



Motivation

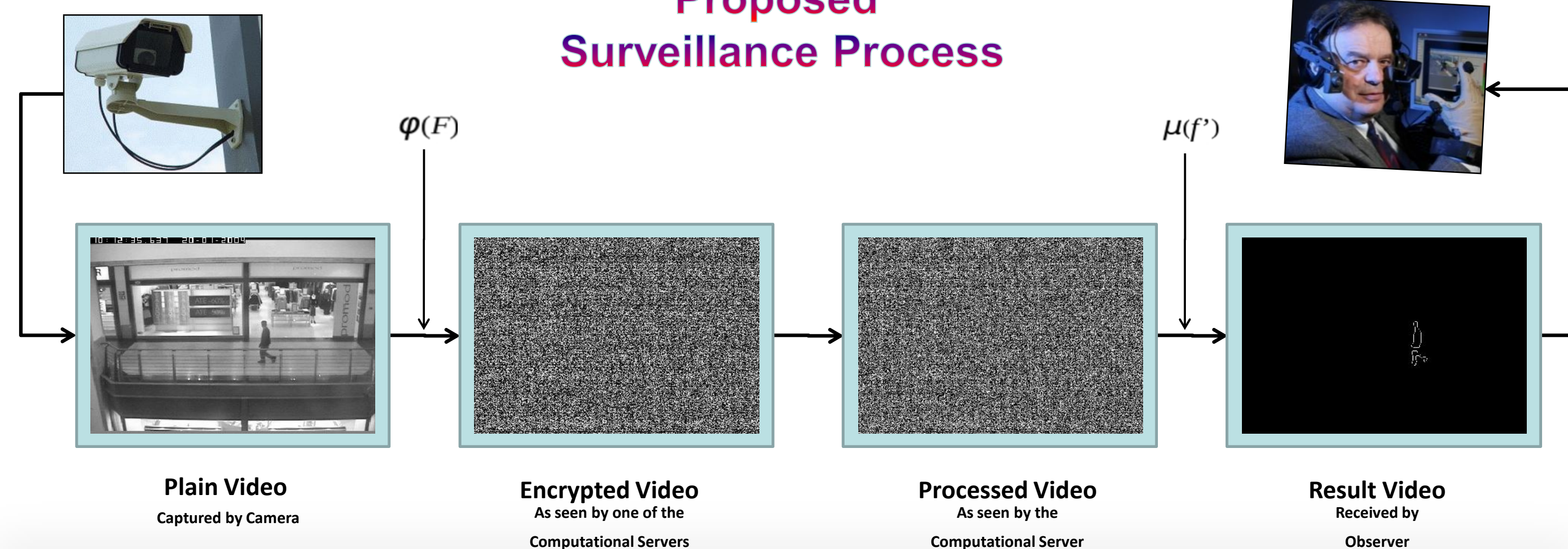
Can we do surveillance without 'seeing' the original video ?

Ability to run video surveillance algorithms, completely in encrypted domain can address most privacy concerns.

Existing methods are either too slow for surveillance applications or do not provide provable privacy.



Proposed Surveillance Process



How do we carry out surveillance on 'Randomized' images ?

Preserve Privacy

- Carry out surveillance on random looking images.

Light weight

- Encrypted domain representation should allow efficient computations.

Limited data expansion

- Obfuscation process should not blow up the video data.

Secure Storage

- Obfuscation should be provably secure to ensure security at un-trusted servers.

