Carnegie Mellon CyLab
4616 HENRY STREET
PITTSBURGH, PA 15213
PH: (412) 268-7195
FX: (412) 268-7196
www.cylab.cmu.edu

Introduction to Biometric Technologies and Applications

Prof. Marios Savvides

ECE & CyLab, Carnegie Mellon University
Marios.Savvides@ri.cmu.edu

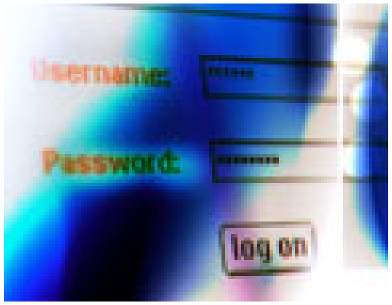
What are Biometrics?

- The term "biometrics" is derived from the Greek words bio (life) and metric (to measure).
- For our use, biometrics refers to technologies for measuring and analyzing a person's physiological or behavioral characteristics. These characteristics are unique to individuals hence can be used to verify or identify a person.

Also Look at report by *Duane M. Blackburn, Federal Bureau of Investigation*
http://www.biometricscatalog.org/biometrics/biometrics_101.pdf or biometrics_101.pdf

Problems with current security systems…

- Based on Passwords, or ID/Swipe cards
- Can be Lost.
- Can be forgotten.
- Worse! Can be stolen and used by a thief/intruder to access your data, bank accounts, car etc….



Some statistics on User/Passwords

- Case Study: Telesis Community Credit Union(CA), a California based financial services provider that manages $1.2 billion in assets.
- The VP of IT, lead a team to run a network password cracker as part of an enterprise security audit last year to see if employees were following Telesis' password policies.
- Result: They were far from doing so…..

http://www.computerworld.com/securitytopics/security/story/0,10801,101557,00.html

Some statistics on User/Passwords

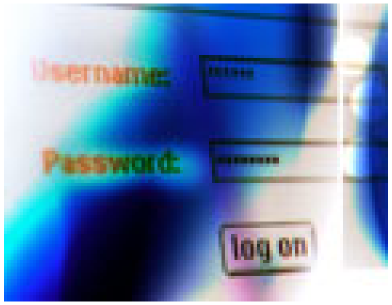
- In fact within **30 seconds** the team was able to identify 80% of people’s passwords!
- The team asked employees to change their passwords and comply with password policies.
- A few days later, the IT team run their password cracking exercise again….
- This time they still were able to crack 70% of the passwords!

Problems with current security systems…

- With increasing use of IT technology and need to protect data, we have multiple accounts/passwords.
- We can only remember so many passwords, so we end up using things we know to create them (birthdays, wife/girlfriends name, dog, cat…)
- Its is easy to crack passwords, because most of our passwords are weak!
- If we create strong passwords (that should be meaningless to us) we will forget them! And there is no way to remember multiple such passwords

Good rules to follow when creating passwords

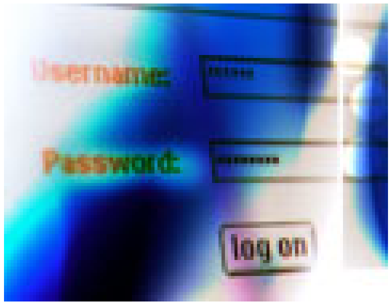
http://csrc.nist.gov/fasp/FASPDocs/id-authentication/July2002.pdf



Many problems with current security authentication systems…

ANSWER:

USE BIOMETRIC TECHNOLOGY



Some Examples of Different Biometrics

- Face
- Fingerprint
- Voice
- Palmprint
- Hand Geometry
- Iris
- Retina Scan
- Voice
- DNA
- Signatures
- Gait
- Keystroke

Applications + Terminology

- **Identification**:
  - Match a person’s biometrics against a database to figure out his identity by finding the closest match.
  - Commonly referred to as 1:N matching
  - ‘Criminal Watch-list’ application scenarios

Applications + Terminology

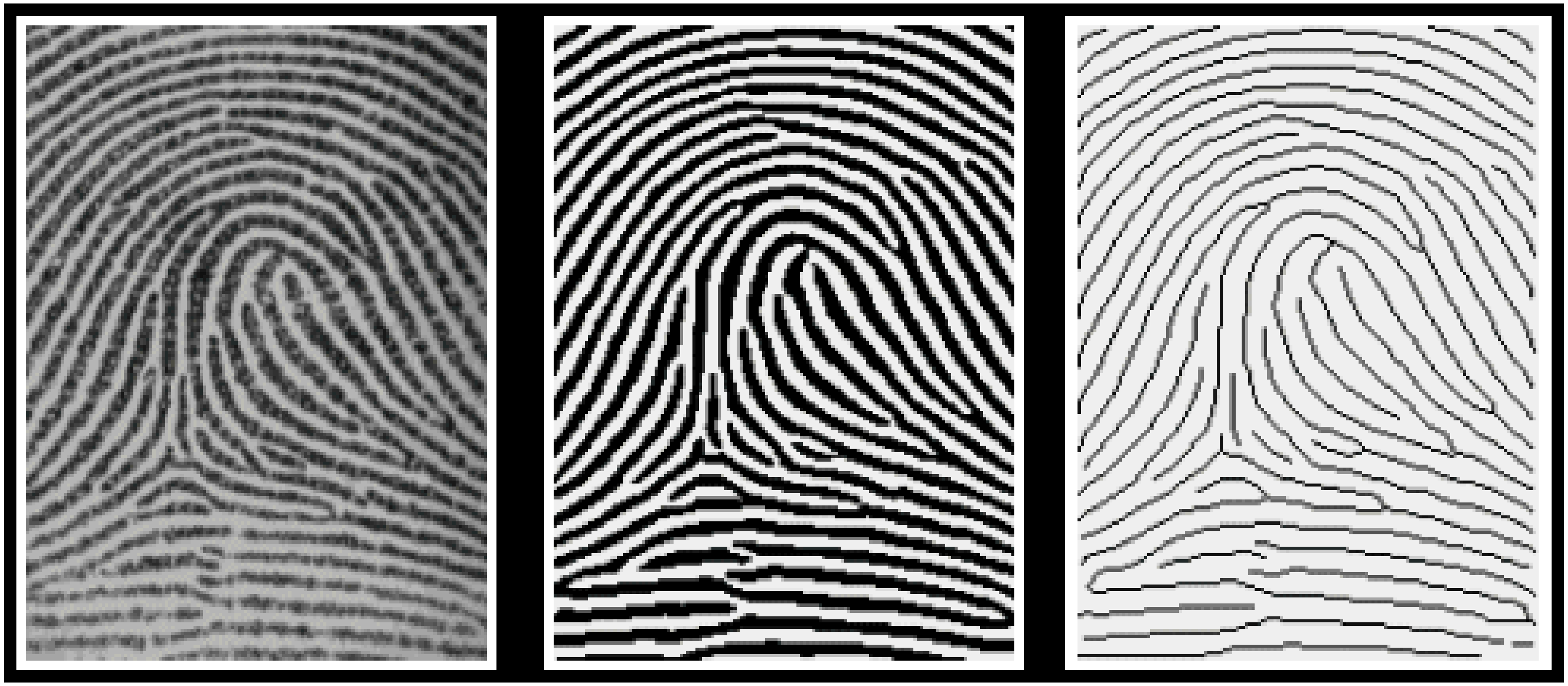
- **Verification**:
  - The person claims to be ‘John’, system must match and compare his/hers biometrics with John’s stored Biometrics.
  - If they match, then user is ‘verified’ or authenticated that he is indeed ‘John’
  - Access control application scenarios.
  - Typically referred as 1:1 matching.

Fingerprint Matching

Minutiae based fingerprint Matching

- This is one of the most commonly used algorithms for extracting features that characterizes a fingerprint.
- The different Minutiae feature locations and types can identify different individuals.
- These are what are stored in the Biometric template.
- Image & Signal processing used to process fingerprint images

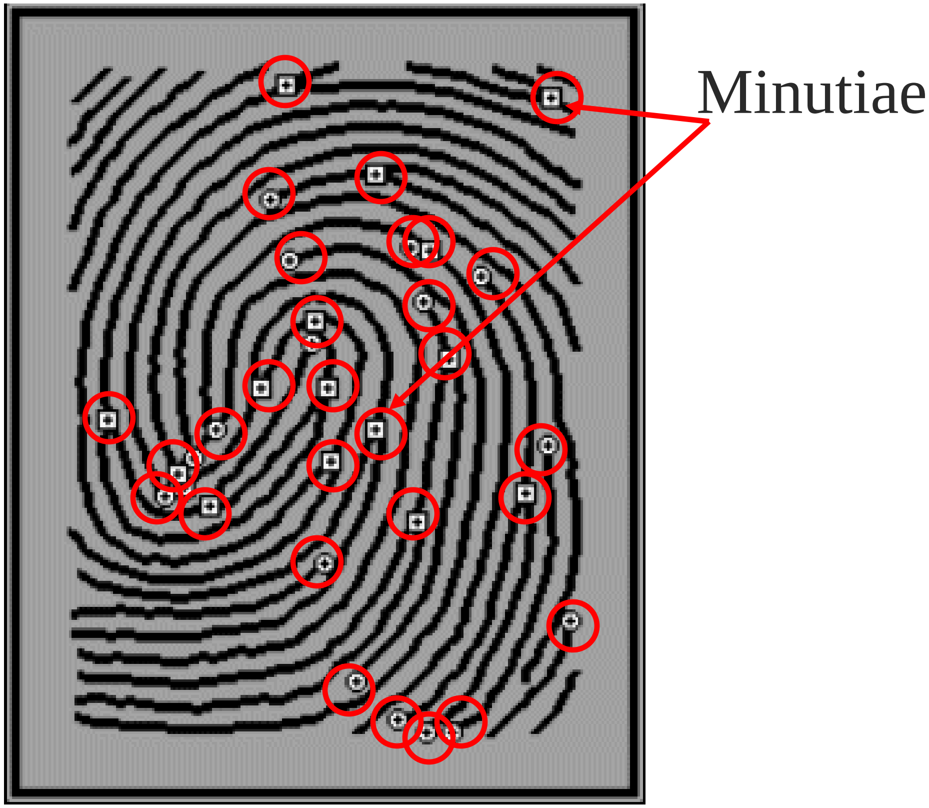
Fingerprint Minutiae Extraction



Original → Processed → Thinning

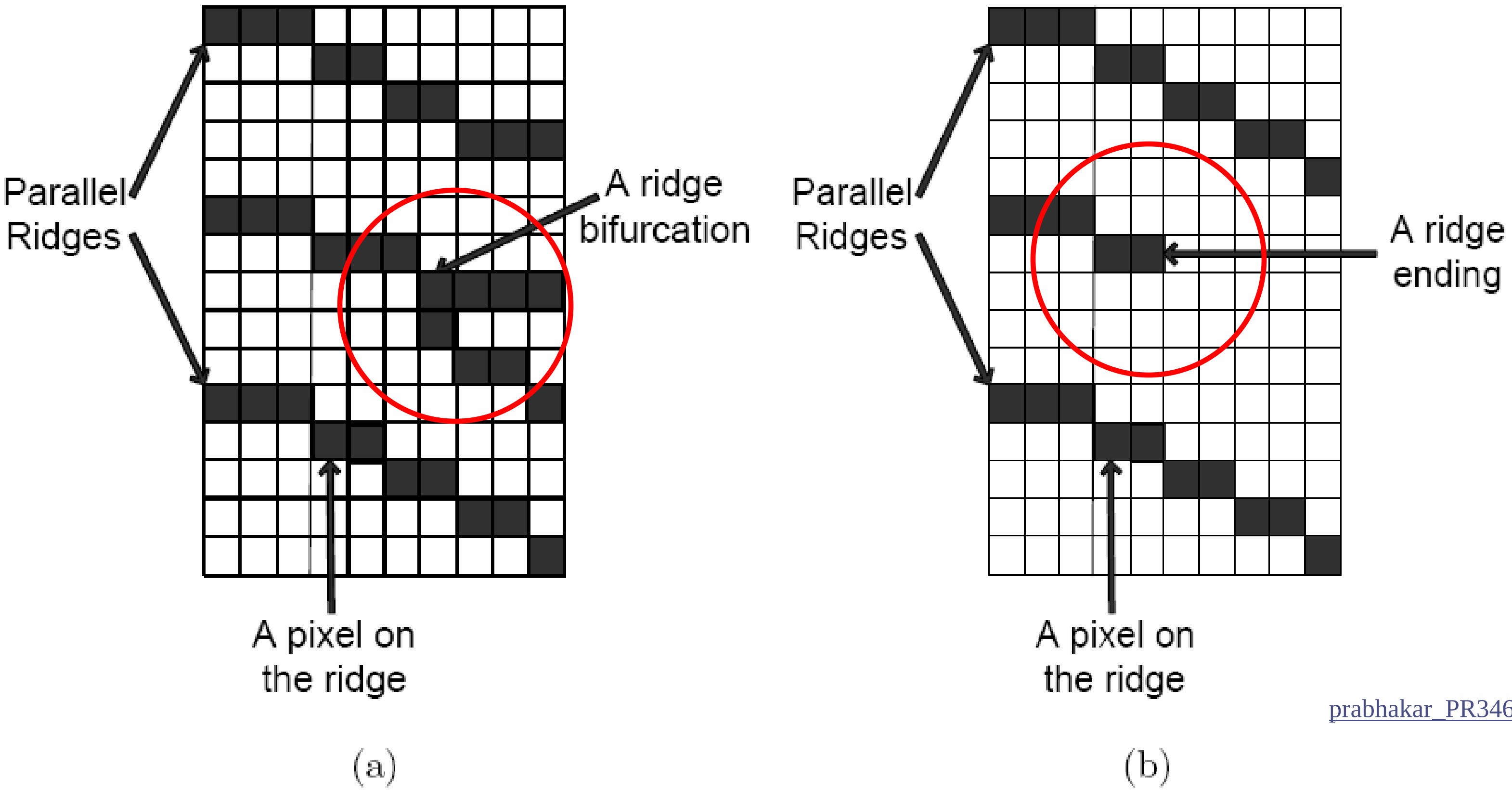
Fingerprint Minutiae Extraction

Original



Final Processed with
Fingerprint Minutiae Detected

Some example Minutiae types

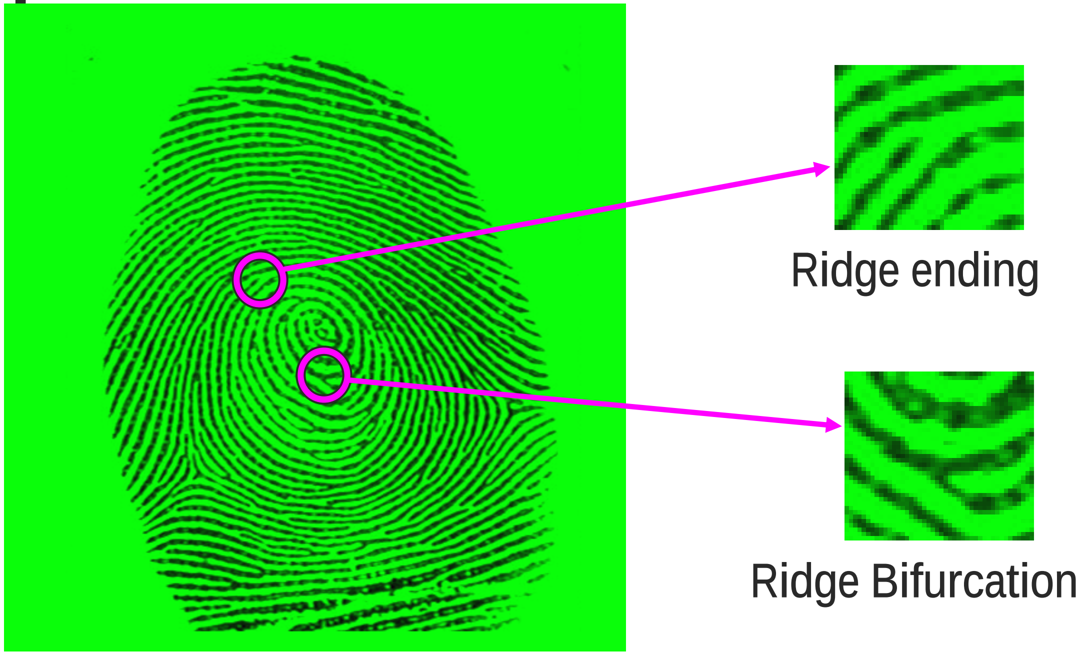


prabhakar_PR3465.pdf

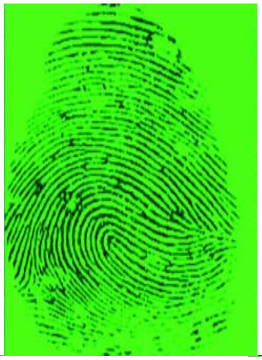
Ref: Salil Prabhakar, Anil K. Jain, Sharath Pankanti: Learning fingerprint minutiae location and type. Pattern Recognition 36(8): 1847-1857 (2003)

Fingerprint Biometric

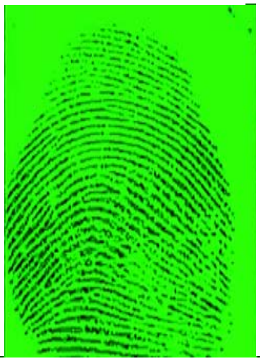
- Local features
  - Minutiae
    - Ridge endings
    - Ridge bifurcations



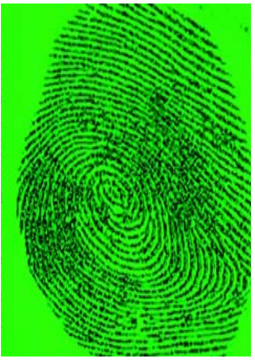
- Global features
  - Ridge orientation
  - Pattern of ridges



