Nucleic acid identity

Andrew D. Ellington
Center for Systems and Synthetic Biology
University of Texas at Austin

As has been shown in the mature field of biometrics, the concept of personal identity is intimately related to biological variables. It can be argued that while personal traits are the result of both nature and nurture, the vast amount of personal information available via DNA is one of the easiest to consider as a metric for determining identity. A person is their sequence.

Ultimately, the question of generating a means of routinely typing personal genomic DNA becomes the question of how to interface DNA with electronics. This is an extremely interesting problem whose basic solution is already extant via any of a variety of electrochemical methods. In its most basic implementation, a given DNA strand hybridizes to its complement on an electrode, yielding a change in electrochemical properties that are sensitively ready out by the electrode.

It is within the realm of possibility that a device could be created to routinely extract DNA from the constantly shed skin cells of an individual, and then electronically compare that DNA with either an individual key, or with a series of probes that would yield a pattern that was the equivalent of a key. However, it is also likely that such a device would require DNA amplification, and this would make the solution far more futuristic. There are many, extremely robust means to amplify even a single DNA molecule, but even in their best MEMS formats they require reagent streams that would have to be maintained over time, making the implementation of routine DNA biometrics difficult. Imagine that a small fluidic chip had to be inserted on a regular basis into your cell phone in order to key that phone to your personal DNA. Depending on the replacement time (likely a few months) such a solution might be palatable to some users, especially in secure communities, but would nonetheless be as fraught with 'bugs' as some versions of Windows.

Thus, while NextGen sequencing data is approaching the point that it will soon be commonplace for individuals to know their own genomes, the routine, high-throughput verification of identity as envisioned in the movie GATTACA will likely remain futuristic for decades to come. Advances in sequencing or other DNA analysis technologies are not likely to become as routine as typing in a password or digitally analyzing a photograph.

Thus, the question becomes whether there can be a surrogate for your whole genomic DNA sequence that could be used to validate identity. One answer to this question is of course to only look at those regions of the genome, such as repetitive sequence polymorphisms, that are highly variable between individuals. This is the approach that is typically taken in medical and legal forensic analyses. Still, such analyses again almost always require amplification and reagents, again ruling out using partial patterns as surrogates for the whole.

The solution we envision is to use DNA taggants as surrogates for natural DNA. DNA taggants would be mixtures of oligonucleotide sequences that would be

assigned to an individual, and that could be delivered to electronic devices either as a liquid key held by the individual, or applied as a long-lasting coating to the thumb or other skin surface. The taggant mixture could either directly reflect the polymorphisms in an individual's own genome, or could be random (but known by some key-holder) sequences that served to uniquely represent the individual.

The obvious disadvantage to this obvious technology is that the key could be readily transferred between individuals, either illicitly or by the simple expedient of shaking hands. However, these flaws can also be viewed as advantages: first, a taggant salve could be like an ID badge, given to an individual for a specified period of time, renewed as necessary. Second, it is highly unlikely that a single metric would be used for identification, and lack of correlation between other biometrics and a taggant would be a useful indicator of fraud or deception. Third, it has previously been proposed that the transfer of taggants between individuals is an extremely useful tool for plumbing networks of human interactions. Just as our electronic presence can be viewed as an amalgam of social networking interactions, our DNA visage could be seen as an amalgam of who we brush off on. And, as with confirmatory biometrics, if an untoward interaction between individuals who should otherwise be separated in a secure environment was detected, this would be a useful indicator of potential security breaches.

The technical implementation of DNA taggant technology would present a number of challenges. First, since the DNA key would be a physical entity, it could presumably be stolen, decoded, and replicated. These possibilities can be rendered virtually moot by a variety of simple expedients, including the use of unnatural nucleotides that are easy to employ as keys but exquisitely difficult to decode, and creating programmable nucleic acid circuitry that would be responsive only to particular combinations and concentrations of individual taggants in the mixture. This latter approach is especially interesting, in that the DNA (not electronic) circuits could be programmed to work in series, such that each new application of a taggant mixture would be activated by the previous one, and in the absence of a correct series of codes no one could would be active or useful. The design and implementation of such a keyed series will be discussed.