Ocular Biometrics in a Mobile Phone

Reza R. Derakhshani, PhD
Associate Professor, UMKC
Chief Scientist, EyeVerify

Vikas Gottemukkula, PhD
Research Scientist, EyeVerify

SCA 13th Government Conference 2014

The Need

-Historically unprecedented global market penetration of mobile devices across all sectors, plus:

-Phones are frequently lost, stolen or hacked

- 1.1B comprised accounts (2004-2013) & 80% of data breaches occur due to exploited or stolen credentials*
- $221B ($54B in US) identify related crimes in 2011*
- 96% of all lost phones were accessed by their finder*

-End users are frustrated with passwords, and it's getting worse

- The average person juggles at least 25 passwords*
- 38% of Americans would rather clean a toilet then think of a new password*
- 36% of Americans think world peace would be easier than remembering all their passwords*
- A recent report by Ericsson Labs found that 48% of consumers say they would like to replace passwords with an eye biometric in 2014

-Passwords and pins are easy for thieves and hackers to guess

- 1234, 1111, 0000 account for 25% of all pins in use*
- Stronger passwords don't help much and reduce usability

Biometric Solution

- Biometrics as the most natural and tentatively the best solution to this fundamental question: *Who is Holding the Phone?*
  - *It's something that you ARE, not something the you know or have (surrogate authentication)*
- Available modalities
  - Which ones make more sense?
    - *Hint: users constantly "touch" and "look at" their phones*
  - What are the issues facing mass consumer adoption?
    - User experience (ease, consistency across use case scenarios)
    - Price
    - Privacy, security, revocability
    - …

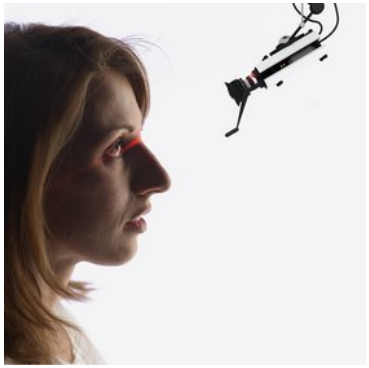
Vascular Patterns as a Strong Biometric

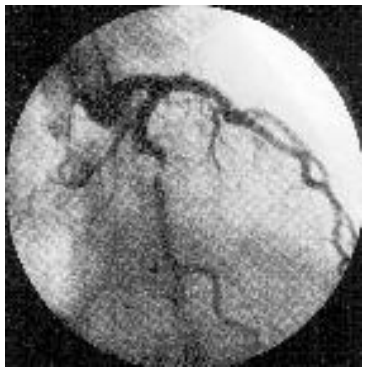
- Complex and unique patterns

Contactless palm vein recognition unit

←Hand and finger vein

Retinal vasculature→

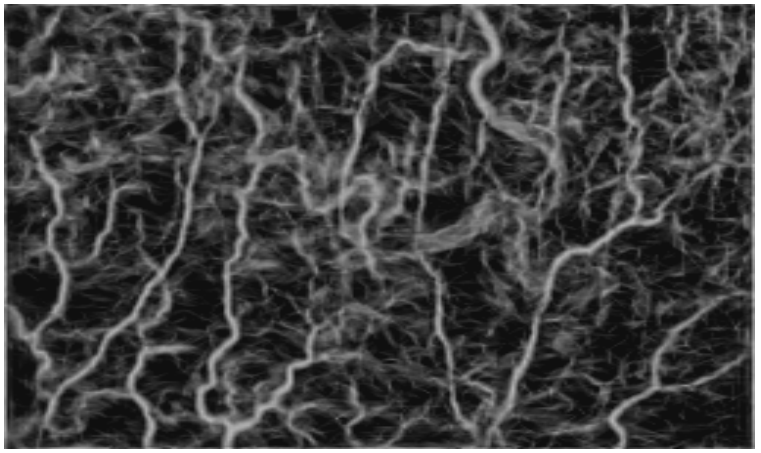




Infrared image

Vein and hand contour

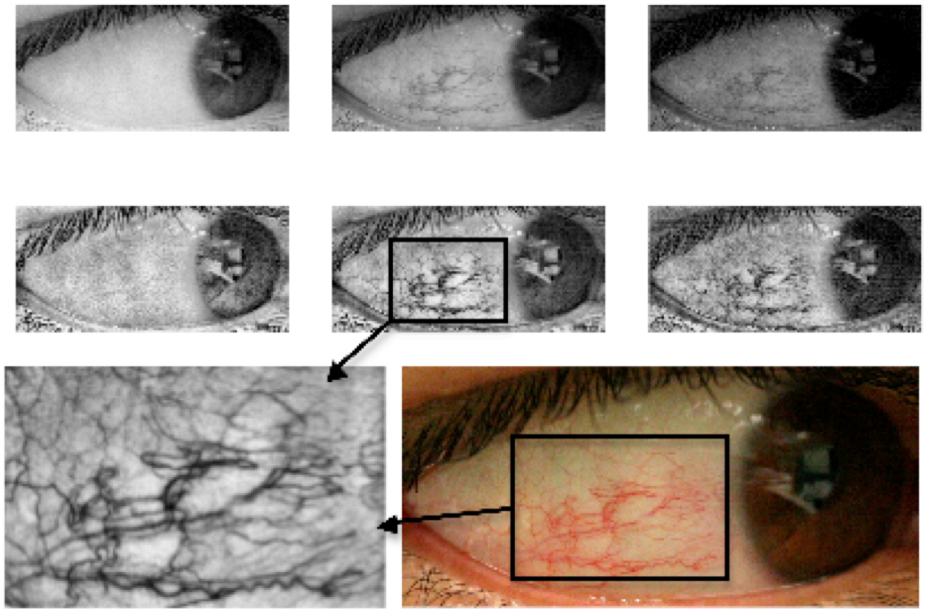
???→

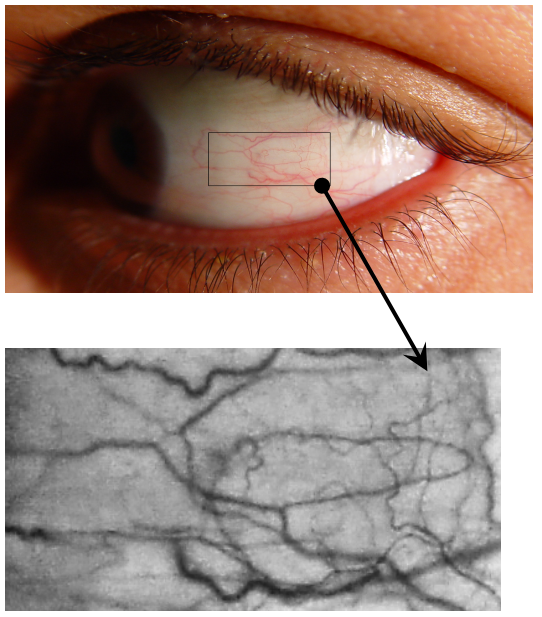


… But hard to get to unless

OR

- Scan the [only] part our body with visible vasculature: whites of the eye
  - Derakhshani R, Ross A, "Conjunctival Scans for Personal Identification," US Patent number 7,327,860; issued on 2/5/2008.
  - Many thanks to CITeR for providing the seed funding for this research in 2005

