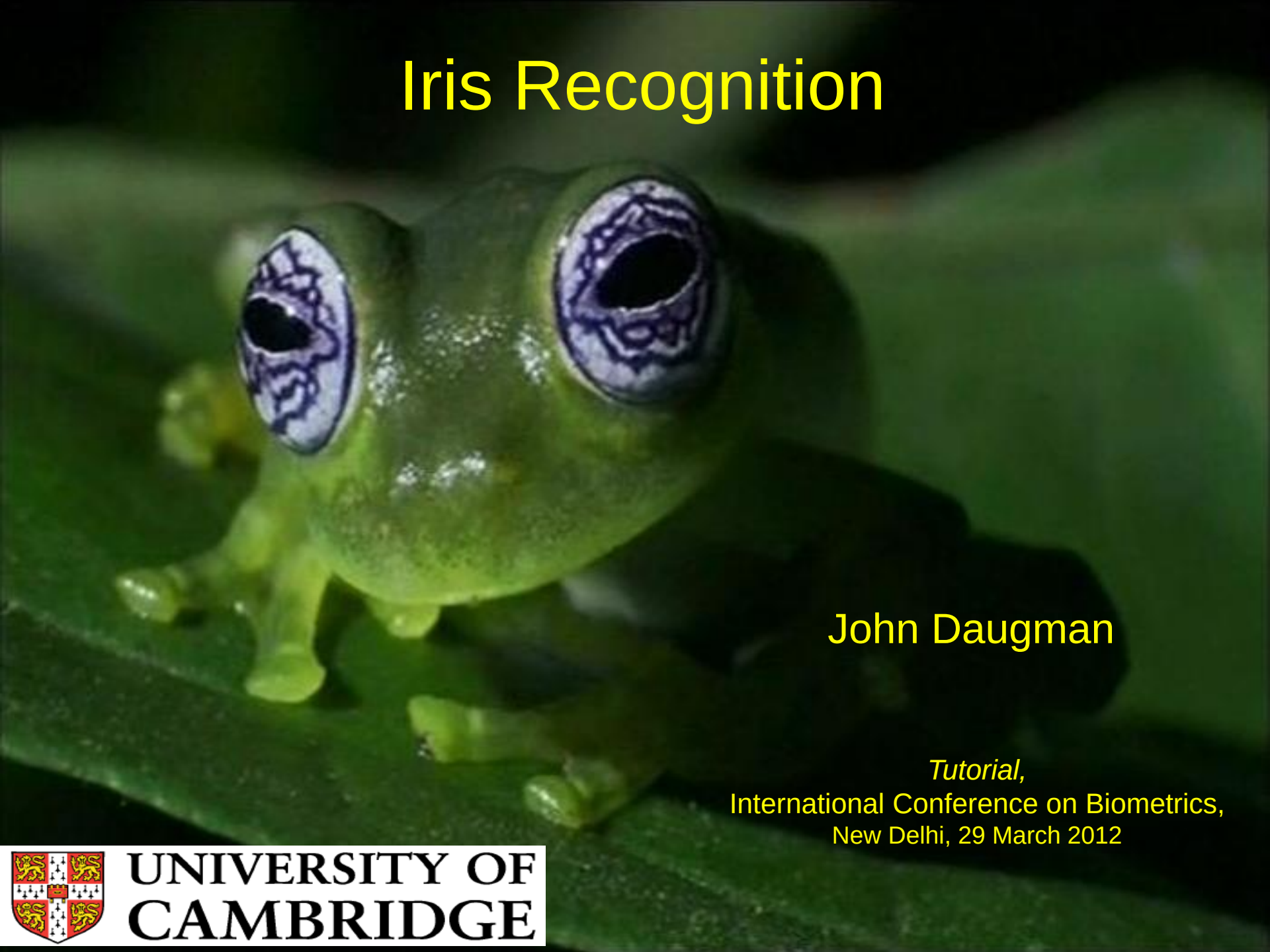
Iris Recognition

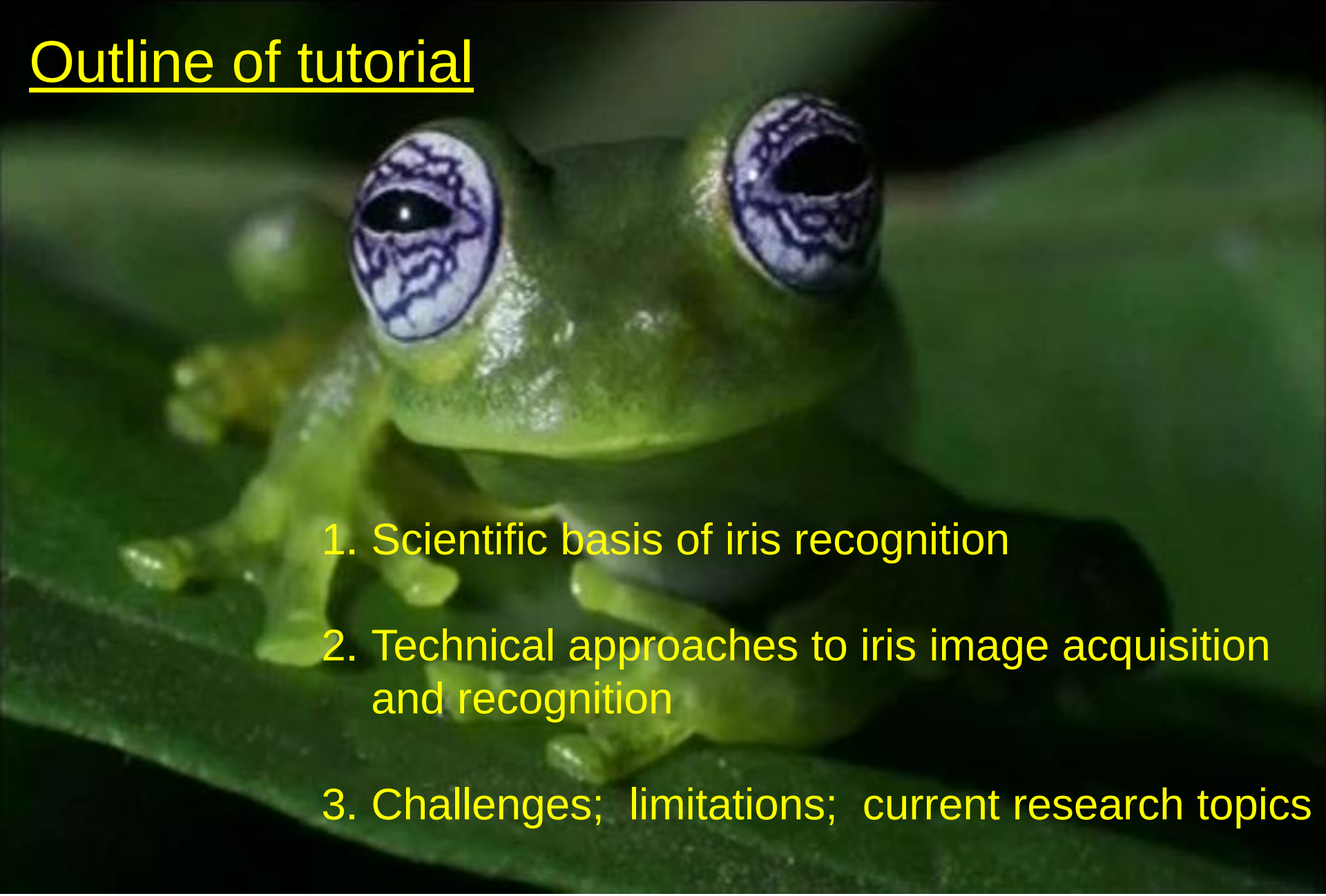


John Daugman

Tutorial,
International Conference on Biometrics,
New Delhi, 29 March 2012

UNIVERSITY OF CAMBRIDGE

Outline of tutorial



1. Scientific basis of iris recognition

2. Technical approaches to iris image acquisition and recognition

3. Challenges; limitations; current research topics

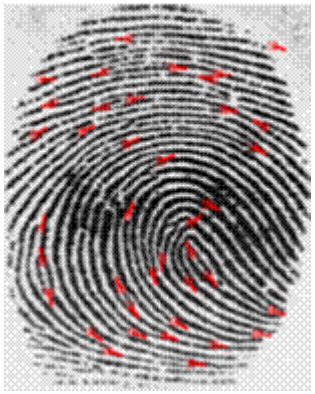
Automatic Identification of Persons

- Traditional Methods:
  - special possessions (cards, documents, keys, ...)
  - secret knowledge (passwords, PIN numbers, ...)
- Biometric [*"Biological Measurement"*] Methods
  - some unique, complex feature of a person's accessible anatomy, physiology, or behaviour
  - E.g. fingerprint, voice, face, iris, retina, DNA...

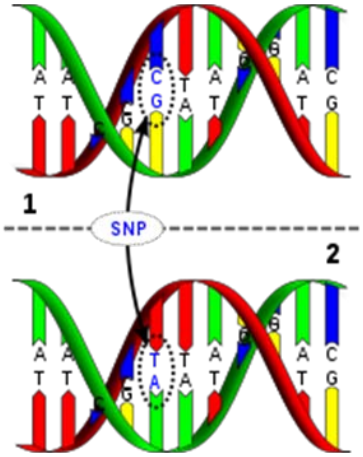
Randomness and complexity are the keys to uniqueness

UNIVERSITY OF CAMBRIDGE

Some examples of biometric methods and applications



Forensics

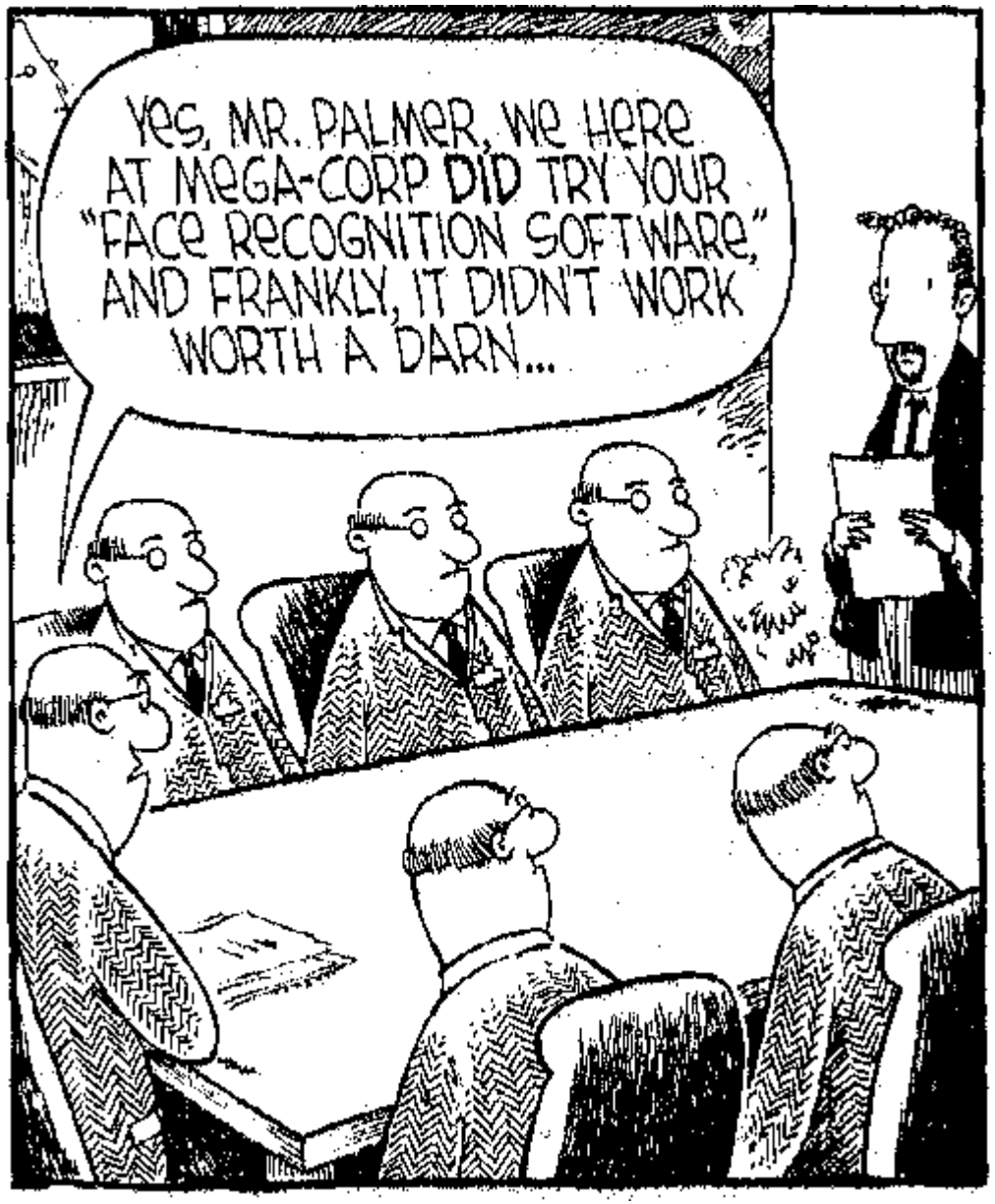


"IrisKids" (US) missing children registration and identification

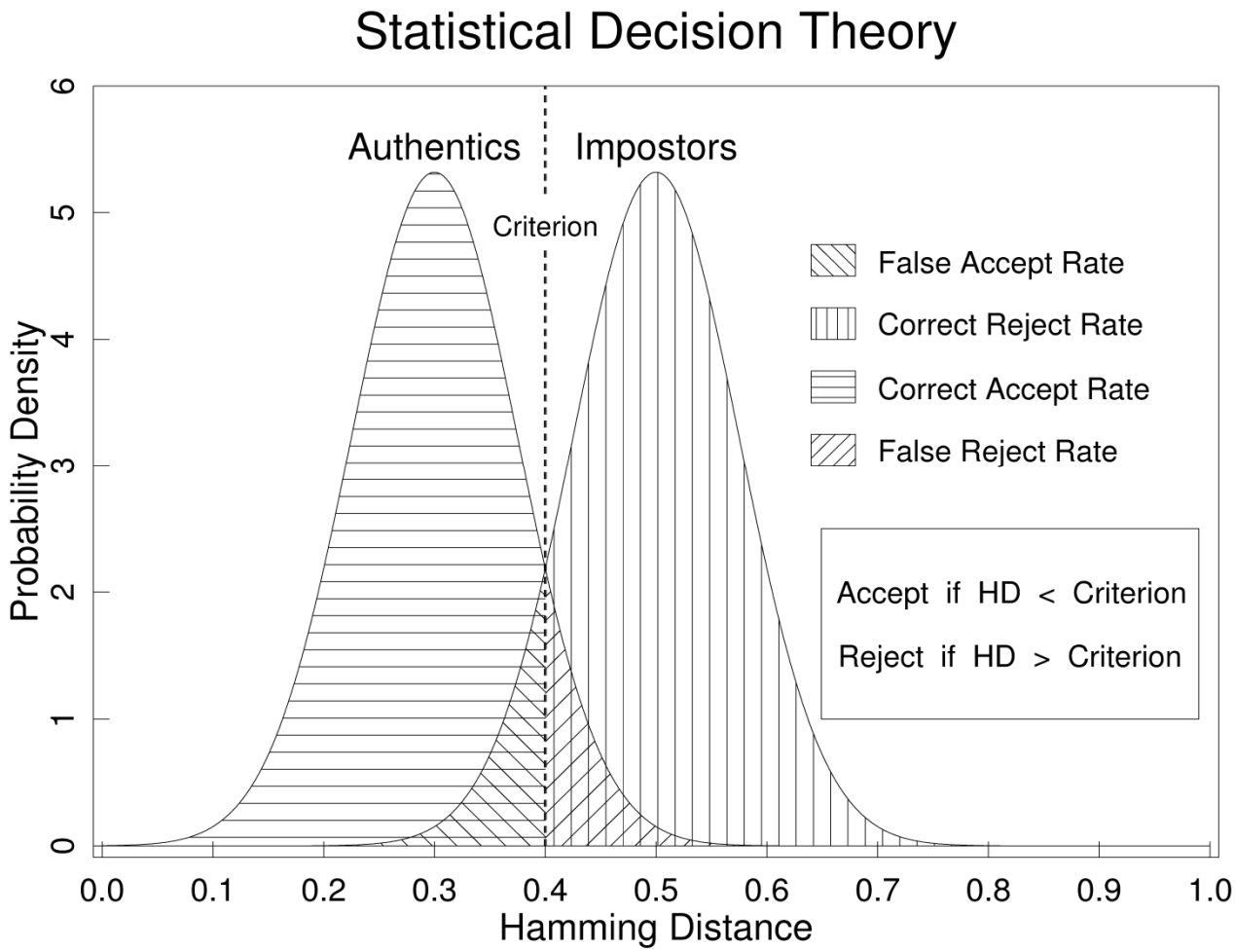
Face recognition ??

Home Office
Border & Immigration Agency

UNIVERSITY OF CAMBRIDGE



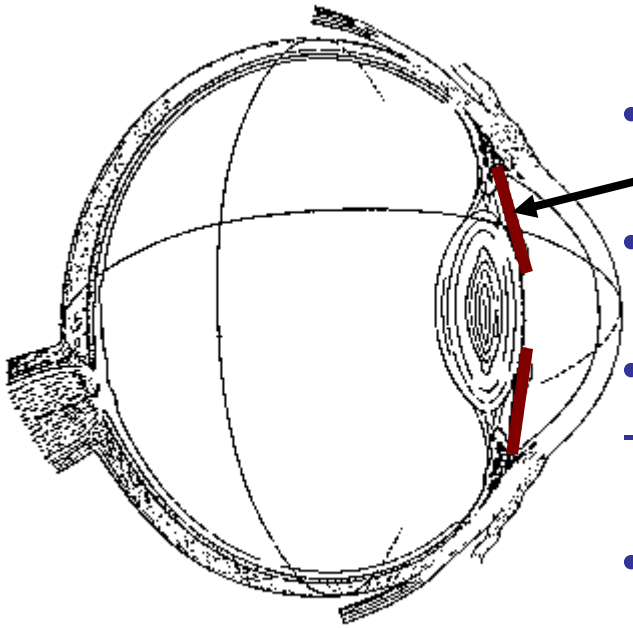
UNIVERSITY OF CAMBRIDGE



Biometric decision power depends on the magnitudes of within-person variability and between-person variability

UNIVERSITY OF CAMBRIDGE

Properties of the Iris as an Identifier



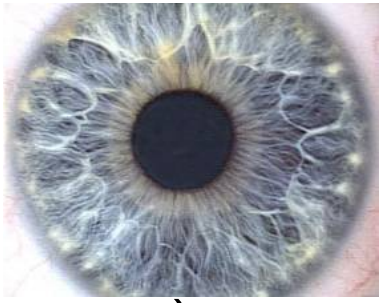
- Highly protected, internal organ of the eye
- Externally visible, from distance up to some meters
- Random pattern of great complexity & uniqueness
  - (keys to uniqueness are randomness + complexity)
- Pattern is epigenetic (not genetically determined)
- Presumed stable, apart from pigmentation changes
  - (no evidence of any visible pattern changes, although there is some evidence that computed IrisCode templates may “age”)

UNIVERSITY OF CAMBRIDGE

Developmental Morphogenesis and Chromatic Properties

• The human iris begins to form during the third month of gestation.

• The structures creating its distinctive pattern are complete by the eighth month of gestation, but pigmentation continues into the first years.



• The layers of the iris have both ectodermal and mesoderma embryological origin, consisting of (from back to front):

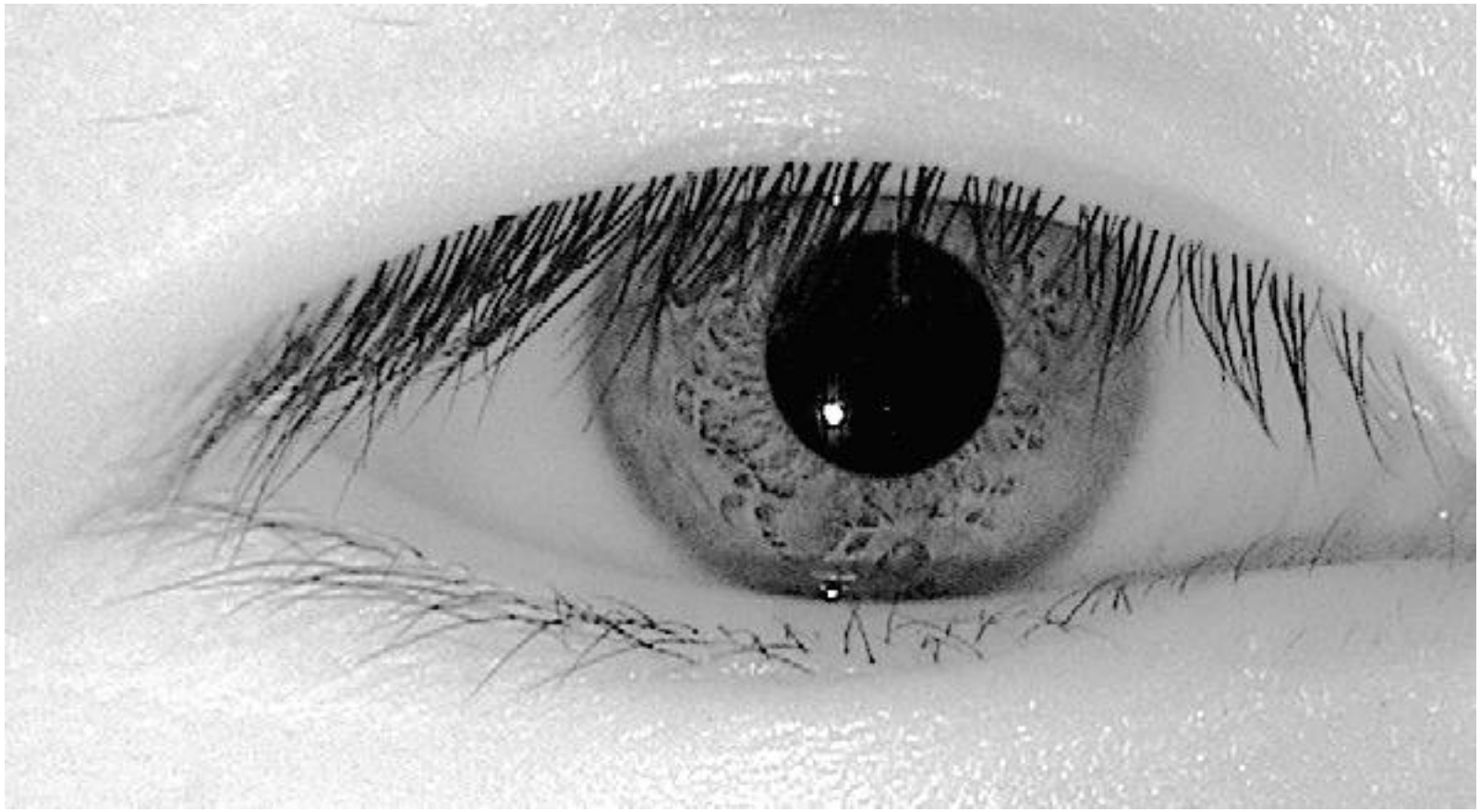
- a darkly pigmented epithelium;
- pupillary dilator and sphincter muscles;
- vascularized stroma (connective tissue of interlacing ligaments);
- an anterior layer of chromataphores and melanocytes with a genetically determined density of melanin pigment granules.

• Iris colour is determined mainly by the density of the stroma and its melanin content, with blue irises resulting from an absence of pigment: longer wavelengths differentially penetrate while shorter wavelengths are scattered, a phenomenon resembling that which makes the sky blue.

In the visible band of light, the iris reveals a very rich, random, interwoven texture (the *“trabecular meshwork”*)

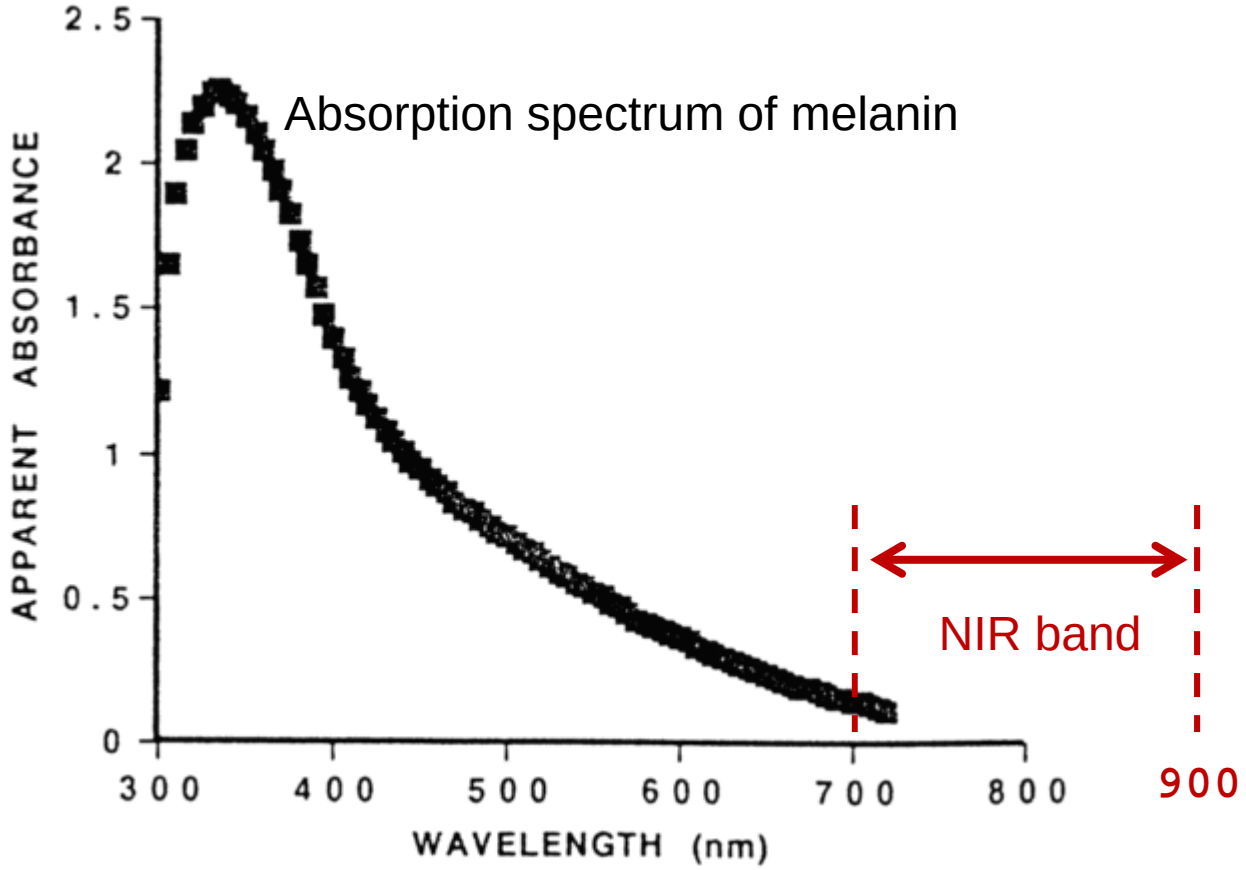
UNIVERSITY OF CAMBRIDGE

But even “dark brown” eyes show rich texture when images are captured in infrared illumination

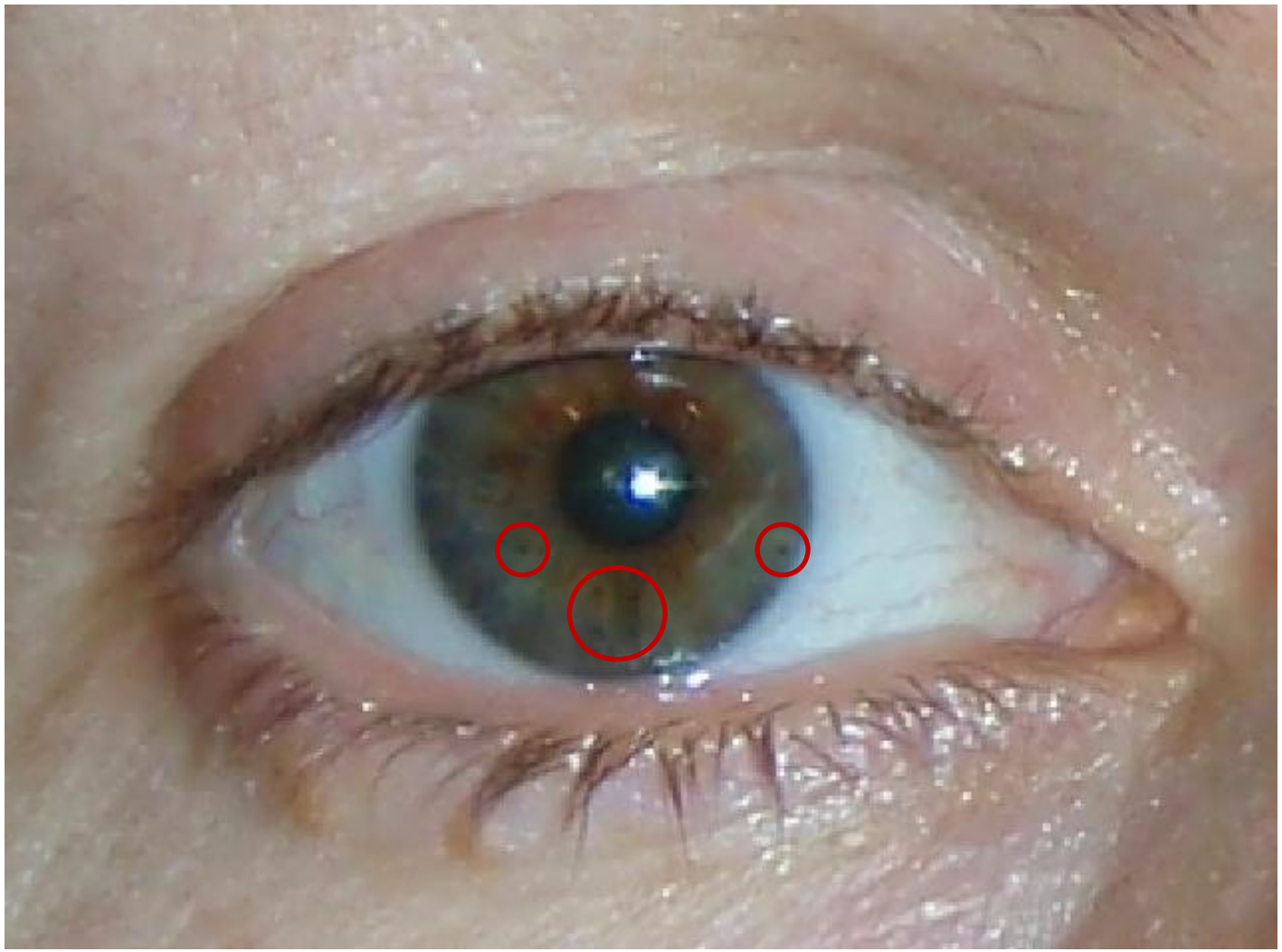


UNIVERSITY OF CAMBRIDGE

All pigmentation variations are due to melanin density. This can sometimes change (e.g. growth of freckles, or pigment blotches); but these are invisible in the NIR (near infrared: 700nm – 900nm) band of light used in all publicly deployed iris cameras, because melanin is almost completely non-absorbing beyond 700nm.

