Scale Me, Crop Me, Know Me Not: Supporting Scaling and Cropping in Secret Image Sharing

Manoranjan Mohanty[1] Wei Tsang Ooi[1] Pradeep K. Atrey[2]

[1] Department of Computer Science, National University of Singapore, Singapore

[2] Department of Applied Computer Science, University of Winnipeg, Canada.

1. MOTIVATION

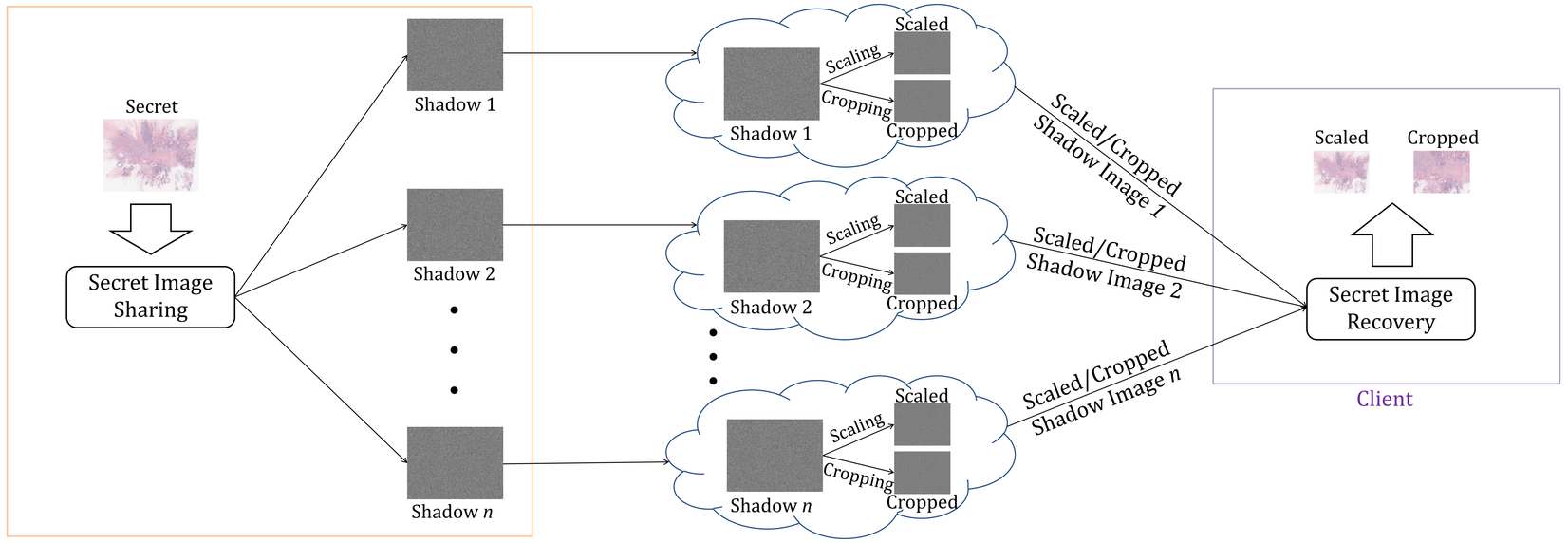
- Huge images such as histopathological images are being increasingly stored and processed in third-party cloud datacenters.
- Allowing a datacenter access to important image leads to security issues as the image can be tampered (data integrity issue), and the information contained in the image can be leaked (data confidentiality issue).
- Existing image hiding schemes are either non-homomorphic to image operations (e.g., watermarking, AES based), or disclose key information about image (e.g., (k, k, n) multi-secret sharing based) when used alone.

2. OBJECTIVE

- To use a cryptographic technique to hide an image from a third-party datacenter such that
  - The datacenters can scale/crop the hidden image without sending additional data to the user of the image.
  - An authorized user (e.g., a doctor) can recover the secret scaled/cropped image from the hidden scaled/cropped image with reasonable overheads.
  - Tampering with image can be detected by the authorized user.

3. METHOD

- By using Shamir's (l, k, n) ramp secret sharing, we propose a new secret image sharing scheme that, in addition to hiding an image, allows scaling and cropping of the hidden image when image scaling is performed by integer-only bilinear interpolation . The important steps of our method are explained below.



Secret Image Sharing

- Secret image is shared by a new image sharing scheme that
  - Uses three color components (i.e., red, green, and blue color) of a pixel as three secrets in a (3, k, n) multi-secret sharing polynomial to decrease size of a shadow image (i.e., share of the secret image).
  - Does not use any other cryptosystem in order to facilitate scaling and cropping of shadow image.
  - Uses at least one random number in the secret sharing polynomial to overcome the loss of information that results due to the spatial coherence of an image and the non-use of an additional cryptosystem.
- Each shadow image is sent to a datacenter for scaling/cropping.

