A BRIEF REVIEW OF
BIOMETRIC IDENTIFICATION

by Tilo Burghardt
University of Bristol, UK
mailto:tilo@cs.bris.ac.uk

1 BASIC CONCEPT:
The Power of Measuring Living Beings

There are three means of authentication, that is approaches to verifying an individual’s identity: 1) by some secret data, e.g. a password, 2) by possession of a device, e.g. keys or tags and 3) by what the individual actually is, e.g. its anatomy, physiology and behaviour [23]. The scientific domain investigating the last is known as ‘biometrics’, a term derived from the Greek words bios (life) and metron (measure). This very etymology captures the core concept of the approach: biometric identification systems are designed to analyse measurements taken from living beings for the purpose of classifying their population, that is either authenticating (1-to-1 match) or identifying (1-to-n match) individuals or groups.

Clearly, the concept of directly measuring an organism – instead of relying on synthetic markers – renders the approach highly suitable for scenarios where little interference with the subjects is permitted, e.g. passive biometrics such as secret surveillance, public observation or, in the case at hand, wildlife monitoring aiming for minimal disturbance.

2 HISTORICAL NOTE:
From Clay Prints to Population Databases

Biometric identification has had a place in human life for more than 4000 years. The approach has been predominantly applied to the problem of profiling and retrieving the identities of humans. Dating back as far as 2000 BC, the ancient Babylonians accompanied contracts with fingerprints pressed in clay to prevent forgery [2, 3]. Figure 1(a) depicts one of the earliest findings of this kind.
Figure 1: **Representation of Fingerprints throughout the History of Biometrics.** The images illustrate the historical advances of biometrical techniques in representing fingerprints. (a) clay print from mesopotamia dated about 2000 BC; (b) ink prints taken by the Buenos Aires police in 1891; (c) digital fingerprint image with extracted minutiae (ridge endings and bifurcations) and ridge directions superimposed – the state of the art in 1996; (d) fingerprints aligned using 2D thin plate splines controlled by minutae matching (top) and ridge curve matching (bottom) conducted in 2006. [images taken from Cummins [3], Rodriguez [26], Jain [13] and Ross et al. [27]]

Subsequently, skin impressions of either hands or feet were used as signatures by early cultures in Asia [19] and North America [2].

Although the uniqueness of skin ridges is mentioned in scripts by renaissance scholars\(^1\), it was only at the onset of the industrial age that European scientists started investigating biometrics on a quantitative, truly scientific basis. The first physiological measurements on humans, that is on their skin ridges, ear-shape, head-shape etc., were systematically categorised and analysed\(^2\) in the mid-19th century. Ever since the introduction of precise sensing devices (e.g. cameras), modern forensic analysis (e.g. population catalogues [26]), and increasing computerisation have gradually removed the need for human inspection. They have made possible the engineering of largely autonomous, active biometric systems that are now applied in a number of security-relevant domains. Most of them, however, rely significantly on the user’s collaboration. Table 1 gives an overview of performance benchmarks of the most widely applied, currently available human biometric systems for comparison with the animal identification system proposed.

The level of robustness, diversity and economical impact of biometric tech-

---

\(^1\)Written during the 1680’s, scripts by N. Grew [4], G. Bidloo [1] and M. Malpighius [21] describe unique entities of human physiology mainly focussing on the observation that human skin carries individual features.

\(^2\)Europeans who investigated biometric entities during the industrial period include J. E. Purkinje [25], W. Herschel, A. Bertillon (as described by Garfinkel [10]), F. Galton [8] and E. Henry. They mainly studied the physical uniqueness inherent to humans for anthropological, economic and, only later, for forensic purposes.
### Table 1: Current Performance Characteristics in Biometrics

The table summarises the authentication performance details of several biometric techniques. A representative subset of the most widely spread techniques in human forensics is listed and sorted by identification accuracy. Note the enormous variance in characteristics amongst the methods. At the bottom part, details of the proposed animal identification system are given for comparison. (Key: FAR...false acceptance rate, FRR...false rejection rate, EER...equal error rate (rate where FAR=FRR), FER...failure to enrol rate, TS...template size, SSD...sensor-subject distance, STR...string comparison methods, IR...infrared capture, MB...minutae based; See the individual references for more details.)