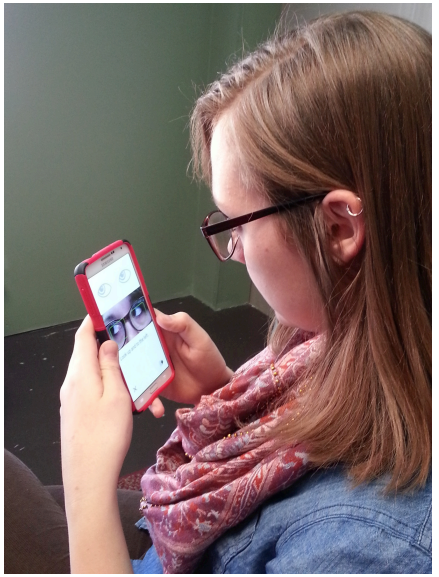


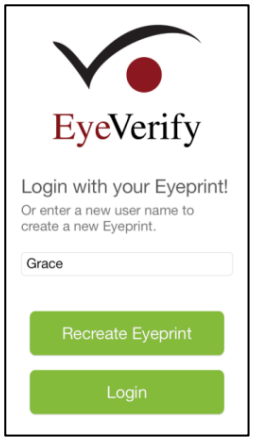


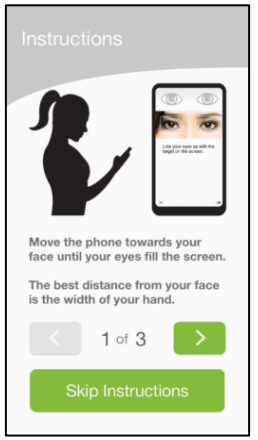
From dSLRs to Cell Phones

2005:

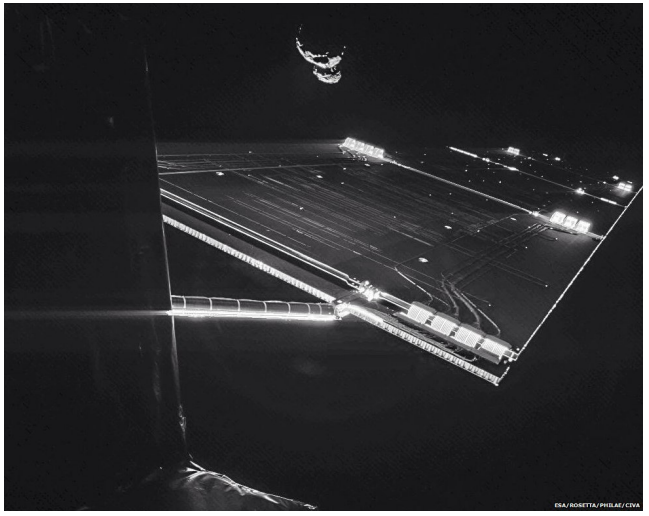
Now:







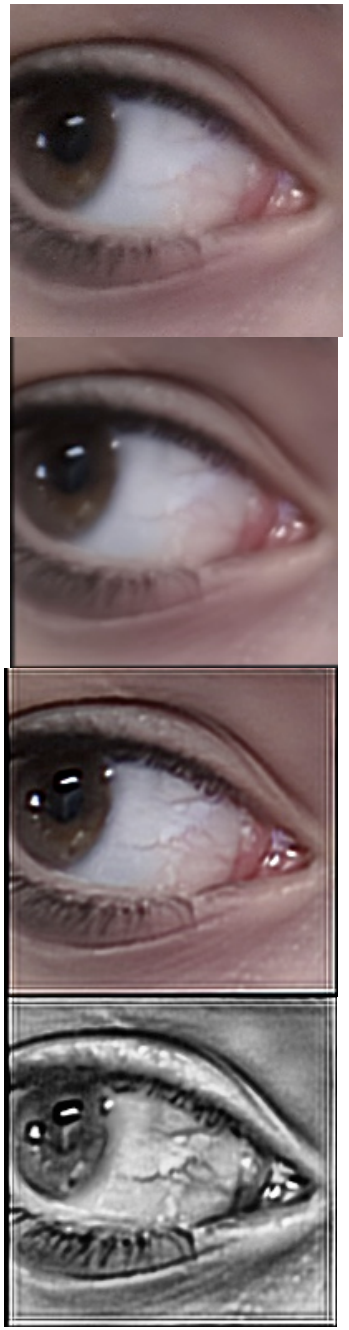
Selfies are in…



Rosetta takes 'selfie' ahead of landing site selection (BBC News)

Challenge 1

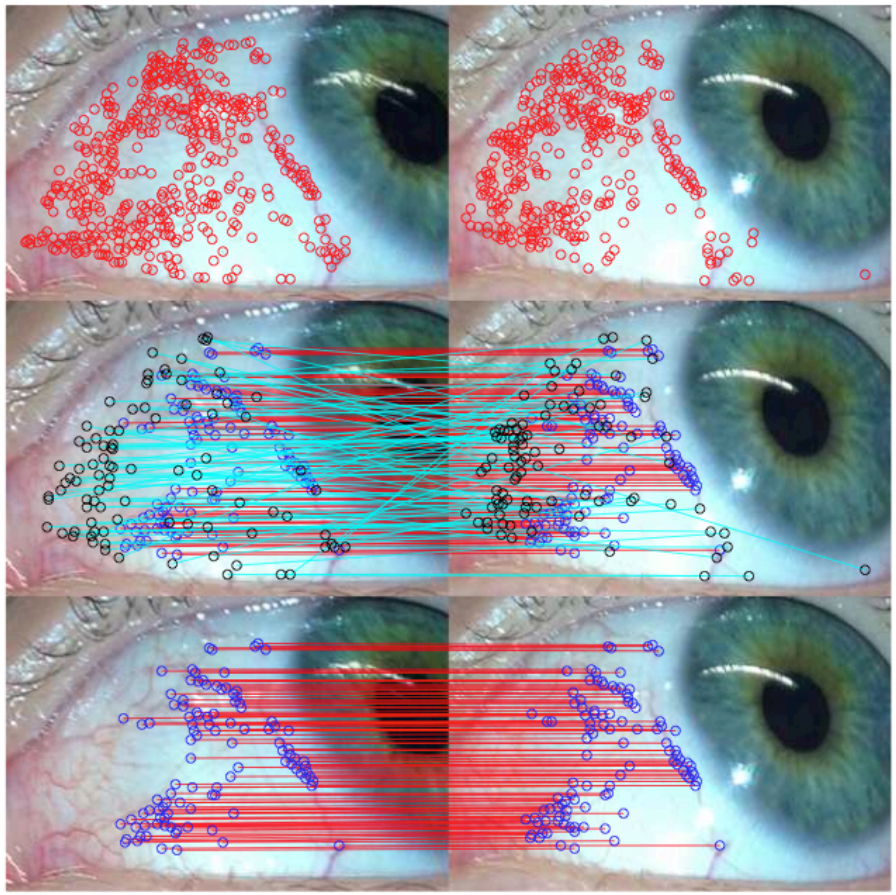
- *Front facing cameras* have lower quality sensors and optics
- Mitigation: computational photography
  - Multi-capture SNR boosting (exposure stepping and averaging)
  - PSF recovery/blind deconvolution
  - Multi-capture feature aggregation
  - Vesselness/eyevein-tuned filter banks

