

The Open Biometrics Project and its Keeper

The Keeper, a software program that challenges hard and fast classification of biometric data, supports the Open Biometrics Project. After two years of development, the concept first proposed as an experiment at ISEA2002¹ is now a robust machine² that can be deployed in public spaces.

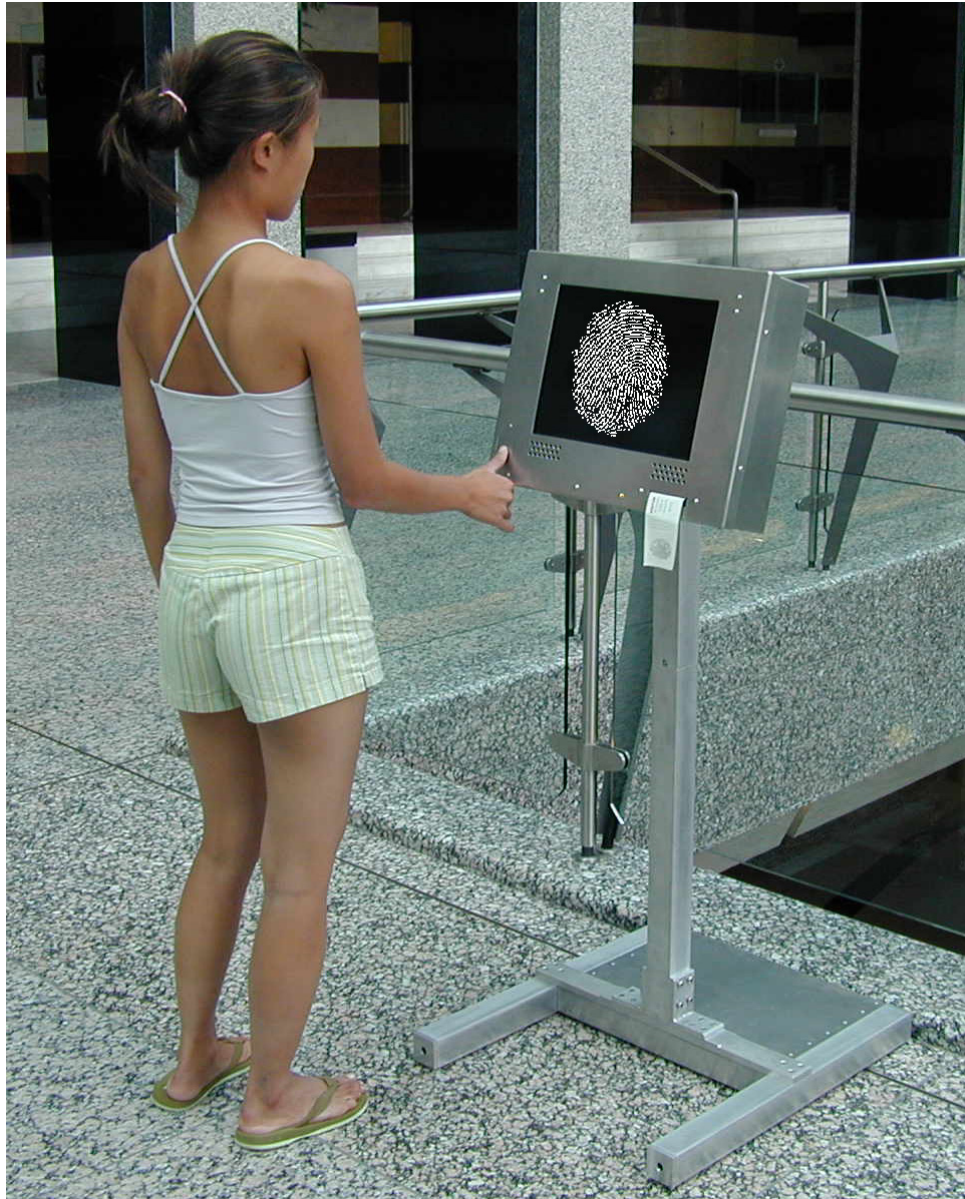


Fig. 1: The machine

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 normalization

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. This is where the Keeper comes into play. The Open Biometric Project and its Keeper crack open the clean fabrication of automated biometric identification at its root. Put your finger on this machine and it will show you what kind of information biometric readers extract from humans.

Identity as probability

A fingerprint is made of 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 techniques that use minutiae-based methods first find minutiae point positions and angles and then compare their relative placements to a reference fingerprint³. The constellation and number of minutiae points build the basis for matching a one fingerprint to another. This is a rather delicate matter. 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; an elegant form of quantifying likelihood. 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. There is nothing wrong with this process. It is elegant, intelligent and conceptually sound. But the results

³ 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.

are not absolutes; rather a kind of suggestion. While the human in the loop might ponder the uncertainties of an assigned task, the machine is programmed to minimize ambiguities for efficiency and authority. The imperative of erring on the side of caution in times of *Angst* only enforces the tendency to simplify such complex operations.

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. Our machine percolates these mathematical substrata to the surface, and 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 the Keeper 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 (ending or bifurcation) and most importantly likelihood. This is not an exercise in techno-cult. *This is the basis for who you may be believed to be.*



Fig 2. The Keeper shows characteristic points together with their coordinates, type code (ridge or ending) and color-coded likelihood. The Keeper also prints this information on a card, a probabilistic Icard for your reference. Keep this pint-out with your documents. It will allow you to question other non-transparent biometric readers.

Open classification systems

The Keeper opens the door to a larger discussion on the role of classification and expert systems. Many 'smart' machines will be devised to 'help' us with tasks deemed too time consuming or too difficult. While knowledge and expertise will always be of value, it will be continuously important to make the processes upon which expert decisions are made transparent. Now is the time to formulate the need for open expert systems whose results can be debated.

Expertise is important but responsibility even more so. Whom do we trust with personal data? Who owns a routinely collected finger scan whose electronic permanence can exceed the time frame of its human originator? Why is the iris scan, used to ensure one's immediate credentials, silently stored beyond its use with no expiration date? Together with transparent expertise we will need systems that responsibly manage data. The Keeper's solution is simple: Keep nothing. Discard everything. In the future, we will need formalisms that guarantee total data deletion. The Keeper instantiates just this. No records are maintained. After you receive your printed probabilistic Idcard, the machine has no record of you.

Art in the Age of Digital Signal Processing

In the computation machine, all is data. All images are maps, conveniently displayed to fool our retinal system. Below the surface of appearance, however, lies a deep ocean. The extraction and classification of information is a technical process that can be opened for discourse. From online reservation, credit card, and visa application systems, information databases are nested in the fabric of life today. It makes sense to declare them material for non-retinal attention and intervention. Nowhere will this matter more than in the process of automated identification. The discourse on automated expertise and classification is a prerequisite to a critical approach to the consequences of digital abstraction and its automation in the social domain. This matters because it changes the way we live our daily lives.