Left loop

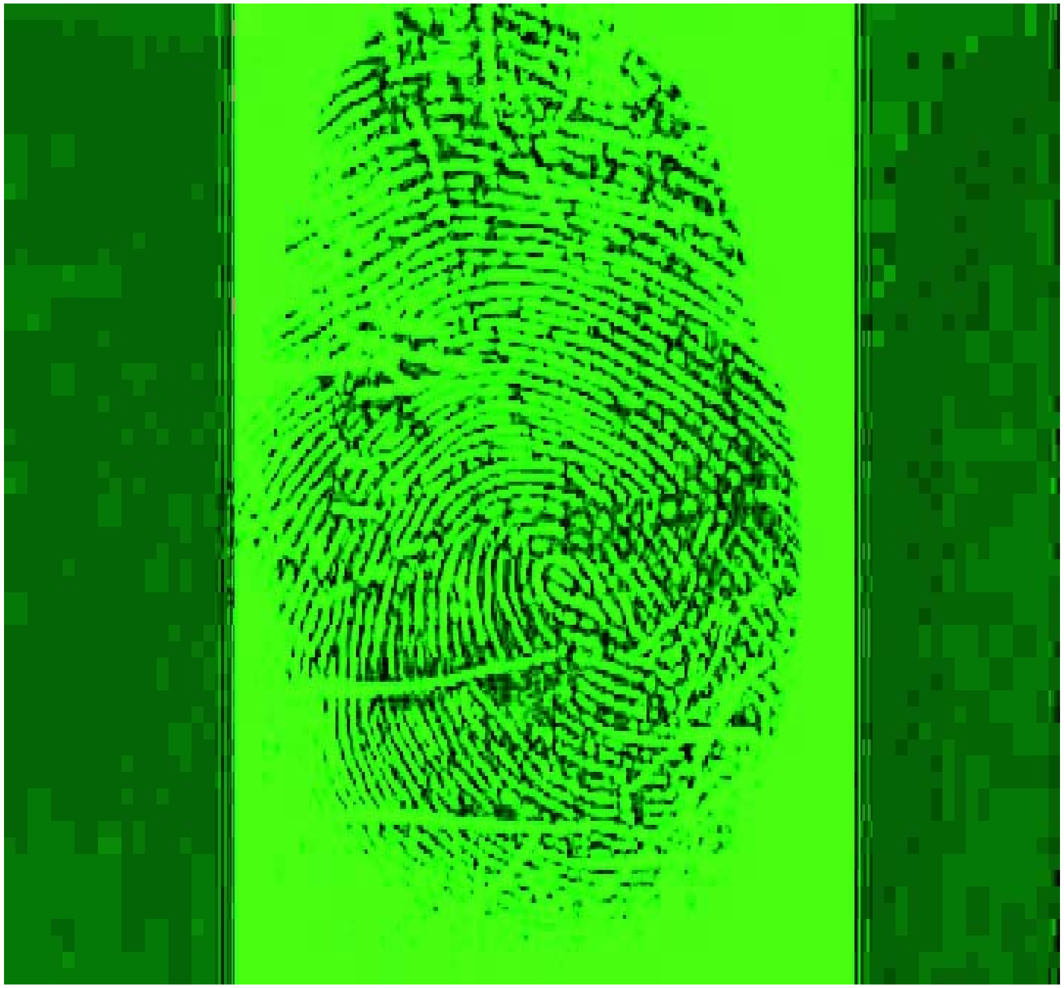


Arch



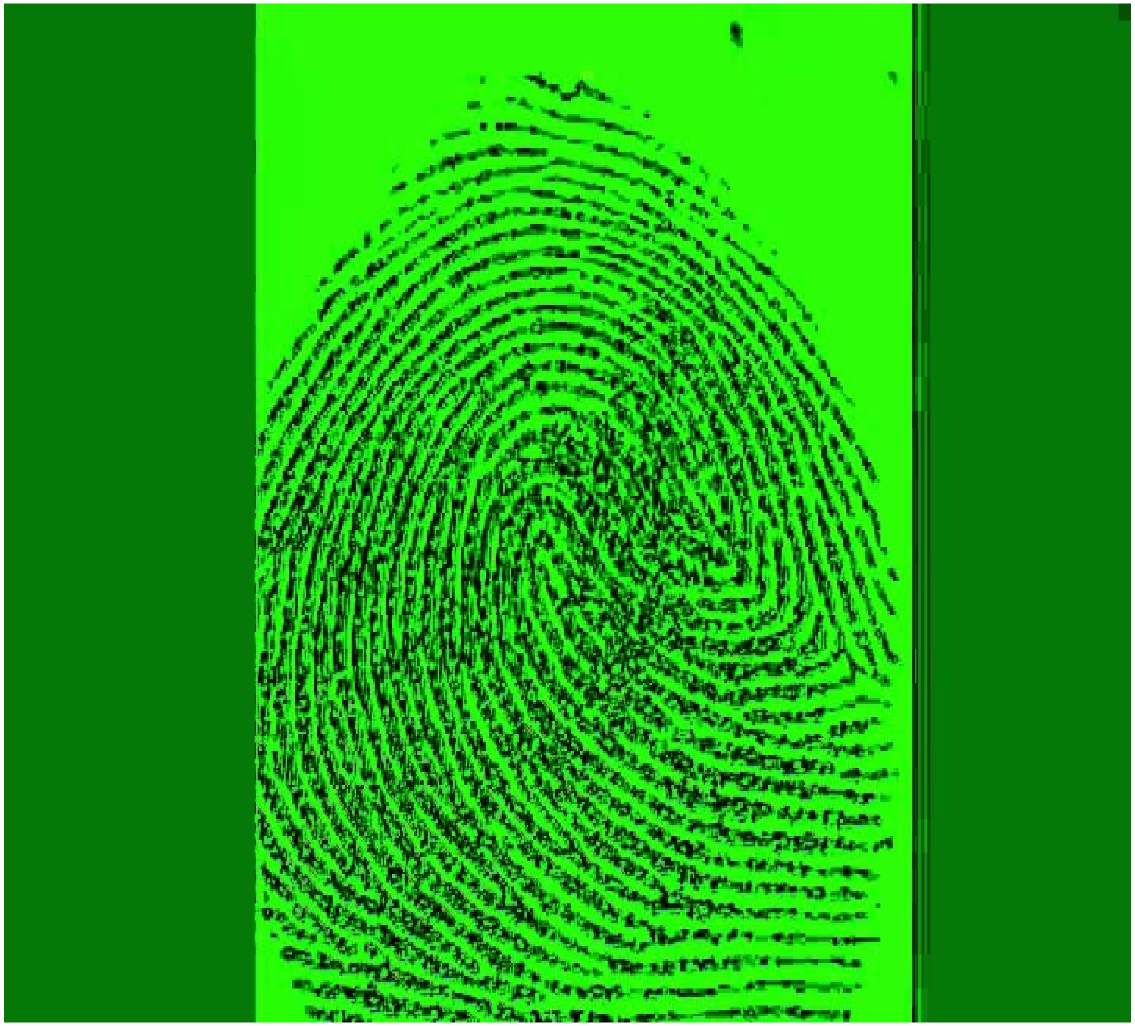
Whorl

NIST 24 database



- Class 3 – Small variation

NIST 24 database



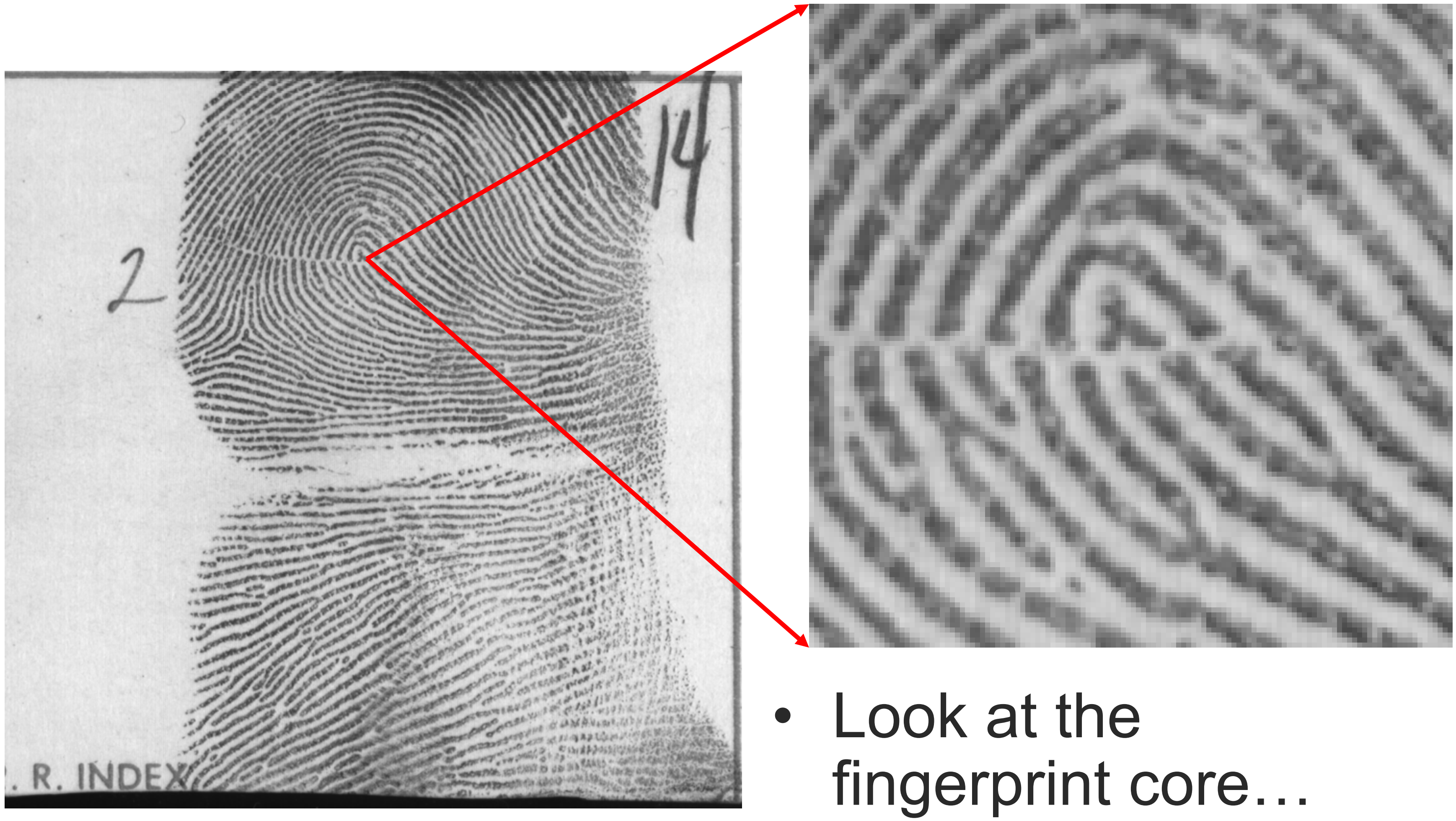
- Class 10 – Large Variation

Fingerprint Compression

Why do we need compression? We have gigabytes of storage right?

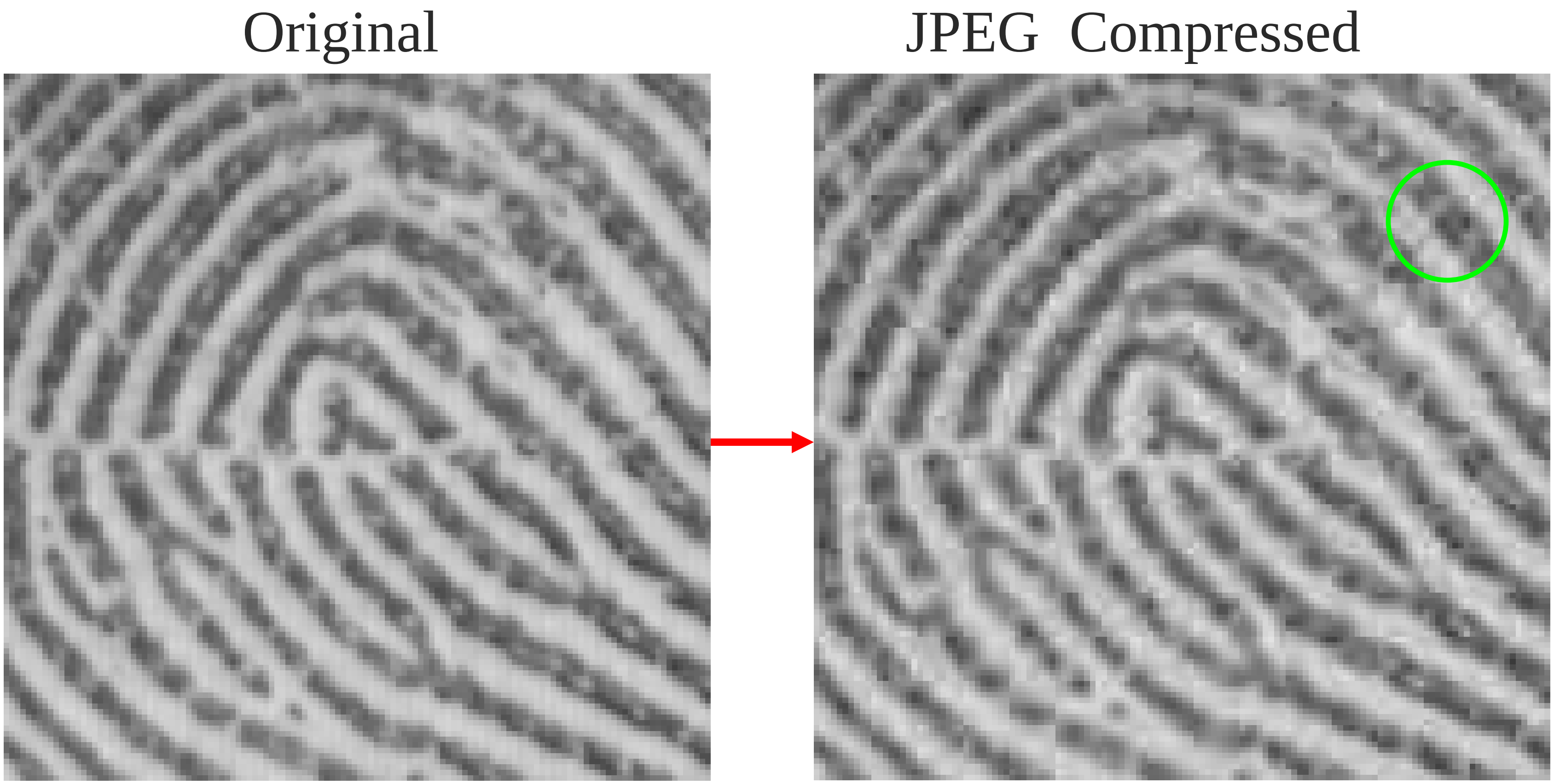
- FBI has been collecting fingerprint cards since 1924! Their collection has grown to over 200 million cards occupying an acre of filing cabinets in the J. Edgar Hoover building back in Washington!
- This includes some 29 million records they examine each time they're asked to `round up the usual suspects'!
- Need over 2,000 Terrabytes of storage..and this number is growing! 30,000-50,000 new cards per day!

Need to use Compression! But what type? Lets see the issues..



- Look at the fingerprint core…

Use JPEG compression (1:12.9)



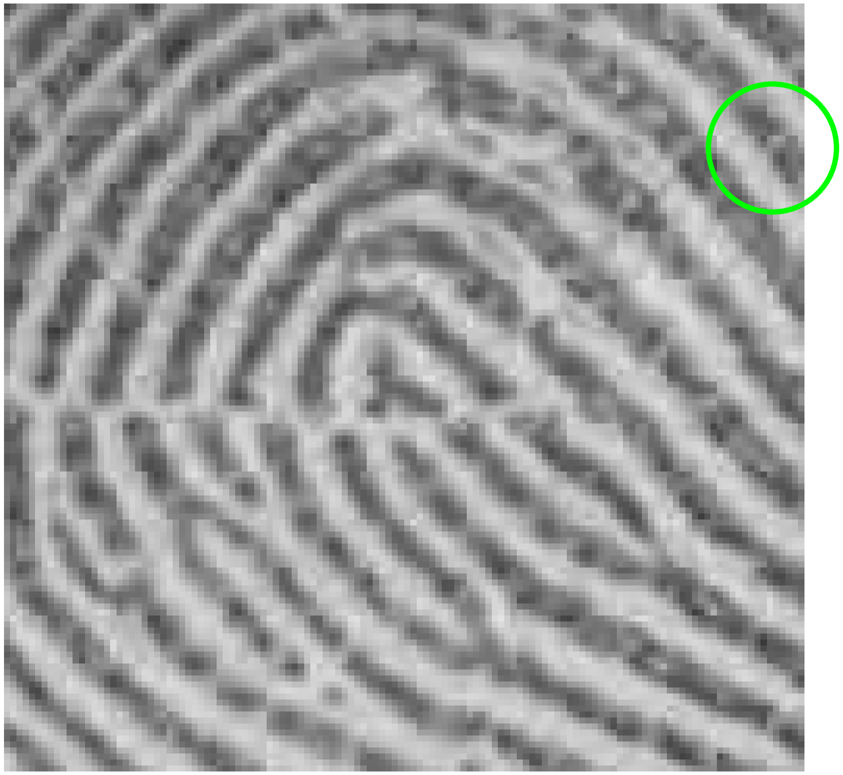
Original

JPEG Compressed

- JPEG compression has too many ‘blocky’ artifacts (it uses an 8x8/16x16 transform coder).

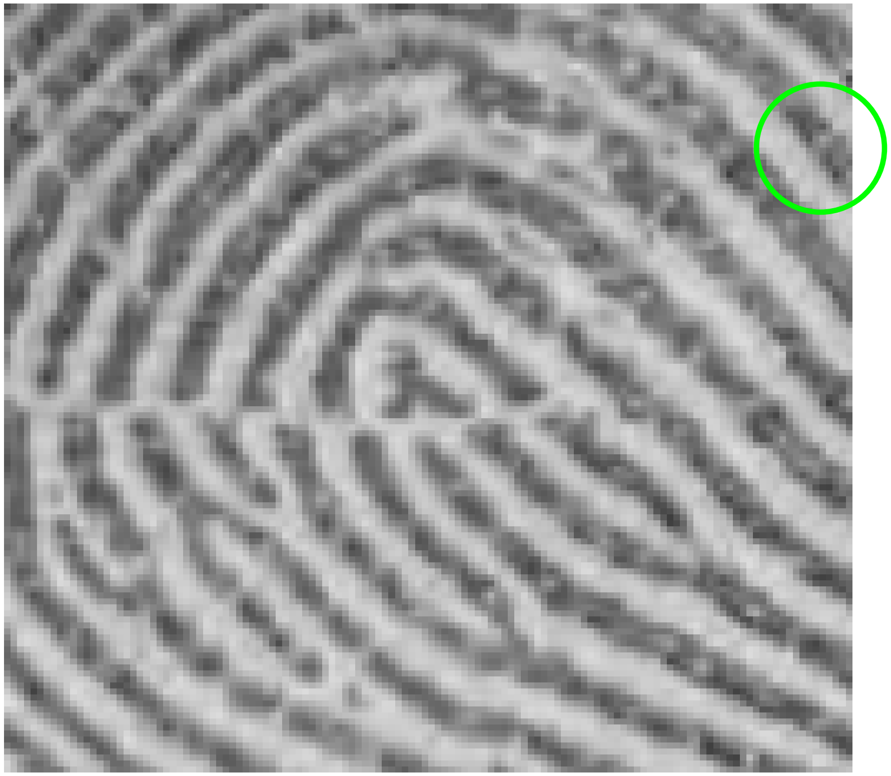
Use Wavelet Compression!

45,853 bytes



JPEG compressed

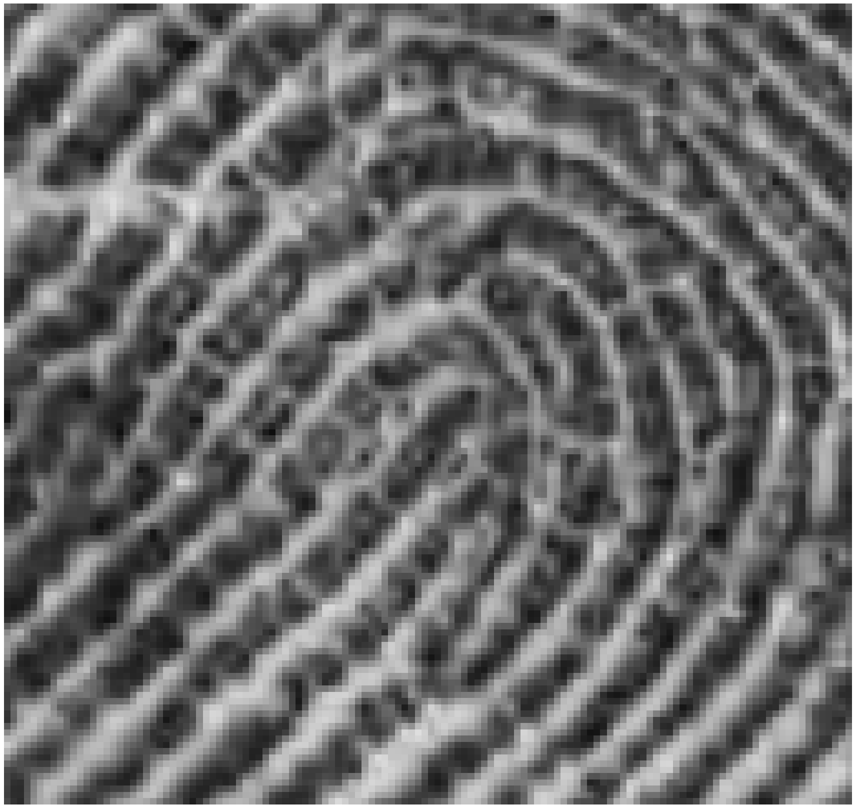
45,621 bytes



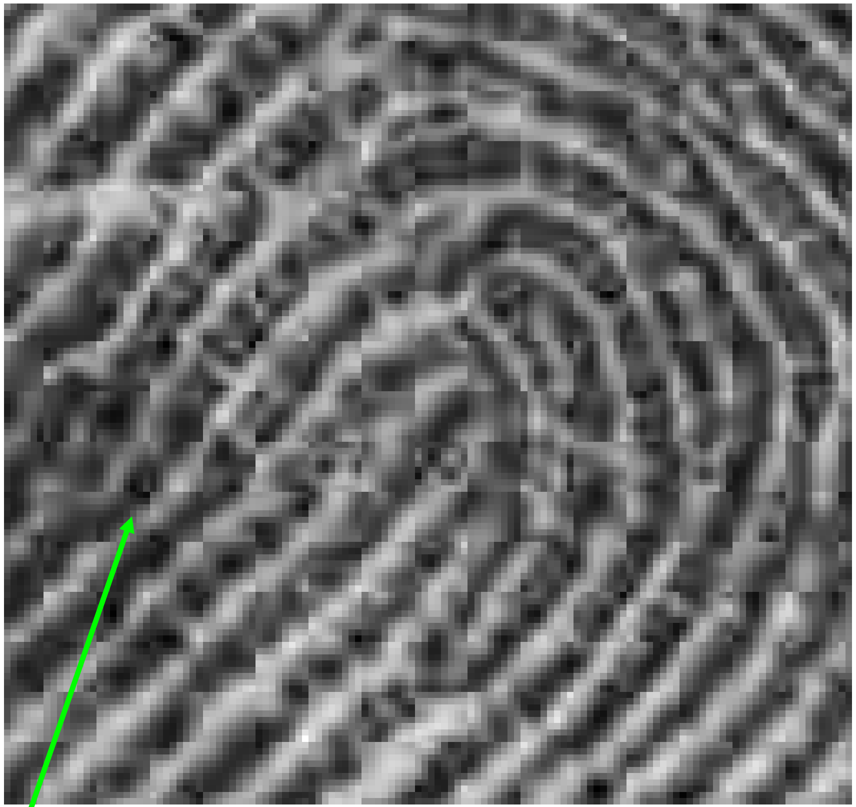
Wavelet Compression

Less compression artifacts!

