21

Linkages between Biometrics and Forensic Science

Damien Dessimoz and Christophe Champod

Forensic Science Institute, School of Criminal Sciences, Batochime - Quartier Sorge, University of Lausanne, 1015 Lausanne-Dorigny, Switzerland.
{damien.dessimoz, christophe.champod}@unil.ch

21.1 Forensic science and biometrics - a general contrast

Using biometric data for classification and/or identification in forensic science dates back to the turn of the 20^{th} century. Biometrics as we know it today can be viewed as extension of Bertillon's anthropometric approach, benefiting from automation and the use of additional features. This chapter presents a historical and technical overview of the development and the evolution of forensic biometric systems, used initially manually and then in a semi-automatic way. Before focusing on specific forensic fields, we will define the area, its terminology and draw distinctions between forensic science and biometrics.

Forensic science refers to the applications of scientific principles and technical methods to an investigation in relation to criminal activities, in order to establish the existence of a crime, to determine the identity of its perpetrator(s) and their modus operandi. It is thus logical that this area was a fertile ground for the use of physiological or behavioral data to sort and potentially individualize protagonists involved in offences. Although manual classification of physical measures (anthropometry), and of physical traces left and recovered from crime scenes (fingermarks, earmarks,...) was largely successful, an automatic approach was needed to facilitate and to speed up the retrieval of promising candidates in large databases. Even if the term *biometrics* usually refers "to identifying an individual based on his or her distinguishing characteristics" [14], biometric systems in forensic science today aim at filtering potential candidates and putting forward candidates for further 1-to-1 verification by a forensic specialist trained in that discipline, in the following traditional typical *cases* (here exemplified using fingerprints):

> *Case 1*: A biometric set of features in question coming from an unknown individual (living or dead), is searched against a reference set of known (or declared as such) individuals. In the fingerprint domain, we can think

of a ten-print to ten-print search based on features obtained from a ten-print card (holding potentially both rolled and flap inked impression from fingers and palms), compared to a database of ten-print cards.
Case 2: An unknown biometric set of features left in circumstances of interest to an investigation, is searched against a reference set of known (or declared as such) individuals based on the features available. We can think of a fingermark recovered from a crime scene that will be searched against a database of ten-print cards. The converse is also possible, meaning the search of the features from a new ten-print card against the database of (unresolved) fingermarks.
Case 3: An unknown to unknown comparison resulting in the possible detection of series of relevant incidents. For fingerprints, it would mean comparing latent prints to latent prints.

Both *case 2* and *case 3* involve biometric features (in physical or other forms) that can be left on scenes relevant to an investigation. In forensic investigation, one of the main objectives is to find marks associating an offender to an event under investigation. These marks can be either left by the perpetrator during the event or found on the perpetrator after it. This mechanism of "exchange" of marks is known under the misnomer of "Locard's exchange principle" in reference to the French criminalist Edmond Locard [59]. Forensic information can be found either as *physical* marks, or as *digital* traces. Physical mark are made for example by the apposition of fingers, ears or feet on any kind of surfaces, while digital traces are analog or digital recordings typically from phone-tapping and security cameras. Face and speech biometrics, and to some extent modalities captured at distance such as ear, iris and gait can be used as digital traces in forensic science.

As a **first distinction** between biometrics and forensic science, it is important to stress that forensic biometric systems are used in practice as sorting devices without any embedded decision mechanism on the truthfulness of the identification (although we do see some developments in that direction). Indeed, the search algorithms are deployed as sorting devices. These ranking tools allow (at an average known rate of efficiency) presenting the user a short list (generally 15 to 20) containing potentially the right "candidate" to a defined query. Here the term "candidate" refers to the result of a search against biometric features originating from either individuals or marks (known or unknown). It is then the duty of the forensic specialist to examine each candidate from the list as if that candidate was submitted through the regular channels of a police inquiry. This first contrast shows that forensic biometric systems are considered by forensic scientists as external to the inferential process that will follow.

The **second distinction** lies in the terminology, performance measures and reported conclusions used in the processes. Although forensic biometric

systems can be used in both *verification* (one to one) or *identification* modes (one to many), depending on the circumstances of the case, the identification mode can be seen as a series of verification tasks. The reported conclusion by the forensic specialist when comparing an unknown to a known entry can take different forms depending on the area considered.

In the fingerprint field, conclusions can take three states: *individualization*, *exclusion* or *inconclusive* (for a more detailed discussion see [20]). The first two are categorical conclusions accounting for all possible entities on the Earth. In other words an individualization of a finger mark is a statement that associates that mark to its designated source to the exclusion of all other fingers or more generally all other friction ridge skin formations. Individualization is often presented as the distinguishing factor between forensic science and other scientific classification and identification tasks [50].

In the fields of face or ear recognition carried out manually by skilled examniers, speaker verification based on phonetic/linguistic analysis, dental analysis or handwriting examination, the three conclusions described above will remain under the same definition, but probabilistic conclusions will also be allowed on a grading scale both in favor or against identity of sources with qualifiers such as: *possible*, *probable* or *very likely*. For a discussion of the adequacy of the scale in forensic decision making refer to [21].

The principles and protocols regarding how these conclusions (outside the DNA area) can be reached by a trained and competent examiner is outside our scope. However, the general principles of the inference of identity of sources are treated in detail by Kwan [55] or by Champod et al. (for fingerprints) [25]. In all these areas, based on different features, the expert subjectively weighs the similarities and dissimilarities to reach his/her conclusion. Nowadays the reliability of these so-called "subjective disciplines" are being increasingly challenged, especially because of (*i*) the development of evidence based on DNA profiles governed by hard data and (*ii*) the evolving requirements for the admissibility of evidence following the Daubert decision by the Supreme Court of the USA[1]. The absence of underpinning statistical data in the classic identification fields is viewed as a main pitfall that requires a paradigm shift [81].

In the field of DNA, the strength of evidence is indeed generally expressed statistically using case specific calculations [97] linked to a likelihood ratio (defined later). In essence the process is probabilistic although we do see some tendencies to remove uncertainty from the debate [18].

It is our opinion that inferences of sources across all forensic identification fields, when put forward to a factfinder in court for example, must be approached within a probabilistic framework even in areas that had been traditionally presented through categorical opinions such as fingerprints [20]. An approach based on the concept of *likelihood ratio* should be promoted. In-

[1] Daubert v Merrell Dow Pharmaceuticals 43 F 3d 1311; 125 L Ed (2d) 469; 509 US 579; 113 S Ct 2786 (1993).

deed, a likelihood ratio (LR) is a statistical measure that offers a balanced presentation of the strength of the evidence [78]. It is especially suitable for assessing the contribution of forensic findings in a fair and balanced way [2]. Note that we restrict our analysis to an evaluative context, meaning that the forensic findings may be used as evidence against a defendant in court. There is a wide scope of application of biometric systems in investigative mode (e.g. surveillance) that we will not cover.

Formally, the LR can be defined as follows:

$$LR = \frac{p(E \mid S, I)}{p(E \mid \bar{S}, I)} \tag{21.1}$$

Where:

E: Result of the comparison (set of concordances and discordances or a similarity measure such as a score) between the biometric data from the unknown source and the biometric data from the putative source.
S: The putative source is truly the source of the unknown biometric features observed (also known as the prosecution proposition).
$\bar{S}$: Someone else, from a relevant population of potential donors, is truly the source of the unknown biometric features observed (also known as the defense proposition).
I: Relevant background information about the case such as information about the selection of the putative source and the nature of the relevant population of potential donors.

This LR measure forces the scientist to focus on the relevant question (the forensic findings) and to consider them in the light of a set of competing propositions. The weight of forensic findings is essentially a relative and conditional measure that helps to progress a case in one direction or the other depending on the magnitude of the likelihood ratio. When the numerator is close to 1, the LR is simply the reverse of the random match probability (RMP) in a specified population. In these cases, reporting the evidence through the RMP is adequate. However most biometric features suffer from within individual variability facing an assessment of the numerator on a case by case basis.

The performance measures for forensic science are obtained from the analysis of the distributions of the LRs in simulated cases with given S and $\bar{S}$. These distributions are studied using a specific plot (called Tippett plot) that shows one minus the cumulative distribution for respectively the LRs computed under S and the LRs computed under $\bar{S}$. These plots also allow study and comparison of the proportions of misleading evidence: the percentage of $LR < 1$ when the prosecution proposition S is true and the percentage of $LR > 1$ when the defense proposition $\bar{S}$ is true. These two rates of misleading results are defined as follows [67]:

$RMED$: Rate of misleading evidence in favor of the defense: among all LRs computed under the prosecution proposition S, proportion of LR below 1.
$RMEP$: Rate of misleading evidence in favor of the prosecution: among all LRs computed under the defense proposition $\bar{S}$, proportion of LR above 1.

Whereas a LR is a case-specific measure of the contribution of the forensic findings to the identity of sources, the Tippett plot and the associated rates ($RMED$, $RMEP$) provide global measures of the efficiency of a forensic biometric system. LR based measures are now regularly used in the forensic areas of speaker recognition [26, 33, 76], fingerprints [67, 66], and DNA [37]. That constitutes a major difference compared to standard global measures of biometric performances based on type I and type II error rates (e.g. Receiver Operating Characteristic (ROC) or Detection Error Tradeoff (DET) curves). For a discussion on the limitations associated with these traditional measures when used in legal proceedings, see [26].

The concept of identity of sources is essential and needs to be distinguished from the determination of civil identity (e.g. assigning the name of a donor to a recovered mark), from guidance as to the activities of the individual or its further unlawful nature. Forensic comparisons aim initially at providing scientific evidence to help address issues of identity of sources of two sets of biometric data; whether these data are coupled with personal information (such as name, date of birth or social security number) is irrelevant for the comparison process. From the result of this comparison and depending on the availability and quality of personal information, then inference as to the civil identity can be made if needed. Likewise there is a progression of inferences between the issue of identity of sources towards their alleged activities and offences. It is a hierarchical system of issues as described by Cook et al. [29]. The forensic biometric comparison process aims at handling source level issues as its primary task: the whole process is not about names or identity, but in relation to source attribution between two submitted sets of features (respectively from a source 1 and a source 2).