Reconstruction of data

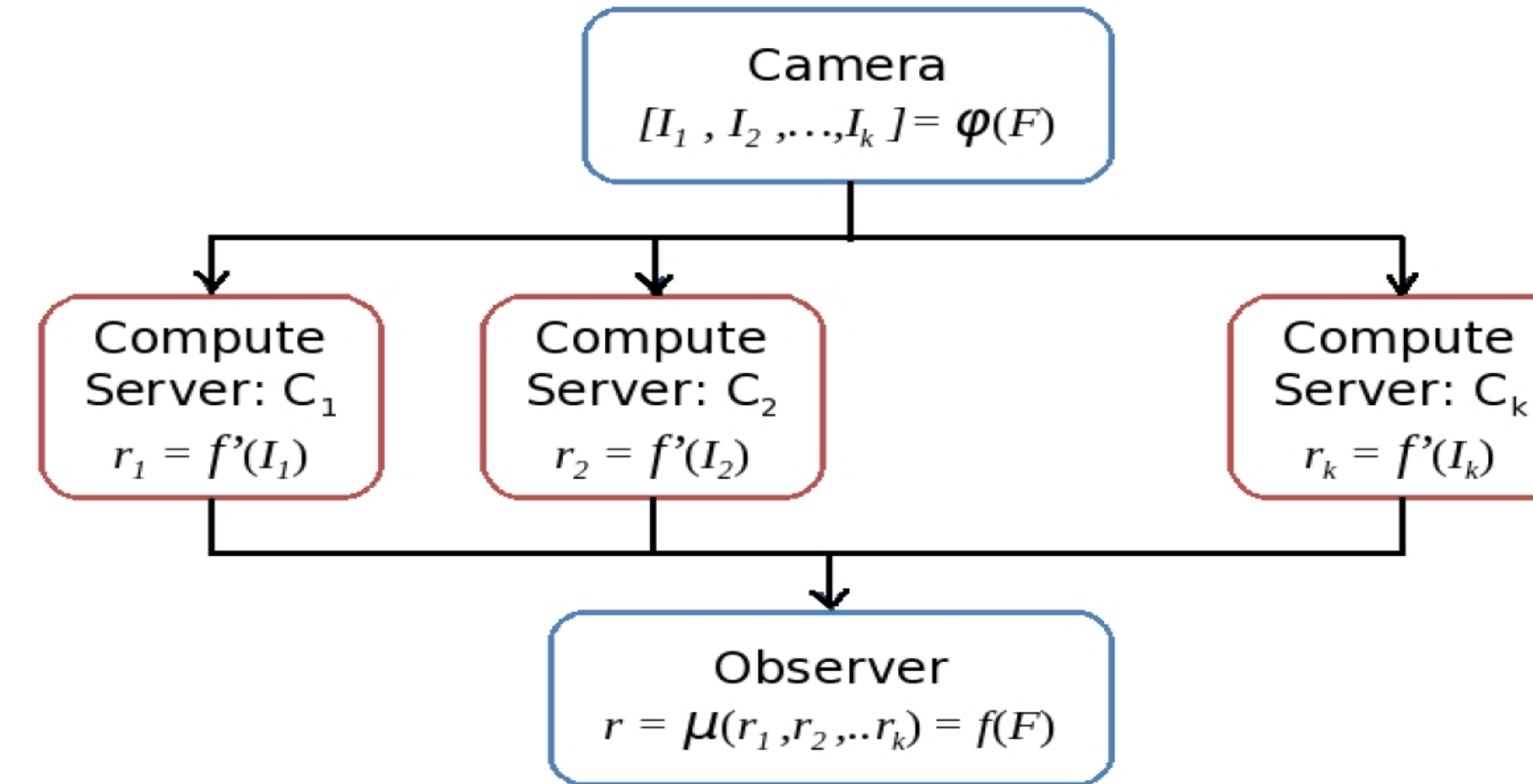
- Only authorized people should be able to recover original plain video.

The Proposed Approach

We have proposed a 'cloud computing' based solution that utilizes the services of $k > 2$ non-colluding computation servers.

The privacy of our surveillance system is based on splitting the information in an image into multiple shares, such that no share by itself conveys anything about the original image.

The protocol in a nutshell:



Shatter Image

- The camera splits each captured frame F , into $k (> 2)$ shares using a pixel level shatter function:
$$d_i = \phi_p(d, p_i) = (d \cdot s + \eta) \bmod p_i,$$
- Each share is then sent to an independent server for processing.

Compute

- To carry out a basic operation f on the input image, each server blindly carries out the equivalent basic operation f' on its share.