Comparing Wavelet compression to JPEG at 0.6 bpp



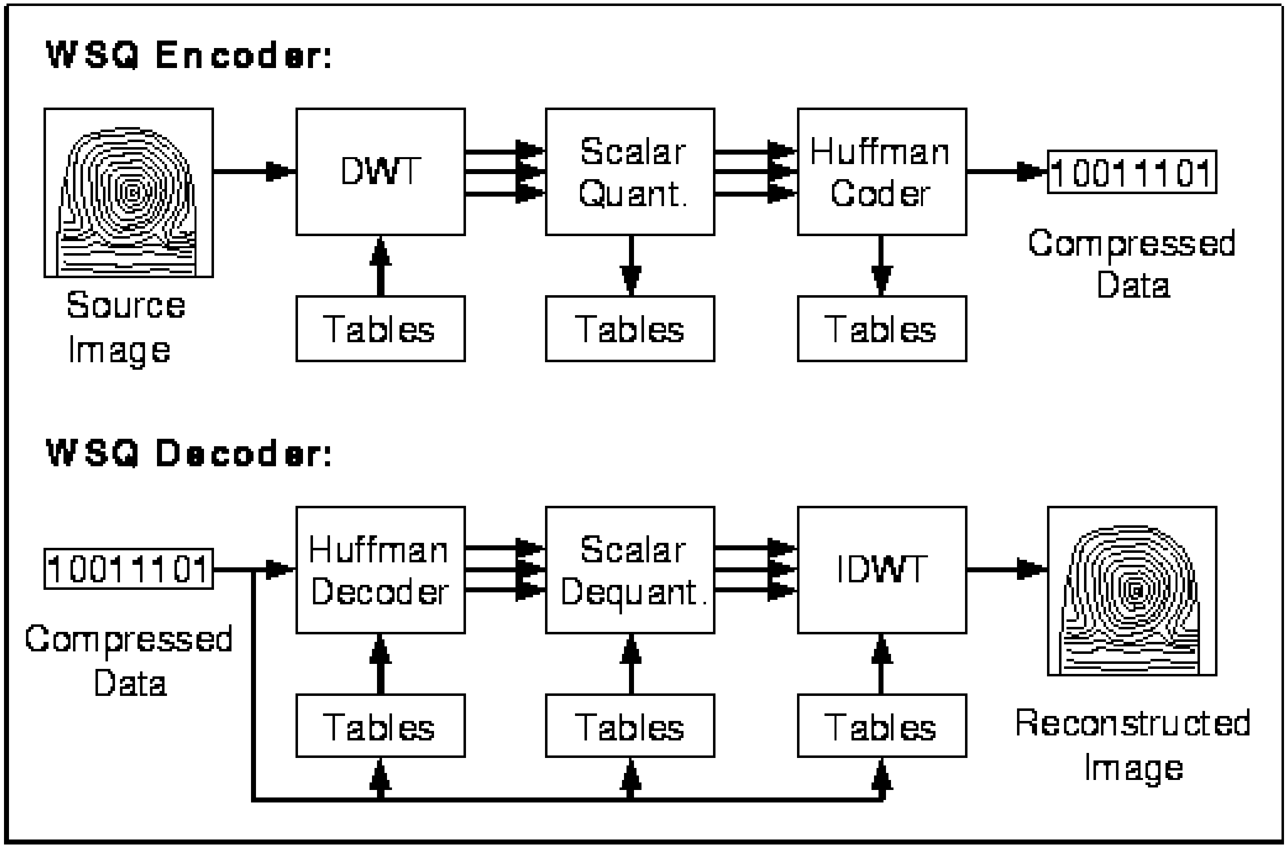
Wavelet Compression @ 0.6bpp



JPEG compression @ 0.6bpp

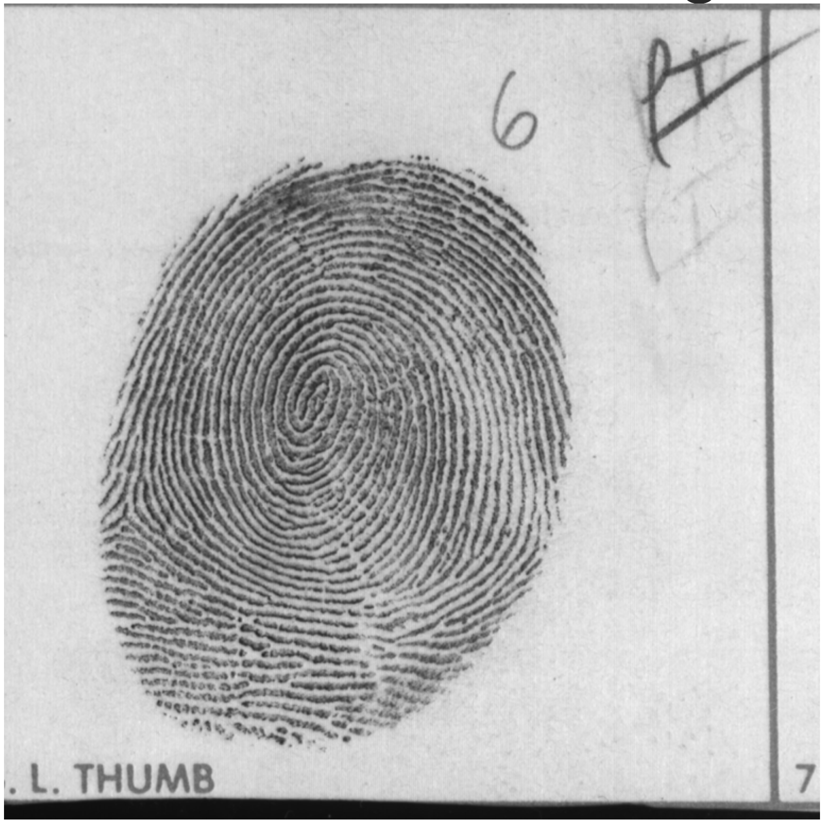
JPEG artifacts are more noticable now!

How it works?

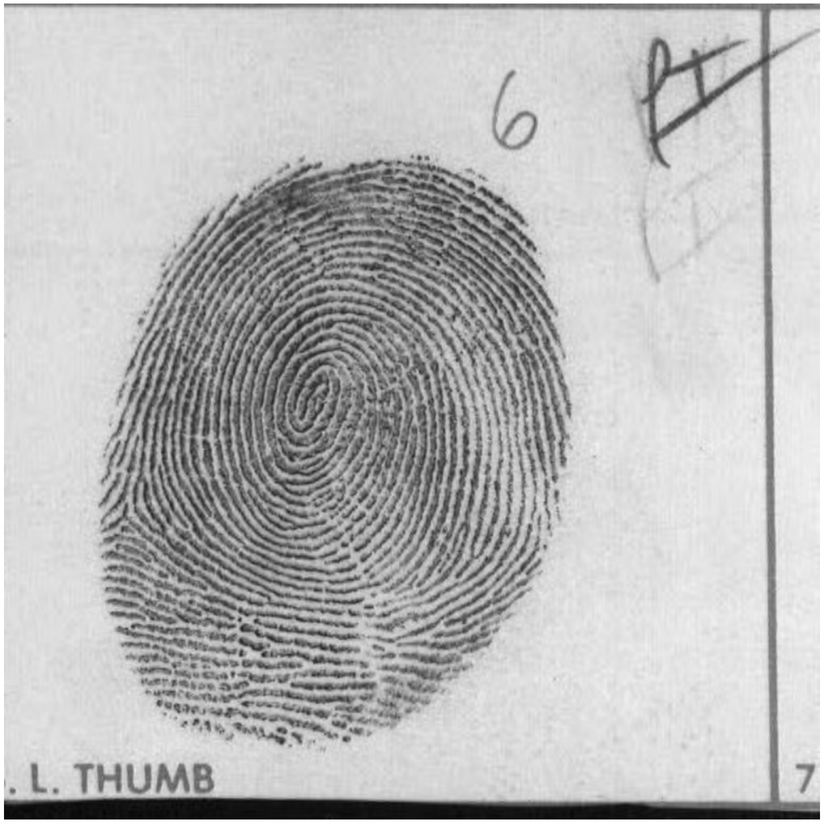


Source: http://www.c3.lanl.gov/~brislawn/FBI/FBI.html

Example of a Complete Fingerprint compressed using this method



Original Fingerprint



Wavelet reconstructed
(compressed at 0.75bpp)

Source: http://www.c3.lanl.gov/~brislawn/FBI/FBI.html

Liveliness Tests

- Possible solutions being explored:
  - – Measure temperature
  - – Measure current flow (inject a small voltage across the fingerprint)
  - – Use IR Led sensors to look for blood veins.

Fingerprint Sensors

Different Fingerprint Sensors

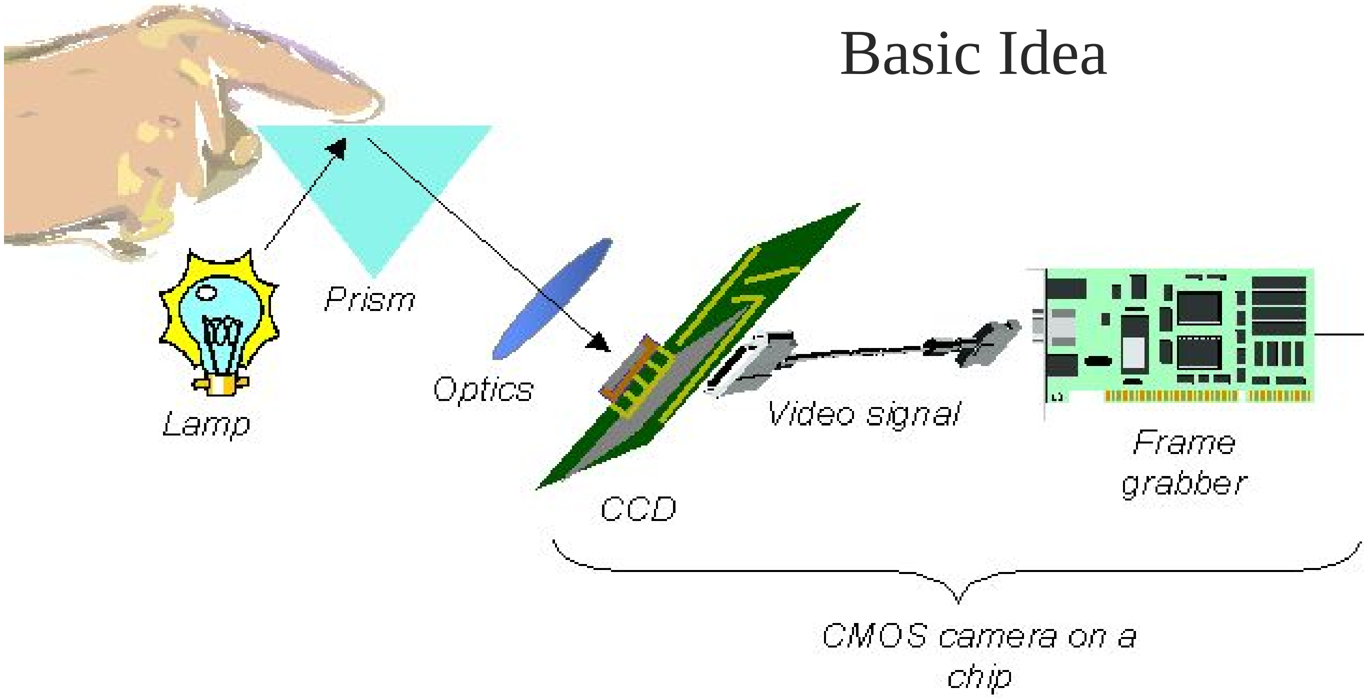
- Optical Sensors
  - Optic reflexive
  - Optic Transmissive
  - Fiber Optic Plate
- Capacitative/semiconductor Sensors
  - Static Capacitative I, II
  - Dynamic Capacitative
- Ultrasound sensors

Pros / Cons

- Semiconductor (capacitative) sensors are considered to be Low Cost. (but some are prone to ESD (Eletro-Static Discharge) problems over long term use.
- Optical Sensors are considered to have a high degree of stability and reliability. (No ESD problems), however are larger in size!
- Ultrasound Sensors are very precise and fraud-free but expensive to implement.

How Optical Sensors work

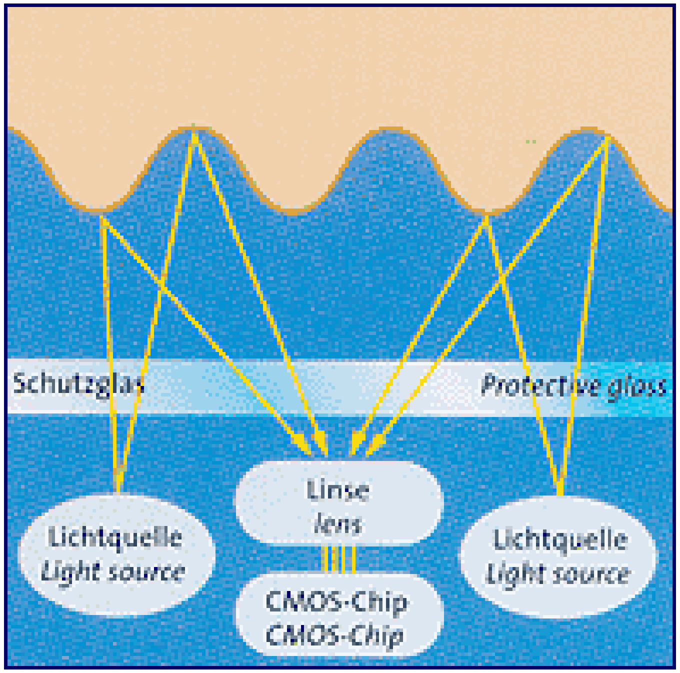
Basic Idea



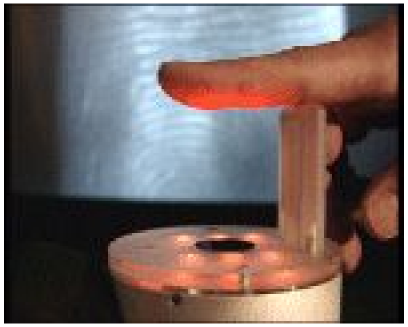
• Fingerprint touches the prism. It is illuminated from one side from the lamp and is transmitted to the CCD camera through the lens using total internal reflection.

- http://perso.wanadoo.fr/fingerchip/biometrics/types/fingerprint_sensors_physics.htm#thermal

Touchless (reflection) Fingerprint Sensors



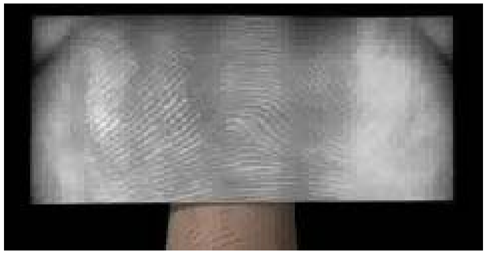
- Light is reflected from the fingerprint itself onto the CMOS sensor to form the fingerprint image.



- http://perso.wanadoo.fr/fingerchip/biometrics/types/fingerprint_sensors_physics.htm#thermal

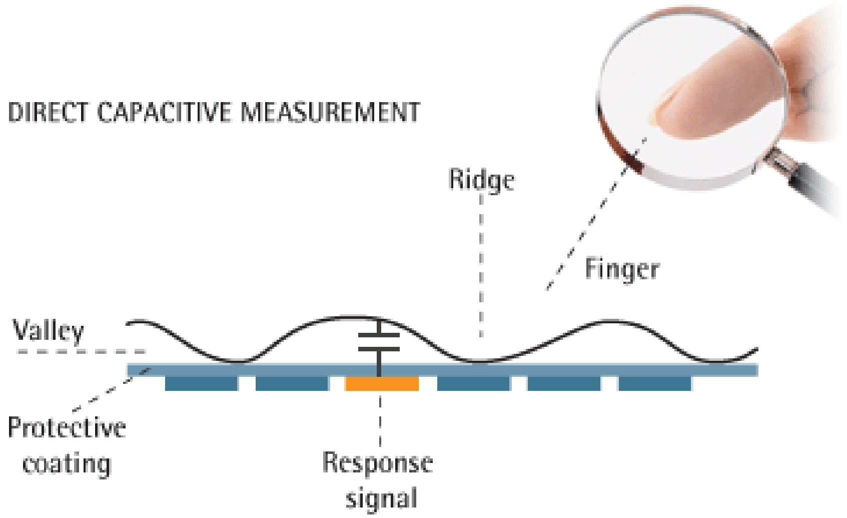
Touch-less Sensors can be used to provide a surround fingerprint

http://www.tbsinc.com/products/finger_sensor/index.php



- Surround Fingerprint is captured

Capacitative Sensors

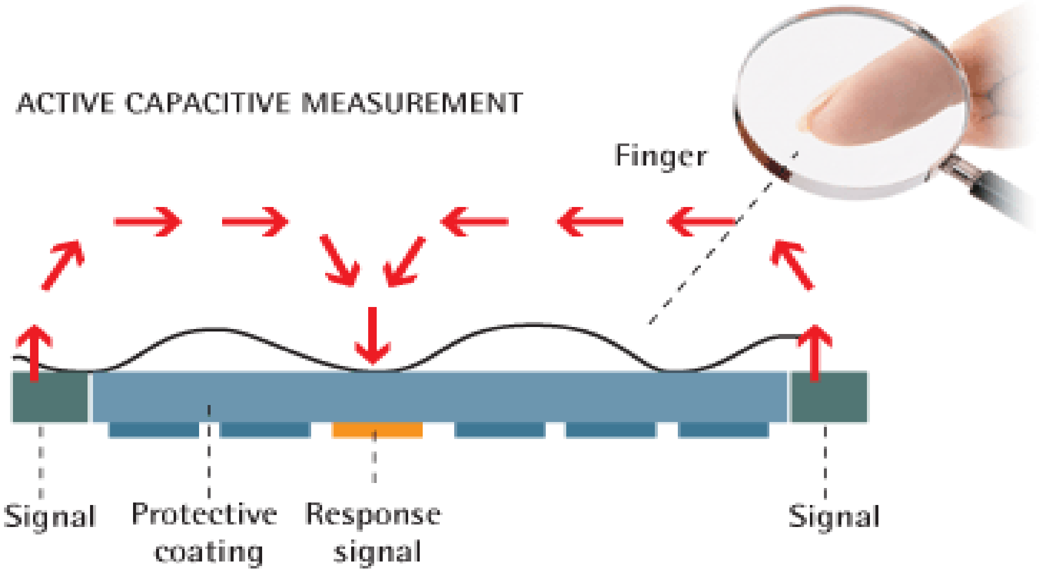


- These sensors measure the capacitance between the skin and the sensor to acquire fingerprints.

- Ridge and valleys of a fingerprint have different capacitance which provide a signature to output a fingerprint image.

- These sensors are typically very cheap but are prone to damage by electro-static discharge (ESD).

RF Field Fingerprint Sensors



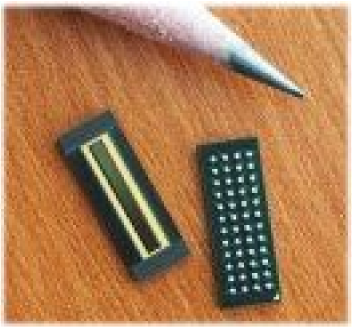
- A low radio frequency (RF) signal is injected into the finger, then read by the sensor array on silicon which act like receiver antennas.

- The signal strength at each antenna (or pixel) depends on the distance between the skin at that point and the sensor. This is how the image of the fingerprint is produced.