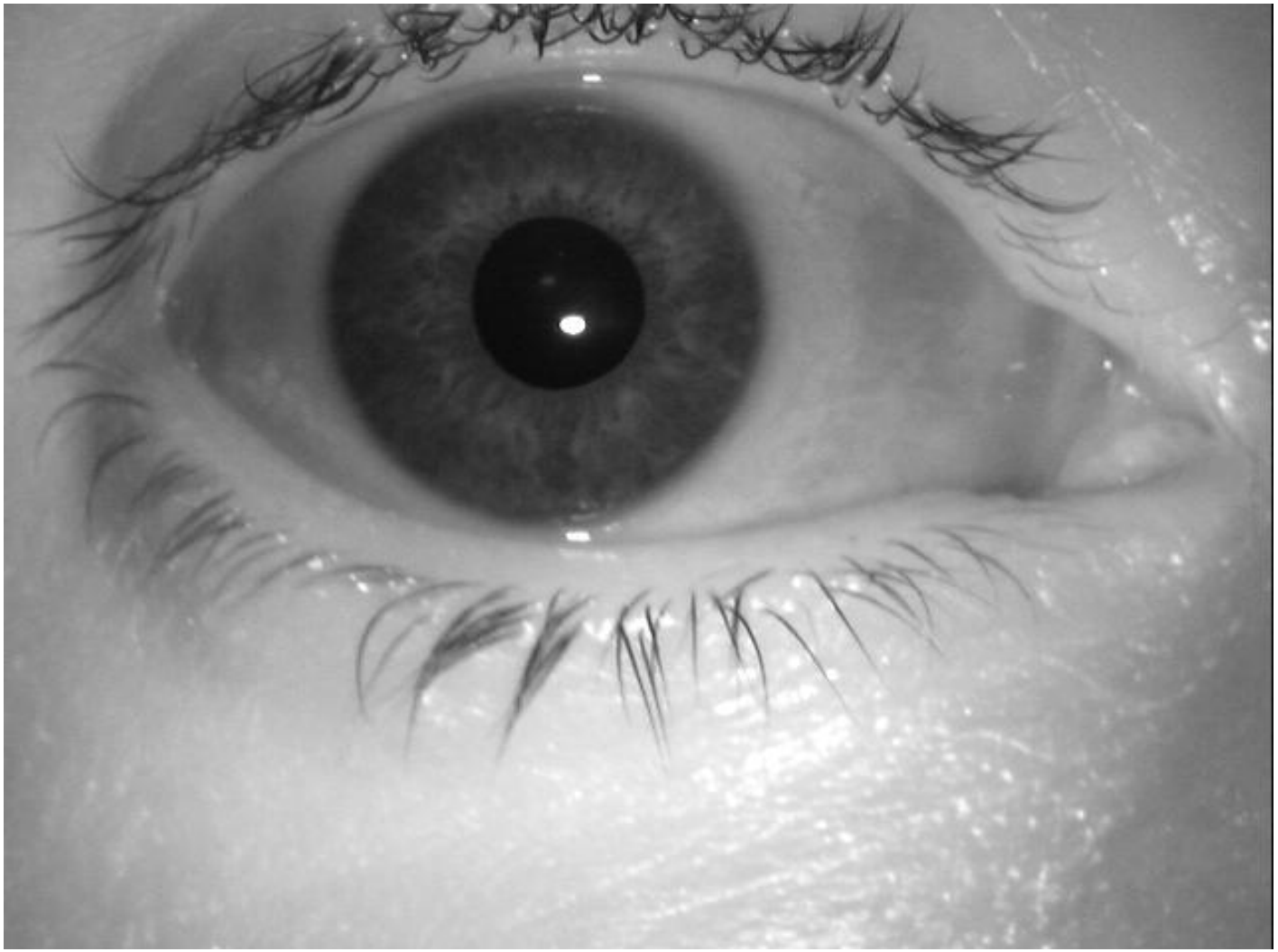


Example of an iris imaged in the visible band of illumination (400nm – 700nm), showing freckles



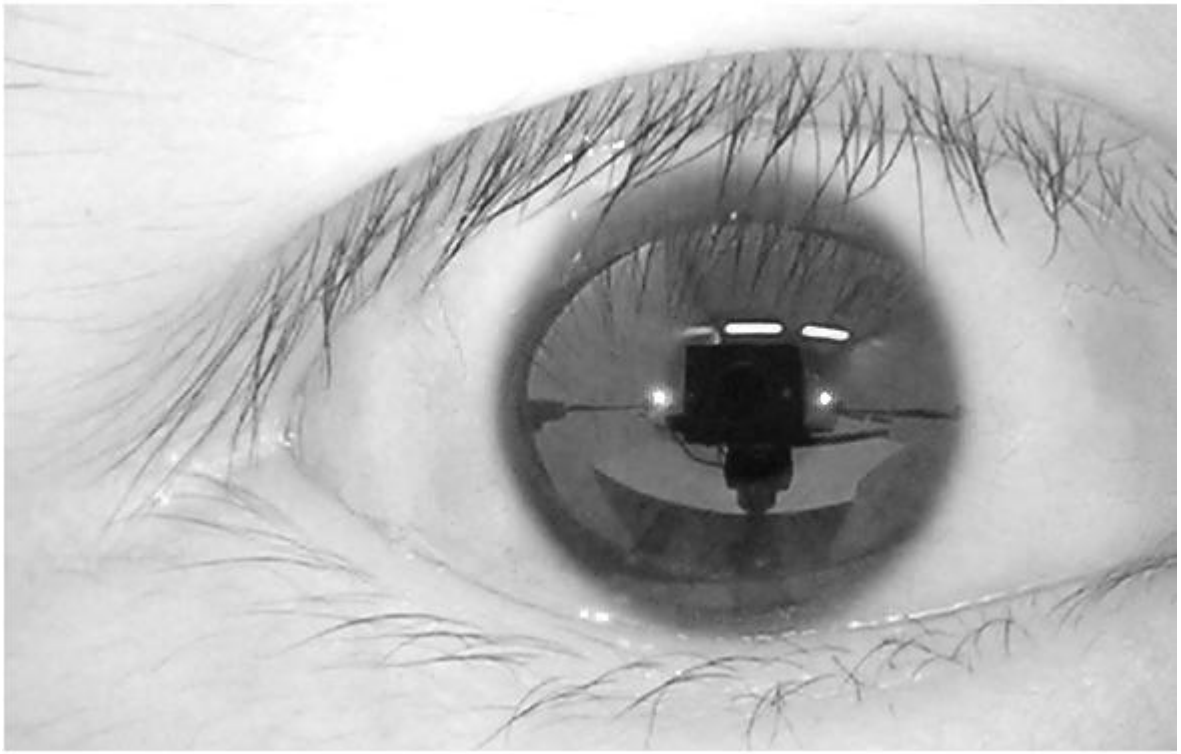
UNIVERSITY OF CAMBRIDGE

The same iris, imaged (almost simultaneously) in the (700nm – 900nm) NIR band: freckles become invisible

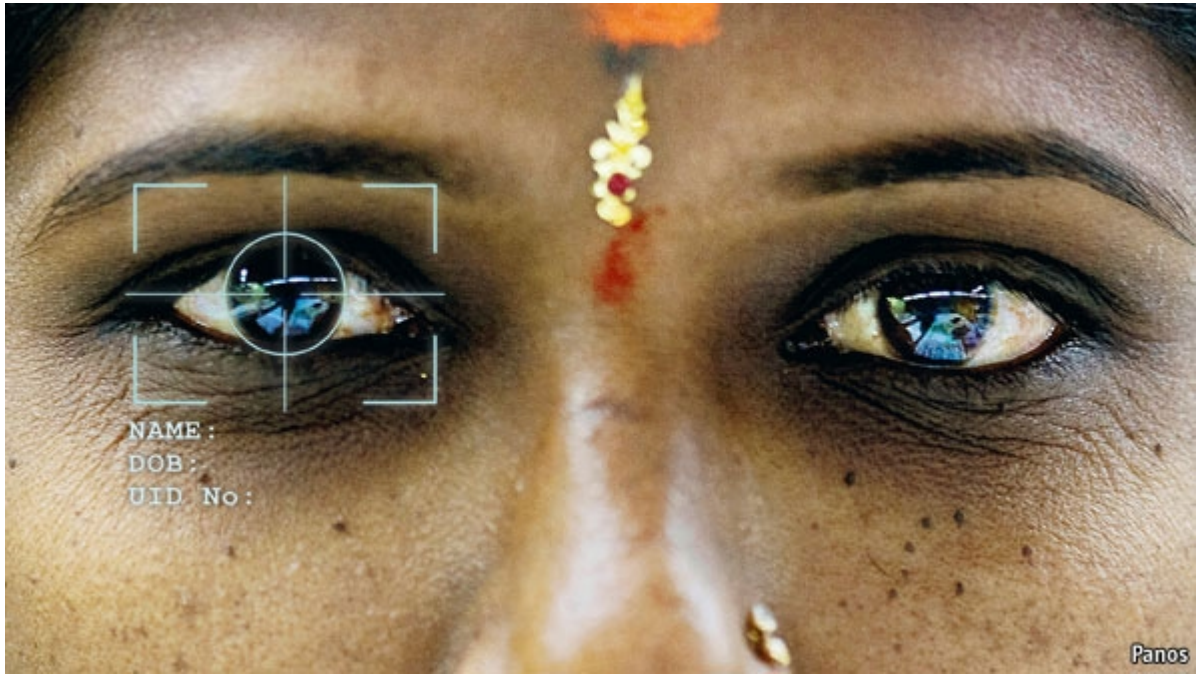


UNIVERSITY OF CAMBRIDGE

In the visible band of light in unconstrained environments (e.g. outdoors), ambient corneal reflections are common. An iris acquired in the visible band often looks like this:



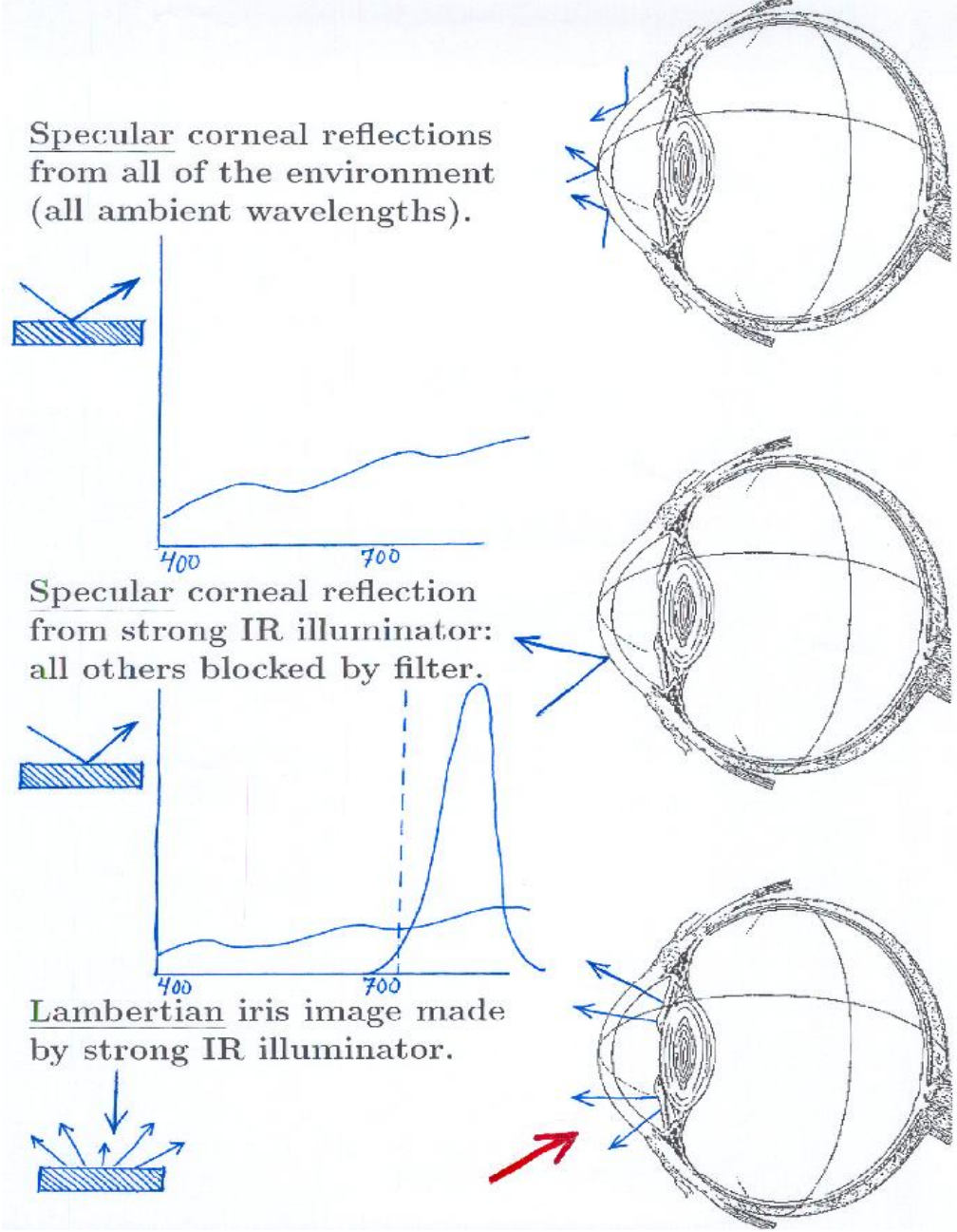
Example of how an iris with low albedo (i.e. dark brown) looks in the visible band: the corneal specular reflections completely dominate the Lambertian iris image. (From *The Economist*, 14 January 2012.)



All surfaces lie somewhere between specular (mirror-like) and Lambertian (scattering light equally in all directions).

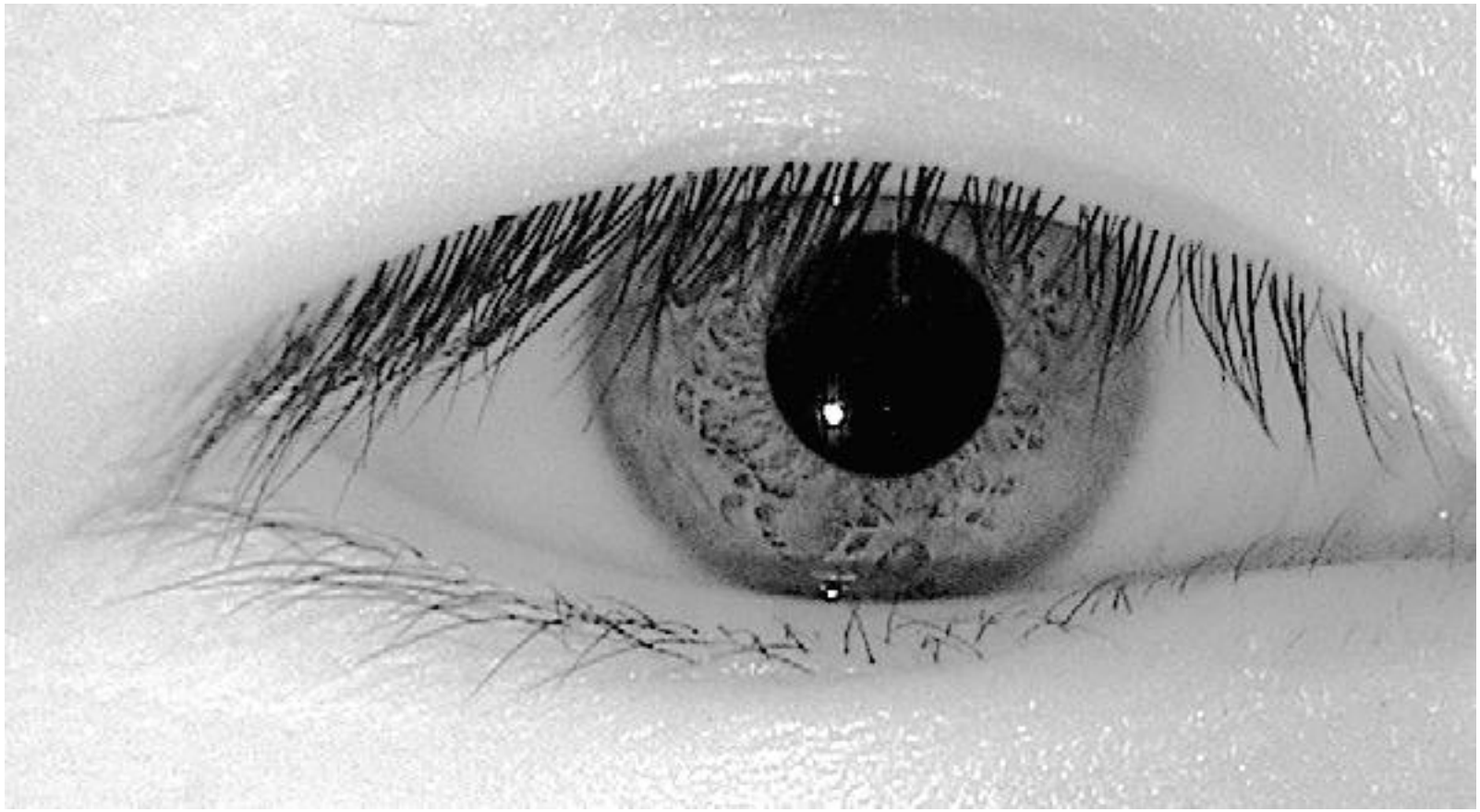
The cornea is a specular surface; the iris is Lambertian. This fact can be exploited to separate out the ambient environmental corneal reflections, which are broadband but weak, from the more narrow-band light in a nominated band projected by the camera onto the eye to obtain a Lambertian image of the iris.

By allowing back into the camera only that same nominated narrow band of light that the iris camera emitted, a band in which there is much more spectral power than in the broadband ambient corneal reflections, these two sources can be separated.



UNIVERSITY OF CAMBRIDGE

The result is an image acquired in narrowband near-infrared light, from which almost all ambient environmental corneal reflections (except for that of the illuminator) have been “scrubbed.”



UNIVERSITY OF CAMBRIDGE

Entropy: the key to biometric collision avoidance

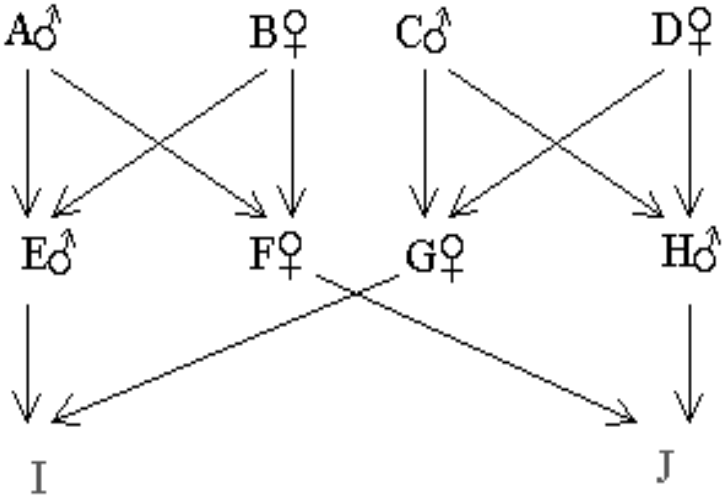
- The discriminating power of a biometric depends on its entropy
- Entropy measures the amount of random variation in a population:
  - the number of different states or patterns that are possible;
  - the probability distribution across those possible states
- Entropy H (in bits) corresponds to 2^H discriminable states or patterns
- Surviving large database searches requires large biometric entropy
- Epigenetic features (not genetically determined) make best biometrics

About 1 percent of persons have a monozygotic (“identical”) twin

UNIVERSITY OF CAMBRIDGE

Epigenetic biometric features are vital if de-duplication of a large national database is required, as in the UID programme in India.

The epigenetic biometric property is especially important in cultures with high rates of group inbreeding (*e.g.* cousin marriage), so that genetically related persons do not collide in their biometrics.



UNIVERSITY OF CAMBRIDGE

Iris Patterns are Epigenetic

Every biometric lies somewhere on a continuum between being genetically determined (genotypic) or not (epigenetic)

Examples of genotypic traits: DNA, blood type, gender, race

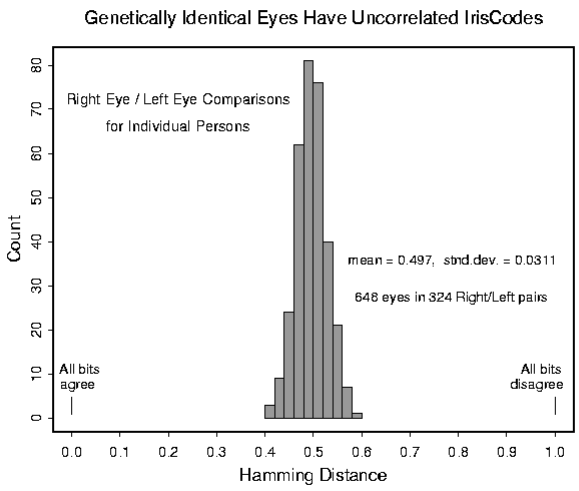
Examples of epigenetic traits: fingerprints (except for type correlations); and iris patterns (except for eye colour)

Example at middle of continuum: facial appearance. (Identical twins look identical, but they both change over time like everyone, yet they track each other as they age.)

UNIVERSITY OF CAMBRIDGE

Genetically identical eyes have iris patterns that are uncorrelated in detail:

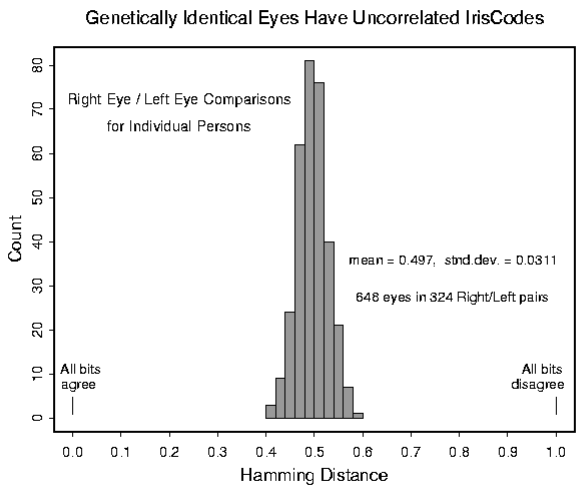
Monozygotic Twins A
(6 year-old boys)



UNIVERSITY OF CAMBRIDGE

Genetically identical eyes have iris patterns that are uncorrelated in detail:

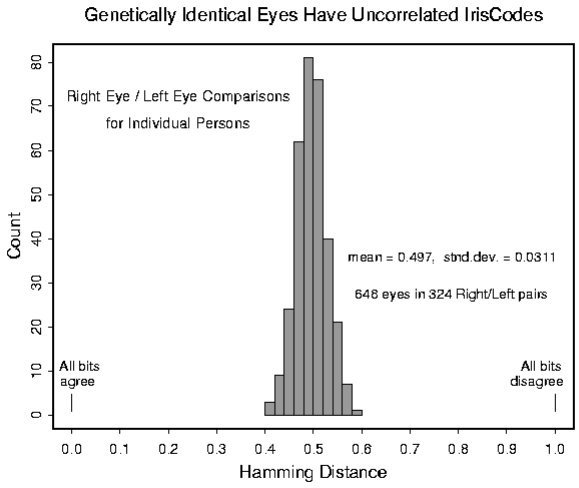
Monozygotic Twins B
(18 year-old women)



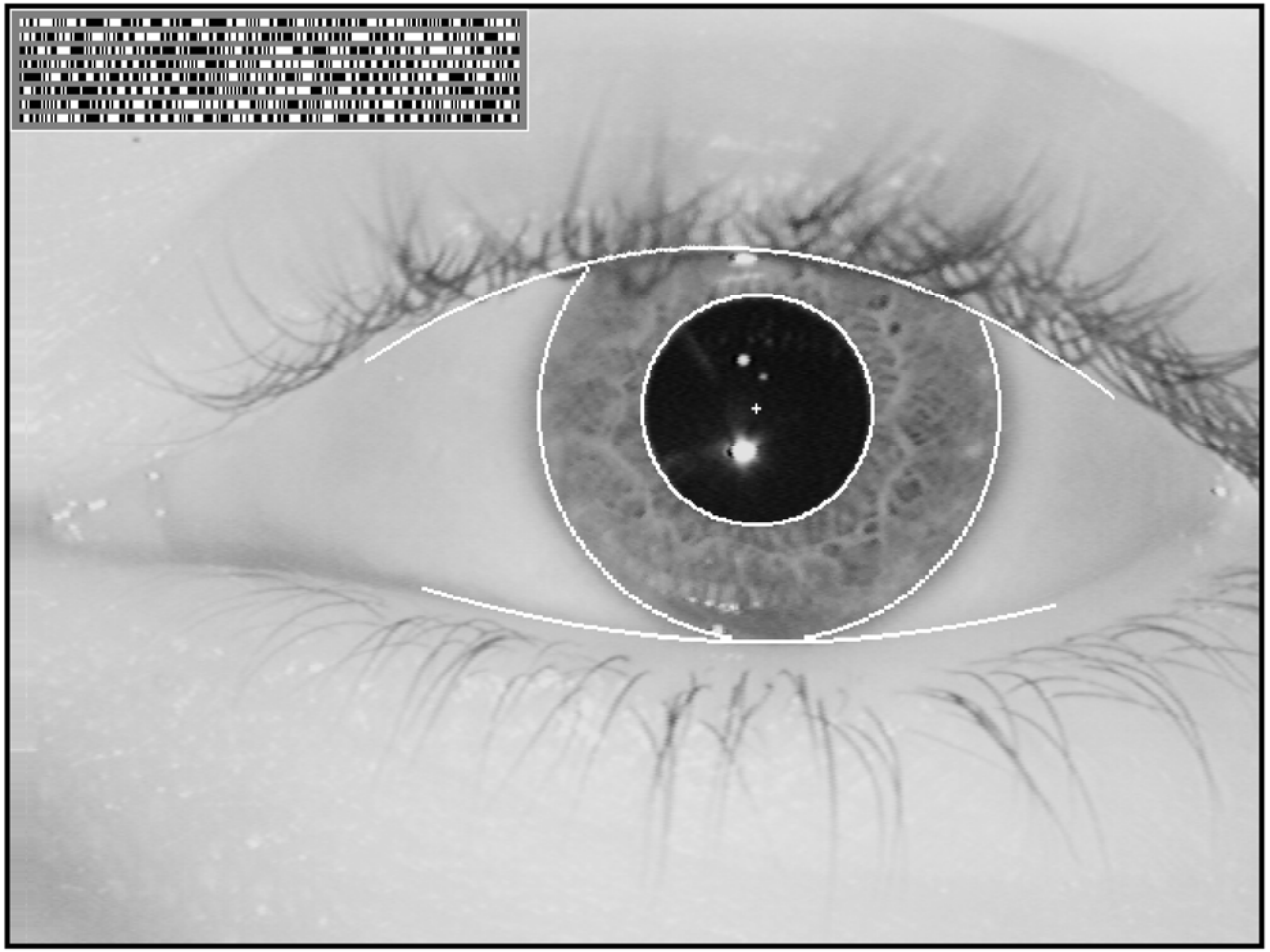
UNIVERSITY OF CAMBRIDGE

Genetically identical eyes have iris patterns that are uncorrelated in detail:

Monozygotic Twins C
(78 year-old men)



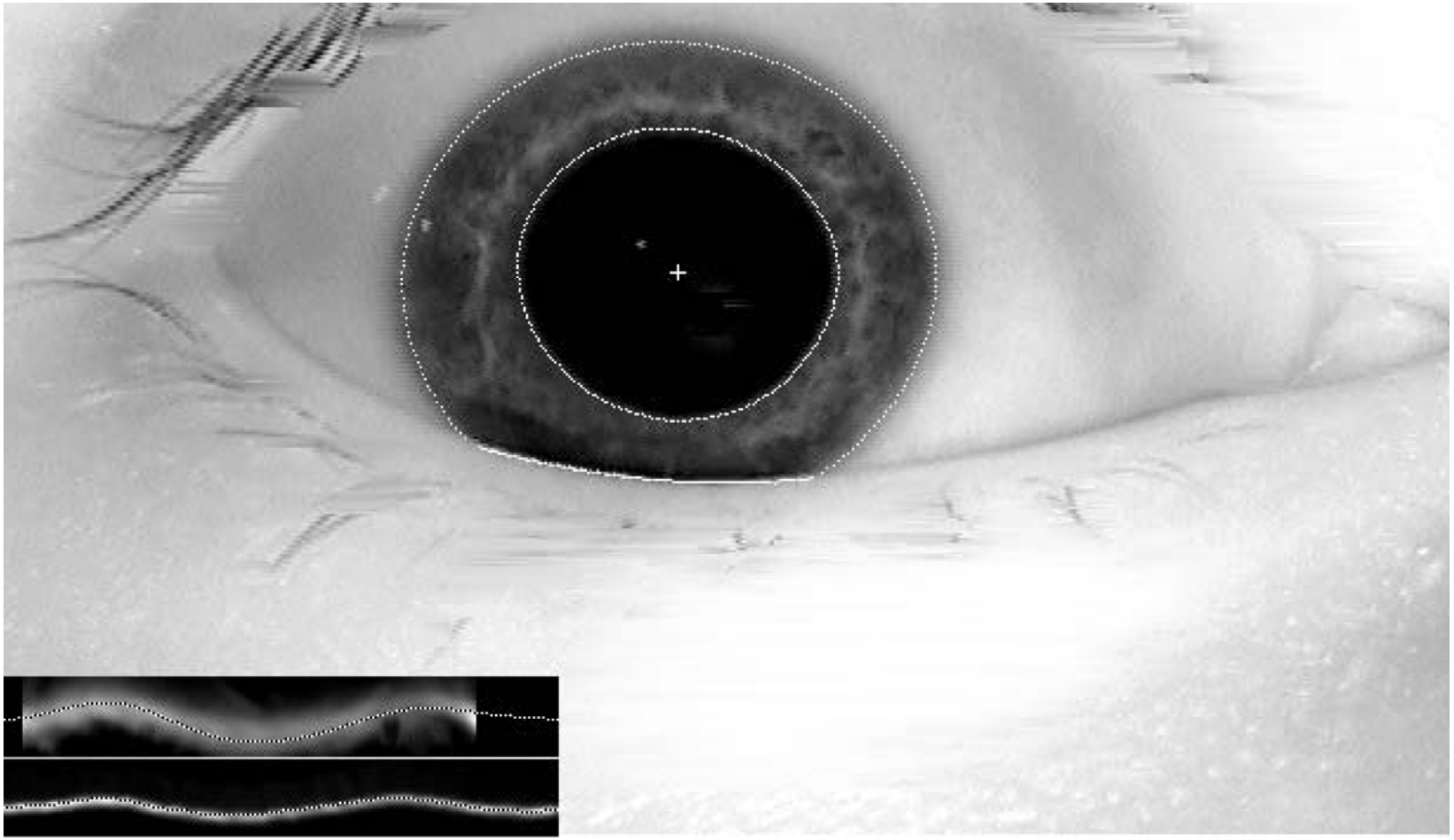
UNIVERSITY OF CAMBRIDGE



$$\max_{(r,x_0,y_0)} \left| G_\sigma(r) * \frac{\partial}{\partial r} \oint_{r,x_0,y_0} \frac{I(x,y)}{2\pi r} ds \right|$$

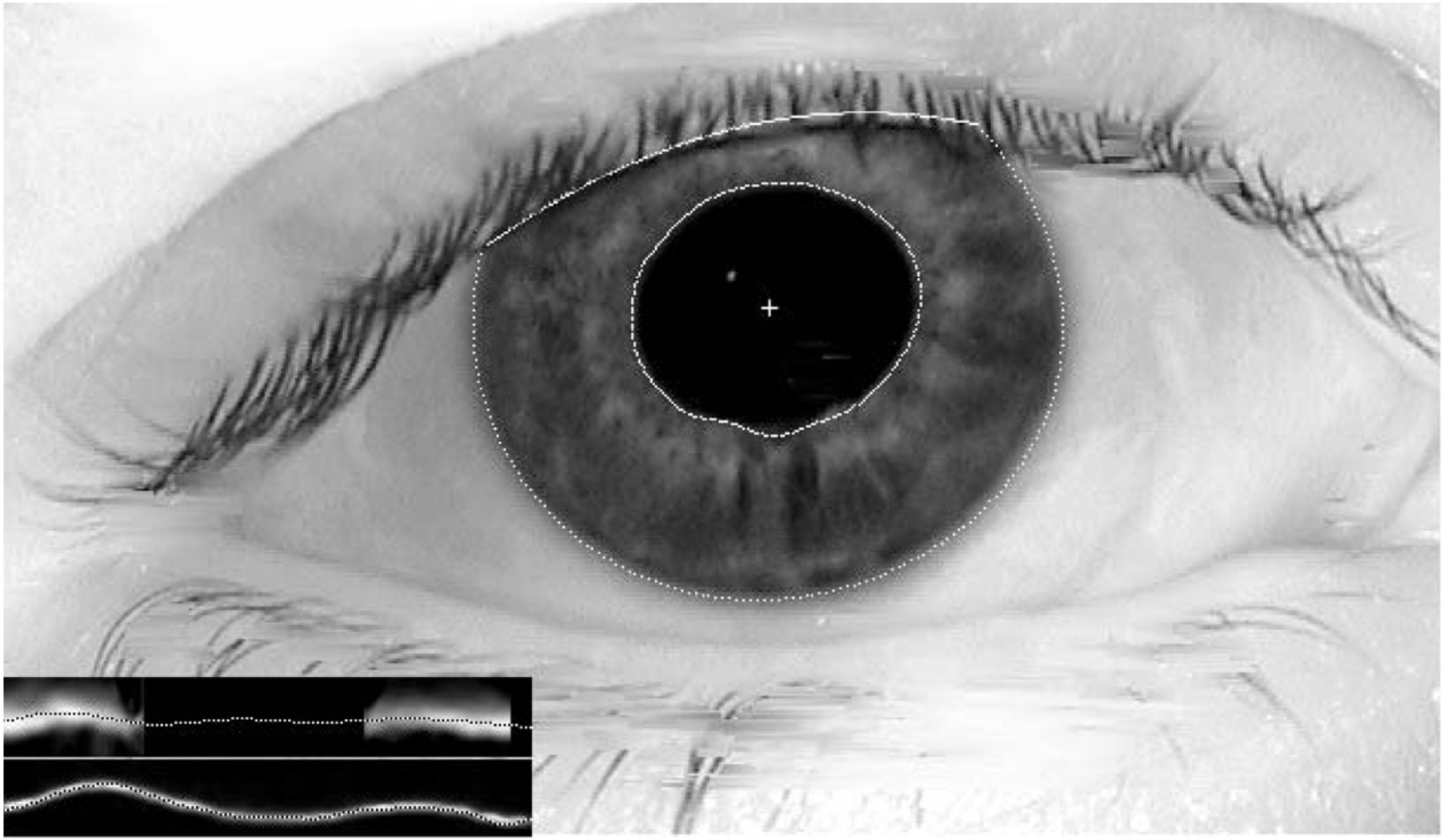
Localizing the iris boundaries by integro-differential operators

UNIVERSITY OF CAMBRIDGE



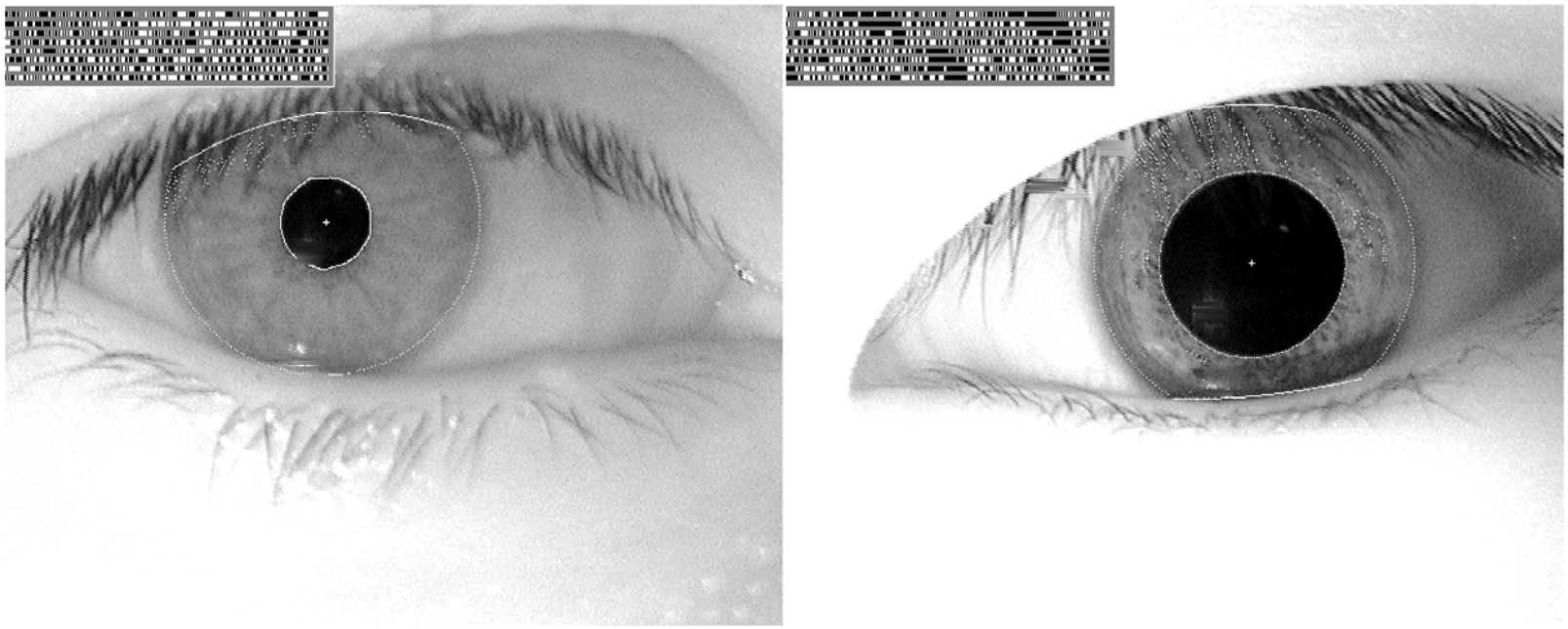
Iris boundaries are often non-round. The coordinate system must...

UNIVERSITY OF
CAMBRIDGE



...create a deformed, non-concentric, doubly-dimensionless iris mapping

UNIVERSITY OF
CAMBRIDGE

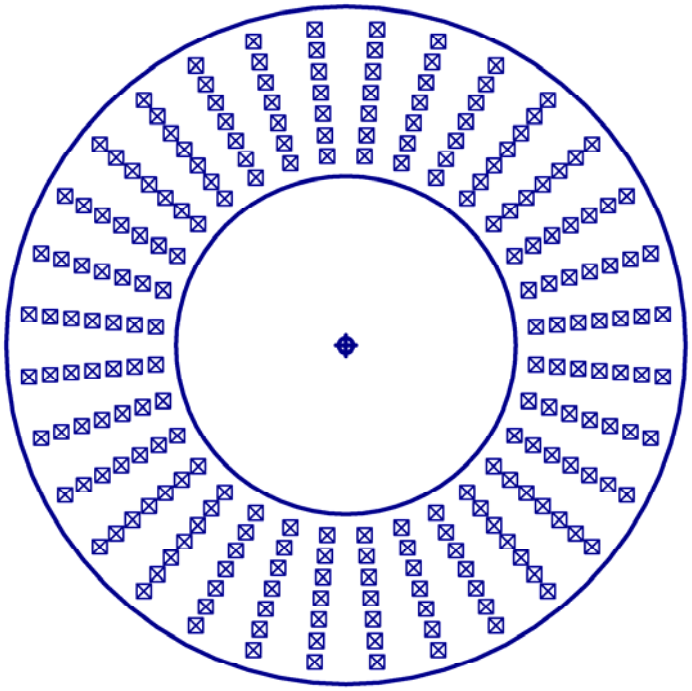


...invariant to distance, magnification, pupillary dilation, and gaze angle.

