Biometrics – Developments and Potential

Introduction

Forensic science is defined as the body of scientific knowledge and technical methods used to analyze and interpret traces, in order to answer questions related to criminal, civil, and administrative law. It focuses in particular on the demonstration of the existence of an offence and its investigation, on the individualization of a person, and on the description of a modus operandi. The practice of forensic science is founded on four basic inferences: identification, individualization, association, and reconstruction [1]. These inferences are structured in three levels: the source level, the activity level, and the offence level [2]. The source level focuses on the question of the origin of a trace, the activity level concentrates on the activity that leads to a trace, and the offence level addresses the question if an activity constitutes an offence, a civil wrong, or an administrative violation.

Biometrics is the set of methods used for the recognition of human beings or traces, measuring and statistically analyzing their distinctive physical and behavioral traits. The method consists of the extraction and comparison of biometric features from a reference and a test sample, followed by the computation of a score representing a distance or similarity measure between the two samples [3].

Currently, a score can be used in three types of forensic inferences at source level: identification and identity verification, individualization, and association. Identification and identity verification are decisions about the identity of a person. Individualization is a description of the evidential value of a trace, in the light of a pair of mutually exclusive hypotheses related to the source of this trace. Association consists of linking and selecting objects, people, and events. More concretely, biometric technology plays a role in several forensic applications: identity management and verification, identification of missing persons from mass disasters, forensic investigation and intelligence as well as the forensic evaluation of biometric traces in court. Together these applications form the field of forensic biometrics.

The field of biometrics still faces severe practical limitations in the forensic context due to an insufficient understanding of its effective use. Even comprehensive documents on biometrics addressing the forensic aspect do not always use the forensic inference models to describe the challenges and opportunities in forensic biometrics [3]. This may be because of the immaturity of the forensic research culture [4, 5] and in the rarity of the literature addressing this specific topic [6].

Development

Methods such as forensic anthropometry [7], forensic dactyloscopy (commonly referred to as friction ridge analysis and comparison) [8], and le Portrait Parlé [9] have existed since the end of the 19th century. They exploit physical and behavioral traits primarily for the individualization of perpetrators of criminal infringements. From the 1960s, the development and implementation of automatic fingerprint identification system (AFIS) constitutes the first forensic automated biometric application: the automation of the identity verification based on 10 print cards [10]. In the 1980s, the discovery of forensic DNA profiling led to the development and implementation of similar tools and applications: the identity verification based on DNA reference material using a computerized DNA database, the selection of subsets of individuals, and the individualization of persons from biological traces.

In the 1990s, speaker, face, and gait recognition became of interest for forensic biometrics, as a consequence of the development of mobile telecommunication and camera surveillance technologies (CCTV). During the same decade, the first solutions combining biometric technologies and the Bayesian likelihood ratio (LR) inference model were proposed for evidence evaluation [11]. After 2001, interest rose for soft biometric modalities such as body measurements (height, width, and weight) and proportions, gender, hair, skin color, and clothing characteristics. This interest was mainly motivated by the possibility of capturing these features in unconstrained environments. However, the limited distinctiveness and
permanence of these features increased the necessity to consider a multimodal approach [12].

**Data and Modalities**

In the forensic context, a reference sample is sometimes named control material or known item, whereas a test sample collected at a crime scene is often denoted as crime scene sample, trace material, questioned item, or unknown item. Case-related biometric data are the reference and test samples collected and used for casework purpose by law enforcement agencies. They are also of great interest for forensic biometric research. In the field of biometrics, different types of biometric information exploited such as the fingerprint, the face, or the speech are named modalities.

Some biometric traces and marks are captured physically (biological traces, fingermarks, earmarks, bitemarks, lipmarks, etc.), others digitally (face, voice, body measurements, gait, etc.). Some attributes closely related to the human body such as clothing and footwear are often treated as biometric modalities in forensic science, because they are collected, analyzed, and interpreted in the same way as biometric traces and exploited using the same inference models. The stability of the biometric information of a modality over time determines the permanence of the case-related data for investigation. Fingerprint and DNA reference and trace specimens may remain usable indefinitely when face and speech specimens may be obsolete after some years or even months.

In order to be of forensic interest, a biometric modality has to be available as a trace and needs to be distinctive. On a crime scene, fingermarks and biological DNA traces are searched in priority because they are often available and can be very distinctive. On the other hand, the iris pattern, even if very distinctive, is only very rarely available as a digital trace. Digital traces may embed information about the body length of a perpetrator, but the use of such a modality is only envisaged if no other option is available, because of its poor distinctiveness [13].