A **third distinction** lies in the wide range of *selectivity* of the biometric data that can be submitted due to varying quality of the material. Selectivity here can be seen as the discrimination power of the features, meaning the ability to allow a differentiation when they are coming from distinct sources. Some of the main modalities will be reviewed in the next sections but there is an all-encompassing phenomenon that goes across modalities in varying degrees. In the commission of a crime, contrary to usual biometric systems (for access control e.g.), it may not be possible to obtain high quality input biometric features - either for the template or transaction data. These biometric data are limited by numerous factors such as: the availability of the person and his/her level of cooperation, the invasiveness of the acquisition,

the various objects and positions one can take or touch while a crime is being committed. The subjects make no effort to present their biometric data to the system in an ideal and controlled way. Hence, whether the biometric data is acquired directly from individuals (living or dead), from images (of individuals, part thereof or X-rays) or marks left by them following criminal activities, the quality of the material available for the biometric comparison process, and thus its selectivity, may vary drastically from case to case and so will the within-person variability. This loss of selectivity is illustrated in Figure 21.1. The overall performance of the system is largely influenced by the quality of the input data conditioned by the acquisition and environmental conditions as summarized in Table 21.1. These factors are common in all biometric deployments, but forensic scenarios tend to maximize their variability.

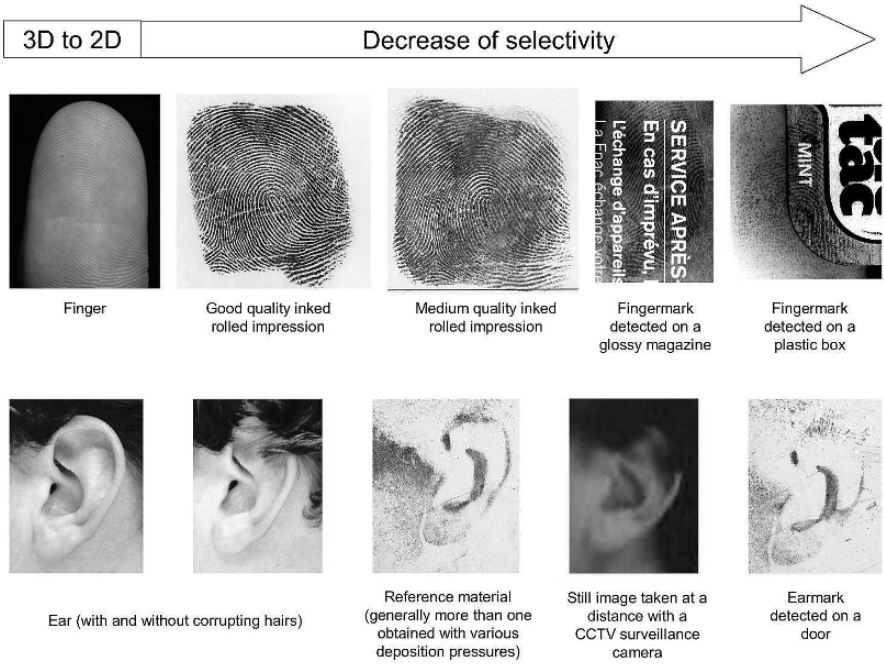

Fig. 21.1. Illustration of the diminishing selectivity of the biometric features as a function of the circumstances and conditions under which the biometric data are collected or obtained. Here is a clear relationship between selectivity and quality of the input information.

The **last distinction** we would like to stress upon is the range of comparisons that can be undertaken in the forensic environment depending on the circumstances of the cases. The three *cases* outlined initially all deal with

Acquisition conditions	Quality of the acquisition device (e.g. resolution). Amount of input information (e.g. a rolled inked fingerprint on a card versus a limited poorly developed fingermark on a curved surface). The availability of multiple templates (e.g. rolled and flap impressions of the same finger). The types of acquisition of both templates and transaction data (declared supervised versus covert). The acquisition at distance, the target size, the object movement, and the horizontal or vertical misalignments between the device and the subject. Presence of corrupting elements (e.g. glasses, beard, hair, clothes, or health condition - living or dead - of the subject). The time interval between the acquisitions of both sets of biometric material to be compared.
Environmental conditions	Background noise and uncontrolled conditions (e.g. illumination, noisy environment).
Data processing	The choice of the feature extraction algorithms and their level of automation (e.g. poor quality fingermarks may need to be manually processed by skilled operator in order to guide the system as to the relevant features). Efficiency of the detection and tracking algorithms (e.g. face detection and tracking). The matching algorithms in place and their hierarchy.
Operator	The operator interaction with the system at all stages (from acquisition to verification of candidates' lists).

Table 21.1. List of the factors affecting the selectivity of biometric information and thus the performances of biometric systems deployed in forensic applications.

comparisons of biometric information (with one side or the other being known) but at differing levels of selectivity. The driving force here is more the selectivity level associated with each compared biometric data sets, which can be similar (*case 1* and *case 3*) or largely different (*case 2*). The availability of known information, such as the name, the date of birth, the social security number (i.e. the *personal data* associated with each compared biometric data set), associated with the biometric features is not directly relevant to the comparison process. This information is although decisive to progress in the hierarchy, but has no impact on the decision of the identity of sources, which is driven by the selectivity of the compared biometric data. This progression is illustrated in Figure 21.2. The distinction between mark and reference material in a forensic case is that in general, marks are of lower quality than reference material (although the reverse could also be true). This concept of selectivity (Figures 21.1 and 21.2) that is driving the move from *case 1* to *case 3* is a continuum on both sides (source 1 and source 2). Essentially, we

can expect performances to degrade as we move down in selectivity levels.

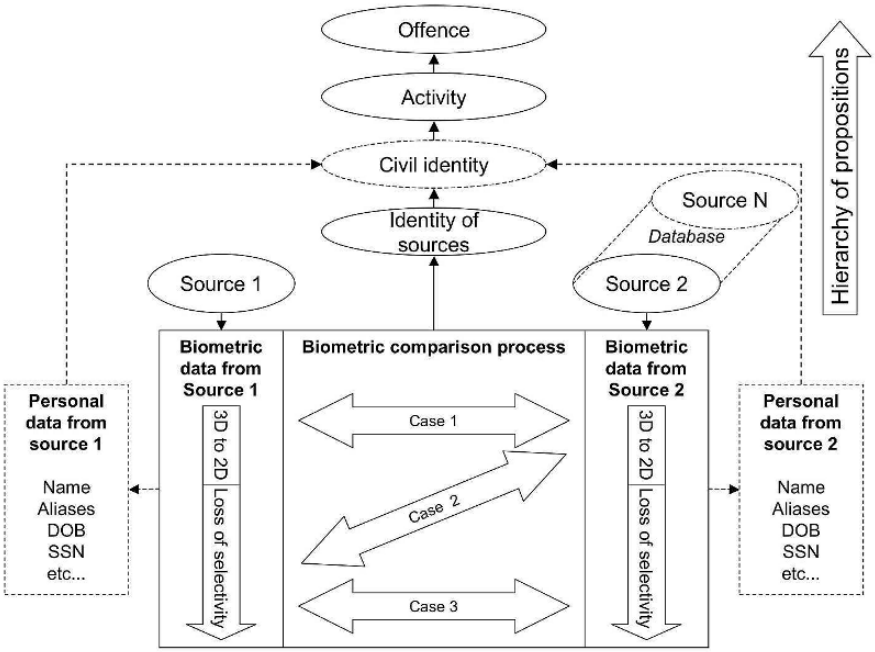

Fig. 21.2. General scheme of a forensic biometric system.

In the following sections we will cover the main forensic biometric modalities and then show how an automatic approach has and will change the conduct of forensic examinations.

21.2 Anthropometry

The abolition in 1832 of physical branding for habitual offenders in France resulted in legal authorities being incapable of recognizing them. The enforcement of new legislation allowing tougher sentences in cases of recidivism remained wishful thinking until the development of a proper identification system.

Some classifications, based on the declared name (not trustworthy) or the type of offence, were introduced, but without more than anecdotal success for obvious reasons. Identity documents or other official documents were not yet issued or, at the time, were prone to forgery. Even adding photography to the

offender card did not solve the issue, because of the lack of standardization and the difficulty extracting commonly understood descriptors to include them in a manual retrieval system.

Facing this state of affairs, Bertillon proposed in 1881 a solution to the problem of the identification of recidivists based on anthropological methods developed by Quételet and Broca [12]. The principles were the following: (*i*) adult bone lengths remain constant, but (*ii*) vary from individuals to individuals and (*iii*) they can be measured with reasonable precision. A classification method was then required, in order to structure these distinctive characteristics. Indeed for Bertillon "The solution of the problem of forensic identification consisted less in the search for new distinctive elements of the individual than in the uncovering of a classification tool"[2]. He proposed the use of the description of the iris' color combined with eleven precise measurements.

These measurable characteristics (Figure 21.3) were divided into three classes (small, medium and large), defined arbitrarily by fixed intervals to ensure equal number of cards for each class, while the iris color was classified in seven classes (Figure 21.4).

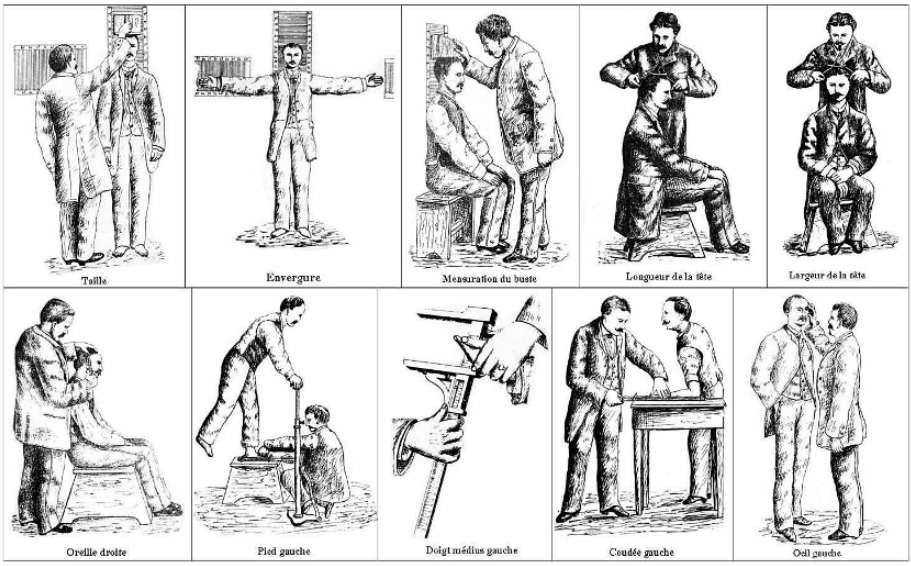

Fig. 21.3. Illustration of Bertillon's anthropometric measurements (adapted from [12]).