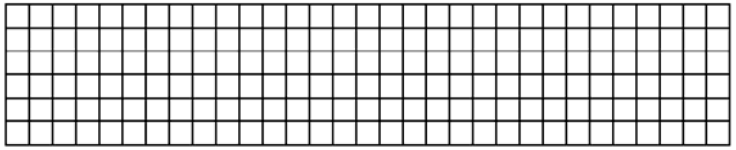
UNIVERSITY OF
CAMBRIDGE

Idealised mapping for a perfectly annular iris: concentric circular boundaries

Iris with concentric circular boundaries



"Unwrapped iris:" polar sampling grid whose columns correspond to the radial samples at each angle around the iris

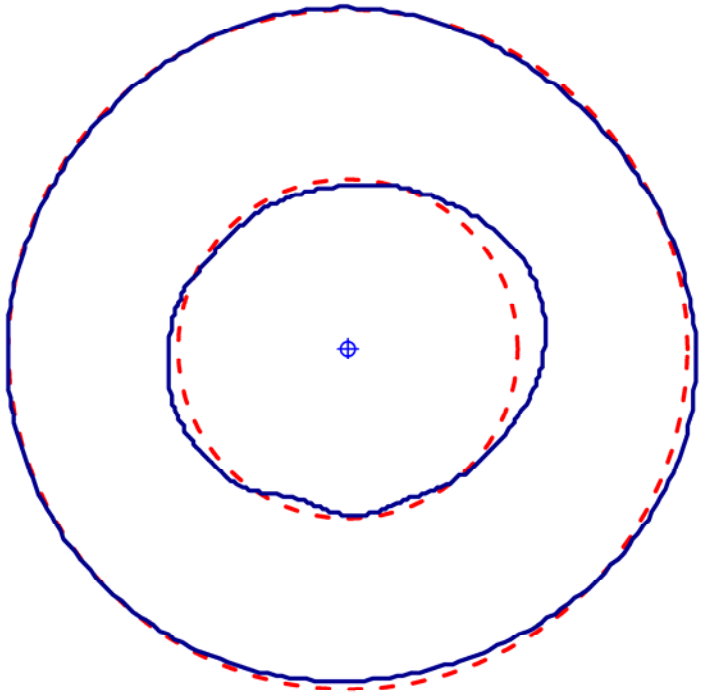


This unwrapping is often called the "Daugman rubber-sheet model," but it is just a coordinate transformation into normalised, and dimensionless, coordinates. The implied change in topology by cutting θ at $0 = 2\pi$ is misleading and incorrect.

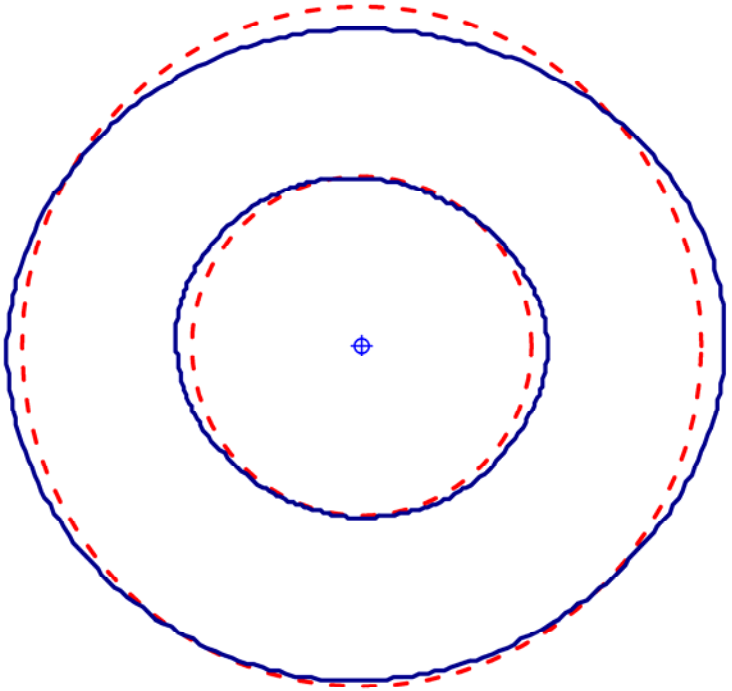
UNIVERSITY OF CAMBRIDGE

How reality differs from the idealised annular model

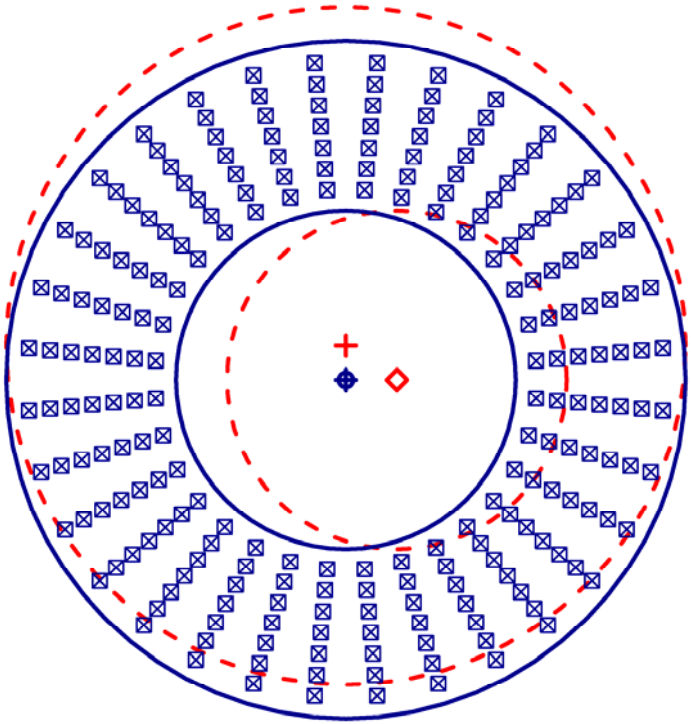
Actual non–circular iris boundaries (blue)



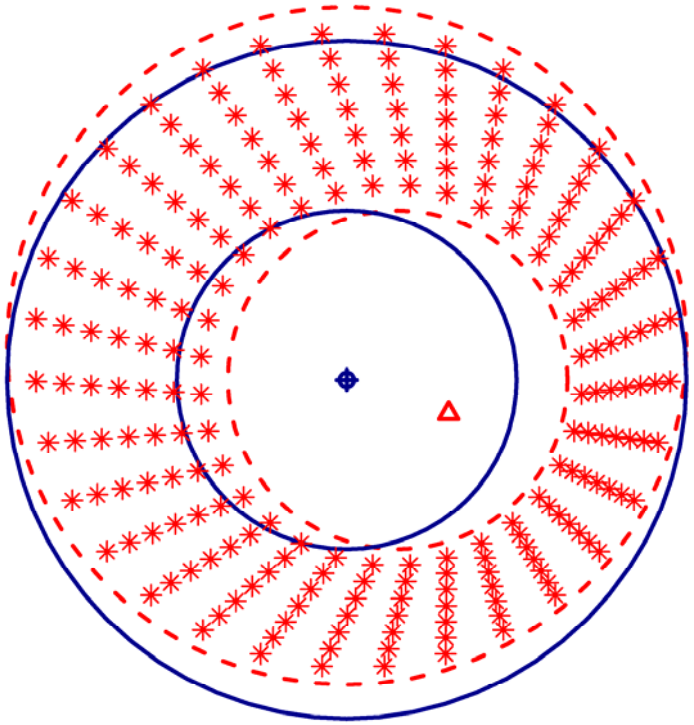
Actual non–circular iris boundaries (blue)



Enforcing circular boundary models for an iris can generate rivalrous solutions, with an effect similar to mislocalising a centre-of-coordinates

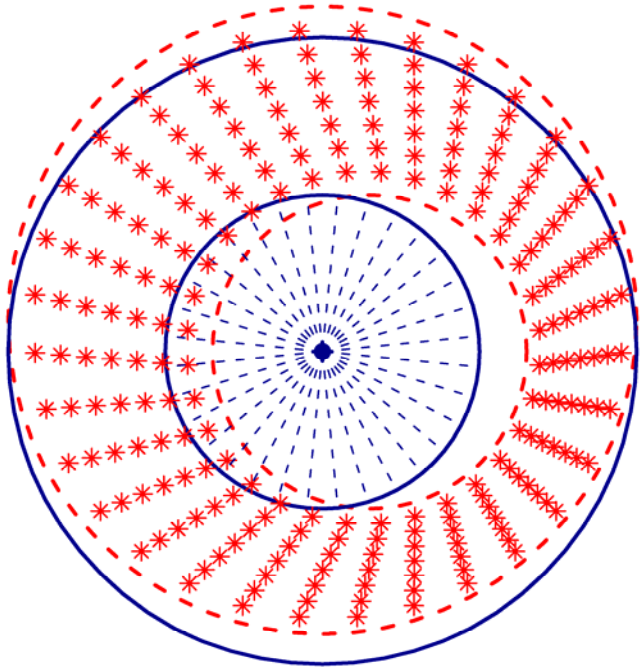


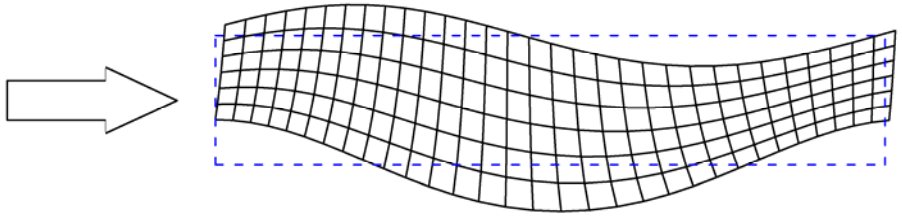
Mislocalisation of pupil and iris centre

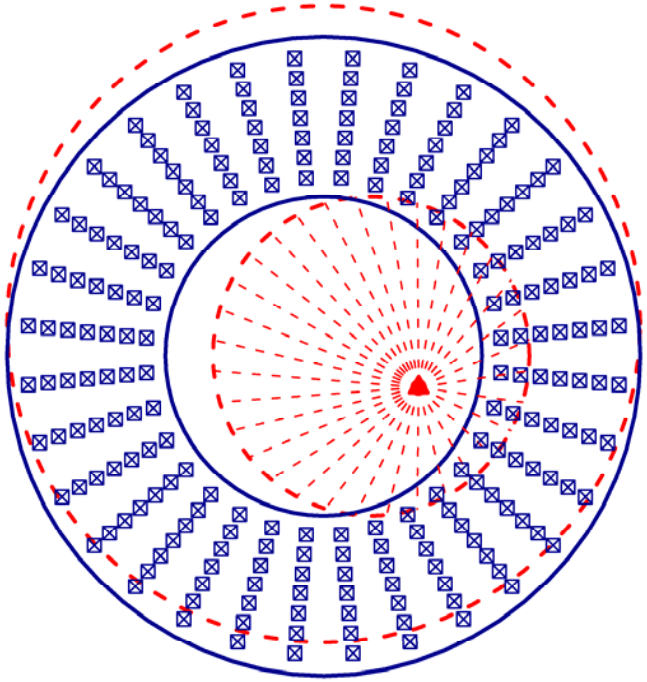


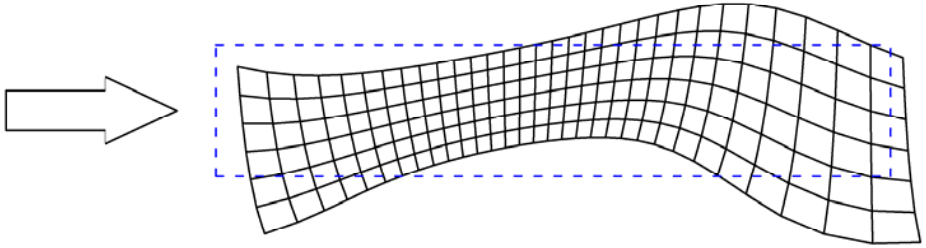
Resulting assignment of the polar grid

Resulting coordinate deformations









Active Contours and non-Circular Iris Coordinates

- Iris boundaries are rarely true circles. Performance is much enhanced by encoding the boundary shapes accurately when mapping iris patterns.
- So: compute a Fourier expansion of N angular samples of radial gradient edge data $\{r_\theta\}$ for $\theta = 0$ to $N-1$ spanning $[0, 2\pi]$. A set of M discrete Fourier coefficients $\{C_k\}$ are derived from the data sequence $\{r_\theta\}$ as follows:

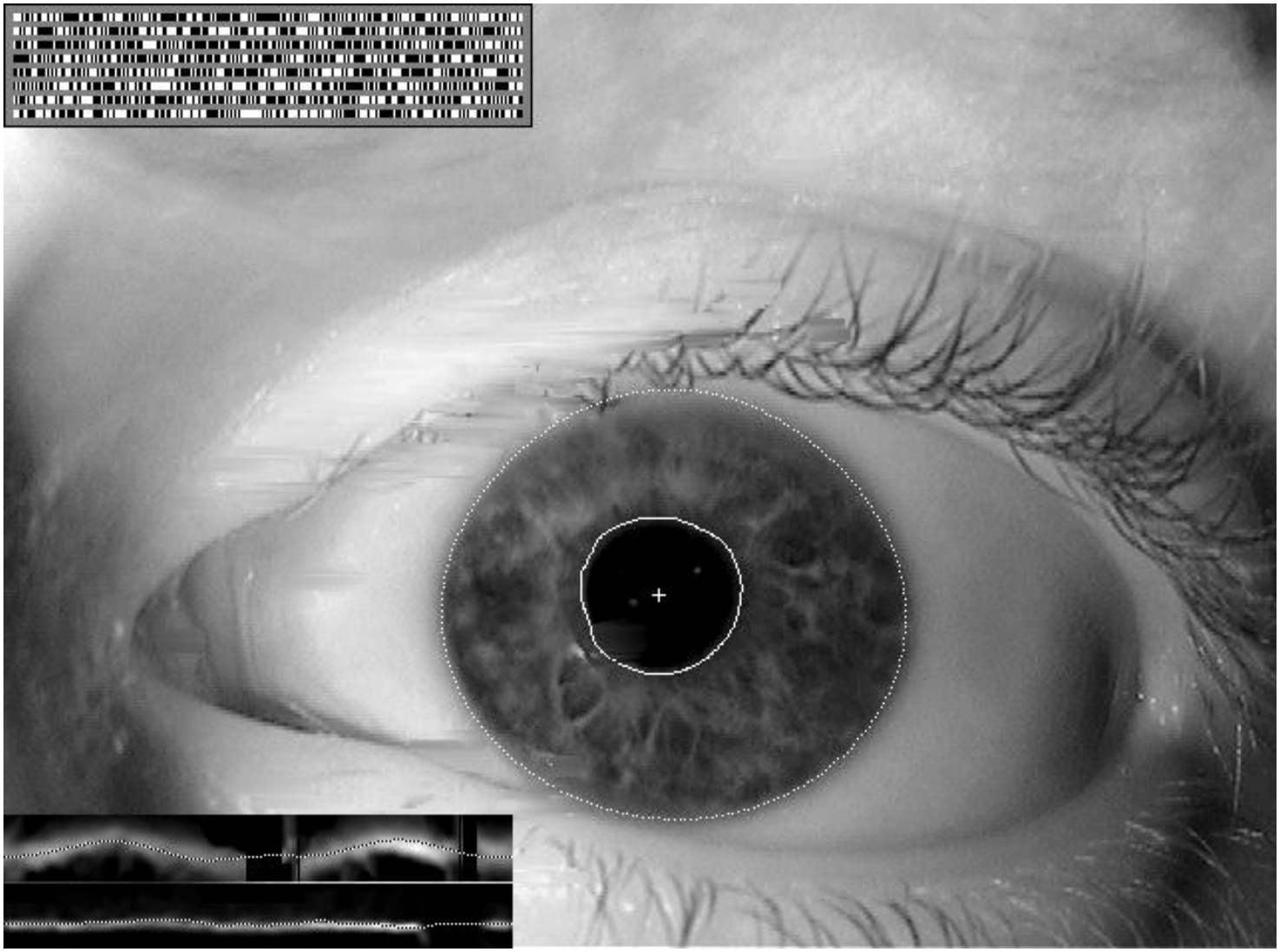
$$C_k = \sum_{\theta=0}^{N-1} r_\theta e^{-2\pi i k\theta/N}$$

- Note that the zeroth-order coefficient or "DC term" C_0 extracts the average curvature of the boundary: its radius if modelled simply as a circle.
- From these M discrete Fourier coefficients, an approximation to the inner or outer iris boundary (now spanning occlusion interruptions, and at a resolution determined by M) is obtained by the Fourier series $\{R_\theta\}$:

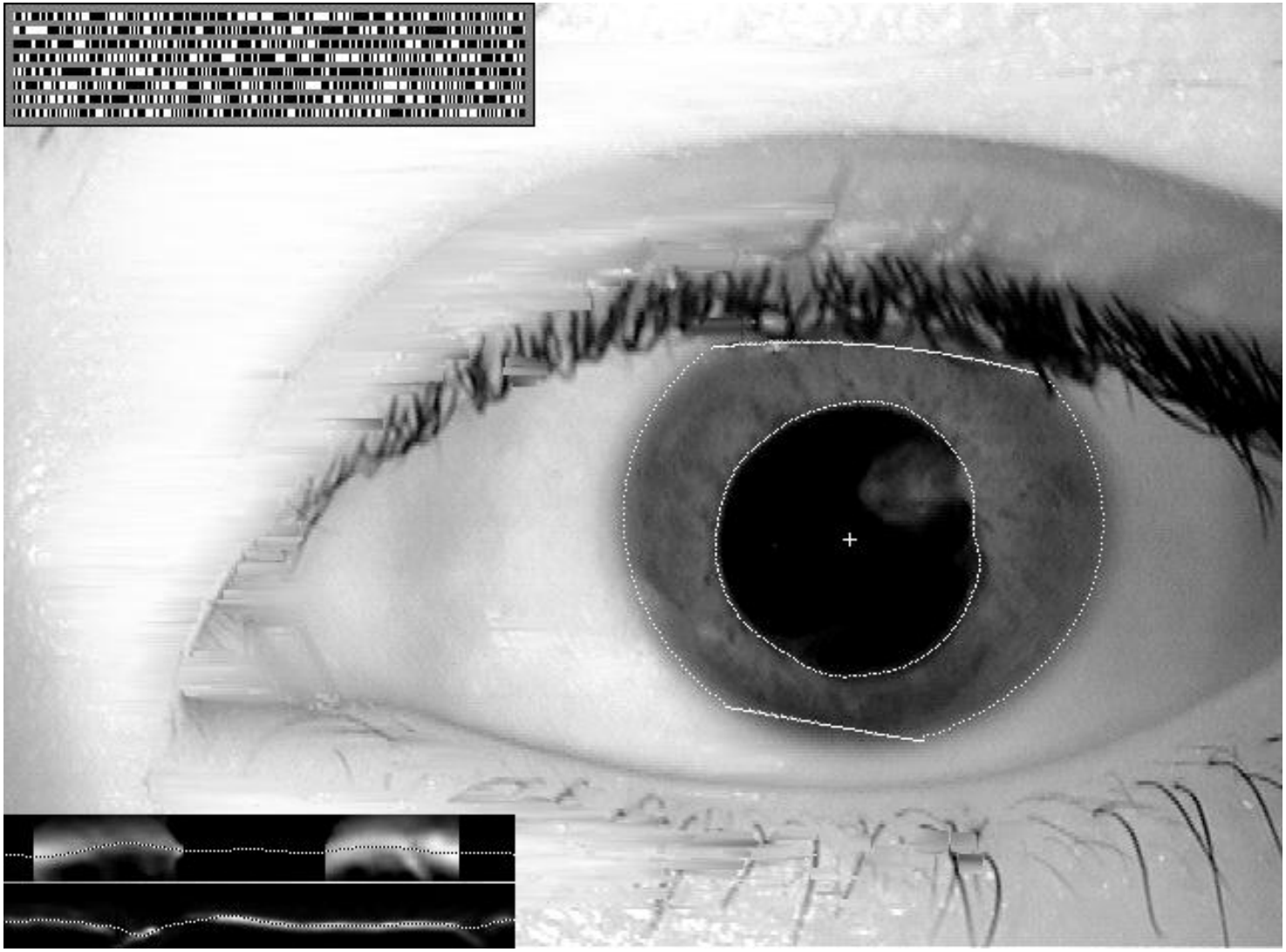
$$R_\theta = \frac{1}{N} \sum_{k=0}^{M-1} C_k e^{2\pi i k\theta/N}$$

- The trade-off between fidelity to the true boundary, and the stiffness of the Active Contour, is set by M, the number of Fourier components used.

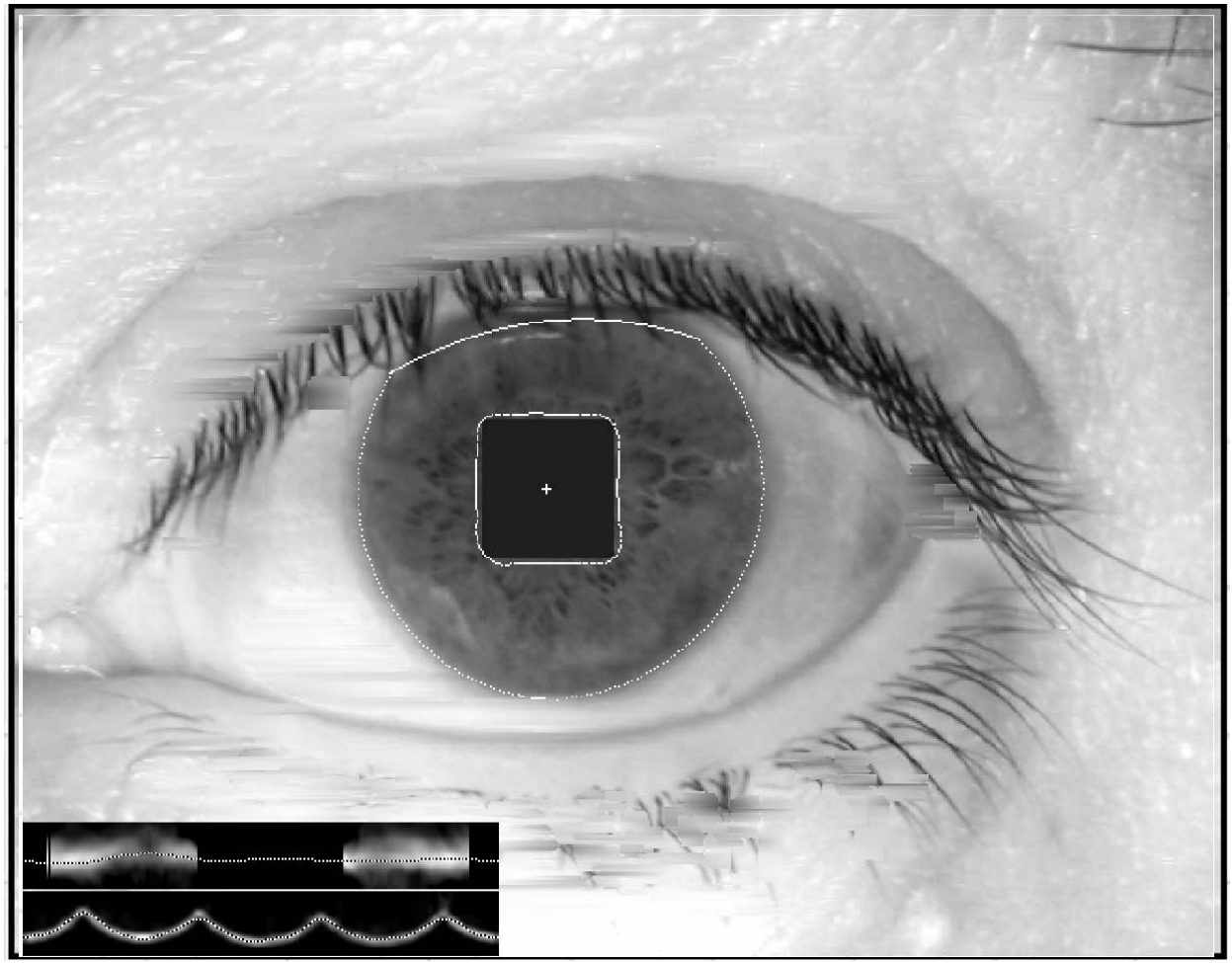
UNIVERSITY OF CAMBRIDGE



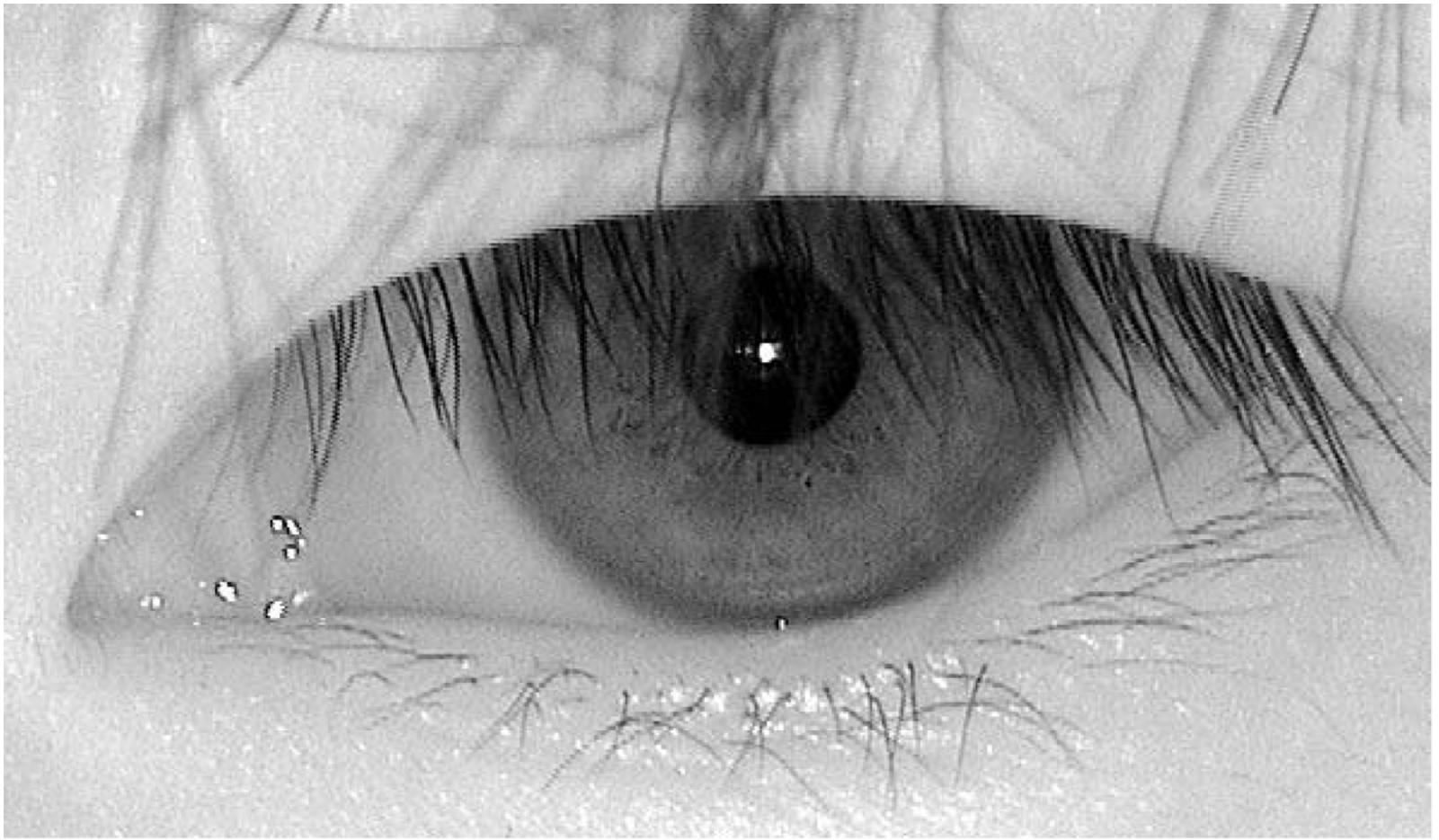
UNIVERSITY OF
CAMBRIDGE



UNIVERSITY OF
CAMBRIDGE



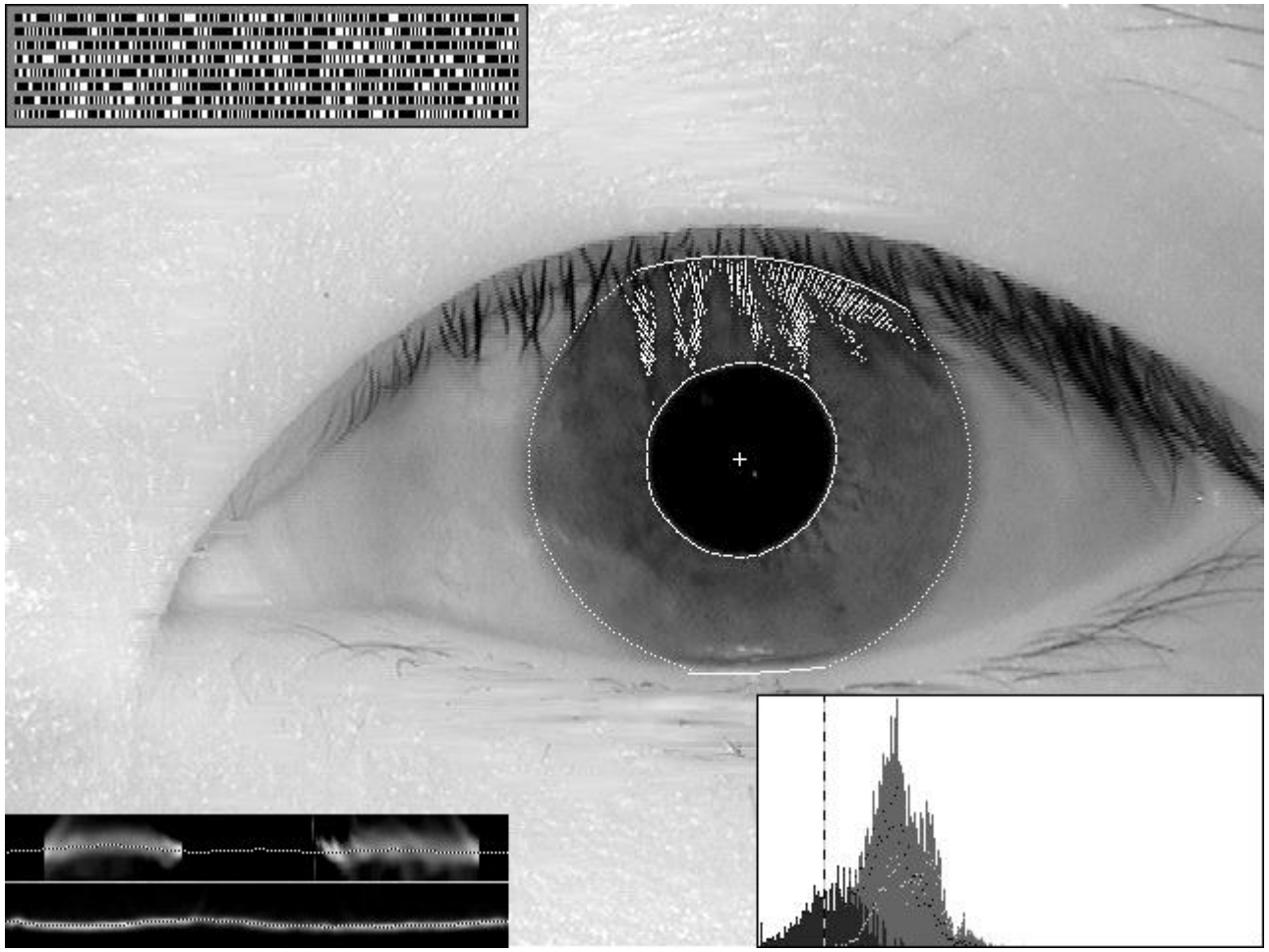
UNIVERSITY OF
CAMBRIDGE



Often the iris (especially in Oriental persons) is covered by eyelashes...

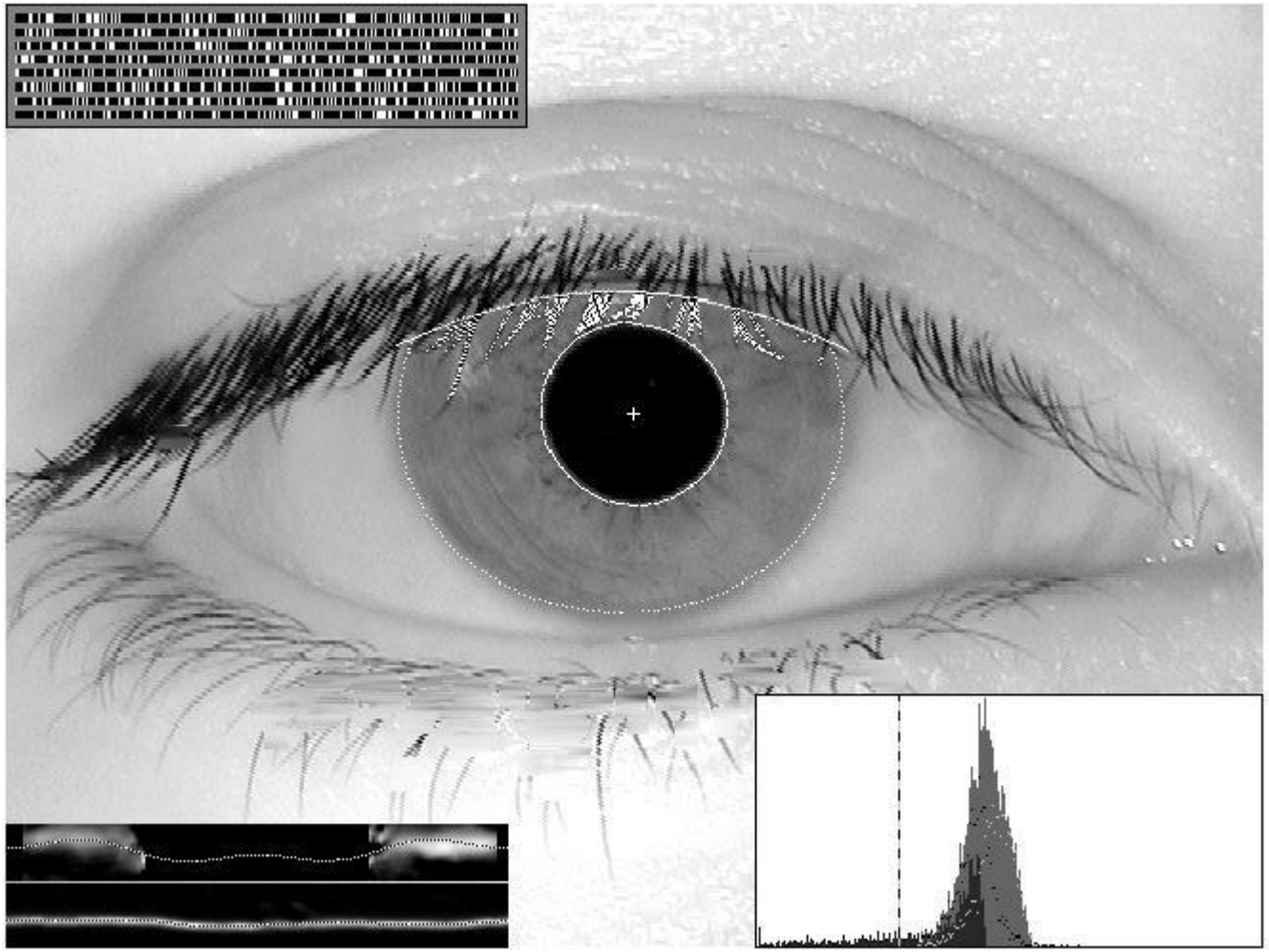
UNIVERSITY OF
CAMBRIDGE

Occluding eyelashes are detected and masked out (prevented from influencing the IrisCode) by statistical



UNIVERSITY OF CAMBRIDGE

hypothesis testing on the distribution of iris pixels, seeking evidence of a sub-population passing a test.



