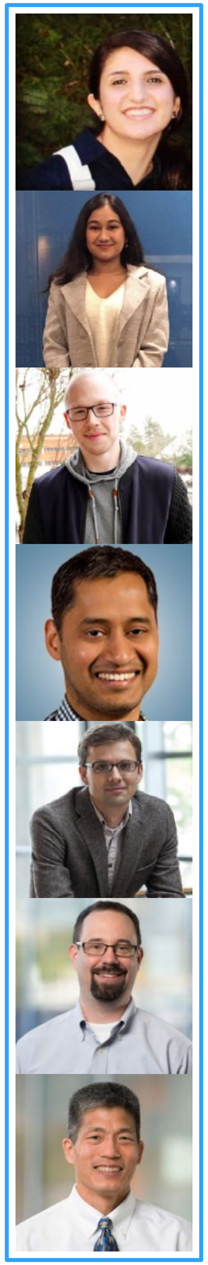
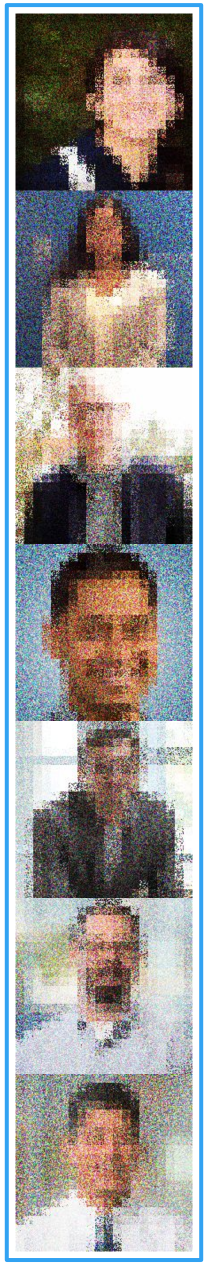


Balancing Image Privacy and Usability with Thumbnail-Preserving Encryption

Kimia Tajik*, Akshith Gunasekaran*, Rhea Dutta†§, Brandon Ellis*, Rakesh Bobba*, Mike Rosulek*, Charles Wright‡, Wu-chi Feng‡

*Oregon State University, †Cornell University, ‡Portland State University



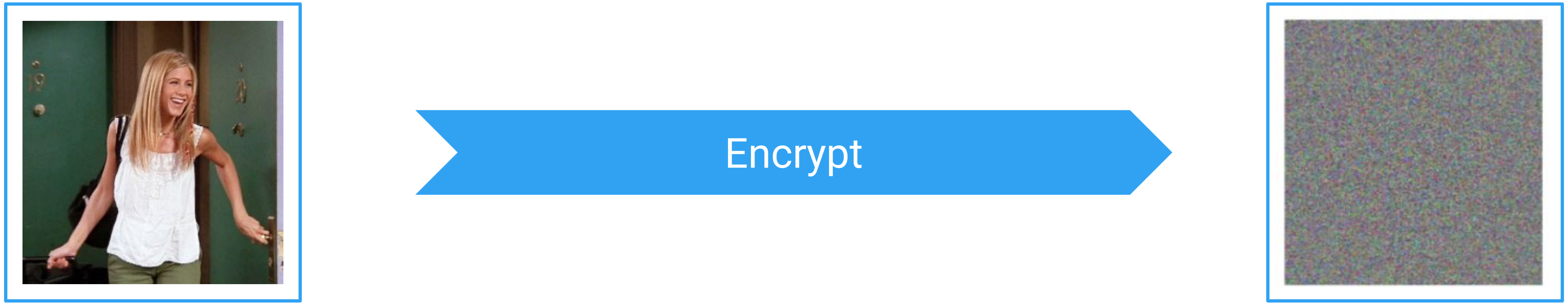
§Rhea Dutta worked on this paper while interning at Oregon State University

Problem Statement

- Ubiquity of cheap high-resolution digital cameras
- Need for online photo storage services
- Exposure to data breaches :(
- We need privacy!

One Solution: Encryption

- Leaks no information (Not usable)

