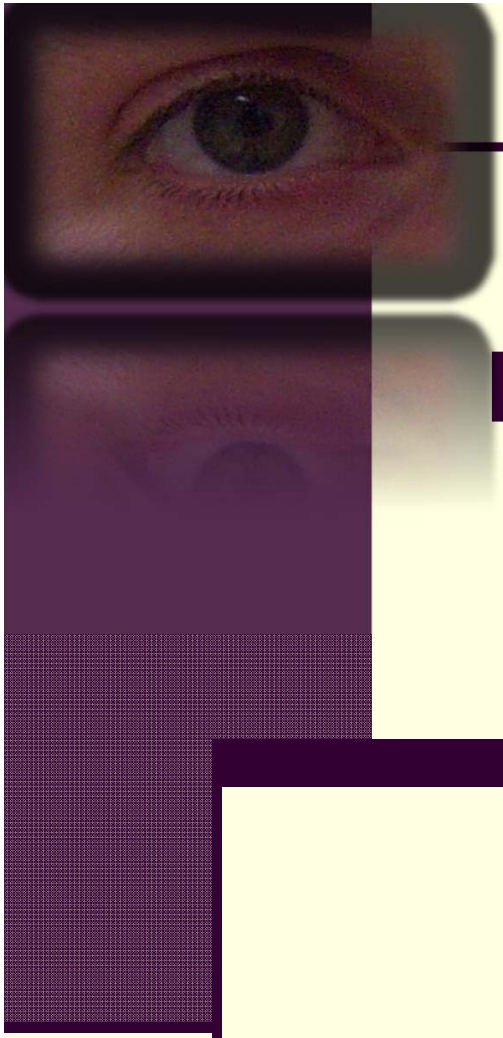


De-identifying biometric images for enhancing privacy and security

Arun Ross

Associate Professor

Michigan State University

rossarun@cse.msu.edu

[Work done with Asem Othman]

http://www.cse.msu.edu/~rossarun

Biometric Data Storage

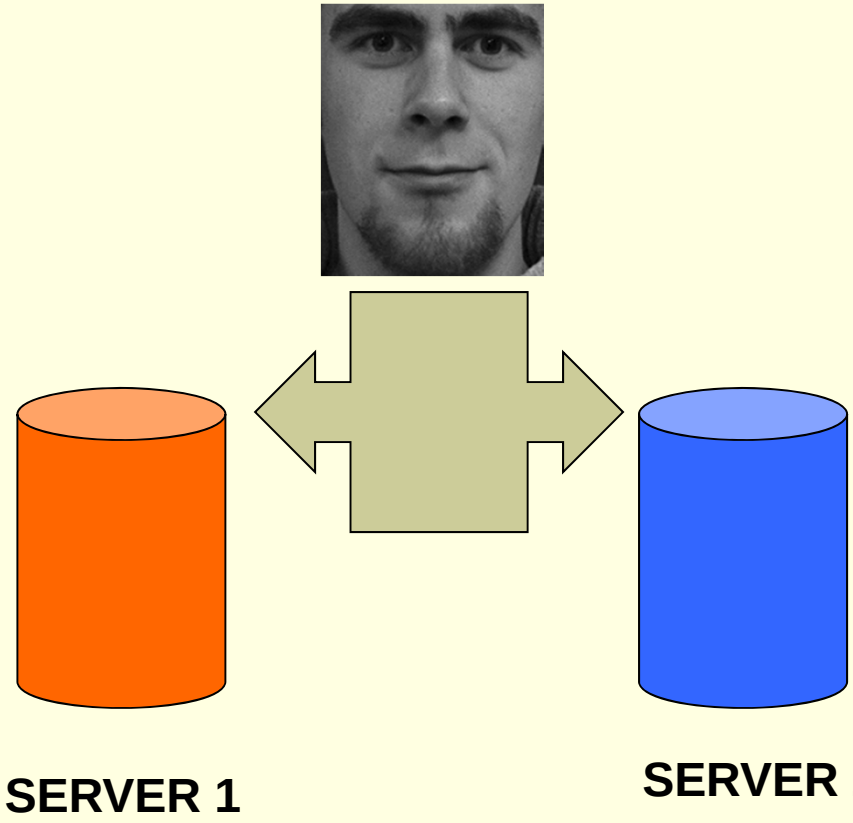
- Biometric data of an individual is sometimes stored in a central database
- Raises issues related to security and privacy of biometric data
  - Unlike compromised passwords, it is difficult to re-issue biometric data
  - Cross-database matching may be done to track individuals
  - Biometric data mining may be performed to glean information about identity

Preserving Privacy: Face

- Face De-identification: Perturb the image so that automated face recognition cannot be reliably done, but preserve details of the face such as expression and gender [Newton et al. (2005), Gross et al. (2006)]
- Face Swapping: Protect identity by automatically replacing faces in an image with substitutes taken from a large library of face images [Bitouk et al. (2008)]
- However, in the case of face swapping and de-identification the original face image can be lost