[2] Free translation from [12], for "La solution du problème de l'identification judiciaire consistait moins dans la recherche de nouveaux éléments caractéristiques de l'individu que dans la découverte d'un moyen de classification".

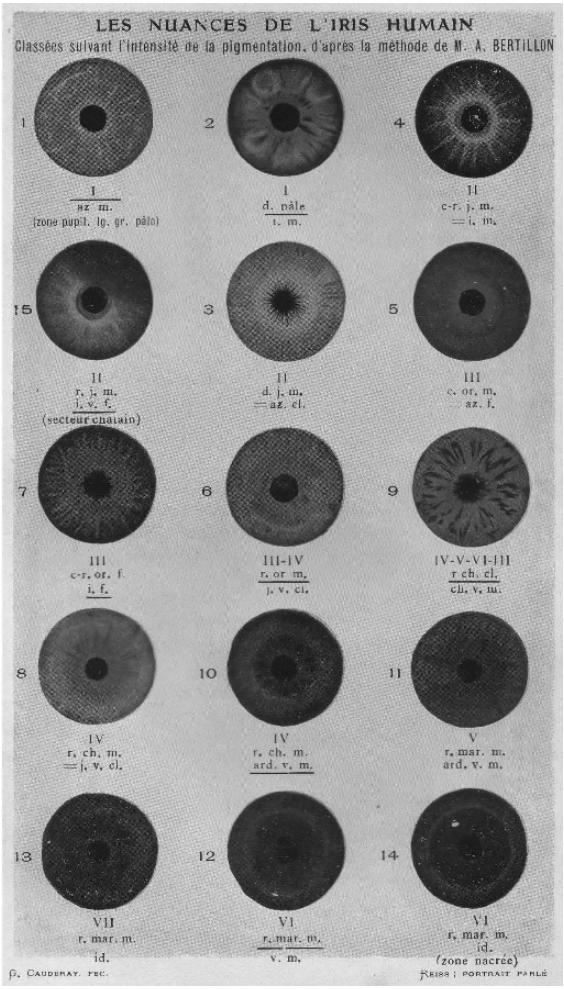

Fig. 21.4. Classification of the iris, classes are numbered I to VII (from [75]).

This classification method could allow theoretically up to 1,240,029 combinations ($3^{11} \times 7$). The measures taken on an arrested individual were registered onto an anthropometric card, together with the photograph, the name and a detailed description of peculiar marks, such as tattoos and scars. Each new card was then manually searched for one or more matches among the cards bearing identity (*case 1*). Bertillon established match criteria according to some tolerance values fixed by reference to variations recorded between operators. For instance, for ear measurements ±1mm was considered as an acceptable variation, ±2mm was a sign of divergence and ±4mm established non-identity (full criteria given in [58], p. 150-152).

It is important to stress that when among the known cards a match (within tolerance) with the unknown was found, the formal identification was only established following the examination of the photographs and the peculiar marks. In the same way that forensic biometric systems are used today, Bertillon's anthropometric approach was not an identification method per se. Indeed, Bertillon never claimed that the same set of measurements could not be shared by two different individuals [89]. It allowed the exclusion of potential candidates and acted as a powerful sorting system used to focus the attention of the investigators on a subset of cards deserving more attention, meaning a systematic analysis of the photographs and peculiar marks. Bertillon's approach was first deployed in 1882 and its efficiency proven by the considerable increase of the amount of habitual offenders identified through the assistance of the system: from 49 identifications in 1883, to 680 in 1892. This approach, recommended in 1885 for use in all French territory, attracted considerable attention abroad.

In parallel, Bertillon developed a standardized forensic photograph method, as well as a nomenclature for the description of the physiological features of the nose, the forehead and the ear, called "portrait parlé" or "spoken portrait" [11]. This standardized language offers description possibilities which can be used among police officers locally and internationally. Bertillon standardized photographic setup (focal distance, negative size, pose and illumination) and proposed taking two facial images, a frontal and a profile one, for each individual, noticing rightly that the profile image gave much more stable information for recognition than the frontal image [11]. Figure 21.5 presents the classification method for the ear, considered as the most identifying part of an individual, as proposed by Bertillon and taken up by Reiss [75]. The combination of the anthropometric method, the forensic photography and the spoken portrait was coined "Bertillonnage". Further bibliographical references to the work of Bertillon on anthropometry and its relationship with fingerprinting can be found in [24, 42].

A rapid spread of Bertillonnage was observed at the turn of the 20^{th} Century across the police departments and penal institutions [28]. This deployment quickly highlighted the limitations of the technique: (*i*) uneven distributions of the measures in the population; (*ii*) the correlation between features; (*iii*) inter-operator variations due to lack of training, instrumentation or non-cooperative subjects and (*iv*) the need of the body and the absence of anthropometric "traces" left on crime scenes.

The deployment of forensic anthropometry was successful but carried out after careful, fit-for-purpose, evaluations. During the same period, fingerprinting started to gain recognition for the same purpose. Hence prominent individuals such as Galton in England, Vucetich in Argentina, or specific committees (Troup and Belper (England), Straton (India Colonial Gov.), Dastre (France)) were tasked to assess the merits of Bertillon's method and prepare

Fig. 21.5. Classification of the shapes of the ear, here the classification of the antitragus (from [75]).

recommendations for their government. The outcome of these assessments, although initially in favor of Anthropometry due to the lack of fully efficient large-scale classification systems for fingerprints, led to the progressive substitution of Bertillonnage by fingerprinting for the advantages that will be detailed in the next section. Even though Bertillon regarded fingerprints with skepticism as the right choice for classifying and searching individuals in large databases, he included them on his anthropometric cards in 1894, convinced of their value in identification as a complement to the individual distinctive marks (tatoos, scars, etc.) and was thrilled by the possibilities to identify offenders based on the fingermarks left at crime scenes. Bertillon is known for the first fingerprint identification in France (1902) based on fingermarks recovered on a murder scene [83].

21.3 Fingerprinting

21.3.1 Ten-print identification systems

Historically [10] the first classification attempt was proposed by Purkinje in 1823, who sorted the friction ridge flows into nine categories: *arch*, tented arch, two types of *loops*, four types of *whorl* and twinned *loop*, for description purposes and without realizing the identification potential of the friction ridge skin. Fifty years later, William Herschel, a colonial administrator in India, proposed fingerprints to identify individuals, while undertaking the first study of permanence (i.e. the fingerprint features do not change over time) [43]. At the same time, Henry Faulds, a medical missionary in Japan, proposed in 1880 to use fingerprints for investigative identification purposes, as fingermarks could be detected on crime scenes [35]. His important contribution remained largely undervalued by his peers.

The main forensic operational contribution came from the work of Galton [39]. He presented in 1892 the basic axioms of fingerprinting, which are the notion of permanence (based on Herschel's work and data), and uniqueness (Galton published the first statistical model on the fingerprint variability). He also mentioned the possibility to reliably classify fingerprints patterns into three basic patterns (*arches*, (inner and outer) *loops*, and *whorls*).

Note that the research on forensic fingerprinting concentrated first on its use as an identification system based on reasonable quality ten-print cards obtained from living or dead individuals (hence *case 1* only). The use of lower quality information (in *case 2* or *3*) from marks recovered on crime scenes, for example, was viewed as a beneficial side effect but without being approached systematically at the outset.

The first classification method proposed by Galton was judged unsuitable to handle large collections of individuals. The method was then drastically improved by Henry (helped by his Indian colleagues), who added a fourth group, called *composites* and refined ridge counting (for loops, the number of ridges crossed on an imaginary line between the core and the delta) and ridge tracing methods (relative positions - classified in three categories: inside, outside and meet - of the right delta relative to the core when ridges and furrows are followed from the left delta). The classification is achieved through a series of imbricated classifying features, namely primary, secondary and sub-secondary classifications and major and final divisions. The primary classification consists of a ratio: the numerator is related to the number of whorls and their position on the even numbered fingers, while the denominator is related to the whorls on the odd numbered fingers. The secondary classification is also a ratio giving the pattern type of the index fingers, as well as an indication of all tented arches, arches and radial loops in other fingers. The fingers of the right hand go into the numerator, while those of the left hand go into the denominator. The sub-secondary classification, the major and final divisions are subsidiary classifiers based on ridge counts or

ridge tracing. This Galton-Henry classification largely gained acceptance for handling large databases such as the FBI central repository [91].

Almost simultaneously, Vucetich elaborated on Galton's proposal and offered a simpler method. General pattern main classification consisted of four basic patterns: *arches*, (internal and external) *loops* and *whorls*, organized in a ratio with a numerator devoted to the right hand and a denominator dealing with the left hand. As secondary classification, Vucetich divided each primary pattern into subclasses using ridge counts on loops and ridge tracing on whorls [96]. Vucetich's system proved very successful for small to medium sized databases.

Argentina adopted fingerprints (and Vucetich's classification method) as the sole method of identification of recidivists in 1896, while Great Britain (first in its overseas colonies) adopted Galton-Henry's system from 1897. In almost all agencies, fingerprint classifications were inspired from either one or the other original systems, but were adapted from country to country. Locard published an overview of the state of affairs in 1909 [58].

Standardization was a big issue already and had to wait until 1914 to see an uniform format for ten-prints cards: positioning of right hand fingers prints (from left to right beginning with the thumb) on a first line, left hand fingers (with the same fingers' order) on a second line, and controlled prints on the bottom of the ten-print card with two flat appositions of all the fingers (called *flaps*).

21.3.2 From ten-prints to single print manual searches

Telegraphic transmission of results of such classifications were not easy, hence 10 simple alphanumerical codes were developed for a 10-finger card. The most widely known is the codification of the National Crime Information Center (NCIC) dating back to 1967 based on the Galton-Henry classification. The NCIC code gives alphanumeric assignments from the right thumb (finger ♯1) to the left little finger (finger ♯10). This detailed NCIC fingerprint classification code was easily transferable between agencies and offered unprecedented efficiency to check if an unknown individual arrested in Washington DC could be known in Las Vegas (based on its NCIC classification).