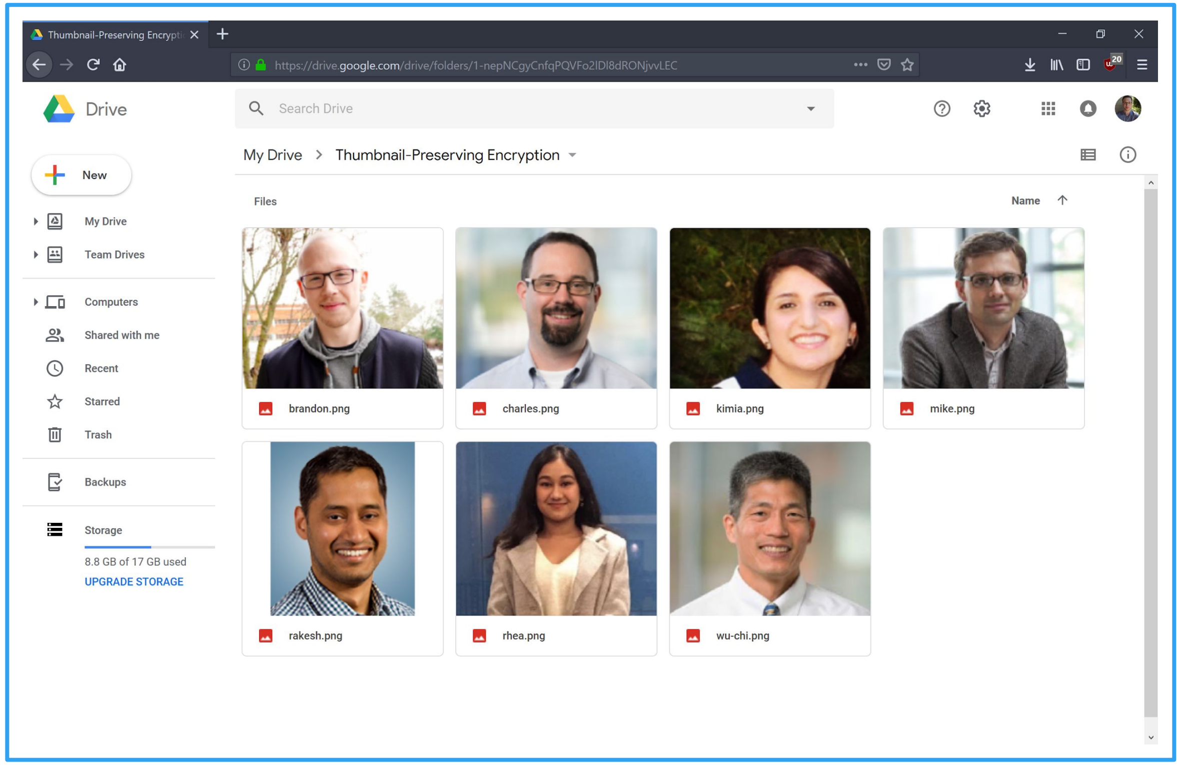


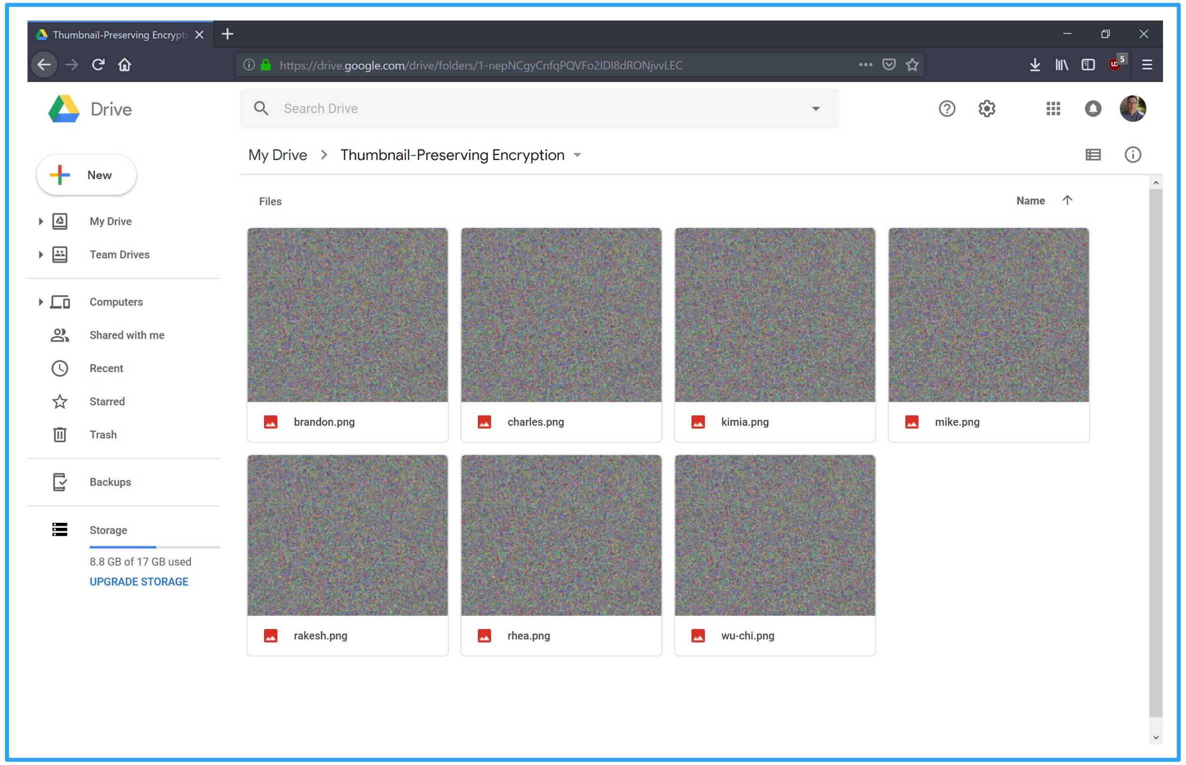
Encrypt

Plaintext

Ciphertext