UNIVERSITY OF CAMBRIDGE

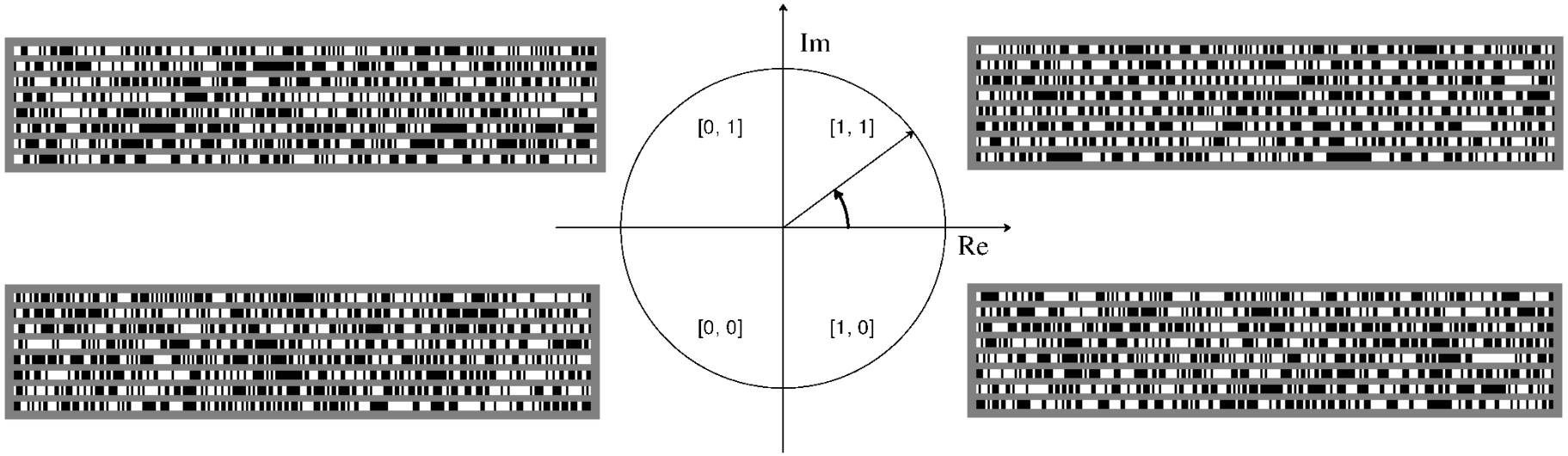
Setting Bits in an IrisCode by Wavelet Demodulation

$$h_{Re} = 1 \text{ if } \mathrm{Re} \int_\rho \int_\phi e^{-i\omega(\theta_0-\phi)} e^{-(r_0-\rho)^2/\alpha^2} e^{-(\theta_0-\phi)^2/\beta^2} I(\rho,\phi)\rho d\rho d\phi \geq 0$$

$$h_{Re} = 0 \text{ if } \mathrm{Re} \int_\rho \int_\phi e^{-i\omega(\theta_0-\phi)} e^{-(r_0-\rho)^2/\alpha^2} e^{-(\theta_0-\phi)^2/\beta^2} I(\rho,\phi)\rho d\rho d\phi < 0$$

$$h_{Im} = 1 \text{ if } \mathrm{Im} \int_\rho \int_\phi e^{-i\omega(\theta_0-\phi)} e^{-(r_0-\rho)^2/\alpha^2} e^{-(\theta_0-\phi)^2/\beta^2} I(\rho,\phi)\rho d\rho d\phi \geq 0$$

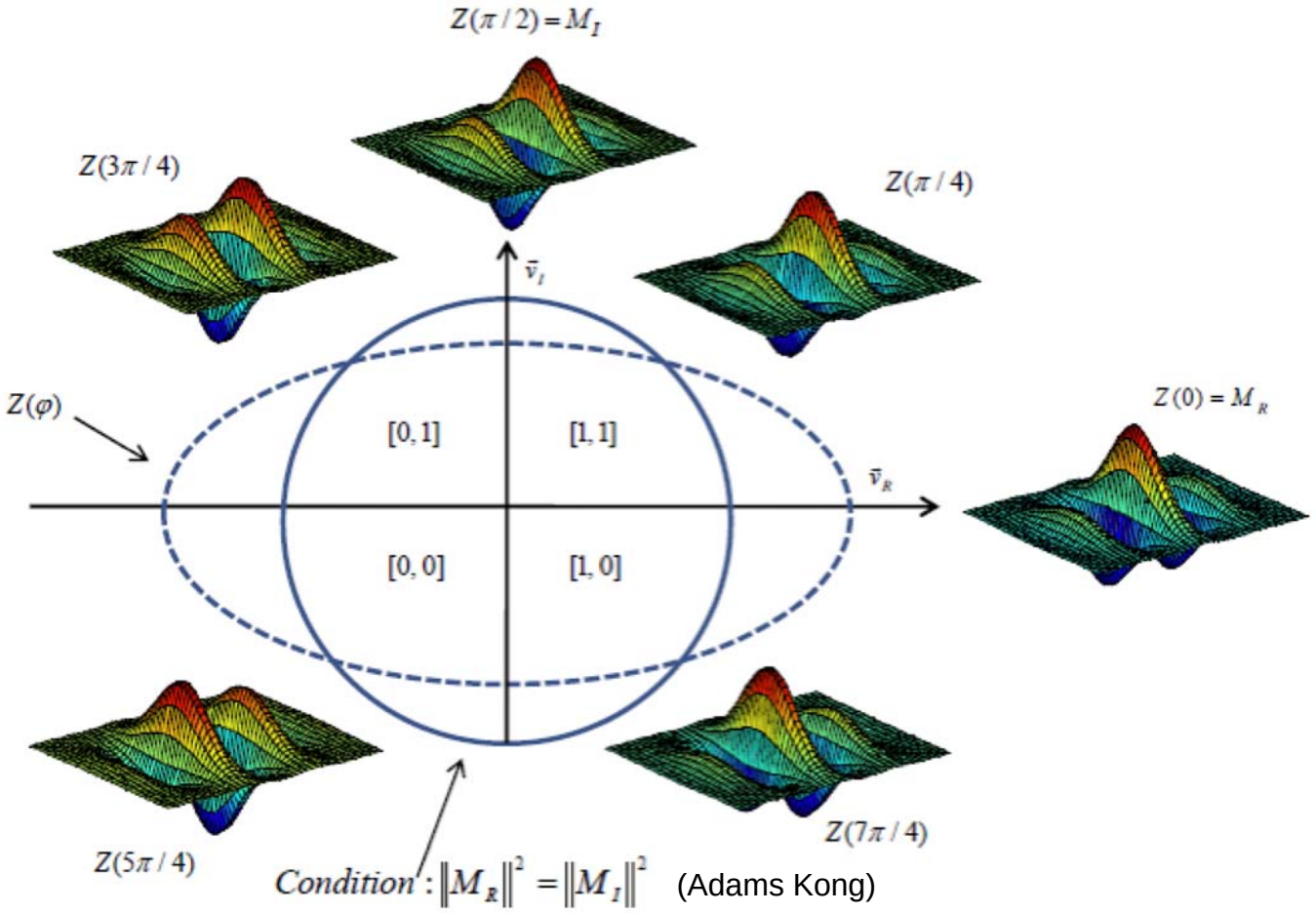
$$h_{Im} = 0 \text{ if } \mathrm{Im} \int_\rho \int_\phi e^{-i\omega(\theta_0-\phi)} e^{-(r_0-\rho)^2/\alpha^2} e^{-(\theta_0-\phi)^2/\beta^2} I(\rho,\phi)\rho d\rho d\phi < 0$$



UNIVERSITY OF CAMBRIDGE

2D Gabor wavelets as phase-steerable detectors

D. Gabor (1900-1979)



(Adams Kong)

Why phase is a good variable for biometric encoding

- Phase encodes structural information, independent of contrast
- Phase encoding thereby achieves some valuable invariances
- Phase information has much higher entropy than amplitude
- In harmonic (Fourier) terms, phase "does all the work"
- Phase can be very coarsely quantised into a binary string
- Phase is equivalent to a clustering algorithm (c.f. Adams Kong)
- Question: what is the best quantisation of phase (2, 4, 8... sectors)?
- Phase can be encoded in a scale-specific, or a scale-invariant, way

Gabor wavelets encode phase naturally, but in a scale- (or frequency)-specific way

Alternatives exist that encode phase in a total way (independent of scale/frequency), such as the Analytic function (the signal minus its Hilbert Transform $i f_{Hi}(x)$ cousin):

$f(x) - i f_{Hi}(x)$, which is a complex function whose 2 parts are "in quadrature"

UNIVERSITY OF CAMBRIDGE

Why IrisCode matching is so fast, parallelisable, and scalable

Bit streams A and B are data words of two IrisCodes.
Bit streams C and D are their respective mask words.

(data) A	1	0	0	1	0	1	1	0	0	0	1	0	1	1	1	0	···
(data) B	0	1	0	1	1	1	0	0	1	0	0	1	0	1	1	0	···
A⊕B	1	1	0	0	1	0	1	0	1	0	1	1	1	0	0	0	···
(mask) C	1	1	1	0	1	0	1	1	0	0	1	1	1	0	1	1	···
(mask) D	0	1	1	1	1	1	0	1	0	1	1	1	0	1	1	1	···
C∩D	0	1	1	0	1	0	0	1	0	0	1	1	0	0	1	1	···
(A⊕B)∩C∩D	0	1	0	0	1	0	0	0	0	0	1	1	0	0	0	0	···

Note that for these 16 bit chunks, only 8 data bits were mutually unmasked by C∩D.

Of those 8, they agreed in 4 and disagreed in 4, so raw Hamming distance is $4/8 = 0.5$ which is typical for comparisons between "Impostors" (unrelated IrisCodes).

Bit-parallel logic programming allows all of this to be done in a single line of C-code, operating on word lengths up to the word-length of the CPU (*e.g.* 64 bits at once):

```
result = (A ^ B) & C & D;
```

Each of the 3 logical parallel operators executes in a single "clock tick" (*e.g.* at 3 GHz).

UNIVERSITY OF CAMBRIDGE

Different use scenarios have different speed requirements

- **Real-time image processing speed** is needed for “iris-on-the-move” applications (*e.g.* must process 30 frames per second if the Subject is walking at 1 meter/second, with camera depth-of-field ~6 cm).

- **Matching speed** may need to survey the entire enrolled database (10^6 – 10^9 ?) per second, but matching is intrinsically parallelisable across platforms, is intrinsically very fast anyway because it is based on bit-parallel logic, and finally it is greatly expedited by Indexing.

- **De-duplication** is highly compute-intensive, because the number of pairings to be considered grows as N^2 for a population of size N. *E.g.* Indian UID: $N = 10^9$, so $N^2 = 10^{18}$. But de-duplication is generally an off-line process, performed as the enrolled database is built, and again it is expedited by parallelisation and Indexing.

UNIVERSITY OF CAMBRIDGE

Speed benchmarks for the publically deployed algorithms

- All image processing operations, including segmentation and template extraction, are performed within 30 milliseconds.

- The bit-parallel matching algorithm allows as many bits as the word-length of the computer (*e.g.* 64 bits) to be compared in a single operation (1 machine instruction) between two IrisCodes.

- Exploitation of ergodicity in (non-identical) IrisCode comparisons by subsampling and “early exit”, further accelerates matching.

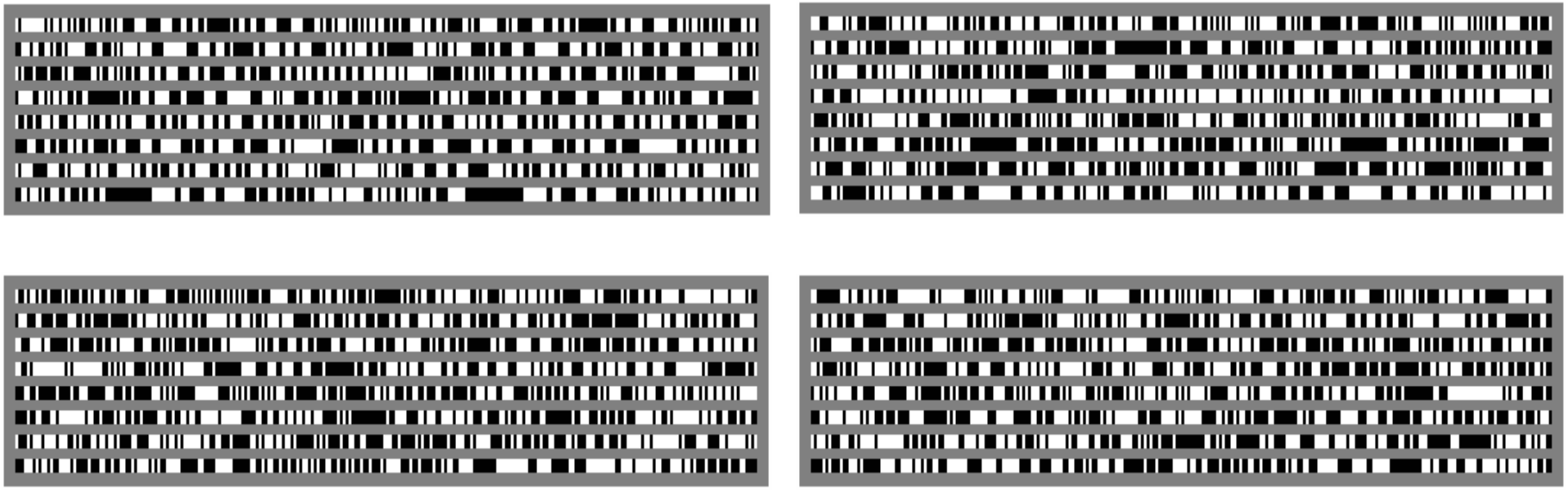
- Routine matching speeds are a million IrisCodes per second, per ordinary (single-core) CPU. Indexing accelerates this by 1 or 2 orders-of-magnitude, *e.g.* 50 nanoseconds including all rotations.

UNIVERSITY OF CAMBRIDGE

But:

UNIVERSITY OF
CAMBRIDGE

Entropy gives resistance against False Matches

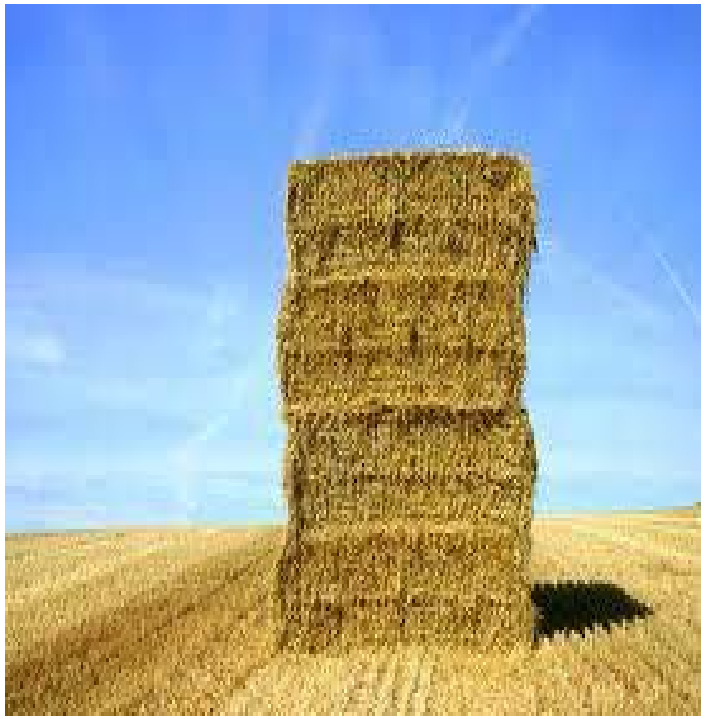


The probability of two different people colliding by chance in so many bits (*e.g.* disagreeing in only one-third of their IrisCode bits) is infinitesimal. Thus the False Match Rate is easily made minuscule.

UNIVERSITY OF CAMBRIDGE

But it's like looking for one of these...

...in one of these.



UNIVERSITY OF CAMBRIDGE

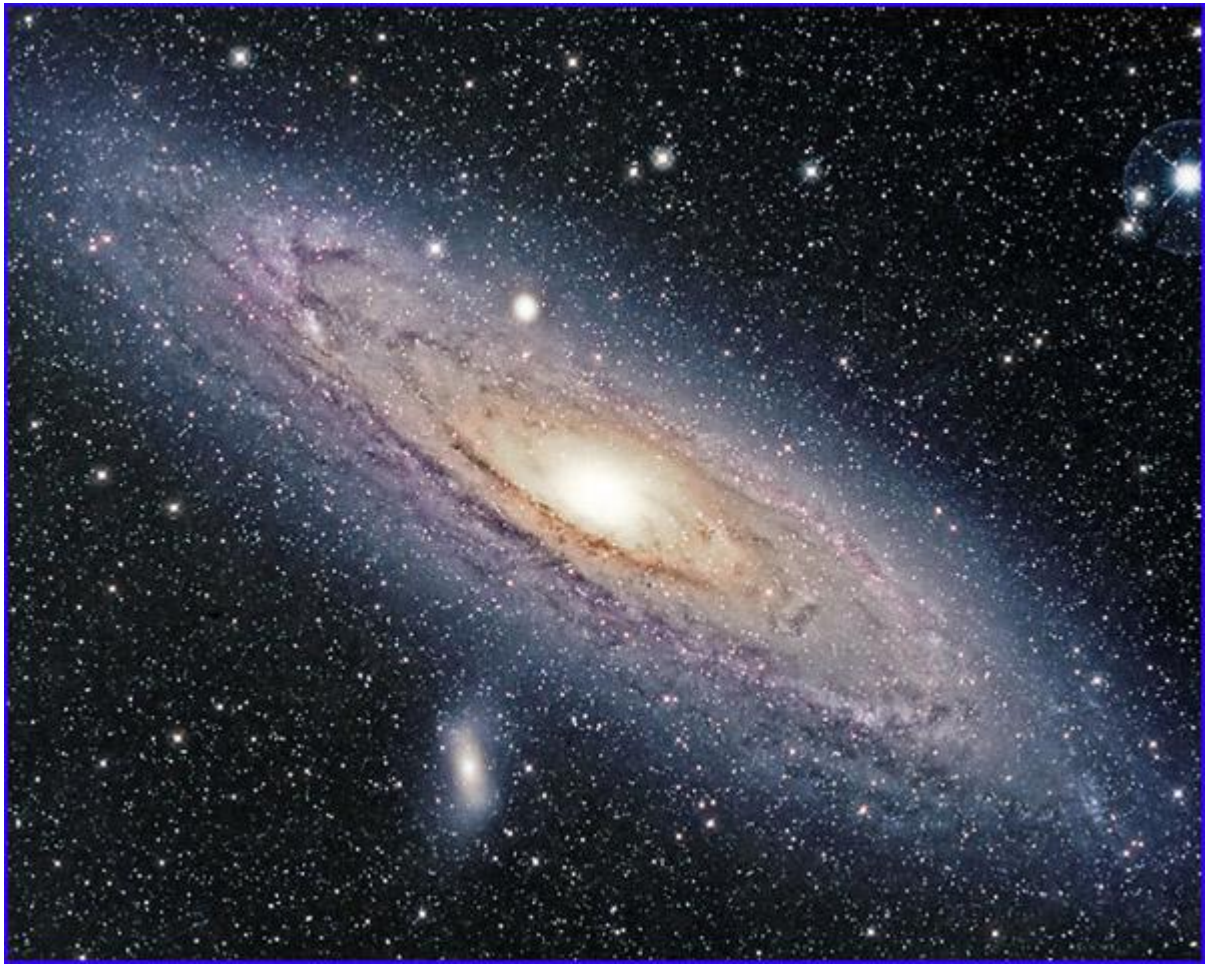
Example of the importance of high entropy

- UIDAI (Unique Identification Authority of India) in 2011 began enrolling iris images of all **1.2 billion** citizens
- As of February 2012, **150 million** had been enrolled
- Currently enrolling **1 million persons per day**
- Each enrolled person is compared against all of those enrolled so far, to detect duplicates (“*de-duplication*”). This requires (1 million x 150 million) = **150 trillion** iris cross-comparisons daily: 1.5×10^{14} per day

The avoidance of biometric collisions among comparisons on this scale requires high biometric entropy, as possessed by IrisCode phase bits, ensuring very rapidly attenuating tails of the distribution obtained when comparing different eyes.

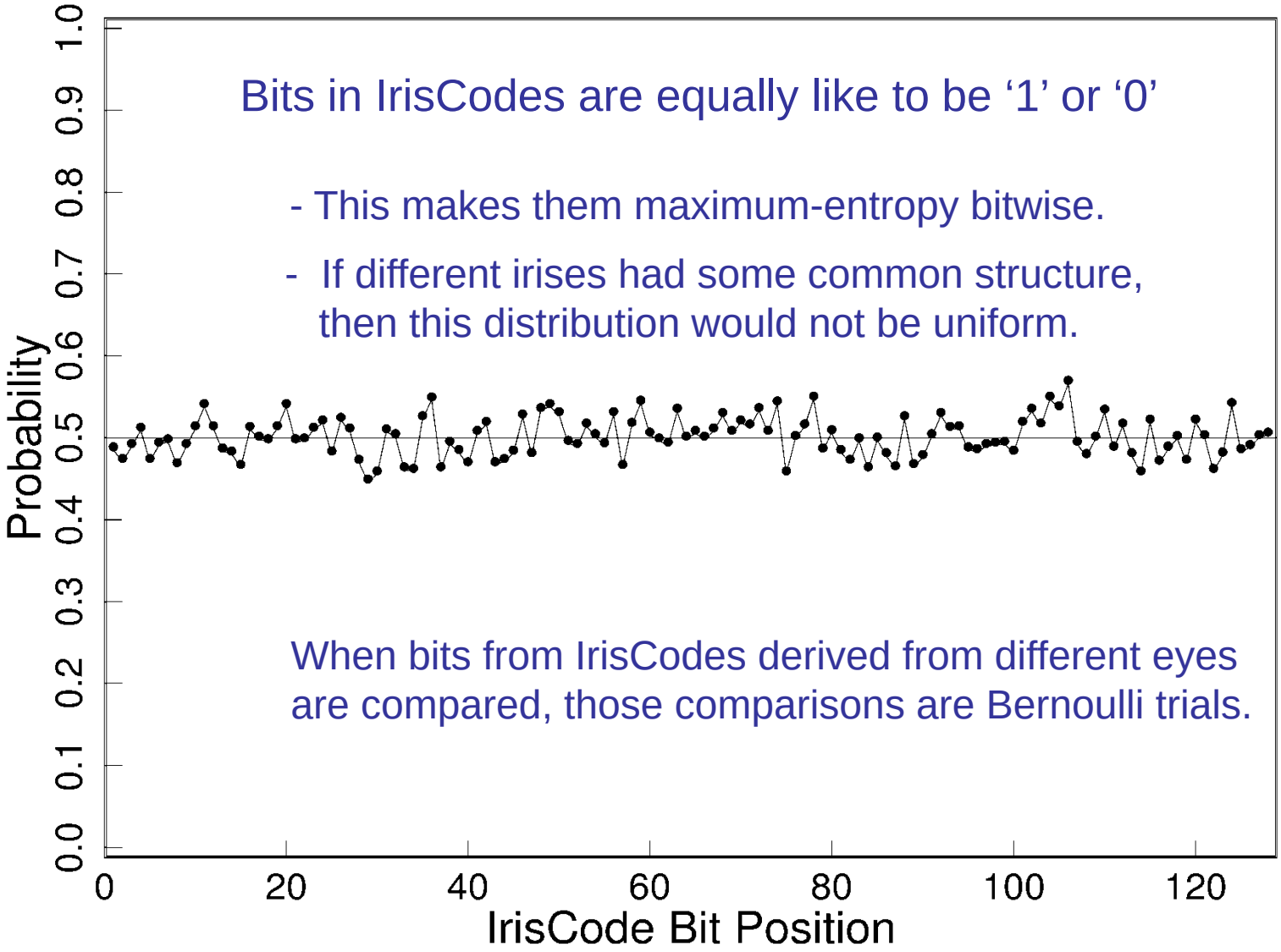
UNIVERSITY OF CAMBRIDGE

10^{14} iris comparisons per day! A typical galaxy contains "just" 100 billion stars (10^{11})... So UIDAI daily workflow equates to the number of stars in 1,000 galaxies

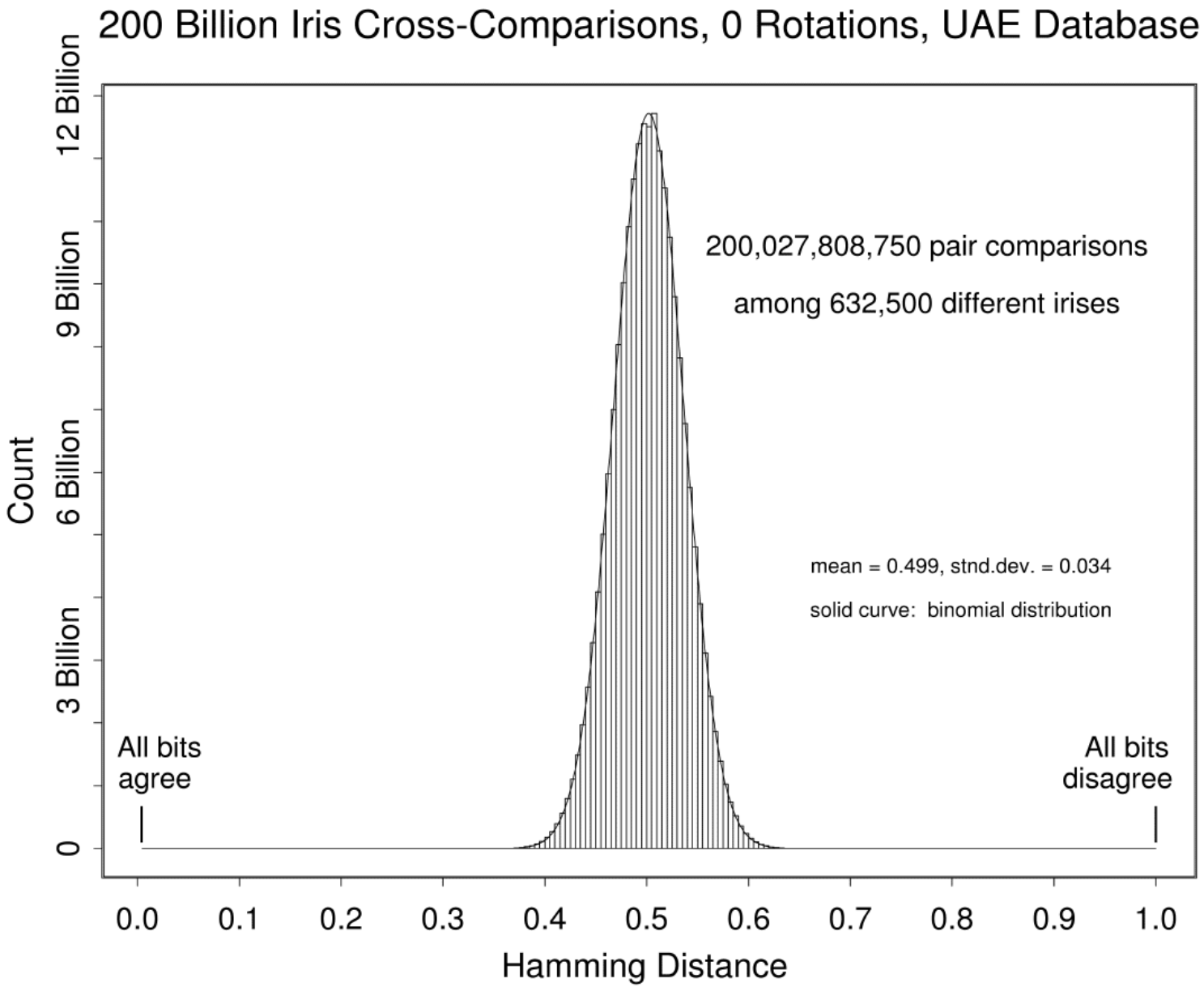


UNIVERSITY OF CAMBRIDGE

IrisCode Bit Probabilities



UNIVERSITY OF CAMBRIDGE



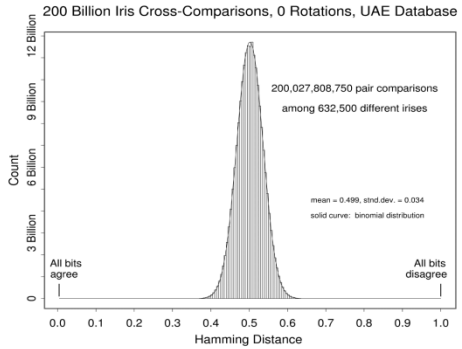
UNIVERSITY OF CAMBRIDGE

IrisCode Bit Comparisons are Bernoulli Trials

Jacob Bernoulli (1645-1705) analyzed *coin-tossing* and derived the binomial distribution. If the probability of "heads" is p, then the likelihood that a fraction $x = m/N$ out of N tosses will turn up "heads" is:

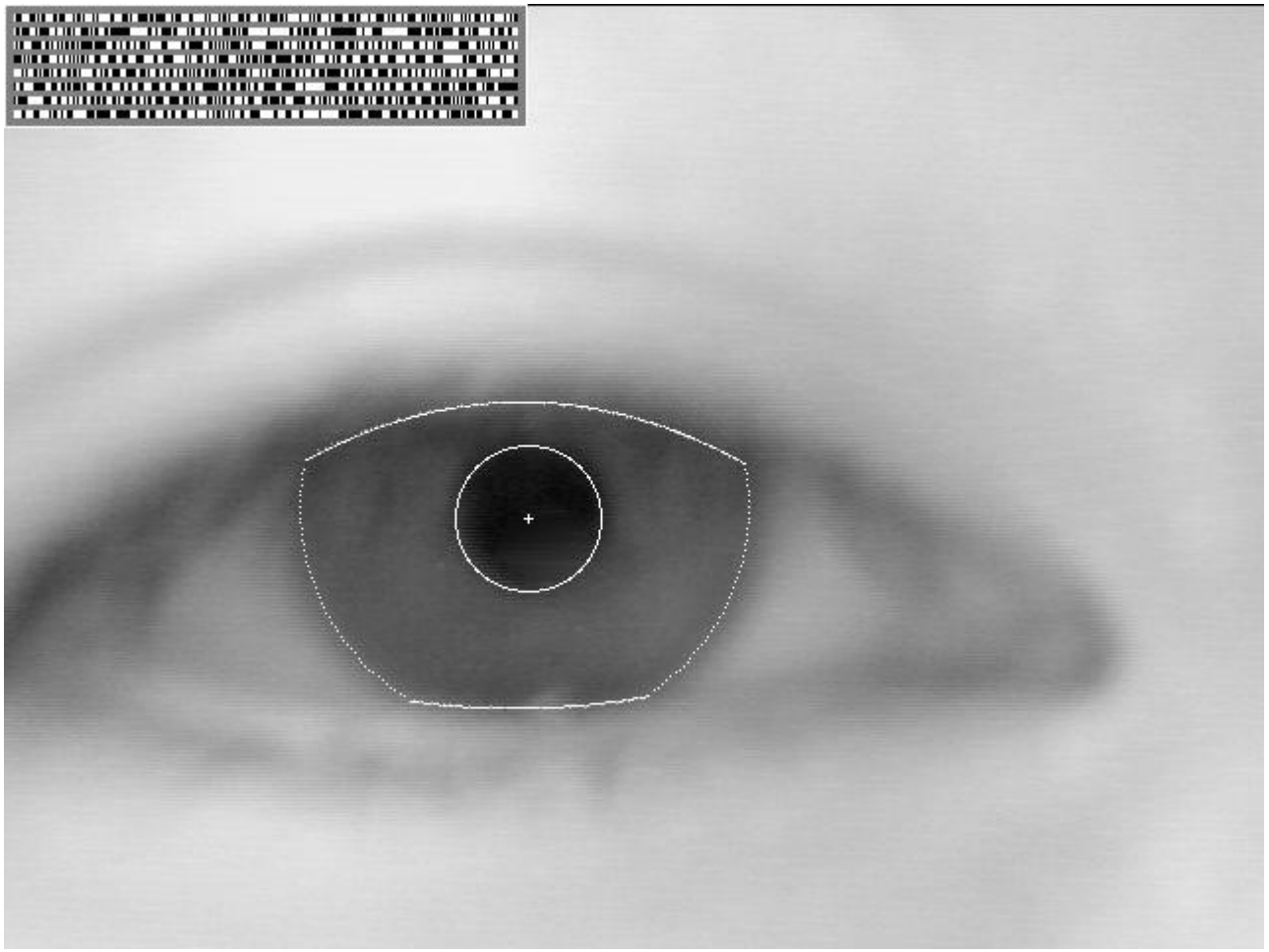
$$P(x) = \frac{N!}{m!(N-m)!}\, p^m\, (1-p)^{(N-m)}$$

University of Groningen



UNIVERSITY OF CAMBRIDGE

Badly defocused iris images do not cause False Matches, because the IrisCode phase bits then just become random, determined by pixel noise. This is an advantage of phase over correlation-based coding methods.



IrisCode Logic and Normalizations

Logic for computing raw Hamming Distance scores, incorporating masks:

$$HD_{\text{raw}} = \frac{\|(codeA \otimes codeB) \cap maskA \cap maskB\|}{\|maskA \cap maskB\|}$$

where $\otimes$ is Exclusive-OR, $\cap$ is AND, and $\|\quad\|$ is the count of 'set' bits.