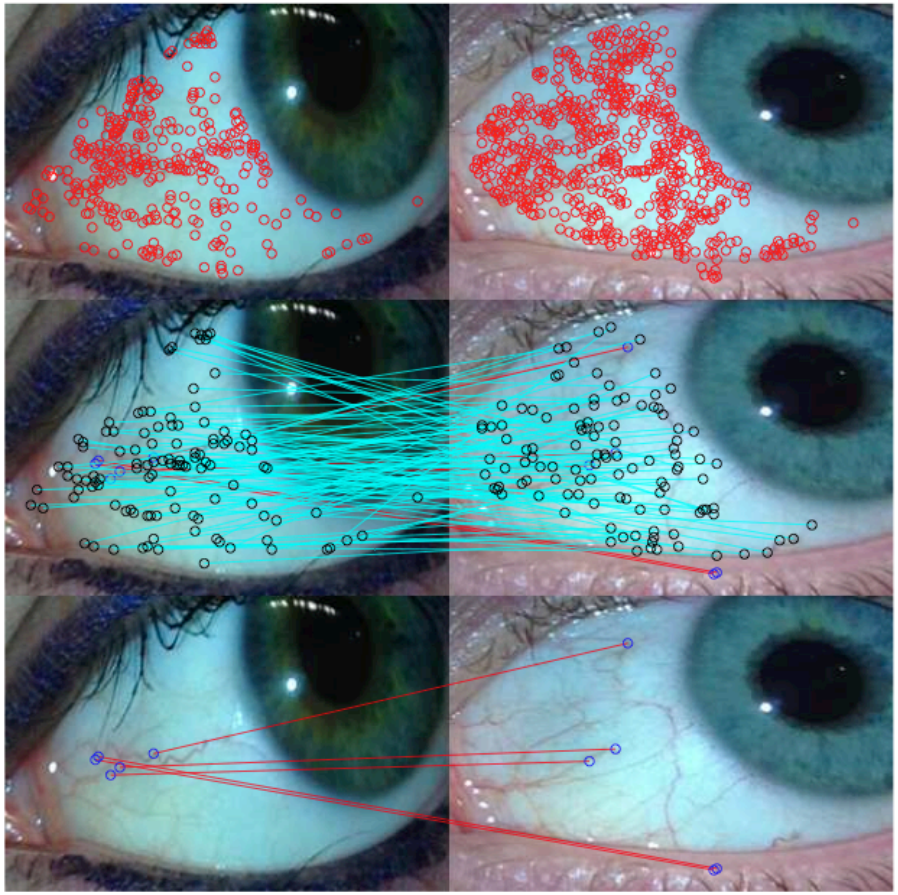


Challenge 2

- *Mobile use case* imaging artifacts
  - Lighting, motion blur, glare and specularities, eyelid/eyelash/glass occlusions
- Mitigation:
  - Lucky imaging/no reference quality metrics
  - Robust features and matching/fusion routines amenable to partial data
  - Multi-sample and context aware multi-template match score fusion

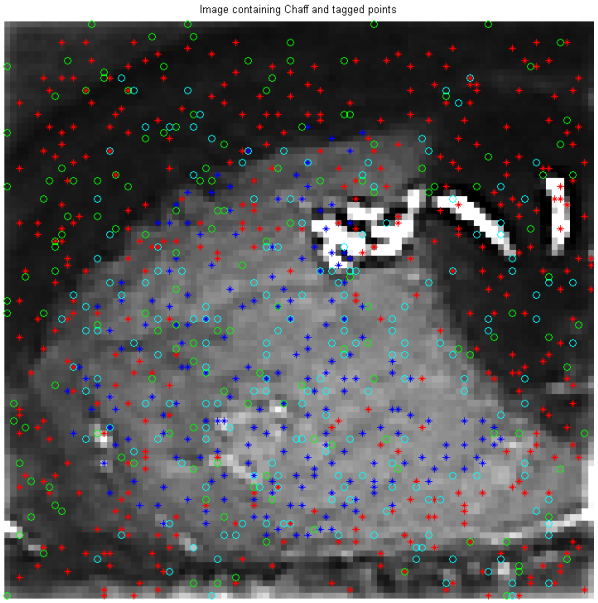
Genuine and Impostor Comparisons





Challenge 3

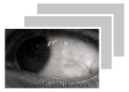
- Template security and revocability
  - Steganography
  - Device-bound isometric transforms
  - Revocable, private, and high entropy private key generation
    - Stable despite biometric intra-class variations
    - Always resolves to a private key, but valid sequence only achieved during successful genuine comparison



Blue - Enrollment Points; Red - Chaff Points; Green - Many2One tagged points; Cyan - Hash tagged points

To Recap:

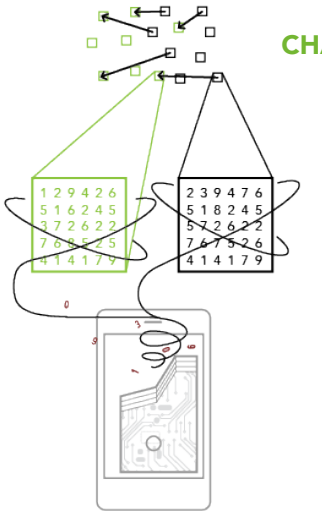
Enrollment



Step 1:
IMAGE CAPTURE

Step 2:
SEGMENTATION & ENHANCEMENT

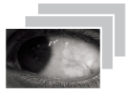
Step 3:
INTEREST POINT DETECTION & FEATURE EXTRACTION

