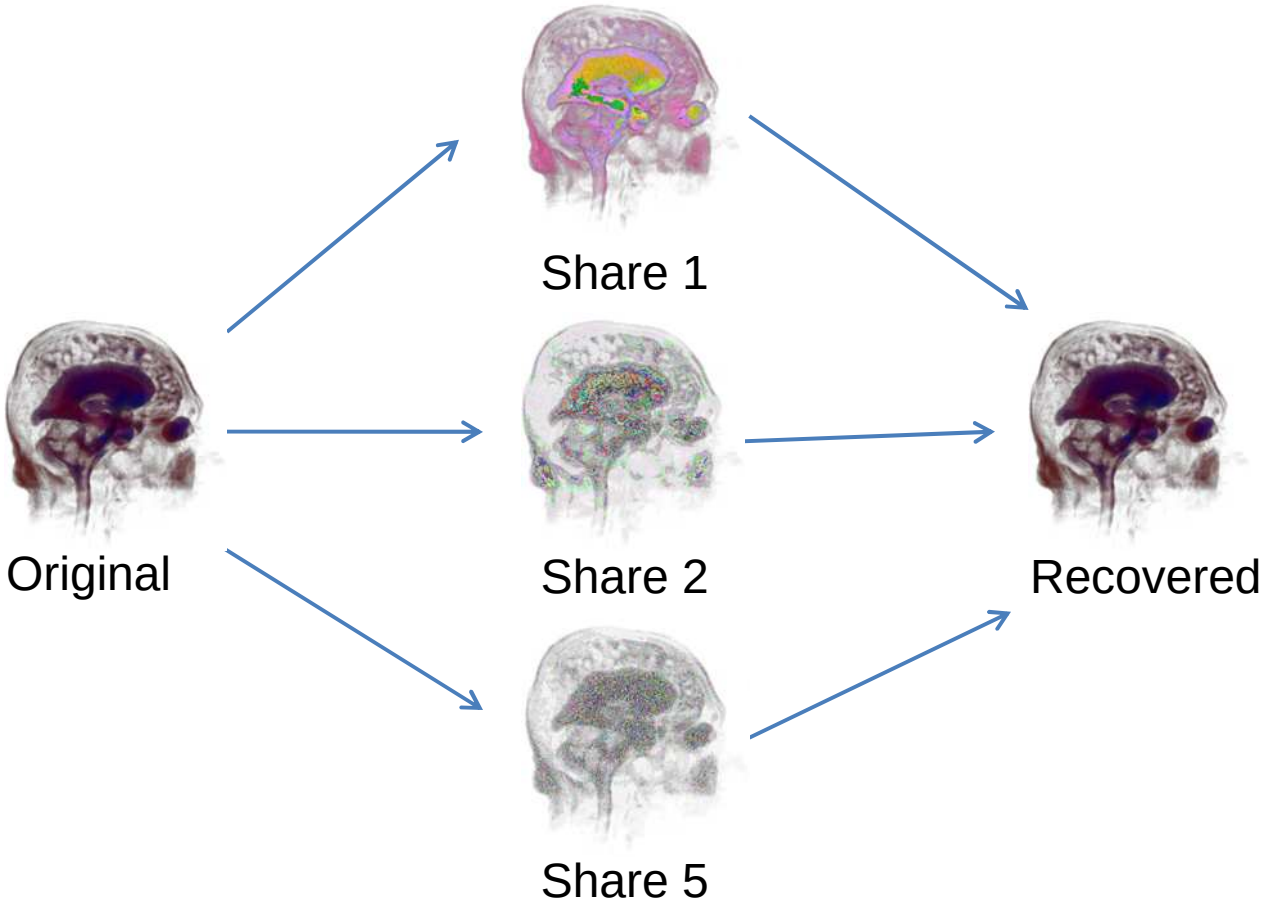
- Data Set

	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