Companies with RF modulation sensing

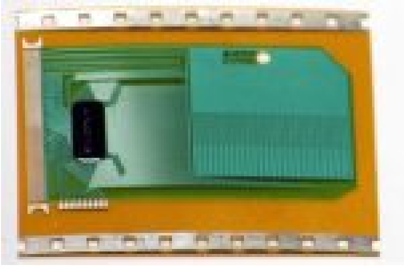
- Authentec:

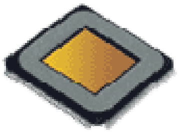
http://www.authentec.com/



- Fingerprint Cards:

http://www.fingerprint.se/page.asp?languageID=2





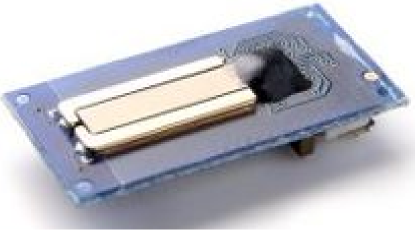
- Idex:

http://www.idex.no/x/Default.asp

- Validity:

http://www.validityinc.com/

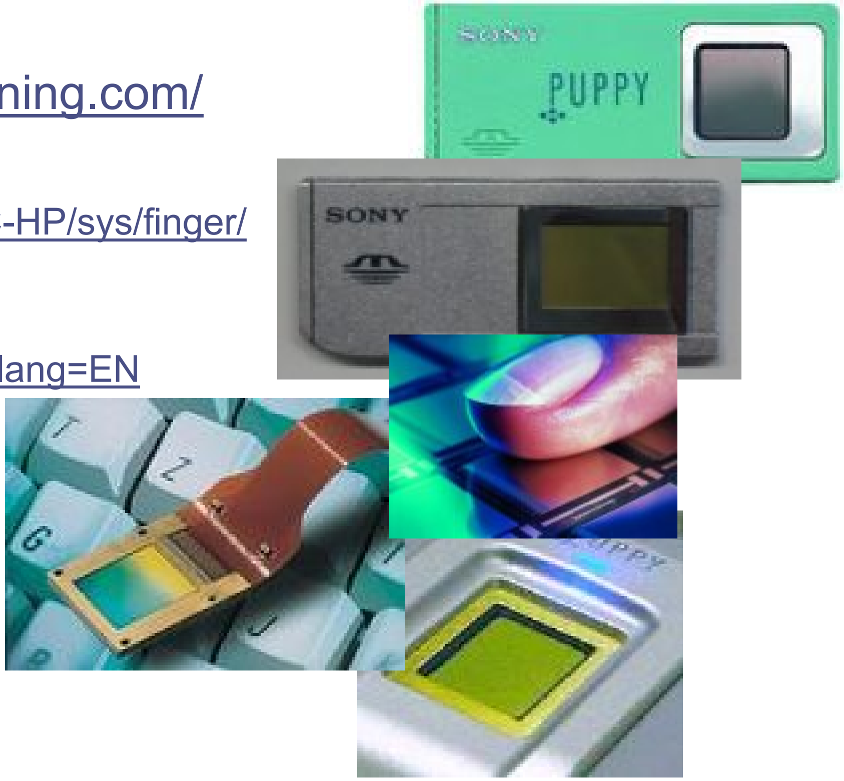
Swipe-sensor



Companies with Capacitative Sensors

- Upek (spin-off from ST-Microelectronics): www.upek.com

- Fujitsu: http://www.fma.fujitsu.com/biometric/
- LighTuning: http://www.lightuning.com/
- SONY: http://www.sony.net/Products/SC-HP/sys/finger/
- Infineon (formerly Siemens): http://www.infineon.com/cgi/ecrm.dll/jsp/home.do?lang=EN
- Atrua: http://www.atrua.com/index.html
- Melfas: http://www.melfas.com/

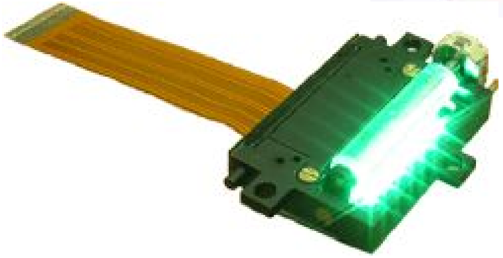


Companies with Optical Fingerprint Sensors

- TesTech (electro-optical)

http://www.testech.co.kr/

- Digital Persona



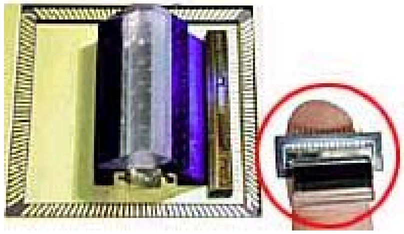
http://www.digitalpersona.com/

- CASIO:

http://www.casio.co.jp/ced/english/fingerprint.html

- **Sannaedle / Cecrop / Kinetic Sciences**

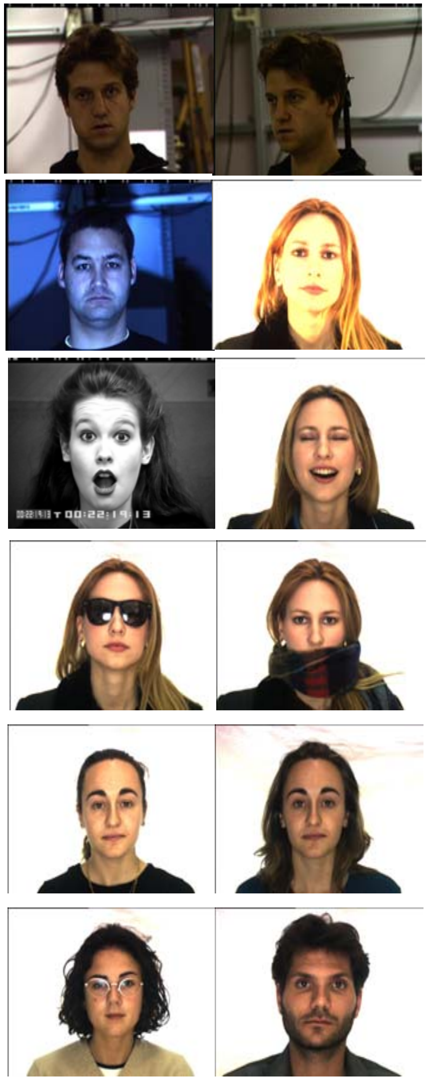
http://www.cecrop.com/



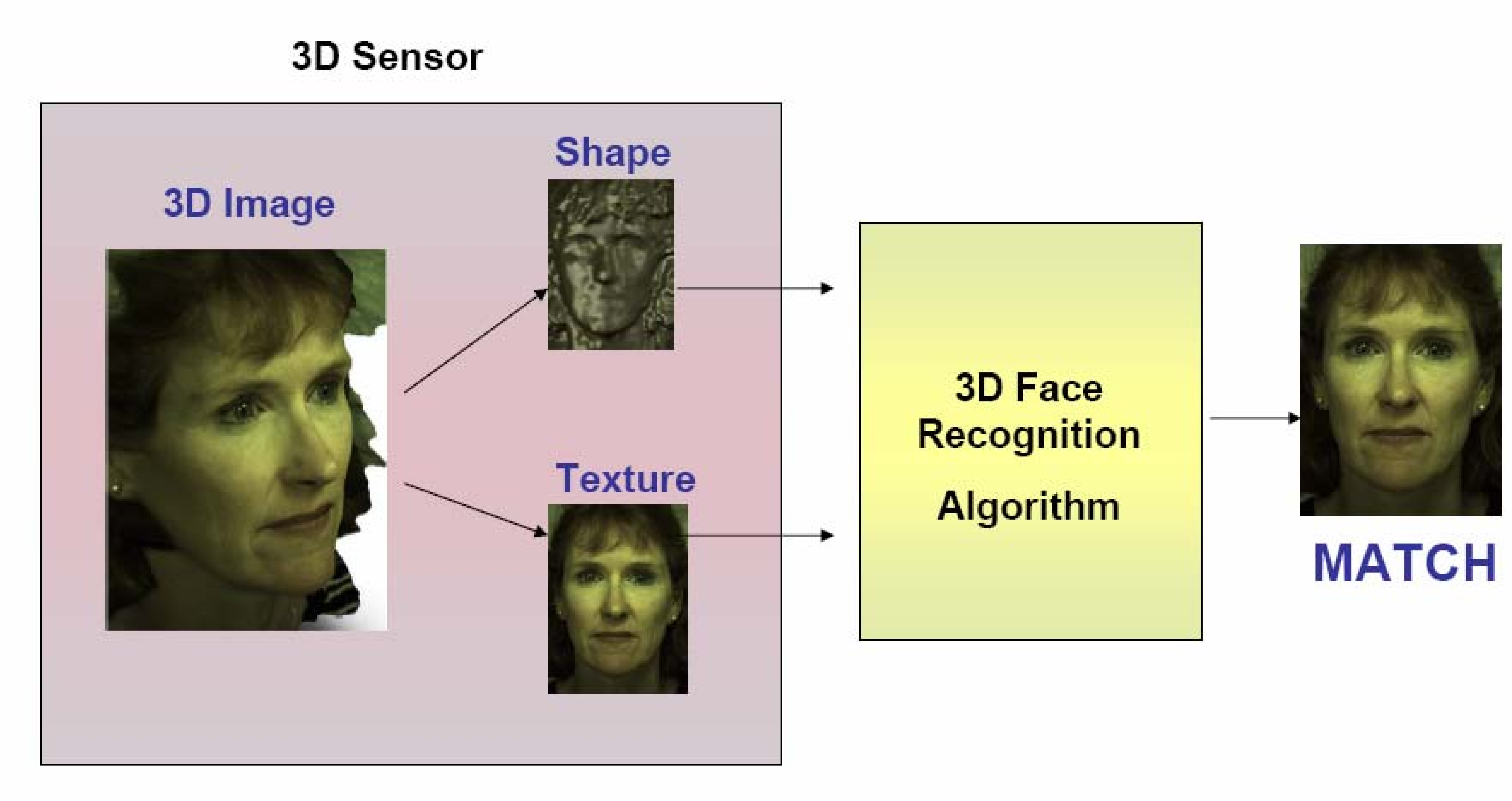
Face Recognition

Challenges in Face Recognition

- Pose
- Illumination
- Expression
- Occlusion
- Time lapse
- Individual factors: Gender

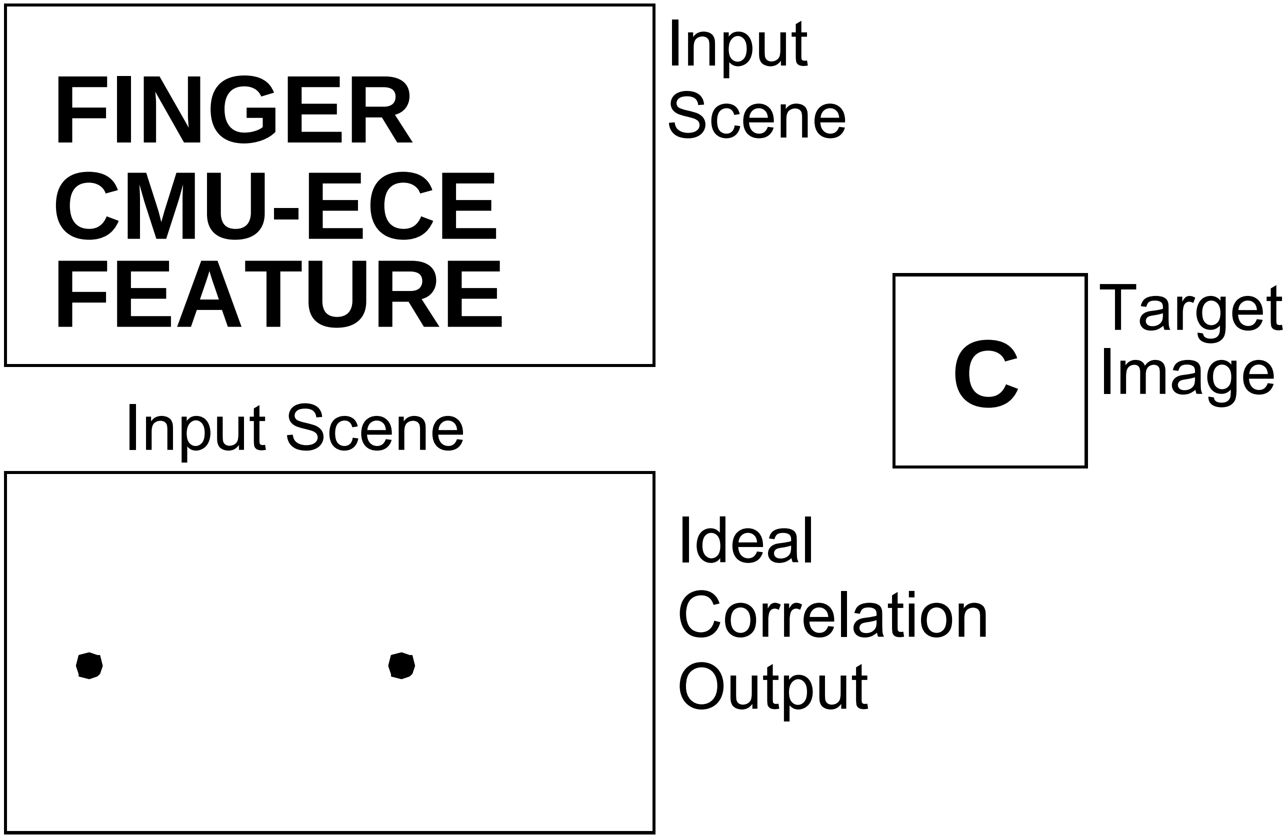


3D Face Matching



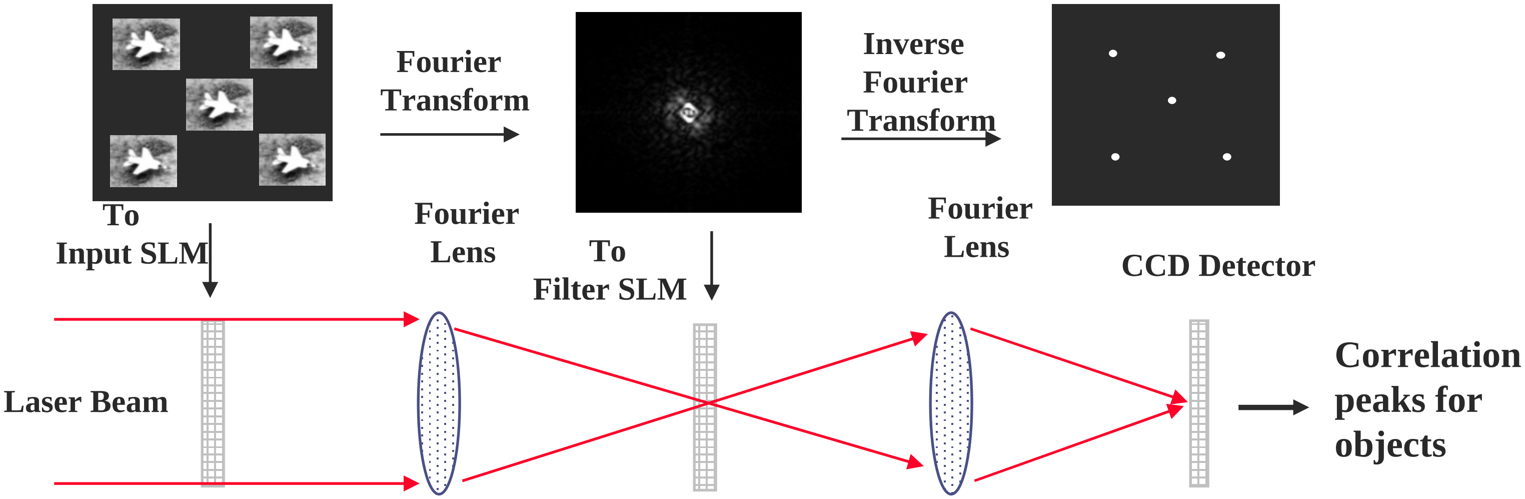
Source: http://www.frvt.org/FRGC/FRGC_Phillips.pdf

Object Recognition using correlation



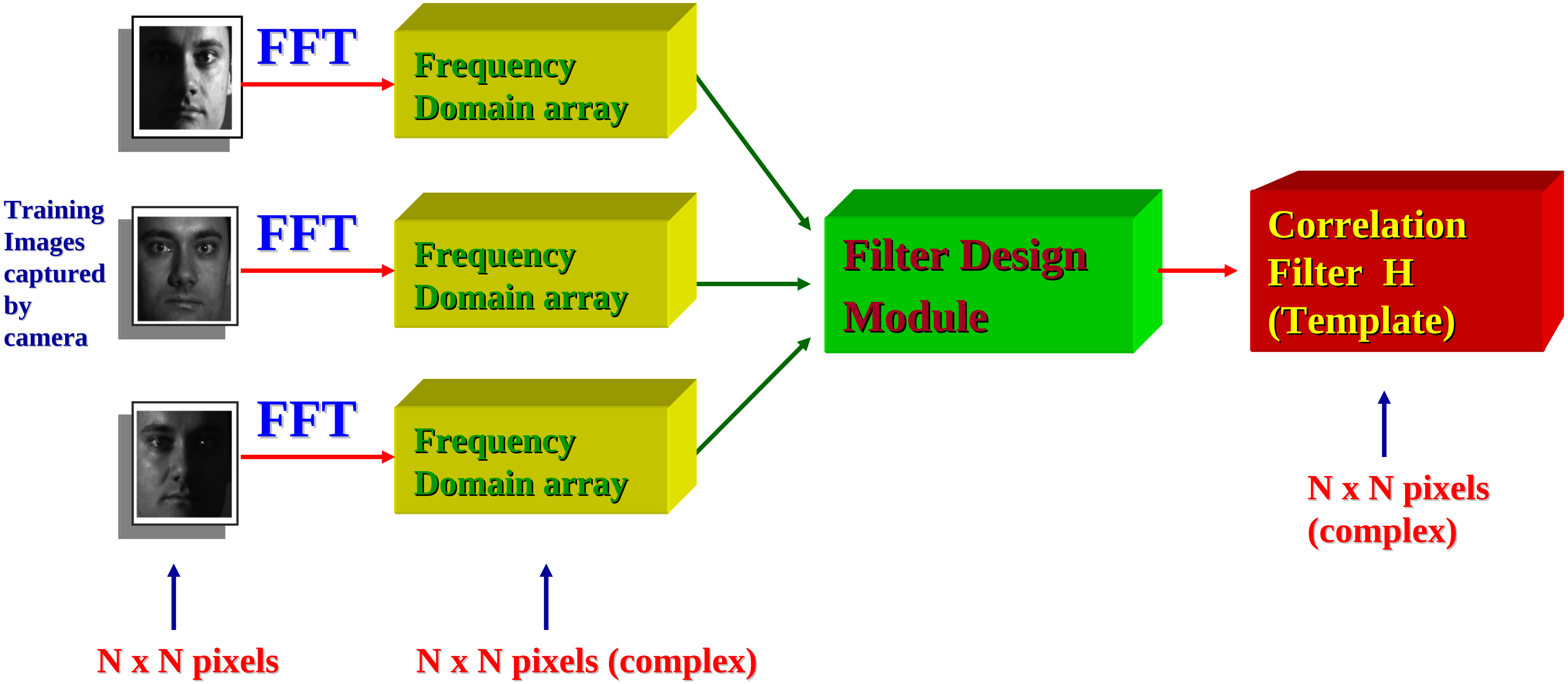
Goal: Locate all occurrences of a target in the input scene

Optical Correlation @ light speed



SLM: Spatial Light Modulator
CCD: Charge-Coupled Detector

Typical Enrollment for Biometric Recognition



Training Images captured by camera

FFT

FFT

FFT

Frequency Domain array

Frequency Domain array

Frequency Domain array

Filter Design Module

Correlation Filter H (Template)

N x N pixels

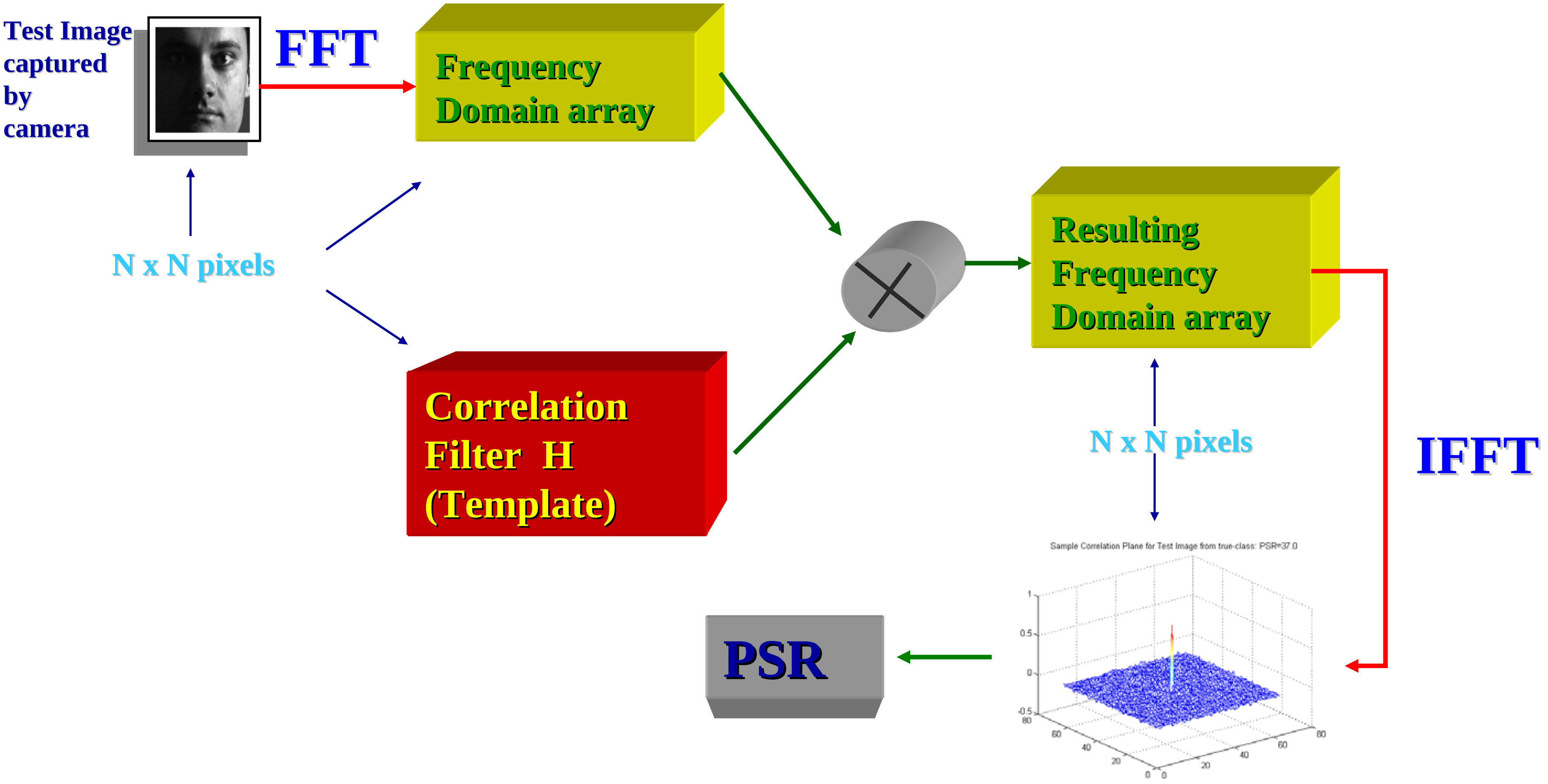
N x N pixels (complex)