Merge Result

- The results of operations on the shares are integrated by the observer using a merge function (CRT), to obtain final result.

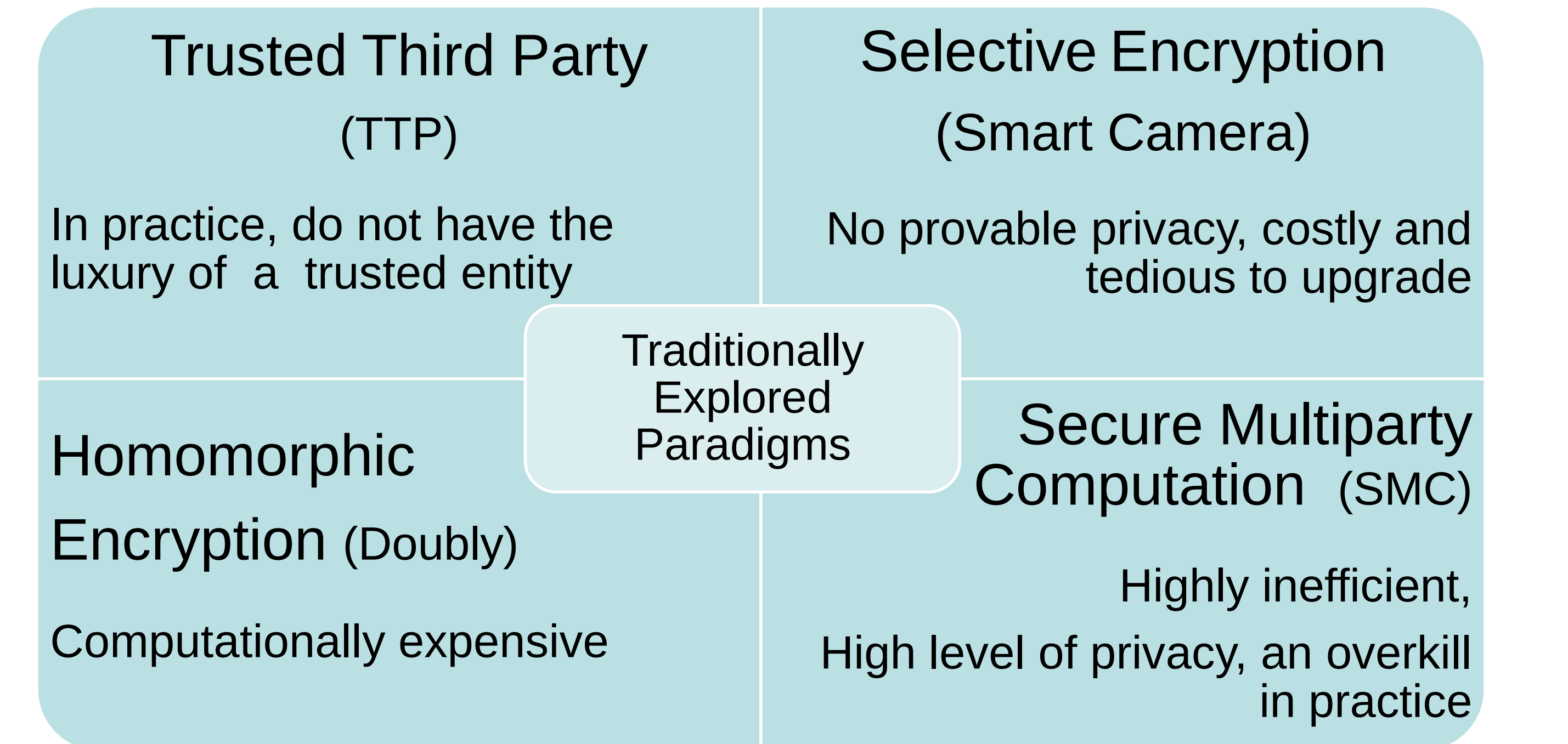
RNS is doubly homomorphic, thus all computation based on '+' and 'x' are defined in modular domain.