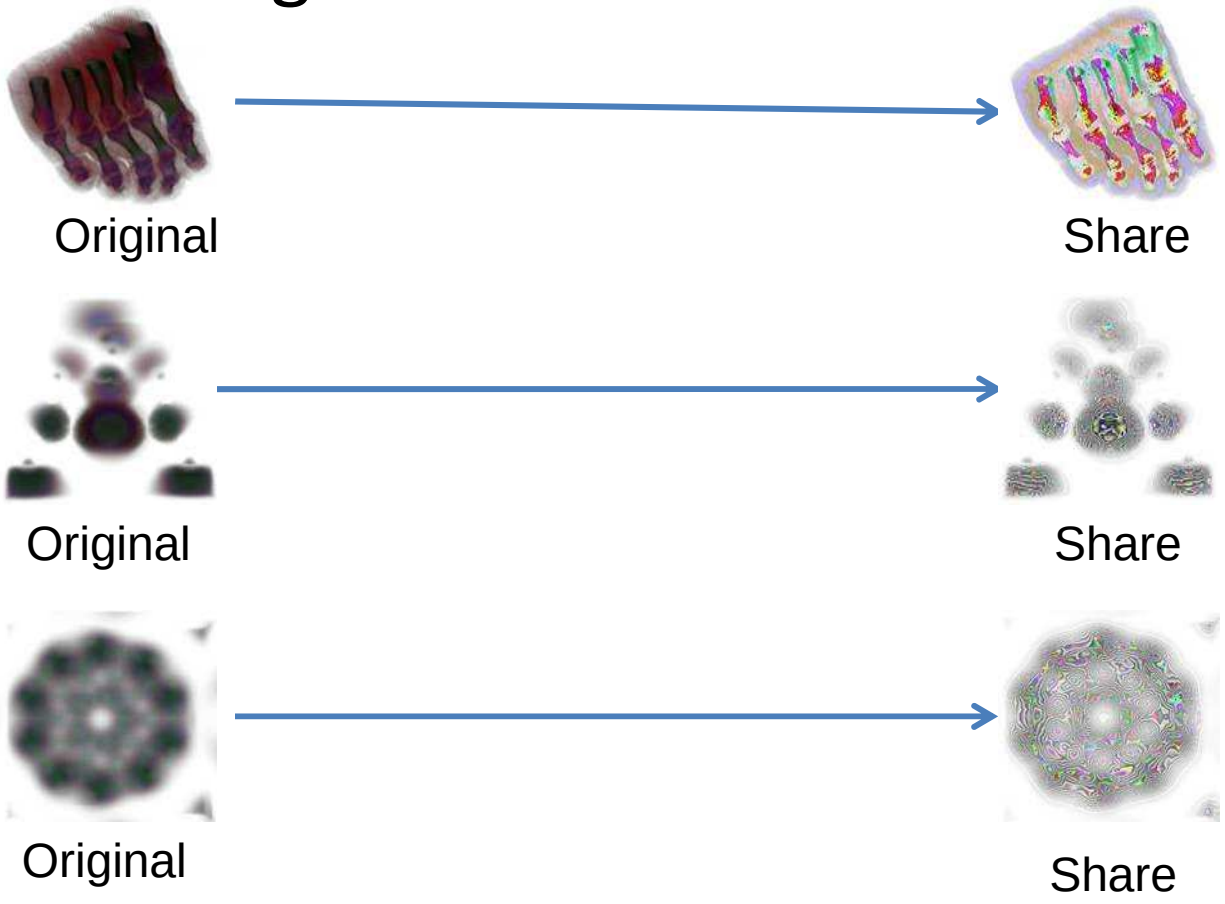
Secure Cloud-based Pre-classification Volume Ray-casting