The identification of missing persons from a mass disaster depends on the form of this disaster, closed or open. A closed disaster, such as an aircraft crash with a passenger list, relates to a known number of individuals from a defined group. Open disasters such as traffic accidents, natural disasters, technical accidents (fires, explosions, etc.), terrorist attacks, and events occurring within the context of war relates to an unknown number of individuals from an undefined group. Combinations of these two forms are also conceivable (e.g., aircraft crash in a residential area) [16]. When the prior probabilities can be assigned, the evidential value of the biometric features can be assessed and the decision thresholds can be determined. Closed-set identification (1 to $N$, where $N$ is the number of people) and open-set identification (1 to $N+1$) frameworks apply, respectively, to these two types of disaster. When the prior probabilities cannot be assigned and the decision thresholds cannot be determined, the LR inference model can be applied to assess the evidential value of the biometric features [17, 18].

**Applications**

This section describes the forensic biometric applications and details the role of biometric technology in each of them. In preamble it has to be stressed that the reliability of any application depends on the integrity of management of the data [14]. For example, before the use of biometric solutions in the Dutch prisons, some individuals were serving sentences and substituting themselves to the convicted criminals. Nowadays, the Netherlands have implemented a system combining the fingerprint and face modalities to identify and verify, in case of serious crime, that the person behind a claimed identity remains consistent [15].

**Forensic Identification of Missing Persons**

The identification of missing persons from a mass disaster depends on the form of this disaster, closed or open. A closed disaster, such as an aircraft crash with a passenger list, relates to a known number of individuals from a defined group. Open disasters such as traffic accidents, natural disasters, technical accidents (fires, explosions, etc.), terrorist attacks, and events occurring within the context of war relates to an unknown number of individuals from an undefined group. Combinations of these two forms are also conceivable (e.g., aircraft crash in a residential area) [16]. When the prior probabilities can be assigned, the evidential value of the biometric features can be assessed and the decision thresholds can be determined. Closed-set identification (1 to $N$, where $N$ is the number of people) and open-set identification (1 to $N+1$) frameworks apply, respectively, to these two types of disaster. When the prior probabilities cannot be assigned and the decision thresholds cannot be determined, the LR inference model can be applied to assess the evidential value of the biometric features [17, 18].
Forensic Investigation

Biometric technology contributes to forensic investigation in associating traces to persons present in a database, producing rank lists and selecting subsets of persons from which the trace may originate. For instance, an automatic fingerprint identification system or a computerized forensic DNA database is used for comparing a trace to the $N$ individuals of a database and selecting the $M$ individuals most similar to the trace (closed-set selection, $M$ from $N$). In a second phase, forensic examiners refine the results of the automatic selection excluding some more reference samples, based on criteria that are not addressed by these automated methods at present. The importance of the human-based phase increases with the complexity of the trace, for example, superimposed fingermarks or biological traces containing mixtures or partial DNA profiles from more than one contributor. This combined approach (automated and human-based) can be described as an open-set selection ($M$ from $N+1$).

Forensic Intelligence

Biometric technology is used for forensic intelligence to associate traces from different cases, producing rank lists and selecting subsets of cases with traces that may be from the same origin. Only comparing trace material is the most challenging application from the point of view of biometrics, because the quality of both specimens is limited [19]. For instance, the information system of Europol [20] will integrate in the near future forensic intelligence capabilities for the DNA, fingerprint, and face modalities.

Forensic Evaluation

The evaluation of biometric evidence in court consists of applying the biometric technology for forensic individualization. The score computed is considered as forensic evidence ($E$) and the evidential value of $E$ is assessed in the light of a pair of mutually exclusive hypotheses about the origin of the trace material. Generally the first hypothesis ($H_p$) is supported by the prosecution and states that the trace material originates from the suspected person. The second hypothesis ($H_d$) is supported by the defense and states that the trace material originates from another individual, randomly chosen within the relevant population of potential sources of the trace. The evidential value is calculated as the ratio of two probabilities: the probability of the evidence when the prosecution hypothesis is true divided by the probability of the evidence when the defense hypothesis is true. $I$ represents the relevant background information about the case, for instance, the selection process of the suspected person and the nature of the relevant population [6]. The result is expressed as an LR, calculated as follows:

$$\frac{Pr(H_p|E,I)}{Pr(H_d|E,I)}$$

The posterior probability ratio is calculated as the multiplication of the prior probability ratio by the LR. The role of the forensic practitioner is limited to the assessment of the LR. To provide the prior probability ratio and to make decisions on the basis of the posterior probability ratio is the duty of the court. This approach is considered as logical and balanced [21] and the LR can be seen as the metric describing the evidential value [22].

A biometric LR-based system is a software system that combines the use of biometric databases, technologies, and the LR approach to assess statistically the evidential value of a biometric trace associated to a reference sample. The quality of the inference strongly depends on the quantity and properties of the data used to estimate the within and between-source variabilities [23]. Such an automatic approach complements the human-based approach, using knowledge and experience to assign personal probabilities. The strength of an LR-based system is to provide statistical probabilities on the set of distinctive features that can be extracted automatically. The strength of human beings lies in the exploitation of features that currently cannot be handled by the biometric technology, such as the third-level details in fingermarks or sociolinguistic aspects of speech. Statistical probabilities are considered as more objective and personal probabilities more subjective.

