



# Architectures for Privacy: Biometric Verification in the Encrypted Domain

Anoop M. Namboodiri

Centre for Visual Info. Technology, IIT, Hyderabad, INDIA

<http://cvit.iiit.ac.in>



M. Upmanyu



K. Srinathan



C.V. Jawahar



A.M. Namboodiri





# Outline

- Privacy and biometric authentication
- The challenge of CryptoBiometrics
- **Blind Authentication**: A cryptobiometric authentication architecture
- **Blind Surveillance**: A distributed video surveillance architecture
- Conclusions and way forward

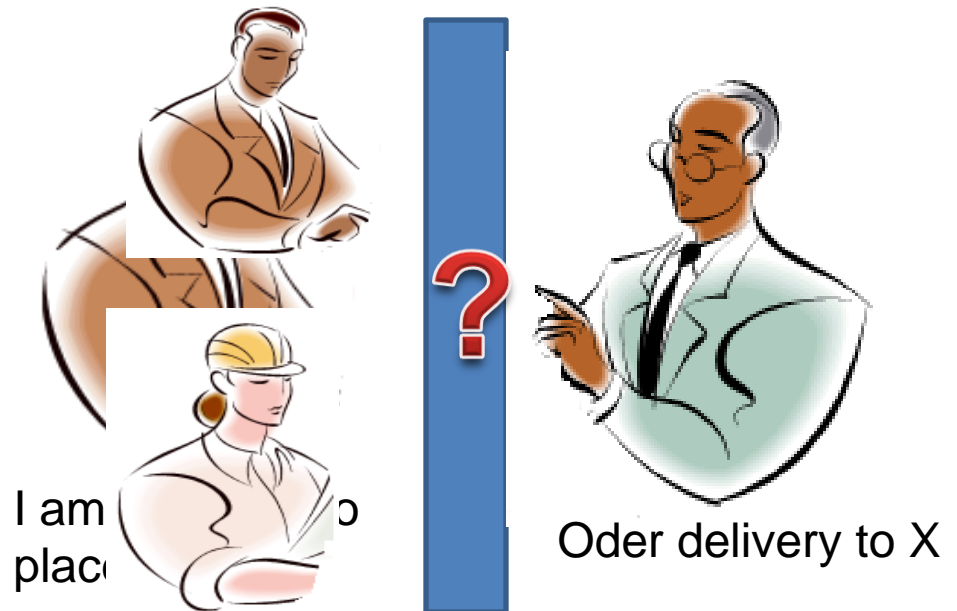




# Privacy in Biometric Authentication

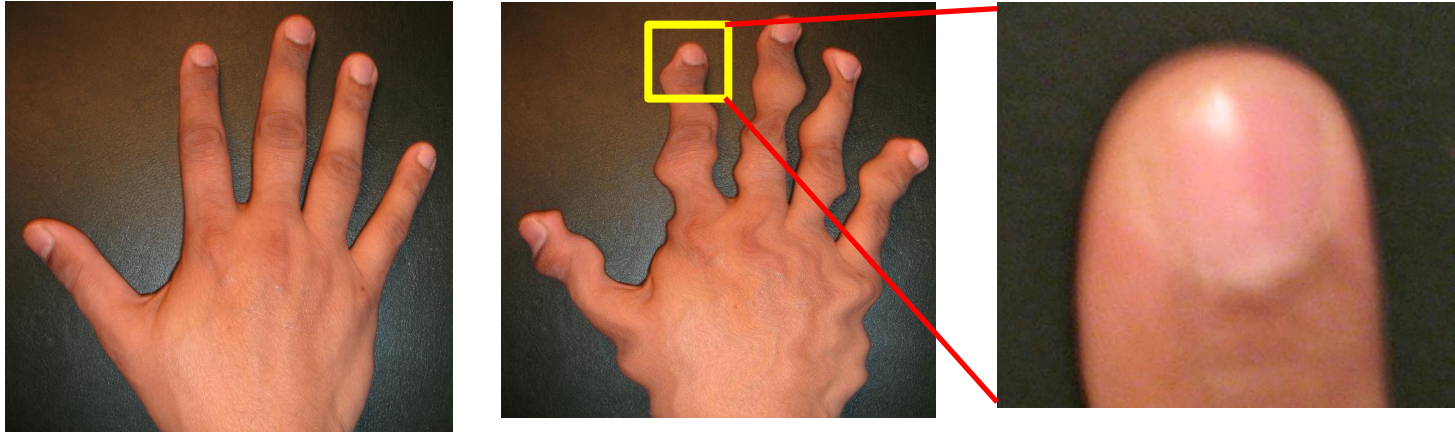
- **Preserving Privacy:** Do not reveal **ANY** information other than identity during the authentication process
- Can we hide even the **identity** ?