- Results: Single View Point



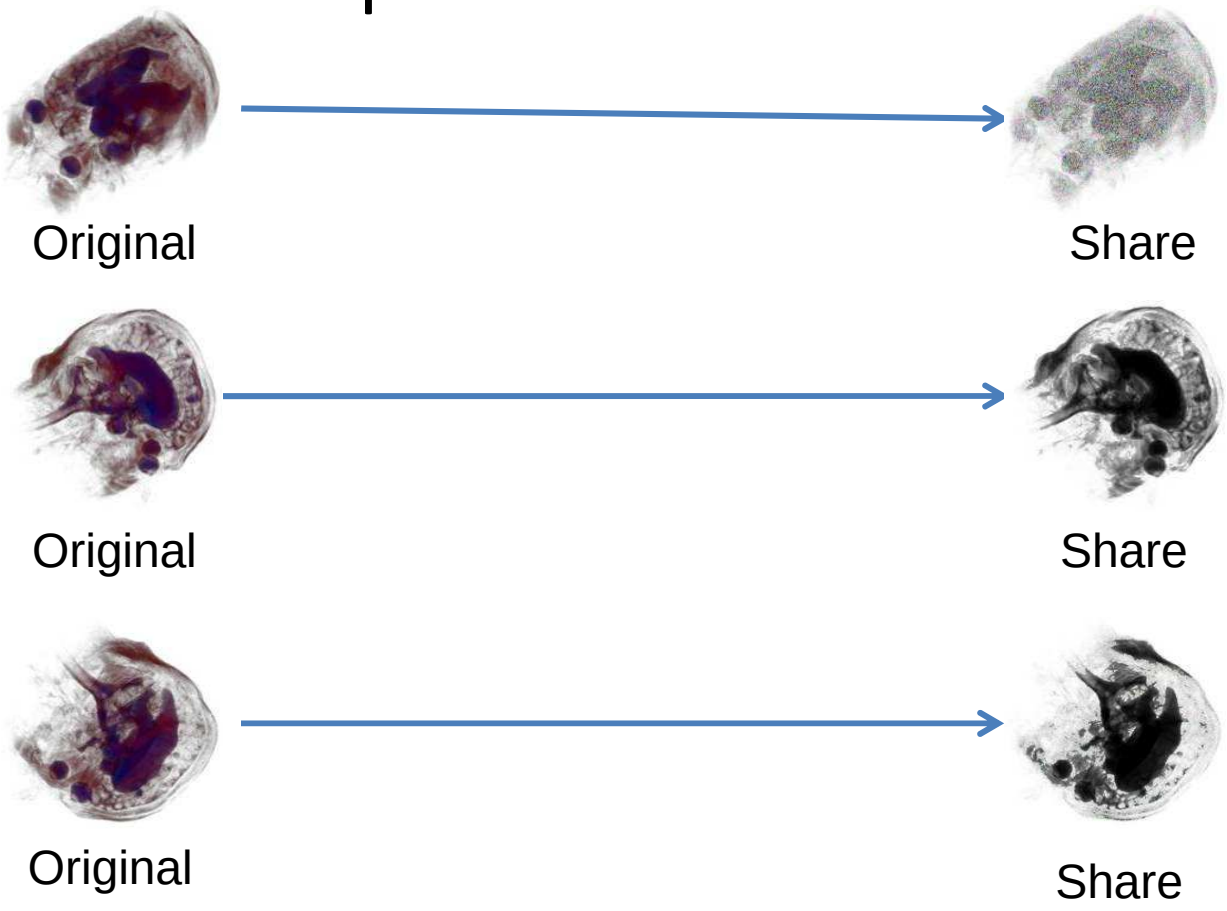
Secure Cloud-based Pre-classification Volume Ray-casting