<table>
<thead>
<tr>
<th>Entity (method)</th>
<th>EER[%]</th>
<th>FAR/FRR[%]</th>
<th>FER[%]</th>
<th>TS[kB]</th>
<th>SSD[m]</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNA (STR)</td>
<td>$\approx 10^{-7}$ [29]</td>
<td>close to 0 [32]</td>
<td>$\approx 0$ [29]</td>
<td>$&gt; 50$</td>
<td>contact</td>
</tr>
<tr>
<td>retinal vessels (IR)</td>
<td>$\approx 10^{-8}$ [32]</td>
<td>$\approx 0/\approx 0.4$ [28]</td>
<td>$\approx 0$ [28]</td>
<td>$\approx 0.05$</td>
<td>$\approx 0.075$</td>
</tr>
<tr>
<td>iris (IR)</td>
<td>$\approx 7.6 \cdot 10^{-4}$ [32]</td>
<td>$&lt; 10^{-3}/\approx 6$ [14]</td>
<td>$\approx 7$ [14]</td>
<td>$\approx 0.3$</td>
<td>$\approx 0.3$</td>
</tr>
<tr>
<td>fingerprint (MB)</td>
<td>$\approx 0.2$ [32]</td>
<td>$\approx 0.1/\approx 0.25$ [35]</td>
<td>$\approx 4$ [35]</td>
<td>$\approx 0.3$</td>
<td>contact</td>
</tr>
<tr>
<td>facial features</td>
<td>n/a</td>
<td>$\approx 10/\approx 4$ [24]</td>
<td>n/a</td>
<td>$\approx 0.05$</td>
<td>$\approx 20$</td>
</tr>
<tr>
<td>voice pattern</td>
<td>n/a</td>
<td>$\approx 10/\approx 15$ [28]</td>
<td>$1-30$ [28]</td>
<td>$\approx 0.02$</td>
<td>$\approx 3$</td>
</tr>
<tr>
<td>penguin spots</td>
<td>n/a</td>
<td>$\approx 10^{-4}/\approx 8$</td>
<td>$\approx 80$</td>
<td>$\approx 0.1$</td>
<td>$\approx 3-7$</td>
</tr>
</tbody>
</table>

Techniques is still steadily and rapidly increasing. In fact, biometric techniques are now being applied to human populations on a large scale: in January 2006 the United States Federal Bureau of Investigation (FBI) officially stored about 47 million fingerprints in its IAFIS\(^3\) database and entity-specific biometric standards for humans are under development within ISO\(^4\) and INCITS\(^5\) [34]. The United States of America as well as the European Union are currently starting to introduce biometric passports for their citizens, creating controversies over the practicality as well as the philosophical and ethical justification of biometric registration procedures in general. Such ventures on the international stage dramatically illustrate an ongoing ‘biometric revolution’ that leaves an ever more prominent footprint on the procedures that underpin life in modern societies.

Meanwhile, the research community has started to leap ahead from the classical forms of visual biometrics, e.g. fingerprint [13, 27], face [22, 31] or iris recognition [6, 30], into new territory. Recent biometrical research starts focussing on passive and ubiquitous biometrics [17], on multi-modal biometric fusion [16], on behavioural fingerprinting [9], and on a number of unconventional identification techniques using signatures of gait [5], hair pattern [7], ear-shape [18], and

\(^3\)The Integrated Automated Fingerprint Identification System (IAFIS) is the main U.S. fingerprint and criminal history system linking several subsystems under a common standard. It is maintained by the FBI. Further information can be found at the US National Science and Technology Council (NSTC) [33].

\(^4\)The International Standards Organisation (ISO) is the major international body for general standardisation covering more than 150 national member organisations and nearly 3000 technical bodies.

\(^5\)The Inter-National Committee for Information Technology Standards (INCITS) is a major body of standardisation in the field of Information and Communications Technologies. It is accredited by, and operates under rules approved by the American National Standards Institute (ANSI).
even odor [15]. Yet the research efforts concentrate almost exclusively on the human subject. While DNA-based methods have become an essential tool for the identification and classification of non-human species in multiple natural sciences [29, 32], the application of visual biometrics is still broadly limited to humans.

3 BIOMETRIC ENTITIES: Individually Characteristic Patterns of Life

In general, two main categories of systems can be differentiated depending on the descriptiveness and granularity of the classification performed. If only broad classes of a population are to be identified by (commonly scalar) measurements, e.g. body weight, eye-colour, height etc., the methods are referred to as soft or weak biometrics [33].

In contrast, procedures that aim to identify individuals with high confidence levels are known as strong biometrics [16]. These methods commonly rely on statistics from multidimensional aspects of physiological or behavioural characteristics that differ (significantly) within the population of interest. This work exclusively focusses on strong biometrics since only they provide reliable identity data – rather than subclass membership information – as needed for individual-based applications in biological and conservational sciences.

Strong biometrics require the presence of a high-dimensional configuration space spanned by some of an individual’s measurable properties. Categories of such properties are known as ‘biometric entities’; they are commonly differentiated by their form and by their location on an organism’s body as well as by the type of information used.

Naturally, an organism carries multiple such entities. Figure 2 depicts a selection of biometric entities used for human identification.

