The Open Biometrics Initiative

The Open Biometrics Initiative challenges hard and fast classification of biometric data. It cracks open the clean fabrication of automated biometric identification. The first version[1] of the Open Biometrics Initiative[2] is dedicated to finger print analysis. A custom designed machine calculates and prints the same data that law enforcement agencies use to check one's identity. Instead of matching the data to a database of criminals, this machine calculates an unfiltered set of characteristic points as a probabilistic IDcard, defying reductionist classification.

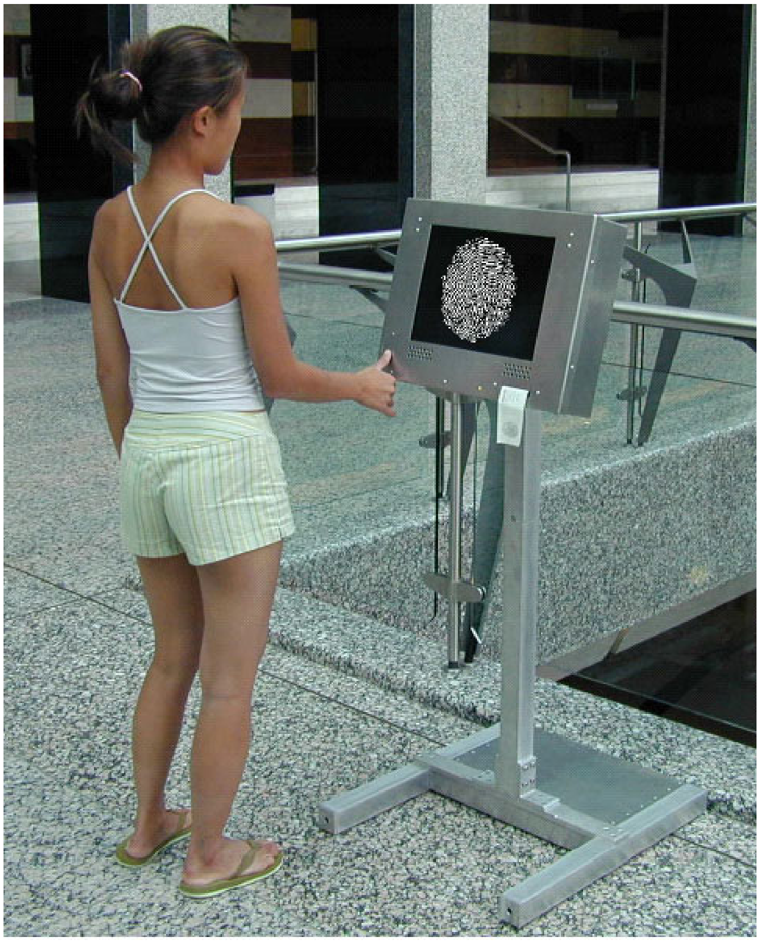


Fig. 1: The machine

[1] "Decontamination, Surveillance and Ready Made Martial Law in the Anthrax Age *International Symposium on Electronic Arts, ISEA2002*, Kanayama, Naka-ku, Nagoya, Japan

[2] Thanks to contributions from first and foremost, Dr. Dsp, also Nicolas Canaple, Eric Crahen, and JTRinker.

Challenging biometric decision landscapes

There have been many attempts to find technical solutions to classifying human beings based on body metrics. At least since Lavater, body metrics is a contested field of character validation. Indeed, critique of body, or more generally biometrics, can occur on a number of levels. While there is much circumstantial evidence, for example, that every human being has a distinct set of fingerprints this has never been statistically proven over all populations and peoples.

The computerized automation of biometric validation is an even trickier issue. It is one thing to solve an isolated problem in biometric data interpretation, and a very different thing to devise and enforce a large-scale system on all members of a population. With advances in signal processing and computation, it is becoming very convenient to automate any numerically tractable problem, however questionable the underlying assumptions may be. Numerous government and private agencies are working towards large-scale biometric identification systems. In the near future, no official government document will be issued without a fingerprint or an eye-scan. Of all biometric validation techniques, finger print based validation is the most established and entrenched in law enforcement through out the world. The Open Biometric Initiative cracks open the clean fabrication of automated biometric identification at its root by making the decision landscape[3] of the classification available to scrutiny.

Identity as probability

A fingerprint is contains a series of ridges and furrows on the surface of the finger. The uniqueness of a fingerprint can be determined by the pattern of ridges and furrows as well as the singular or minutiae points, local ridge characteristics that occur at either a ridge bifurcation or a ridge ending. The extraction of the minutiae points from a scan delivers the structural basis of identification. Fingerprint matching[4] techniques that use minutiae based methods first find minutiae point positions and angles and then compare their relative placements to a reference fingerprint. The constellation and number of minutiae points build the basis for matching a one fingerprint to another.