- Results: Single View Point



Secure Cloud-based Pre-classification Volume Ray-casting

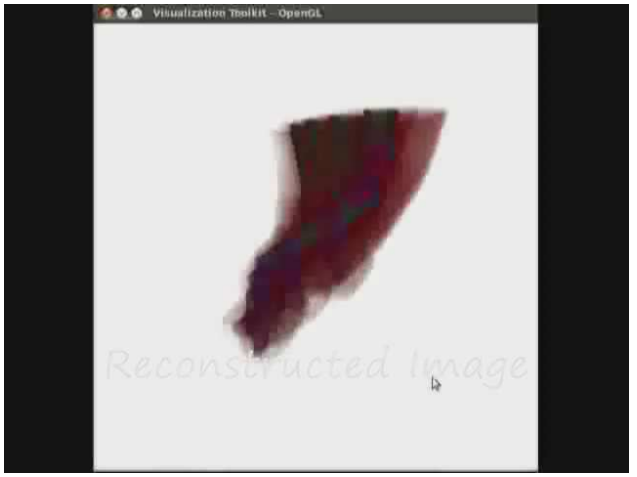
- Results: Multiple View Point



Secure Cloud-based Pre-classification Volume Ray-casting

Head MRI volume data

Foot volume data



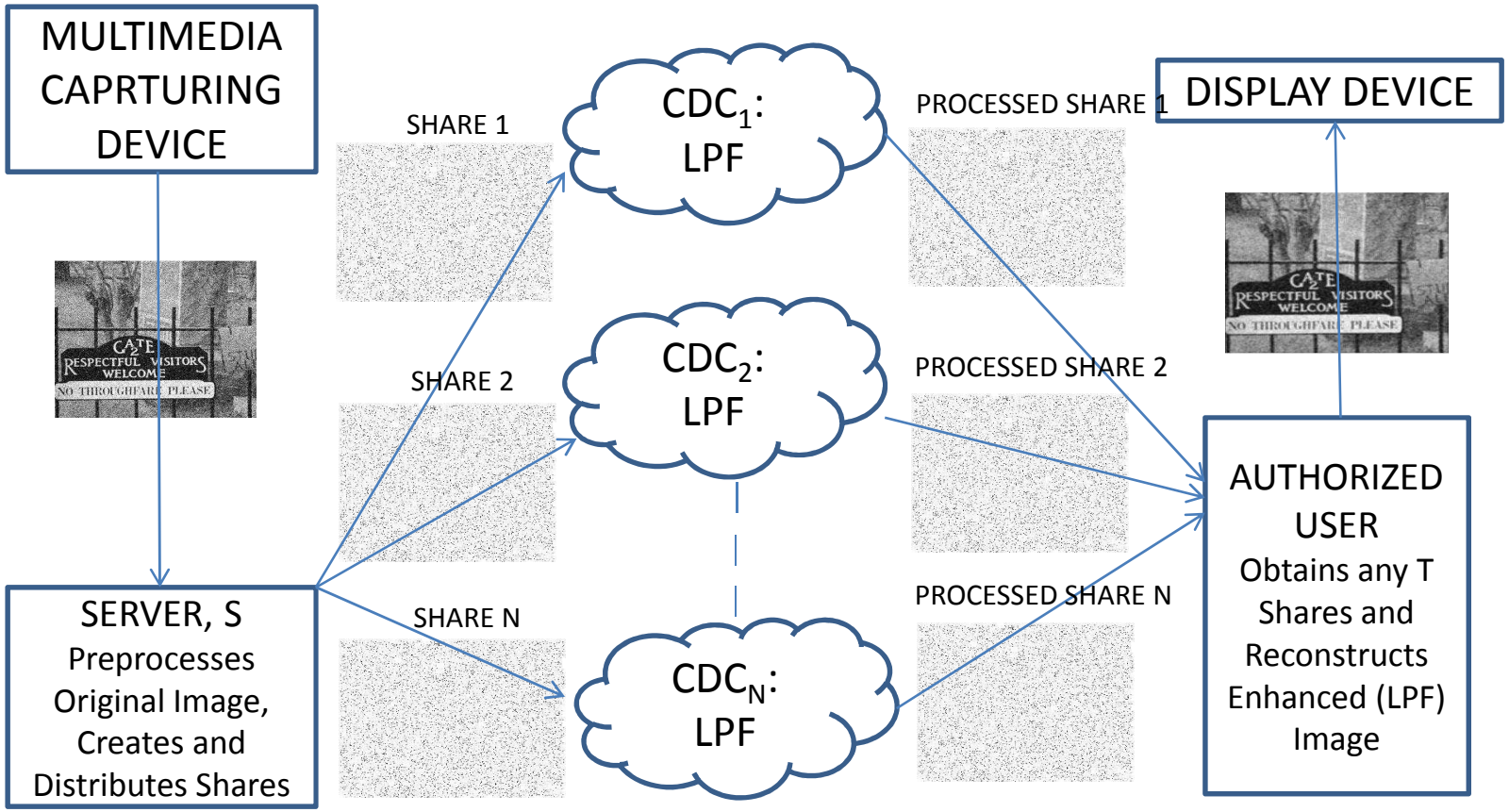
THE UNIVERSITY OF WINNIPEG

Rest of the talk

- Introduction
- Addressing the Challenges
  - Finding a Cryptosystem
  - Using Real Numbers in a Cryptosystem
- Three Frameworks
  - Secure Cloud-based Image Scaling/Cropping