Proposed Strategy

- The input image is decomposed and stored in two separate servers: either server will be unable to deduce original identity



Visual Cryptography*

- Given an original binary image *T*, it is encrypted in *n* images, such that:

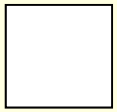
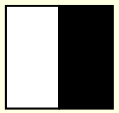
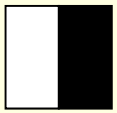
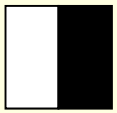
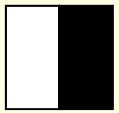
$$T = S_{h_1} \oplus S_{h_2} \oplus S_{h_3} \oplus \ldots \oplus S_{h_k}$$

where $\oplus$ is a Boolean operation , S_{hi} is an image which appears as noise, $k \leq n$, and n is the number of noisy images

- This is referred to as *k-out-of-n* VCS

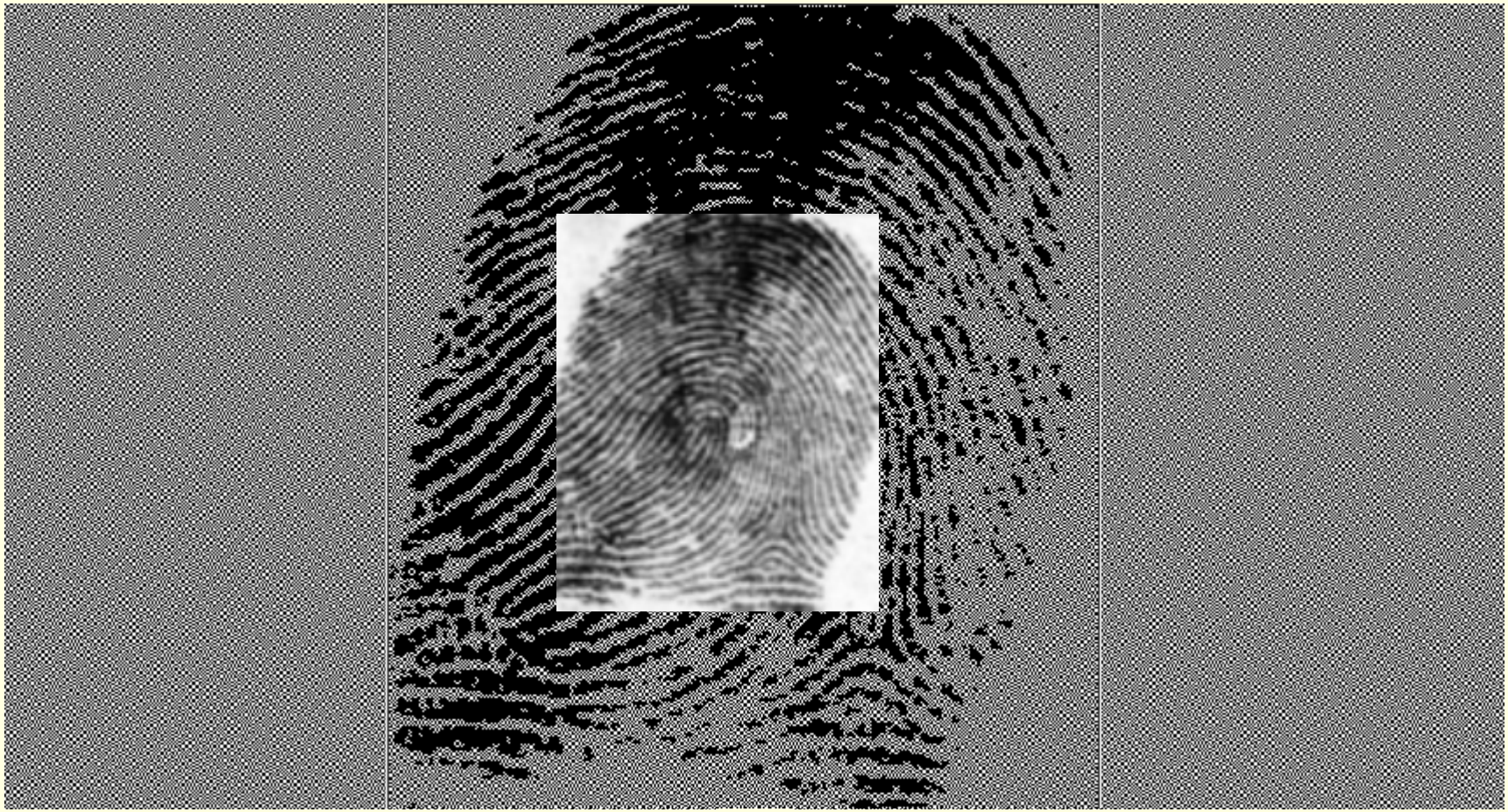
* M. Naor and A. Shamir, "Visual cryptography," in EUROCRYPT, pp. 1–12, 1994.