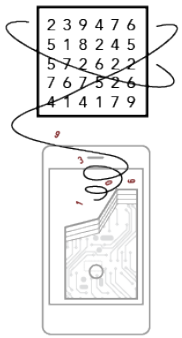


Step 4:
CHAFF POINTS ADDED & TAGGED

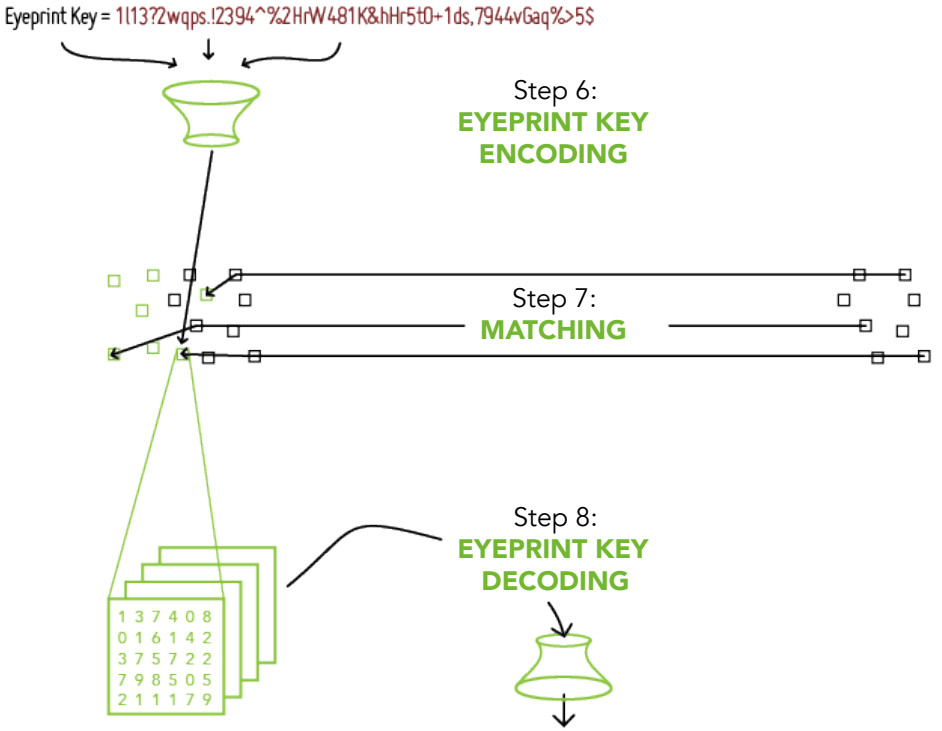
Step 5:
SCRAMBLE DESCRIPTORS

Verification





Enrollment



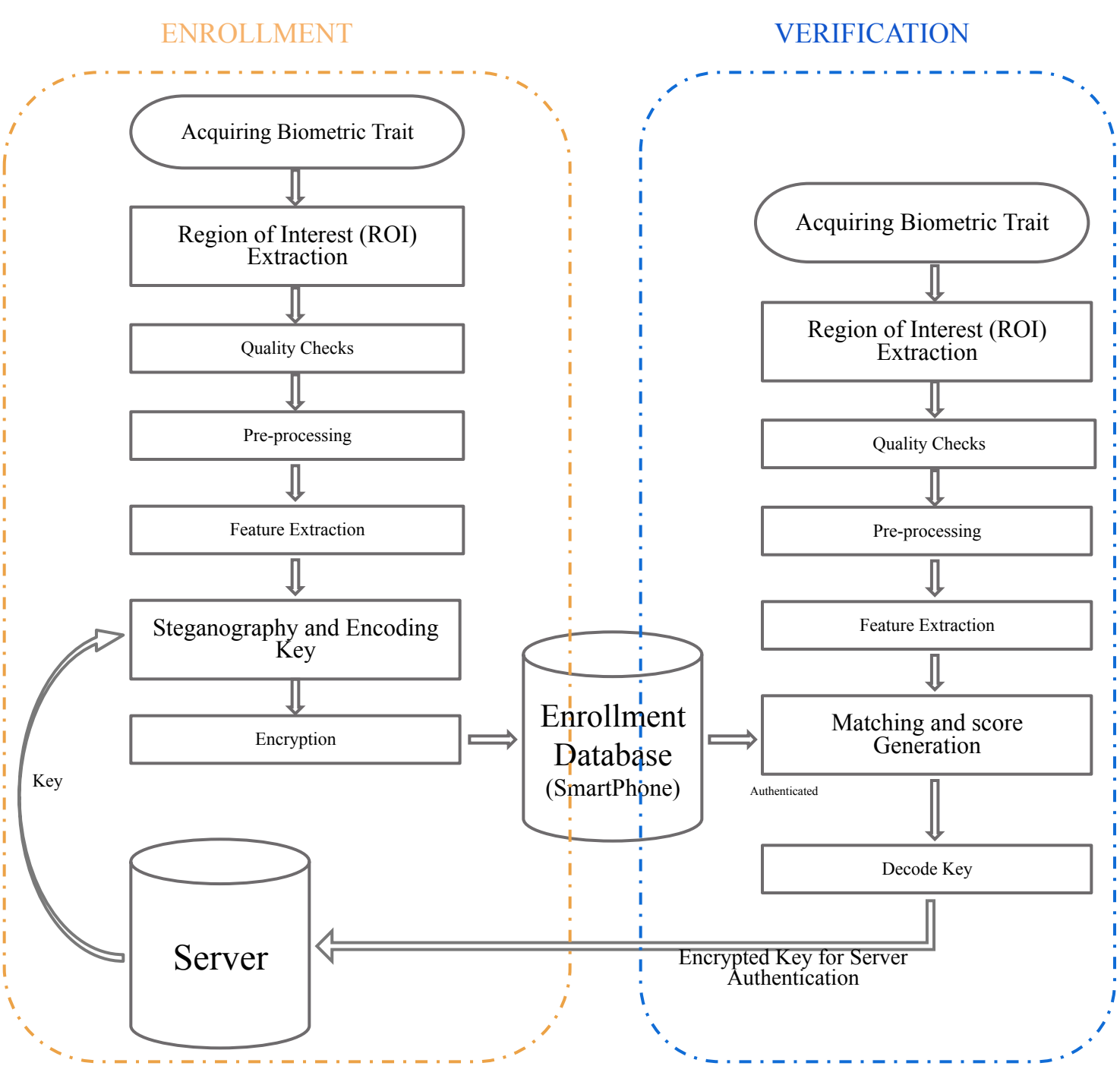
Verification

Eyeprint Key = 1l13?2wqps.!2394^%2HrW481K&hHr5t0+1ds,7944vGaq%>5$

Thanks

- To my R&D team and colleagues at EyeVerify, UMKC, MSU, and CITeR for their contributions and support
- Questions?

Extras Slides


ENROLLMENT
VERIFICATION
Acquiring Biometric Trait
Region of Interest (ROI) Extraction
Quality Checks
Pre-processing
Feature Extraction
Steganography and Encoding Key
Encryption
Key
Server
Enrollment Database (SmartPhone)
Acquiring Biometric Trait
Region of Interest (ROI) Extraction
Quality Checks
Pre-processing
Feature Extraction
Matching and score Generation
Authenticated
Decode Key
Encrypted Key for Server Authentication

Segmentation

Back Facing Captures (8-Megapixel)

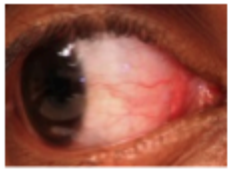
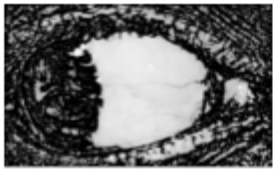
- Done using morphological operations and by measuring intensity variations in an image.

* *Led by Pavan Tankasala*

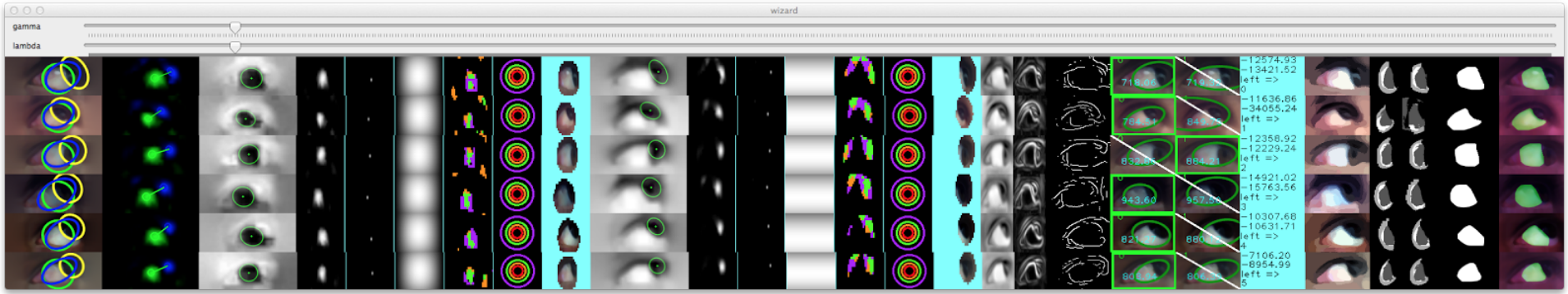
Front Facing Captures (1.3-Megapixel)

- Using the estimated eye shapes, upper eyelid, lower eyelid and limbus boundary across various color spaces, the definitive foreground and background are used to derive the final segmentation using GrabCut.

* *Led by David Hirvonen*

Above - Back facing captures. Below - Front facing captures



Accuracy

3rd Party Testing by Purdue University

Biometric Standards, Performance and Assurance Lab

- 250 subjects, broad cross section of races and ethnicities
- Independent data capture and analysis by Purdue
- Eyeprint FAR False Accept Rate = 2/100,000 at 0.88% FAR

Detailed White Paper available here

Stable Biometric Feature Set

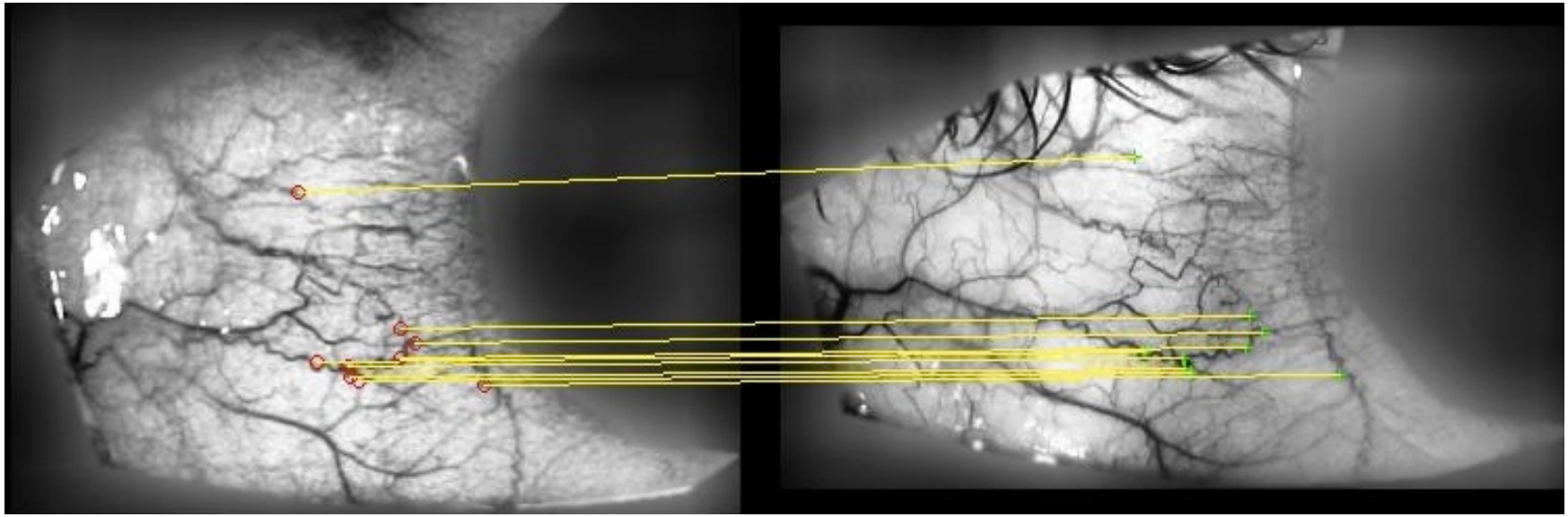
All vein patterns including eye veins are absolutely unique to each human