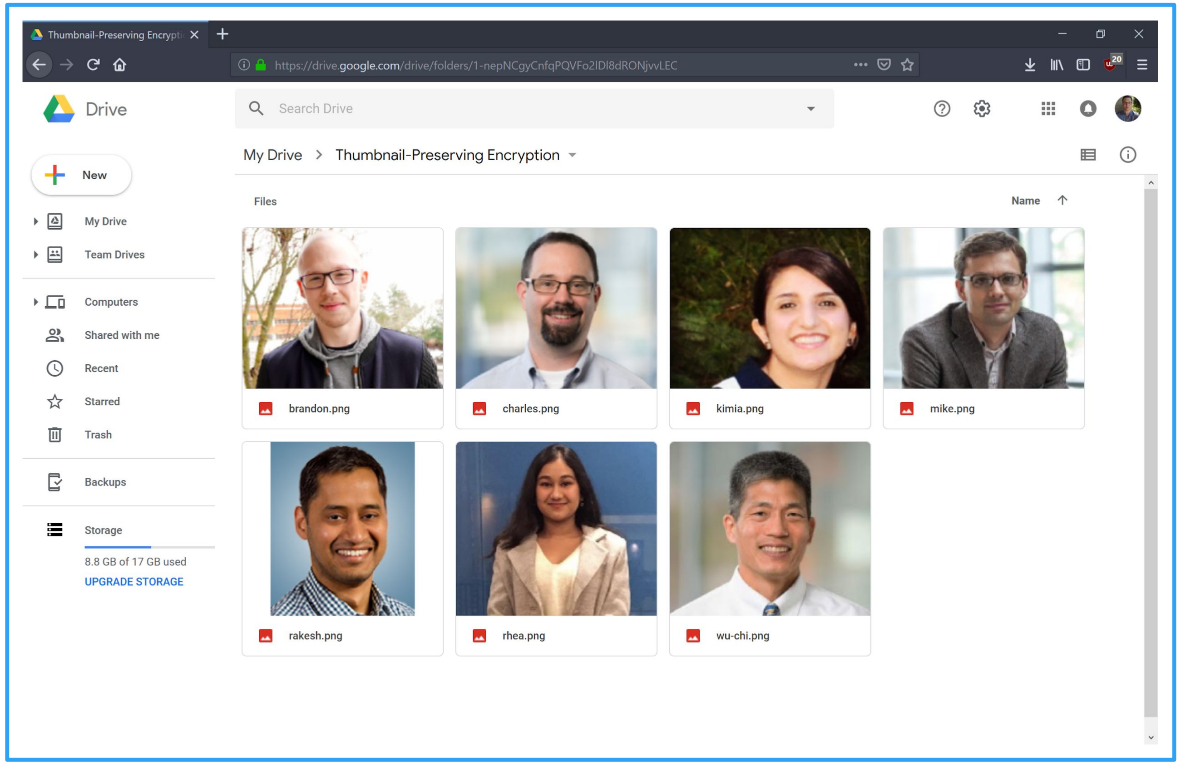
One Solution: Encryption

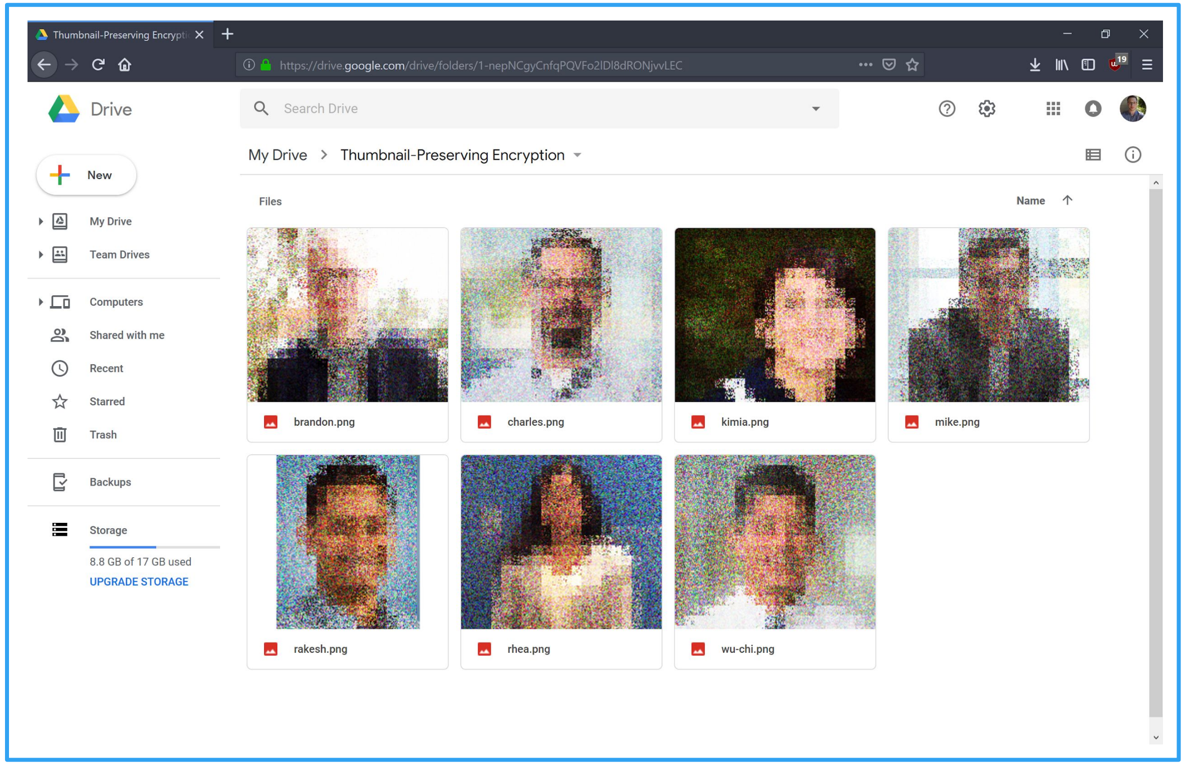




Encryption

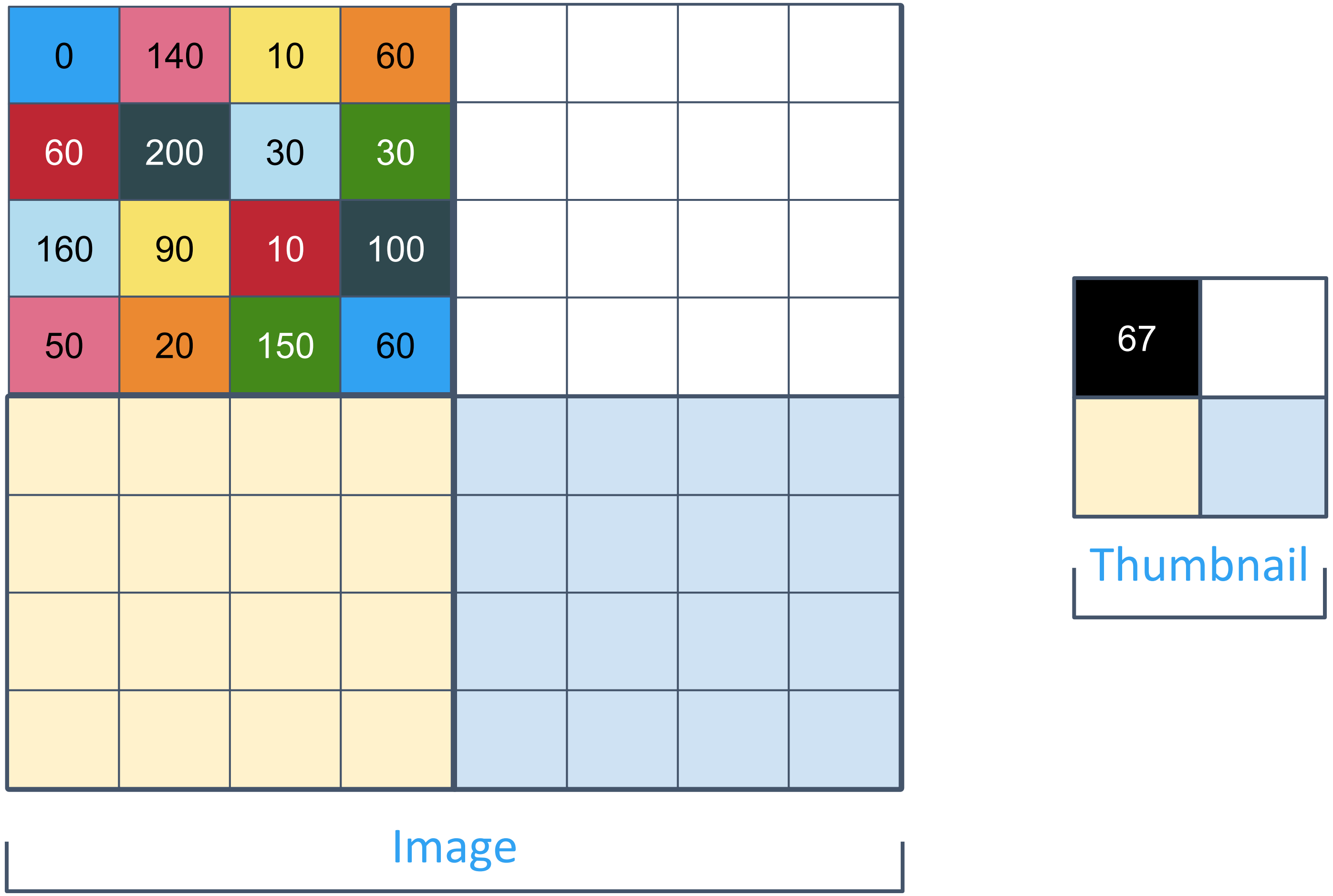
Another Solution: Thumbnail-Preserving Encryption





Thumbnail-Preserving Encryption

What is a Thumbnail?