2-out-of-2 VCS

Pixel	Probability	Shares #1	Shares #2	Superposition of the two shares	
	$p = 0.5$				White Pixels
	$p = 0.5$				
	$p = 0.5$				Black Pixels
	$p = 0.5$				

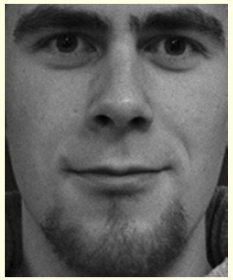
Sharing a secret image: Binary

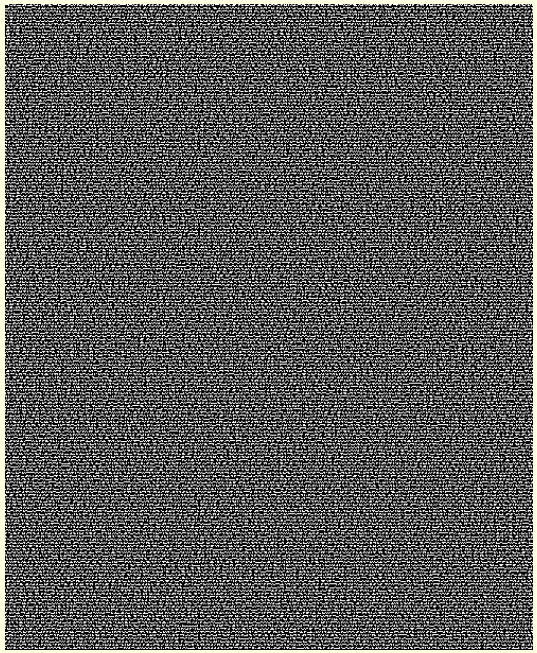
- Decomposing a fingerprint into two random images

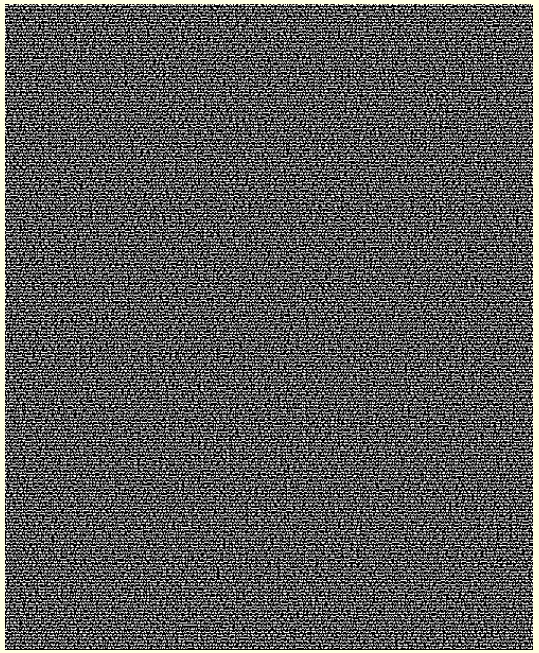


Sharing a secret image: Binary

- Decomposing a face into two random images







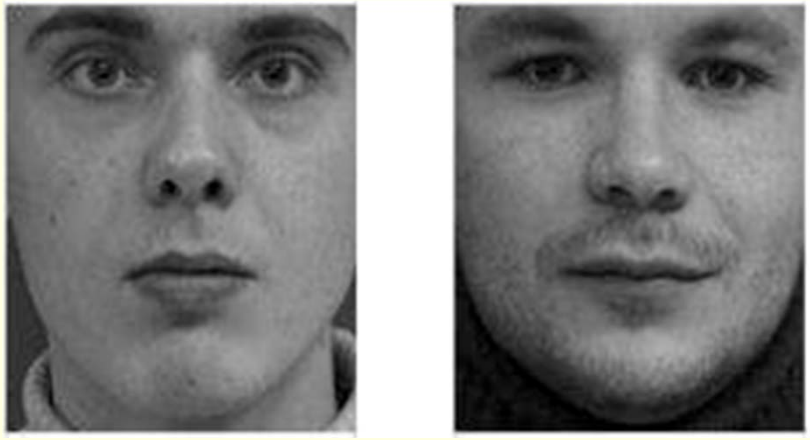
Gray-level Extended Visual Cryptography Scheme (GEVCS)

- VCS allows us to encode a secret image into n sheet images
- These sheets appear as a random set of pixels
- The sheets could be reformulated as natural images – known as host images

M. Nakajima and Y. Yamaguchi, “Extended visual cryptography for natural images,” Journal of WSCG 10(2), pp. 303–310, 2002.