- Even identical twins and clones have unique vein patterns

Eyeprints are stable

- Research shows stability for a minimum of 2 years
- Anecdotal evidence indicates seven year plus stability
- Templates can be updated over time to ensure aging of user and templates remain consistent

2006 2013

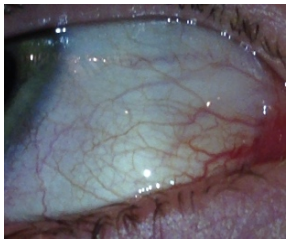


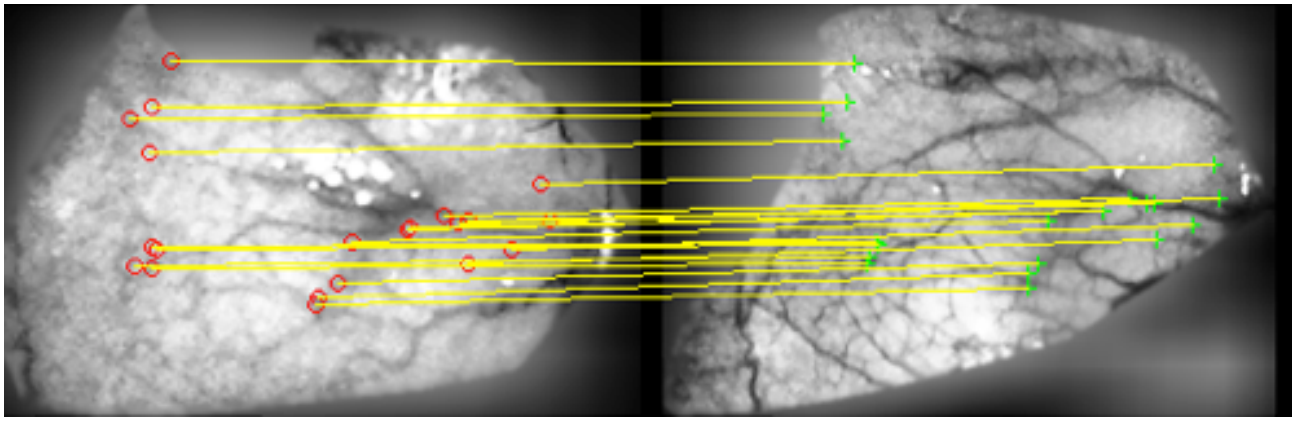
Images of the same person – seven years later - the vein patterns match perfectly

Stable Biometric Feature Set

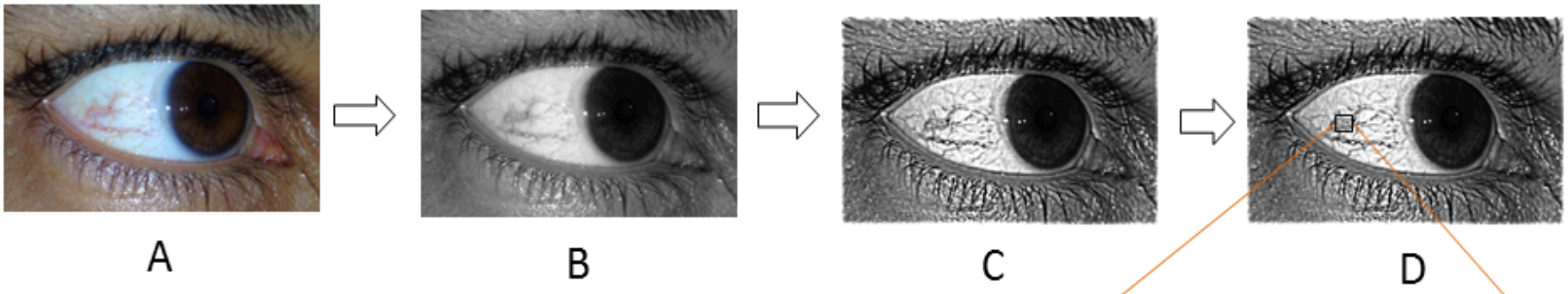
Eyeprint users with contact lenses and eye glasses, even red and bloodshot eyes are no problem (hangover, dust, pink eyes)

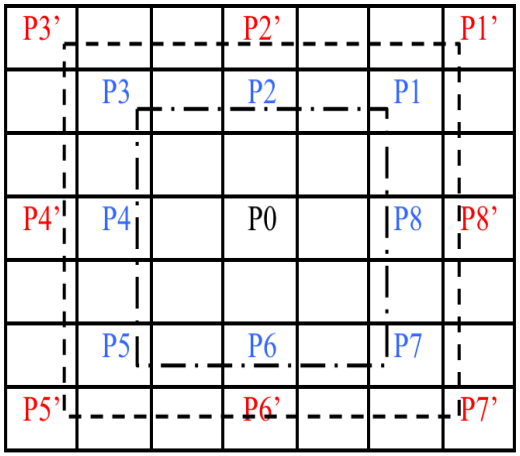
- Eyeprint algorithms look for strong vein patterns and descriptors
- Small capillaries or more pronounced veins have very little impact