Score re-normalisation to compensate for number of bits compared:

$$HD_{\text{norm}} = 0.5 - (0.5 - HD_{\text{raw}})\sqrt{\frac{n}{911}}$$

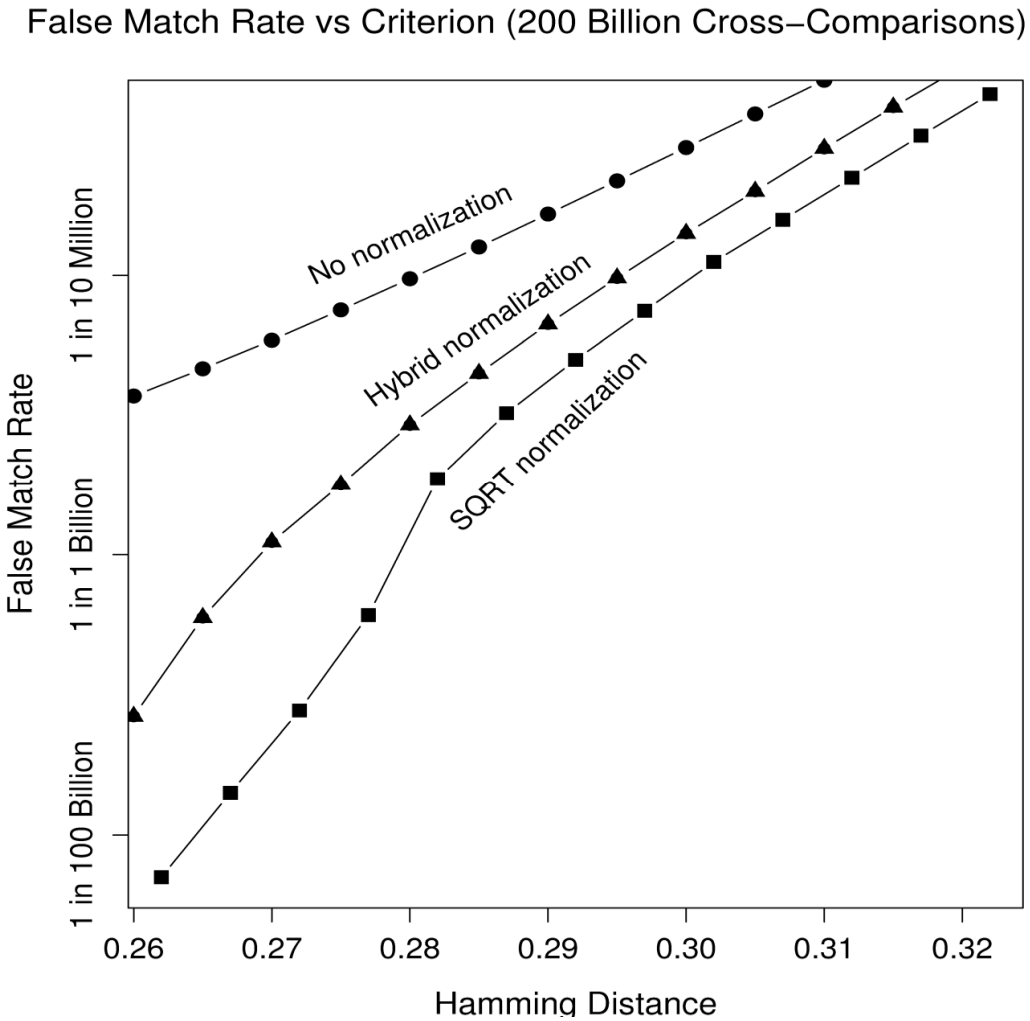
Decision Criterion normalisation by database size and query rate:

$$HD_{\text{Crit}} \sim 0.32 - 0.012 \ \log_{10}(N \times M)$$

where N is the search database size, M is the number of queries to be compared against the full database, while requiring nil False Matches

UNIVERSITY OF CAMBRIDGE

Score normalisation rules and principles for Matching Engines



UNIVERSITY OF CAMBRIDGE

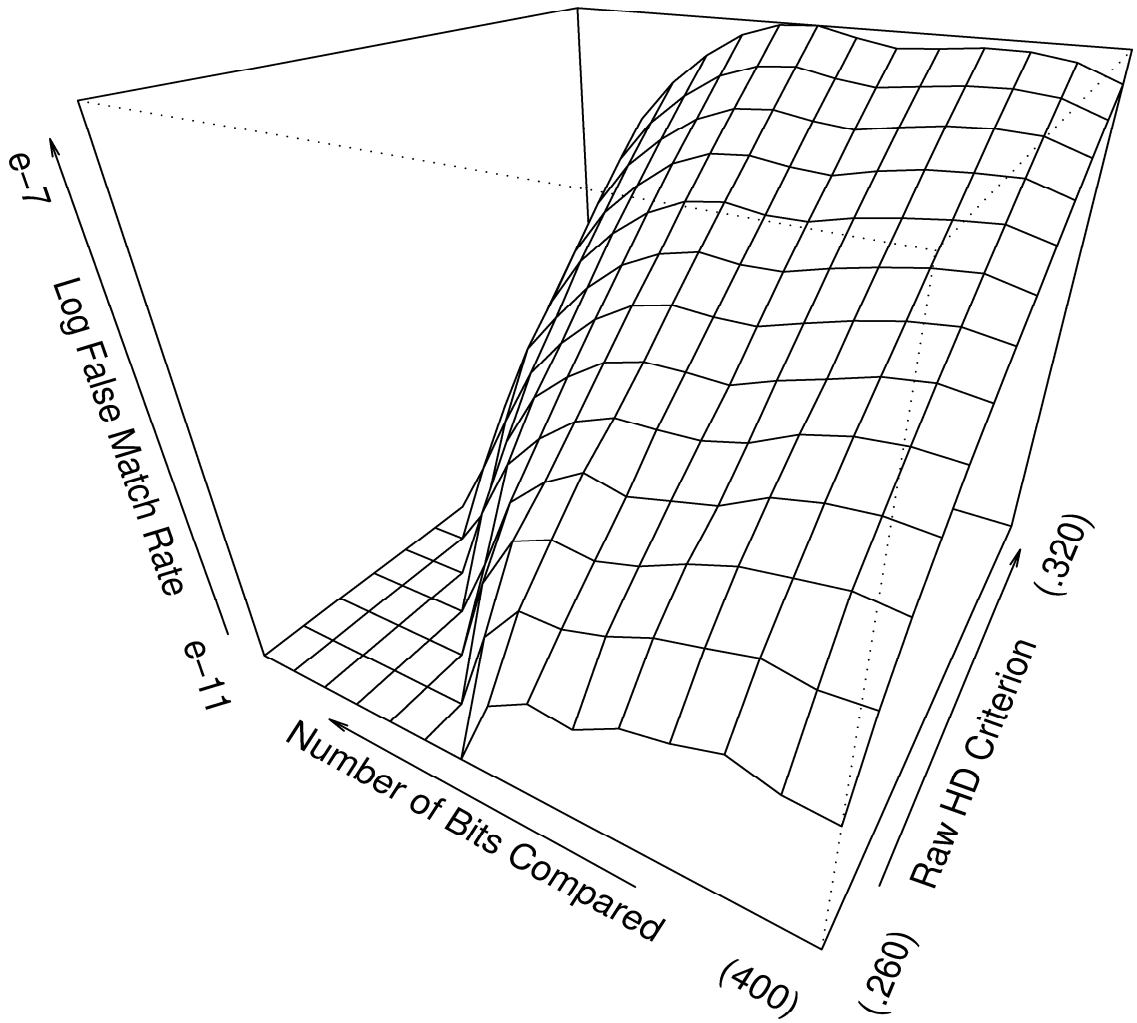
False Match Rate without Score Normalization: Dependence on Number of Bits Compared and Criterion

HD_{Crit}	400 bits	500 bits	600 bits	700 bits	800 bits	900 bits	1000 bits
0.260	$2 \cdot 10^{-9}$	$5 \cdot 10^{-10}$	$3 \cdot 10^{-10}$	$1 \cdot 10^{-10}$	0	0	0
0.265	$3 \cdot 10^{-9}$	$8 \cdot 10^{-10}$	$5 \cdot 10^{-10}$	$2 \cdot 10^{-10}$	$4 \cdot 10^{-11}$	0	0
0.270	$4 \cdot 10^{-9}$	$1 \cdot 10^{-9}$	$9 \cdot 10^{-10}$	$5 \cdot 10^{-10}$	$2 \cdot 10^{-10}$	0	0
0.275	$7 \cdot 10^{-9}$	$2 \cdot 10^{-9}$	$1 \cdot 10^{-9}$	$9 \cdot 10^{-10}$	$5 \cdot 10^{-10}$	$3 \cdot 10^{-11}$	0
0.280	$1 \cdot 10^{-8}$	$4 \cdot 10^{-9}$	$2 \cdot 10^{-9}$	$2 \cdot 10^{-9}$	$1 \cdot 10^{-9}$	$2 \cdot 10^{-10}$	0
0.285	$2 \cdot 10^{-8}$	$7 \cdot 10^{-9}$	$4 \cdot 10^{-9}$	$3 \cdot 10^{-9}$	$2 \cdot 10^{-9}$	$5 \cdot 10^{-10}$	$2 \cdot 10^{-11}$
0.290	$3 \cdot 10^{-8}$	$1 \cdot 10^{-8}$	$8 \cdot 10^{-9}$	$7 \cdot 10^{-9}$	$4 \cdot 10^{-9}$	$1 \cdot 10^{-9}$	$1 \cdot 10^{-10}$
0.295	$4 \cdot 10^{-8}$	$2 \cdot 10^{-8}$	$1 \cdot 10^{-8}$	$1 \cdot 10^{-8}$	$9 \cdot 10^{-9}$	$3 \cdot 10^{-9}$	$4 \cdot 10^{-10}$
0.300	$6 \cdot 10^{-8}$	$3 \cdot 10^{-8}$	$3 \cdot 10^{-8}$	$2 \cdot 10^{-8}$	$2 \cdot 10^{-8}$	$7 \cdot 10^{-9}$	$9 \cdot 10^{-10}$
0.305	$9 \cdot 10^{-8}$	$6 \cdot 10^{-8}$	$5 \cdot 10^{-8}$	$4 \cdot 10^{-8}$	$4 \cdot 10^{-8}$	$1 \cdot 10^{-8}$	$2 \cdot 10^{-9}$
0.310	$1 \cdot 10^{-7}$	$1 \cdot 10^{-7}$	$8 \cdot 10^{-8}$	$8 \cdot 10^{-8}$	$7 \cdot 10^{-8}$	$3 \cdot 10^{-8}$	$5 \cdot 10^{-9}$
0.315	$2 \cdot 10^{-7}$	$2 \cdot 10^{-7}$	$1 \cdot 10^{-7}$	$2 \cdot 10^{-7}$	$1 \cdot 10^{-7}$	$6 \cdot 10^{-8}$	$1 \cdot 10^{-8}$
0.320	$3 \cdot 10^{-7}$	$3 \cdot 10^{-7}$	$2 \cdot 10^{-7}$	$3 \cdot 10^{-7}$	$3 \cdot 10^{-7}$	$1 \cdot 10^{-7}$	$2 \cdot 10^{-8}$

UNIVERSITY OF CAMBRIDGE

Log False Match Rates versus HD_crit and Number of Bits Compared

for 200 Billion Iris Comparisons, non–Normalised Scores



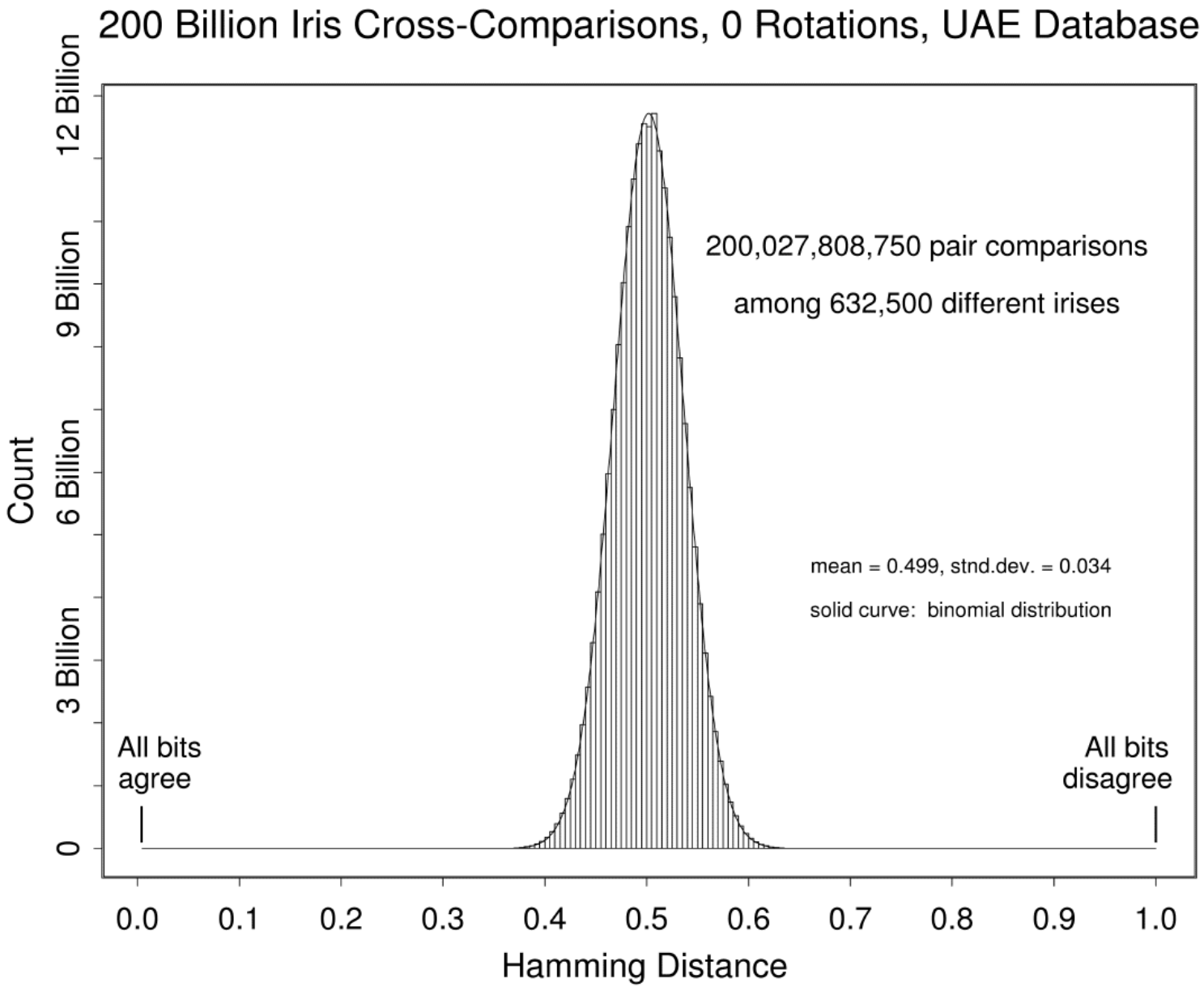
UNIVERSITY OF CAMBRIDGE

Effect of the "Amount of Iris Visible"

- If eyelids occlude much of the iris, fewer IrisCode bits are available for comparison with other IrisCodes
- Decision criterion then becomes correspondingly more demanding
- Renormalisation is based on equal-confidence contours for binomial combinatorics, whatever the number of bits compared
- All of the matches in this table are equivalently decisive:

number of bits compared	*approximate percent of iris visible*	*maximum acceptable fraction of bits disagreeing*
200	17%	0.13
300	26%	0.19
400	35%	0.23
500	43%	0.26
600	52%	0.28
700	61%	0.30
800	69%	0.31
911	79%	0.32
1000	87%	0.33
1152	100%	0.34

UNIVERSITY OF CAMBRIDGE



UNIVERSITY OF CAMBRIDGE

"Extreme Value Distribution" for Best Match Score after Multiple Rotations

The new distribution after k rotations of IrisCodes in the search process still has a simple analytic form that can be derived theoretically. Let $f_0(x)$ be the raw density distribution obtained for the HD_{norm} scores between different irises after comparing them only in a single relative orientation; for example, $f_0(x)$ might be the binomial distribution. Then $F_0(x)$, the cumulative of $f_0(x)$ from 0 to x, is the probability of getting a False Match in such a test when using HD_{norm} acceptance criterion x:

$$F_0(x) = \int_0^x f_0(x)dx \tag{1}$$

or, equivalently,

$$f_0(x) = \frac{d}{dx}F_0(x) \tag{2}$$

Clearly, then, the probability of *not* making a False Match when using decision criterion x is $1 - F_0(x)$ after a single test, and it is $[1 - F_0(x)]^k$ after carrying out k such tests independently at k different relative orientations. It follows that the probability of a False Match after a "best of k" test of agreement, when using HD_{norm} criterion x, regardless of the actual form of the raw unrotated distribution $f_0(x)$, is:

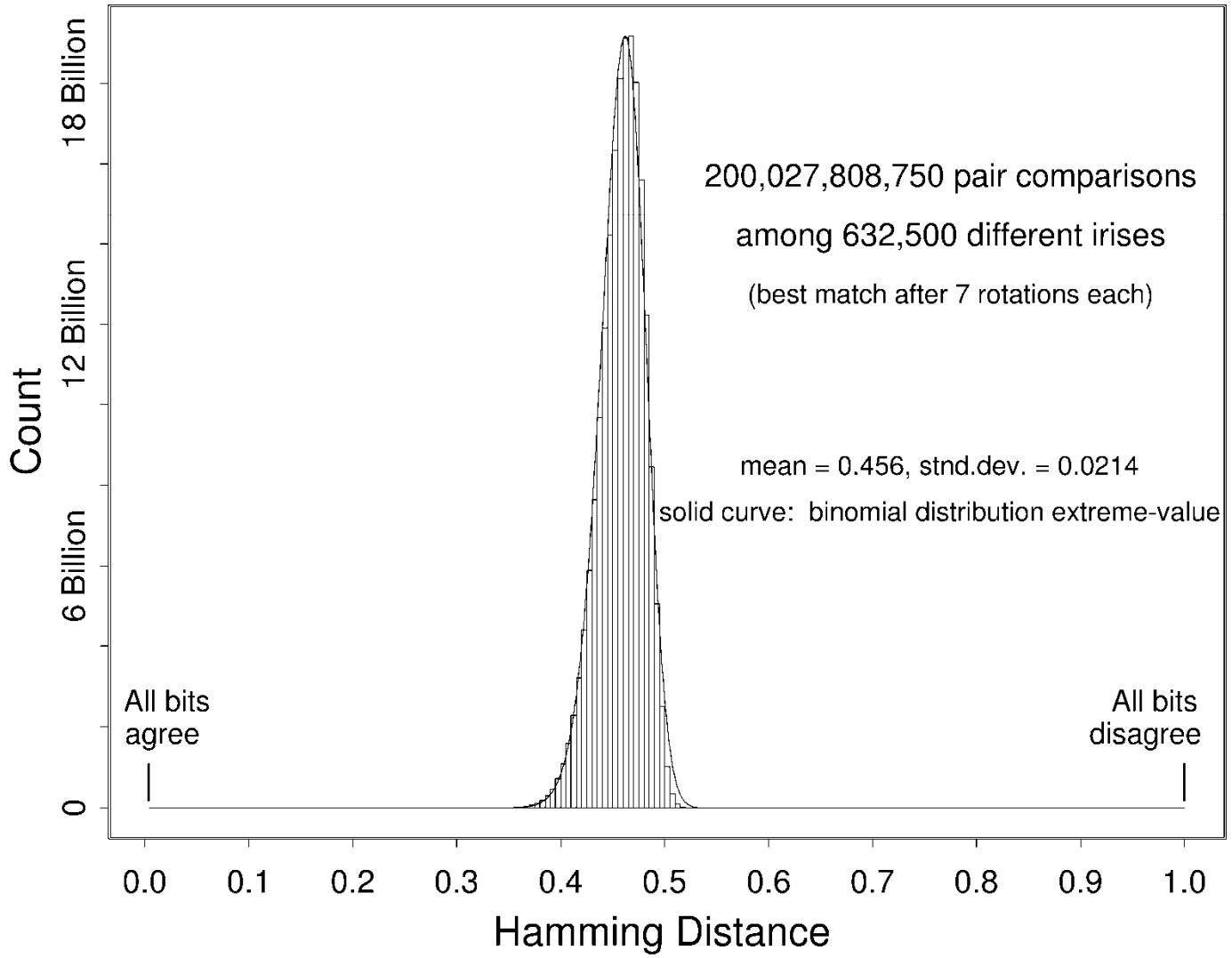
$$F_k(x) = 1 - [1 - F_0(x)]^k \tag{3}$$

and the expected density $f_k(x)$ associated with this cumulative is:

$$\begin{aligned} f_k(x) &= \frac{d}{dx}F_k(x) \\ &= k f_0(x) \left[1 - F_0(x)\right]^{k-1} \end{aligned} \tag{4}$$

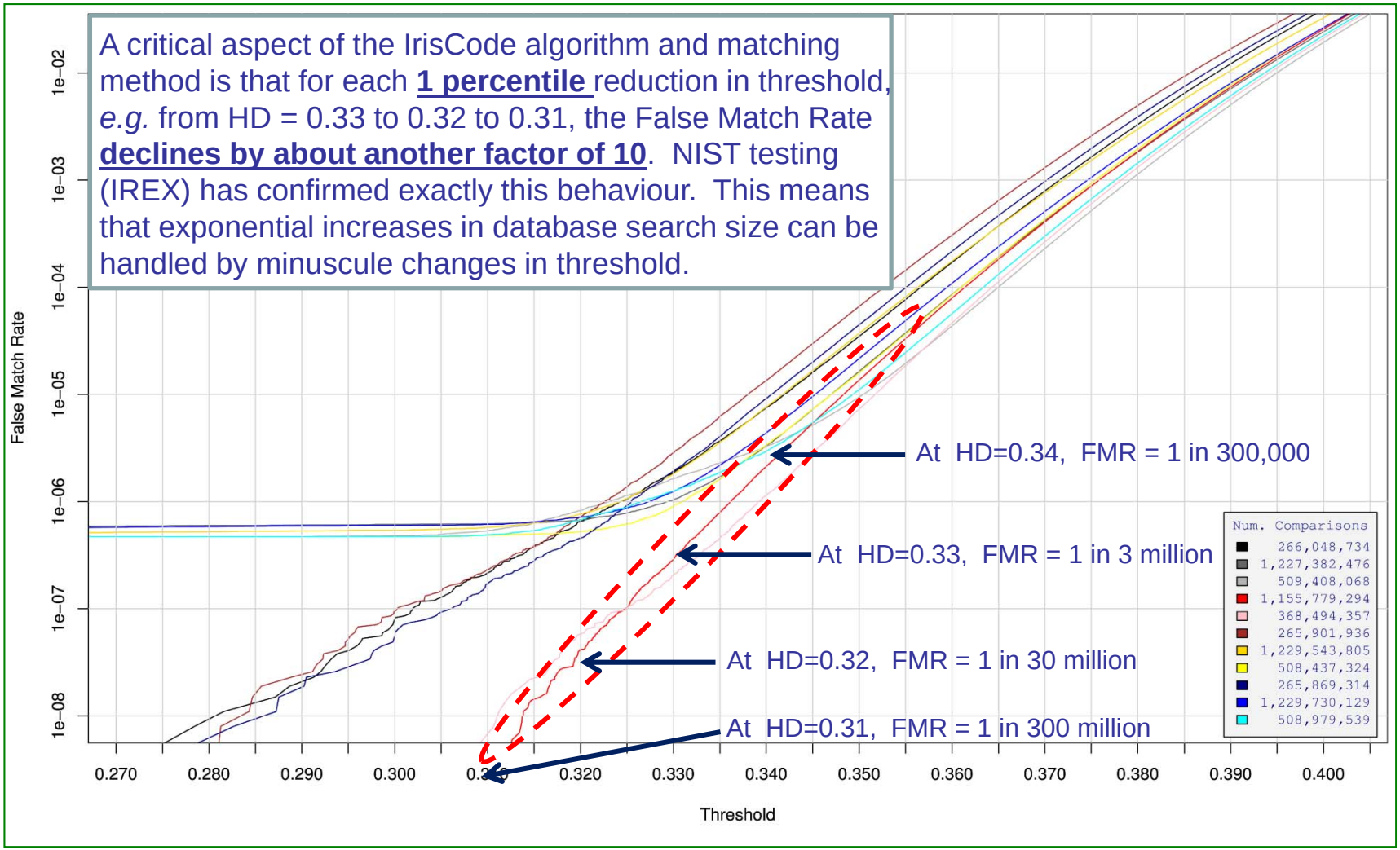
UNIVERSITY OF CAMBRIDGE

Score Distribution for 200 Billion Iris Comparisons after Rotations



UNIVERSITY OF
CAMBRIDGE

NIST (IREX-1) confirmation of the exponential decline in False Match Rate with minor threshold reductions



UNIVERSITY OF CAMBRIDGE

False Match Rates with HD_{norm} Score Normalization: Dependence on Criterion (200 Billion Comparisons, UAE Database)

HD Criterion	*Observed False Match Rate*
0.220	0 (*theor: 1 in* 5×10^{15})
0.225	0 (*theor: 1 in* 1×10^{15})
0.230	0 (*theor: 1 in* 3×10^{14})
0.235	0 (*theor: 1 in* 9×10^{13})
0.240	0 (*theor: 1 in* 3×10^{13})
0.245	0 (*theor: 1 in* 8×10^{12})
0.250	0 (*theor: 1 in* 2×10^{12})
0.255	0 (*theor: 1 in* 7×10^{11})
0.262	1 in 200 billion
0.267	1 in 50 billion
0.272	1 in 13 billion
0.277	1 in 2.7 billion
0.282	1 in 284 million
0.287	1 in 96 million
0.292	1 in 40 million
0.297	1 in 18 million
0.302	1 in 8 million
0.307	1 in 4 million
0.312	1 in 2 million
0.317	1 in 1 million

The benefit of fusion:

This entire range of False Match probabilities can be squared, if both eyes are used ("AND "rule), because they are independent. *E.g.*. If both eyes give HD scores below 0.28 (for which FMR~10^{-9}), then their joint FMR is ~10^{-18}

Empirical performance in this range was confirmed also by IBG's ITIRT Report (2005) testing these algorithms.

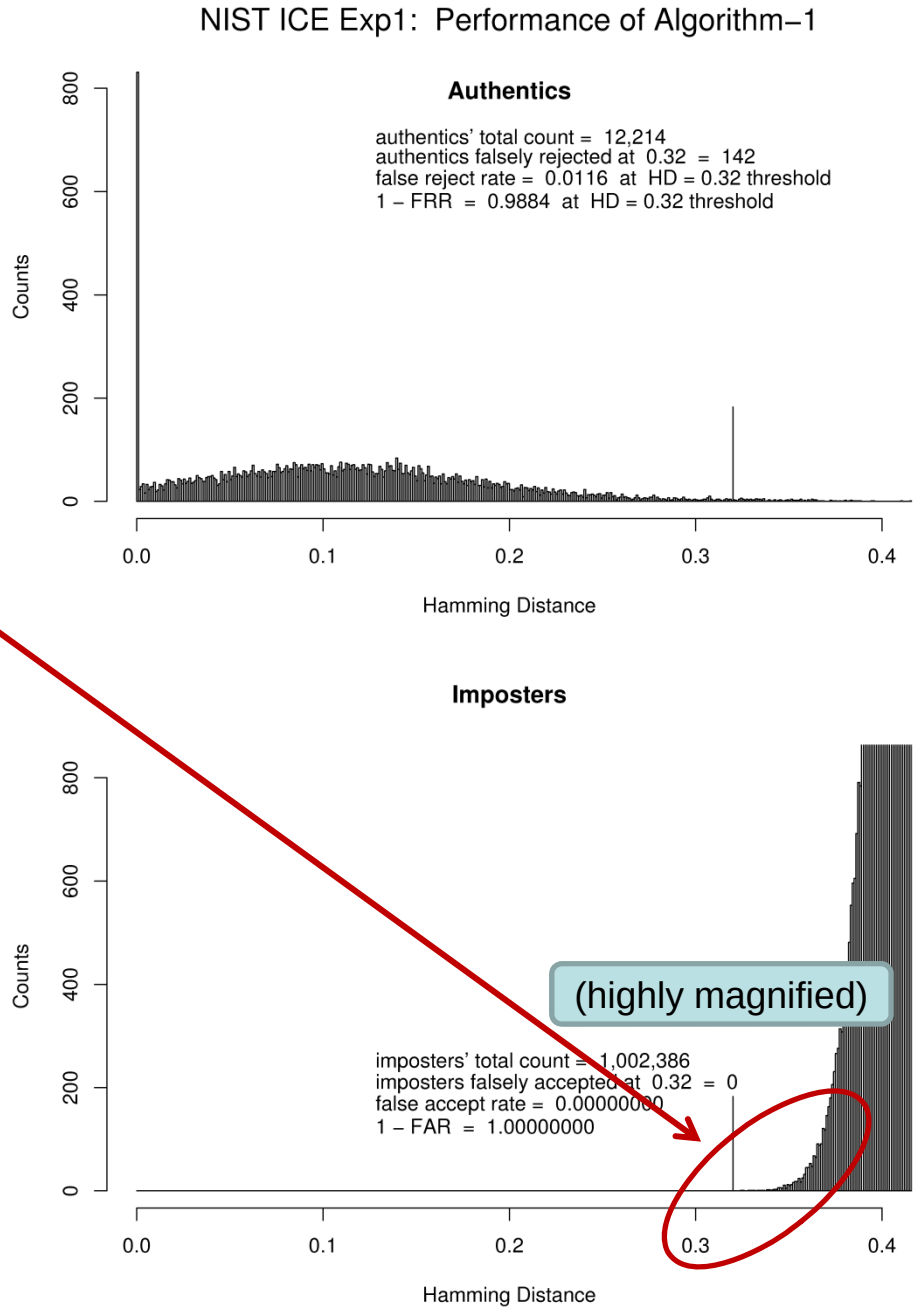
In 1.7 billion comparisons between different irises, the smallest HD score observed by IBG was in the vicinity of 0.28 (consistent with this Table).

UNIVERSITY OF CAMBRIDGE

In biometrics, it is the tail attenuation that matters!

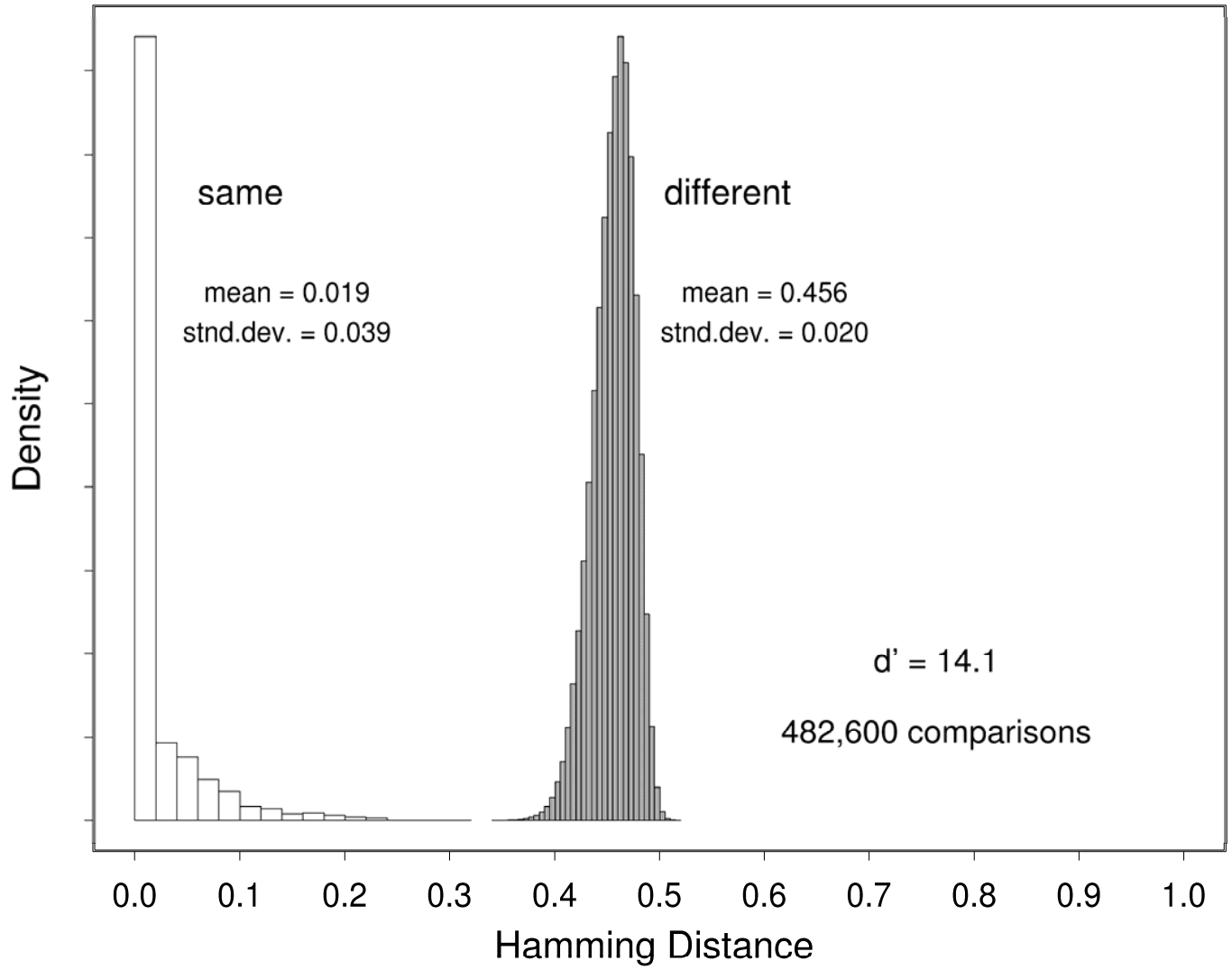
The key to iris recognition's resistance to False Matches is the very rapid attenuation of the tail of the distribution for Impostor iris comparisons.

This property seems to be unique to this biometric, and it reflects the great entropy of the iris code.