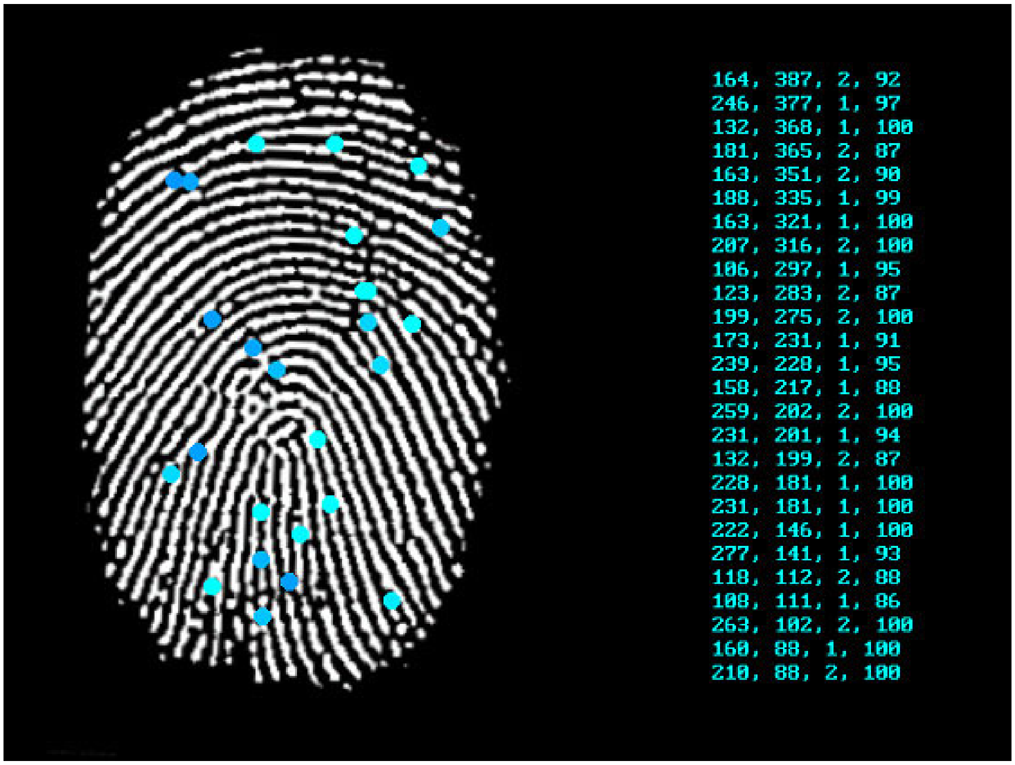
Formerly a domain reserved for human forensics experts, minutiae extraction can now be translated into executable computer code. In the machine, both minutiae map and minutiae matching are found within degrees of error and translated into probabilities.. However, the results of these mathematical operations generate information that is valid within certain limits and under certain assumptions. The rules of probability theory ensure that the assumptions are computationally tractable. Error is translated into a fraction of unity. It is elegant and technically elegant way of representing likelihood. But the results are not absolutes; rather a kind of suggestion that require some form of judgment. Technically, one usually defines a threshold value as an arbitrator. Values above a set threshold belong to one class while those below belong to a different one. While the human in the loop might ponder the uncertainties of a classification task, the machine is programmed to minimize ambiguities for efficiency and authority. The imperative of erring on the side of caution only enforces the tendency to simplify such complex operations.

[3] John Daugman, "Biometric decision landscapes", Technical Report, Number 482, Computer Laboratory, University of Cambridge, ISSN 1476-2986

[4] There are alternatives to the minutiae method (such as correlation based methods); we use this standard approach. See the following US government documents for technical details:
Garris M. and McCabe, R., *NIST Special Database 27, Fingerprint Minutiae from Latent and Matching Tenprint Images*, National Institute of Standards and Technology, Gaithersburg, June 30 2000.
Summary of NIST Standards for Biometric Accuracy, Tamper Resistance and Interoperability. National Institute of Standards and Technology, Gaithersburg, November 13, 2002.

Unfolding the basis of automated fingerprint based identification

It is the field of signal analysis and image processing that delivers the tools for biometric analysis. All of the underlying processes (noise removal, image enhancement, feature extraction) are strongly dependent on the premises of probability theory. This machine opens a window onto the reality of signal processing constraints. As opposed to claiming binary clarity and ultimate authority, the result set of a finger scan from this machine is a mathematically precise but open list of probable results. It allows the user insight into the internals of an otherwise hidden process. The machine prints this information as a map with all characteristic points of a finger scan together with class (ridge ending or bifurcation) and most importantly likelihood. Final evaluation of the significance of this data is left open.



```
164, 387, 2, 92
246, 377, 1, 97
132, 368, 1, 100
181, 365, 2, 87
163, 351, 2, 90
188, 335, 1, 99
163, 321, 1, 100
207, 316, 2, 100
106, 297, 1, 95
123, 283, 2, 87
199, 275, 2, 100
173, 231, 1, 91
239, 228, 1, 95
158, 217, 1, 88
259, 202, 2, 100
231, 201, 1, 94
132, 199, 2, 87
228, 181, 1, 100
231, 181, 1, 100
222, 146, 1, 100
277, 141, 1, 93
118, 112, 2, 88
108, 111, 1, 86
263, 102, 2, 100
160, 88, 1, 100
210, 88, 2, 100
```

Fig 2. Characteristic points together with their coordinates, type code (ridge ending or bifurcation) and color-coded likelihood. The machine also prints this information on a card, a probabilistic IDcard for your reference.