- ID of the person
- Which biometric trait





# Personal Information Revealed

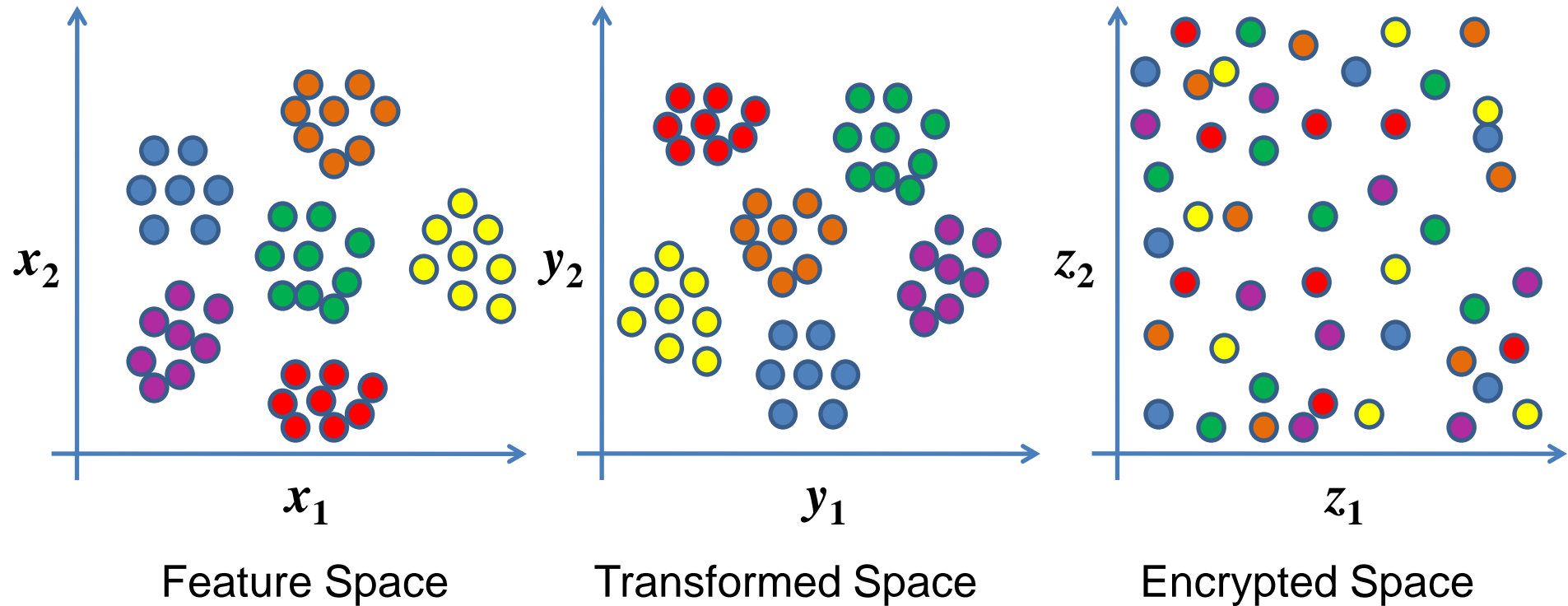


- We do not know what personal information to hide
- Even the presence or absence of a biometric could be personal
- To achieve complete privacy, we need **strong encryption**





# Matching in Encrypted Domain



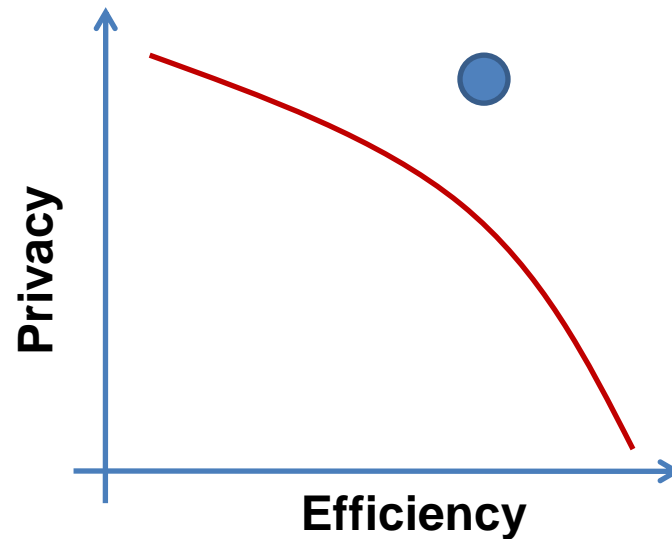
- Encryption and Matching are contradictory





# Breaking the Tradeoff

- A method that provides *provable security/privacy*, while allowing *efficient computations* for generic vision algorithms have remained elusive.