Image Scaling and Cropping

- Each datacenter performs scaling/cropping on its shadow image.
- Scaling is performed by the modified bilinear interpolation that performs integer-only operations by converting the real number operands to integers by rounding off a real number by d decimal places and multiplying 10^d to the rounded off value.
- Cropping is performed by selecting the colors of only the pixels those are part of the requested region on interest.

Secret Image Recovery

- The user recovers the scaled/cropped secret image from at least k scaled/cropped shadow images received from k datacenters.
- The colors of a pixel are found from k color shares by first using Lagrange interpolation to reconstruct a polynomial

$$L(x) = \left(R + Gx + Bx^2 + \sum_{l=3}^{k-1} D_l x^l \right) \; mod \; q,$$

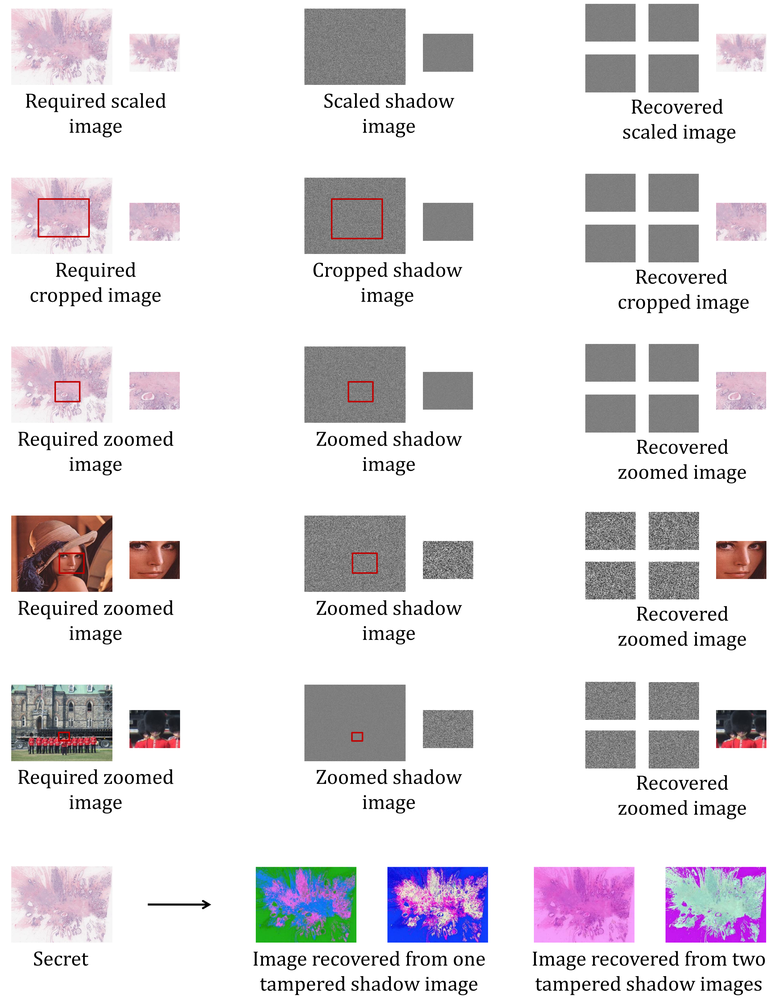
Red color · Green color · Blue color · Random number · Prime number

and then solving $L(x)$.

- In case of scaling, colors are divided by 10^d to obtain the final color.
- An scaling error bounded by $\pm 5.1 \times 10^{-d}$ is introduced, leading to loss of information in the obtained scaled secret image.

4. IMPLEMENTATION AND RESULTS

- We simulate the server, datacenters, and the client in a PC powered with Intel 2.83 GHz dual core processor and 4GB RAM.
- By using C as the programming language, we implement (3, 4, 5) ramp secret sharing, and modify bilinear interpolation by setting d=1.



5. PROPERTIES

- The secret image is hidden to an adversary who can access to at most (k-1) datacenters.
- An adversary having access to more than (k-3) datacenters, however, can get some information about the secret as the (3, k, n) ramp secret sharing, unlike Shamir's secret sharing, is not a perfectly secured cryptosystem.
- Tampering with shadow image can be detected if total number of datacenters is more than the minimum number of datacenters required to recover the secret image (i.e., if $n > k$).
- For a 512 × 512 image, the data overhead is 1.4 times more than the conventional image streaming, and the computation overhead is 78.65 ms.