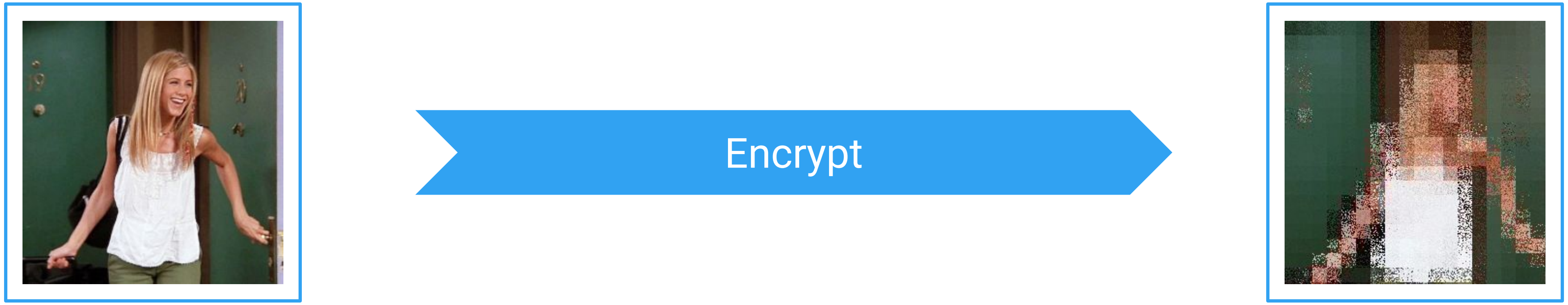


0	140	10	60				
60	200	30	30				
160	90	10	100				
50	20	150	60				

67	

Thumbnail-Preserving Encryption

- Leaks the thumbnail (Thus, more usable)

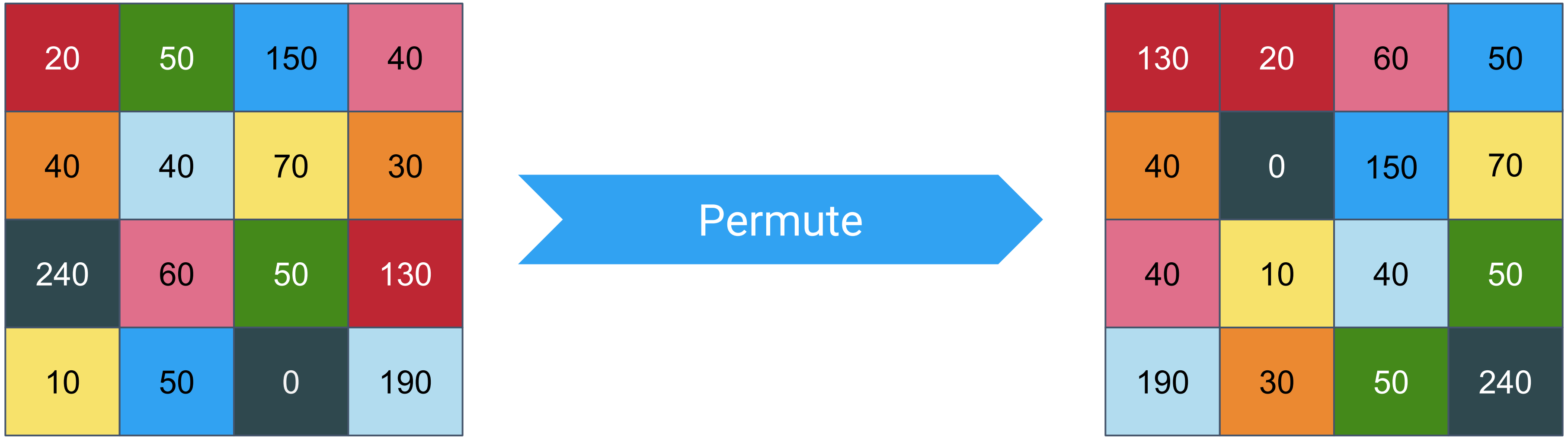


Encrypt

Plaintext

Ciphertext

Previous Thumbnail-Preserving Encryption



20	50	150	40
40	40	70	30
240	60	50	130
10	50	0	190

Permute

130	20	60	50
40	0	150	70
40	10	40	50
190	30	50	240

Leaks the actual values of pixels :(

* Charles V. Wright, Wu-chi Feng, and Feng Liu. Thumbnail-preserving encryption for jpeg. In *Proceedings of the 3rd ACM Workshop on Information Hiding and Multimedia Security*, MMSec '15, pages 141–146, New York, NY, USA, 2015. ACM.