The classical “forensic identification” disciplines, relying mainly on personal probabilities for the
assessment of the evidence are being increasingly challenged [24], especially because of the development of evidence based on DNA profiles, governed by statistical data and the evolving requirements for the admissibility of evidence following the Daubert decision by the Supreme Court of the United States [6]. The LR approach is considered as promising in forensic biometrics. It has been first implemented for DNA [21], followed by LR-based systems developed for speaker recognition [25], and more recently for fingerprinting [26]. In this respect, forensic biometrics can be considered as a forerunner in the “forensic identification science paradigm shift” [24].

Improve the Current Applications

**Modalities**

Despite the widely spread usage of the biometric technologies within forensic science, some biometric modalities have failed to catch the attention of the biometric community, probably due to the fact that they are only exploited for specific forensic purposes. For instance, forensic anthropologists exploit the size and shape of hard tissues (soft bones, bones, and teeth) and the results of dentistry and surgery on these tissues for postmortem identification. These features are considered as very distinctive, but more systematic statistical research is desirable to be able to assess their evidential value. Together with fingerprints and biological traces, earmarks and footwear marks are collected in high-volume crime for forensic investigation, intelligence, and individualization purpose. But contrary to fingerprints and DNA, no analytical model is available yet to describe the distinctive features present in ear and footwear marks. They still represent a challenge for pattern recognition and statistics, limiting the possibility to build forensic biometric systems based on these [19].

**Technology**

Biometric feature extraction and comparison algorithms are generally fully automatic and optimized to minimize processing time. In the forensic context, the need for speed has a lower priority and semiautomatic feature extraction can be considered. Specific implementations designed for the feature extraction and comparison from forensic data should focus on the amount of distinctive information usable in the forensic data, even at the cost of increasing the processing time. For instance, the feature extraction and comparison of fingerprints and fingerprints focuses on the minutiae (position and angle), but a systematic use of the extended fingerprint feature set as defined in the ANSI/NIST ITL-1 2011 standard may improve the performance [27]. In the same way, the automatic processing of higher level speaker-dependent features from speech samples of forensic quality may be beneficial [28].

**Data and Testing**

Biometric data intrinsically involve some privacy issues, meaning that their use for research usually requires authorizations. Their statute of real data raises the question of the ground truth of their origin, which is formally unknown for trace samples. The amount of case-related data depends on the forensic process. They may be collected in large quantities and structured in databases for forensic investigation. For forensic evaluation, the amount of data is strongly case dependent. The requirement in terms of quantity and quality of data depends on which forensic application of the technology is intended. When approaching the quality of real data, simulated data should be used in the training phase, because their production is controlled and the ground truth of their origin is known. The test phase should at least contain some sets of real data, and the validation of a system should be performed using mostly real data. Research databases constituted of case-related biometric data remain unfortunately too rare [29, 30].

The limitation of access to real forensic data for research purpose is a reality, but improvement is possible in line with the open data strategy of the EU, summarized in the 2020 Digital Agenda for Europe as “Data is the new gold”. A way to provide an indirect access to the data without compromising their security and privacy consists of developing online evaluation platforms on which the biometric technology is uploaded and the data stored securely and anonymously without possibility of download. Such a mechanism allows for the evaluation of biometric systems using real forensic data against appropriate performance metrics without direct access to the data. It requires, firstly, to make explicit the forensic biometric processes and to agree on the relevant metrics for their evaluation. Secondly, it requires
implementing the evaluation mechanisms and sharing the data and resources. Finally, it requires coordinated action to feed the most relevant results to standardization bodies, in order to improve international standardization. The EU project “Biometric Evaluation and Testing” \[31\], develops such an approach, but not for forensic biometrics.

Applications

Closed-set (1 to \(N\)) and open-set (1 to \(N+1\)) forensic biometric identification processes are evaluated in standard operational conditions with standard error measures (false identification rate/false acceptance and false rejection rates) and performance metrics – cumulative matching curve (CMC), equal error rate (EER), detection error trade-off (DET) curve. However, in the forensic context, more transparency is needed in the way the prior probabilities are assigned, the evidential value from the biometric data is assessed and the thresholds are determined, globally or personally.

The scalability of the technology in the forensic biometric processes depends on the modality. But within a modality, it also largely depends on the process and the quality of data involved. The US National DNA Index (NDIS) contains reference DNA profiles from more than \(10^7\) individuals. The performance of this technology is sufficient to implement an identity verification application based on the comparison of reference samples, but more performance studies are desirable for forensic intelligence and investigation dealing with test samples mimicking the limited quality of the traces \[32\]. Appropriate performance metrics are also needed to characterize selection processes. The rank of a target as a function of the quality of the test data may be studied using cost functions based on the CMC, in order for the size of the short list \(M\) not to be fixed but being a function of the quality of the data.