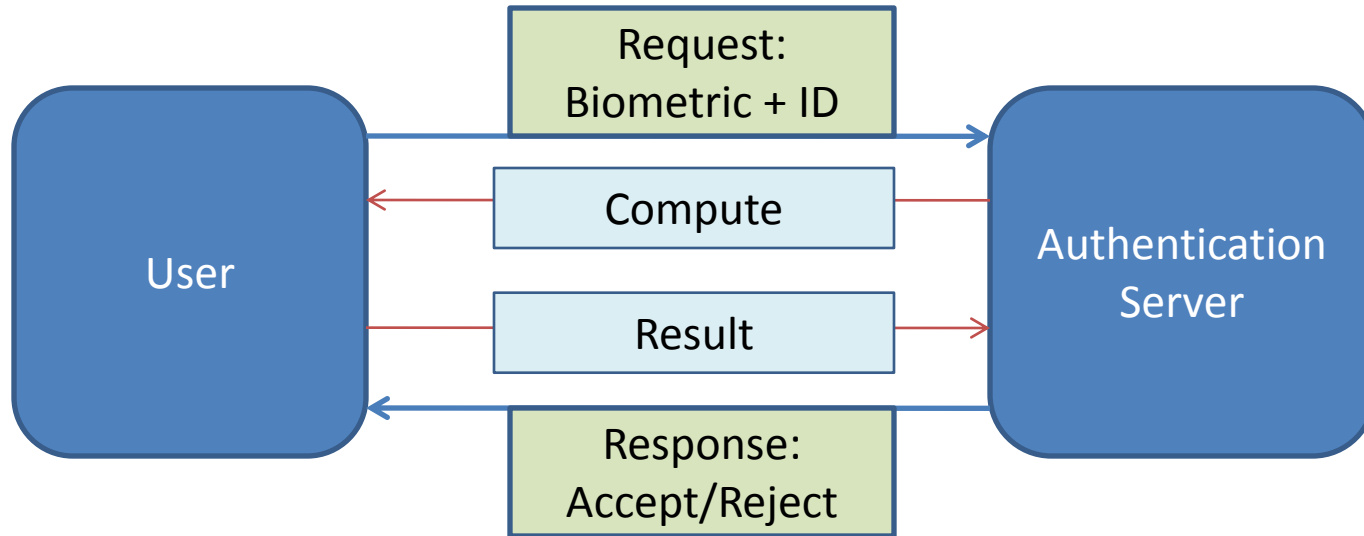


“One can exploit certain properties inherent to natural/visual data to break this seemingly impenetrable barrier”





# Rethinking the Architecture



- User wants to be authenticated
- Collaborate with the user to establish identity





# Use of Homomorphic Encryption

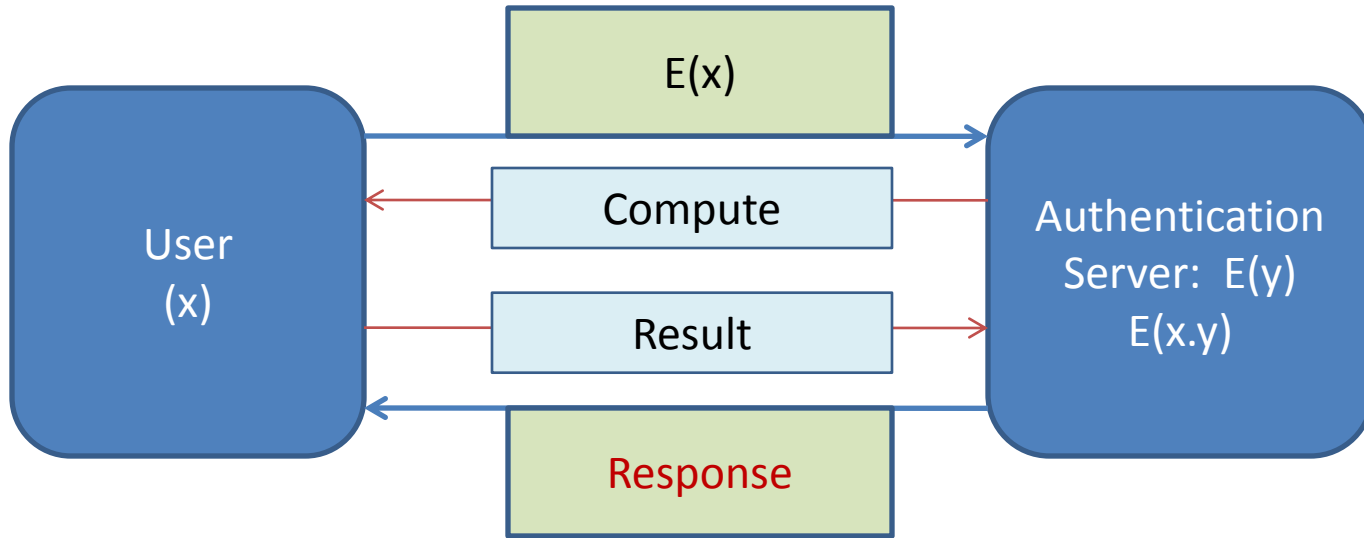
- Let  $x$  and  $y$  are two numbers
- $E(x)$  and  $E(y)$  are the encryptions of  $x$  and  $y$
- $E( )$  is homomorphic to the operator  $\otimes$  iff
  - $E(x) \otimes E(y) = E(x \otimes y)$
- If you have and encryption that is homomorphic to  $+$  and  $\times$ , you can carry out any operation
- Unfortunately such encryptions **did not**\* exist

\* Craig Gentry, “Fully homomorphic encryption using ideal lattices,” *STOC*, pp.169–178, 2009.