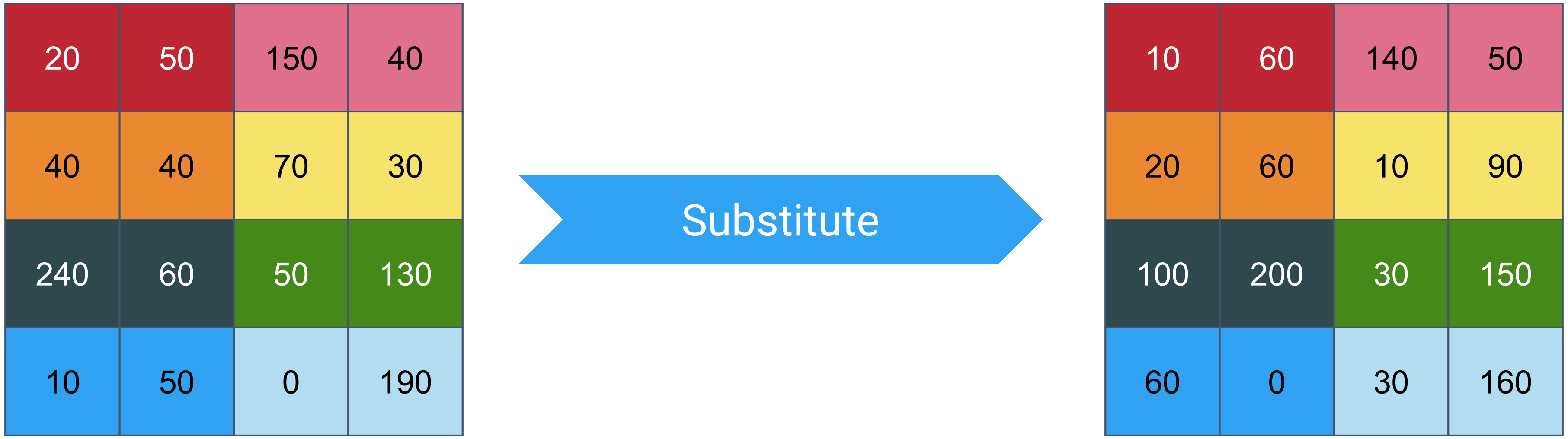
Our Contribution: Ideal Thumbnail-Preserving Encryption

- A new thumbnail-preserving encryption algorithm is proposed, in which the pixel intensities are mixed in a block such that:
  - Their sum is preserved.
  - Nothing else is leaked.
- Security analysis is done to prove the above claim.
- User study is conducted to analyze the trade-off between usability and privacy.