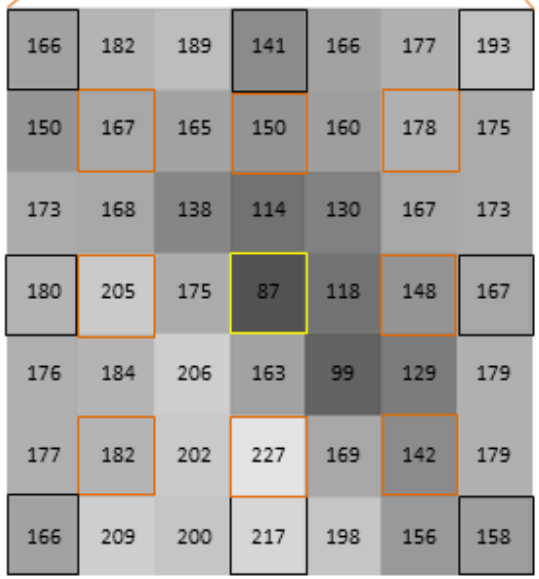




Preprocessing and Interest Point Finders

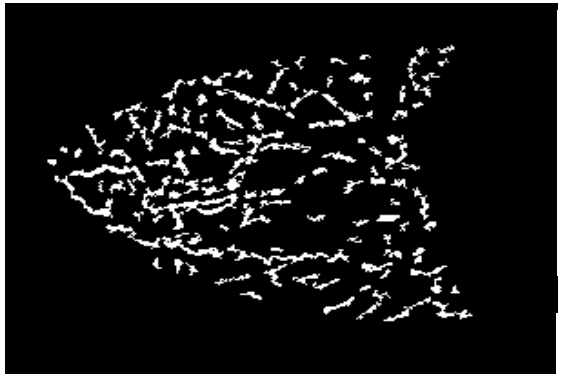






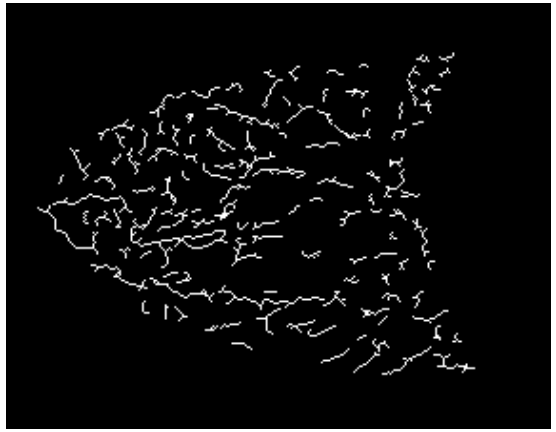
E

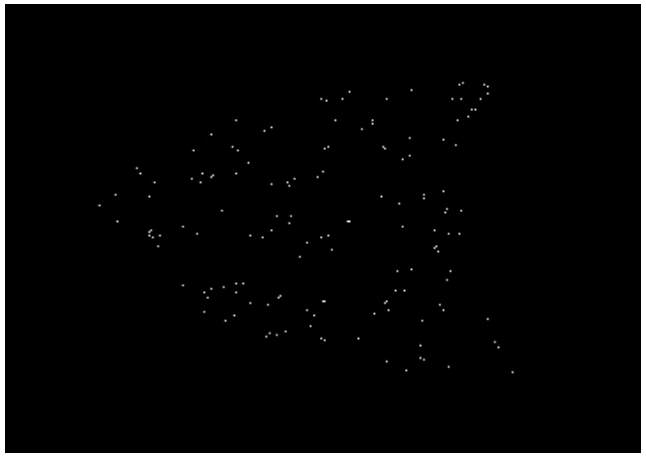
Finding Points of Interest



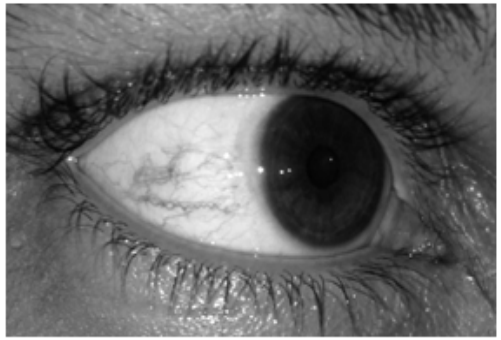
-1	0	1
-2	0	2
-1	0	1

1	2	1
0	0	0
-1	-2	-1

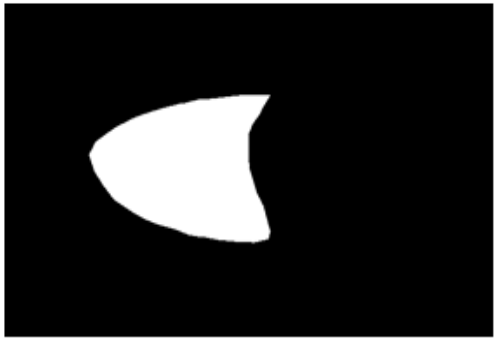




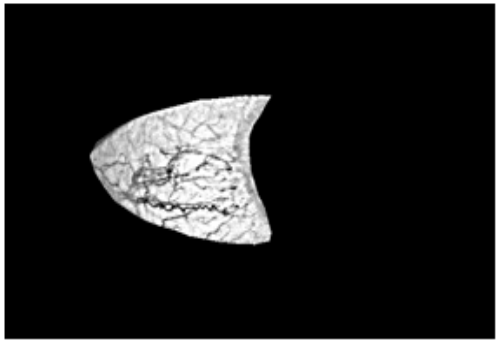
Result For Stage 1 Feature Extraction



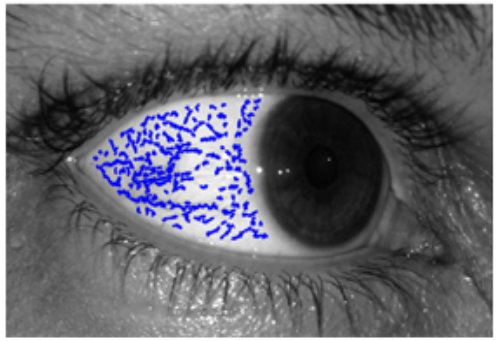
A



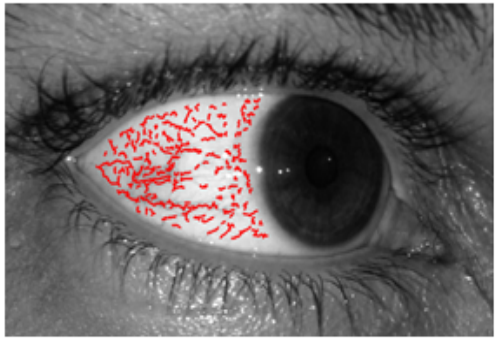
B



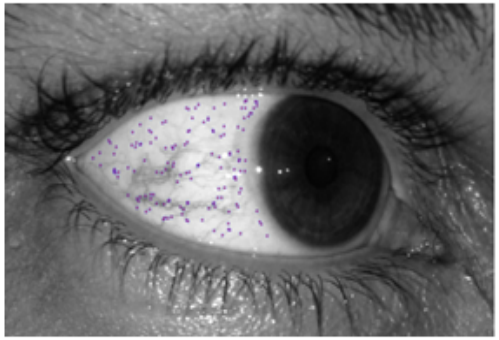
C



D



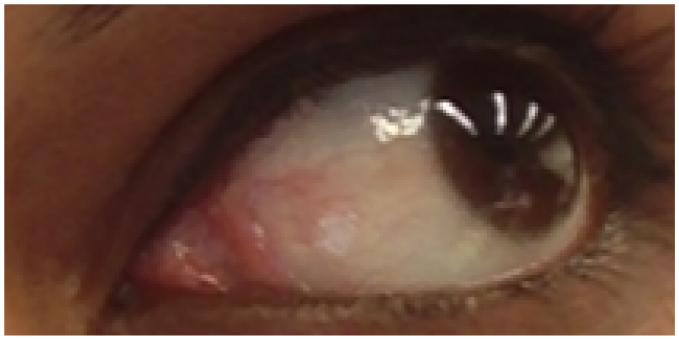
E



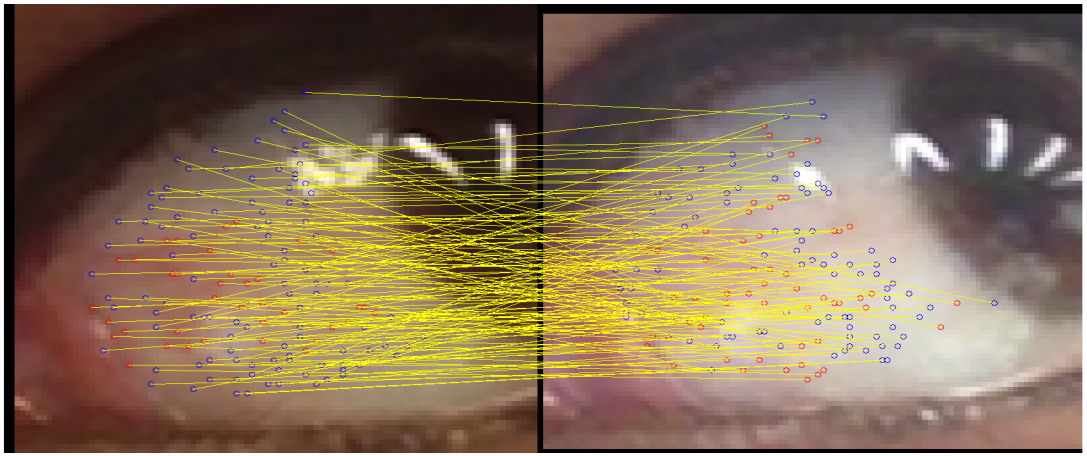
F

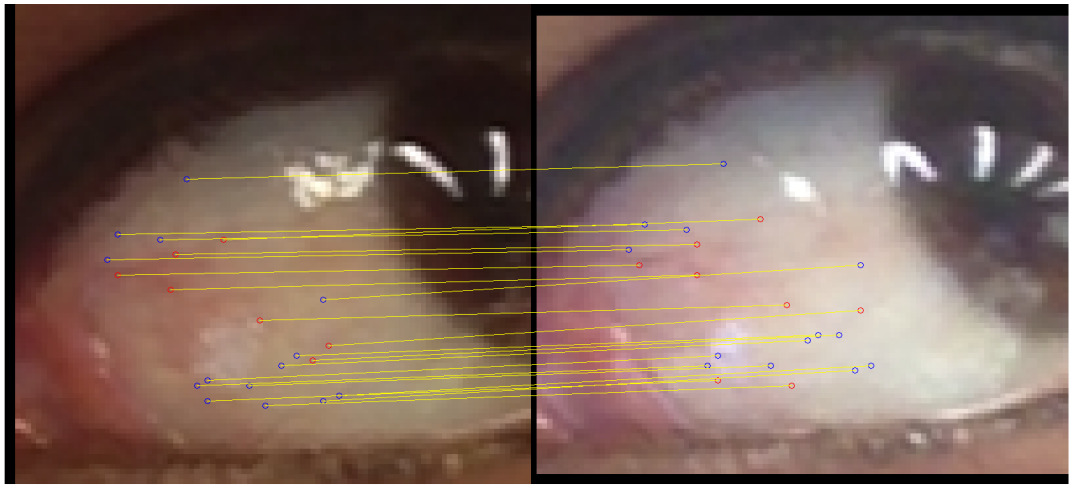
- Next: multi descriptor fused match score followed by hypothesis based registration and outlier detection for robust matching