N x N pixels (complex)

*B.V.K. Vijaya Kumar, Marios Savvides, C. Xie, K. Venkataramani, J. Thornton and A. Mahalanobis, “Biometric Verification using Correlation Filters”, Applied Optics, 2003

*B.V.K. Vijaya Kumar, M. Savvides, K. Venkataramani, C. Xie, "Spatial frequency domain image processing for biometric recognition," IEEE Proc. of International Conference on Image Processing (ICIP), Vol. I, 53-56, 2002

Recognition stage



Test Image captured by camera

FFT

Frequency Domain array

N x N pixels

Correlation Filter H (Template)

Resulting Frequency Domain array

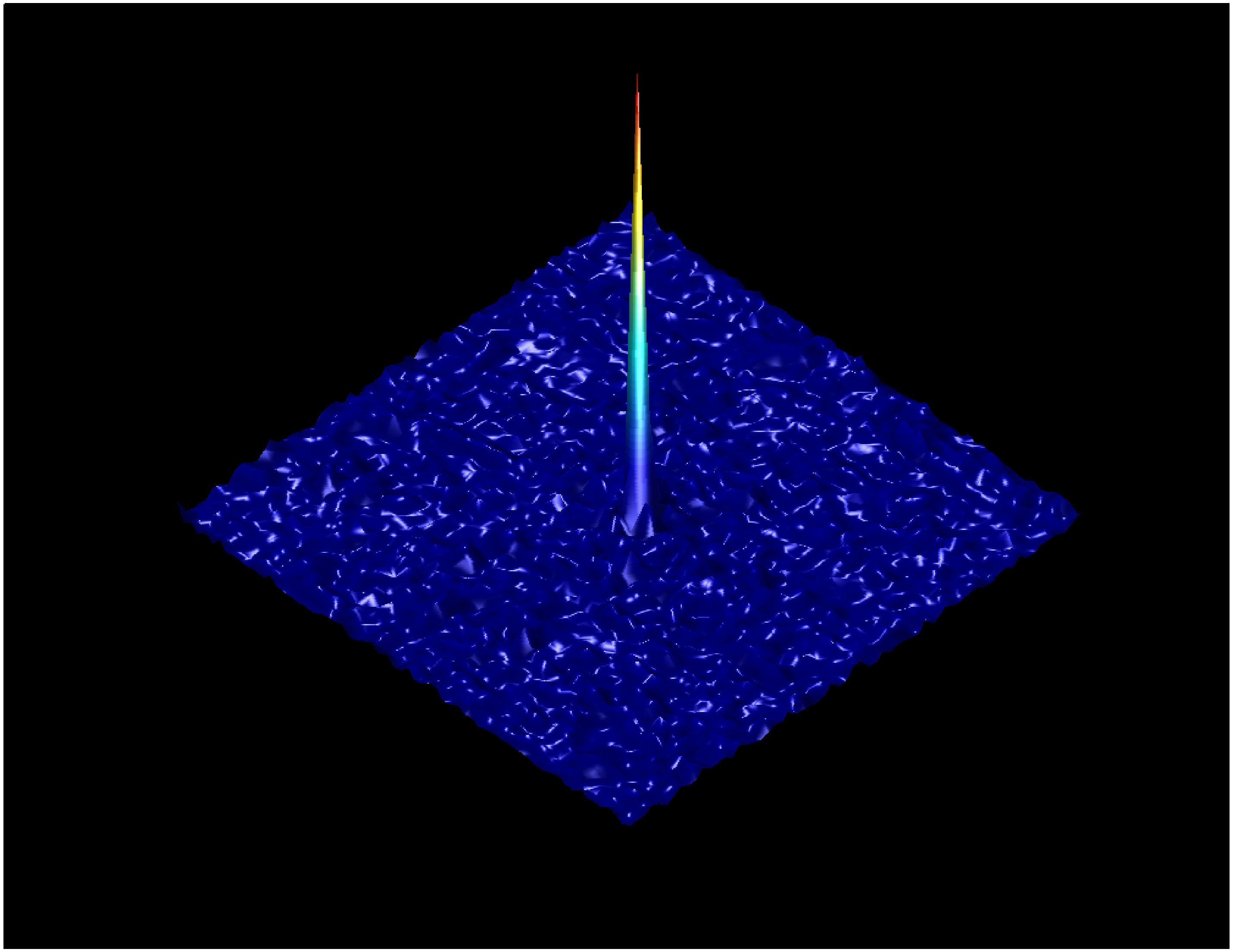
N x N pixels

IFFT

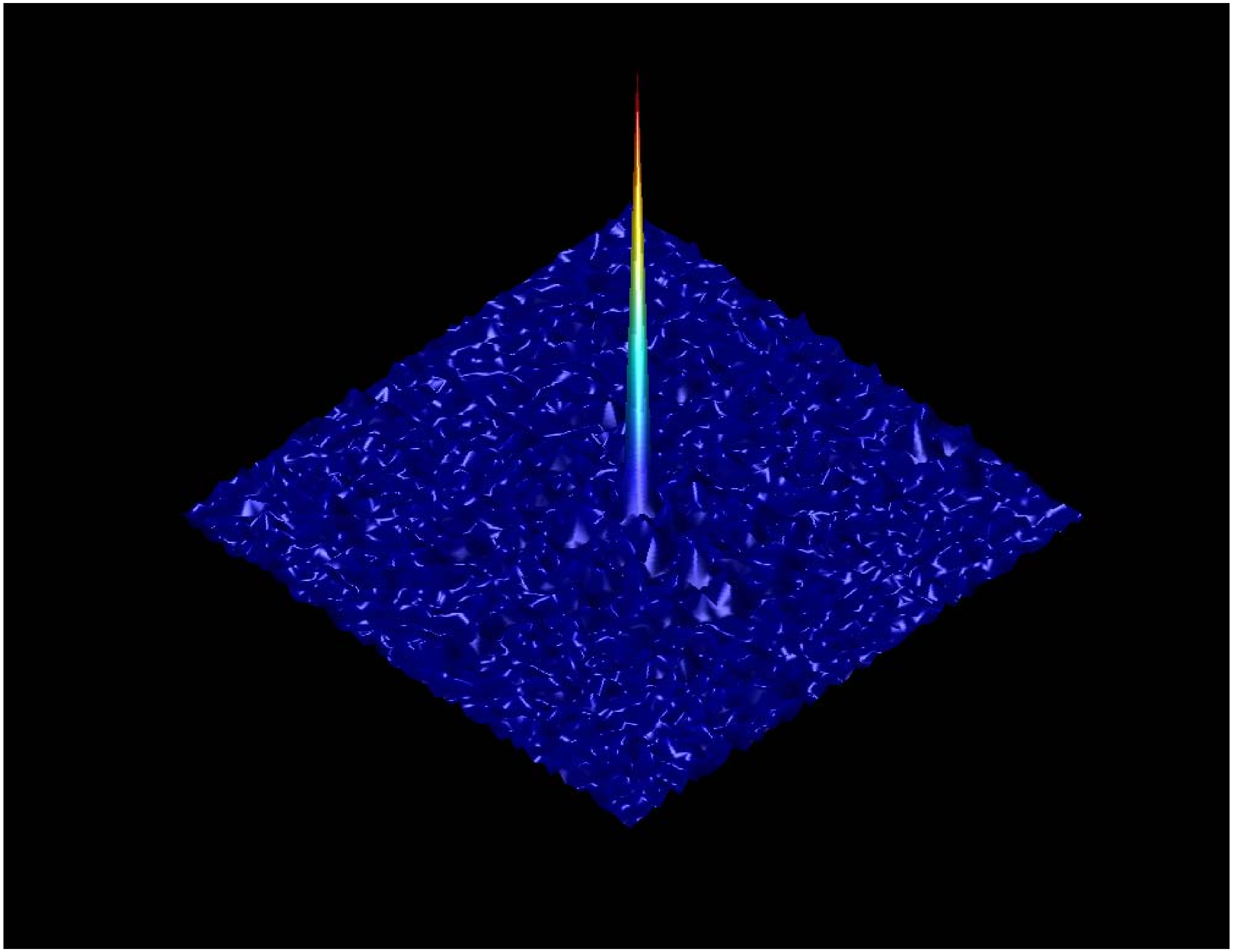
PSR

Sample Correlation Plane for Test Image from true-class: PSR=37.0

Example Correlation Outputs from an Authentic

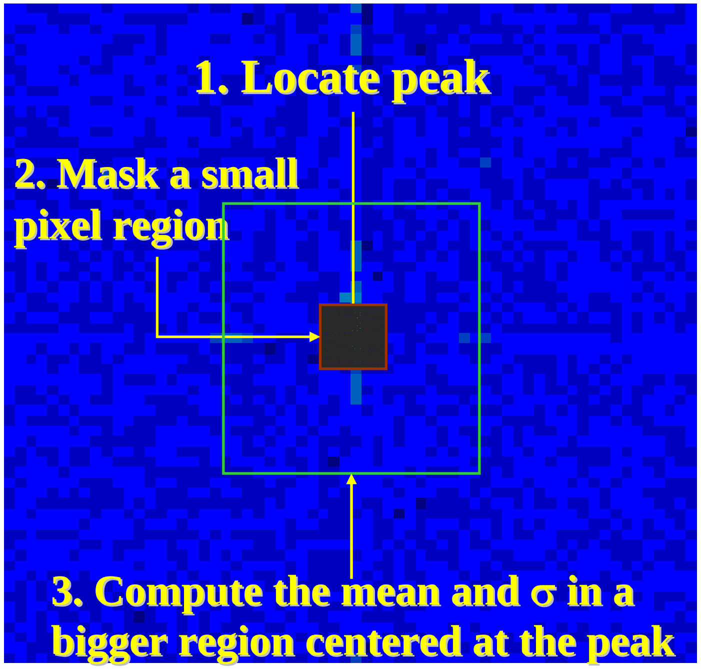


Example Correlation Outputs from an Impostor



Peak to Sidelobe Ratio (PSR)

- PSR invariant to constant illumination changes


1. Locate peak
2. Mask a small pixel region
3. Compute the mean and σ in a bigger region centered at the peak

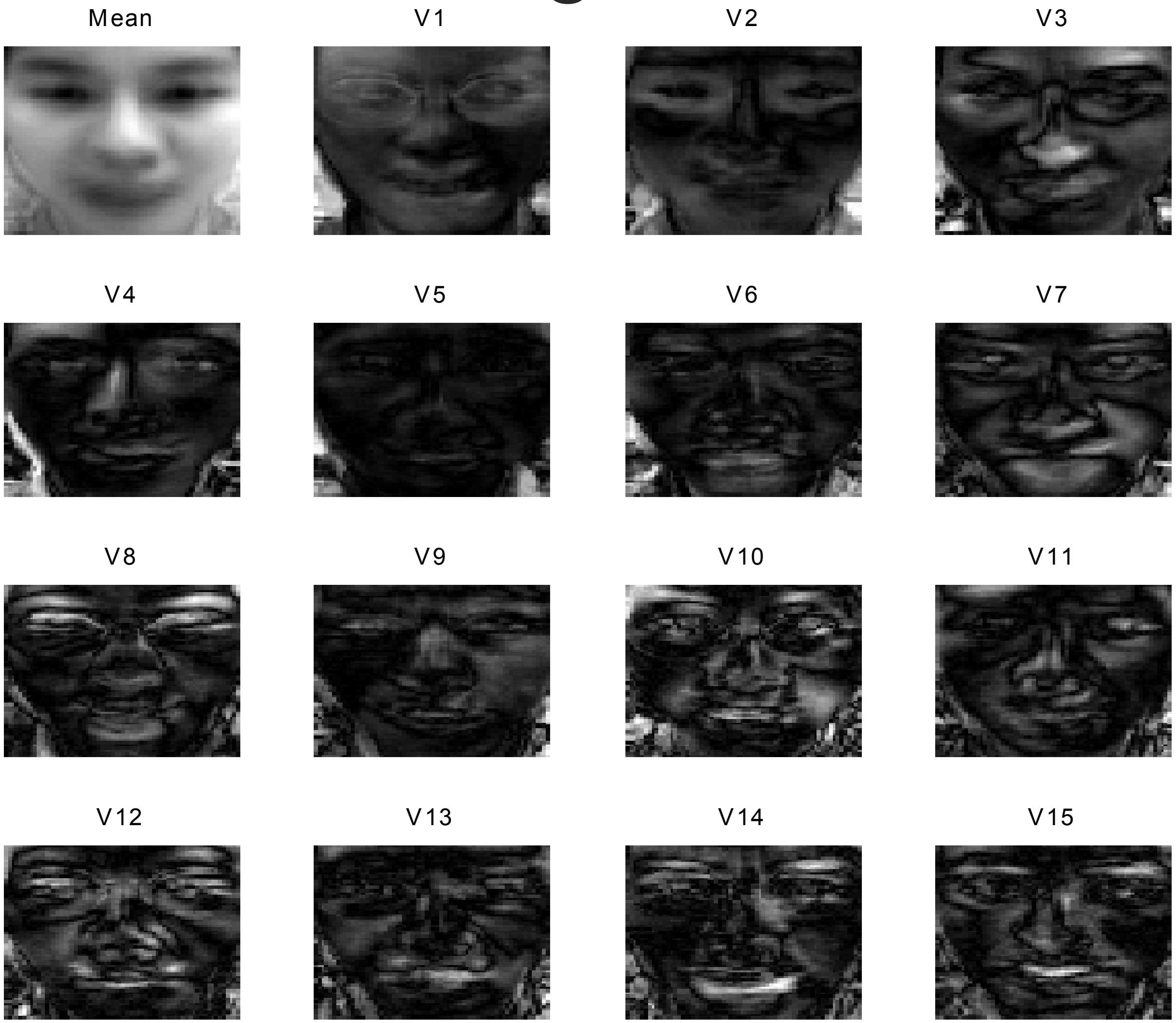
$$PSR = \frac{Peak - mean}{\sigma}$$

- Match declared when PSR is large, i.e., peak must not only be large, but sidelobes must be small.

Eigenfaces

- Is a very well known Face Recognition algorithm in the research community.
- Has become a baseline for comparing new algorithms and how they perform better.
- Uses Linear Algebra math to decompose a ‘basis’ vectors which can describe training face data.
- These basis vectors are called ‘Eigenvectors’ or ‘Eigenfaces’ since these vectors look like faces.

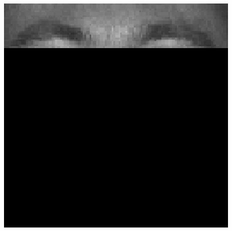
What do some eigenvectors look like?



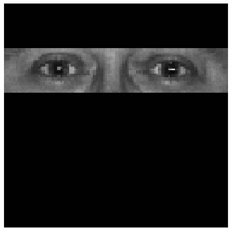
Source: Dr. Marios Savvides, Lecture Notes in Pattern Recognition Course, Electrical & Computer Eng, Carnegie Mellon University

Recognition using selected face regions

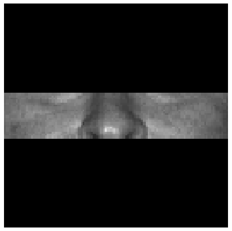
Face Section #1



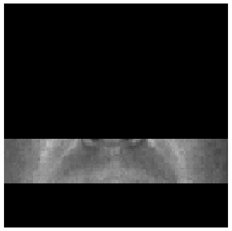
Face Section #2



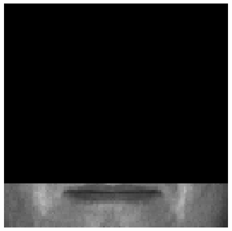
Face Section #3

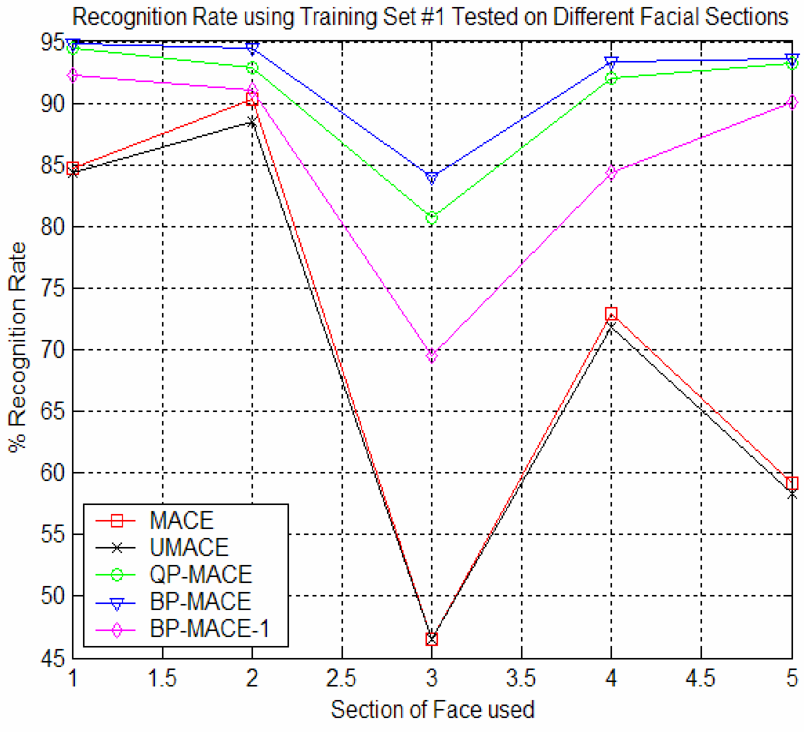


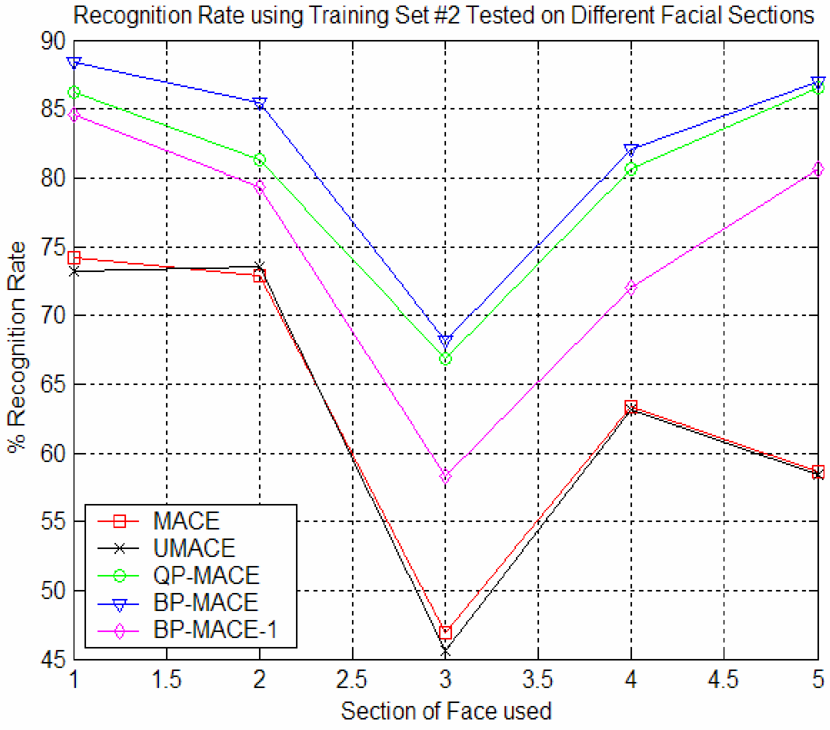
Face Section #4



Face Section #5





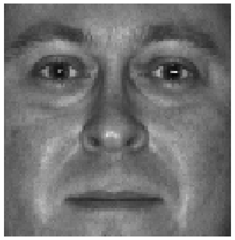


Using Training set #1 (3 extreme lighting images)

Using Training set #2 (3 frontal lighting images)

