BioSocieties (2008), **3**, 81–86 © London School of Economics and Political Science
doi:10.1017/S1745855208005966

Interview

Pattern Recognition: Biometrics, Identity and the State—An Interview with John Daugman

Mathew Kabatoff*
BIOS Centre, London School of Economics and Political Science, Houghton Street, London WC2A 2AE, UK
E-mail: m.a.kabatoff@lse.ac.uk

John Daugman
University of Cambridge, Computer Laboratory, William Gates Building, 15 JJ Thomson Avenue, Cambridge CB3 0FD, UK

John Daugman is the inventor of the 'IrisCode', the *de facto* iris recognition algorithm used in all publicly deployed iris recognition systems worldwide. Iris recognition is used in two main ways today: the determination of a person's identity by searching a database of enrolled iris patterns, for example to obviate passport presentation; and watch-list screening where a security database of 'undesired' identities is registered. In both modes of use, the technology needs to be very robust against making false matches, since a large database provides many opportunities for a false match during an exhaustive search through it. In both modes of operation, the user does not assert any identity (although some weaker biometrics are used in single-comparison, assertion-verification mode). The output from the identification mode of operation is the person's name if they are enrolled; the output from the watch-list mode of operation is a statement of whether or not the person matches any watch-list identity.

The advantage of iris recognition in performing both of these tasks is its robustness in comparison to other biometrics such as face or fingerprint recognition, or, for that matter, traditional identity tokens such as paper passports. Iris recognition is increasingly being used

Mathew Kabatoff is a PhD candidate in the BIOS Centre at the London School of Economics and Political Science. His doctoral research concerns the relationship between identity, security and risk within post-9/11 border security and immigration practices within the US and EU.

John Daugman received his AB and PhD degrees at Harvard University and then taught at Harvard before coming to Cambridge University (UK). He has held the Johann Bernoulli Chair of Mathematics and Informatics at the University of Groningen (NL), and the Toshiba Endowed Chair at the Tokyo Institute of Technology, Japan. His areas of research and teaching at Cambridge include computer vision, information theory, statistical pattern recognition, and neural computing. Daugman is the inventor of iris recognition and his algorithms currently underlie all public deployments of this technology worldwide. Some 60 million persons have been enrolled by these algorithms, which are today owned by L-1 Identity Solutions. Daugman works with L-1 as Chief Scientist for Iris Recognition, while remaining based at Cambridge. Awards for his scientific and technical work include the US Presidential Young Investigator Award, the Information Technology Award and Medal of the British Computer Society, the 'Millennium Product' Award of the UK Design Council, the 'Time 100' Innovators Award, and the OBE, Order of the British Empire.

*Corresponding author.

in border-crossing applications. In the UK's Iris Recognition Immigration System (IRIS) Project, for instance, it is used as a substitute for passport identification. In the United Arab Emirates it is used to screen all individuals who require a visa to enter the country against a watch-list—10 billion real-time comparisons are performed at this border crossing each day.[1] To date, 60 million individuals have had their irises enrolled in iris recognition systems throughout the world.

However, in a post-9/11 Anglo-American context, biometric technology has been regarded as a key security tool of the state. In the US, the argument has focused on its use in the fight against terrorism; in the UK, the stress has been on its role as technology to mitigate a number of social problems such as identity theft, terror, organized crime and benefit fraud. The science of biometrics has thus entered into the socio-political arena, where the debate over the use and efficacy of the technology has focused on the apparent tension between the imperative for state security and the individual right to privacy and liberty. In the US, this debate has been most intense in relation to the border security programme US-VISIT, and in the UK it has come to a head over the proposed scheme to introduce biometric identity cards.

The following interview considers the science behind iris recognition and how it has radically altered how identity is understood, and it explores Daugman's views on the use of iris recognition and biometrics within the context of state security and identification.

Mathew Kabatoff: Can you explain how iris recognition works? How can it claim to be so statistically accurate in its ability to distinguish between millions of unique individuals? If I were a twin, or a clone for that matter, why won't my irises match those of my twin or my clone?

John Daugman: Automatic identification of persons by iris recognition is based on the existence of a great deal of random variation amongst different persons in the detailed patterns that are visible in the iris of the eye. Iris patterns are very complex, and the combination of complexity with randomness across a population confers mathematical uniqueness to a given iris pattern. Mathematical algorithms—such as the ones I developed for the 'IrisCode', which is used in all current public deployments of iris recognition—extract that random pattern into a compact digital signature that can serve as a robust biological identifier. The pattern is inseparable from a person yet can be captured without contact, using a special camera at a distance that may be up to several metres but is more commonly within arm's length, as used for example in airports today in lieu of passport presentation. The cameras also need to confirm that a real live iris pattern is being imaged, and not just (for example) a photograph or a printed contact lens, by tests such as detecting the stretching of the iris pattern as the pupil changes in size, among others.