Visual Cryptography: An Example

PRIVATE IMAGE



HOSTS (PUBLIC IMAGES)

PRIVATE IMAGE AFTER DECRYPTION

HOSTS AFTER ENCRYPTION

Visual Cryptography

Actual Face

=

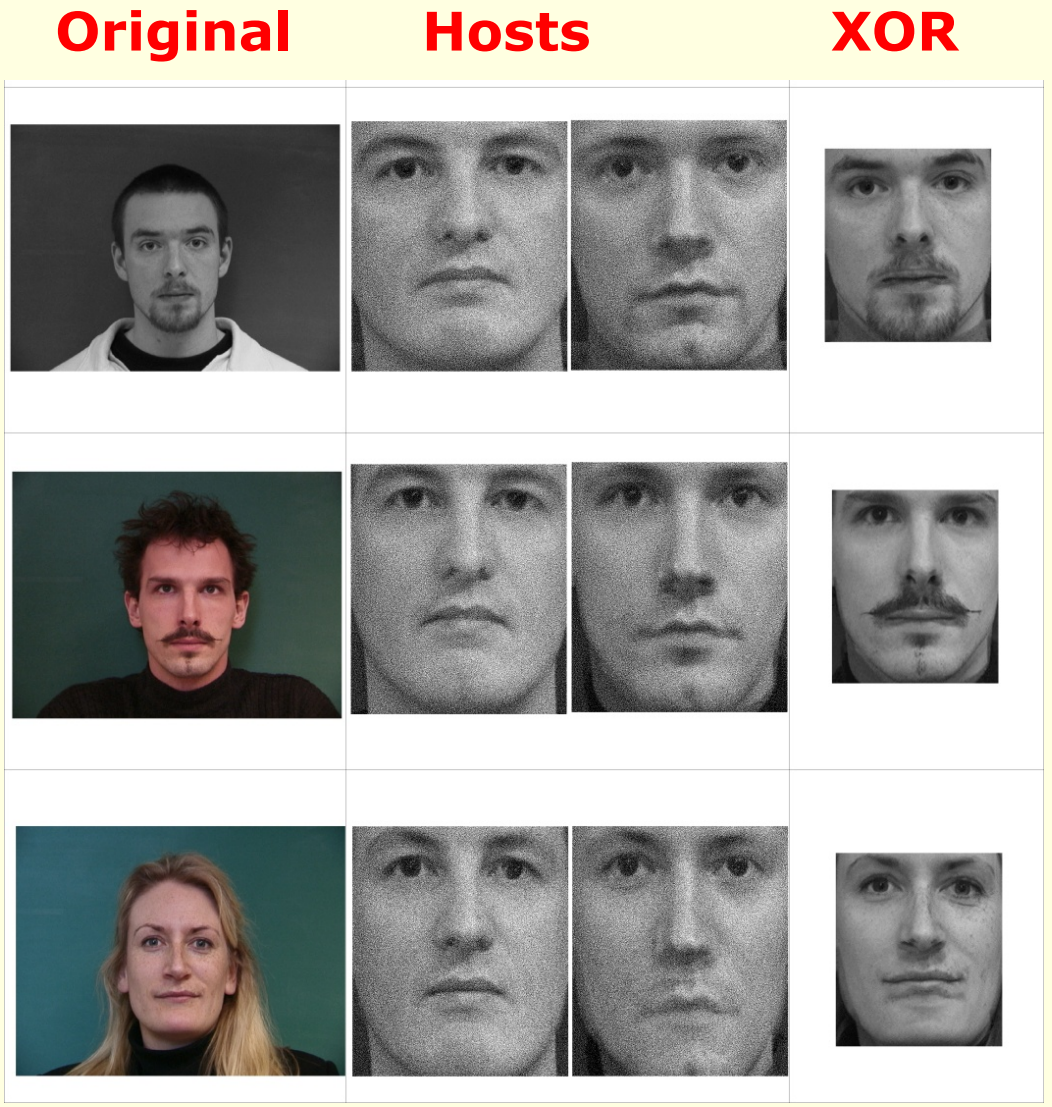
HOST IMAGE 1

+

HOST IMAGE 2

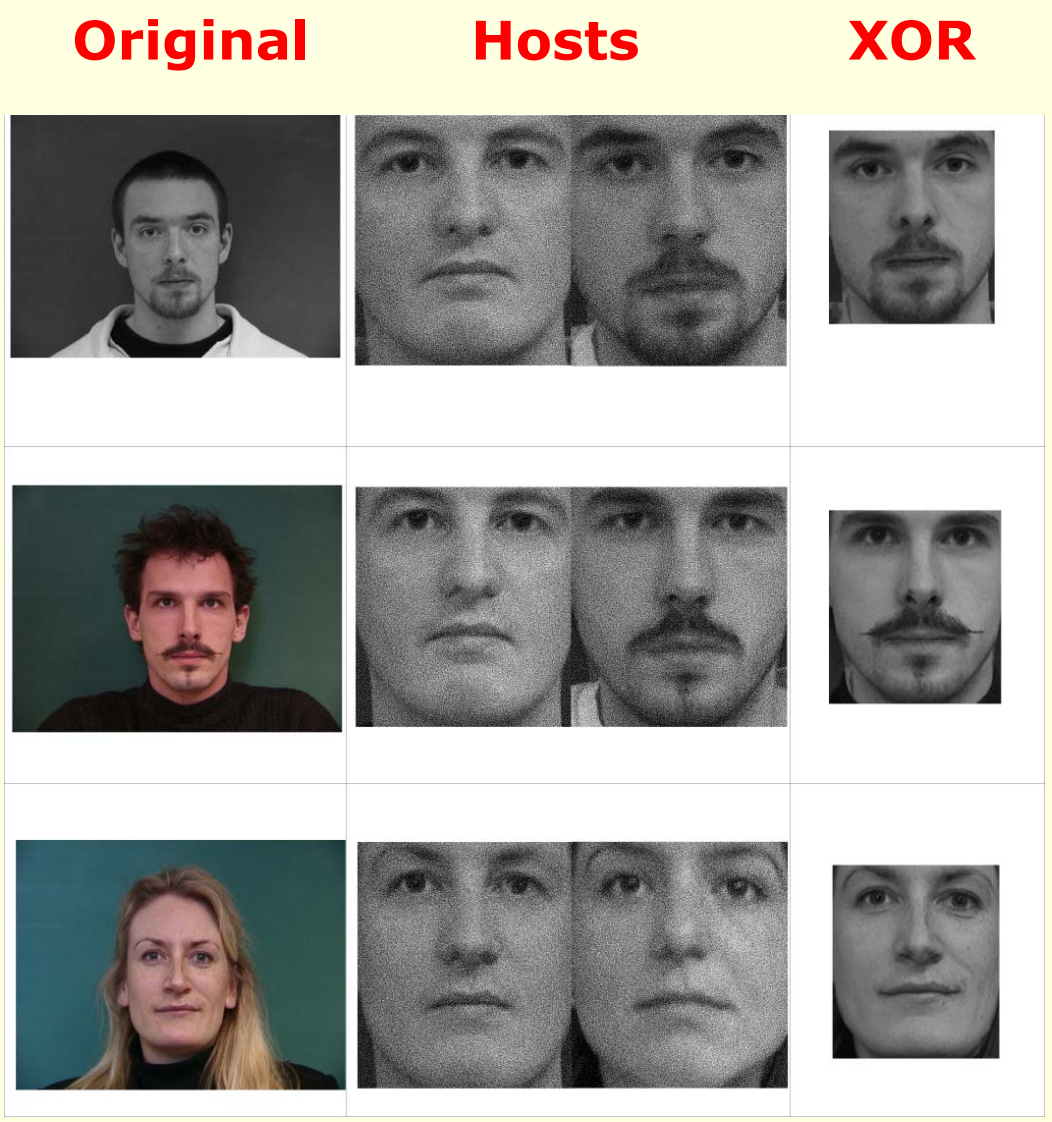