  - Secure Cloud-based Pre-classification Volume Ray-casting
  - **Secure Cloud-based Surveillance Video Quality Enhancement**
- Conclusions

Encrypted-domain Video Quality Enhancement over Cloud

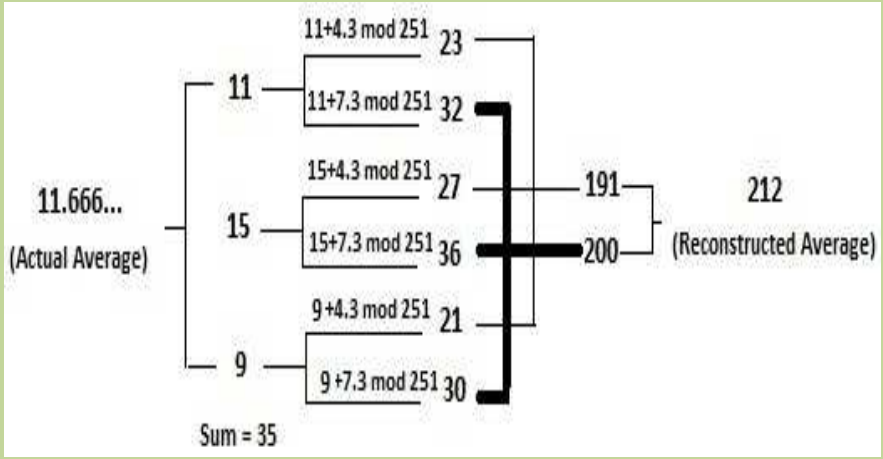
- Architecture and Workflow



A. Lathey, P. K. Atrey and N. Joshi. **Homomorphic low pass filtering on encrypted multimedia over cloud**. *IEEE International Conference on Semantic Computing (ICSC'2013)*, September 2013, Irvine, CA, USA.

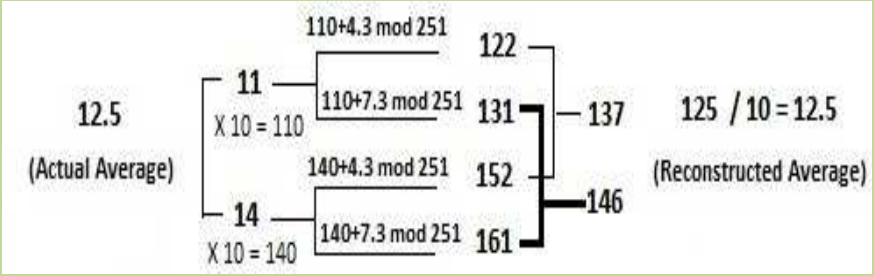
THE PROBLEM:

Non-terminating averaged value

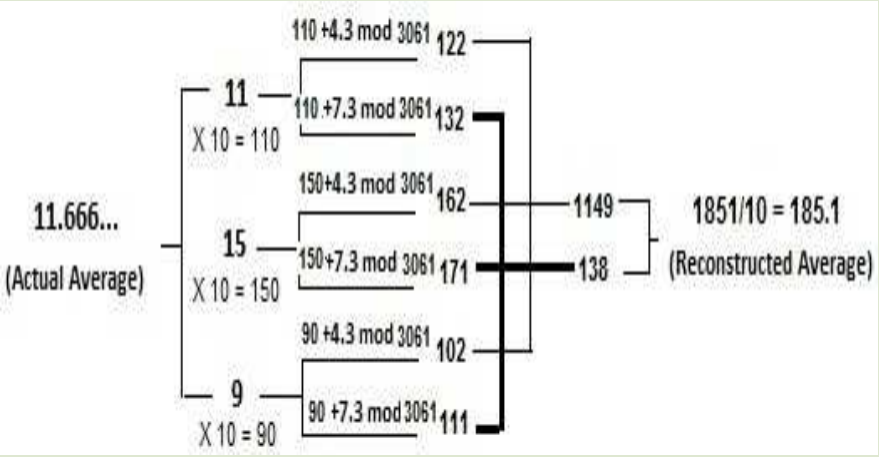


SOLUTION BASED ON PREVIOUS METHOD

Multiply each pixel intensity value by a factor of 10^d, where d depends upon the precision of the desired decimal digits up to which we want to process the real numbers. The prime number should always be chosen as greater than $(255+51\times10^d)\times10^d$

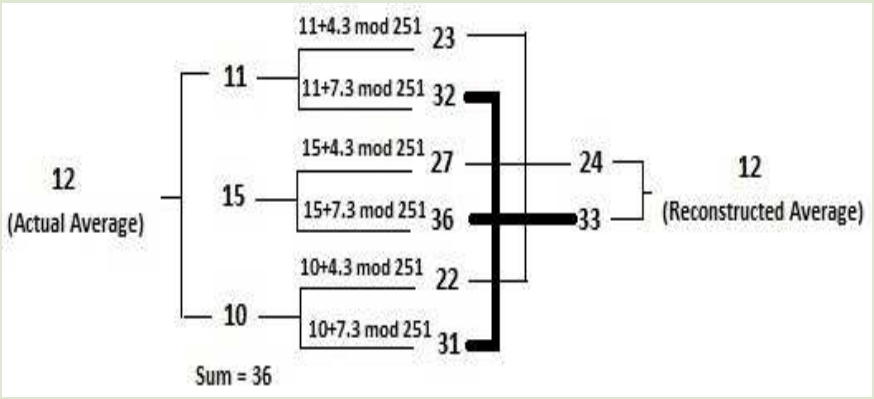


APPLIED TO THE PROBLEM:



PROPOSED SOLUTION:

pre-process the image data in such a way that averaging is performed on completely divisible values only.



Encrypted-domain Video Quality Enhancement over Cloud

Scheme I: Multiplying each original intensity value by the mask size, (*m*×*n*). In other words, convert each pixel *I(u,v)* to a multiple of (*m*×*n*) by,