# Issues in Using Homomorphic Encryption

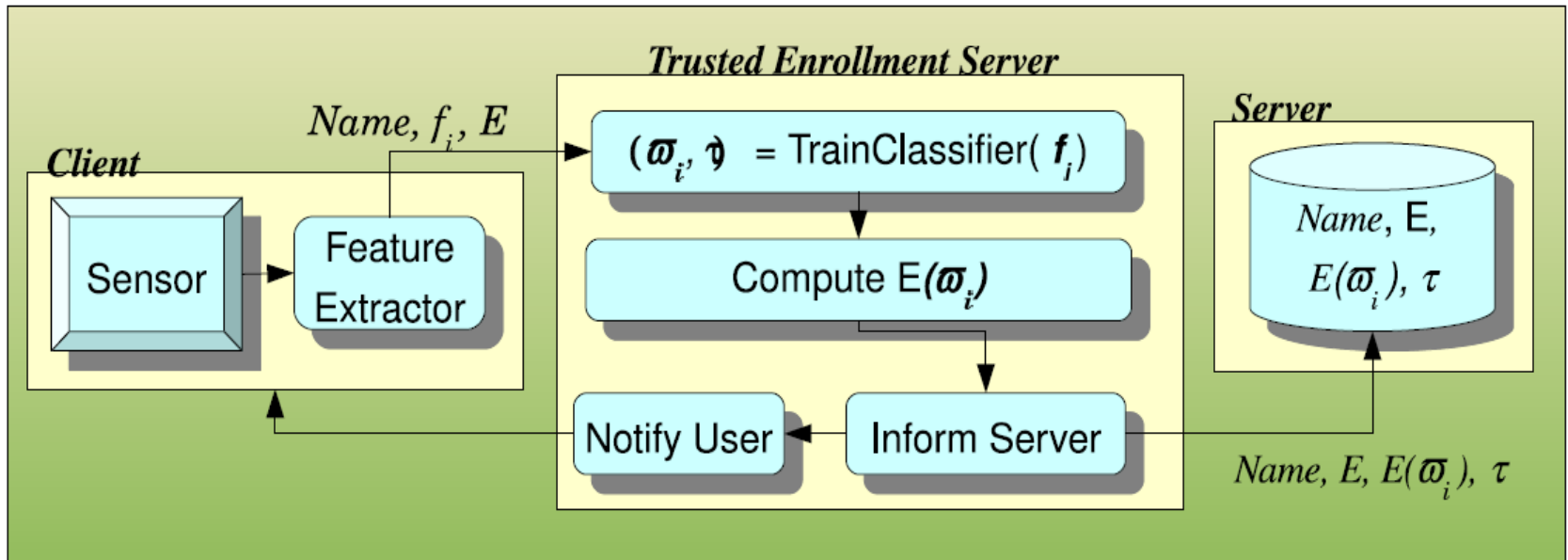


- How to compute a “sum-of-products”
- How to reveal the result to server, reliably.