Vertical crop + texture #2

0% Pixels Blocked

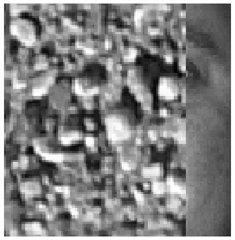


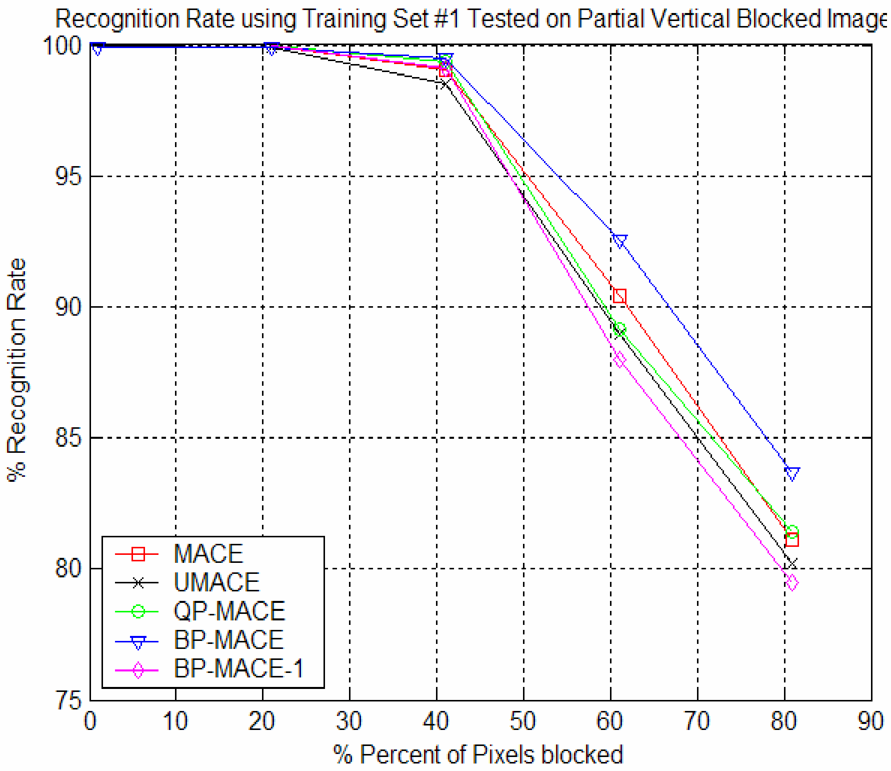
20% Pixels Blocked

40% Pixels Blocked

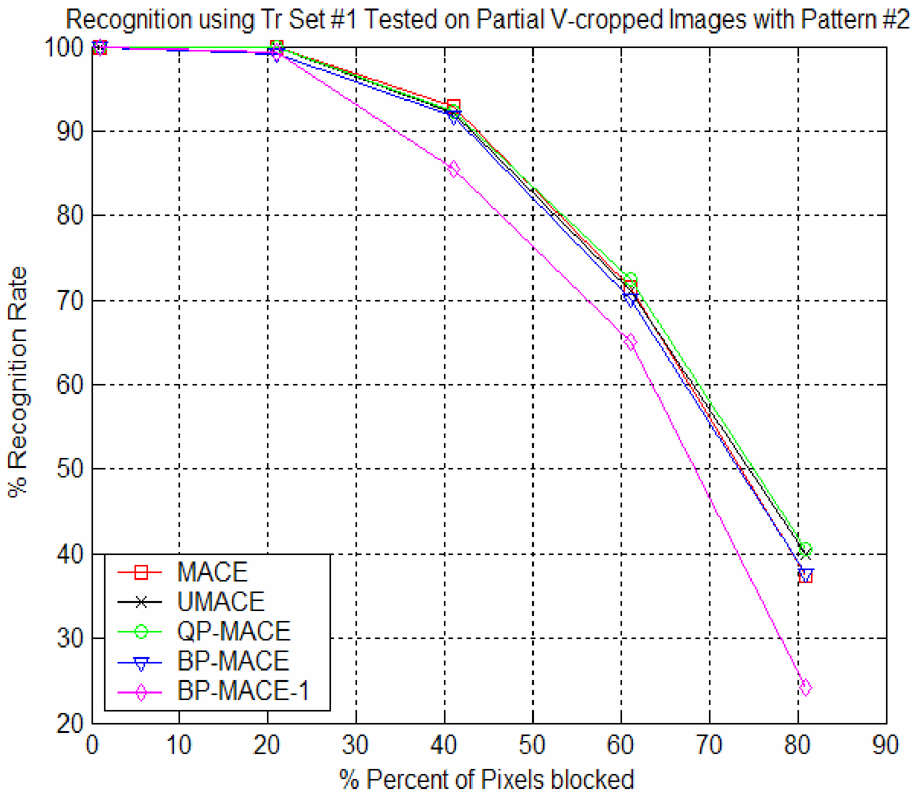
60% Pixels Blocked

80% Pixels Blocked



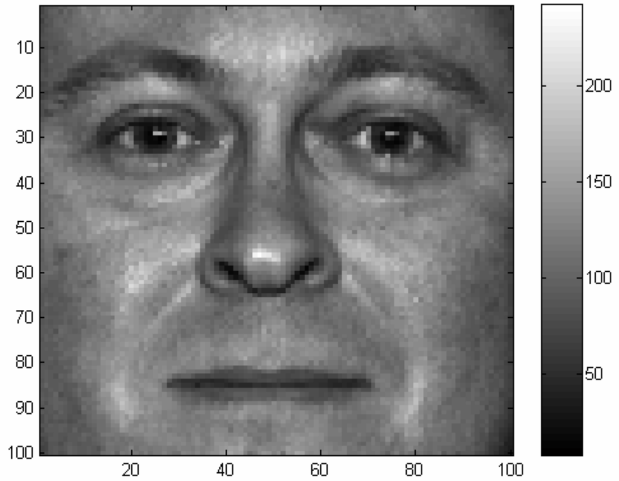

Recognition Rate using Training Set #1 Tested on Partial Vertical Blocked Image
% Recognition Rate
100
95
90
85
80
75
0
10
20
30
40
50
60
70
80
90
% Percent of Pixels blocked
MACE
UMACE
QP-MACE
BP-MACE
BP-MACE-1

Zero intensity background



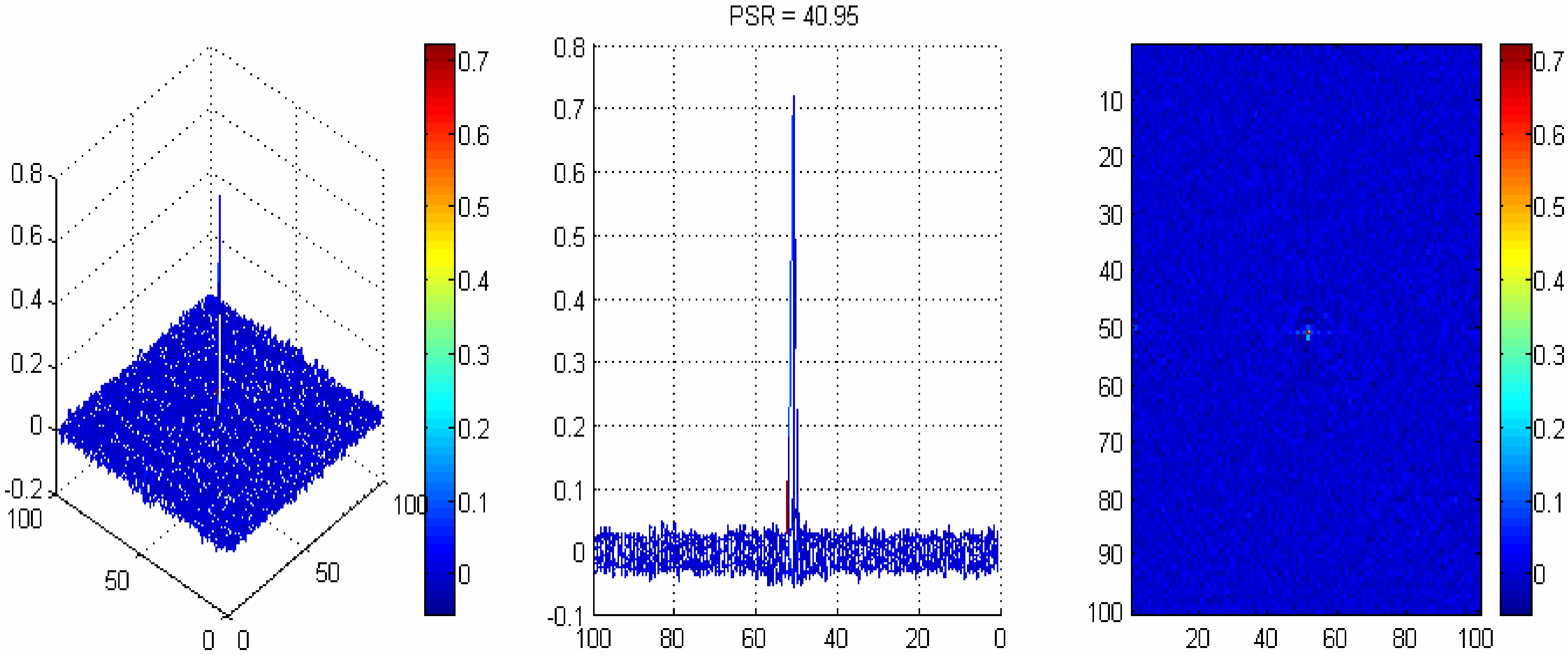
Textured background

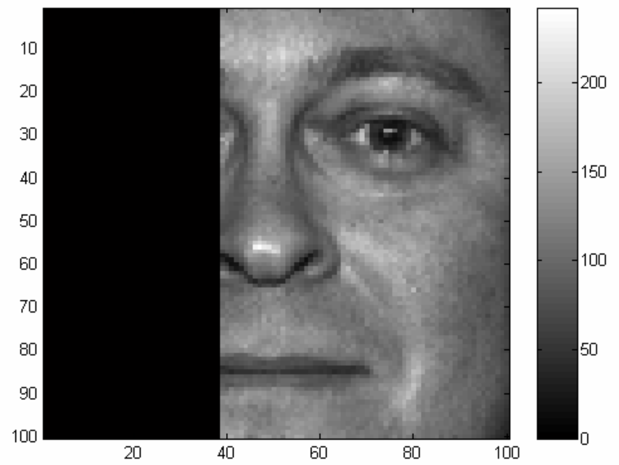
*M. Savvides, B.V.K. Vijaya Kumar and P.K. Khosla, "Robust, Shift-Invariant Biometric Identification from Partial Face Images", Defense & Security Symposium, special session on Biometric Technologies for Human Identification (OR51) 2004.



Train filter on illuminations 3,7,16.

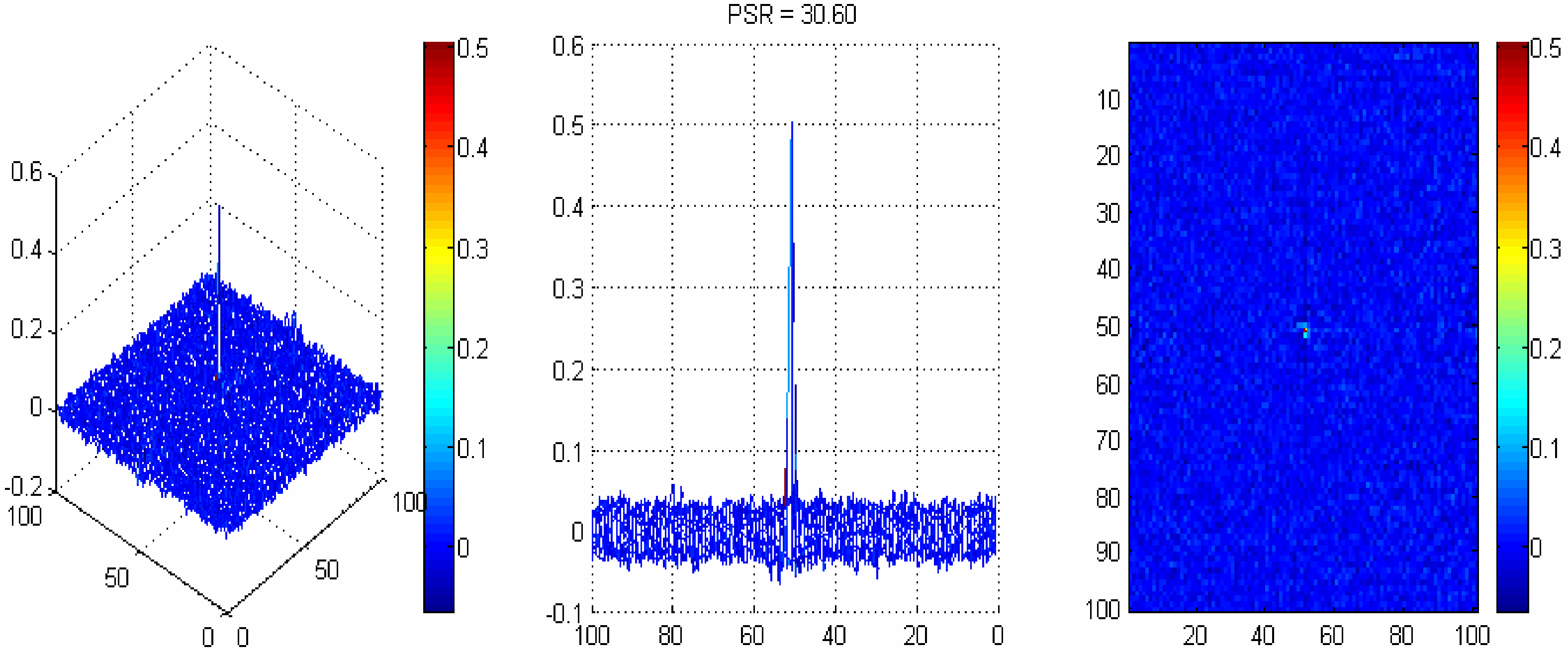
Test on image 10.

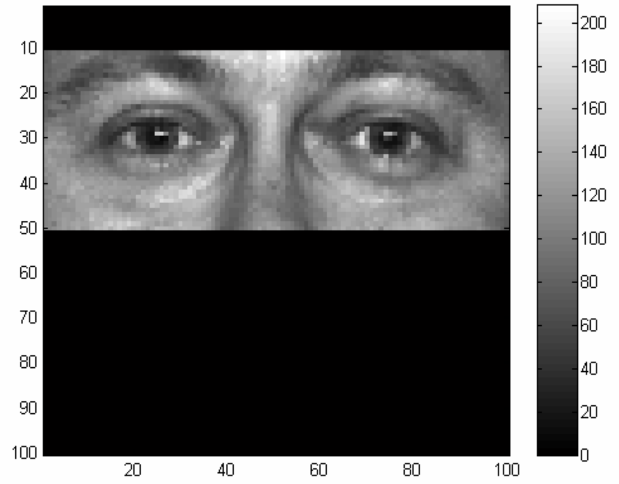




Using same Filter trained before,

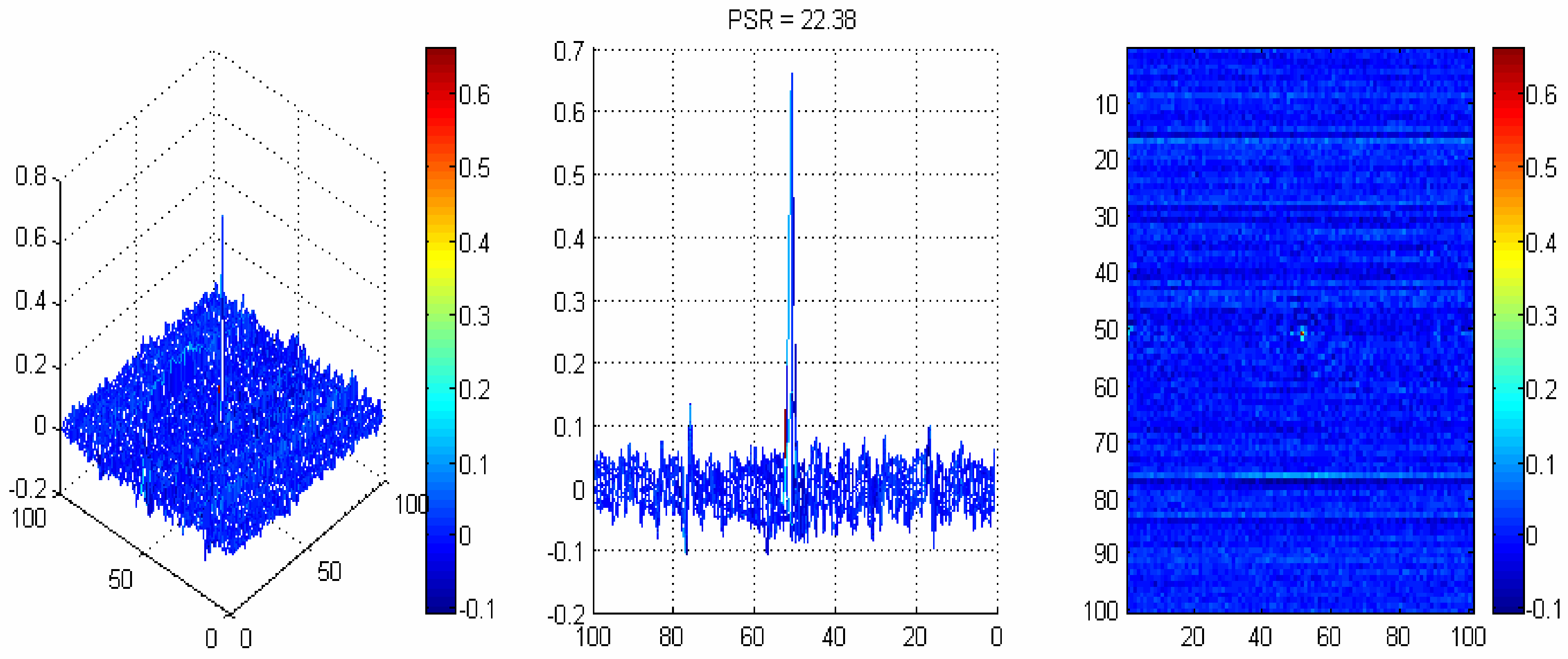
Perform cross-correlation on cropped-face shown on left.