Two fixed host images

- The original image is encrypted into two fixed host images



Automated Host Image Selection

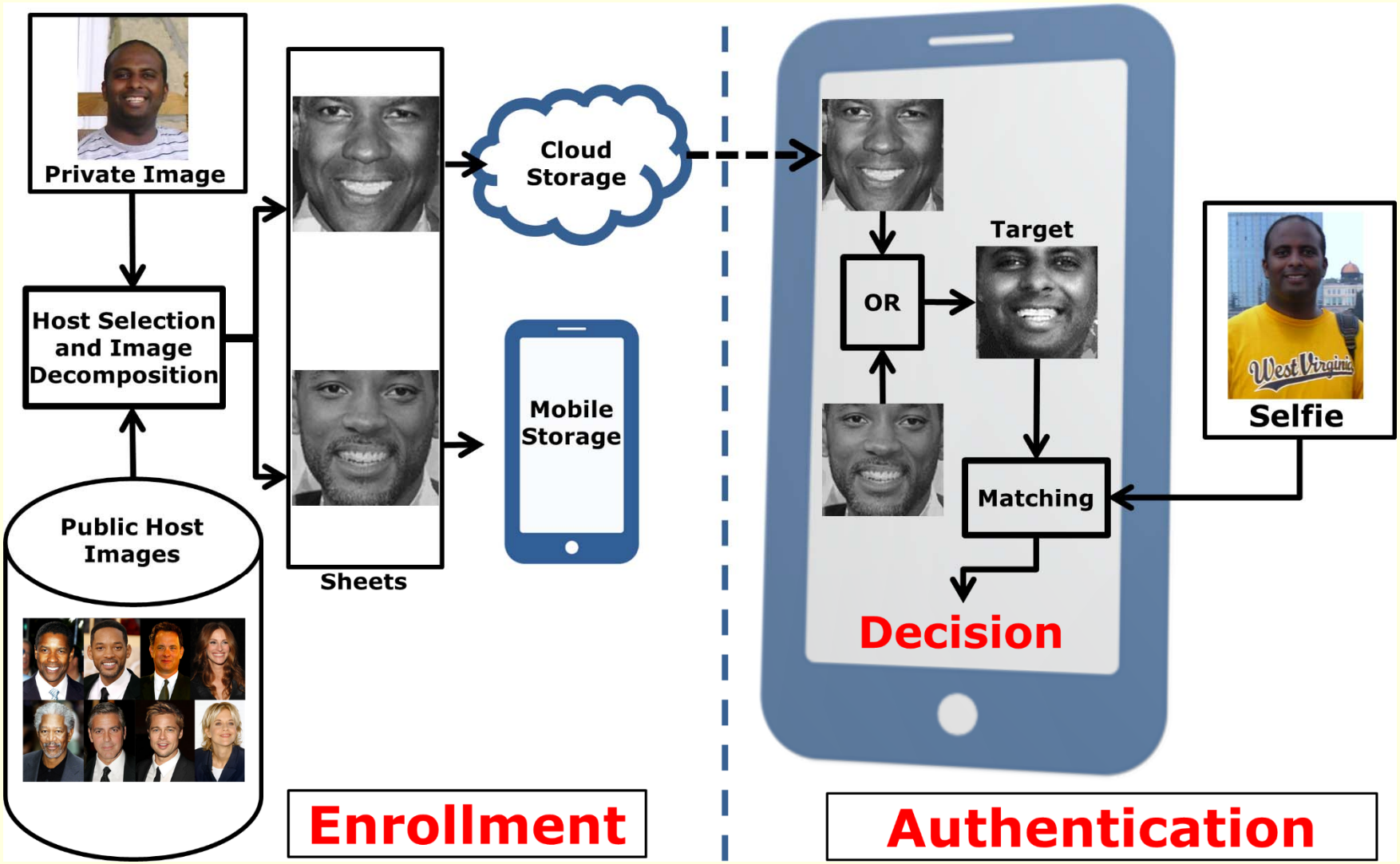
- The original image is encrypted into two dynamically selected host images