Ideal Thumbnail-Preserving Encryption

- Two-steps:
  - Neighborhood-based substitutions
  - Block-based permutations

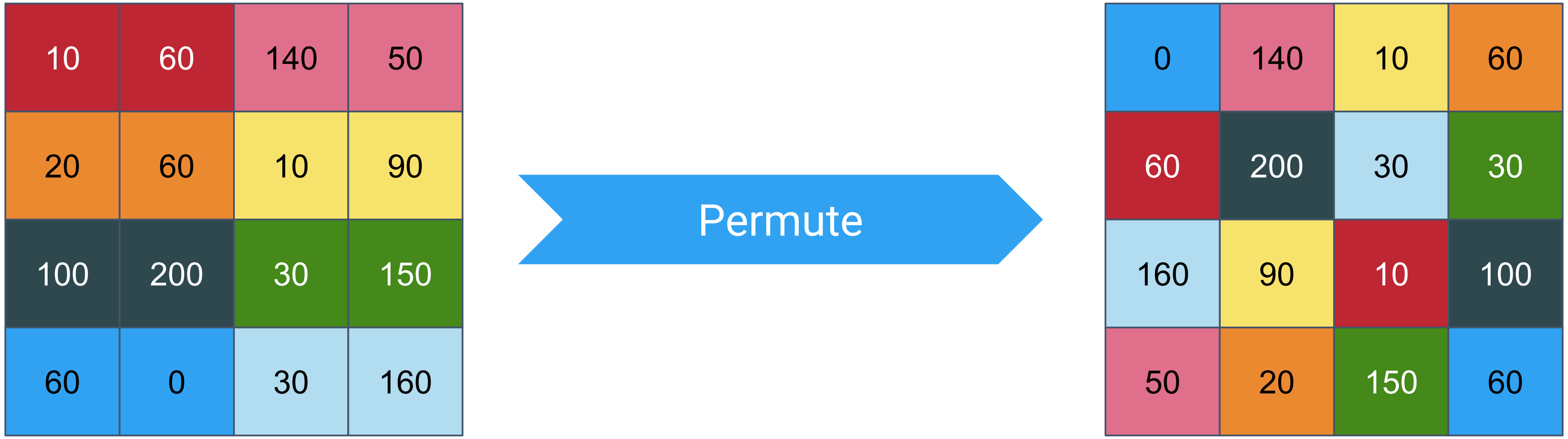
Neighborhood-Based Substitution



20	50	150	40
40	40	70	30
240	60	50	130
10	50	0	190

10	60	140	50
20	60	10	90
100	200	30	150
60	0	30	160

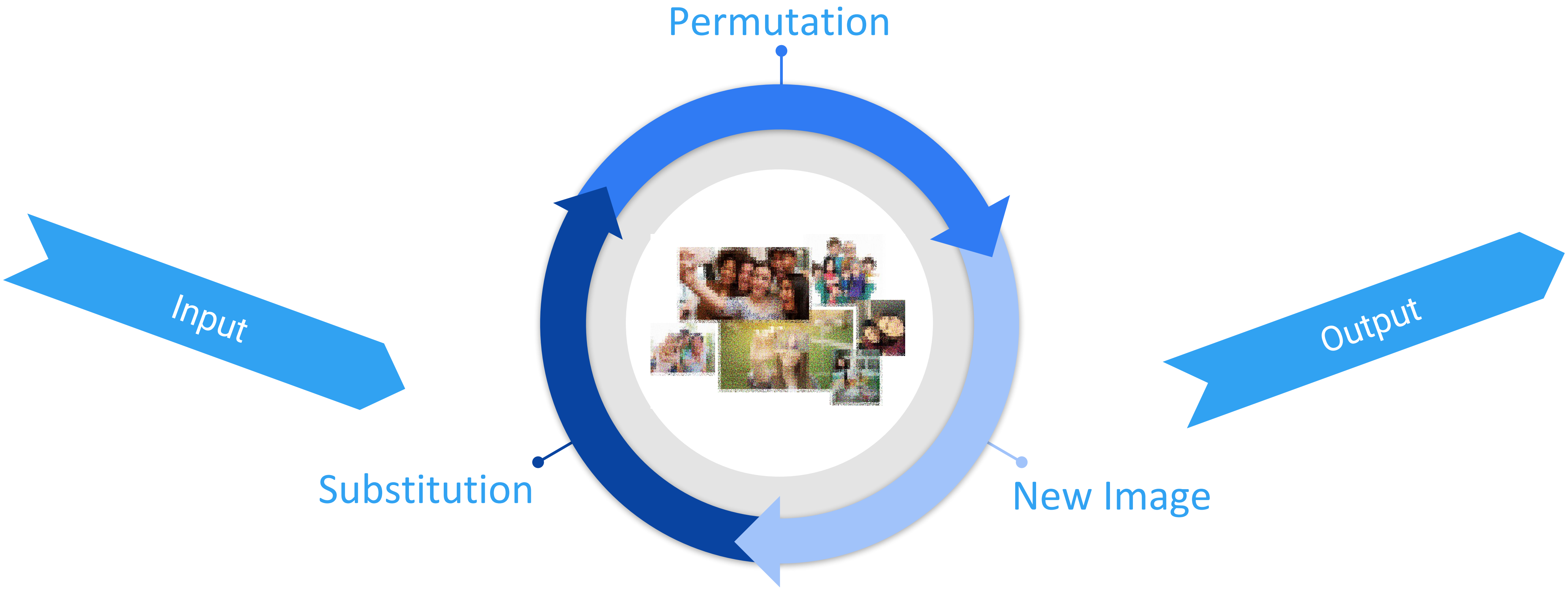
Block-Based Permutation



10	60	140	50
20	60	10	90
100	200	30	150
60	0	30	160

0	140	10	60
60	200	30	30
160	90	10	100
50	20	150	60

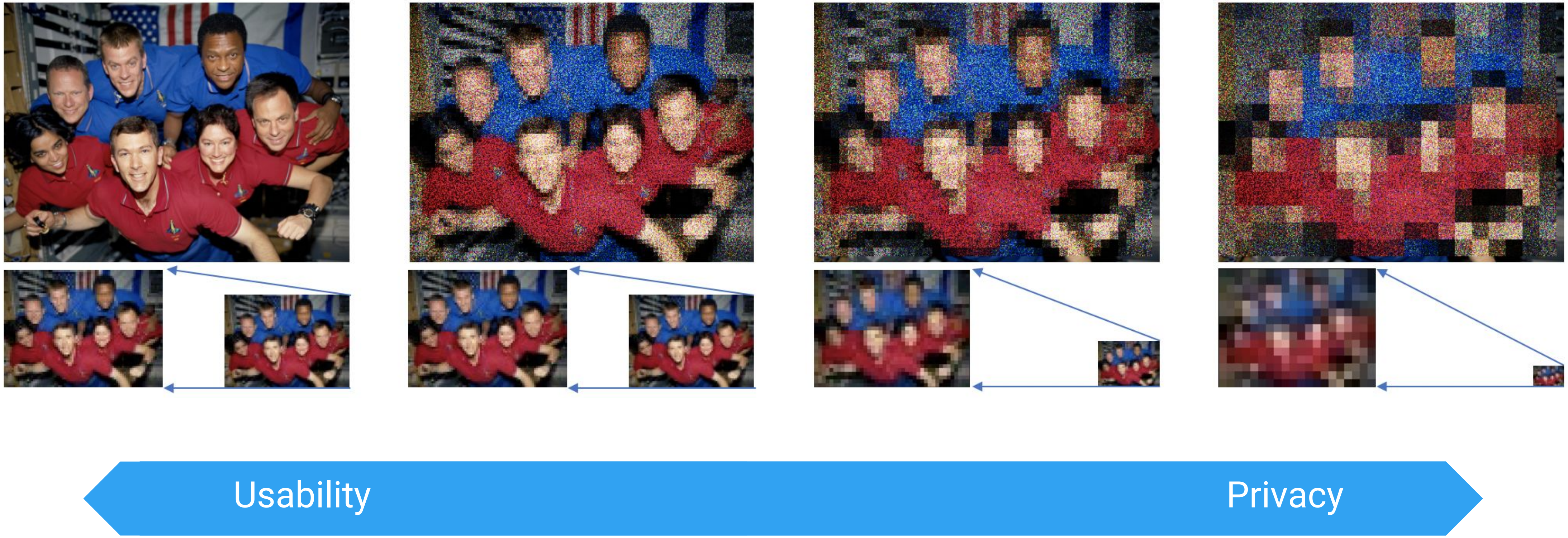
Encryption Rounds



Security Analysis

- Claim: With enough rounds, ciphertext is random image with same thumbnail as plaintext.
- The encryption algorithm is modeled with a Markov chain.
- The number of iterations until output looks random is related to the mixing time of the chain.
- The bound on mixing time is analyzed (so is the number of required iterations).

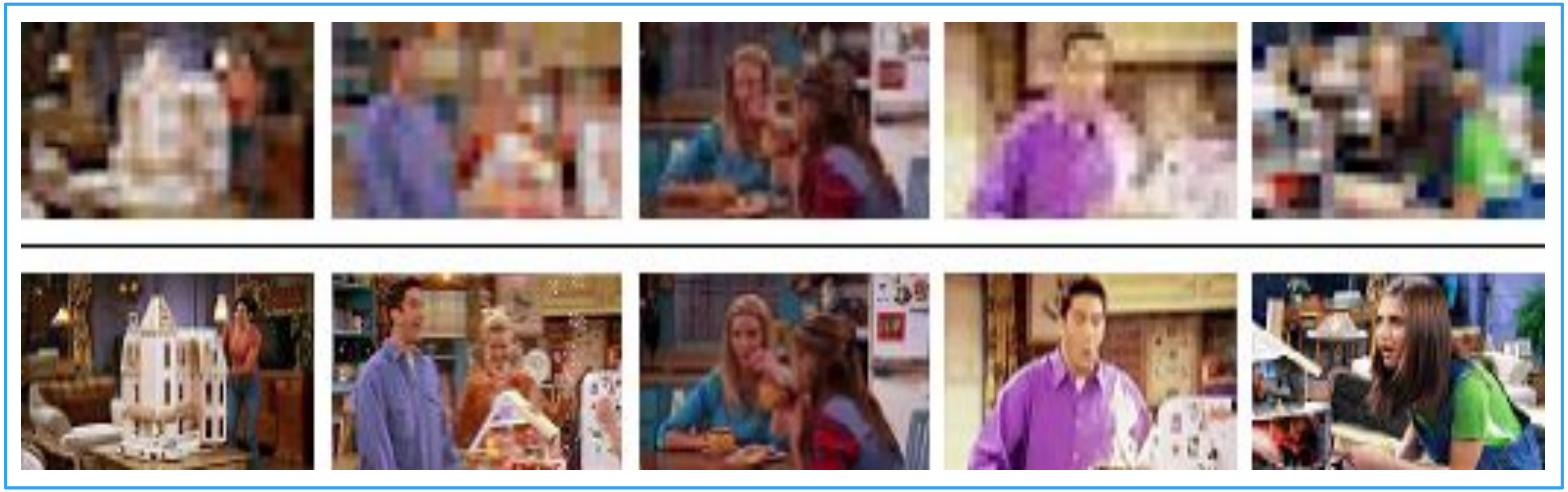
Usability Privacy Trade-Off Analysis



Identify Image from Description

- Prompt:
  - Pick an image that matches the description.
- Description:
  - Monica is introducing her dollhouse.

Thumbnail



High-resolution

Usability Privacy Trade-Off Analysis

- Both time and correctness scores are compared for visual recognition tasks involving thumbnail and original images.
- 80 images are selected from a popular TV series, called Friends.
- Images are pixelated to Google’s Vision API’s failure point.

Usability Privacy Trade-Off Analysis: Results

- TOST (Two One-Sided Test) is used to study the similarity between the two distributions.
- Take-away: Thumbnails have similar usability as high-resolution images, even at a resolution where computer vision fails.

Conclusions and Future Directions

- Image privacy and usability are growing concerns.
- Thumbnail-preserving encryption is a promising way to balance these concerns.
  - Works with existing storage services.
- Some future directions:
  - More quantitative privacy and usability analysis.
  - Computing explicit iteration bounds.
  - Using AI to predict suitable thumbnail sizes.

Thanks!

My email address: tajikk@oregonstate.edu
Project website: https://photoencryption.org/