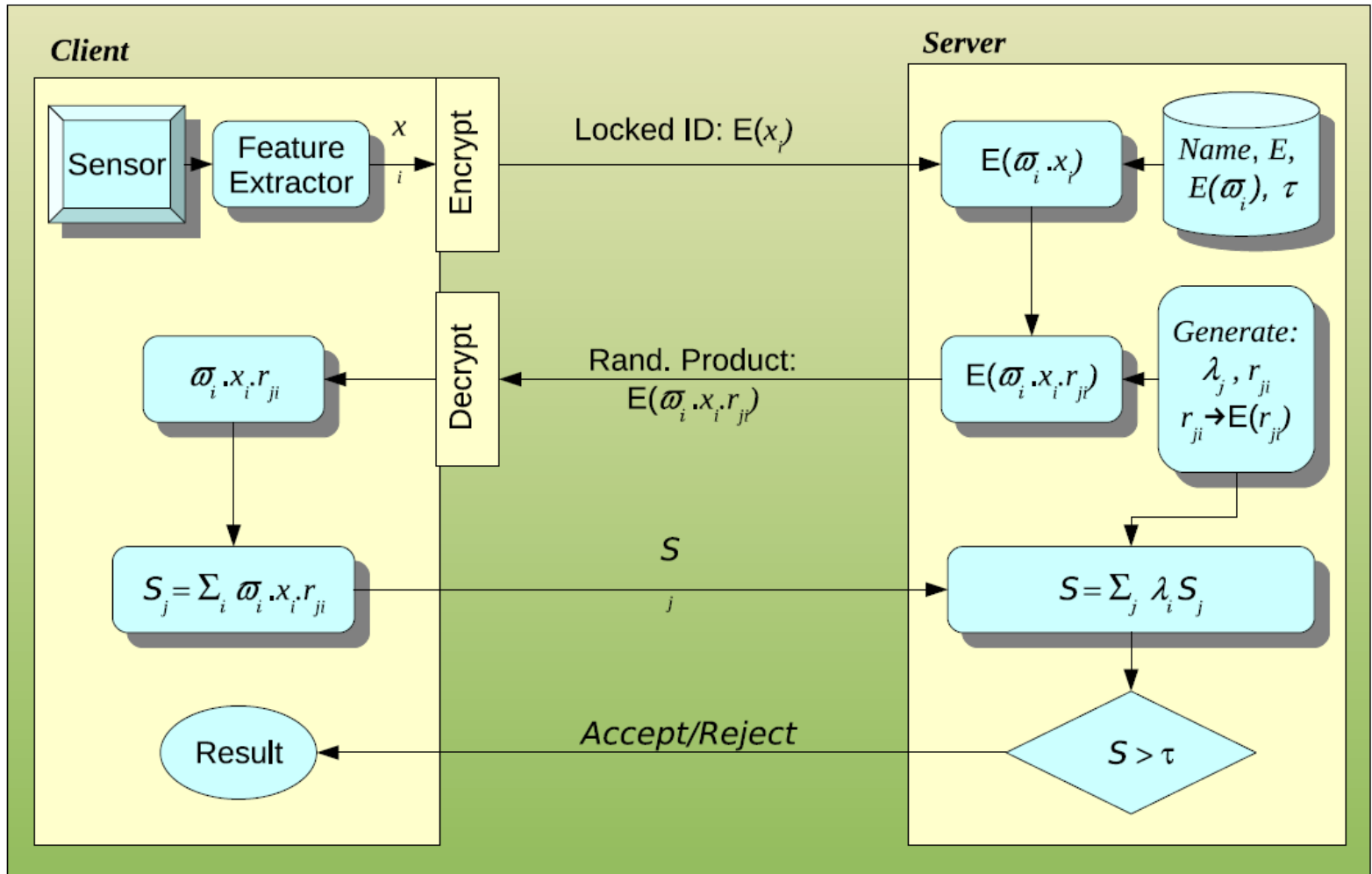


# Enrollment using a Trusted Server



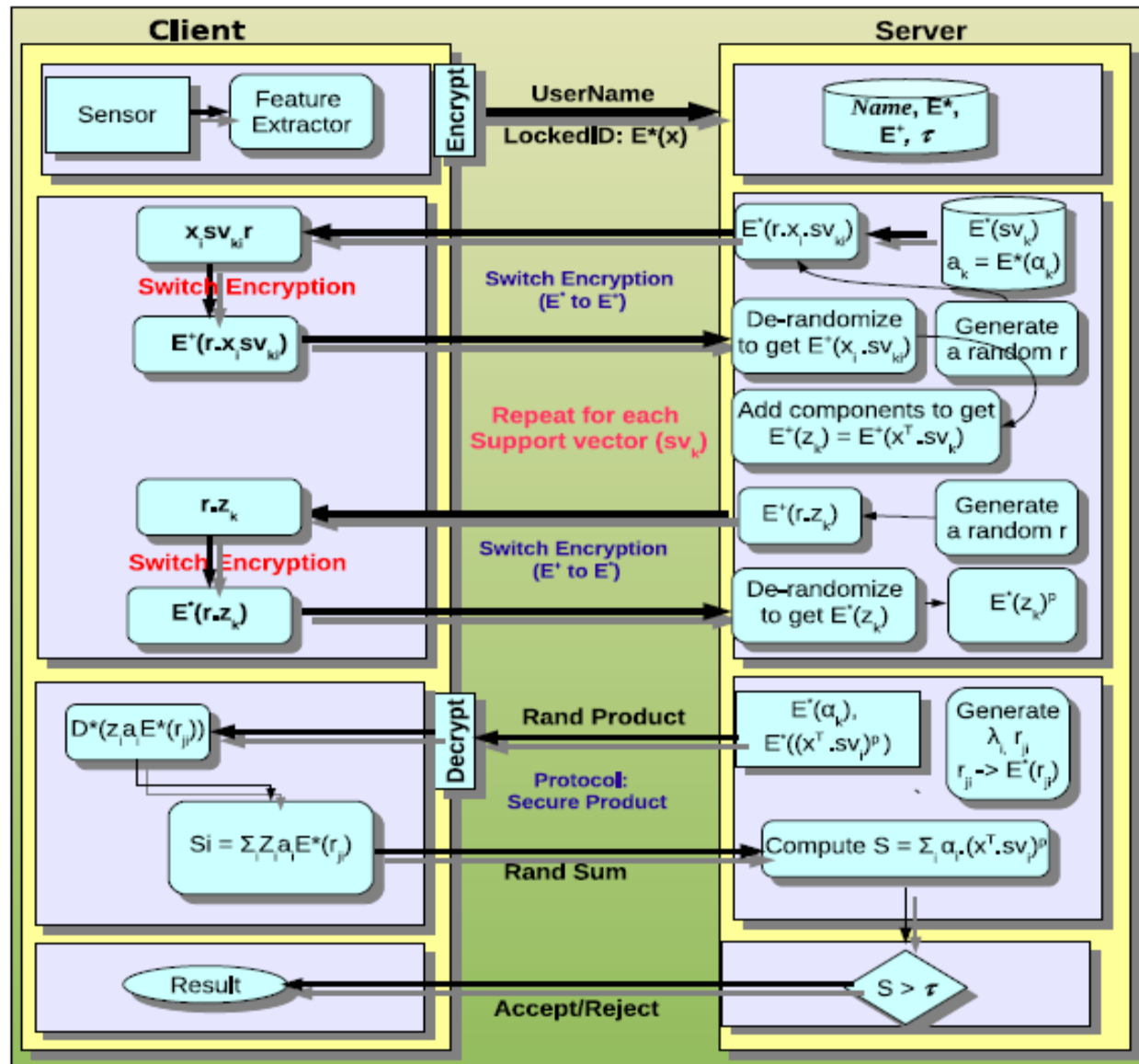


# Authentication: Linear Kernel





# Authentication: Generic Kernel





# Verification Accuracy

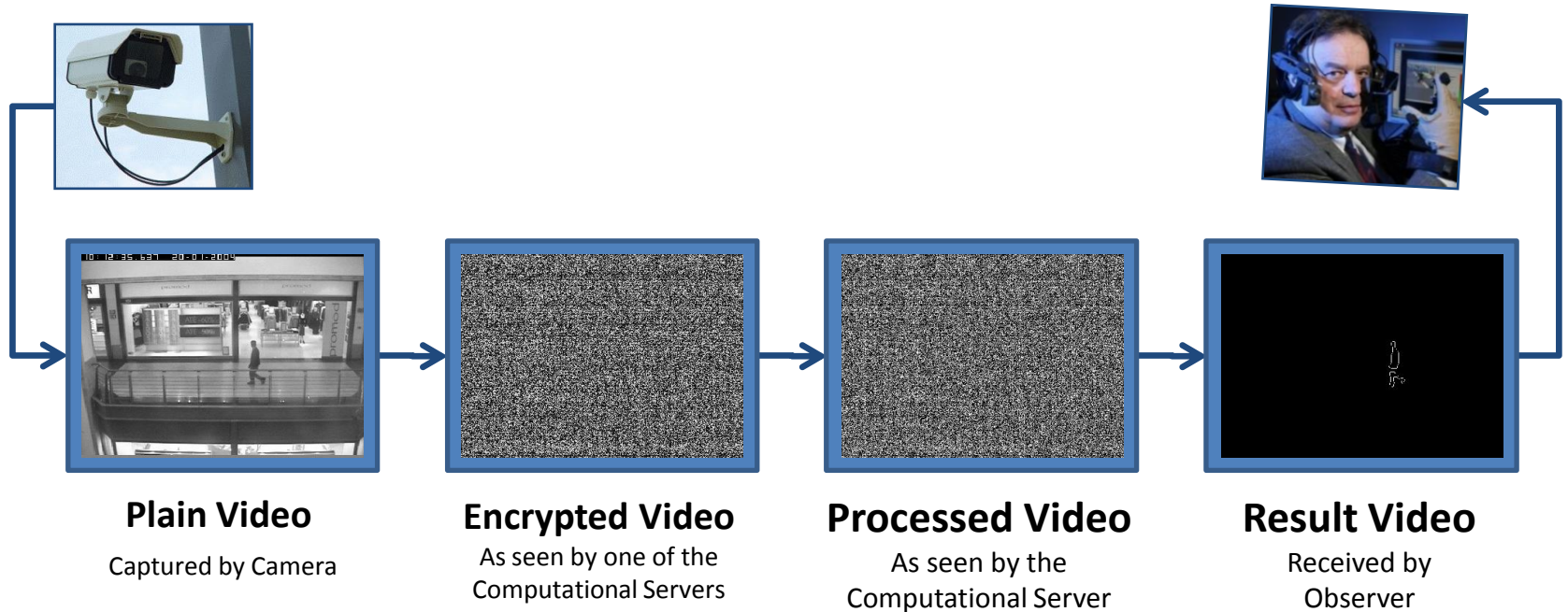
Dataset	Num. Features	Average # SVs	Accuracy
Hand Geometry	20	310	98.4%
Yale Face	102	88	96.9%
CASIA Iris	9600	127	98.2%
FVC 2004	7	440	84.5%

Total time on current desktops: **Less than 1s** excluding encryptions