Face Privacy: Results

- Method to protect privacy of face images by decomposing it into two independent host (public) face images
- Original face image can be reconstructed only when both host images are available
- Either host image does not expose the identity of the original face image

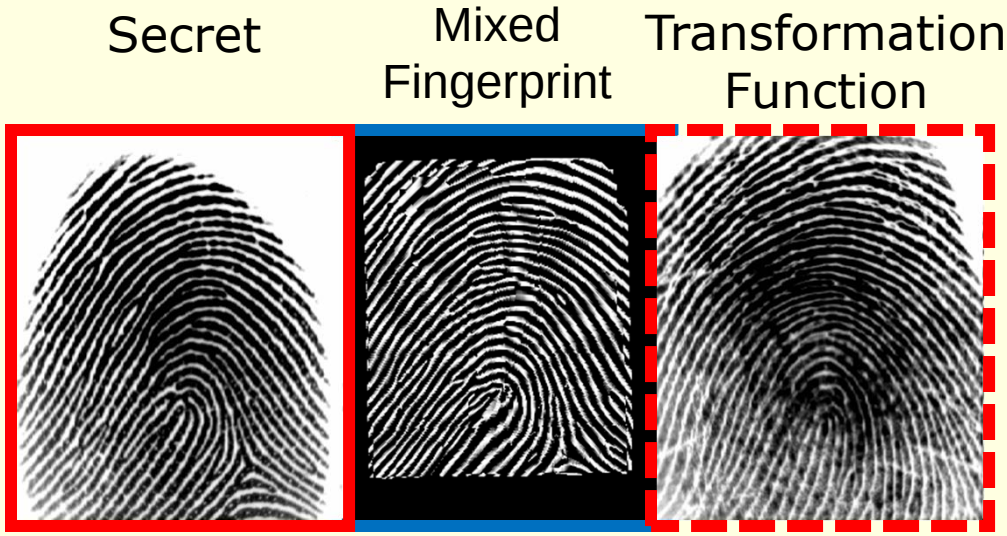
Application



Mixing Fingerprints

- An input fingerprint image is mixed with another fingerprint (e.g., from a different finger)
  - produces a new mixed fingerprint image that obscures the identity of the original fingerprint
- We consider the problem of mixing two fingerprint images in order to generate a new cancelable fingerprint image

Mixing Fingerprints



- Mixing fingerprints creates a new entity that looks like a plausible fingerprint:
  - It can be processed by conventional fingerprint algorithms
  - An intruder may not be able to determine if a given fingerprint is mixed or not

Hologram Model

- The ridge flow of a fingerprint can be represented as a 2D Amplitude and Frequency Modulated (AM-FM) signal:

Realistic appearance

$$I(x, y) = a(x, y) + b(x, y)*\cos[\Psi(x, y)] + n(x, y)$$

Ridges and minutiae

K. G. Larkin and P. A. Fletcher. A coherent framework for fingerprint analysis: are fingerprints holograms? Opt. Express, 15(14):8667–8677, 2007.