These classification systems of fingerprints were above all, as the anthropometrical approach, sorting systems of full records obtained from the 10 fingers. These comparisons - known as ten-print to ten-print - were efficient only when the input data was complete (or almost). In other words, efficiency was achieved for *case 1*, but when input data consisted of, for example, a poor quality single mark recovered from a crime scene, the retrieval efficiency was more limited (when no suspect was available). Hence ten-print classification systems lacked efficiency for both *case 2* and *case 3*. The solution lay in the development of single-print classification systems (such as Battley [9]). They

were very demanding in terms of manpower and "cold" searches against the database based on a single mark were still very costly in terms of time.

21.3.3 Development of AFIS systems

Automatic fingerprint processes are already presented in Chapter 2. This section will thus concentrate only on the first automation attempts as well as the specific standardization efforts in the area. The book by Komarinski serves as an introduction to forensic AFIS systems [52].

With the increase of ten-print card collections and the difficulties of single latent searches, the evolution of automatic (analogue or digital) retrieval processing systems took off in parallel with the technological advances. Manual systems were improved by the use of punch card retrieval systems, the addition of videofiles for images (Ampex bands) and in the late sixties the first efforts to digitize and automatically process fingerprint images were made. Several computer-based fingerprint comparison systems were developed concurrently in many countries and these initiatives laid down the basis of modern Automatic Fingerprint Identification Systems (AFIS). For example, in the United States, the Project SEARCH (System for Electronic Analysis and Retrieval of Criminal Histories) has been allowed to finance, coordinate, and supervise research projects in this area [36]. The National Bureau of Standards (now known as the National Institute of Standards and Technology NIST) and the FBI proposed in 1968 a computer matching fingerprint system, based on minutiae features. The work by Wegstein et al. still remains a cornerstone of the development of AFIS [64]. The development work towards the Printrak system (now owned by Motorola) also dates back to these early years [99]. In France, Thiebault presented in 1967 a first computer matching fingerprint system, based on minutiae features and their spatial relationship [90]. This approach led to the development of the Morpho system (now part of Sagem) [79]. Likewise, researchers in Japan proposed a computer matching fingerprint system based on minutiae features, that served as a basis for the NEC AFIS [8].

All forensic AFIS are largely based on minutiae matching. The extracted template encompasses mainly the x,y coordinates of detected minutiae, their orientation and, for some providers, the ridge counts between minutiae. The main advantages of an AFIS are the ability to compare a single print, as well as a ten-print card to the whole database, hence covering all types of *cases*. We recall that although an AFIS provides a list of best candidates (according to a scoring/ranking metric), the identification process is not completed by the system, but manually by an expert (through a dedicated user interface). Of course, advances in computer technologies have increased speed and efficiency of the encoding and retrieval. Computational power allows now the use of both rolled and flap impressions and the introduction of palm marks and prints in AFIS and above all with a very quick response time and high reliability. Operational efficiency has been monitored by law enforcement agencies [13, 51,

56, 74]. Benchmarking has allowed monitoring of progress and improvements in this field. The NIST is today a reference in this area[3].

Standardization of forensic AFIS technology gained large momentum when fierce competition between providers brought to the fore the difficulties of interoperability between systems both nationally and internationally. The ANSI/NIST ITL-1 2000 standard manages the interoperability between all proprietary minutiae classification methods [6]. It also includes recommendations regarding data interchange of facial, scar mark and tattoo (SMT) information. This standard proposes the classification in fourteen pattern types, four minutiae types, with a localization (x,y-coordinates) and a direction (angle). The standard is currently under review and additional features beyond minutiae will be added to the ANSI/NIST ITL-1 2006 standard for the next generation AFIS. The extended features proposed[4] are finer classification of general patterns, additional ridge path elements, ridge flow quality for detecting open fields (areas without minutiae) and a larger spectrum of features (dots, incipient ridges, creases, scars, ridge shapes and width,...).

Another driving force is the willingness to provide this specific market with devices of known and recognized qualities. For example the FBI recommendations on the image quality specifications [30] propose (for fingerprint scanners) specific characteristics on geometric image accuracy, modulation transfer function, signal-to-noise ratio, range of gray-scale, gray-scale accuracy and output gray level uniformity. Furthermore, to archive large fingerprint databases, an efficient compression algorithm was required. The FBI proposed the Wavelet Scalar Quantization (WSQ) image compression algorithm as a way to standardize the digitization and compression of gray-scale fingerprint images [17]. This algorithm, capable of compressing images in the recommended 15:1 ratio, is based on discrete wavelet transform decomposition, scalar quantization and Huffman entropy coding. It is expected that WSQ will be replaced by JPEG2000 in a very near future.

The last big shift in technology is the widespread provision of livescan devices for law enforcement agencies to acquire ten-print forms instead of using the traditional procedure of inking fingerprints on paper. The use of small livescan devices for border control or police control is increasing rapidly (in Switzerland e.g. [71]).

21.3.4 A snapshot on the Swiss national fingerprint identification database and processes

Table 21.2 presents the statistics of the Swiss fingerprint criminal justice database for 2005[5]. 694,788 ten-print (TP) cards, provided from Swiss can-

[3] `http://fingerprint.nist.gov/`

[4] `http://fingerprint.nist.gov/standard/cdeffs/index.html`

[5] The statistical data on the Swiss fingerprint criminal justice database were kindly provided by Dr Axel Glaeser, Managment AFIS DNA Services - Federal Office of Police.

tonal police departments and from asylum centers, as well as 28,107 two-fingerprint (2-FP) sets and 34,485 latent prints, are stored in the Swiss fingerprint database. The 2-FP sets are used for identification purposes for police, border controls or embassy visa requests based on livescan images of two fingers. Due to legal regulations, only a fraction of them can be kept in the national database. Furthermore, for each latent print, about three encoded searches are stored in the database, which corresponds to about 10,000 unsolved fingermarks. Most transactions have been requested through police investigation, either for TP searches (28,005 requests in 2005) or 2-FP searches (38,131 requests in 2005). The annual numbers of requests for asylum or border control transactions are smaller (8,907 TP searches and 23,747 2-FP searches respectively). 14,500 TP versus TP matches (*case 1*) have been obtained from these transactions during a year, as well as 1,444 identification of latent prints versus TP or TP versus latent prints (*case 2*). Around a quarter of these hits result from TP versus latent transactions. The number of latent identifications includes about 233 matches with palm prints. Until now, latent prints were not compared to other registered latent prints (*case 3*), but some tests are currently being conducted to evaluate the benefits of such comparison in a Swiss perspective [7]. 22,202 and 5,383 2-FP matches have been obtained from the police and border control/embassy transactions respectively.

The average response time is about 3 to 10 minutes for 2-FP transactions, maximum 4 hours for TP transactions, and about 4 working days for latent transactions (urgent cases are processed within a couple of hours). For reasons of quality control, two fingerprint experts work on each latent case independently.

Records		
TP	2-FP	Latent
694,788	28,107	34,485
Transactions		
Police	Asylum	Border control
28,005 (TP) 38,131 (2-FP)	8,907 (TP)	23,747 (2-FP)
Hits		
TP-TP	Latent-TP / TP-Latent	2-FP
14,500	1,444	22,202 (Police) 5,383 (Border control / Embassy)

Table 21.2. Statistics for 2005 of the Swiss fingerprint criminal justice database.

21.3.5 Recent research on evidential value of fingerprints

The weaknesses of the statistical models developed to date in fingerprint identification have motivated recent research projects [87]. These have as main objective the assessment of the evidential contribution of fingermarks that can be partial, distorted, and with a poor signal/noise ratio. Although conclusions in the fingerprint area have traditionally been categorical, there is no obstacle to treat that type of evidence from a probabilistic perspective as discussed by Champod and Evett [22].

The strength of evidence is evaluated by a likelihood ratio according to the within- and between-sources variability of three or more minutiae [66, 67]. The feature set consists of the type of minutiae, their location, orientation and relative position, avoiding strong independence assumption. Fingerprint images acquired under different distortion conditions and feature sets generated artificially using a distortion model, have been used to model the within-source variability of the feature set. To model the between-sources variability of the feature set, fingerprints from randomly selected individuals from a criminal justice database have been used. The forensic qualities of the system have been assessed by studying simulations of the distributions of the likelihood ratios. This can be done considering the respective propositions of identity or non-identity of sources, combined with the estimation of the rates of misleading evidence ($RMEP$ and $RMED$). The results demonstrate that even partial fingermarks with three minutiae can contribute significantly to the evaluation of the strength of evidence for forensic cases. The performance increases with the number of minutiae.

21.4 DNA

Deoxyribonucleic acid (DNA), a chain of nucleotides contained in the nucleus of our cells, can be used as a biometric tool to classify and guide the identification of unknown individuals or biological samples left by them. The analysis of the DNA molecule in forensic science is called forensic DNA profiling. The book, "Forensic DNA Typing", by Butler [19], is an exhaustive and up to date reference. The objective of this section is to introduce the concepts and highlight how DNA analysis differs from biometrics. We will concentrate on DNA contained in the nucleus and the analytical processes that have led to large forensic databases. For the use of mitochondrial DNA, mini-STRs, Y-specific STRs and *single nucleotide polymorphisms* (SNPs), the reader should refer to [19].

DNA contains in its coding parts the genetic instructions allowing the encoding of different biological functions. About 32,000 genes are part of the human DNA. The nucleotide chain (about three million pairs of nucleotides) enables the encoding of sequences of amino acids in all proteins required for

cellular life. The gene pool of each individual is transmitted by his/her biological parents: a half by the father and the other half by the mother.

Non-coding parts, which represent about 98% of the total DNA, contain at different locations (*loci*) highly variable number of repetitive sequences, called *Short Tandem Repeat* (STR) which have a large polymorphism. At a given locus, one individual will show two specific numbers of repetitions of the given sequence of nucleotides. These two numbers called (*alleles*) give the biometric template for that locus. Note that one allele results from the genetic transmission from the biological father, while the biological mother transmits the other. When both alleles are identical, the individual is *monozygote* (at that locus), and when they are different, the individual is termed *heterozygote* (at that locus). Currently, most forensic DNA profiling systems used for database purposes are based on the analysis of STRs. The advantage of using STRs is that they are stable within individuals, but vary greatly between individuals. STR population genetics are well documented, and when located on different chromosomes, STRs have shown robust independence from a statistical perspective. They can hence be combined to achieve a very high discrimination power. The template for a DNA profile obtained with a STR profiling system is then a simple string, as in Table 21.3.