# Blind Surveillance



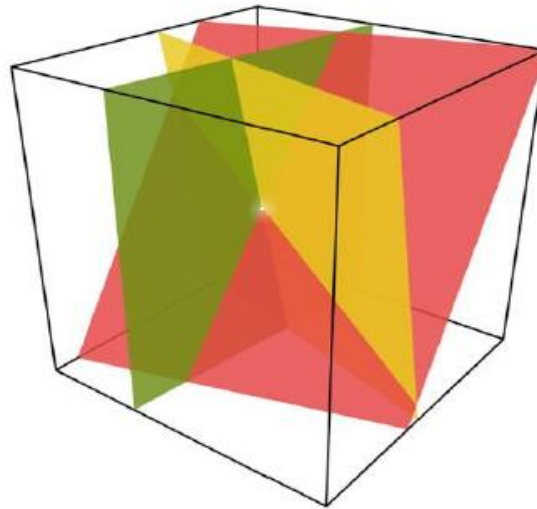
How do we carry out surveillance  
on *'Randomized'* images ?





# Secret Sharing

- A method of **distributing a secret** among a group of servers, such that:
  - Each server on its own has no meaningful information
  - Secret is reconstructed only when all shares combine together



- Existing methods are highly inefficient
- Asmuth-Bloom overcomes this limitation by working in *Residue Number System (RNS)*.