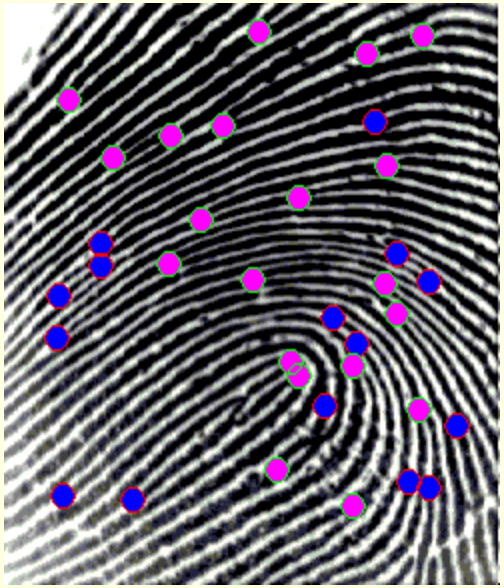
Helmholtz Decomposition

- Based on the Helmholtz Decomposition theorem, the phase **Ψ(x, y)** can be uniquely decomposed into two components:

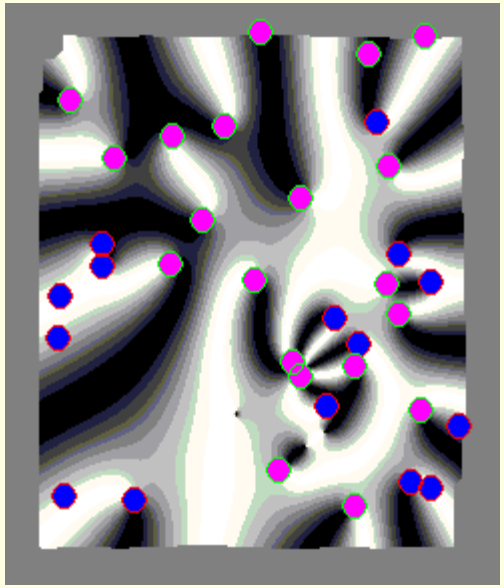
$$\Psi(x, y) = \Psi c(x, y) + \Psi s(x, y)$$

- The continuous component, **Ψc(x, y)**, defines the local ridge orientation
- The spiral component, **Ψs(x, y)**, characterizes the minutiae locations

Fingerprint Decomposition



Original



Spiral Phase

Continuous Phase

Mixing Fingerprints

- Let F_1 and F_2 be two different fingerprint images from different fingers, and let $\boldsymbol{\Psi c_i(x, y)}$ and $\boldsymbol{\Psi s_i(x, y)}$ be the pre-aligned continuous and spiral phases, i = 1,2.

$$MF_1 = \cos[\Psi c_2(x, y) + \Psi s_1(x, y)]$$

$$MF_2 = \cos[\Psi c_1(x, y) + \Psi s_2(x, y)]$$

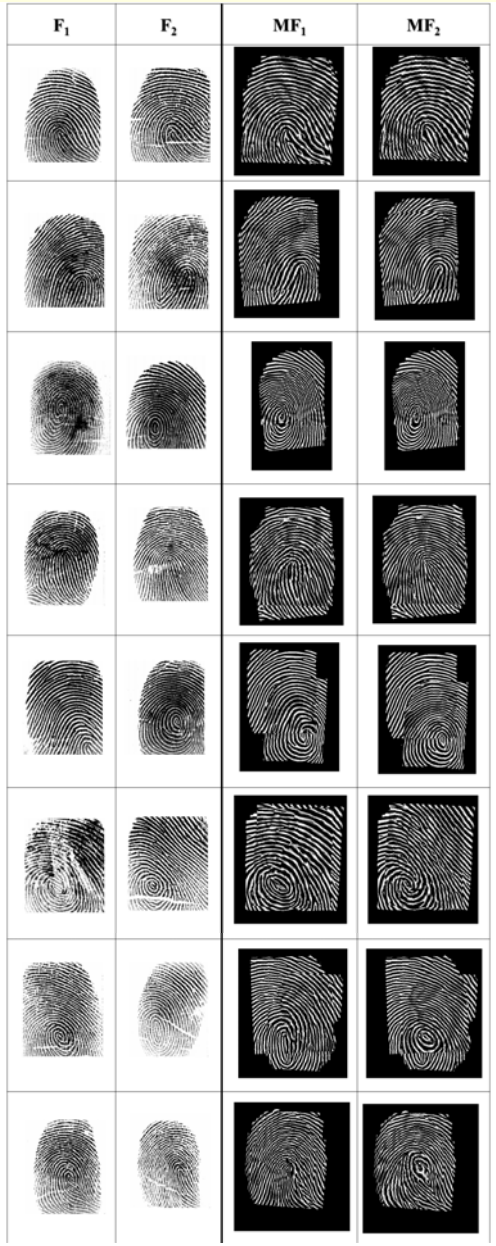
- The continuous phase of F_2 is combined with the spiral phase of F_1 which generates a new fused fingerprint image $\boldsymbol{MF_1}$

