Getting to know...John Daugman, IAPR Fellow

Biometric Entropy: Searching for Doppelgängers
(ICB 2016 IAPR Senior Biometrics Investigator Award Lecture)

John Gustav Daugman, IAPR Fellow

ICPR 2012, Tsukuba Science City

For contributions to computer vision, pattern recognition and biometrics

John Daugman received his degrees at Harvard University and then taught at Harvard before coming to Cambridge University, where he is Professor of Computer Vision and Pattern Recognition. He has held the Johann Bernoulli Chair of Mathematics and Informatics at the University of Groningen, and the Toshiba Endowed Chair at the Tokyo Institute of Technology.

His areas of research and teaching at Cambridge include computer vision, information theory, neural computing and statistical pattern recognition.

Awards for his work in science and technology include the Information Technology Award and Medal of the British Computer Society, the "Time 100" Innovators Award, and the OBE, Order of the British Empire. He has been elected to Fellowships of: the Royal Academy of Engineering; the Institute of Mathematics and its Applications; the International Association for Pattern Recognition; the British Computer Society; and the US National Academy of Inventors. He received the 2016 Senior Biometrics Investigator Award from the IAPR. He was one of three finalists for the European Inventor of the Year Award, and recently he has been inducted into the US National Inventors Hall of Fame.

Editor's note:
John Daugman is the recipient of the 2016 IAPR Senior Biometrics Investigator Award (SBIA) at ICB 2016 (see report). For this feature article, we asked Prof. Daugman to explain his award lecture for a general audience. A detailed discussion on the topic can be found in "Searching for doppelgängers: assessing the universality of the IrisCode imposters distribution" by John Daugman and Cathryn Downing and published in IET Biometrics.

The SBIA is presented at ICB in alternate years with the Young Biometrics Investigator Award (YBIA). Please see the Call for Nominations for the 2017 YBIA.
~ Arjan Kuijper, Editor-in-Chief

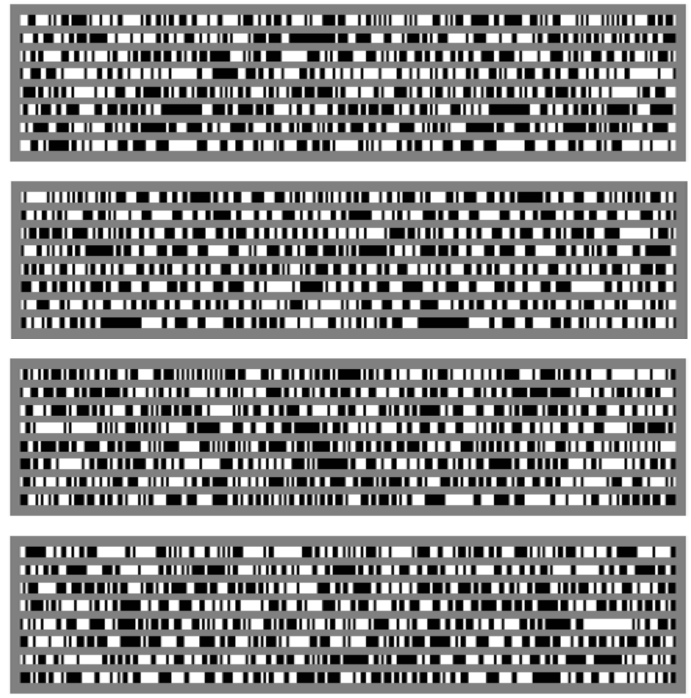
by John Daugman, Professor of Computer Vision and Pattern Recognition, University of Cambridge

The science of pattern recognition has deep roots in ancient philosophical concepts of the universal and the particular. In order to classify a thing as belonging to a class of objects, such as faces or bicycles, one must learn and detect the generic properties that should be universally possessed by members of such classes. But in order to discriminate among members of any such class and detect a particular one (Anna's face; my bicycle), one must learn and detect the features specifically unique to such instances. These two fundamental notions relate broadly to Plato's concept of "ideal forms" (of which any particular instance is just a transient projection), and to Aristotle's concept that the essence of a particular thing is "that which makes it different from everything else".

The tasks of face recognition begin, of course, with detecting faces generically (e.g. the Viola-Jones algorithm), then identifying a particular face (e.g. with Google FaceNet), perhaps with invariance across facial expressions; or perhaps the converse task of detecting and classifying facial expressions with invariance to person identity. Face identification is plagued by the “Doppelgänger problem”: there is not sufficient entropy (or statistical variation) among different faces to support large-scale database searches without drowning in false matches. Gold standard verification performance targets a false match rate (FMR) of one in 1,000 (depending on database difficulty). But in analogy with the “birthday problem”, (namely, that once 23 or more persons are randomly assembled it becomes more likely than not that at least one pair of them share a birthday), we have a collision problem here. At the benchmark FMR = 0.001 for single comparisons between different faces, then once a facial database is only as large as 38 persons, it becomes more likely than not that at least one pair of them would be falsely matched to each other (since 0.999 raised to the power 38x37/2, the number of possible pairings, is less than one-half). Facial Doppelgängers abound.

Information Theory teaches that avoiding accidental collisions (false matches) in database searches depends on using features with sufficiently high entropy (random variation) to ensure uniqueness. This is for exactly the same reason that cryptographic keys with higher entropy are stronger. Many years ago, I invented automatic iris recognition, identifying persons by the random patterns visible in the iris of an eye from some distance. My algorithms remain the basis of all public deployments of this technology worldwide, and the Government of India has now nearly finished enrolling all 1.2 billion citizens’ iris patterns (together with fingerprints) in a national ID and welfare entitlements distribution system. The principle behind these algorithms is that you are recognised because you failed a test of statistical independence against a template enrolled previously for yourself. This is an extremely powerful basis for pattern recognition, when there is sufficiently high entropy across different templates that the probability of chance collisions among different templates is minuscule. Each new enrolee in the Indian scheme is compared against all existing enrolees, for de-duplication checks. The portrayals here of actual IrisCodes (bit sequences that encode the phase structure of iris patterns) illustrate by their obvious entropy why false matches are avoided, despite such vast numbers of opportunities to make false matches. This is why there are no iris Doppelgängers.

Since the phase bits are equally likely to be 1 or 0, and thus any given bit from two different eyes’



IrisCodes are equally likely to agree or disagree, the distribution of such similarity scores (Hamming distances) whenever different eyes are compared is almost universal and invariant. It is remarkably narrow, and it corresponds to the distribution you would get from tossing a fair coin about 250 times in a row and tallying up the fraction of “heads” obtained: it is exceptionally rare to deviate much from a 50/50 fraction. We performed 100 billion comparisons between IrisCodes from different eye pairings, generating 316,250 different distributions (each for one eye against all of the others). Their standard deviations rarely differed by more than 2 percent. Thus, we have here the exceptional situation in pattern recognition that whenever different things are compared, their similarity scores are always drawn from the same, narrow, universal distribution! This is one reason why large biometric entropy is the key to avoiding false matches in huge, national-scale identifications.

The bit-sequence encoding also lends itself to extremely fast search, because IrisCode matching only requires a bit-parallel Exclusive-OR, on as many bits at once as the word-length of the machine. This allows millions of IrisCodes to be compared per second per single-core CPU. Prior image processing steps (segmentation of the visible iris at its boundaries, detecting occlusions, and normalising the iris texture into a dimensionless, pseudo-polar mapping) are executed as fast as the video frame-rate. The actual encoding of the bit stream resembles what is now called a convolutional neural network; but some readers of this newsletter may rejoice that it has nothing to do with “Deep Learning”!