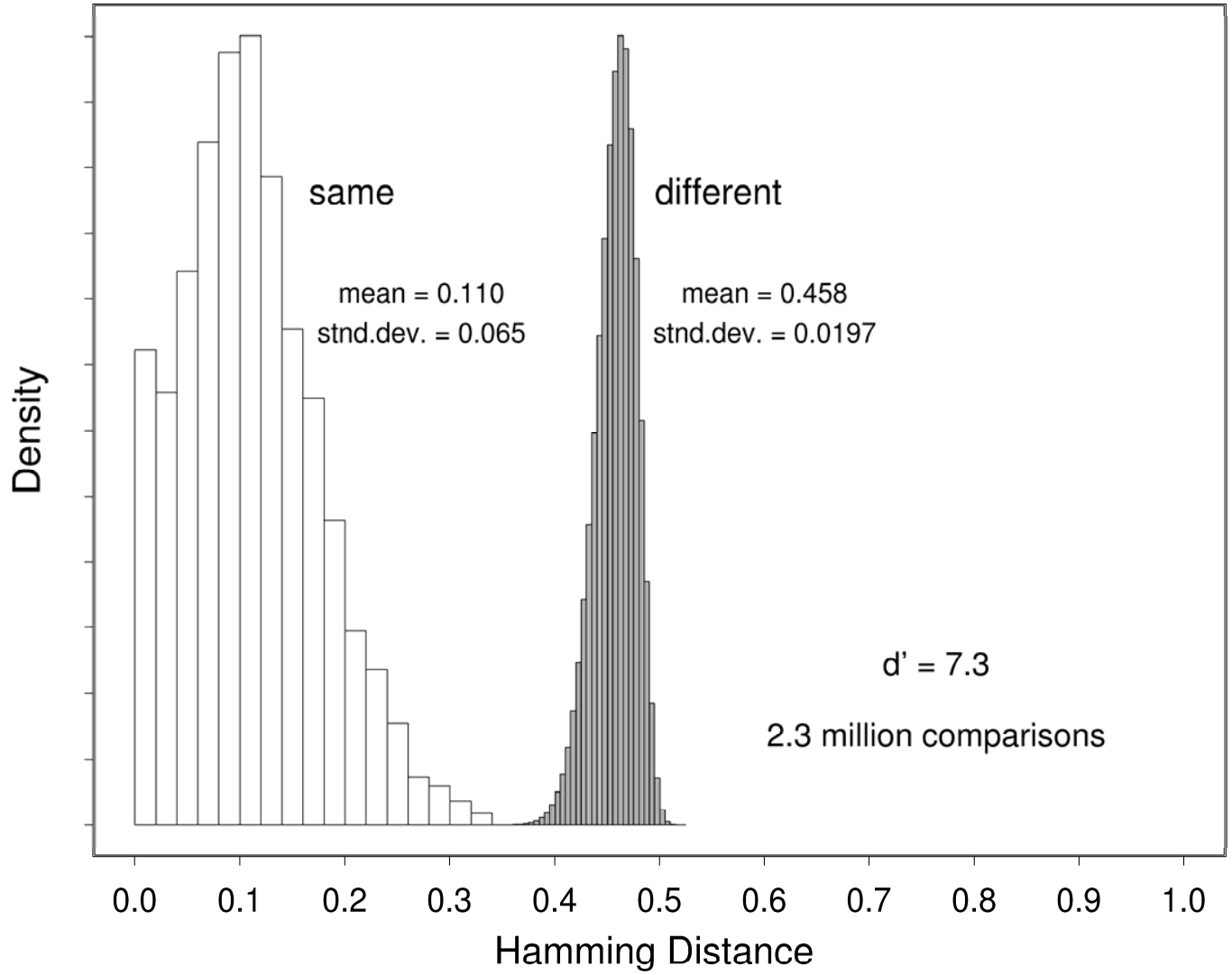
UNIVERSITY OF CAMBRIDGE

Decision Environment for Iris Recognition: Ideal Imaging

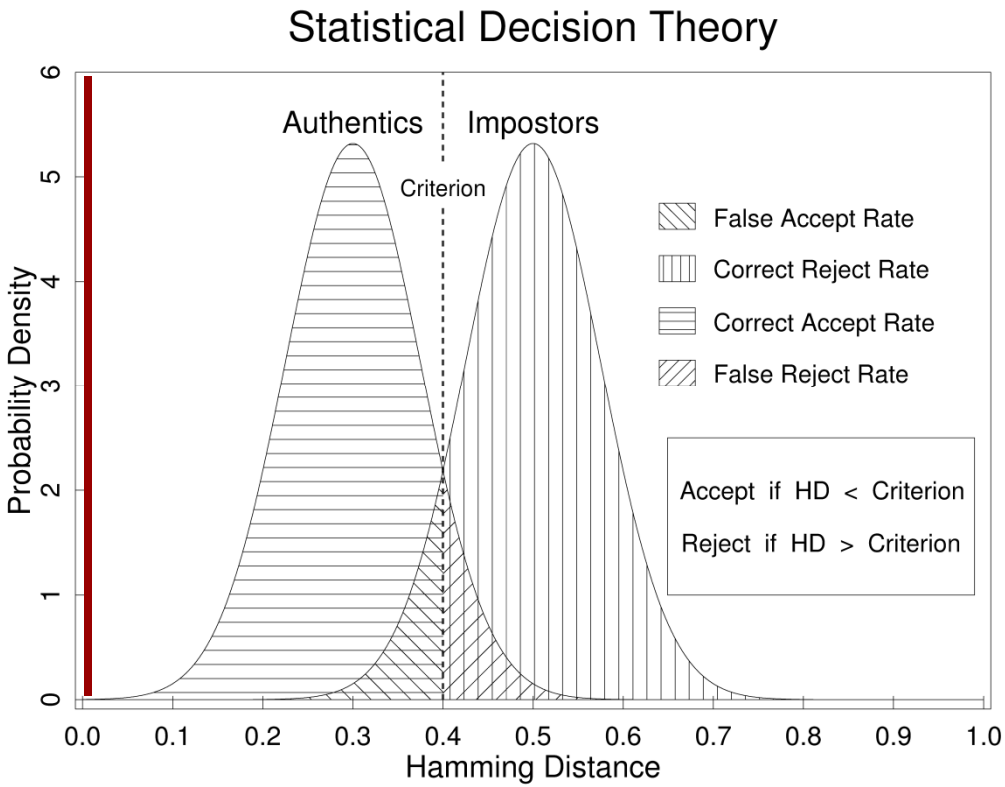


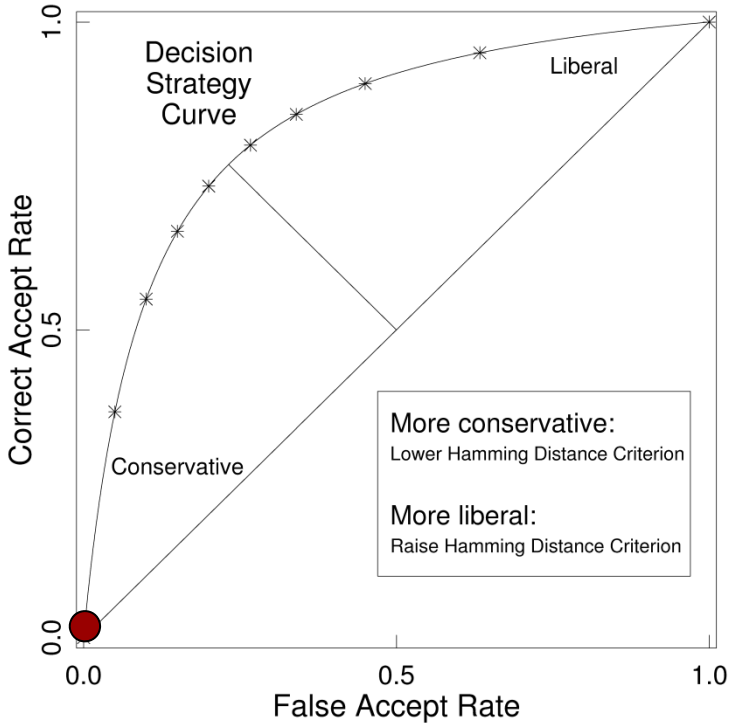
UNIVERSITY OF CAMBRIDGE

Decision Environment for Iris Recognition: Non-Ideal Imaging



UNIVERSITY OF CAMBRIDGE



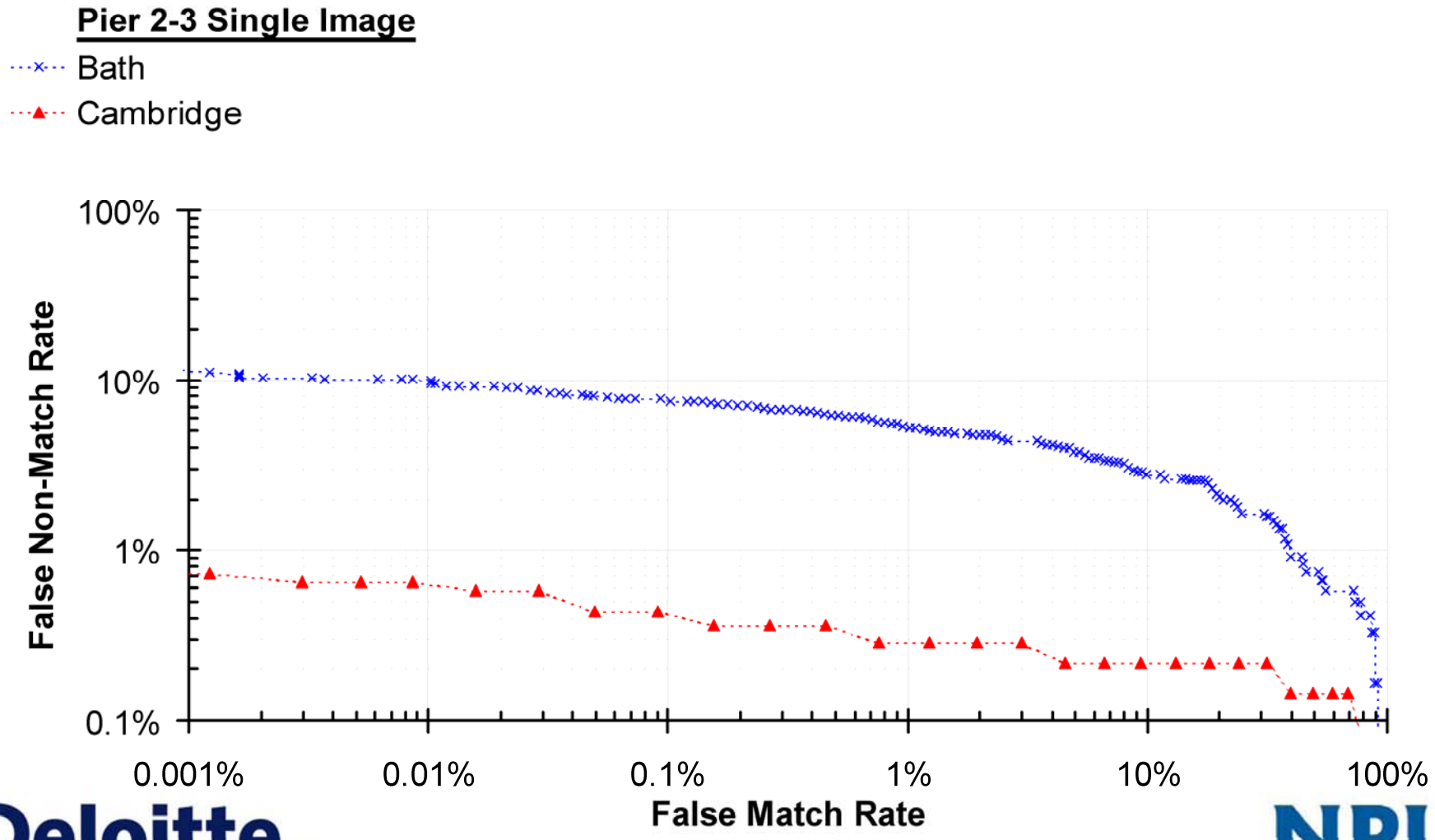


Generating ROC (or DET) curves requires moving the decision threshold, from conservative to liberal, to see the trade-off between FMR and FnMR errors.

The slope of the ROC curve is the likelihood ratio: ratio of the two density distributions at a given decision threshold criterion. Flat ROC curves permit FMR to be greatly reduced by small threshold changes, at little cost to FnMR.

UNIVERSITY OF CAMBRIDGE

Performance of iris comparison algorithms



Deloitte.

NPL

7.7.1 Intra-Visit Enrollment Comparison DETs (Single-Attempt)

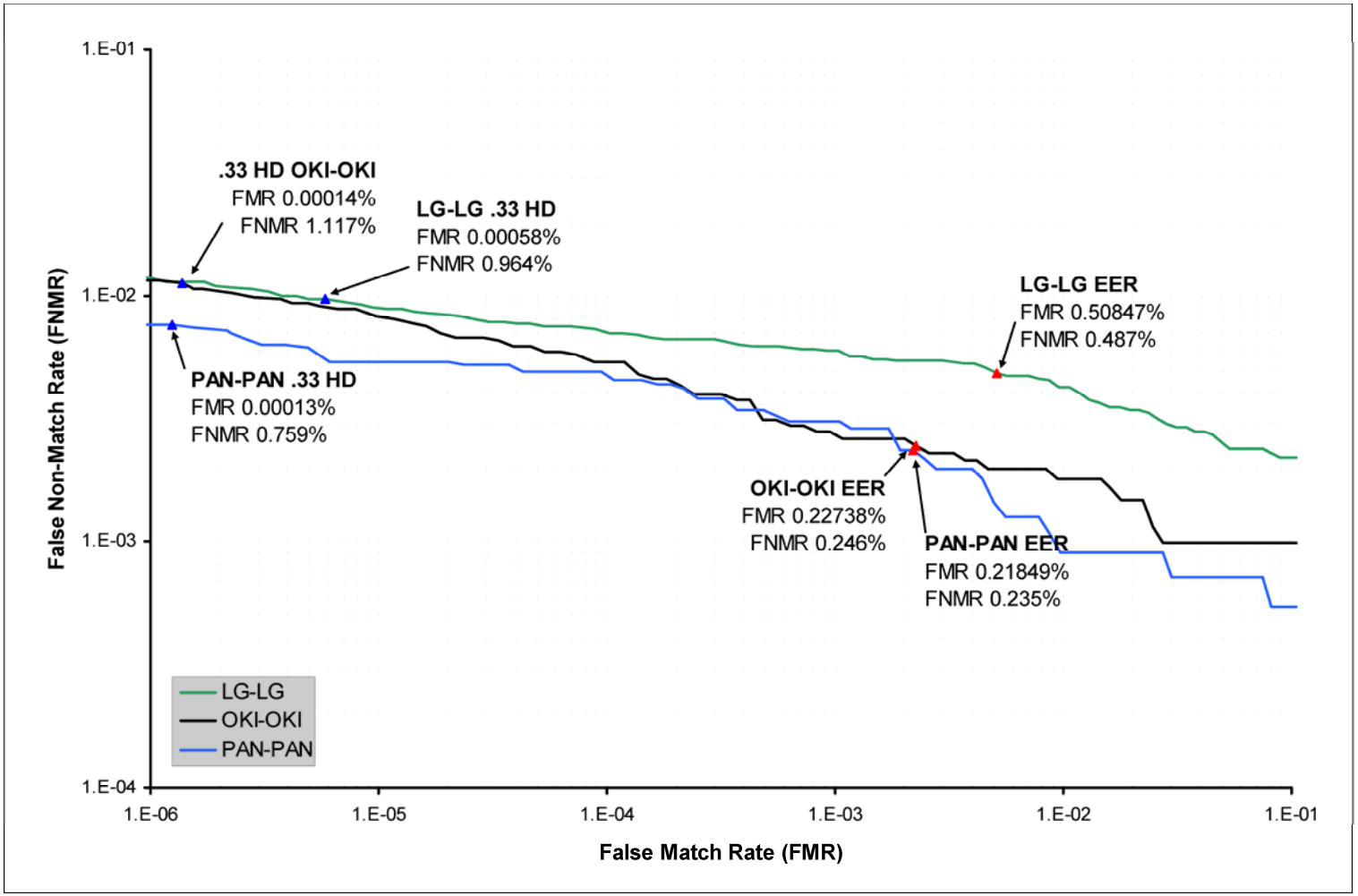


Figure 55: Intra-Visit Enrollment Comparison DETs (Single-Attempt)

Some significant public deployments of the algorithms

- UK Project IRIS: Iris Recognition Immigration System

A "frequent flier" programme that allows enrolled participants to enter the UK from abroad without passport presentation, and without asserting their identity in any other way. Cameras at automated gates operate in identification mode, searching a centralised database exhaustively for any match.

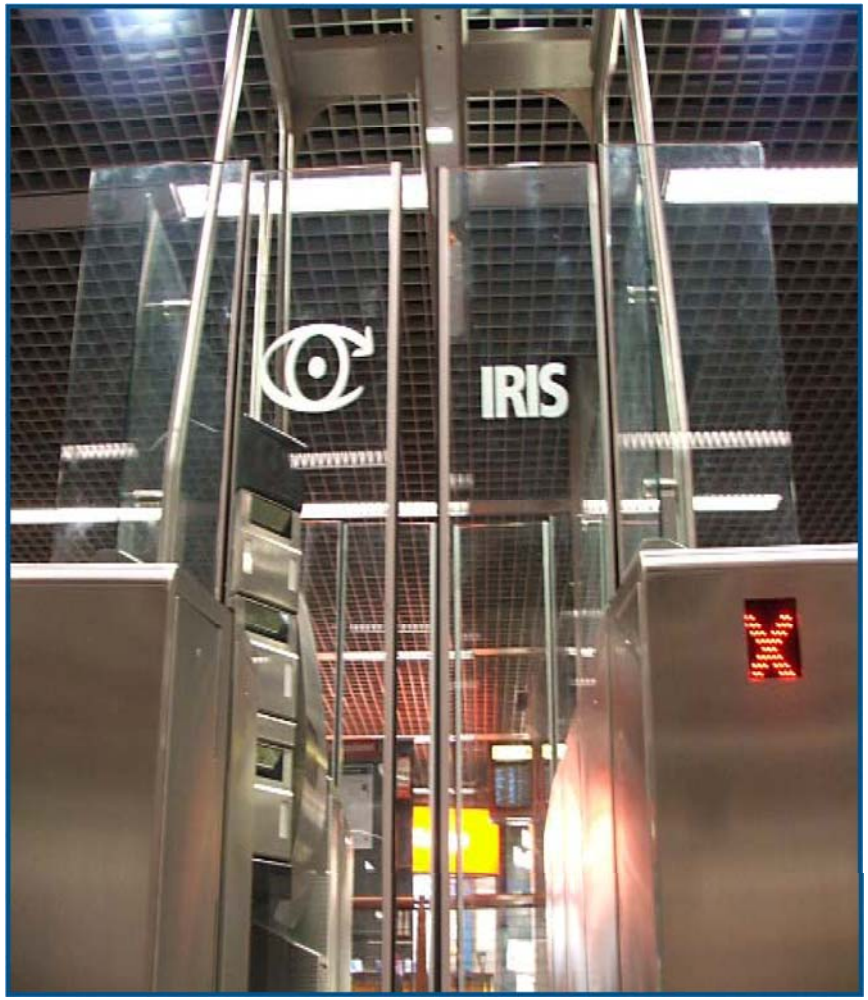
Home Office
Border & Immigration Agency

IRIS statistics as of June 2009:

" > 1 million frequent travellers have been enrolled, growing by 2,000 per week, and there have been about 4 million IRIS automated entries since January 2006, with currently almost 20,000 IRIS arrivals into the UK per week."

UNIVERSITY OF CAMBRIDGE

UNIVERSITY OF CAMBRIDGE



IRIS gates at 10 UK airport terminals for registered frequent travellers in lieu of passport presentation

US-Canadian border crossing in lieu of passports

UNIVERSITY OF CAMBRIDGE

- The United Arab Emirates iris-based border security system

- Deployed at all 32 air, land, and sea-ports
- 1,190,000 IrisCodes registered in a watch-list
- On a typical day 12,000 irises are compared to all on the watch-list (14 billion comparisons/day)
- Each exhaustive search takes < 2 seconds
- About 30 trillion (30 million-million) comparisons of irises have been done since 2001
- After an amnesty for violators of work permit laws or other offences in 2001, expellees' iris patterns were encoded. About 150,000 persons have since been caught trying to re-enter illegally.

UNIVERSITY OF CAMBRIDGE

UNIVERSITY OF CAMBRIDGE

Residency Permit Applications

UNIVERSITY OF CAMBRIDGE

U.S. Police Departments: bookings and releases

UNIVERSITY OF CAMBRIDGE

Takhtabaig Voluntary Repatriation Centre, Pakistan-Afghan border

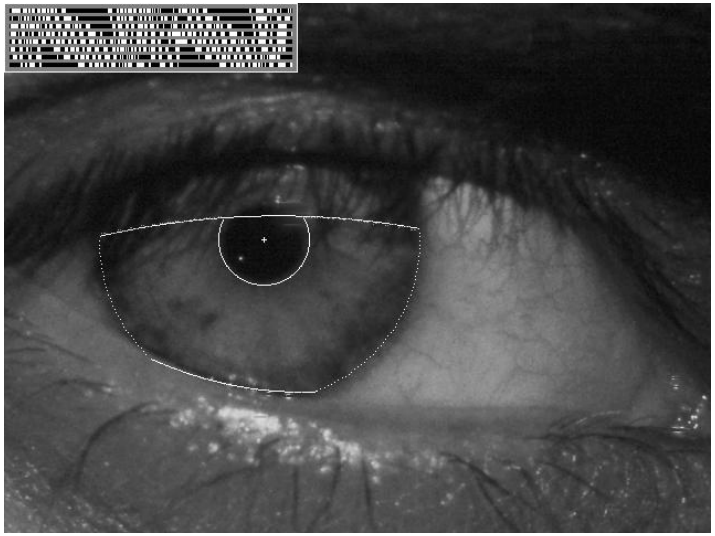
The United Nations High Commission for Refugees (UNHCR) administers cash grants for returnees, using iris identification.

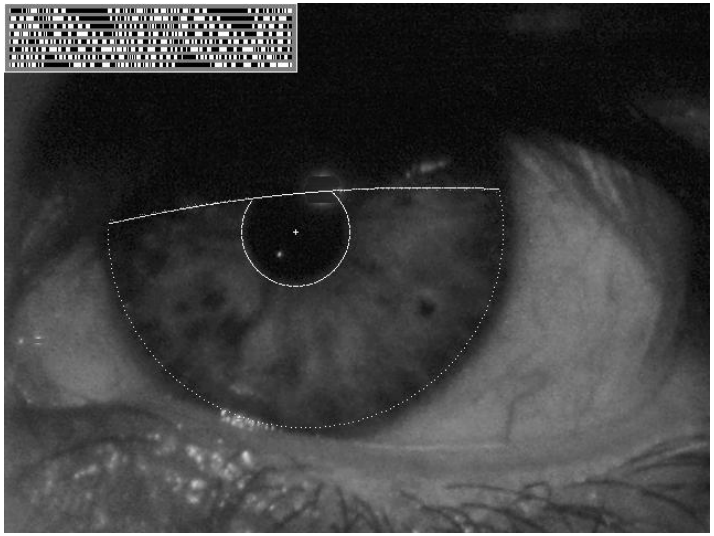
UNIVERSITY OF CAMBRIDGE

UNIVERSITY OF
CAMBRIDGE

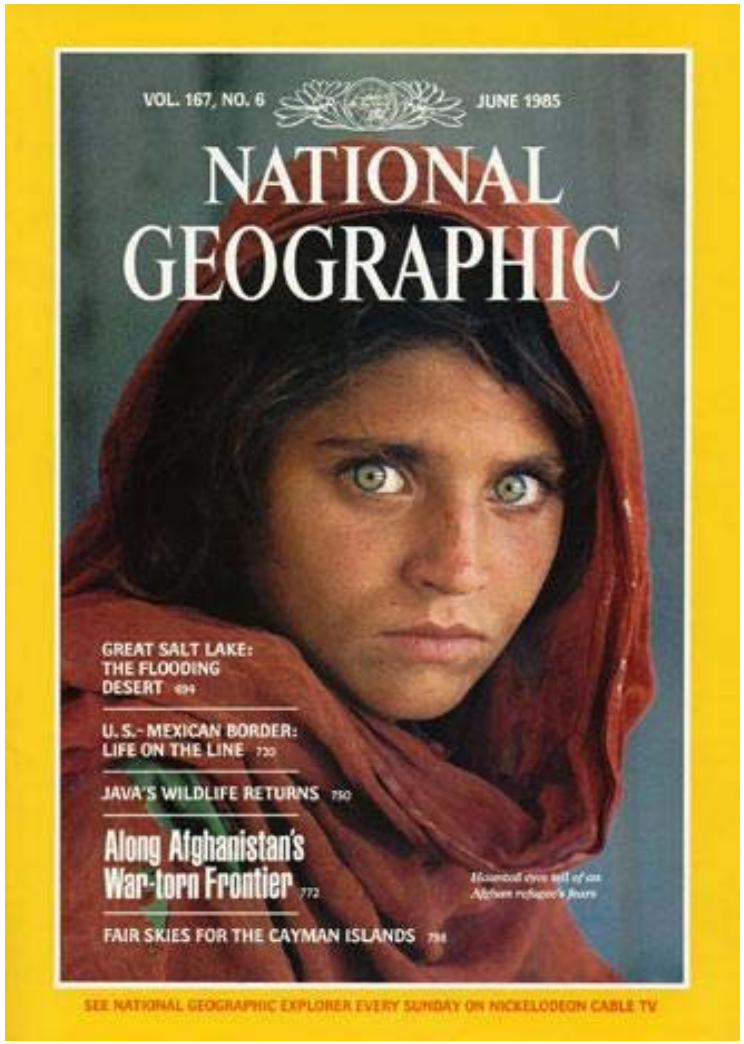
Sharbat Gula (1984); identified (2002) by these iris algorithms
(based on photographs taken by *National Geographic*)

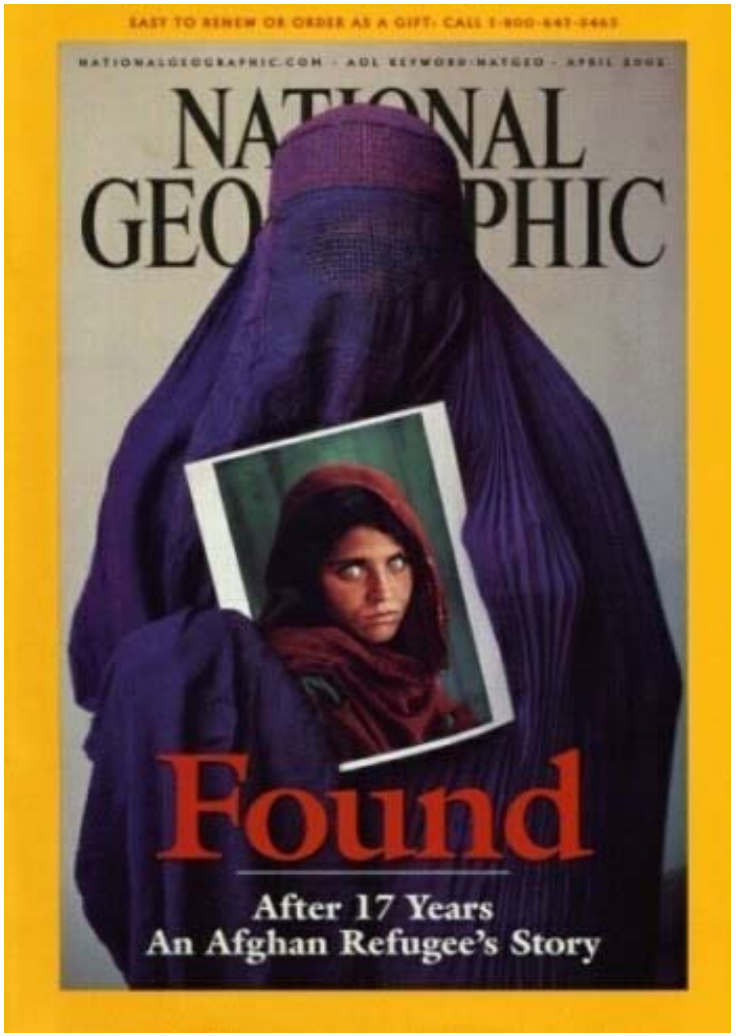
UNIVERSITY OF
CAMBRIDGE



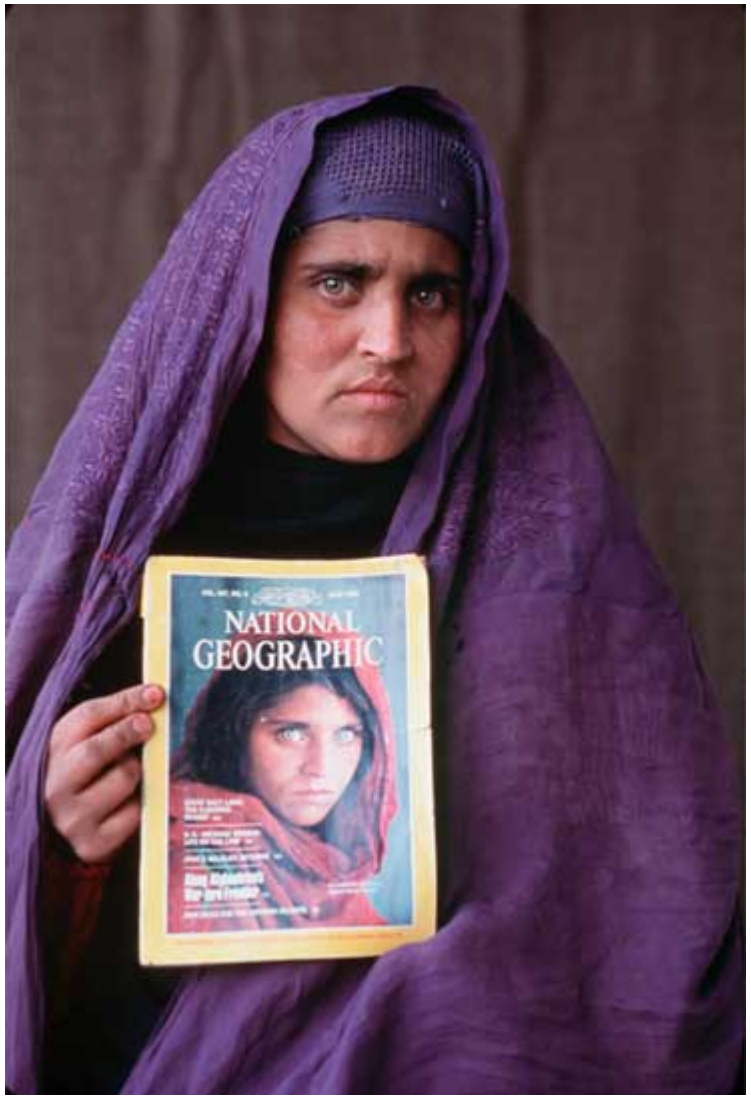


UNIVERSITY OF CAMBRIDGE





UNIVERSITY OF CAMBRIDGE



UNIVERSITY OF
CAMBRIDGE


Schiphol Airport (NL):
iris recognition in lieu of
passport presentation

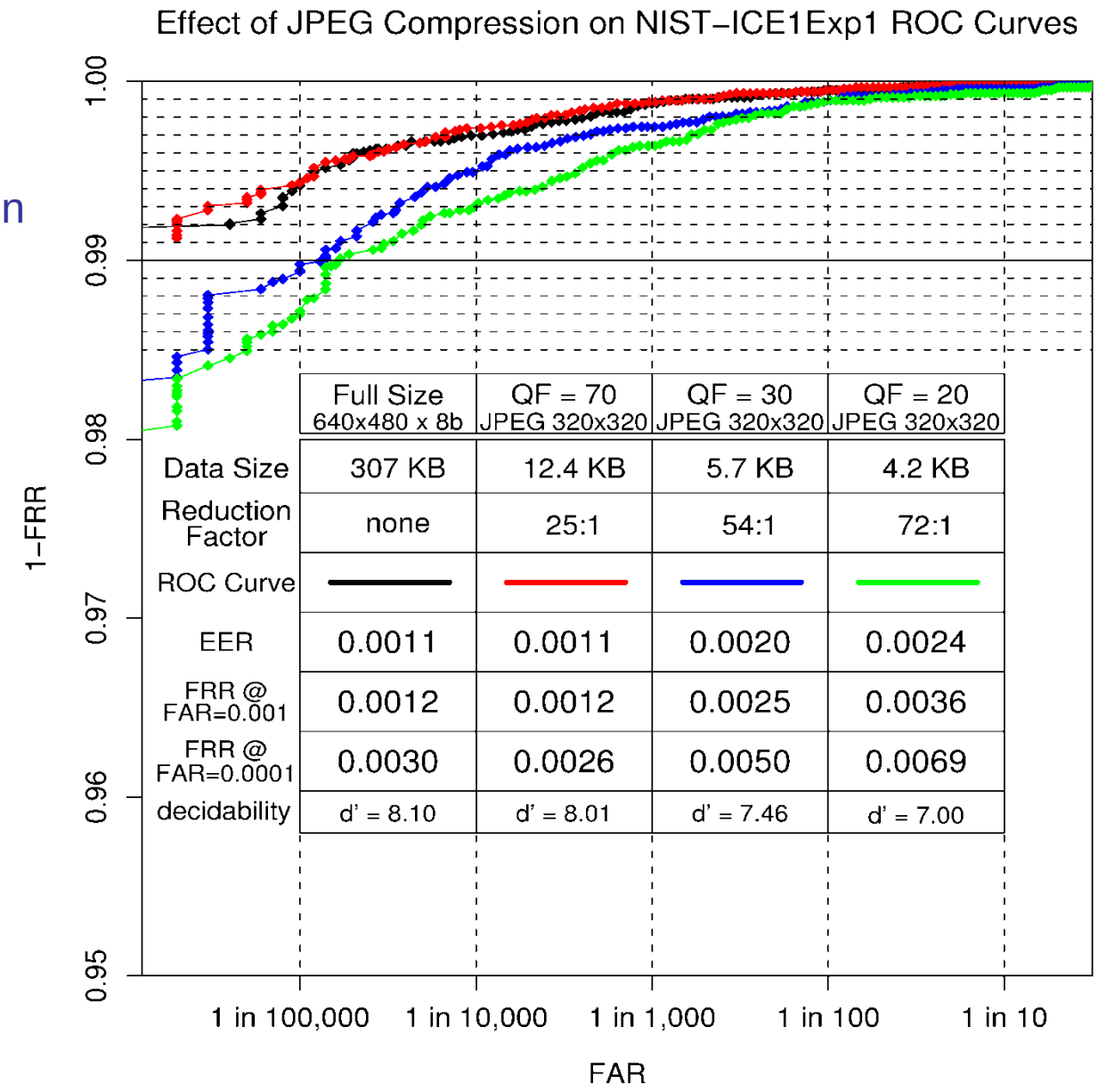
Access to condominium building, and programming the lift (!), by iris recognition

Iris image standard; data formats; compressibility

- ISO/IEC 19794-6 Iris Image Data Interchange Format Standard (revision published in 2011)
- Inter-operable image formats were required, not proprietary IrisCode templates (vendor neutral)
- NIST IREX study endorsed new compact formats: iris image compression to as little as 2 KB using JP2K (not JPEG), with cropping and ROI masking; or lossless compression using PNG container
- Revision process was **empirically-based** (process promoted by Prof. C. Busch, and driven by NIST)

UNIVERSITY OF CAMBRIDGE

Effect of JPEG compression



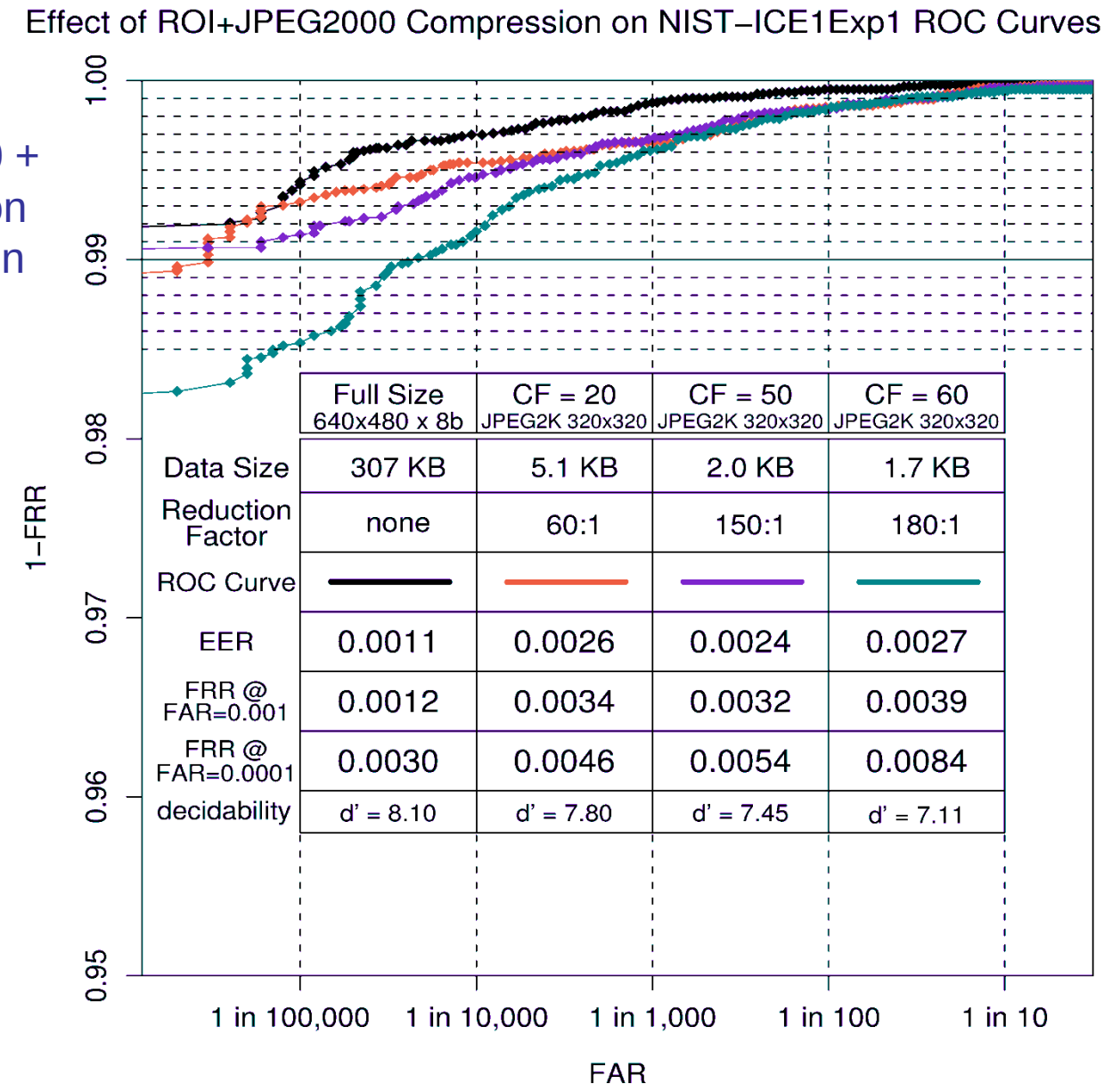
UNIVERSITY OF CAMBRIDGE

Region-of-Interest cropping and JPEG-2000 compression allows iris images

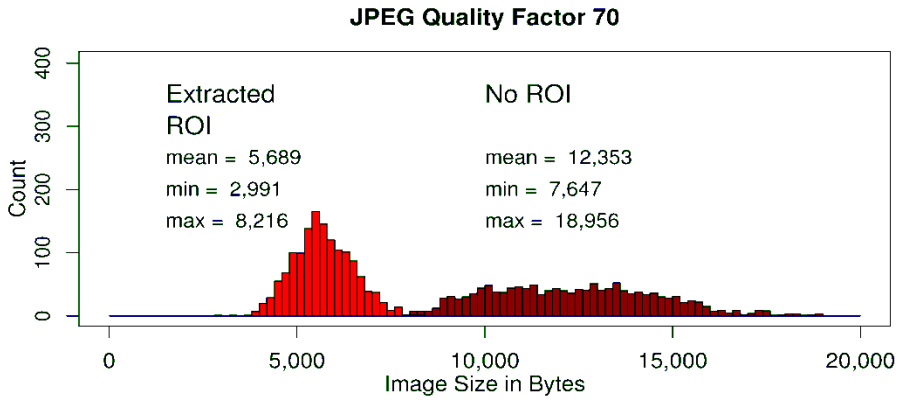
to be compressed to only 2,000 – 2,500 bytes with little impact on performance