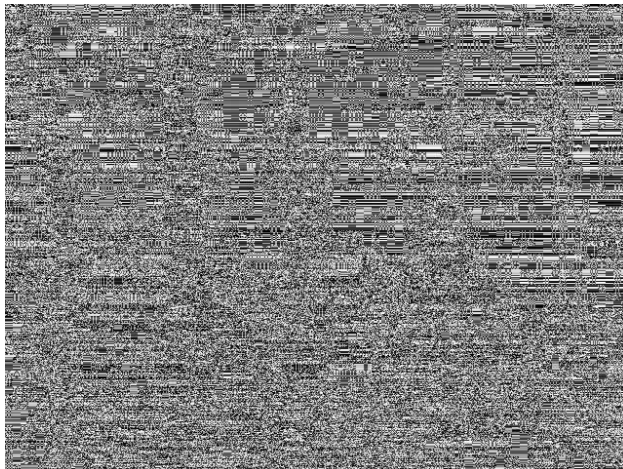
# Shattering a Frame



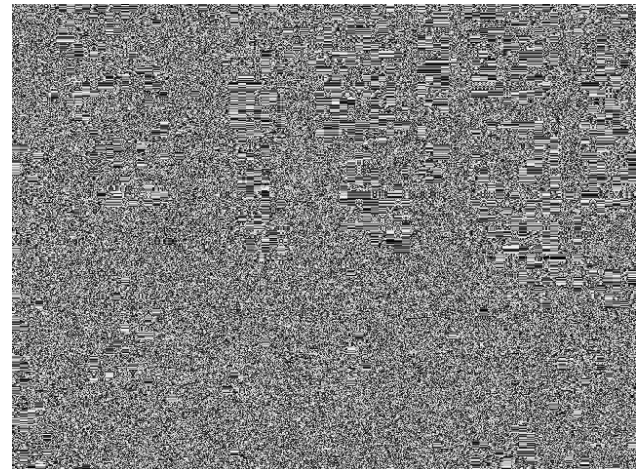
Img: Original Image



Img % 89



$(\text{Img} * 44 + \eta) \% 89$

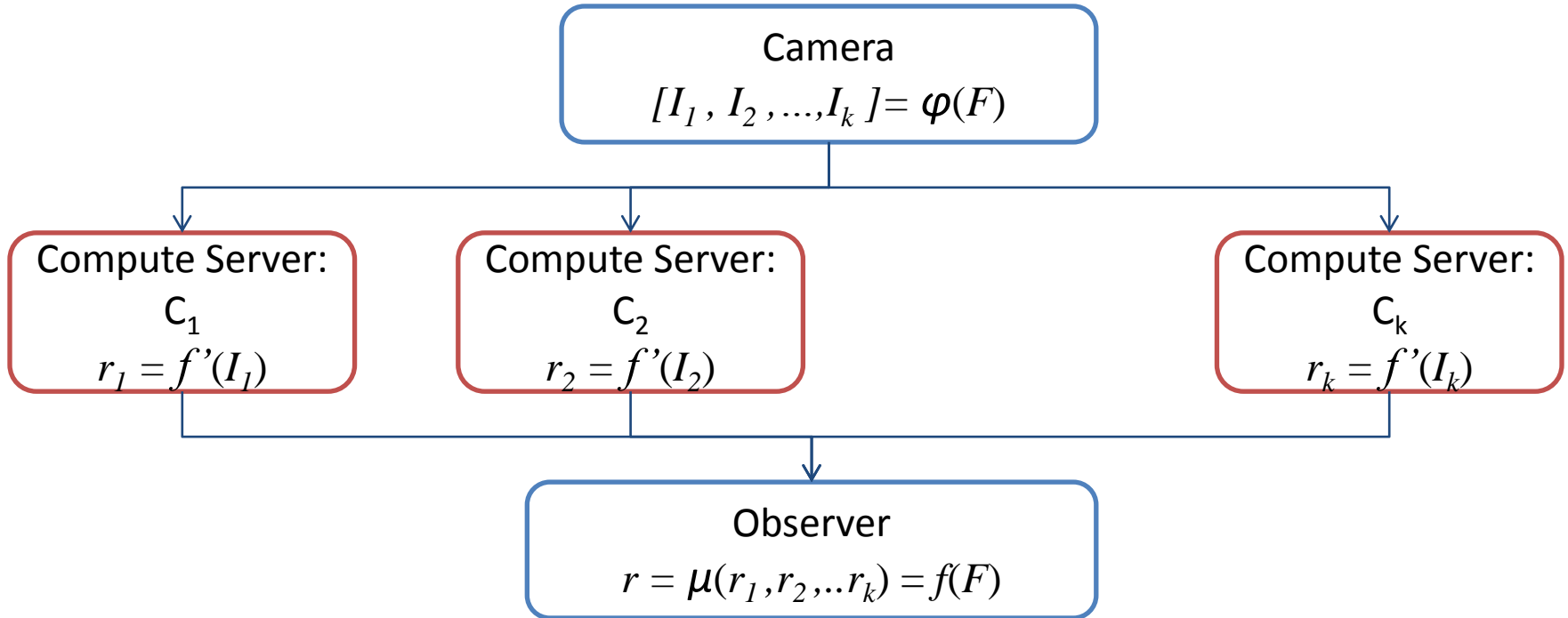


$(\text{Img} * 109 + \eta) \% 89$





# Protocol in a nutshell



**Merge  
Result**

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





# Characteristics of the System

## 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.





# Experimental Results

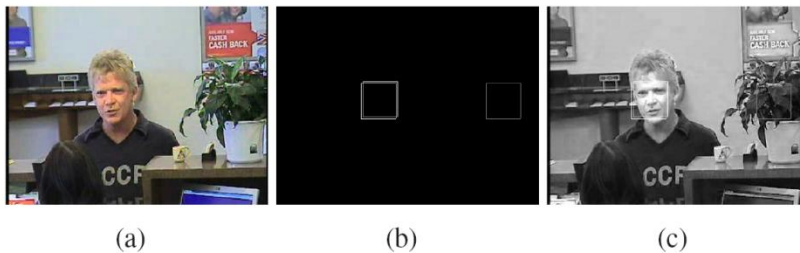
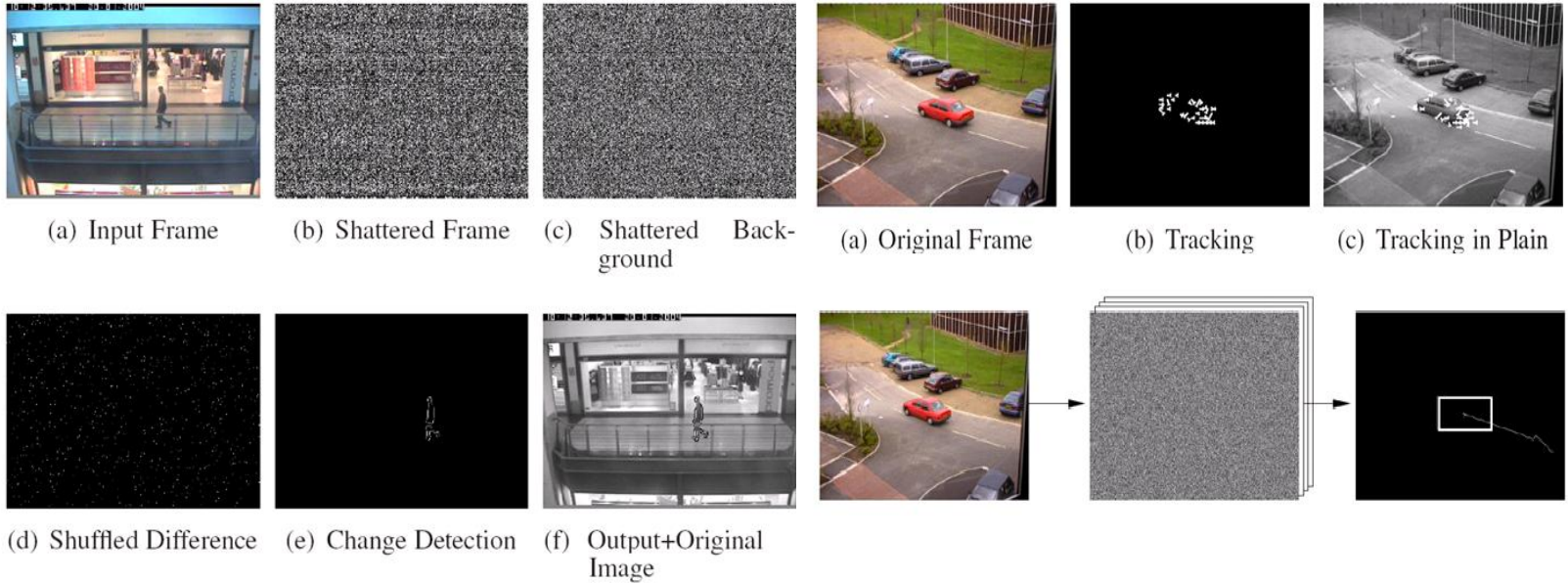
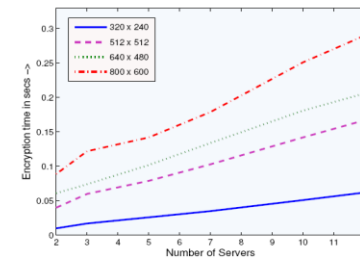
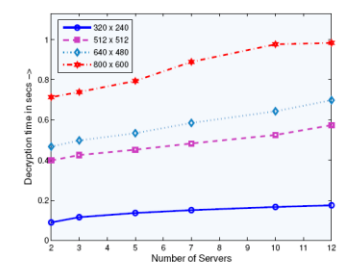


Figure :- Face detection (a): Captured input image, (b): Result as received by observer, and (c) Detection result, if run on the plain image. The detected faces are shown in white boxes and the current window being processed is shown in gray.



(a) Shattering Time



(b) Merging Time

Figure :- Time required to shatter/merge a frame with increasing number of servers.





# Conclusions

- Encrypted domain matching provides: Template protection, Privacy, Security, Revocability, Non-repudiability
- Understanding the problem setting and data can help in deriving efficient methods
- Methods are generic and applicable to other problems also





# Thank You

## Additional Information

<http://cvit.iit.ac.in/>

## Related Publications:

- Maneesh Upmanyu, Anoop M. Namboodiri, K. Srinathan and C.V. Jawahar, **“Blind Authentication - A Secure Crypto-Biometric Verification Protocol”**, in *IEEE-Transactions on Information Forensics and Security*, **June 2010**
- Maneesh Upmanyu, Anoop M. Namboodiri, K. Srinathan and C.V. Jawahar, **“Efficient Privacy Preserving Video Surveillance”**, in *ICCV - 2009*