The two eyes of one person have independent and uncorrelated iris patterns, as do the four eyes of monozygotic twins, because the detailed iris patterns (unlike colour) are epigenetic: they develop during gestation without genetic specification. Because the patterns are epigenetic, we can expect that when human clones arrive, the $2N$ eyes possessed by N common clones will also be as different and independent as are the four (genetically identical)

1 Each time a new iris biometric is matched at the UAE border an $N \times N$ (all-against-all) comparison is performed on the iris database to determine if the individual appears on the UAE's watch-list. The watch-list itself has a population of approximately 365,000 iris templates. This matching process is only performed on foreign nationals who require a visa to enter the UAE.

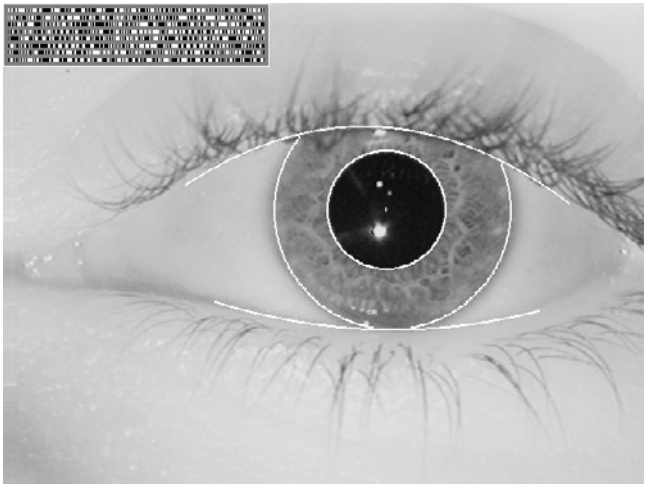

Figure 1. An iris with its 'IrisCode' (and localization graphics)
Photo: Courtesy of John Daugman

eyes of monozygotic twins, or the two (genetically identical) eyes possessed by any one person—as readers may confirm by close inspection in a mirror.

Mathematically, iris recognition works by the failure of a test of statistical independence. You are (statistically) guaranteed to *pass* a test of independence when one of your iris patterns is compared with that from any other eye (independence here meaning that the patterns *will not* match) but you will *fail* that test of independence when images of your eye are compared with itself (that is to say, the patterns *will* match, so they will not be independent). The confidence level associated with inferring your identity from your failure of that test of statistical independence is dictated by the huge number of 'degrees of freedom' in iris patterns—a measure of the amount of random variation that exists in a population, just as entropy is a measure of randomness.

But the fact that iris patterns appear to be stable throughout life (at least as far as all existing data indicates), means that the random variation is all 'between-class' but not 'within-class'. The entire science of pattern recognition depends on the between-class variation being larger than the within-class variation; in other words, that the spacings between the classes are larger than the diameters of the classes. That is what is achieved by iris patterns having so much complexity and randomness: it means that 'collisions' between iris patterns from different eyes are statistically extremely improbable, even astronomically improbable when a demanding threshold is imposed. Therein arises the identification power of iris recognition: not making false matches.

Mathew Kabatoff: What significant improvement does biometric technology bring to the identification of an individual, when compared with the traditional passport token, especially where the individual is interfacing with the state?

John Daugman: Obviously object tokens such as passports, and secrets such as passwords, are not tightly bound to an individual. They may be transferred, lost, stolen, hacked or obtained by other fraudulent means. I guess that using tokens or secrets for human identification is as old as priestly amulets or military passwords of Roman centurions. Biometrics escalates the technology by basing identification decisions on features that are more inseparable from a person, and more unique to a particular person.

Mathew Kabatoff: A recent round of criticism against the use of fingerprint biometrics in large-scale government applications argues that if they are stolen an assailant will have access to an individual's 'raw biometric', and that this 'raw biometric' can be used to commit identity fraud. Is this vulnerability present with all biometrics, or only with the fingerprint?

John Daugman: All biometrics are vulnerable to spoofing by artificial means, and it is a mistake to regard any biometric pattern as a secret. A person's facial appearance is certainly not a secret; an iris pattern is visible even in a high-resolution facial photograph; and people leave their fingerprints on everything they touch. Any biometric technology must be able to confirm the vitality of the presenting pattern. The engineering term of art in this field is 'countermeasures against subterfuge'. But this game is a kind of a Cold War game: for every anti-ballistic missile designed, there is an anti-anti-ballistic missile on the drawing board . . .

Mathew Kabatoff: What significant advantage does iris recognition have over fingerprint biometrics? What new possibilities for identification, matching and screening are made possible if authorities have the ability not only to 'verify' an individual's identity, but to perform 'identification' against a watch-list?

John Daugman: The main advantage is that iris is much more robust against making false matches, because the randomness of iris patterns is greater than that of fingerprints, partly because it spans many scales of analysis or spatial frequency ranges, whereas fingerprint patterns are all defined by a 0.5mm ridge flow field and only about 20 or 30 minutiae. Another big difference of course is that iris recognition is non-contact, acquired at some distance, whereas fingerprint requires contact. This confers a forensic advantage for fingerprints—people generally do not leave their iris patterns behind at crime scenes—but I gather that some persons consider the non-contact nature of iris recognition an advantage in terms of user acceptability. But most people find it easier to present a good fingerprint than a good iris image, so there is a problem with 'failure-to-acquire' rates in iris recognition, and a failure-to-acquire means a failure to match. Some people also have difficulties with fingerprint readers. But an advantage for fingerprints is that the average person has five times more fingers than eyes.