The domain of RNS is finite, thus generic division is not defined. We adopt randomization with 3rd party based protocol.

Role of Visual Data

Limited and Fixed Range	Scale Invariance	Approximate Nature
Pixel Value is finite and is from a limited and fixed range, known apriori.	Image remains unchanged even if we change the units of measurement.	Visual correctness is as good as original.

Paradigm Shift

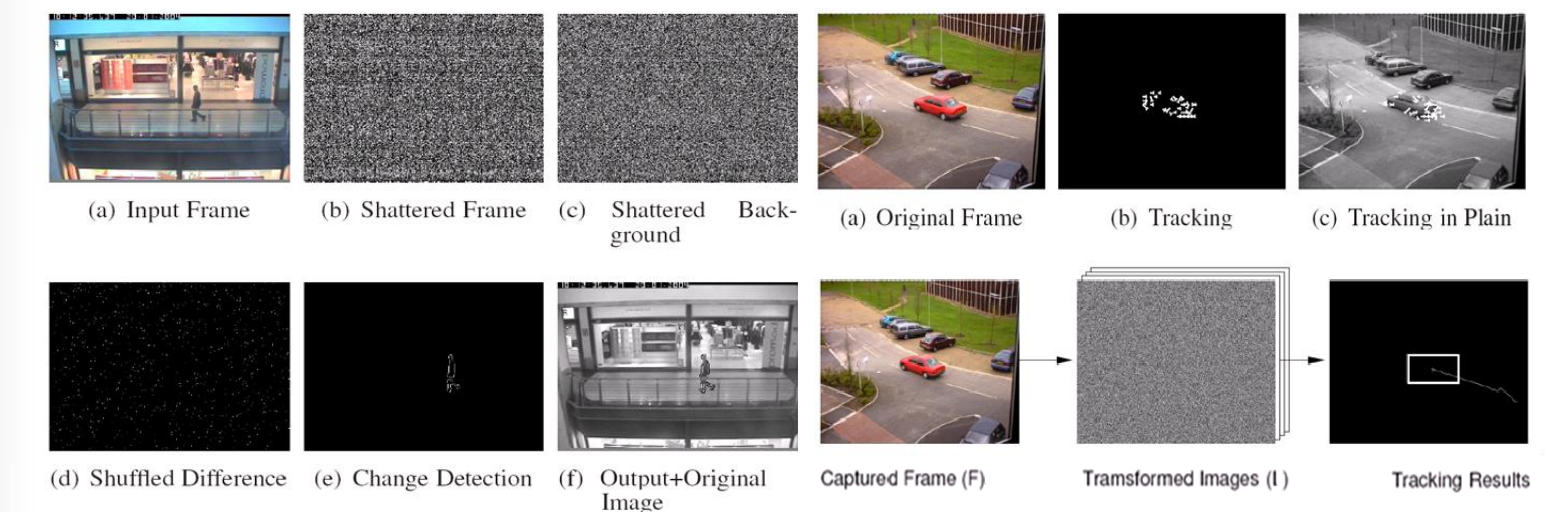


We use the paradigm of secret sharing to achieve private and efficient surveillance.

We exploit the desirable properties of the image data to define a vision specific secret sharing scheme.

Privacy preserving surveillance addresses the contrasting requirements of confidentiality and utility.

Experimental Results



- Servers are un-trusted and the network may be insecure.
- Near loss-less data encoding (PSNR~51).
- No compromise in accuracy.
- Inexpensive capture device, and a unidirectional data flow.
- Negligible overheads to make private computation practical.
- Secure as long as servers do not collude.