![Selection of Human Biometric Entities](image)

Figure 2: Selection of Human Biometric Entities. The images illustrate some unique human biometric entities that can serve as a source of individuality data. Illustrated are the unique structure of (from left to right) ridge lines in finger and palm prints, shapes of X-rayed teeth, blood vessel shape in the retina, iris patterns and ear shapes. [images taken from Jain et al. [14]]

A number of human biometric entities can also be found (and theoretically used) in mammals, e.g. iris patterns, skin-ridge prints, voice etc. However, measuring them to the necessary detail proves difficult in field scenarios, if not
Table 2: Characteristics of Biometric Entities. The quality of a biometric entity can be characterised by five essential and four system-dependent measures listed in the table above. Key: ↑...high; ↓...medium; ±...low; ×...n/a; D...DNA; R...retina; I...iris; F...fingerprint; Fa...face; V...voice; CP...coat patterns (penguin spot patterns and scapular zebra stripes in particular); [extended comparison based on an earlier suggestion by Jain et al. [12]]

In contrast, coat patterns, while not present in humans, provide an entity of full body size that is (even intended to be) visible over distance, providing excellent measurability.

Table 2 compares coat patterns to classical biometric entities with respect to the properties relevant for identification. The characteristic properties of a set of biometric entities are termed a ‘biometric profile’. The profile is used to represent the individual in an information system or population database. The substitution of an identity by a profile is, however, based on the assumption that an individual’s identity is intrinsic to the information locked in its biometric entities [20, 37]. Hence, in order to qualify as a biometric entity, a feature set must satisfy a number of properties. Jain [12] presented a set of properties that approximate this condition. His suggestions are listed and extended below (they also form the basis of Table 2). I suggest categorising the properties into three fundamental groups of accountable factors:

**Physiological Factors.** First, the feature set has to contain components that are both singular in their physical/behavioural structure (uniqueness) and constant in their appearance over time (permanence). In addition, a feature set should be all-inclusive in the sense that – ideally – each and every member of the population carries it (universality). Naturally, the process of identifying potential entities in a species is guided by these criteria.

**Technological Factors.** Second, and this is an engineering requirement, biometric entities must be ‘collectable’, suggests Jain. Here, it is proposed to split his criteria into measurability and comparability since these two features directly relate to the components of feature extraction and pattern matching found in the design of actual identification systems.
Interactive Factors. In terms of interaction requirements, *invasiveness* (not mentioned by Jain [12]) is relevant to wildlife applications. Passive visual methods are non-intrusive by their nature and, therefore, highly applicable. Social *acceptability* and active *circumvention*, on the other hand, are mainly important in human security applications.

Assuming that the five fundamental conditions mentioned – namely universality, uniqueness, permanence, measurability and comparability – are met, biometric systems can operate without the use of synthetic markers. Accordingly, a biometric profile cannot be separated from an individual in a natural way – if not occluded, they are omnipresent. Coat patterns can, therefore, be observed with a relatively low level of cooperation of the individual investigated (passive biometrics). Thus, for the purpose of animal identification, coat pattern biometrics can potentially excel over other identification techniques since they are applicable in wildlife scenarios 1) where cooperation is unlikely, 2) where devices are difficult to fit, and 3) where interaction with or disturbance of endangered species is to be avoided.

4 DESIGN OF BIOMETRIC SYSTEMS:
Study of Components and Operational Modes

Having discussed the properties of biometric entities, the focus is now shifted towards the methodology of extracting the uniqueness-bearing information inherent to them. Modern biometric designs achieve identification by a number of system components that perform conceptually different tasks along one, widely common recognition pipeline. In accordance with previously suggested models, by for instance Jain et al. [14] or Hüseyin [11], Figure 3(a) depicts the broad architecture of biometric systems in form of a flow chart. The model comprises the stages of acquisition, extraction, storage, matching and application. The extraction component is resolved further where green bars indicate how this ties in with the ‘locate-pose-identify’ paradigm proposed. It can be seen that the registration (object detection) and the normalisation (pose identification) components are identified as tasks in their own right. This is, so to say, a ‘vision view’ on biometric systems, a view that recognises the complexity of locating and posing the biometric entity in the first place. Each of the five components fulfills a different task:

**Acquisition.** The initial measurements on individuals are taken by one or multiple sensors\(^6\) referred to as *acquisition devices*. This work deals exclusively with optical input from the visual spectrum\(^7\).

---

\(^6\)Sensors may include cameras operating at different electromagnetic wavelengths, pressure sensors, chromatographs, scales, accelerators, microphones, distance sensors, chemical sensors or even more sophisticated techniques such as DNA sampling or tomographic techniques.