For forensic individualization, the absence of underpinning statistical data in the “classic forensic identification disciplines” is viewed as a main pitfall that requires a paradigm shift \[24\]. Outside of DNA profiling, the results computed by LR-based systems using biometric technology are rarely integrated in the forensic evaluation. Firstly, no general method is currently described and available to evaluate and calibrate the results of LR-based systems. Agreement exists on the use of Tippett plots \[33\] and the measure of the rates of misleading evidence in favor of \(H_p\) and \(H_d\) \[34\] to measure the performance of such systems and on the use of the cost log likelihood ratio (CLLR) for their discrimination and calibration. Calibration is a measure of reliability of the LR value. The evidential value of calibrated LRs tends to increase when the discrimination power of the LR-based system increases \[35\]. The way to evaluate some other aspects of LR-based systems such as their robustness, coherence, and generalization is still work in progress.

Secondly, the development of methods to combine the evidential value computed by automatic approaches and assessed by human-based approaches is still in progress. Technical solutions exist within biometrics to combine results at different levels (feature, match score, and decision), using rule-based approaches (majority voting, sum rule, product rules), or algorithms based on Support Vector Machine, fuzzy clustering, radial basis neural networks, or even to fuse information between different levels \[36\]. These solutions may be tested and adopted for soft biometric multimodal approaches developed for forensic investigation and intelligence and for the fusion of the modalities used for the identity verification and identification in the criminal justice chain. But for forensic evaluation there are some particular demands in terms of logic and transparency for the methodology used to combine results \[37\]. The solution currently explored by the forensic community relies mainly, though not exclusively, on the use of Bayesian networks, but despite providing logic and transparency to the process, its complexity is a major obstacle to its implementation \[38\].

Implementation

At local and national level, numerous biometric solutions are implemented within law enforcement, but the forensic biometrics field remains fragmented. For instance, countless face recognition products have been acquired locally, tested and implemented independently in the last decade to support forensic investigation and intelligence, despite known poor results, which was confirmed again for the UK riots of 2011 \[39\]. Research and development provides solutions to improve the capture of biometric data, such as intelligent cameras that can automatically detect, zoom in, and follow faces, but organizational aspects such as complying with minimal
quality requirements and technical standards are necessary to stimulate the implementation of new technology.

AFIS systems and computerized DNA databases are best operable at national level, but ensuring their interoperability at a larger scale such as the connection of the EU-national fingerprint and DNA databases under the umbrella of the Prüm Treaty or the international exchange of biometric information through Interpol remains a challenge.

**Develop New Applications**

The current forensic research mainly focuses on identification, individualization, and association at source level, trying to answer to the question: who is at the origin of a trace? Less attention has been given to reconstruction at activity level, trying to answer the questions: how and when the trace was made? However, analyzing and interpreting the position of fingerprints, the quantity of DNA, the movement of a body, or the expression of a face to an activity is of great forensic interest. A similar challenge consists of dating traces, for instance, exploiting spectroscopic properties of physical traces outside of the visible range may.

The flaws of the identity management infrastructures and processes offer a new role for forensic biometrics: contributing to the investigation of identity fraud and to find remedies against it. The role is not just limited to criminal cases such as the substitution of convicted persons in prison, but it also extends to civil cases such as family relatedness claims (paternity, lineage, etc.) or administrative cases such as residence or social benefits claims. DNA can certainly play a central role in the enrolment phases of these processes, but for the verification phases, other modalities seem more suitable because of the complex and long analytical process of DNA and its risk of contamination.

**Conclusion**

Making forensic biometrics one community, improving the current forensic biometric applications, and developing new forensic biometric applications is a challenge. It necessitates collaboration to set up research directions embedding several aspects, generally in the hands of different actors: the relevant data, the relevant inference process, the relevant technology, and the relevant evaluation framework. However, this is the challenge identified by the European Council to face the field of high tech and cyber crime in its conclusion on the vision for European Forensic Science 2020. It recognizes the central role of the exchange of information including biometrics and other data generated by forensic processes in the prevention of and the fight against crime and criminal activities. It also emphasizes the need to define commonly accepted minimum forensic science standards for the collection, processing, use, and delivery of forensic data relating *inter alia* to data concerning DNA profiles, as well as dactyloscopic and other biometric data.

**References**


Related Articles

Evidence Interpretation: a Logical Approach
Statistical Evidence in Court
Identification and Individualization
Earprint Comparison: Automated Systems
Automated Fingerprint Identification System

Didier Meuwly and Raymond Veldhuis