Contribution

Circumvent theoretical bounds. Extremely efficient over SMC

Not only efficient, but also provably secure

Scalable, inexpensive and generic, thus practical

Our approach shows that privacy and efficiency co-exists in the domain of visual data

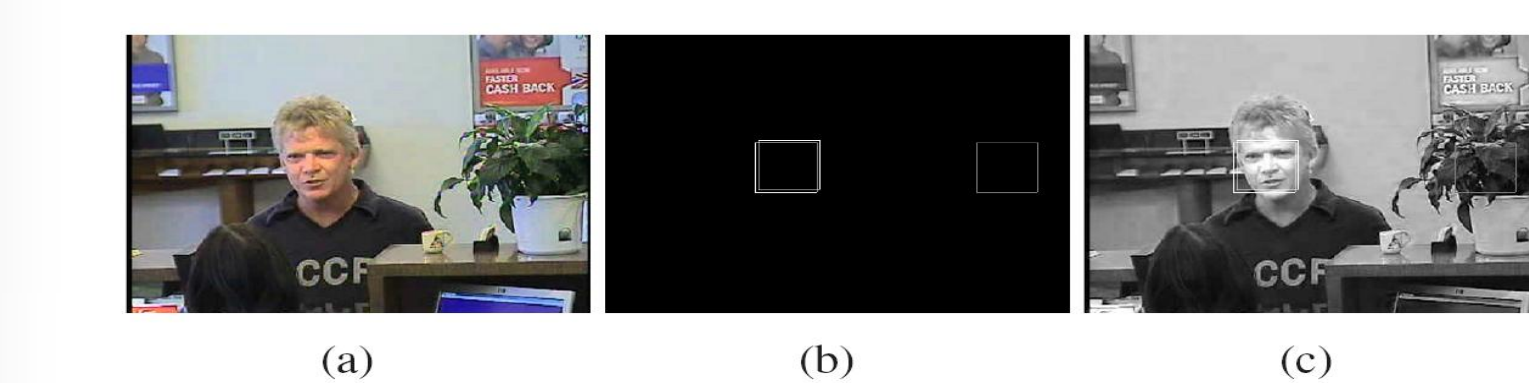


Figure 1: Face detection (a): Captured input image, (b): Result as received by observer, and (c) Detection result, if run on the plain image. The detected faces are shown in white boxes and the current window being processed is shown in gray.

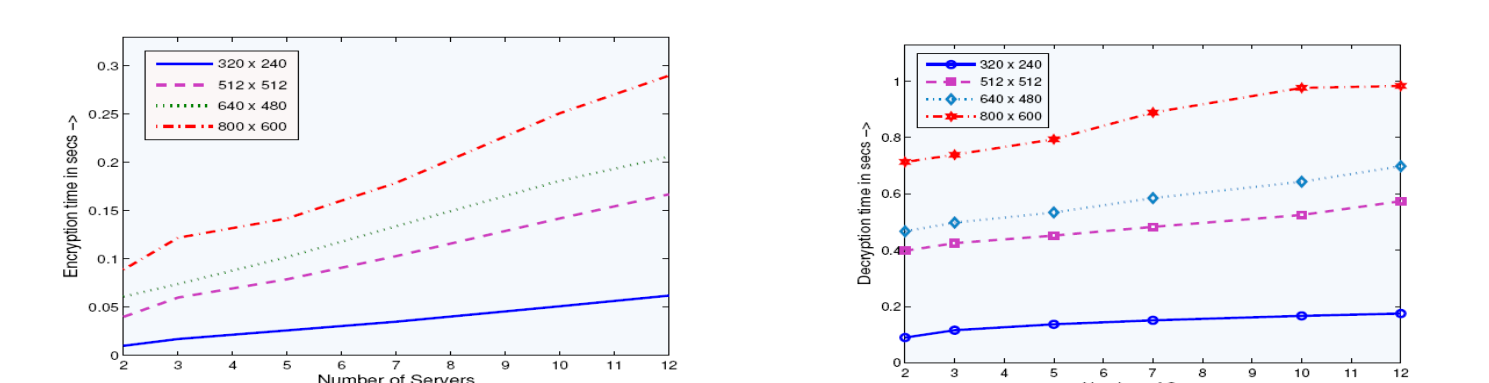


Figure 2: Time required to shatter/merge a frame with increasing number of servers. (a) Shattering Time, (b) Merging Time