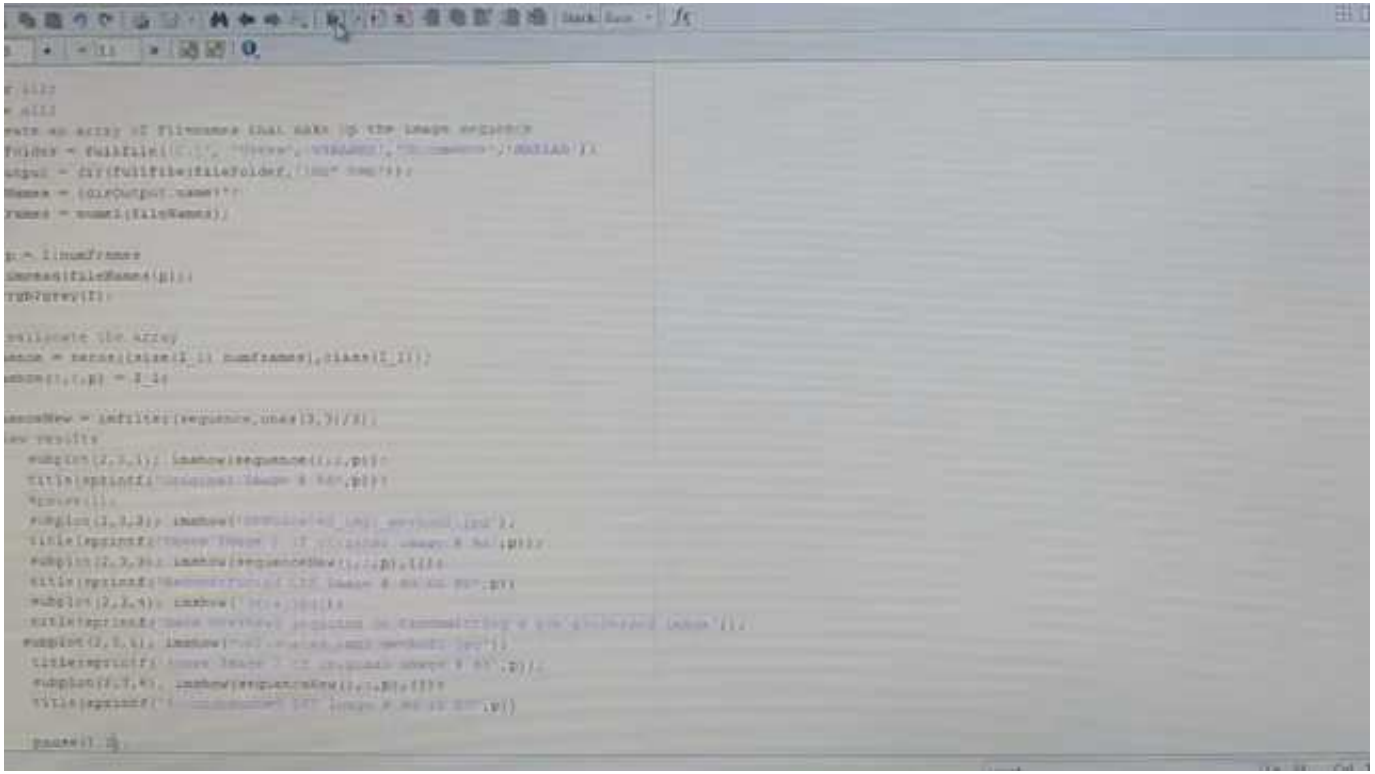
$$I^{'}(u,v) = I(u,v) \times (m \times n)$$

Scheme II: Changing each original intensity value to the nearest multiple of (*m*×*n*) by adding or subtracting a maximum of values to or from its current value, where the range of lies between 1 and Γ m-n/2⍰. In other words, convert each pixel I(u, v) to a multiple of (*m*×*n*) by,