D3		**VWA**		**D16**		**D2**		**D8**	
12	13	16	17	10	11	18	19	8	9

D21		**D18**		**D19**		**THO1**		**FGA**	
26	27	14	15	10	11	5	6	29	30

D3		**VWA**		**D16**		**D5**		**D8**		**D7**		**TPOX**	
14	15	20	21	10	13	6	7	15	16	10	10	10	12

D21		**D18**		**D13**		**THO1**		**FGA**		**CSF1PO**	
27	31	19	19	23	24	6	7	24	24	6	6

Table 21.3. Example of a DNA profile obtained with a 10-loci system (SGM Plus 10 loci system used for the UK national DNA database) at the top and, below, with a 13-loci system (core STR markers for the US/FBI Combined DNA Index System - CODIS). Note that both systems share the same 8 loci. Currently the number of STRs used in commercial kits can amount to 16 loci.

Nuclear DNA can be extracted from all biological tissues. For living persons, a buccal swab is the easiest non-invasive way to obtain reference material. Profiles can be generated from biological stains or cells left behind at crime scenes, typically stains of blood, saliva, urine or semen, from hairs (with roots) and from skin cells (left by mere contact e.g. such as a fingermark). Obtaining DNA samples from living or dead bodies generally does not constitute a difficulty. For traces left behind, the location and retrieval is done manually, by visual examination (helped by the use of specialized light sources and magnification), and using presumptive tests. Traces are also more prone

to DNA degradation and interference during the extraction or amplification process. It means that for low-quantity or degraded samples, the DNA profile obtained may be partial (not all loci allow allelic designation) and/or mixed (when more than one individual contributed DNA to the sample). In all cases, the template will maintain the same format with either limited information or more than two alleles detected at one or more locus.

The extracted DNA is amplified using a sensitive and selective DNA replication method known as the *Polymerase Chain Reaction* (PCR). It is used to amplify, through multiple thermal cycles (between 28 to 34), the selected STRs for all loci in a multiplex way. This amplification provides extraordinary sensitivity, theoretically, even down to the detection of a single DNA molecule. In practice, sensitivity to levels below 100 pg of DNA (a few cells) can be achieved. The benefit is evident: it allows obtaining profiles from very limited amounts of DNA, hence widening the investigative possibilities in difficult cases. The drawback lies in the technical capacity to amplify not only the relevant DNA but also background DNA left for reasons not linked to the alleged activities of forensic interest.

The detection of these amplified repetitive sequences is completed by *capillary electrophoresis* (CE) and fluorescence detection. CE is an analytical technique that separates charged DNA amplified fragments according to their size, by applying voltage across buffer-filled capillaries. The whole DNA profiling process requires specialist laboratory staff, costly analytical equipment and a minimum of 12 hours. Automation of most parts of this procedure is achievable with current technology, but still requires some hours of processing time.

DNA profiles can easily be arranged in databases for law enforcement purposes or the management of large disasters (such as the 9/11 terrorist acts or the 2005 tsunami). The American FBI CODIS now has more than 4 million profiles from individuals and 150,000 crime scene sample profiles[6]. The UK national DNA database reaches more than 3 million subjects and a yearly rate of crime scene submissions of about 50,000 profiles [65]. These are the two largest national DNA databases in use.

Seven STR loci were selected by the European Network of Forensic Science Institutes (ENFSI) and Interpol [47] to ensure a minimal consensus on databasing in Europe. The American FBI CODIS database is built on thirteen loci, including the seven selected by the ENFSI. This standardization ensures a relative interoperability between all countries, in order to enable collaborations between jurisdictions for forensic cases. Even if a consensus on a restricted set of loci has been adopted, the nature of the population registered on national DNA databases (i.e. the introduction criterion for profiles in these databases) differs greatly from state to state, especially in Europe [98]. Some member states incorporate in their databases all individuals suspected or arrested for any recordable offences, such as the United Kingdom,

[6] `http://www.fbi.gov/hq/lab/codis/`

while other states register only individuals convicted for crimes and offences sanctioned by imprisonment, such as Switzerland.

Table 21.4 gives the 2005 statistics of the Swiss DNA criminal justice database managed with the CODIS software (but based on the SGM Plus STR system)[7]. 69,019 DNA profiles from known individuals, with 11,125 unresolved stain profiles, provided by Swiss cantonal police departments are stored in the Swiss DNA criminal justice database. About 15,000 DNA profiles and 5,000 crime scene profiles have been compared to the database in one year, from which 2,800 crime scene to person and 2,100 crime scene to crime scene matches have been obtained.

Records	
Profiles	Crime scene
69,019	11,125
Transactions	
Profiles	Crime Scene
15,000	5,000
Hits	
Crime scene-Person	Crime scene-Crime scene
2,800	2,100

Table 21.4. 2005 statistics of the Swiss DNA criminal justice database.

When there is no need to consider relatives or mixtures, the matching process is straightforward: for a match to be declared, all alleles from the unknown profile should correspond to the profile from the known. Currently, most operational forensic DNA matching systems are based on the search for equalities. Research is currently under way to improve searches with degraded profiles, mixed profiles and when only relatives are available. Forensic applications of DNA are wide, as presented in Table 21.5.

It is important to stress that a match between two DNA profiles does not conclusively establish the identity of sources. Indeed, although the selectivity of DNA profiling is very high, there exists a probability for an adventitious association. The methods for computing match probabilities have received considerable attention among scholars and, after some initial controversies, gained general acceptance. A full account of these methods, including the use of likelihood ratios, is given in [37, 97]. In general terms, for a complete unmixed DNA profile, the predicted random match probability with unrelated individuals is in the order of 1 in a billion [38]. However, note that the match probabilities are of a complete different order of magnitude for relatives. For

[7] The statistical data on the Swiss DNA criminal justice database were kindly provided by Dr Axel Glaeser, Managment AFIS DNA Services - Federal Office of Police.

Activity	**Levels of selectivity of the information**
Comparison of the DNA profile of unknown individuals against profiles from known individuals.	*High* when the collected DNA is not degraded, (provides a full profile on all analyzed loci). *Lower* when part of the DNA available is degraded, hence giving a partial DNA profile.
Comparison of the DNA profile obtained from human remains (missing persons or disaster victims) against profiles from known missing persons or relatives thereof.	*High* as above when the comparison is made against DNA profiles from known missing persons. *Lower* when part of the DNA available is degraded or when the data used as reference are provided through blood relatives (at various levels).
Filiations testings (paternity, maternity and any types of blood relationship)	*High* when the direct putative genitors are available. *Lower* when the DNA profile from one or both putative genitors is informed from data collected among his/her blood relatives (ancestors or descendants).
Comparison of DNA profile obtained from biological stains, material or contact traces recovered in association with criminal activities against profiles from known individuals.	*High* when the recovered material is in large quantity and its analysis lead to a full unmixed DNA profile. *Lower* when the recovered material is of low quantity or degraded and consequently offers a partial DNA profile. Equally when the sample gave a mixed DNA profile of 2 or more contributors.
Forensic intelligence gathered through the systematic comparison of DNA profiles coming from various scenes. Familial searches on the DNA database.	Depending on the quality of the DNA information obtained.

Table 21.5. Inventories of the forensic applications of DNA profiles.

the SGM Plus system (10 loci), an average match probability for a potential brother/sister is 1 in 10'000.

For assigning statistical weights to relationships based on DNA mixtures or filiation cases, refer to [97]. As a general principle, when the quality of the information decreases, the weight of the DNA findings tends to decrease as well. Hence, the more the DNA is partial or distant in terms of genetic relationship, the higher the uncertainty. With DNA, the selectivity of the available information can be assessed by its extent (quantity of DNA and number of loci) and the amount of predicting information allowed by the profiles obtained from relatives.

21.5 Voice

Forensic speaker recognition is the process of determining if a specific individual is the source of a questioned occurrence. Typically, forensic speaker recognition by experts relies on a variety of techniques (used alone or in combination), such as aural comparison (careful listening), semi-automatic methods for extraction of certain parameters (e.g. formant frequencies, average fundamental frequencies, pitch contour, etc.), visual comparison of spectrograms, and automatic speaker recognition (computer-based) [53, 62, 76]. Three main processes can be used in forensic speaker recognition: the auditory (also known as aural perceptual), semi-automatic (also known as auditory instrumental) and the automatic analysis.

In *auditory* analysis, trained phoneticians carefully listen to recordings and use the perceived differences in the speech to form an opinion about their similarity [68]. They base their judgment on parameters such as the voice (e.g. timbre and pitch), speech (e.g. articulation and speech rate), language (e.g. prosody and style) and linguistic characteristics (e.g. syntax and breathing). This is a challenging task requiring training and a careful ear. Voice comparison by untrained (also called naive) listeners is not often used in forensic cases, although they have shown to perform well in certain conditions [5].

In *semi-automatic* analysis, the experts measure various acoustic parameters, such as average fundamental frequency, vowel formants, pitch contour, spectral energy, etc. They assess those characteristics either subjectively or objectively, using signal processing tools to quantify them. They can even combine approaches to formulate their conclusions, according to verbal probability equivalents [40]. One of the semi-automatic methods, which uses visual spectrographic comparison (popularly known as "voice printing"), has come under severe criticism in recent years. It consists of visually comparing graphical representations of spectrums of identical speech utterances. It was first proposed in 1962, and some weak points, such as the large variability of these spectrograms for a same individual and the fact that the visual representation of these spectrograms is not specifically speaker-dependent, were quickly highlighted. In 1976, the US National Academy of Sciences recommended that this approach should only be used in forensic cases with utmost caution [15]. A strong word of caution is certainly deserved [16].

In terms of *automatic* speaker recognition, two types of approaches are available, as mentioned in Chapter 8: the text-dependent and the text-independent (often required in forensic cases). Several feature characterizations and statistical modeling tools have been developed for automatic speaker recognition and have been successfully applied to forensic cases [33, 54]. Automatic methods perform well in similar recording conditions, but are sensitive to distortions due to recording and/or in transmission conditions. In forensic cases, the recording conditions of the trace and the reference materials are rarely similar and ideal, but rather recorded in different and unconstrained conditions [4], e.g. through mobile communications (GSM) transmission and

with background noise. Due to these factors, the comparison is often undertaken under adverse conditions.