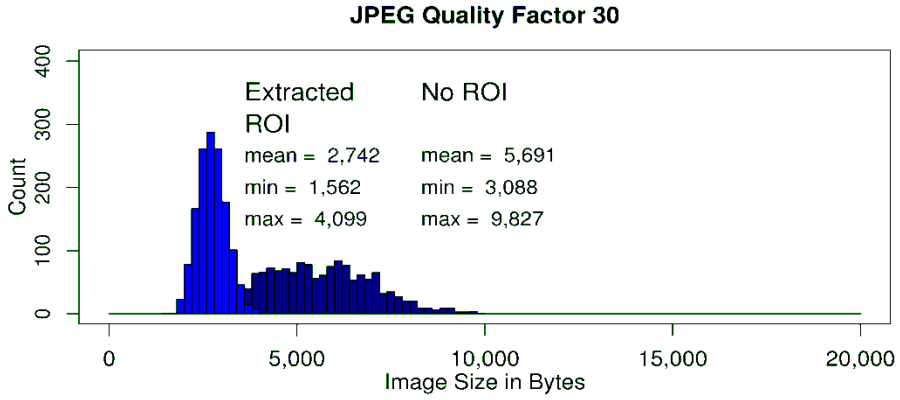
UNIVERSITY OF CAMBRIDGE

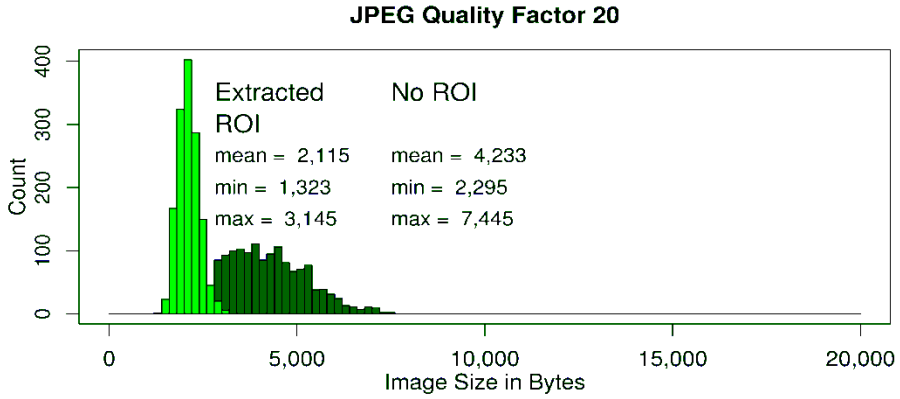
Effect of JPEG-2000 + ROI isolation compression

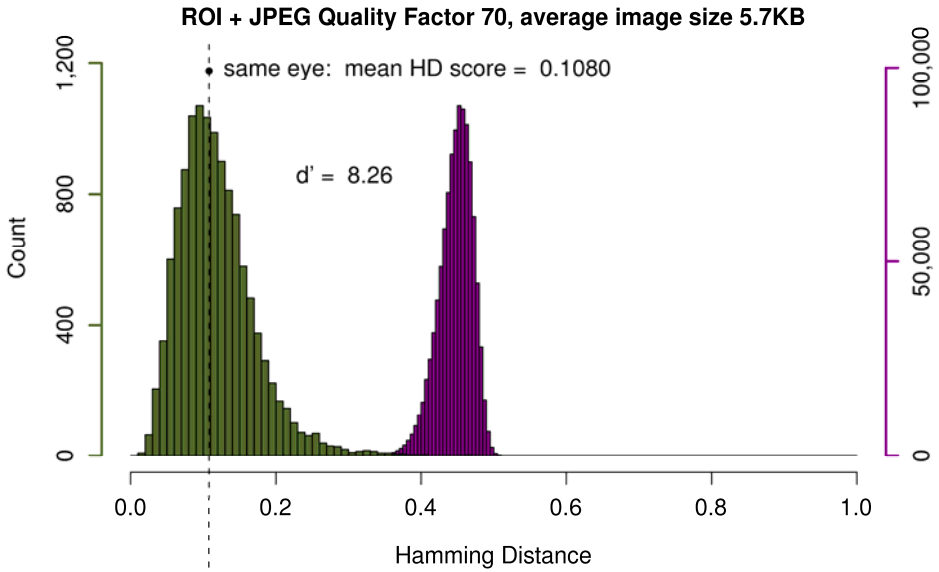


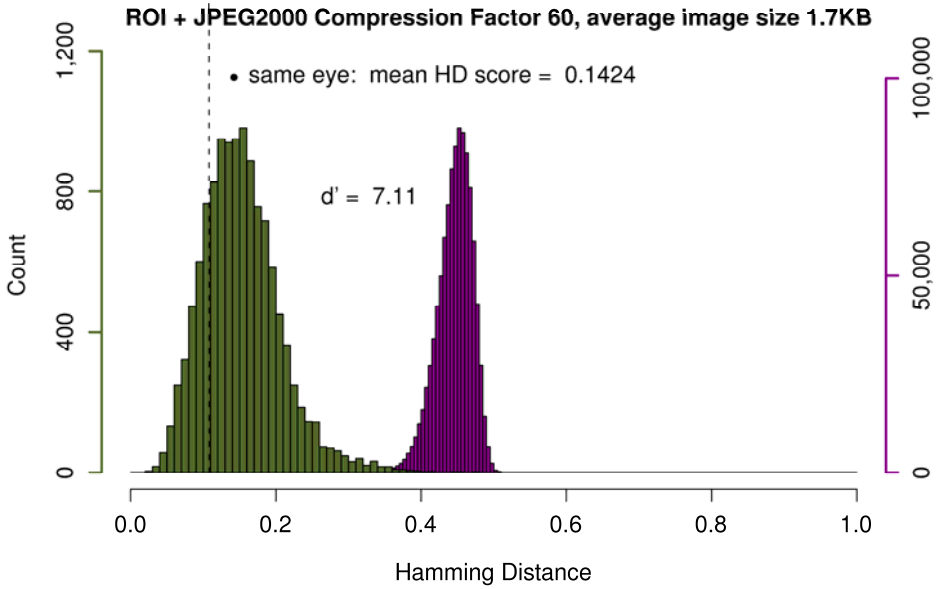
UNIVERSITY OF CAMBRIDGE











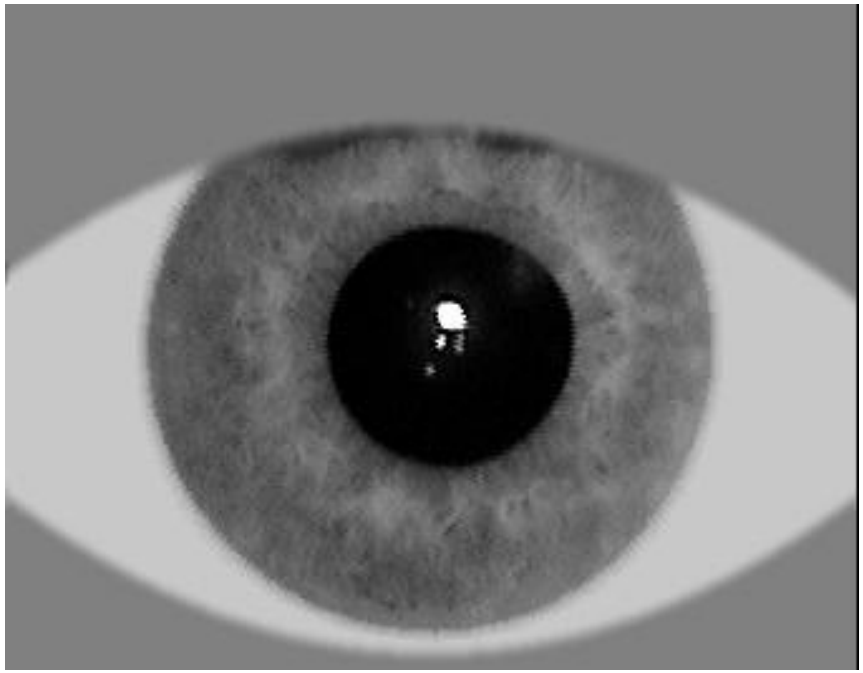
UNIVERSITY OF CAMBRIDGE

Strategy	Compression Parameter	Average Image Size	Interoperability Hamming Distance
Cropping (320 x 320) + JPEG Compression	QF = 70	**12.4 KB**	0.006
	QF = 30	**5.7 KB**	0.011
	QF = 20	**4.2 KB**	0.021
Cropping + ROI + JPEG Compression	QF = 70	**5.7 KB**	0.015
	QF = 30	**2.7 KB**	0.021
	QF = 20	**2.1 KB**	0.031
Cropping + ROI + JPEG2000 Compression	CF = 20	**5.1 KB**	0.018
	CF = 50	**2.0 KB**	0.027
	CF = 60	**1.7 KB**	0.035

Interoperability of the ROI and compression methods, compared with original

UNIVERSITY OF CAMBRIDGE

New ISO Standard: highly compact iris image format, compressed to as little as 2,000 bytes



- Cropping, and masking non-iris regions, preserves the coding budget
- Pixels outside the ROI are fixed to constant values, for normal segmentation
- Softening the mask boundaries also preserves the coding budget
- At only 2,000 bytes, iris images are now much more compact than fingerprints

UNIVERSITY OF CAMBRIDGE

Combining **biometrics** (fuzz data, unreliable bits) with **cryptography** (requires exactly correct bits in keys):

--Can error-correcting codes give stable "biometric keys"?

- Familiar example of error-correcting codes: the "Hamming 7/4" Code uses 7 bits to transmit 4 bits reliably over a noisy channel

- How it works: before transmission, 3 error-correcting bits are derived from the 4 data bits by XORing triples of them. Then all 7 bits are then transmitted as a block.
- Upon reception, 3 *syndromes* are computed by XORing each of the received error-correcting bits with the data bits (as received) that should have defined them.

- If all 3 syndromes equal 0, there was no error. Else, they specify which one bit in a 7-bit block was bad.

UNIVERSITY OF CAMBRIDGE

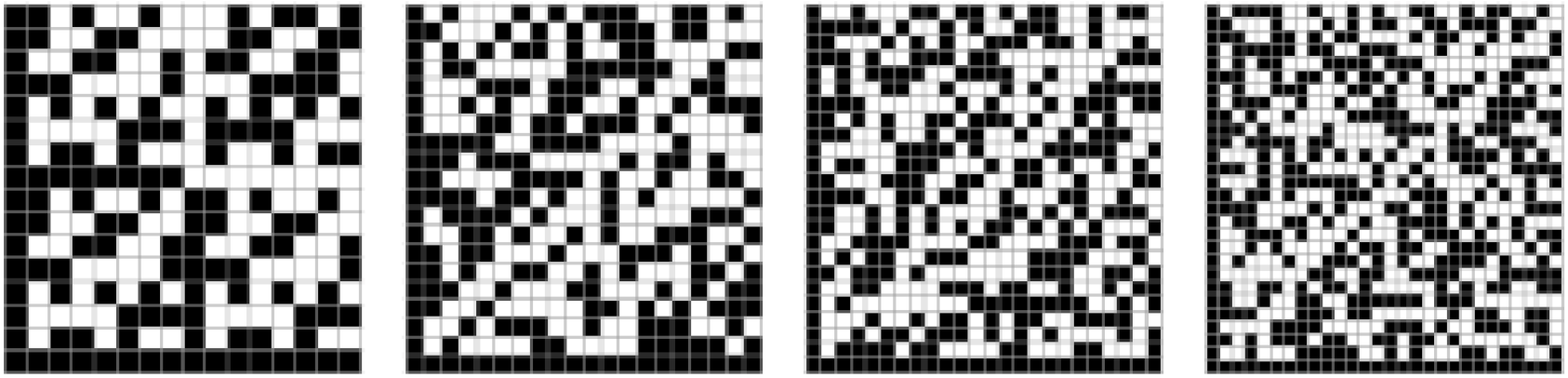
$$
\begin{aligned}
b_4 &= b_5 \oplus b_6 \oplus b_7 \text{ and,} \\
s_4 &= b_4 \oplus b_5 \oplus b_6 \oplus b_7 \\
b_2 &= b_3 \oplus b_6 \oplus b_7 \text{ and,} \\
s_2 &= b_2 \oplus b_3 \oplus b_6 \oplus b_7 \\
b_1 &= b_3 \oplus b_5 \oplus b_7 \text{ and,} \\
s_1 &= b_1 \oplus b_3 \oplus b_5 \oplus b_7
\end{aligned}
$$

On reception if the binary number $s_4 s_2 s_1 = 0$ then there is no error, else $b_{s_4 s_2 s_1}$ is the bit in error.

Note that this code will correct at most 1 bad bit in each block of 7. It used 3 bits to correct any of 7 possible block errors.

Many other error-correcting codes exist. E.g. a *Golay code* uses 23 bits to transmit 12 bits reliably, correcting up to 3 bit errors in each block. Compact discs use *Reed-Solomon codes* that correct up to 4,000 bits in an error burst (= 2.5 mm long).

Hadamard Matrix Codes



A Hadamard matrix is a square orthogonal matrix with binary elements: the inner product of any two rows or columns is 0. The rows (columns) can be used as codewords by projecting binary data (e.g. IrisCodes) onto them and finding the closest match. They allow extraction of stable keys.

Example: a 64 x 64 Hadamard matrix generates 128 codewords, and so (by encoding a 64-bit data string into a codeword using its 7-bit address) can "correct" up to 15 errors in each block of 64 data bits. From every 64 bit chunk of biometric data, we can extract 7 stable bits of biometric key.

UNIVERSITY OF CAMBRIDGE

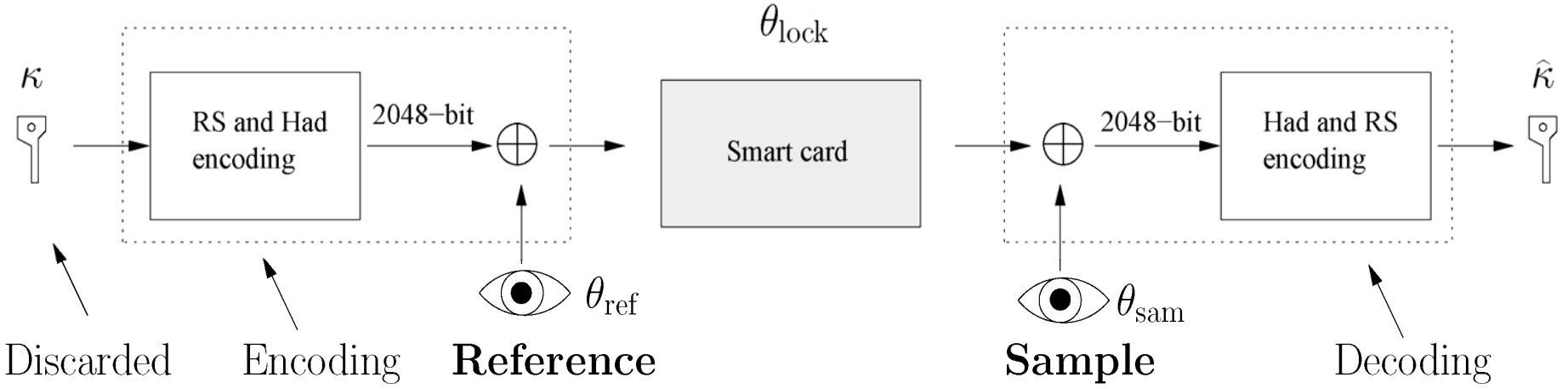
Combining biometrics with cryptography:

(Hao Feng PhD dissertation, Cambridge 2007)

- Use Hadamard+RS coding of a randomly generated key (embedding error correction) and XOR this with a 2048-bit user IrisCode. Securely discard the original random key, but store the "locked (XORed) IrisCode" on a token.
- XOR a user-presented IrisCode: retrieve a corrupted key, from which the error-correction retrieves the original key.
- This encoding is stable with up to 15 bit "errors" in each chunk of 64 IrisCode bits. (Tolerates 23% variation.)
- The Reed-Solomon encoding corrects for block errors ("burst errors" in which more than 15 bits are bad in any block of 64, e.g. due to eyelashes, reflections, etc.)
- This allows extraction of 20 stable blocks from 32 blocks, yielding 140 bits (20 x 7 bits) of stable biometric key.
- Tested on 700 same-eye IrisCodes from 70 eyes: in all but 3 cases (0.47%) the stable key could be generated.

UNIVERSITY OF CAMBRIDGE

(Hao Feng PhD dissertation, continued)



Recall that the Boolean XOR operator $\oplus$ combines two strings such that when the resulting string is again XORed with either of the first two strings, the other string emerges:

A	B	C = A⊕B	C⊕A = B	C⊕B = A
0	0	0	0	0
1	0	1	0	1
0	1	1	1	0
1	1	0	1	1

Truth Table for XOR

Thus XORing with the Sample IrisCode retrieves the key in slightly corrupted, but correctable, form.

UNIVERSITY OF CAMBRIDGE

(Hao Feng PhD dissertation, continued)

- The 140-bit stable biometric key means that identification of persons can be performed biometrically but without storing a central database of biometric templates.
- (Instead, what is stored is only the 140-bit key extracted from a locked IrisCode, but not reversible into it. Storing a locked code + key-hash on token gives a citizen control over its use, and importantly, provides revocability.)
- A citizen establishes their identity by biometrically generating / extracting their stable 140-bit key.
- The 140 bits of stable biometric key extracted from the iris compares favourably with the 69 bits extractable from fingerprints (Clancy 2003), which could be done in only 70% of samples.

UNIVERSITY OF CAMBRIDGE

A short bibliography on biometric crypto-systems

1. Soutar, Roberge, Stoianov, Gilroy, and Vijaya-Kumar (1999) "Biometric Encryption" *(ICSA Guide to Cryptography, McGraw-Hill)*
2. Davida, Frankel, Matt, and Peralta (1999) "On the Relation of Error Correction and Cryptography to an Off-Line Biometric ID Scheme"
3. Clancy, Kiyavash, and Lin (2003) "Secure Smart Card-based Fingerprint Authentication" *(Proc. 2003 ACM SIGMM Workshop)*
4. Goh and Ngo (2003) "Computation of Cryptographic Keys from Face Biometrics" *(Proc. 2003 Int'l Fed. for Information Processing)*
5. Uludag, Pankanti, Prabhakar, and Jain (2004) "Biometric Crypto-Systems: Issues and Challenges" *(Proc. IEEE, vol. 92, 2004)*
6. Hao, Anderson, and Daugman (2006) "Combining Crypto with Biometrics Effectively" *(IEEE Trans. Computers, vol. 55(9), 2006)*
7. Hao, Daugman, and Zielinski (2008) "A Fast Search Algorithm for a Large Fuzzy Database" *(IEEE Trans.Info.Foren.Sec. 3(2), 2008)*

UNIVERSITY OF CAMBRIDGE

Fuzzy database matching with a Codex

- (based on Technical Report circulated in March 2006: Hao, Daugman, and Zielinski, *"A fast search algorithm for a large fuzzy database"*, published in *IEEE T-IFS*, **3**(2), pp. 203-212.)

- Uses Indexing for large databases, instead of exhaustive search.
- The concept is similar to Content-Addressable Memory (CAM), in which the data itself is used as an address.
- A Codex is constructed, listing IrisCodes containing various bit patterns. When enough collisions, or "suspicious coincidences" occur between IrisCodes, they (and *they alone*) are considered candidates for matching. Speed-up arises from ignoring others.
- Pruning factor (therefore speed-up factor) approaches ~ 100:1. Adoption of Indexing should be gated by Quality Assessment.

UNIVERSITY OF CAMBRIDGE

The Doctrine of Suspicious Coincidences

When the recurrence of patterns just by chance is a highly improbable explanation, it is unlikely to be a coincidence.

UNIVERSITY OF CAMBRIDGE

“Panopticon” indexing, in lieu of exhaustive search

After enrollment of a large database, an off-line indexing stage classifies IrisCodes by bit patterns, hoping to avoid exhaustive search.

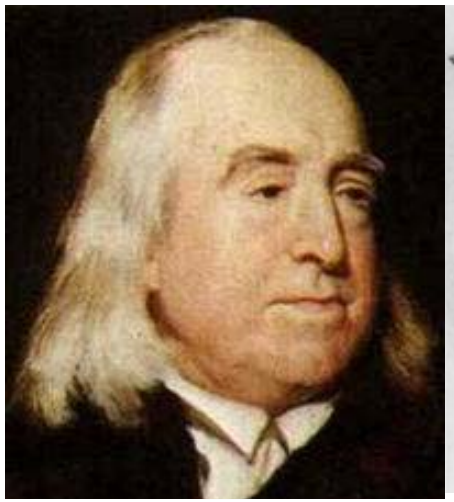
The concept is similar to Content-Addressable Memory (CAM), in which the data itself is used as an address.

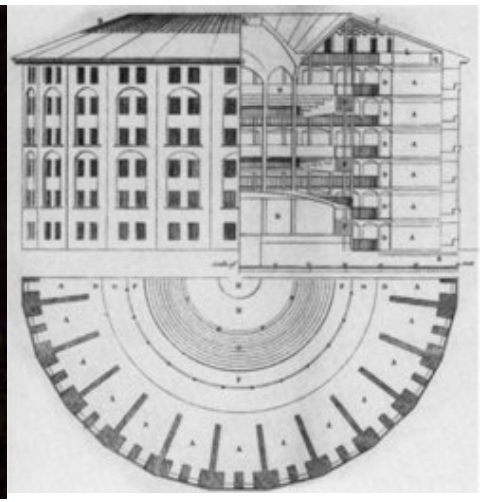
A Codex is constructed, listing IrisCodes containing all possible 10-bit patterns, for all positions. When enough “suspicious coincidences” (collisions) occur between IrisCodes, they (*alone*) are considered candidates for matching. Speed-up arises from ignoring the others.

Named “**Panopticon**” (after Jeremy Bentham’s 1791 prison design) because the entire database is surveyed at once, not sequentially.

Pruning factor (therefore speed-up factor) can approach ~ 100:1. Adoption of Indexing should be gated by Quality Assessment.

By **surveying the entire database simultaneously**, the Codex resembles Bentham's (1791) prison design called "Panopticon"





Contemporary implementation

The "Auto-Icon"

Jeremy Bentham today, at University College London, which he founded. He is still brought out to meetings of the College Council, listed as "present but not voting."

UNIVERSITY OF CAMBRIDGE

Active research areas: iris acquisition in less constrained imaging conditions

- iris on-the-move (normal walking, 1 meter/sec)
- iris at-a-distance (3 meters, even 10+ meters?)
- iris off-axis (deviated gaze: not looking at camera)
- iris recognition in ambient, uncontrolled illumination
- iris recognition in unsupervised conditions

  (countermeasures against spoofing attacks)
- iris recognition at reduced resolution

UNIVERSITY OF CAMBRIDGE

Iris-on-the-Move, Iris-at-a-Distance

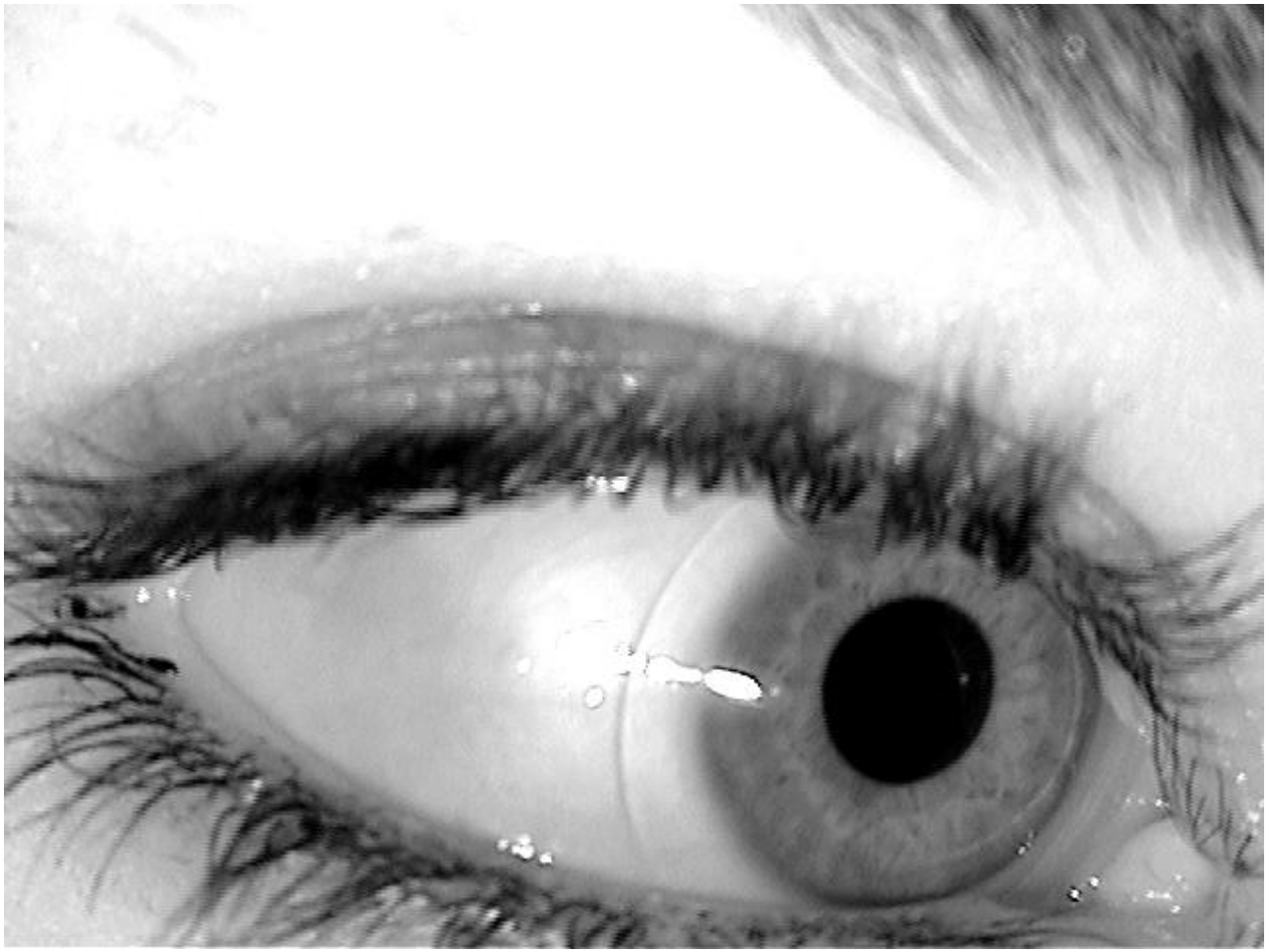
Parameters of Sarnoff IoM system
(Matey et al., *Proc IEEE*, 94, Nov. 2006)

- camera distance: 3 meters, hidden
- capture rate: 15 frames/sec
- subject walking speed: 1 meter/sec
- inter-frame travel distance: ~ 6 cm
- sensor: 2048 x 2048 pixels (Pulnix)
- resolution at subject: 0.1 mm/pixel
- (so iris diameter is about 100 pixels)
- lens focal length: 210 mm
- illumination: NIR LEDs on portal
- capture volume: 20 cm x 20 cm x 10cm (depth of field), so one or two well-focused images can be captured at a walking speed of 1 meter/sec

Fig. 6. ***Illustration of the concept of operation for the IOM system. The panels behind the subject are the sides of a commercial metal detector. The stanchions just in front of the subject support an array of NIR illuminators. The camera package is at the far right of the subject.***

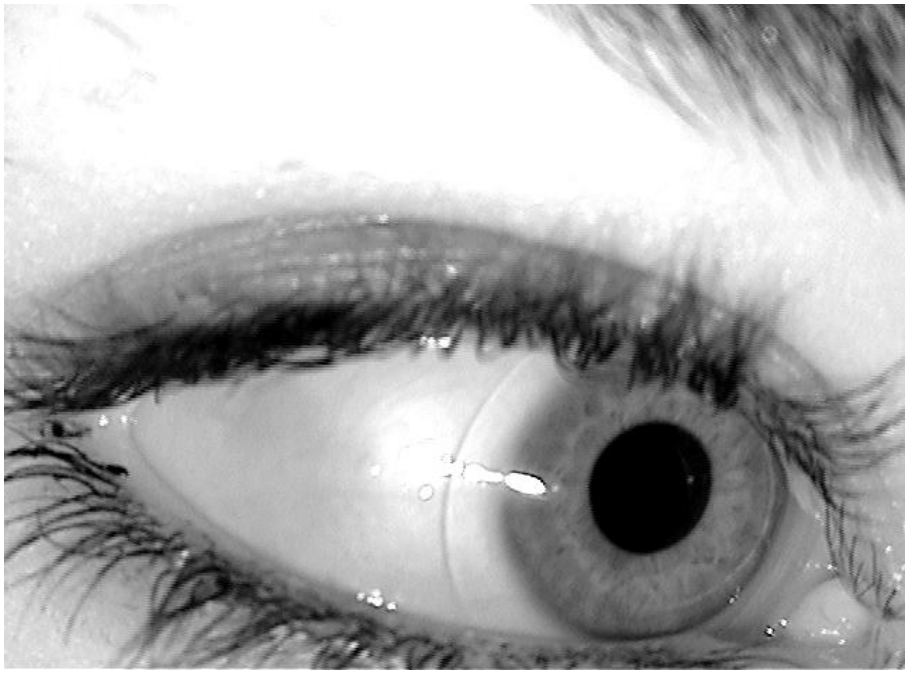
In t
lens
and
requ
leng
avai
Syst
of i
in F
volu
20 c
we
The
two

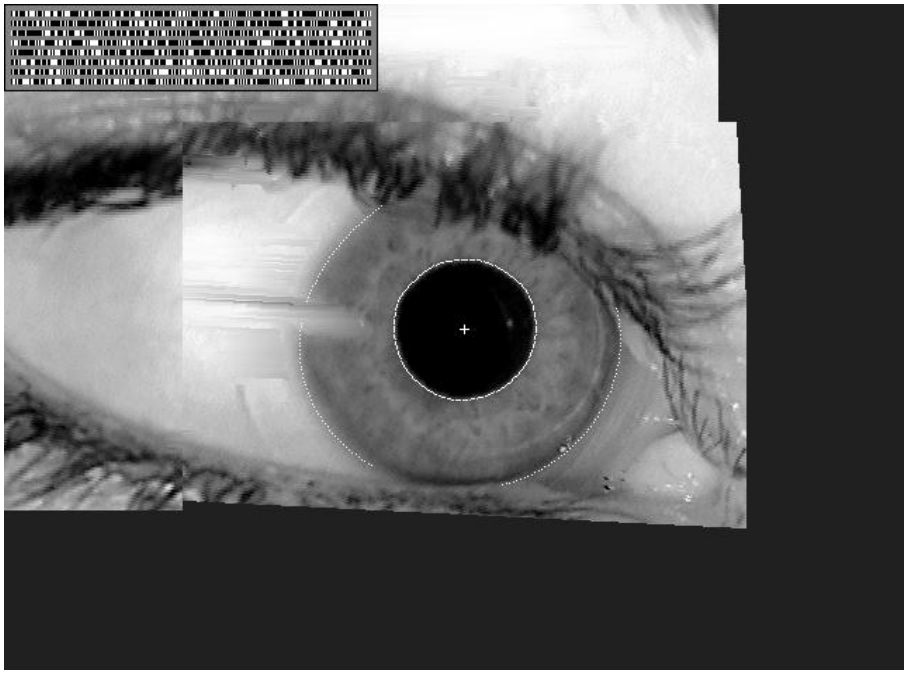
Iris images acquired off-axis…



UNIVERSITY OF
CAMBRIDGE

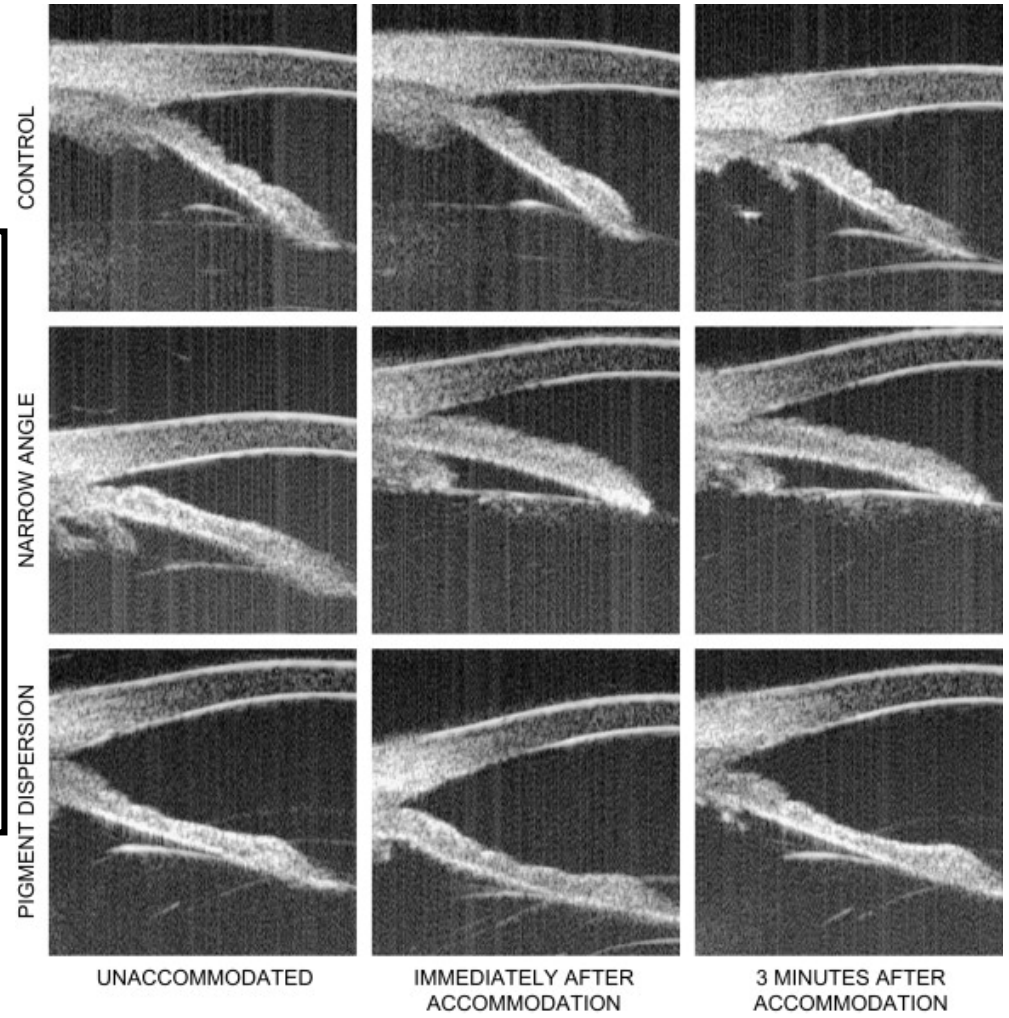
…can be “corrected” by Fourier-based trigonometry to estimate the gaze angle and make a corrective affine transformation, effectively “rotating the eye in its socket, towards the camera:”





Complication: Ultrasound images of the iris in cross-section reveal that it is not planar, and that its curvature changes with lens accommodation. Also, ultrasound reveals that it "bunches" when it dilates (non-elastic deformation).