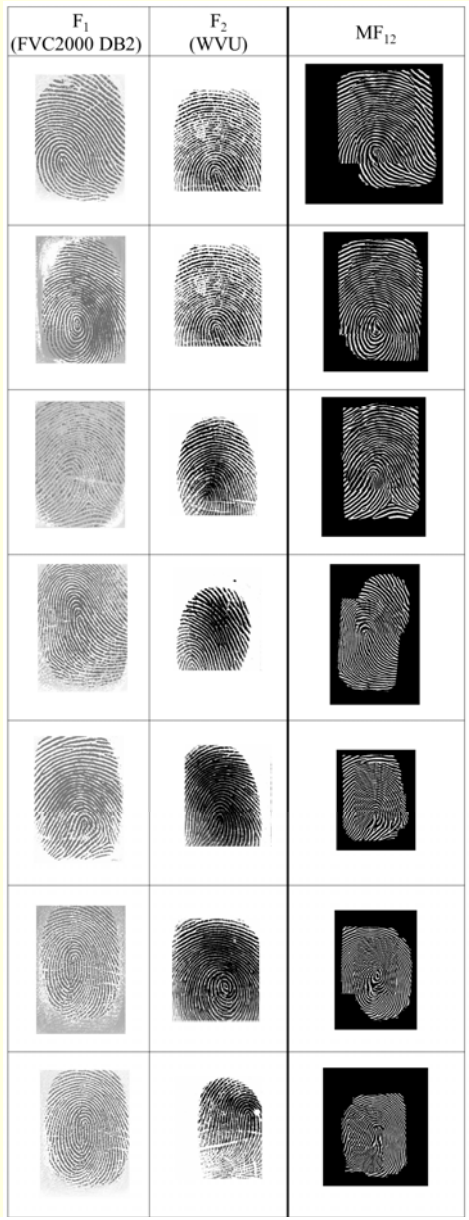
Mixed Fingerprint Images

F_1 (FVC2000 DB2)	F_2 (WVU)	MF_1
		
		
		
		

Mixed Fingerprints

WVU with WVU





WVU with FVC

Mixing Fingerprints: Results

- Can the mixed fingerprint be used as a new biometric identity? (Yes)
- Are the original fingerprint and the mixed fingerprint correlated? (No)
- Does mixing result in cancelable templates? (Yes)
- If two different fingerprints are mixed with a common fingerprint, are the mixed fingerprints similar? (No)

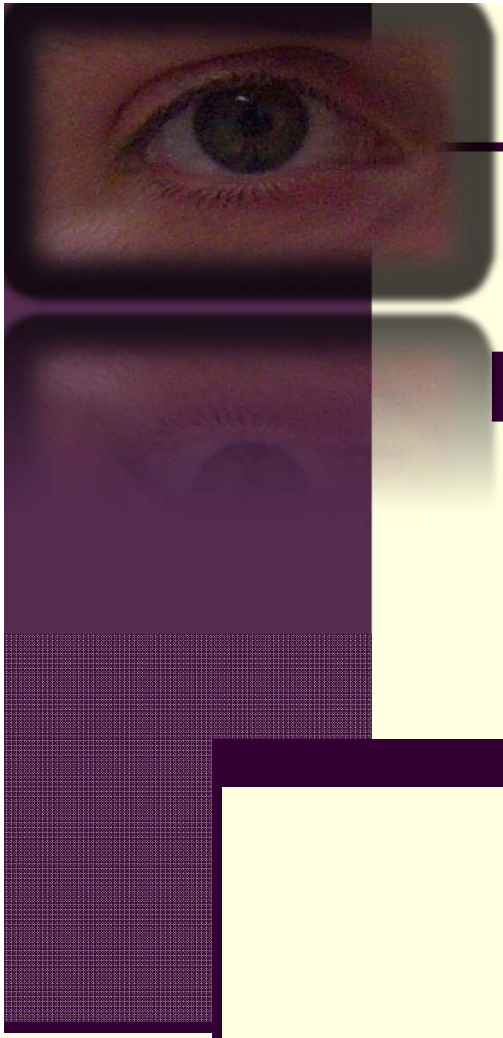
Summary

- Visual Cryptography for decomposing a face and storing it in two separate servers
  - Individual servers cannot identify the face
- Mixing fingerprints by combining the spiral and continuous phase components of two fingerprint images
  - Cancellable fingerprints
  - Joint identity/Group Authentication

Publications

[Funded by NSF CAREER Award]

- A. Ross and A. Othman, "Visual Cryptography for Biometric Privacy," IEEE Transactions on Information Forensics and Security (TIFS), Vol. 6, Issue 1, pp. 70 - 81, March 2011
- A. Othman and A. Ross, "On Mixing Fingerprints," IEEE Transactions on Information Forensics and Security, Vol. 8, Issue 1, pp. 260 - 267, January 2013
- A. Ross and A. Othman, "Mixing Fingerprints for Template Security and Privacy," Proc. of the 19th European Signal Processing Conference (EUSIPCO), (Barcelona, Spain), August/September 2011
- A. Othman and A. Ross, "Mixing Fingerprints For Generating Virtual Identities," Proc. of IEEE International Workshop on Information Forensics and Security (WIFS), (Foz do Iguacu, Brazil), November/December 2011



De-identifying biometric images for enhancing privacy and security

Arun Ross

Associate Professor

Michigan State University

rossarun@cse.msu.edu

[Work done with Asem Othman]

http://www.cse.msu.edu/~rossarun