As with other forensic fields, a likelihood ratio-based approach was proposed for forensic speaker recognition [26] and gained acceptance among practitioners [76]. The proposed statistical-probabilistic methodology uses three different databases, in addition to the digital trace [33, 41, 63]: a suspect reference database (R), a suspect control database (C) and a potential population database (P). The P database is used to model the variability of the potential population. The R database is used to model the variability of the suspect's voice, according to the recording conditions of the P database. The C database is used to evaluate the variability of the suspect's voice, according to the recording conditions of the trace. The similarity scores, obtained by comparing the recordings of databases C and R, model the within-source variability, while those obtained by comparing the recordings of database P to the trace, model the between-sources variability. The score obtained by comparing the trace to the model of the suspect's voice, created with database R, gives the evidence E. The LR is computed by the ratios of the heights of the probability densities of the within- and between-sources distributions at a score of E. The LRs obtained with this methodology can assess the common origin of two speech signals in a specific forensic case. The readers can refer to [4, 32, 63, 76] and to Chapter 8 for further reading and additional bibliographical references on forensic and non-forensic speaker recognition.

21.6 Face and ear

As presented in Section 21.2, the face was already used at the end of the 19^{th} century for forensic discrimination purposes. Bertillon standardized the lighting conditions, as well as the posture of the subject. He proposed that two facial images were taken for each individual, namely a frontal and a profile (with the latter considered as more reliable).

21.6.1 Non-automatic forensic face recognition

Forensic face recognition was until recently generally performed by human operators using different approaches [48, 100]: morphological analysis of facial structures, anthropometric measurements and superimposition of images.

The *morphological analysis-based* approach can be described as the scientific follow-on to Bertillon's spoken portrait (Section 21.2). It is based on a nomenclature for the description of the physiological aspects of the nose, the forehead and the ear. The morphological classification describes facial physiological characteristic, such as the facial shape, the hairline, the forehead height and width, the mouth and the chin shapes, the nose length, breadth and shape, and the ear size and form. These characteristics can be described, using the following sets of terms: "none, few, moderate, extreme; small, medium, large;

absent, slight medium, pronounced; thin, average, thick". In addition, information such as facial wrinkles, can also be used. As this description is rather subjective, variations were observed between the descriptions of a same set of photographs made by operators for some features [95]. According to these authors, other features were nevertheless proven to be invariant between operators and to have some discriminating power, without explicitly specifying these features. Additional limits of this approach are the variability of the features for an individual due to changes in expression, photographic angles and changes due to aging. It is difficult to determine if these features are statistically independent [48].

The *anthropometric-based* approach can be described as the quantification of physiological proportions between specific facial landmarks. This method is only used for the comparison of faces having the same orientation. These landmarks are for example the midpoint of the hairline, the most anterior point of the forehead, the deepest point of the nasal root, the most anterior point of the nose tip, the midpoint of the occlusal line between the lips, the most anterior and inferior points of the chin, the corners of the mouth and the most superior, inferior and posterior points of the ear [48]. Other landmarks can be chosen, as long as they are clearly visible on the facial images. In order to avoid any scale and absolute size differences between photographs, relative ratios should be calculated from these landmarks. The use of the maximum dimension as denominator for each of these ratios is recommended for linear measurements. Even if the quantifications of these proportions reduce subjectivity, some problems still remain. Lighting conditions, camera distortions, camera positioning, facial orientation, facial expressions and aging may result in different ratio values. However, the main problems are the high correlation between some measurements and the lack of statistical data to determine the relative contribution of these measurements in a specific population [60]. Anthropometric measurements could be used for forensic purposes if these problems were resolved.

The *image superimposition-based* approach is the juxtaposition or the superposition of facial images, taken under similar acquisition conditions (the orientation, pose and size) in order to verify the correspondence of the facial features. This approach is either represented by an image where both 2D facial photographs are vertically or horizontally juxtaposed, or by an animation where the first photograph appears and then disappears into the other. This latter demonstration tool should not be used to assess a correspondence between two facial images, because of the subjectivity generated by such visualization. Matches are not only based on a superimposition correspondence, but significant features matches need to be included as well, such as ears and scars [94]. However, the superimposition-based approach is considered as the least accurate facial comparison method [48]. The comparison between photographs can be reliably performed only if they were taken under the same conditions and with identical poses. A solution to these issues, a 2D/3D approach has been developed. It consists of modeling the 3D shape of the

suspect's face and comparing it to the 2D questioned facial image [100]. The advantage of this method is that it is possible to adjust the pose and orientation of the suspect's face to the facial image. Furthermore, some objective computer-assisted matching criteria can be obtained with this approach.

21.6.2 Automatic forensic face recognition

The three main comparison approaches discussed in Section 21.6.1 do not consider automatic face recognition, except the 2D/3D superimposition approach described above. Automatic face recognition can be described as a visual pattern recognition problem, where selected facial features of a query image were compared to the features of a reference image or a database. As presented in [57], face recognition attempts to represent the complex multidimensional features extracted from the image of a face in simpler and more general representations using e.g. principal component analysis (PCA), shape and texture or Gabor wavelets, and to perform the classification between the different patterns using e.g. Bayes, linear discriminant analysis (LDA), independent component analysis (ICA) or Graph matching. The contribution of such systems in surveillance activities and access control (see Chapter 3), especially with the performance improvement highlighted recently with the Face Recognition Vendor Test (FRVT) 2006 [72], will gain more and more importance. However, we will only mention one attempt of using automatic face recognition in an evaluative and *LR*-based framework [70]. The experiments of this study were based on a small set of subjects, recorded under fixed constraints with passport type photographs. The conditions generating the most significant variations in facial images (i.e. illumination, pose, expression, age, image quality,...) in forensic scenarios were not explored in a large scale scenario.

As ruled by the UK Court of Appeal Criminal Division decision in *R. v. Gray* ([2003] EWCA Crim 1001), an adequate evaluation methodology for face recognition, based on reliable statistical data, is needed. Our view is that automatic face recognition systems will have a large role to play here. Before automatic face recognition is accepted in court, a full and systematic assessment of the technology must be conducted under realistic conditions using fit-for-purpose forensic efficiency measures.

21.6.3 Ear

The ear was considered by Bertillon as the most identifying part of an individual (see Section 21.2). This modality was then quickly used for identification purposes in forensic cases. This identification can be based on photographs (or still images from video recordings) or based on earmarks left at crime scenes (for example when a burglar presses his ear against a door or windowpane to listen into a room). Forensic ear comparison is traditionally performed by

skilled examiners. The principles and protocols for ear and earprint examination can be found in [46, 92].

The identification is mainly demonstrated by overlaying transparent known and unknown images or by using a photomontage of various sections of the ears. There is a big difference in terms of selectivity between a well-taken photograph of an ear and its impression on a door (see Figure 21.1). However, to date there have not been sufficient systematic studies about forensic identification decision making using these impressions. Thus the evidential contribution of earmark to earprint comparisons has been criticized [23]. The large variability of the ear morphology has been covered well in the literature, but the variability of earmarks has been relatively poorly treated. This is also the same with within-subject variations. A recent Court of Appeal judgment[8] expressed some reservations as to the absolute strength of the earmark evidence presented. For the comparison between video recordings of ears, a recent study has shown how the quality of the video images determine to a large extent the ability to identify a person [44].

The first forensic earmark recognition proof of concept was presented in [23], it uses the antihelix area of the mark to extract some features, such as the width, the height and the inner and outer contours. Another concept system is presented in [80]. It uses as features manually annotated intersection points between a grid and the mark or the print. A maximum of four points on the inner side of the helix, and four points on the outer side of the antihelix are selected. A polygon matrix based on these tags is calculated. The only performance data presented in this article refers to a verification protocol where the earmarks tested were always identified at a 100% probability match (highest score) to the corresponding prints. The number of tests carried out and cases where marks were identified to non-corresponding prints at a 100% probability match were unfortunately not mentioned. The authors also propose alternatively the use of centroids for each separate earmark's part as features, in order to avoid the mark's variability due to pressure changes. The Forensic Ear IDentification (FearID) project (funded by the 6^{th} EU research framework) proposed to use weighted width, angular development and anatomical annotation as distinctive features for their semi-automatic system [3]. Manual annotations on the prints and marks are performed before the matching process to facilitate the segmentation of the images and to locate anatomical points. With a set 7364 prints and 216 marks from 1229 donors, this approach reached an equal error rate (EER) of 3.9% for lab quality prints, and an EER of 9.3% for simulated marks against the prints database. At this stage of research, to our knowledge, no operational system has been deployed in forensic services. For further reading on automatic ear recognition, refer to Chapters 7 and 16.

[8] *R. v. Dallagher* No (2002) EWCA Crim 1903, July 25.

21.7 Dental features

Dental features are heavily used by forensic odontologists for the identification of human remains in cases of missing persons or mass disasters [88]. The features used range from the standard dental record (indications of missing teeth, restorations, crowns,...) to dental radiographs that provide information about teeth, including tooth contours, relative positions of neighboring teeth, and shapes of the dental work. These anatomical features have shown very good stability and variability and the teeth serve as a suitable repository of the history of man-made operations that left various marks and shape changes. The diversity of the dental record features and their use for identification have been recently documented [1]. Alphanumerical data can easily be organized in databases and such systems are used operationally in cases of mass disasters.

The use of radiographs recently received attention from the biometric community with promising results [34, 27, 49, 69, 101].

The area of bitemark identification is covered in [31]. To our knowledge, no automatic feature extraction and matching procedures have been proposed to handle these marks.

21.8 Handwriting

The principles and procedures used by forensic experts to assign questioned handwritten documents to known individual are described in [45]. The forensic expert tries to assess existing similarities and dissimilarities between control and recovered samples through a subjective estimation of the individuality and variability of the material at hand. Again, such a subjective approach has come under criticism and the profession has been urged to move towards more objective measures of selectivity [82].

In this context, a few embryonic methods for databasing and systematically analyzing handwriting have been presented: the computer-based measurement and retrieval of letter shapes of the WANDA-system [93], the use of Fourier descriptors to discriminate between writers [61], the automatic identification of a writer by the use of connected-component contours [84] and the CEDAR-FOX identification/verification system [85, 86]. The scope for development is important both to provide tools to assist the evaluation of forensic evidence but also to bring investigative possibilities based on handwriting. Gannon Technologies Group recently announced a breakthrough in the area following research at George Mason University and the FBI[9].

No forensic attempts towards automation are known for signatures despite the very large development of biometric systems based on this modality (see Chapter 10).