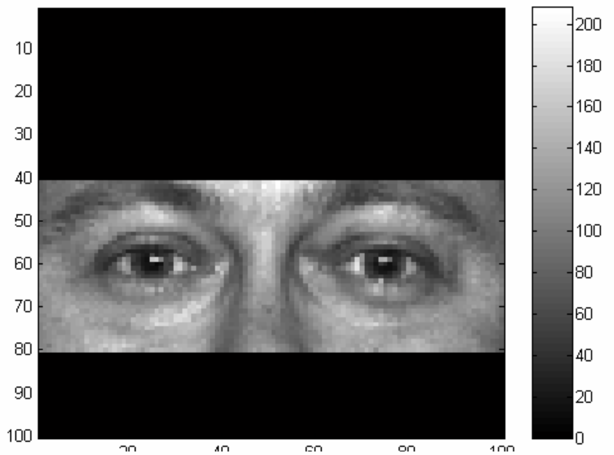




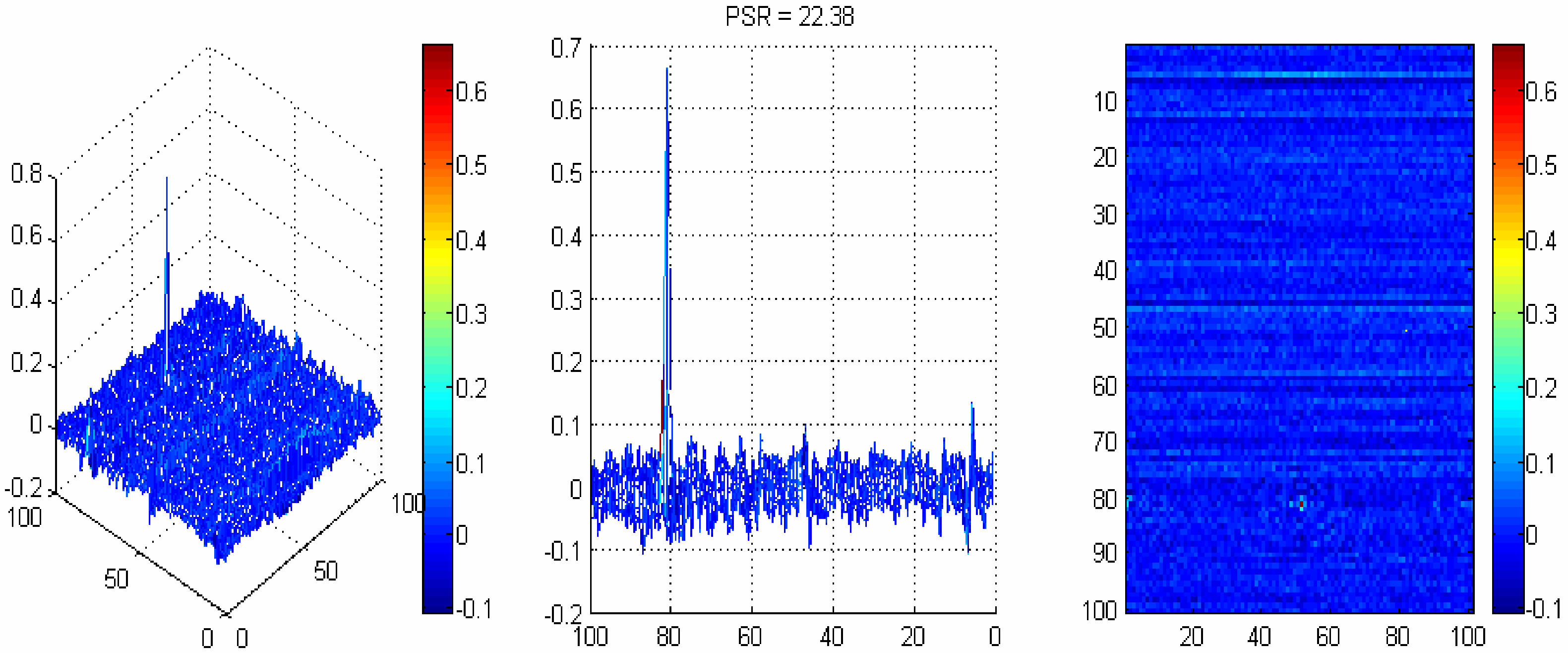
Using same Filter trained before,

Perform cross-correlation on cropped-face shown on left

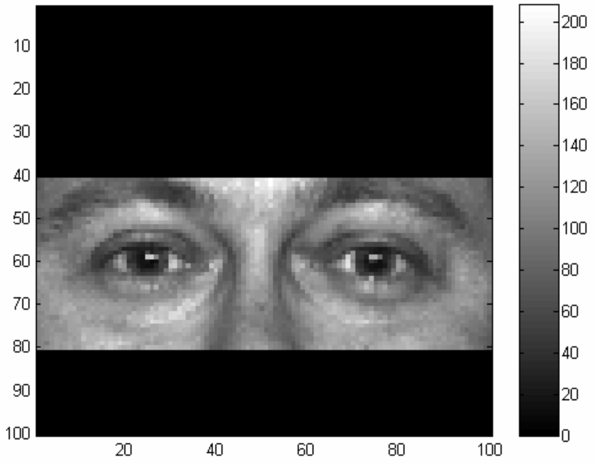




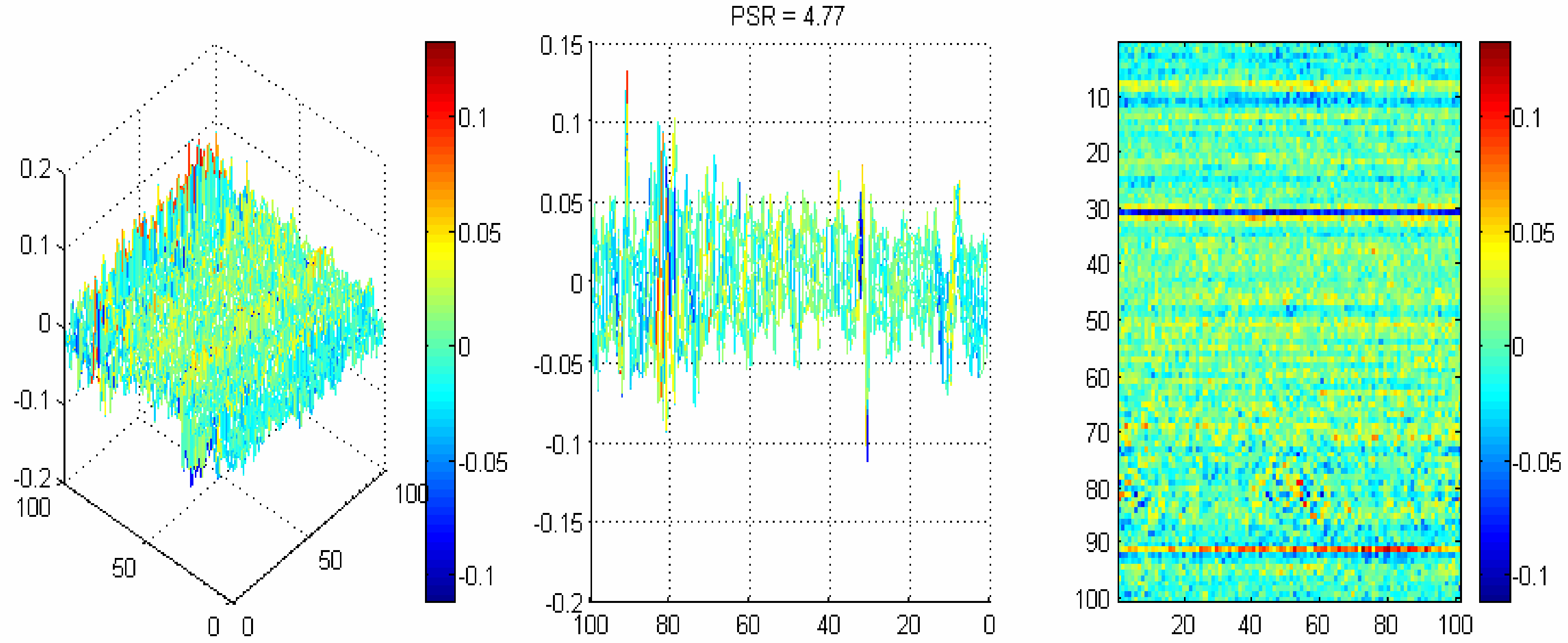
- **CORRELATION FILTERS ARE SHIFT-INVARIANT**
- **Correlation output is shifted down by the same amount of the shifted face image, PSR remains SAME!**



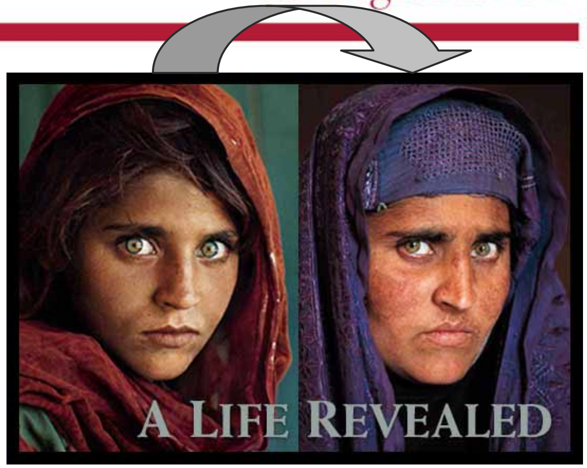
*M.Savvides and B.V.K. Vijaya Kumar, "Efficient Design of Advanced Correlation Filters for Robust Distortion-Tolerant Face Identification", IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS) 2003.



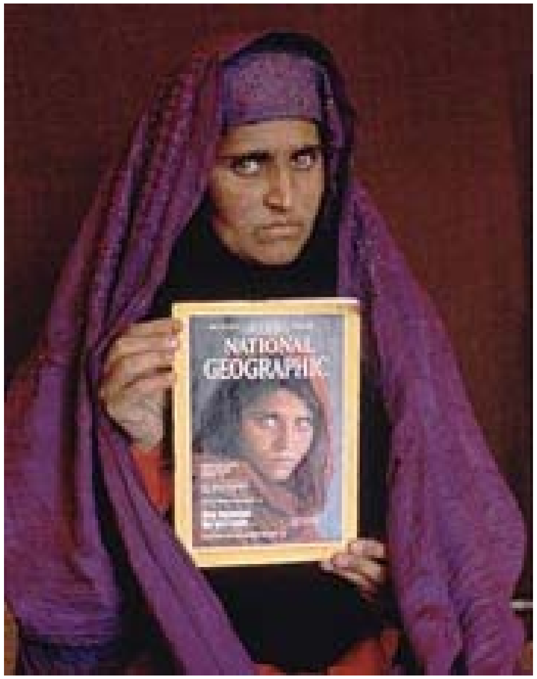
- **Using SOMEONE ELSE’S Filter,…. Perform cross-correlation on cropped-face shown on left.**
- **As expected very low PSR.**


PSR = 4.77

Iris Biometric got really famous in the lost Afghan girl story..



Source: National Geographic Magazine



- In 1994 National Geographic photographer Steve McCurry took a picture of a little Afghan girl called Sharbat Gula in refugee camp in Pakistan.

- Her photo (she had amazing green eyes) made it to National Geographic 100 best Pictures!

- McCurry later tried to trace and find the girl, until finally 17 years later he located a girl with those same haunting green eyes.

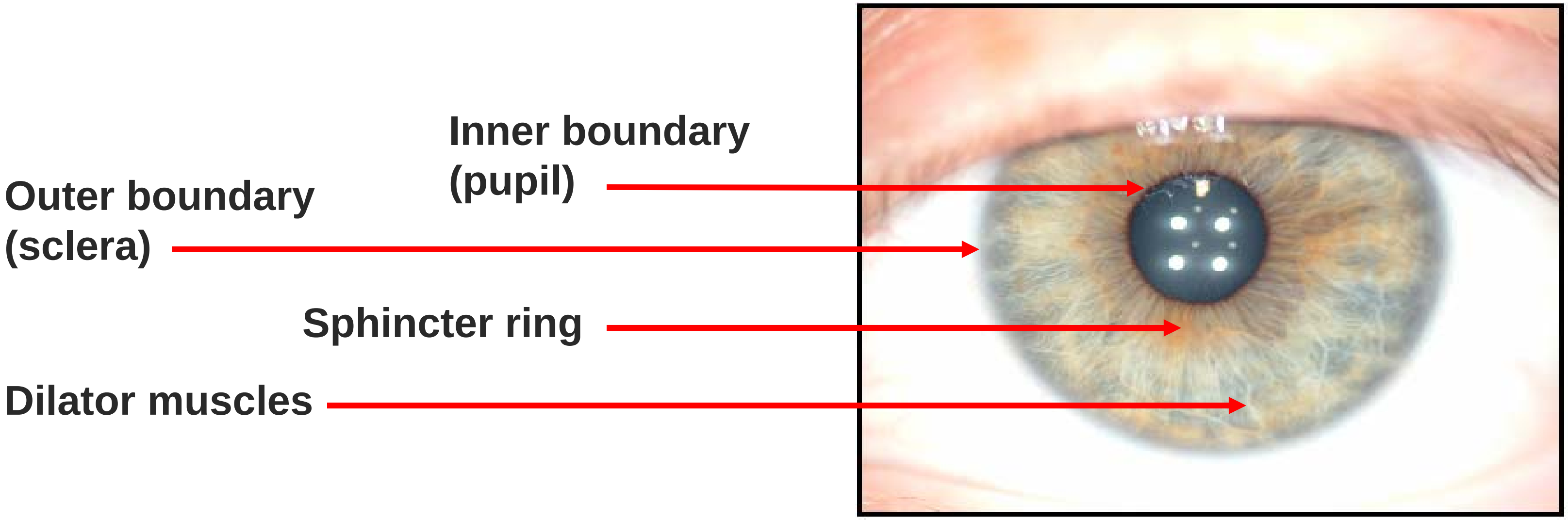
http://news.nationalgeographic.com/news/2002/03/0311_020312_sharbat.html

17 years passed…how to verify if this was the same girl?

- Hard-ship changed the girl's appearance. But she had those same haunting green eyes…
- The Explorer team got verification using U.S. FBI iris scanning technology. They used iris image from old taken photograph and compared to the new one.
- Iris code declared a 'match'!
- This was indeed the same girl! Iris biometric made it possible to verify this.

Iris as Biometric

The iris is the colored portion of the eye surrounding the pupil. Its pattern results from a meshwork of muscle ligaments, and its color and contrast are determined by pigmentation.



Inner boundary (pupil)

Outer boundary (sclera)

Sphincter ring

Dilator muscles

Biometric Advantages

- thought to be very unique, potentially more discriminate than fingerprints
- remains stable over an individual’s lifetime
- for cooperating subjects, iris pattern is captured quickly in an image

Iris as a Biometric

The iris is the colored portion of the eye surrounding the pupil. Its pattern results from a meshwork of muscle ligaments and pigmentation.

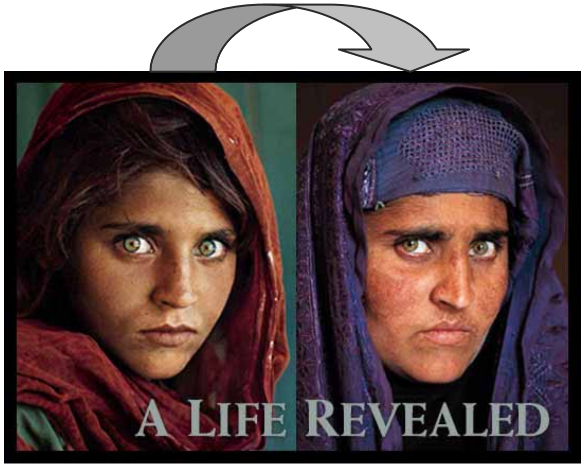
Biometric Advantages

§ thought to be very unique, potentially more discriminate than fingerprints.

§ remains stable over an individual's lifetime (does not change with aging)

§ captured quickly in a cooperative scenario

18 years later

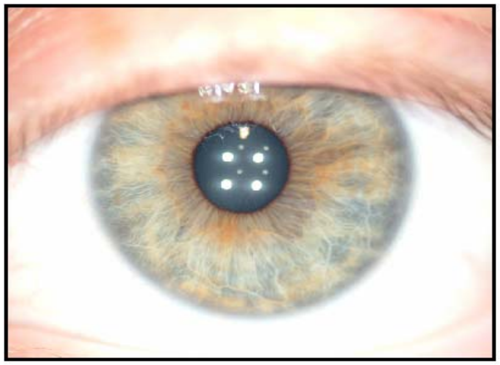


Source: National Geographic Magazine

Iris Camera Equipment

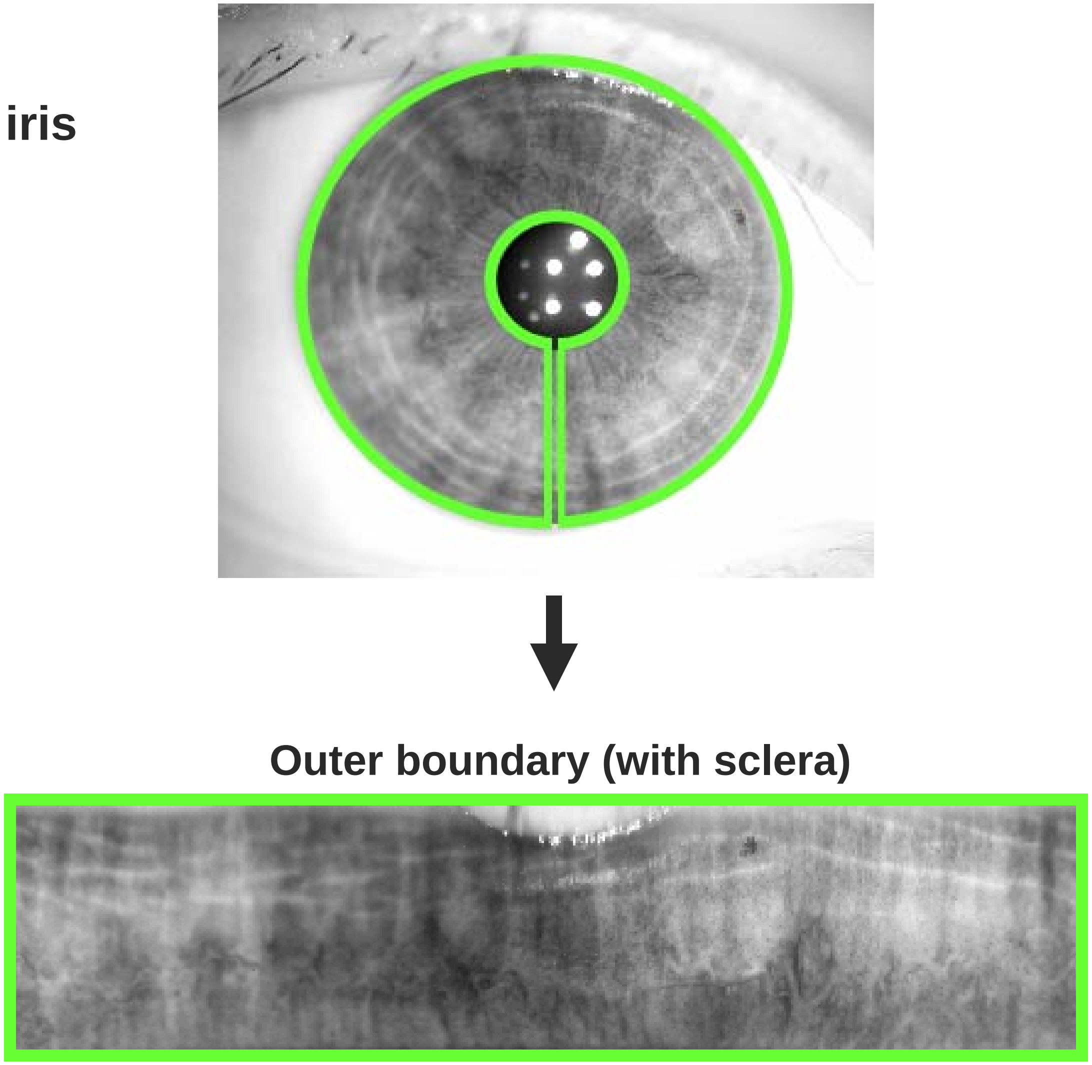
§ We acquire images using equipment built around a Fuji S1 Pro digital camera (pictured left).

§ Images are taken at close range under normal illumination, and at very high resolution (12 megapixels).



First Step: Iris Segmentation

“Unwrapping” the iris

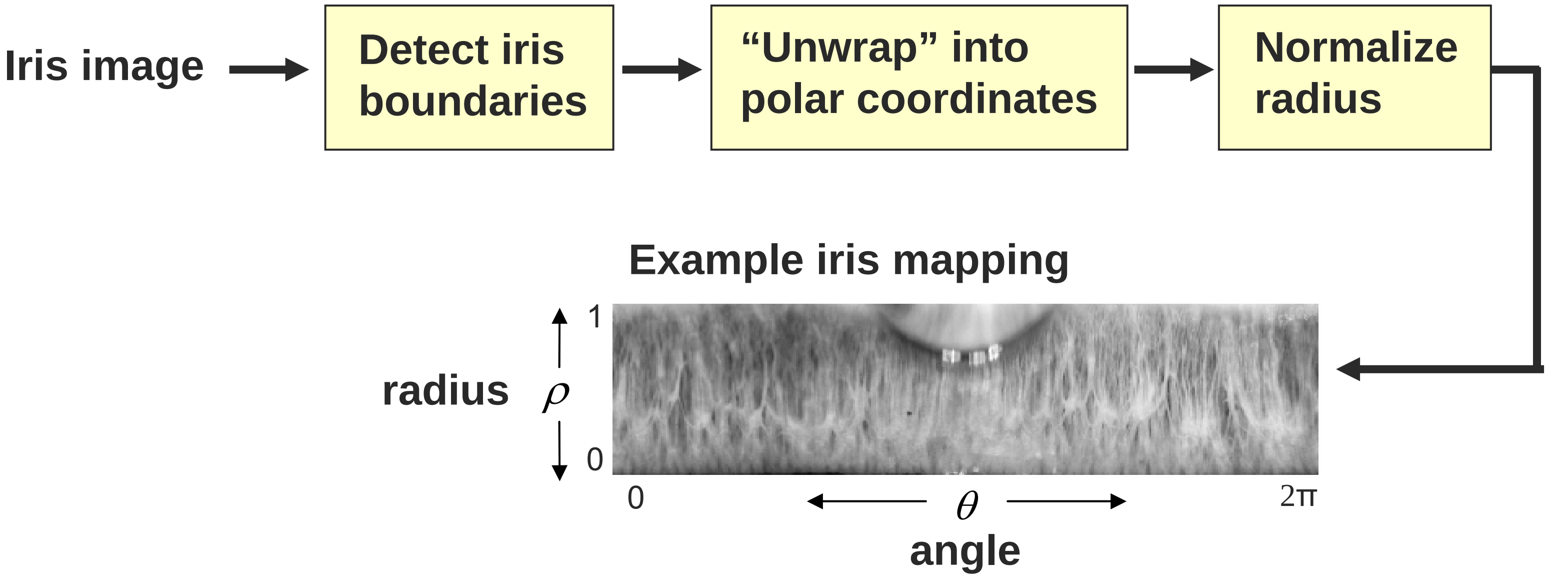


Outer boundary (with sclera)

Inner boundary (with pupil)

Iris Segmentation

Segmentation procedure, first suggested by Daugman[1]:



Iris image → Detect iris boundaries → "Unwrap" into polar coordinates → Normalize radius

Example iris mapping

- Iris is mapped into a rectangle in normalized polar coordinate system.
- Segmentation normalizes for scale change and pupil dilation.

[1] J.G. Daugman, "High Confidence Visual Recognition of Persons by a Test of Statistical Independence," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 15, no. 11, pp. 1148-61, Nov. 1993.