The great advantage conferred by the high level of randomness within iris patterns is that it provides enough uniqueness that systems operate in identification mode, not mere verification mode. A verification biometric is one in which a user must assert their identity in some way, and then a mere one-to-one test is done on that asserted identity. But with an identification biometric like iris recognition, the user is not even asked to assert an identity: instead identity is determined by an exhaustive search of the enrolled database (if the person is enrolled). This is how, for example, all major UK airports currently deploy their IRIS systems.

There is no request for a passport presentation, or any other explicit assertion of identity: you just look at the camera, and if you are recognized the gate opens and your immigration formalities are over. To operate in this mode is far more demanding for algorithms and requires far greater robustness than operating in mere verification mode, since the technology must survive vast numbers of opportunities to make false matches during the database search process, without actually making any.

Mathew Kabatoff: In the past you have stated that registered traveller programmes that rely on biometrics can be seen as a social good acting both as a form of security and as a convenience. You have also suggested that biometrics when used strictly for the purposes of watch-list screening can be viewed as a punitive use of the technology. Do you feel this distinction still holds? At the heart of my question is your view on the distinctions between the use of biometrics such as IRIS as part of a registered traveller programme as a convenience, and their use for the purpose of watch-list screening and as a population control.

John Daugman: If one makes a contrast between the interest of the state and the interest of the individual, one could say that the benefit of a Frequent-Flyer programme like IRIS redounds primarily to the individual (except for some savings in efficiency for the state since less manpower is required at border crossings for passport inspection), whereas the benefit of a watch-list screening application like the United Arab Emirates redounds primarily to the state, by empowering and enforcing policy.

But under the 'General Will' theory (Rousseau's formulation of the Social Contract), citizens collectively benefit from the existence of police forces, border controls and other arms of the state; so this contrast of interests is something of a false dichotomy. User attitudes to watch-list deployments are also fickle and a bit paradoxical: passengers may resent the biometric check against a watch-list of suspected terrorists when passing immigration controls to enter a country, but they seem to appreciate knowing that their fellow passengers are similarly screened when being allowed to board the same aircraft as them.

Mathew Kabatoff: The use of biometrics for security applications has led to a number of objections from privacy advocates who argue that the collection of biometrics—for such things as an identity card scheme or border security programme—is an invasion of an individual's privacy since it requires an unwarranted amount of personal information to be handed over to the state, and creates new regimes of surveillance that have the potential to curtail an individual's freedom or liberty. Do you agree with this argument? Do you feel that there is a right to privacy that should be maintained? What balance should be struck between the individual and the state in respect to security and privacy?

John Daugman: I think it is important to distinguish between a right to privacy—which I guess is interpreted roughly as a 'right to be left alone'—and a putative right to anonymity. These two assertions have often been confused and used interchangeably in the public debate. It seems to me that the *quid pro quo* between rights and responsibilities as envisioned by Social Contract theory can only be applied if the identity of an individual can be determined with certainty. If not, then how are rights and duties exchanged, or contracts enforced? How could the state ever guarantee a contract between citizens, or comply with or enforce a contract between itself and a citizen, if identity can remain fluid or indeterminate?

It is important to note that among Enlightenment-era formulators of the theory of the liberal state, I am aware of only one who actually proposed and advocated a 'right to anonymity'. That was the (Swiss-born) French liberal thinker Benjamin Constant (1767–1830), who advocated this idea in his *Principes de politique*. His theory of the minimal state seemed to have promoted this 'value of obscurity' as a reaction against Bentham, who advocated the full identification of all members of society (as embodied in his famous proposal of 1791 for a 'Panopticon'). I find it interesting that with the (relatively late) exception of Benjamin Constant, the idea of anonymity appears not to have been regarded as an important expectation of the individual within the theory of the liberal state.

I think that a classical utilitarian calculus can be used to decide under what conditions 'the greatest good for the greatest number' is served by mandatory strong identification—e.g. when boarding an aircraft—versus benign situations in which the common good is not enhanced by demanding the surrender of anonymity. The arguments are not unlike those relating to the Social Contract in the formulations by Enlightenment philosophers such as Hobbes, Locke, Bentham and Rousseau: the benefits gained by submitting to 'the general Will' and thereby avoiding life in the state of nature generally justify the price paid in liberties surrendered. The argument about a right to anonymity is not unlike the argument about taxation: extreme 'all or none' theories of either are doomed, and the sensible positions are in the middle. The question is really just about 'how much' of either thing we need: perhaps the good liberal state lets you keep about 70 percent of your income after taxation and lets you remain anonymous in about 70 percent of your transactions with the state or its services. But it would be perverse to argue that any public good, or social good, or political good, is served by continuing to use the conventional unreliable (non-biometric) means of identification in those circumstances where the greatest good really is served by requiring strong identification.

Mathew Kabatoff: These balances are hard to strike in any liberal state! Thank you, Dr Daugman, for this very clear account of the technological and social issues raised by this emerging technology.