$$I^{'}(u,v) = I(u,v) \pm \Delta$$

Encrypted-domain Video Quality Enhancement over Cloud

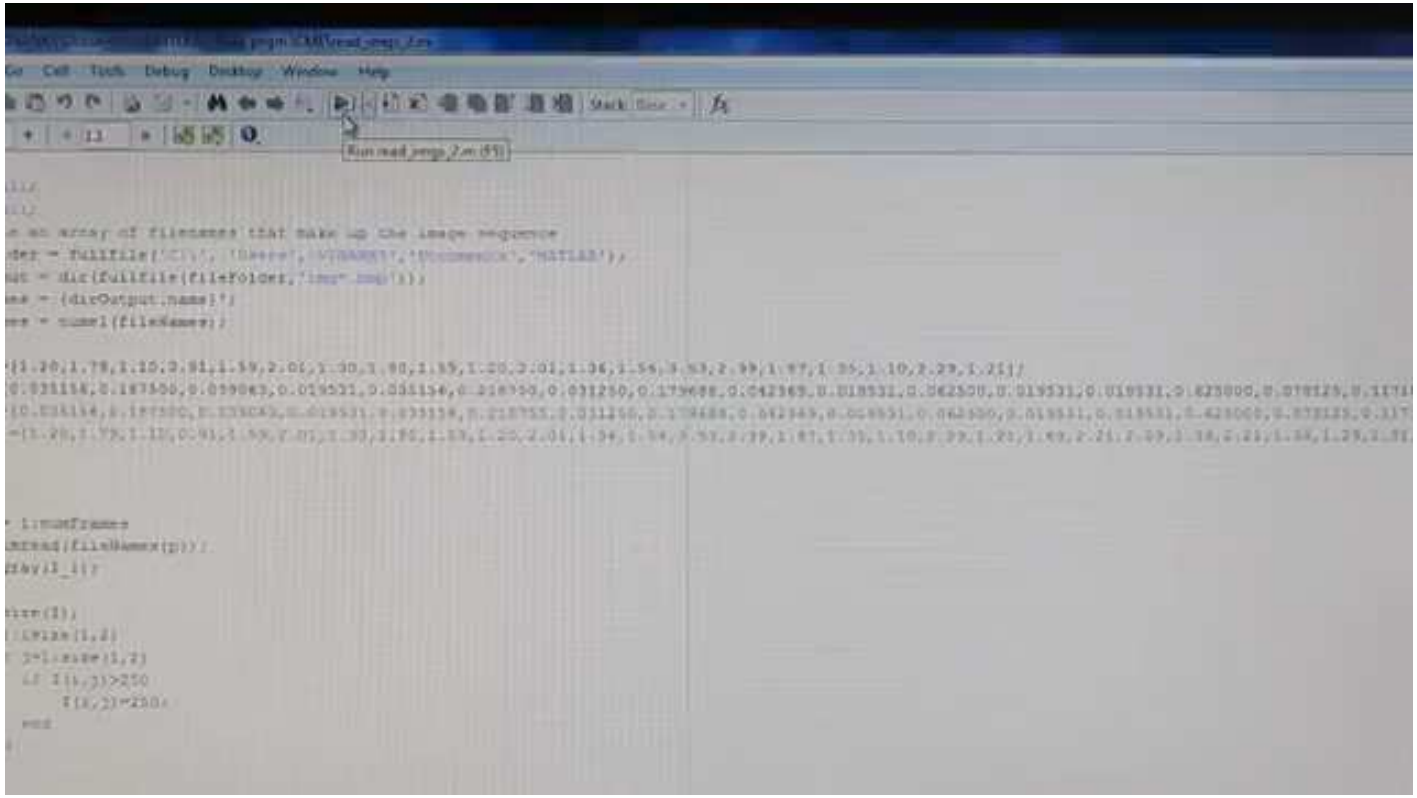
- Results – Scheme 1



http://www.youtube.com/watch?v=hJg67v3IbmU&feature=youtu.be

Encrypted-domain Video Quality Enhancement over Cloud

- Results – Scheme 2



http://www.youtube.com/watch?v=TqRHJ6KrZY0&feature=youtu.be

Conclusions

- Addressed incompatibility of a cryptosystem with real number
- Proposed three frameworks using Shamir's secret sharing as principal cryptosystem
- More secure cloud-based systems can be built using somewhat homomorphic cryptosystems

Publications

- A. Lathey, P. K. Atrey and N. Joshi. **Homomorphic low pass filtering on encrypted multimedia over cloud**. *IEEE International Conference on Semantic Computing (ICSC'2013)*, September 2013, Irvine, CA, USA.

- M. Mohanty, W.-T. Ooi and P. K. Atrey. **Scale me, crop me, know me not: Supporting scaling and cropping in secret image sharing**. *IEEE International Conference on Multimedia and Expo (ICME'2013)*, July 15-19, 2013, San Jose, CA, USA.

- M. Mohanty, P. K. Atrey and W.-T. Ooi. **Secure cloud-based medical data visualization**. *The ACM International Conference on Multimedia (ACMMM'12)*, October 29-November 2, 2012, Nara, Japan.

What Next?

- This is not the end of the world.

- Need to examine the suitability of the proposed frameworks in other cloud-based applications such as:
  - Scaling/cropping on compressed images/videos
  - Compression in encrypted domain
  - Processing other media e.g. text documents and audio