Enrollment Image

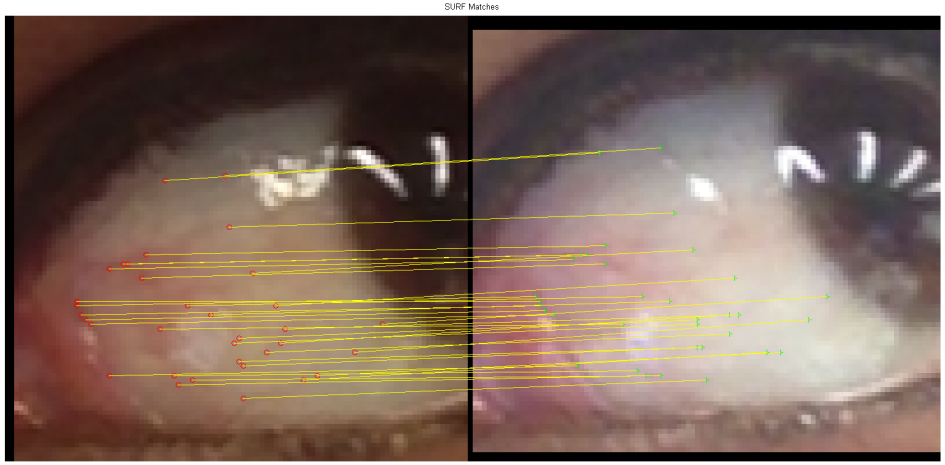


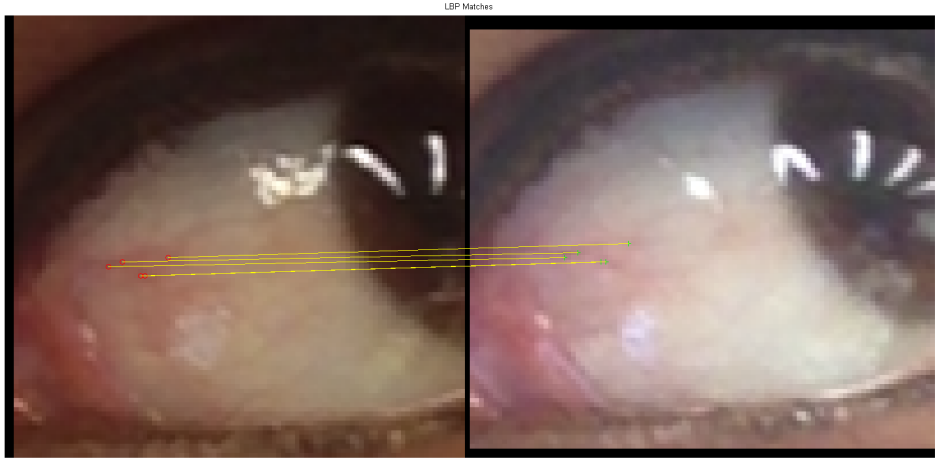
Verification Image

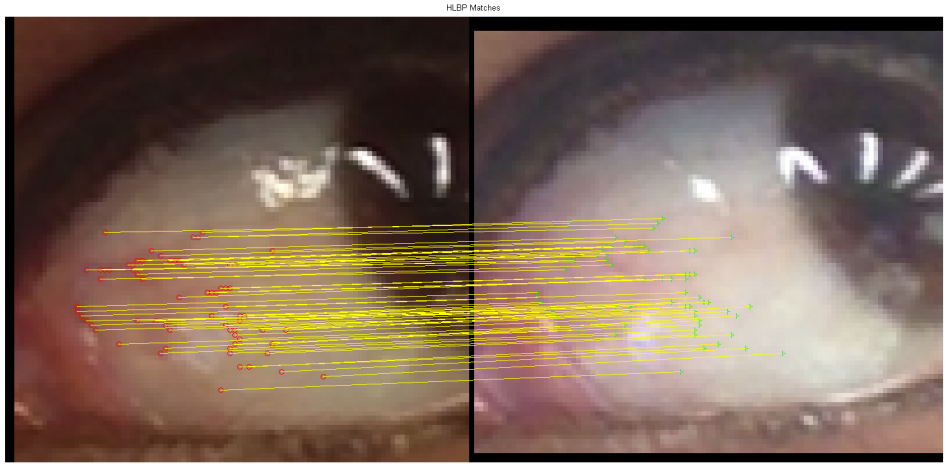


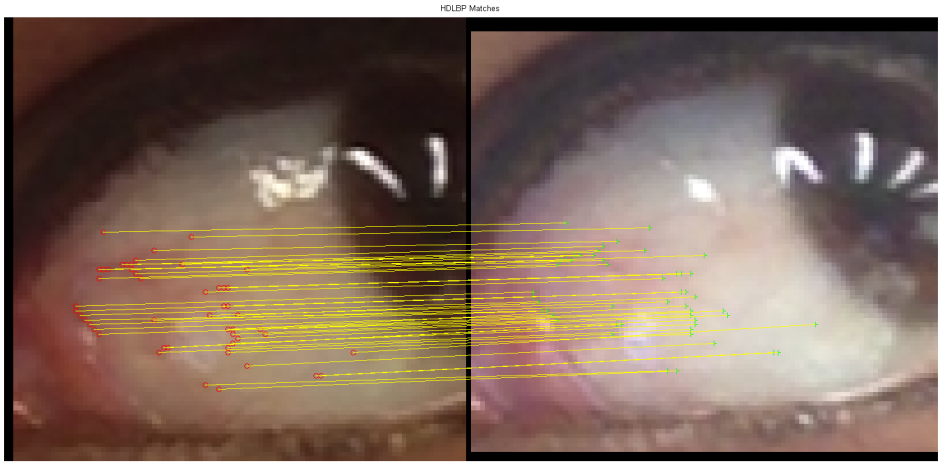


Our New vs. Existing Descriptor Matches

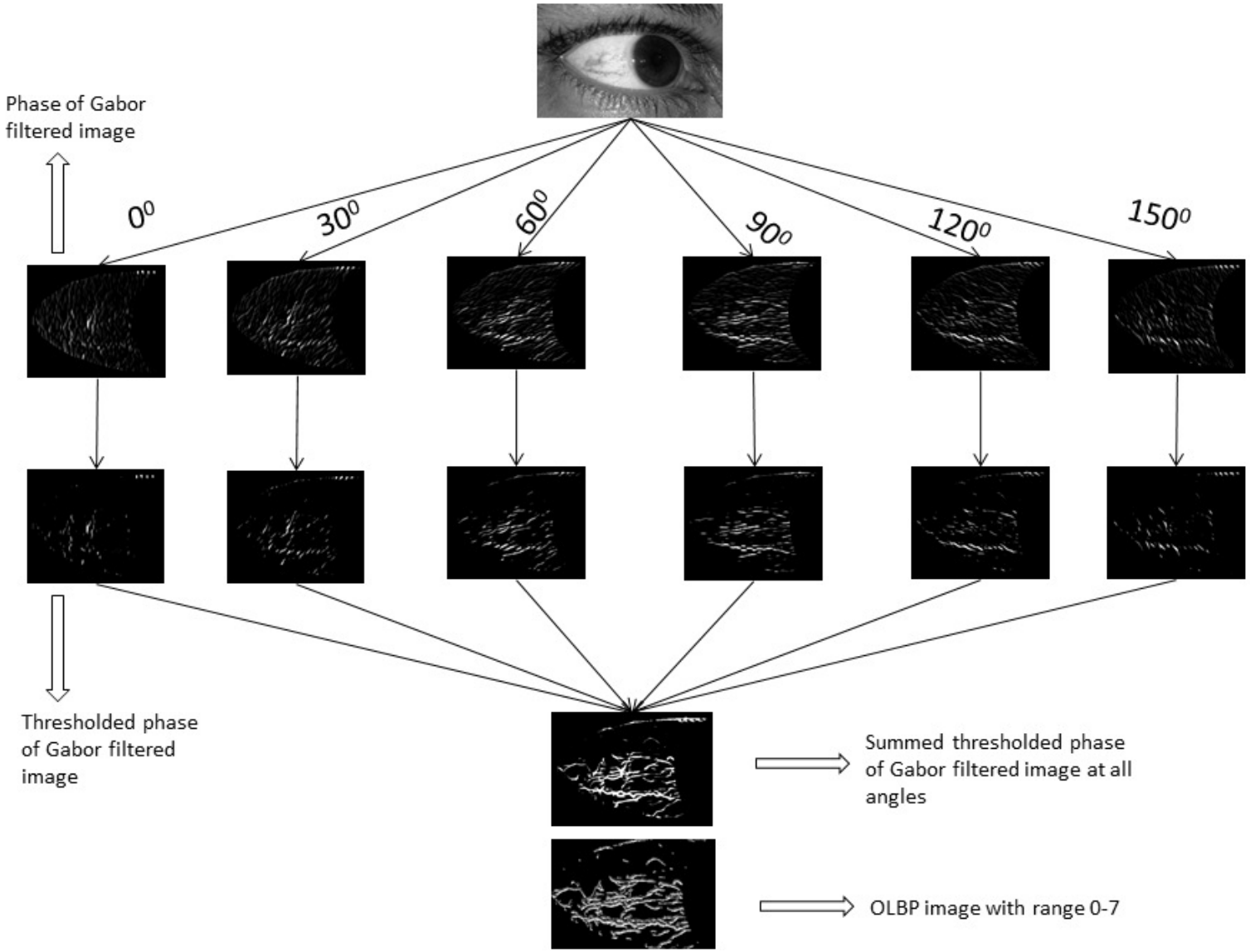






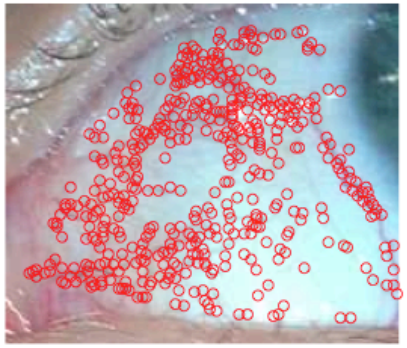


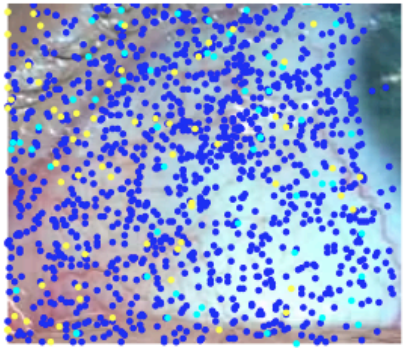
Gabor Preprocessing

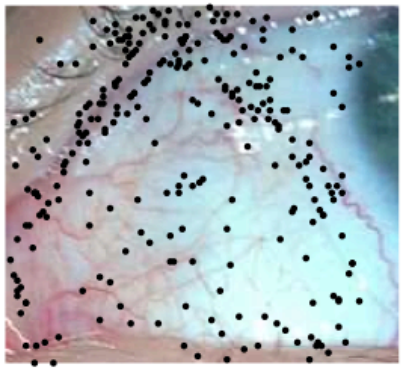


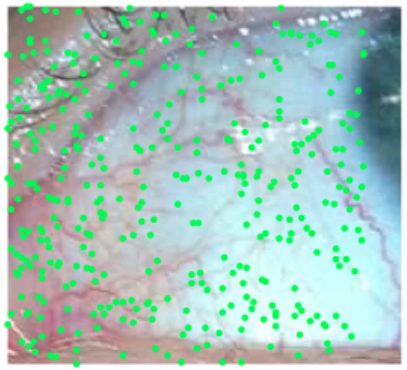
Template Security

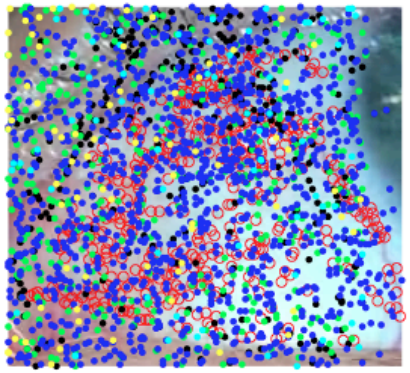
- Templates are steganographed by insertion of chaff points and fake but statistically indistinguishable descriptors.
- The template is device-bound by additive distance preserving transforms, lossy compression loadings, and whitening.
- Valid released chaff handshake (using OTP hashes, different from key material) upon genuine verification with a third party for private server side surrogate verification and revocability, and possible attack vector detection.
- System of equations based key encoding and retrieval from properly tagged chaff (only upon successful authentication)

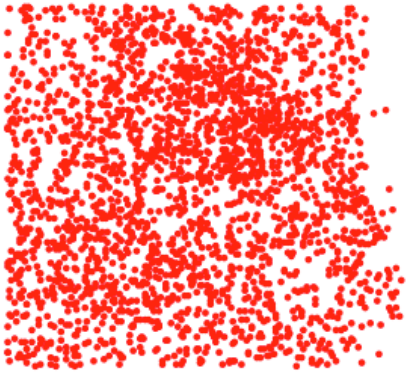












Obfuscation of original points (Left to right and top to bottom:

- OP
- {CP, TCP, SCP}
- TP
- SP
- {OP, TP, SP, CP, TCP, SCP}
- {OP, TP, SP, CP, TCP, SCP}