Violations of the assumptions of "rubber-sheet" elasticity, and of planarity, limit the validity of an affine correction for the projective geometry of off-axis gaze, and of pupil dilation.



Optical axis (approximate)

Countermeasures against spoofing

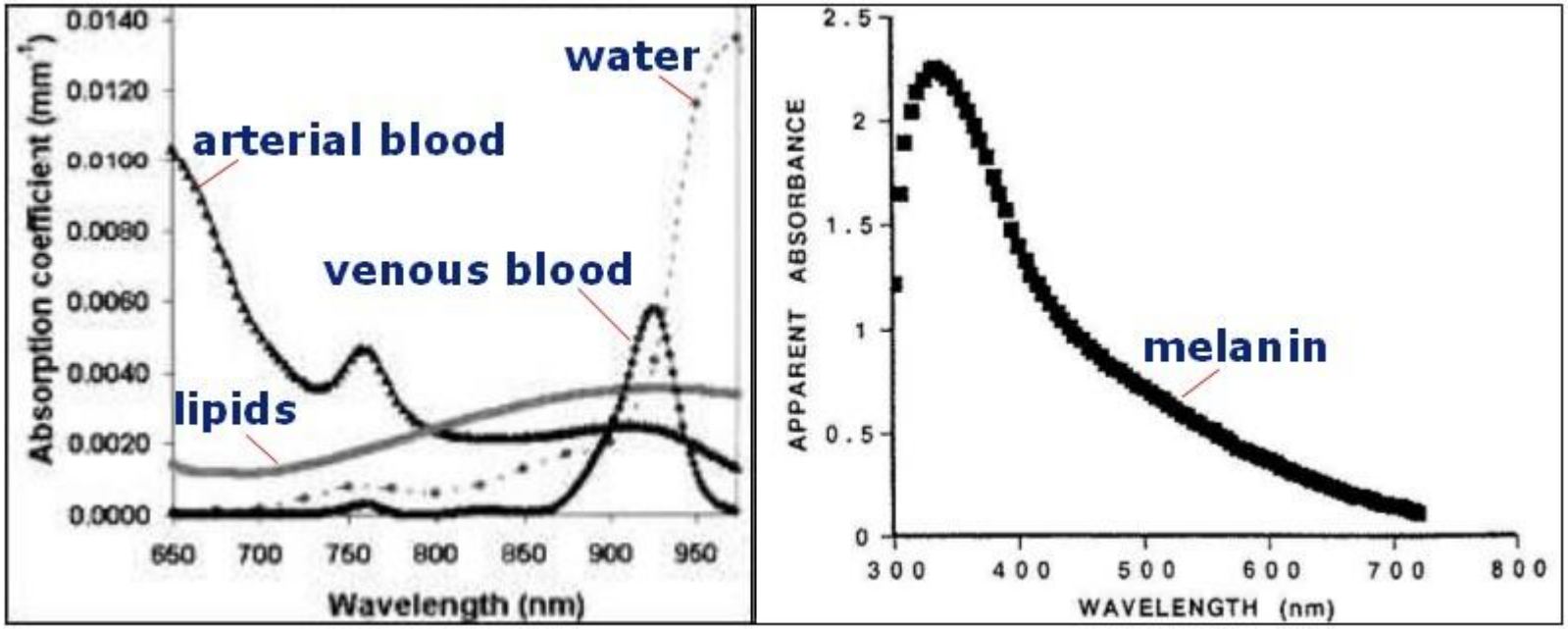
All biometrics are vulnerable to spoof attacks, either to conceal an identity, or to impersonate another.

No biometric pattern is a secret. How can iris vitality be proven?

- spectrographic and photonic countermeasures
- behavioural countermeasures
- detection of analog attacks
- permutation of IrisCode bytes to invalidate digital replay attacks

UNIVERSITY OF CAMBRIDGE

Photonic properties of living tissue (wavelength dependence of reflected light) may help distinguish a living eye from a fake artefact in a “spoofing” attack.

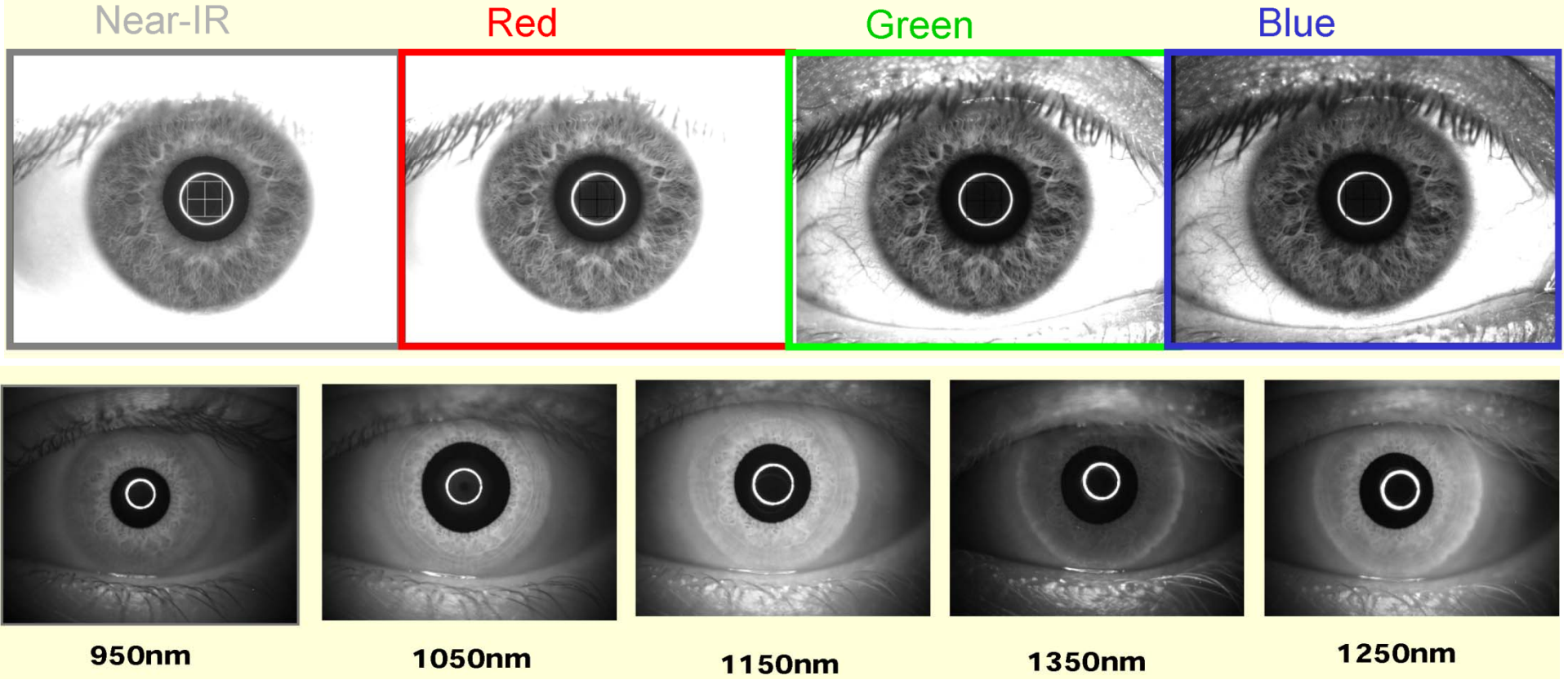


Other possibilities: pupillary light response (dilation / constriction / hippus); dynamic specular reflections from cornea; cavity optics properties (retinal back-reflection; 4 Purkinje reflections); eye blinks and movement challenges; etc.

Biophotonics as a countermeasure against spoofing with an artificial iris:

living tissue responds differently to different wavelengths of light

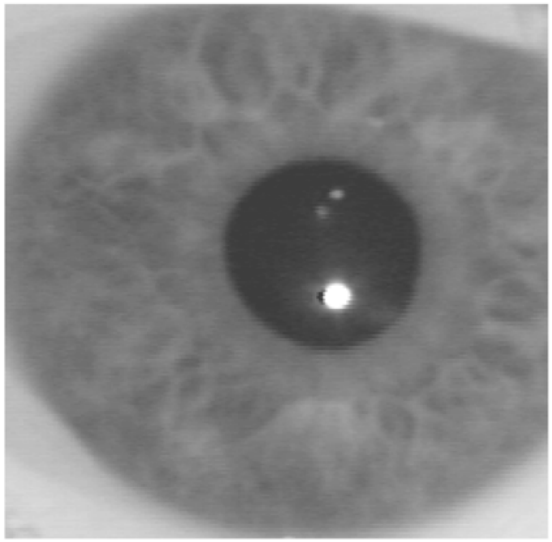
- Boyce et al, "Multispectral Iris Analysis: A Preliminary Study," CVPR Workshop on Biometrics, June 2006



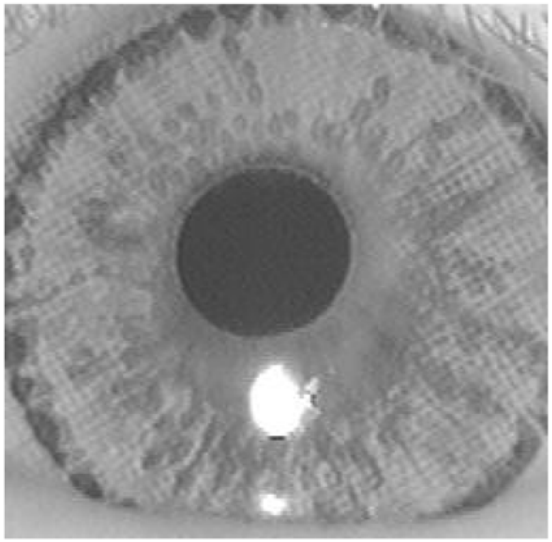
(Multispectral iris photographs from Laboratory of Arun Ross)

Detecting the presence of a printed, fake, patterned contact lens by the 2D Fourier spectrum of the printing dot matrix.

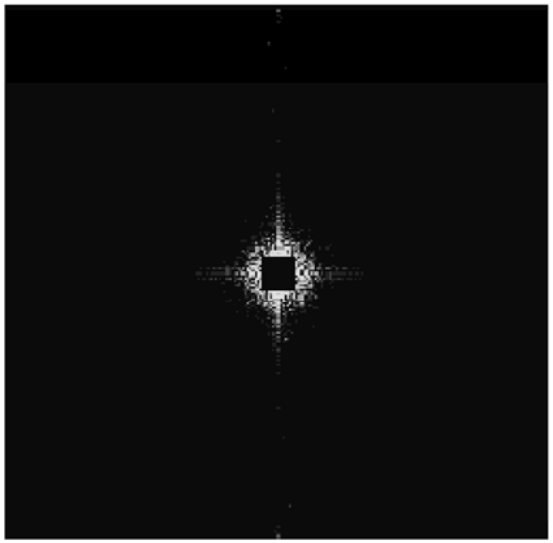
Such lenses are popular as cosmetic accessories to change one's natural eye colour.



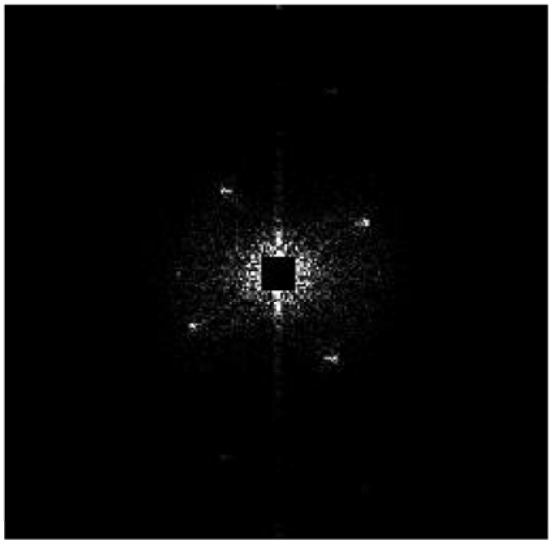
Natural iris



Fake iris printed on a contact lens



2D Fourier spectrum of natural iris



2D Fourier spectrum of fake iris

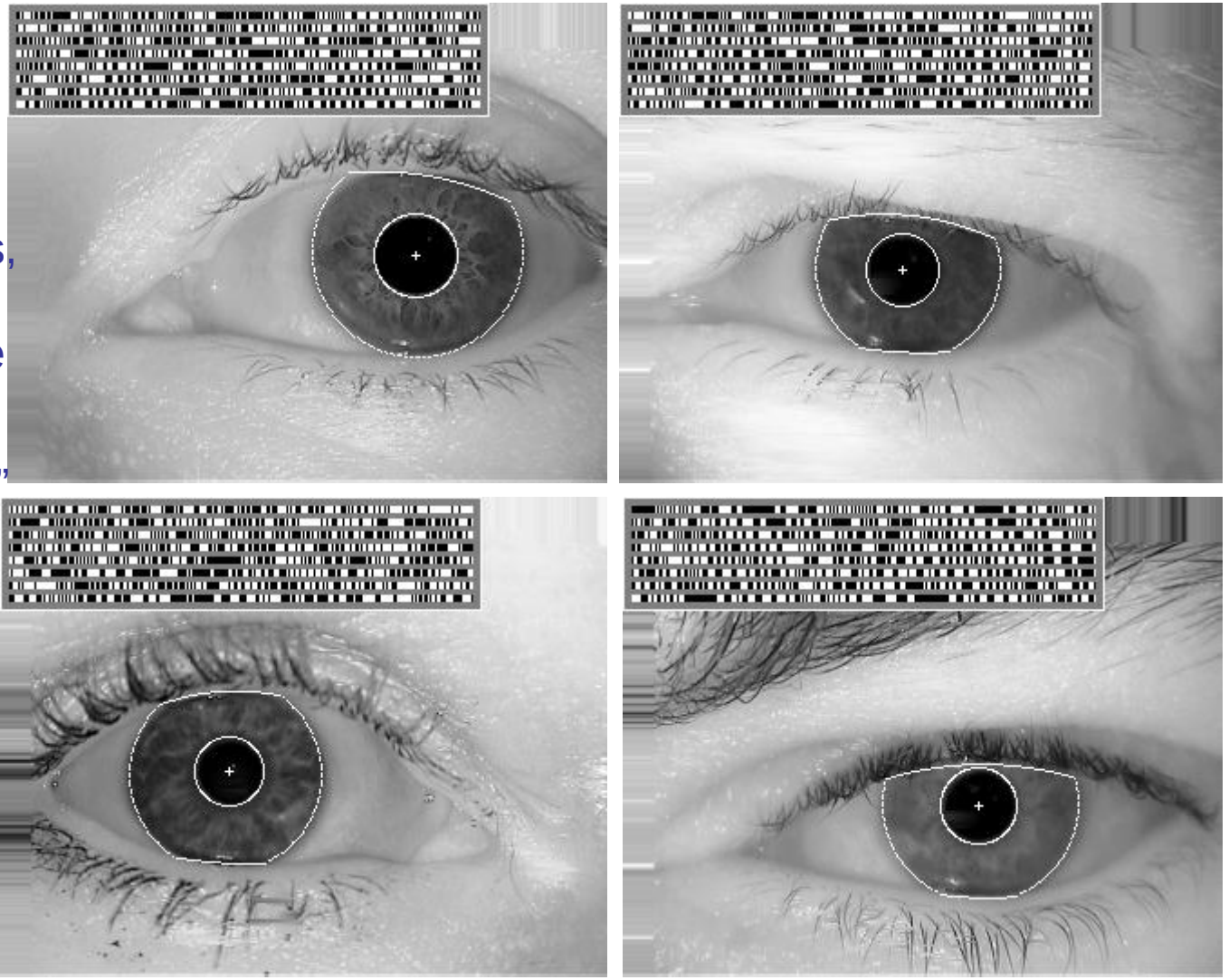
UNIVERSITY OF CAMBRIDGE

Reduced resolution and compression

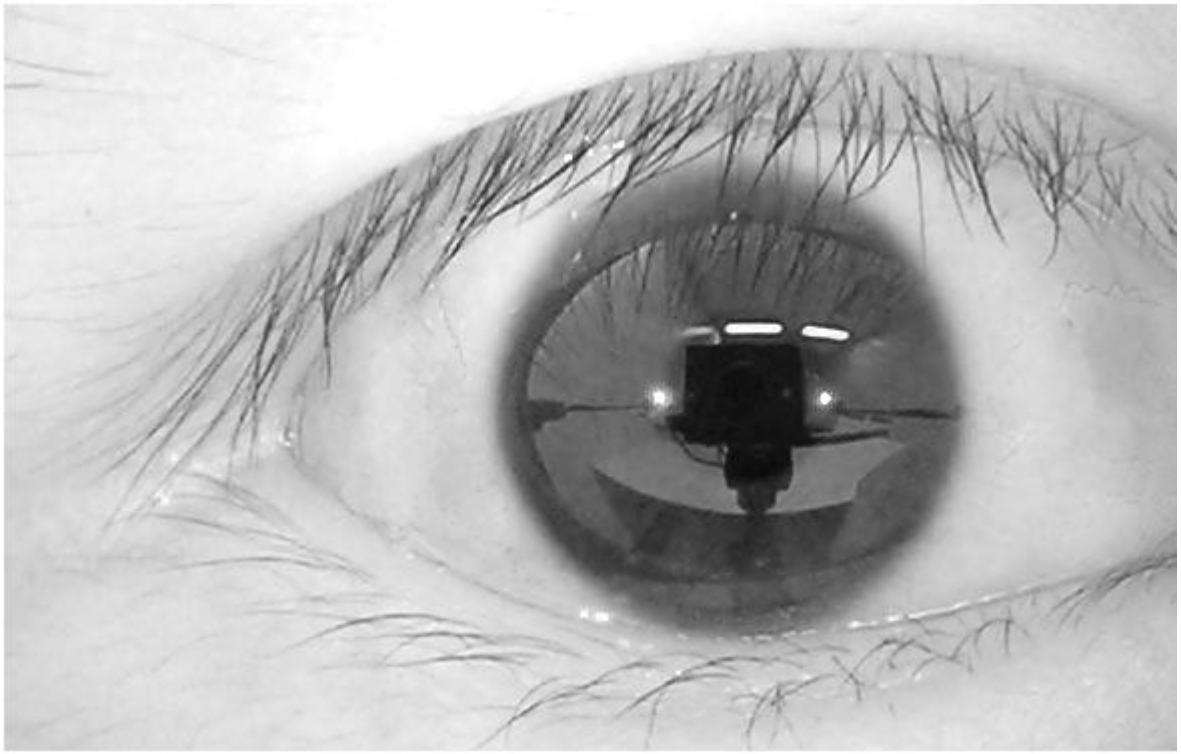
Half-size resolution in QCIF (Quarter Common Intermediate Format), in which the iris radius may typically be only 50 pixels, seems acceptable. No impact on FMR; but there is a small cost in FnMR.

Sarnoff “iris-on-the-move” and “iris-at-a-distance” acquires iris images at this resolution, and then up-samples.

How much further can reduction in resolution requirement be pushed?



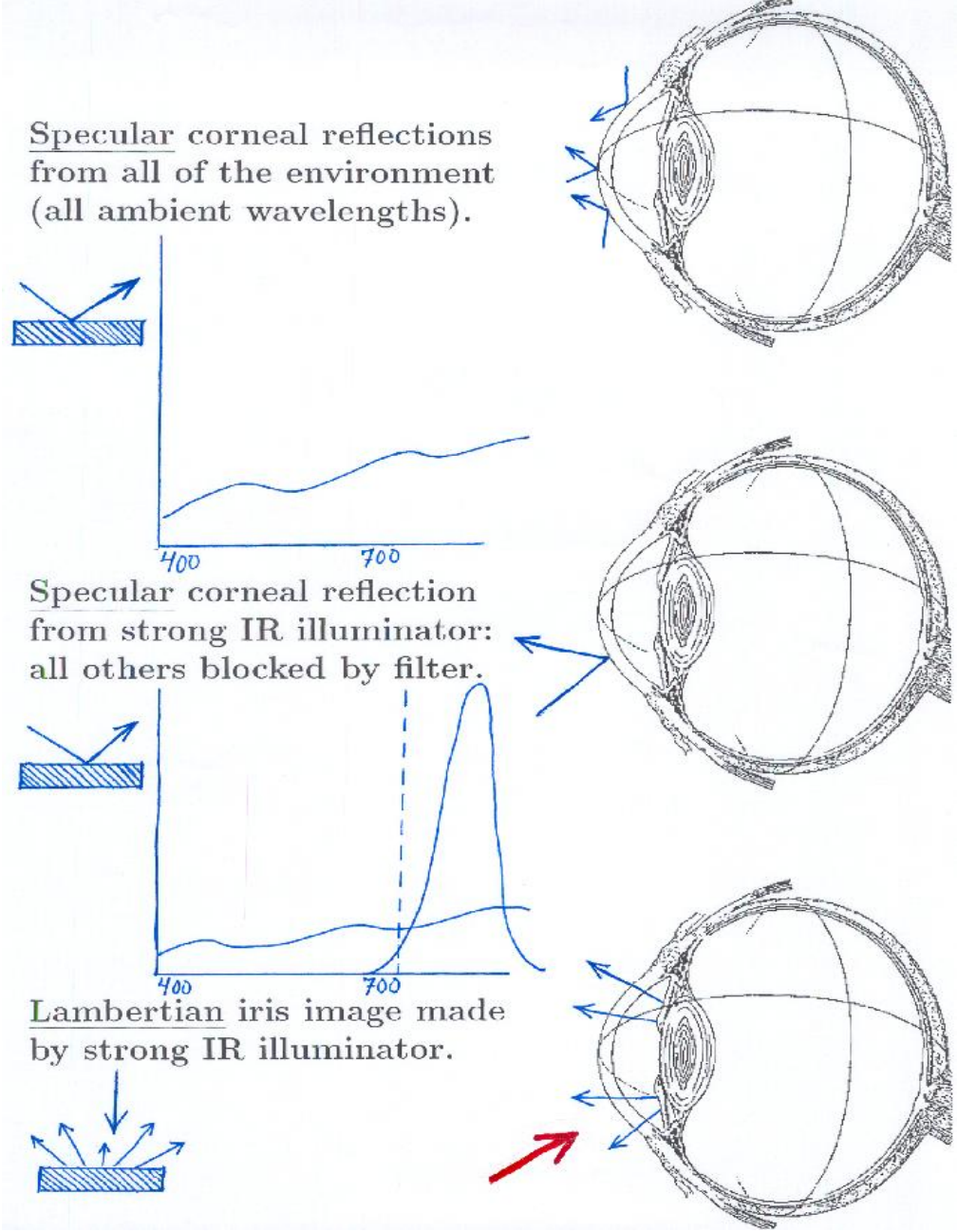
In the visible band of light in unconstrained environments (e.g. outdoors), ambient corneal reflections are common. An iris acquired in the visible band often looks like this:



All surfaces lie somewhere between specular (mirror-like) and Lambertian (scattering light equally in all directions).

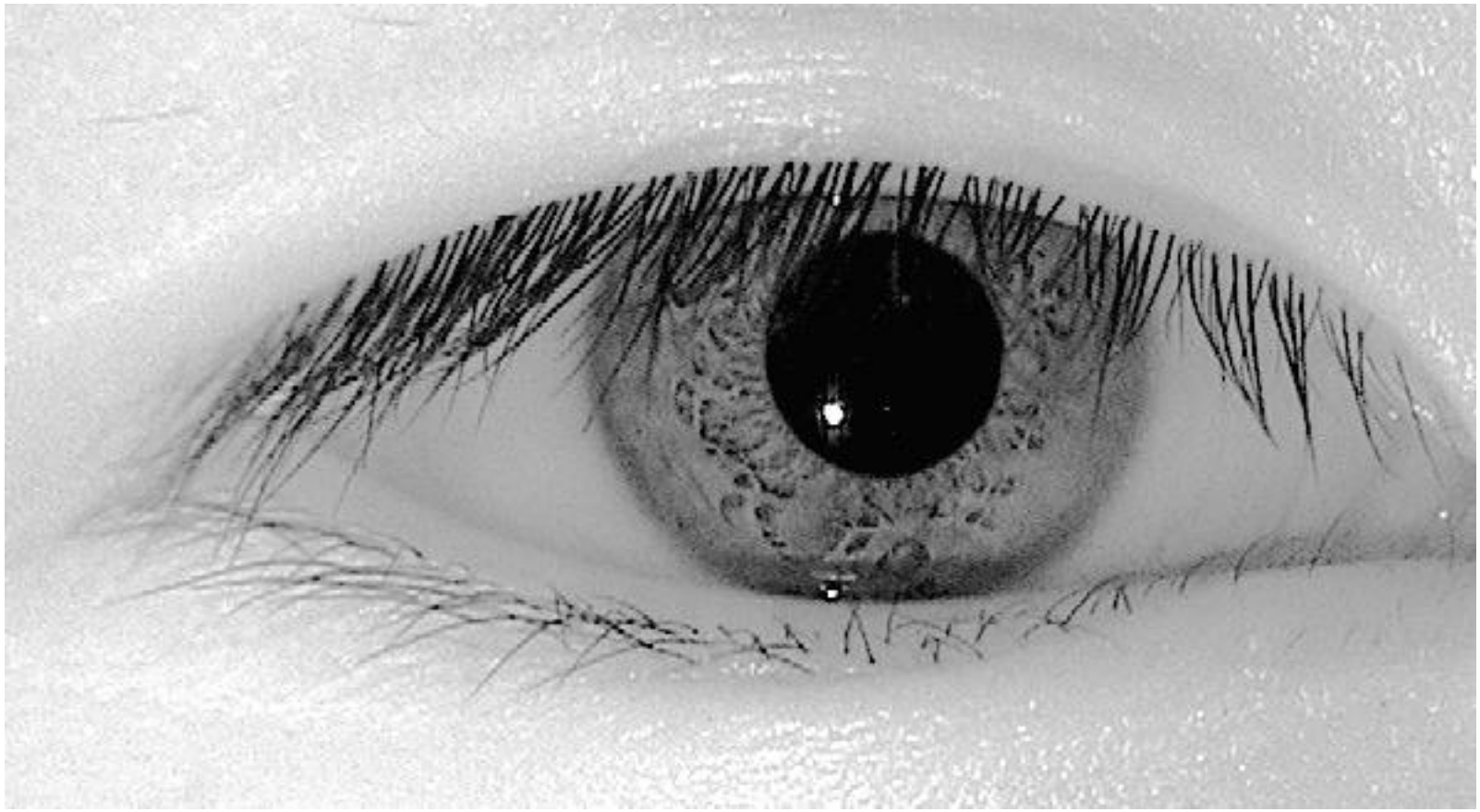
The cornea is a specular surface; the iris is Lambertian. This fact can be exploited to separate out the ambient environmental corneal reflections, which are broadband but weak, from the more narrow-band light in a nominated band projected by the camera onto the eye to obtain a Lambertian image of the iris.

By allowing back into the camera only that same nominated narrow band of light that the iris camera emitted, a band in which there is much more spectral power than in the broadband ambient corneal reflections, these two sources can be separated.

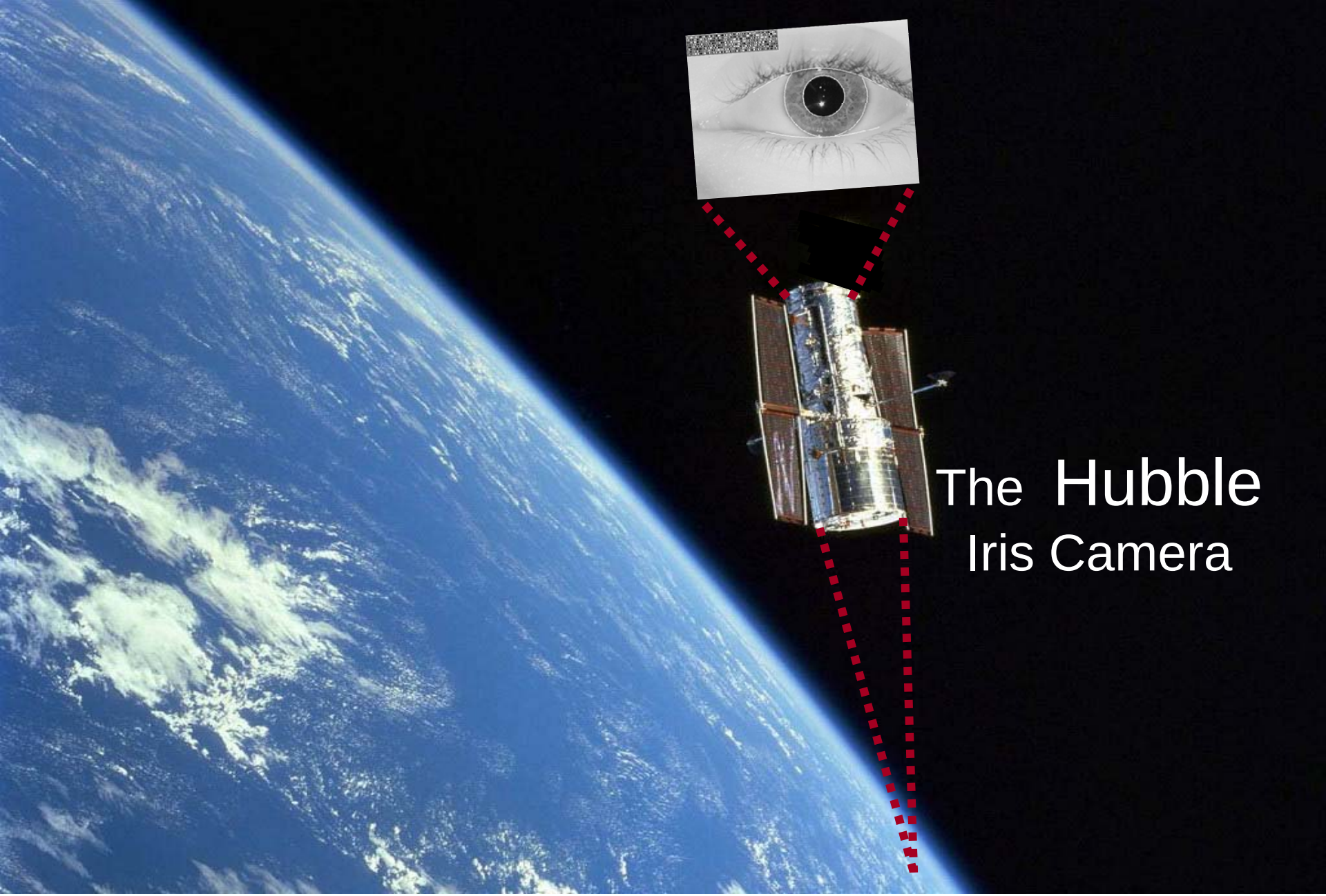


UNIVERSITY OF CAMBRIDGE

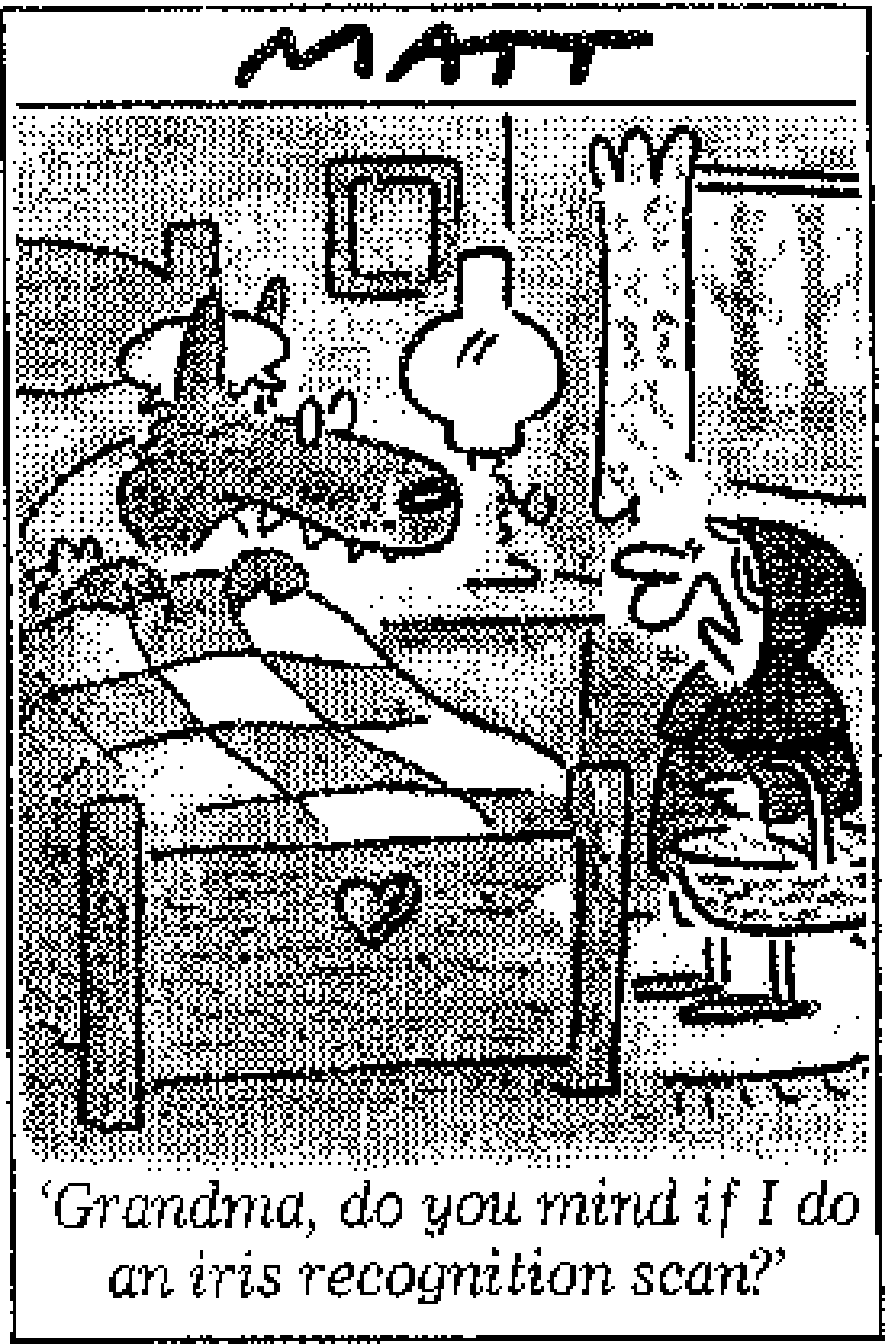
The result is an image acquired in narrowband near-infrared light, from which almost all ambient environmental corneal reflections (except for that of the illuminator) have been “scrubbed.”



UNIVERSITY OF CAMBRIDGE



UNIVERSITY OF CAMBRIDGE



'Grandma, do you mind if I do an iris recognition scan?'


Thank you
http://www.CL.cam.ac.uk/users/jgd1000/