[9] `http://gazette.gmu.edu/articles/8037/`

21.9 Discussion and perspectives

As presented in Section 21.1, forensic science and biometrics are differentiated by four main distinctions. First, forensic biometric systems are mainly used as sorting devices, presenting to the forensic specialist a short list of candidates, while traditional biometric systems report their conclusions with binary decisions ("accepted" or "rejected"). Secondly, adequate global measures ($RMED$, $RMEP$) should complement the assessment of the efficiency of forensic biometric systems (in addition to the traditional biometric measures such as ROC and DET curves). Thirdly, forensic biometric applications are characterized by the wide range of selectivity of the biometric data that are submitted, while traditional biometric systems use data acquired in rather controlled conditions. Finally, the last distinction concerns the range of comparisons that can be undertaken in the forensic environment depending on the circumstances of the cases.

Despite these differences, the same scientific principles and technical methods are used for handling biometric data in non-forensic and forensic applications. The research efforts undertaken in the biometric community will help to address the issues of the selectivity decrease encounter in forensic applications. Furthermore, multimodal approaches (see Chapters 14 to 16 and [77]) may handle not only the limitations of each single modality (i.e. intra-class variability, distinctiveness, non-universality, etc.), but the selectivity decrease as well, which occurs in forensic biometrics at distance for example. The application of multimodal approaches on forensic data should increase the reliability of such biometric systems in unconstrained conditions, for investigative and evaluation purposes.

Recognition at distance, based on biometric data, will quickly be the major component of forthcoming forensic inquiries. The UK Police Information Technology Organization (PITO) recommends the development of more effective tools to handle the large amount of Closed-Circuit Television (CCTV) images, not only for human identification, but also for crime detection and prevention [73]. New kinds of digital traces will thus be used for law enforcement purposes. While face and voice are already used as digital traces for human identification, modalities such as ear, iris and gait may also be involved in forensic science. The increasing forensic needs and the advances in the biometric research community mean that forensic science and biometrics will be more intertwined in the future.

Acknowledgments

The authors are grateful to Dr Axel Glaeser for providing us with statistical data on the Swiss fingerprint and DNA criminal justice databases and to Dr Anil Alexander for his valuable remarks and suggestions.

References

1. B. J. Adams. The diversity of adult dental patterns in the united states and the implications for personal identification. *Journal of Forensic Sciences*, 48:497–503, 2003.
2. C. Aitken and F. Taroni. *Statistics and the Evaluation of Evidence for Forensic Scientists*. John Wiley & Sons, Ltd, 2004.
3. I. Alberink and A. Ruifrok. Performance of the FearID earprint identification system. *Forensic Science International*, 166:145–154, 2007.
4. A. Alexander. *Forensic Automatic Speaker Recognition using Bayesian Interpretation and Statistical Compensation for Mismatched Conditions*. PhD thesis, Swiss Federal Institute of Technology, Lausanne, 2005.
5. A. Alexander, D. Dessimoz, F. Botti, and A. Drygajlo. Aural and automatic forensic speaker recognition in mismatched conditions. *International Journal of Speech, Language and Law*, 12(2):214–234, 2005.
6. ANSI/NIST. *ANSI/NIST-ITL 1-2000 Data Format for the Interchange of Fingerprint, Facial, Scar Mark and Tattoo (SMT)*. American National Standard Institute - National Institute of Technology, 2000.
7. A. Anthonioz, A. Aguzzi, A. Girod, N. Egli, and O. Ribaux. Potential use of fingerprint in forensic intelligence: Crime scene linking. *Z Zagadnien Nauk Sadowych - Problems of Forensic Sciences*, 51:166–170, 2002.
8. K. Asai, Y. Kato, Y. Hoshino, and K. Kiji. Automatic fingerprint identification. In *SPIE - Imaging Applications for Automated Industrial Inspection and Assembly*, volume 182, pages 49–56, 1979.
9. H. Battley. *Single Finger Prints*. H. M. Stationery Office, London, 1930.
10. J. Berry and D. A. Stoney. The history and development of fingerprinting. In R. E. Gaensslen, editor, *Advances in Fingerprint Technology*, pages 1–40. CRC Press, Boca Raton, 2001.
11. A. Bertillon. *La Photographie Judiciaire*. Gauthier-Villars et fils, Paris, 1890.
12. A. Bertillon. *Identification Anthropométrique et Instructions Signalétiques*. Imprimerie administrative, Melun, 1893.
13. B. Blain. Automated palm identification. *Fingerprint Whorld*, 28:102–107, 2002.
14. R. M. Bolle, J. H. Connell, S. Pankanti, N. K. Ratha, and A. W. Senior. *Guide to Biometrics*. Springer-Verlag, New-York, 2003.
15. R. H. Bolt, F. S. Cooper, D. M. Green, S. L. Hamlet, J. G. McKnight, J. M. Pickett, O. Tosi, B. D. Underwood, and D. L. Hogan. *On the Theory and Practice of Voice Identification*. National Research Council, National Academy of Sciences, Washington D.C., 1979.
16. J. F. Bonastre, F. Bimbot, L. J. Boe, J. P. Campbell, D. A. Reynolds, and I. Magrin-Chagnolleau. Person authentication by voice: A need for caution. In *Proceedings of Eurospeech 2003*, pages 33–36, Geneva, Switzerland, 2003.
17. C. M. Brislawn, J. N. Bradley, R. J. Onyshczak, and T. Hopper. The FBI compression standard for digitized fingerprint images. In *Proceedings of the SPIE*, volume 2847, pages 344–355, 1996.
18. B. Budowle, R. Chakraborty, G. Carmody, and K. L. Monson. Source attribution of a forensic DNA profile. *Forensic Science Communications*, 2(3), 2000.
19. J. M. Butler. *Forensic DNA Typing*. Elsevier Academic Press, Burlington, MA, 2005.

20. C. Champod. Identification/Individualization: Overview and meaning of ID. In Jay M. Siegel, Geoffrey C. Knupfer, and Pekka J. Saukko, editors, *Encyclopedia of Forensic Sciences*, pages 1077–1084. Academic Press, London, 2000.
21. C. Champod and I. W. Evett. Commentary on: Broeders, A. P. A. (1999) 'Some observations on the use of probability scales in forensic identification', Forensic Linguistics, 6(2): 228-41. *Forensic Linguistics*, 7:238–243, 2000.
22. C. Champod and I. W. Evett. A probabilistic approach to fingerprint evidence. *Journal of Forensic Identification*, 51:101–122, 2001.
23. C. Champod, I. W. Evett, and B. Kuchler. Earmarks as evidence: A critical review. *Journal of Forensic Sciences*, 46(6):1275–1284, 2001.
24. C. Champod, C. Lennard, and P. Margot. Alphonse Bertillon and dactyloscopy. *Journal of Forensic Identification*, 43(6):604–625, 1993.
25. C. Champod, C. Lennard, P. Margot, and M. Stoilovic. *Fingerprints and Other Ridge Skin Impressions*. CRC Press, Boca Raton, 2004.
26. C. Champod and D. Meuwly. The inference of identity in forensic speaker recognition. *Speech Communication*, 31(2-3):193–203, 2000.
27. H. Chen and A. K. Jain. Dental biometrics: Alignment and matching of dental radiographs. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 27:1319–1326, 2005.
28. S. Cole. *Suspect Identities: A History of Fingerprinting and Criminal Identification*. Harvard University Press, 2001.
29. R. Cook, I. W. Evett, G. Jackson, P. J. Jones, and J. A. Lambert. A hierarchy of propositions: Deciding which level to address in casework. *Science & Justice*, 38:231–240, 1998.
30. Criminal Justice Information Services Division. *Electronic Fingerprint Transmission Specifications CJIS-RS-0010 (V7)*. Department of Justice, Federal Bureau of Investigation, Criminal Justice Information Services Division, Washington, D.C., 1999.
31. B. J. Dorion. *Bitemark Evidence*. Marcel Dekker, New York, 2005.
32. A. Drygajlo. Forensic speaker recognition. *IEEE Signal Processing Magazine*, 24(2):132–135, 2007.
33. A. Drygajlo, D. Meuwly, and A. Alexander. Statistical methods and bayesian interpretation of evidence in forensic automatic speaker recognition. In *Eurospeech*, pages 689–692, Geneva, 2003.
34. G. Fahmy, D. E. M. Nassar, E. Haj-Said, H. Chen, O. Nomir, J. Zhou, R. Howell, H. H. Ammar, M. Abdel-Mottaleb, and A. K. Jain. Toward an automated dental identification system. *Journal of Electronic Imaging*, 14(4):043018, 2005.
35. H. Faulds. On the skin-furrows on the hands. *Nature*, 22:605, 1880.
36. R. D. Foote. Fingerprint identification: A survey of present technology, automated applications and potential for future development. *Criminal Justice Monography*, V(2):1–33, 1974.
37. L. A. Foreman, C. Champod, I. W. Evett, J. A. Lambert, and S. Pope. Interpreting DNA evidence: A review. *International Statistical Review*, 71:473–495, 2003.
38. L. A. Foreman and I. W. Evett. Statistical analyses to support forensic interpretation for a new ten-locus STR profiling system. *International Journal of Legal Medicine*, 114:147–155, 2001.
39. F. Galton. *Finger Prints*. Macmillian and Co., London, 1892.
40. S. Gfroerer. Auditory instrumental forensic speaker recognition. In *Proceedings of Eurospeech 2003*, pages 705–708, Geneva, Switzerland, 2003.