\(^7\)There is no physiological or technical reason that prevents the capture of biometric entities
Extraction. Separating the descriptive components of the biometric entities from redundant data in the images is taken care of by a registration procedure applied to locate the entity within the measurement. During this process parameters are generated that describe the context of the detection such as pattern size, lighting, viewpoint, pose or the pattern visibility. These parameters are then used to normalise the extracted pattern, decreasing the intra-class variance caused by different acquisition conditions. The raw biometric patterns, i.e. images of relevant body parts, are generally large (usually several 100 KB) while only a small subset of this data is individually discriminative (a few bytes). Therefore, uniqueness-bearing features are extracted in order to decouple the subject-specific data component. The individually discriminative features can then be combined to form a biometric template providing a data structure for an efficient handling of biometric information.

Storage. During an enrolment phase, templates are saved in a population database together with a unique identifier, e.g. a name tag or some integer etc. In praxis, the size of the database can grow rapidly to several million entries, even above actual population sizes since profiles might be stored over several generations. In order to keep matching times down, a cascaded database design that emphasises the concepts of rigorous indexation, parallel processing and working sets is usually employed.

Matching. During submission, that is the actual runtime phase, the system performs identification by establishing an association between a measurement on the coats of penguins or zebra in the IR/UV spectrum for instance in order to enable night observation.
and entries in the population database. A matching scheme, usually a distance measure, is employed to compare an input with the existing profiles either exhaustively or stepwise by means of indexation.

**Application.** Finally, the matching results (or the newly formed templates in the case of enrolment) are presented to the application together with metadata on the entity’s quality and the anticipated certainty of the produced result.

Summarising the model, the system as a whole is built around a core recognition pipeline of vision algorithms (extraction and matching) that extract and compare a biometric entity presented to a sensor (acquisition device) against stored profiles (database). According to the match calculated, the system finally reacts to the input presented (application).

### 5 PERFORMANCE CHARACTERISTICS:
**Measuring the Quality of System Operation**

Essentially, a visual biometric system constitutes a classification framework that maps from images to identities. Its performance is, therefore, traditionally quantified by characteristics that describe the statistics of a classifier. Assuming authentication, i.e. matching against a single profile in the database, biometric systems are required to categorise an individual as either genuine (accept) or as an impostor (reject).

For a set of test images presented to the system, this binary classification scheme translates into two error measures, that is the *false acceptance rate* (FAR) and the *false rejection rate* (FRR). Complementary, the *genuine acceptance rate* (GAR) is $1 - \text{FRR}$ and the *genuine rejection rate* (GRR) is $1 - \text{FAR}$. By adjusting the parameters of an identification system, one can typically trade an increase in GAR for an increase in FAR. Hence, introducing a particular point in this trade-off, the *equal error rate* (EER) – defined as the cross-over value where FAR and FRR coincide – is often used to compare the performance of different systems.

However, in this work the entire spectrum of GAR-FAR-pairs, that is the ‘*receiver operating characteristic*’ (ROC), will be used for performance description. This approach provides more complex a measure, accounting for different system behaviours at different GAR-FAR-trade-offs (see [36] for details). Note that one point on the ROC curve is chosen as the *working area*, pinpointing the system to operate at one specific trade-off ratio.

Not all individuals of a population are typically able to register or ‘enrol’ with a biometric system. Insufficient quality\(^8\) of biometric entities (lack of universality) as well as inappropriate capturing conditions (lighting, pose, occlusion, motion blur etc.) can cause a *failure of enrolment* (FoE). In the animal kingdom a lack of entity quality is often caused by injuries (predation marks, bricklayers, steel workers) or miss the entity entirely (accidents, disabilities).

\(^8\)For instance, a subset of the human population have fingerprints of poor quality (bricklayers, steel workers) or miss the entity entirely (accidents, disabilities).
loss of body parts), genetic conditions (albinos) or natural variance (lack of chest spots in African penguins). For illustration, Figure 4 visualises the distribution of spot counts over a penguin subpopulation (note the log scale of the graph). The proportion of the population that fails to complete the enrolment

Figure 4: Histogram of Spot Counts in African Penguins. Manual screening of 400 African penguins revealed the above histogram of spot counts. On average, there were 12.2 spots on a penguin’s chest, while most penguins carried 7 spots (bin 6-8). It can be seen that the entity is widely universal to the sample population, yet about 3% of animals fall below the defined failure of enrolment (FoE) barrier of a minimum of 3 spots where less than 1% did not carry any chest spots. Apart from regularly patterned penguins with no spots, rare albinos (shown on the left) fall into this category. They miss all dark colouration of feathers, beak and skin. [image sources: I12, I01]

is specified by the failure to enrol rate (FER) indicated by red marks in the histogram above. It reflects the combined universality (given by the distribution of spot counts) and measurability (represented by a manually introduced failure of enrolment (FoE) barrier which is defined in order to reject entities below a certain quality measure) ■

Note that this document is based on parts of the second chapter of a PhD thesis:

References
[weblink: http://special.lib.gla.ac.uk/anatomy/bidloo.html].


[weblink: http://ctl.ncsc.dni.us/biometweb/BMCompare.html].