Iris Segmentation: Boundary Detection

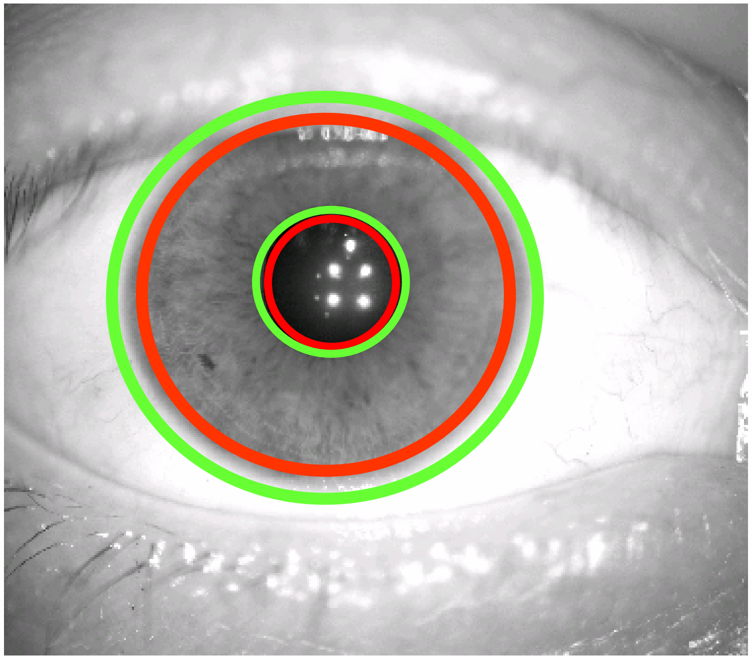
- Segmentation is simplified by modeling the inner and outer iris boundaries as non-concentric circles.

- For each boundary, we must find 3 parameters: ***x*** and ***y*** of center, and radius ***r***

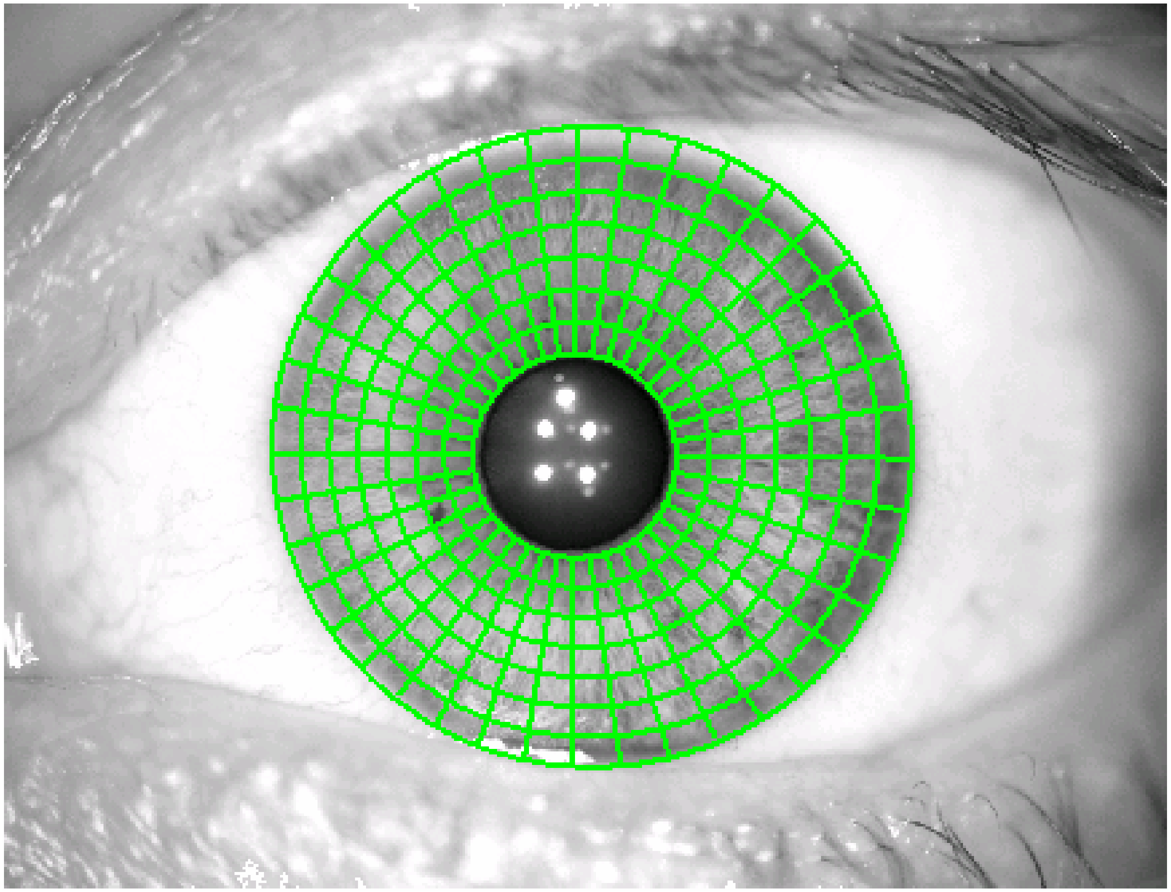
Search Criteria

- intensities along an expanding circular contour become suddenly brighter

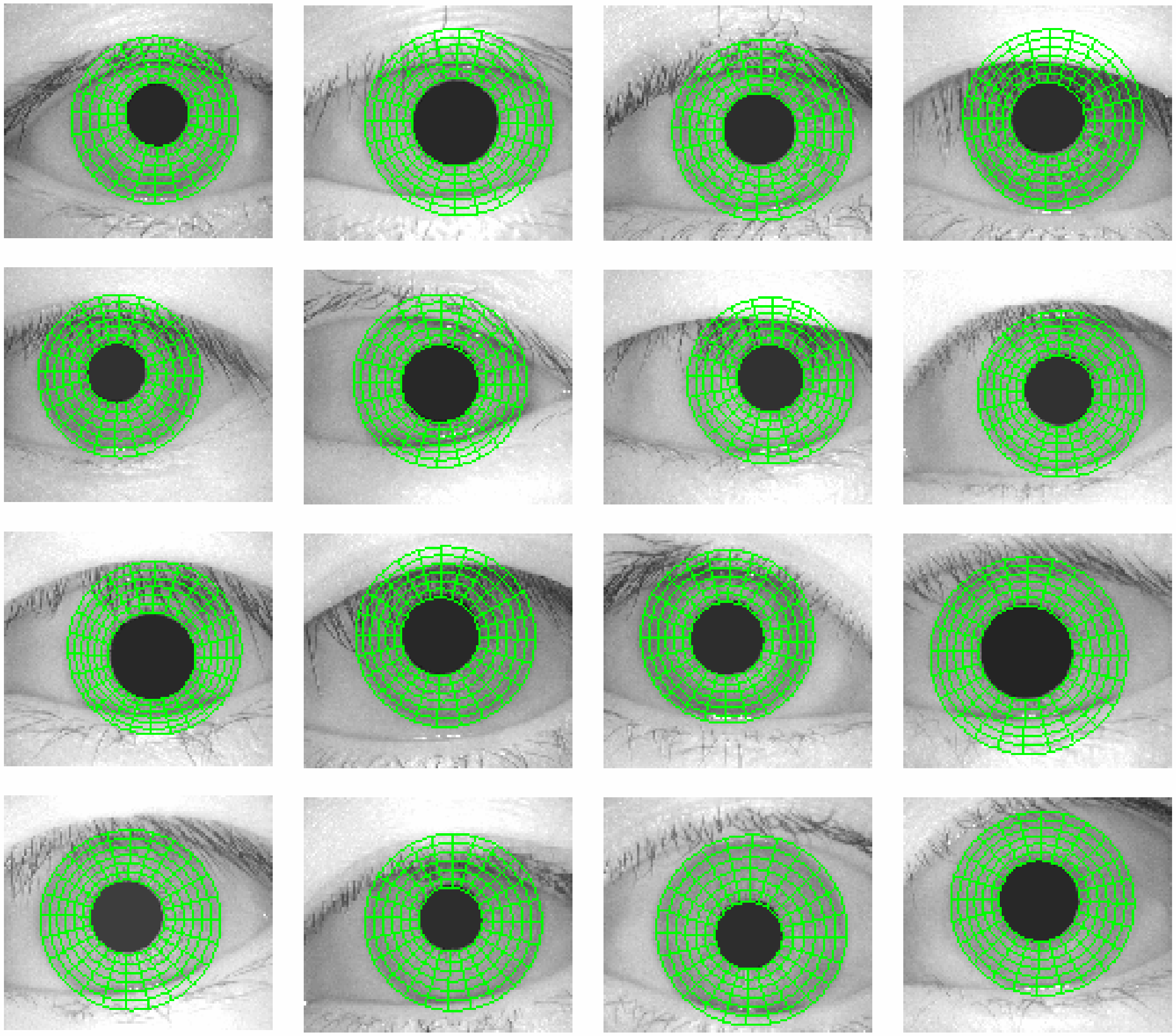
(from red circles to green circles)



Boundary Detection: Example

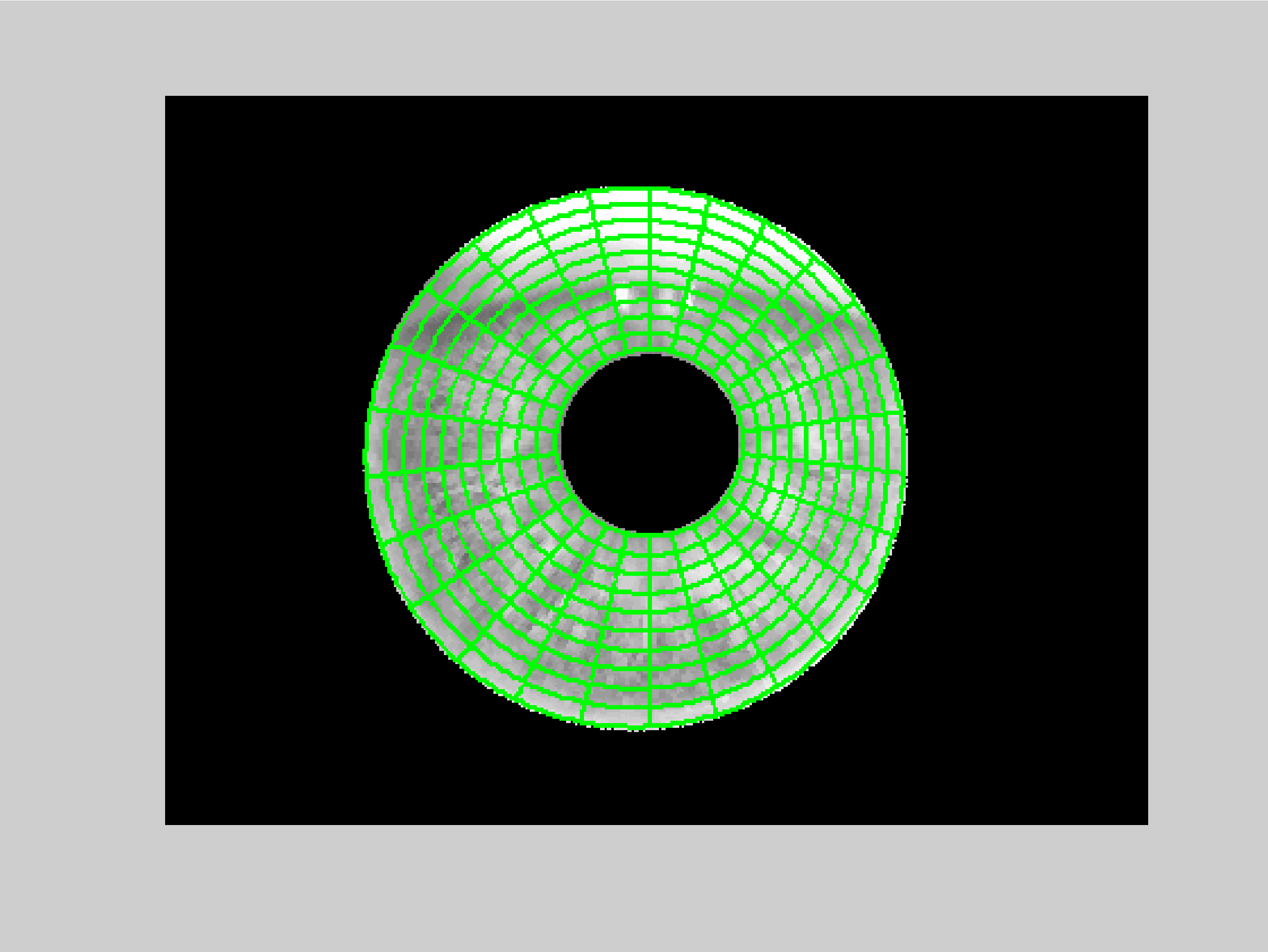


Other Fast Segmentation Examples (from CASIA)



Iris Polar Mapping

Video : Illustration of the mapping into normalized polar coordinates



Common Algorithm: Gabor Wavelets

John Daugman[1] proposed Gabor wavelet feature extraction.

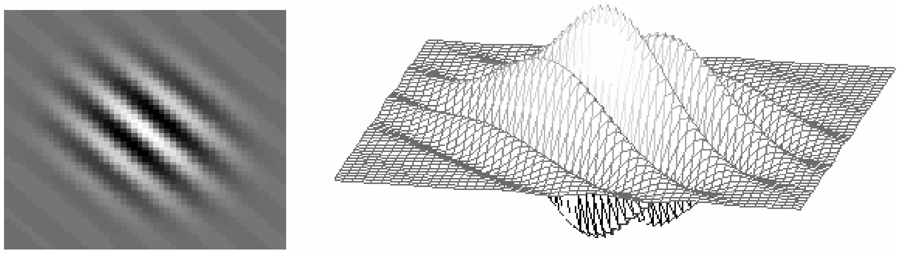
Gabor wavelets have the form:

$$\psi(x, y) = \exp\left[-\frac{x^2}{2\sigma_x^2} - \frac{y^2}{2\sigma_y^2} - j\omega y \right]$$

- Complex exponential with a Gaussian envelope
- Localized in both space and frequency

Gabor wavelet (real part)

Left: 2D, Right: 3D

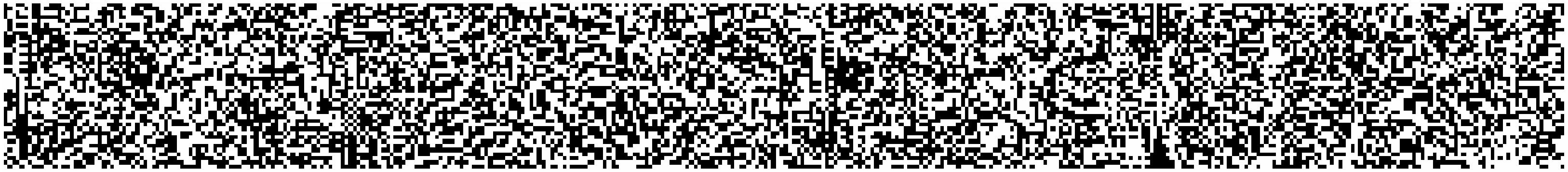


[1] J.G. Daugman, “High Confidence Visual Recognition of Persons by a Test of Statistical Independence,” *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 15, no. 11, pp. 1148-61, Nov. 1993.

Implementation

Our implementation of Daugman’s method:

Result : 15,696 bit code for each iris pattern



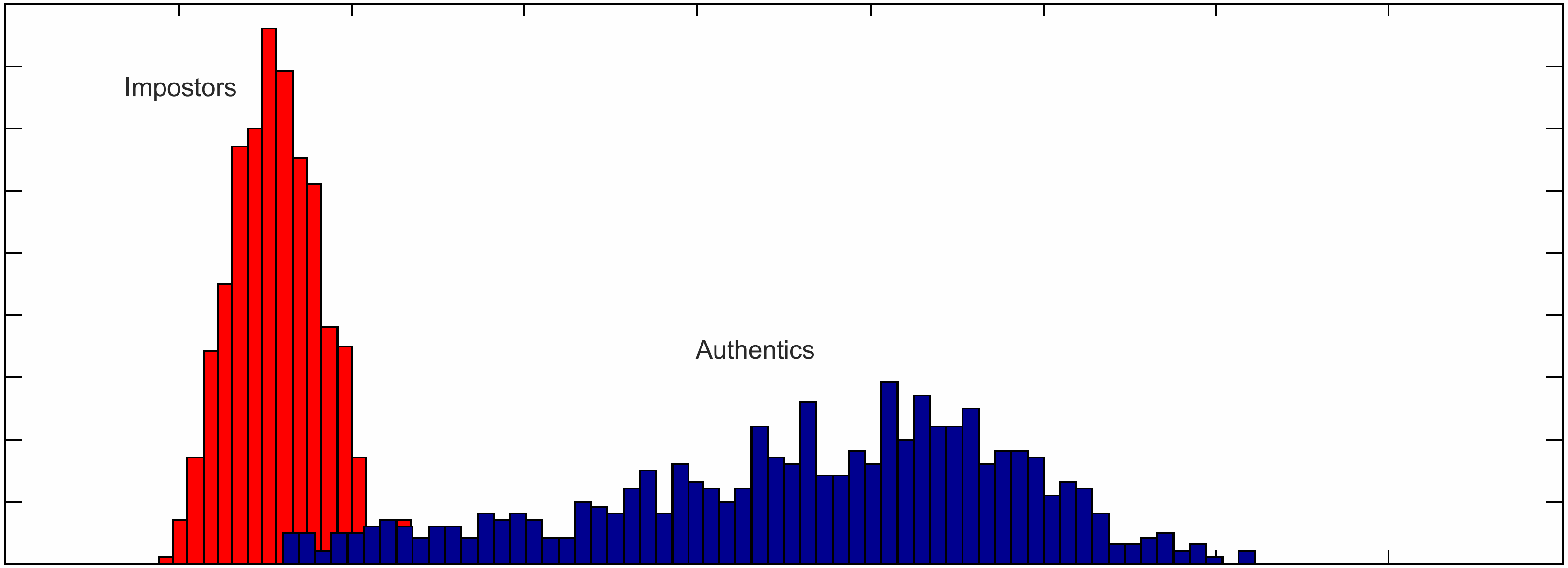
Shifts : We store multiple codes at 10 shifts (3 pixels apart)

Comparison: Iris Code

Using Libor Masek's[2] implementation of Daugman's Gabor wavelet iris code algorithm[1]:

Training on first image only:

Overall Equal Error Rate (EER): **4.09 %**

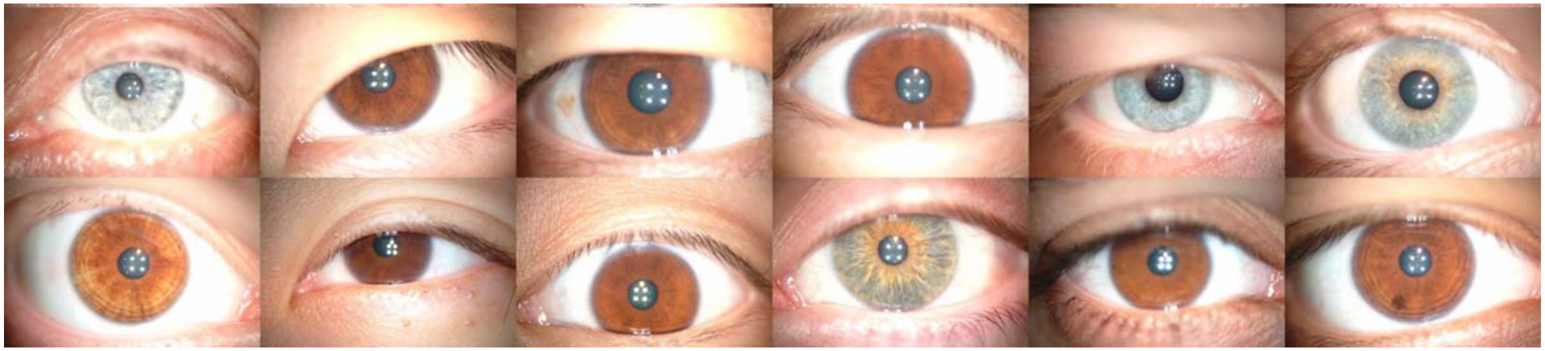


Normalized histograms of Hamming similarities
(red = imposters, blue = authentics)

Further Experiments: CMU Iris Database

We collected an iris image database for testing recognition algorithms.

Sample images



- 101 different iris classes

- Every class contains approx. 24 images from same eye, collected on 2 different days

- Collected at high resolution under *visible illumination*

Iris Acquisition Devices

Acquisition Device	**Presentation Method**	**Acquisition Process**	**Audio/Visual Feedback**
LG IrisAccess 3000 EOU, 3000 ROU	L/R iris presented **separately**	L/R iris acquired in **separate** sequences	**Audio** feedback
OKI IrisPass-WG	L/R iris presented **simultaneously**	L/R iris acquired in **separate** sequences	**Visual** feedback
Panasonic BM-ET300	L/R iris presented **simultaneously**	L/R iris acquired in **same** sequence	**Audio and visual** feedback

Panasonic

LG

OKI

www.Biometricgroup.com