41. J. Gonzalez-Rodriguez, A. Drygajlo, D. Ramos-Castro, M. Garcia-Gomar, and J. Garcia-Ortega. Robust estimation, interpretation and assessment of likelihood ratios in forensic speaker recognition. *Computer Speech and Language*, 20:331–355, 2006.
42. K. Hashimoto. *De la classification à l'identification: Alphonse Bertillon (1853-1914) et l'anthropométrie judiciaire*. Mémoire de DEA d'Epistémologie, Histoire des sciences et des techniques, Université de Nantes, 2003.
43. W. Herschel. Skin furrows on the hand. *Nature*, 23:76, 1880.
44. A. J. Hoogstrate, C. van den Heuvel, and E. Huyben. Ear identification based on surveillance camera images. *Science & Justice*, 41:167–172, 2001.
45. R. A. Huber and A. M. Headrick. *Handwriting Identification: Facts and Fundamentals*. CRC Press, Boca Raton, 1999.
46. A. V. Iannarelli. *Ear Identification*. Paramont Publishing Company, Fremont, CA, 1989.
47. Interpol DNA Monitoring Expert Group. *Interpol Handbook on DNA Data Exchange and Practice*. International Criminal Police Organization, Lyon, 2001.
48. M. Y. Iscan. Introduction of techniques for photographic comparison: Potential and problems. In M. Y. Iscan and R. P. Helmer, editors, *Forensic Analysis of the Skull: Craniofacial Analysis, Reconstruction, and Identification*, pages 57–70. Wiley-Liss, New York, 1993.
49. A. K. Jain and H. Chen. Matching of dental X-Ray images for human identification. *Pattern Recognition*, 37:1519–1532, 2004.
50. P. L. Kirk. The ontogeny of criminalistics. *Journal of Criminal Law, Criminology and Police Science*, 54:235–238, 1963.
51. D. Klug, J. L. Peterson, and D. A. Stoney. Automated fingerprint identification systems: Their acquisition, management, performance and organizational impact. Report, National Institute of Justice, 1992.
52. P. Komarinski. *Automated Fingerprint Identification Systems (AFIS)*. Elsevier Academic Press, New York, 2005.
53. H. J. Kunzel. Current approaches to forensic speaker recognition. In *Proceedings of the 1st ESCA Workshop on Speaker Recognition, Identification and Verification*, pages 135–141, Martigny, Switzerland, 1994.
54. H. J. Kunzel and J. Gonzalez-Rodriguez. Combining automatic and phonetic-acoustic speaker recognition techniques for forensic applications. In *Proceedings of the 15th International Congress of Phonetic Sciences*, pages 1619–1622, Barcelona, Spain, 2003.
55. Q. Y. Kwan. *Inference of Identity of Source*. Phd thesis, Department of Forensic Science - University of California, Berkeley, 1977.
56. M. J. Leadbetter. The use of automated fingerprint identification systems to process, search and identify palm prints and latent palm marks. *Journal of Forensic Identification*, 49:18–36, 1999.
57. C. Liu and H. Wechsler. Face recognition. In J. L. Wayman, A. K. Jain, D. Maltoni, and D. Maio, editors, *Biometric Systems: Technology, Design and Performance Evaluation*, pages 97–114. Springer-Verlag, London, 2005.
58. E. Locard. *L'Identification des Récidivistes*. A. Maloine, Paris, 1909.
59. E. Locard. *L'Enquête Criminelle et les Méthodes Scientifiques*. Ernst Flammarion, Paris, 1920.
60. K. V. Mardia, A. Coombes, J. Kirkbride, A. Linney, and J. L. Bowie. On statistical problems with face identification from photographs. *Journal of Applied Statistics*, 23(6):655–675, 1996.

61. R. Marquis, M. Schmittbuhl, W. D. Mazzella, and F. Taroni. Quantification of the shape of handwritten characters: A step to objective discrimination between writers based on the study of the capital character o. *Forensic Science International*, 150:23–32, 2005.
62. D. Meuwly. Voice analysis. In J. M. Siegel, G. C. Knupfer, and P. J. Saukko, editors, *Encyclopedia of Forensic Sciences*, pages 1413–1421. Academic Press, London, 2000.
63. D. Meuwly. *Reconnaissance de Locuteurs en Sciences Forensiques: l'Apport d'une Approche Automatique.* PhD thesis, Université de Lausanne, 2001.
64. R. T. Moore. Automatic fingerprint identification systems. In H. C. Lee and R. E. Gaensslen, editors, *Advances in Fingerprint Technology*, pages 163–191. Elsevier Science Publishing Co., Inc., New-York, 1991.
65. National DNA Database. The national DNA database, annual report 2004-2005. Annual report, ACPO, 2006.
66. C. Neumann, C. Champod, R. Puch-Solis, N. Egli, A. Anthonioz, and A. Bromage-Griffiths. Computation of likelihood ratios in fingerprint identification for configurations of any number of minutiae. *Journal of Forensic Sciences*, 52(1):54–64, 2007.
67. C. Neumann, C. Champod, R. Puch-Solis, N. Egli, A. Anthonioz, D. Meuwly, and A. Bromage-Griffiths. Computation of likelihood ratios in fingerprint identification for configurations of three minutiae. *Journal of Forensic Sciences*, 51(6):1255–1266, 2006.
68. F. Nolan. Speaker identification evidence: its forms, limitations, and roles. In *Proceedings of the conference "Law and Language: Prospect and Retrospect"*, Levi (Finnish Lapland), 2001.
69. O. Nomir and M. Abdel-Mottaleb. A system for human identification from X-ray dental radiographs. *Pattern Recognition*, 8:1295–1305, 2005.
70. C. Peacock, A. Goode, and A. Brett. Automatic forensic face recognition from digital images. *Science & Justice*, 44(1):29–34, 2004.
71. P. W. Pfefferli. Rapid - Response - AFIS. In J. Almog and E. Springer, editors, *Proceedings of the International Symposium on Fingerprint Detection and Identification*, pages 225–256, Ne'urim, Israel, 1996.
72. P. J. Phillips, W. T. Scruggs, A. J. O'Toole, P. J. Flynn, K. W. Bowyer, C. L. Schott, and M. Sharpe. FRVT 2006 and ICE 2006 large-scale results. Technical report, National Institute of Standards and Technology (NIST), March 29 2007.
73. Police IT Organisation. Part 1: Identification roadmap 2005-2020 - Biometrics technology roadmap for person identification within the police service. Report, Police IT Organisation, 2005.
74. J. A. Ratkovic. Increasing efficiency in the criminal justice system: the use of new technology for criminal identification and latent print processing. The rand paper series, The Rand Corporation, 1980.
75. R. A. Reiss. *Portrait Parlé.* Th. Sack, Lausanne, 2nd edition, 1914.
76. P. Rose. *Forensic Speaker Identification.* Taylor & Francis London, London, New-York, 2002.
77. A. A. Ross, K. Nandakumar, and A. K. Jain. *Handbook of Multibiometrics.* Springer, New York, 2006.
78. R. M. Royall. *Statistical Evidence - A Likelihood Paradigm.* Chapman Hall, London, 1997.

79. T. Ruggles, S. Thieme, and D. Elman. Automatic fingerprint identification systems I. North American Morpho System. In H. C. Lee and R. E. Gaensslen, editors, *Advances in Fingerprint Technology*, pages 211–226. Elsevier Science Publishing Co., Inc., New-York, 1991.
80. G. N. Rutty and A. Abbas. Could earprint identification be computerised? An illustrated proof of concept paper. *International Journal of Legal Medicine*, 119:335–343, 2005.
81. M. J. Saks and J. J. Koehler. The coming paradigm shift in forensic identification science. *Science*, 309:892–895, 2005.
82. M. J. Saks and D. M. Risinger. Science and nonscience in the courts: Daubert meets handwriting identification expertise. *Iowa Law Review*, 82:21–74, 1996.
83. C. Sannié. Alphonse Bertillon et la dactyloscopie. L'affaire Scheffer. *Revue Internationale de Police Criminelle*, 5(41):255–262, 1950.
84. L. Schomaker and M. Bulacu. Automatic writer identification using connected-component contours and edge-based features of upper-case western script. *IEEE Transactions on Pattern Analysis and Machine Intelligence (PAMI)*, 26:787–798, 2004.
85. S. N. Srihari, M. J. Beal, K. Bandi, V. Shah, and P. Krishnamurthy. A statistical model for writer verification. In *Proceeding of the International Conference on Document Analysis and Recognition*, pages 1105–1109, 2005.
86. S. N. Srihari, S.-H. Cha, H. Arora, and S. Lee. Individuality of handwriting. *Journal of Forensic Sciences*, 47:1–17, 2002.
87. D. A. Stoney. Measurement of fingerprint individuality. In H. C. Lee and R. E. Gaensslen, editors, *Advances in Fingerprint Technology*, pages 327–387. CRC Press, Boca Raton, 2001.
88. D. Sweet and I. A. Pretty. A look at forensic dentistry - part 1: The role of teeth in the determination of human identity. *British Dental Journal*, 190:359–366, 2001.
89. F. Taroni, C. Champod, and P. Margot. Forerunners of bayesianism in early forensic science. *Jurimetrics Journal*, 38:183–200, 1998.
90. R. Thiebault. Automatic process for automated fingerprint identification. In *Proceedings of the International Symposium on Automation of Population Register Systems*, volume 1, pages 207–226, 1967.
91. United States Department of Justice and Federal Bureau of Investigation. *The Science of Fingerprints*. U.S. Government Printing Office, Washington DC, 1984.
92. C. van der Lugt. *Earprint Identification*. Elsevier Bedrijfsinformatie, Gravenhage, 2001.
93. M. van Erp, L. Vuurpijl, K. Franke, and L. Schomaker. The WANDA measurement tool for forensic document examination. *Journal of Forensic Document Examination*, 16:103–118, 2004.
94. P. Vanezis and C. Brierley. Facial image comparison of crime suspects using video superimposition. *Science & Justice*, 36(1):27–34, 1996.
95. P. Vanezis, D. Lu, J. Cockburn, A. Gonzalez, G. McCombe, O. Trujillo, and M. Vanezis. Morphological classification of facial features in adult Caucasian males based on an assessment of photographs of 50 subjects. *Journal of Forensic Sciences*, 41(5):786–791, 1996.
96. J. Vucetich. *Dactyloscopia comparada: El nuevo sistema argentino*. Jacobo Peuser, La Plata, Argentina, 1904.

97. S. J. Walsh, C. M. Triggs, and J. S. Buckleton. *Forensic DNA Evidence Interpretation: Methods and Interpretation.* CRC Press, Boca Raton, 2004.
98. R. Williams and P. Johnson. Forensic DNA databasing : A european perspective. Interim report, School of Applied Social Sciences, University of Durham, June 2005.
99. F. G. Wood. Automatic fingerprint identification systems II. De La Rue Printrak system. Technical report, Elsevier Science Publishing Co., Inc., 1991.
100. M. Yoshino. Conventional and novels methods for facial-image identification. *Forensic Science Review*, 16(2):104–114, 2004.
101. J. Zhou and M. Abdel-Mottaleb. A content-based system for human identification based on bitewing dental X-ray images. *Pattern Recognition*, 38:2132–2142, 2005.