Forensic Biometrics:

From two communities to One Discipline

Didier Meuwly*, Raymond Veldhuis**

*Netherlands Forensic Institute, WISK, 2490AA The Hague, The Netherlands
**The University of Twente, SAS, 7500AE Enschede, The Netherlands
*d.meuwly@nfi.minvenj.nl
**r.n.j.veldhuis@utwente.nl

Abstract: This article describes how the fields of biometrics and forensic science can contribute and benefit from each other. The aim is to foster the development of new methods and tools improving the current forensic biometric applications and allowing for the creation of new ones. The article begins with a definition and a summary of the development in forensic biometrics. Then it describes the data and biometric modalities of interest in forensic science and the forensic applications embedding biometric technology. On this basis it describes the solutions and limitations of the current practice regarding the data, the technology and the inference models. Finally, it proposes research orientations for the improvement of the current forensic biometric applications and suggests some ideas for the development of some new forensic biometric applications

1 Introduction

Forensic science is defined as the body of scientific knowledge and technical methods used to analyse 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 and the investigation of an offence, on the individualization of a perpetrator and on the description of a *modus operandi*. The practice of forensic science is founded on 4 basic inferences: identification, individualization, association and reconstruction [IR98]. These inferences are structured in 3 levels: the source level, the activity level and the offence level [Co98]. 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 adresses the question if an activity is constitutive of an offence.

Biometrics is the set of automated methods used for the recognition of human beings, measuring and analyzing statistically their distinctive physical and behavioural 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 a similarity between the two samples [Wh10].

Currently scores are used in 3 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: the identity management and the identity verification in the criminal justice chain, the identification of missing persons from a mass disaster, the forensic investigation and intelligence as well as the forensic evaluation of biometric evidence in court. Together these applications form the field of forensic biometrics.

A lot of biometric solutions are implemented in the forensic practice, often as the result of a request of the law enforcement agencies towards industrial and academic partners. But the field still faces severe practical limitations due to an insufficient understanding of its context and needs for an optimal implementation of tools and methods. Even comprehensive documents on biometrics addressing the forensic aspect do not use the forensic inference models to describe the challenges and opportunities in forensic biometrics [Wh10]. A cause may be found in the immaturity of the forensic research culture [Mn11] and in the rarity of the literature addressing this specific topic [DC08].

The aim of this article is to describe how the fields of biometrics and forensic science can contribute and benefit from each other, in order to foster the development of new methods and tools improving the current forensic biometric applications and allowing for the creation of new ones.

2 Development

Methods like forensic anthropometry [Be86], forensic dactyloscopy [Ga92] and le portrait parlé [Re05] exist from the end of the 19th century. They exploit physical and behavioural traits for the individualization of perpetrators of criminal infringements. From the 1960's the development and implementation of automatic fingerprint identification system (AFIS) constitutes the first forensic biometric application: the automation of the identity verification on basis of ten print cards [BS01]. In the 1980's the discovery of forensic DNA profiling led to the development and implementation of similar tools and applications: the identity verification on basis of DNA reference material using a computerized DNA database, the selection of subsets of individuals and the individualization of persons from biological traces.

In the 1990's 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 inference model were proposed for evidence evaluation [CM00].

After 2001 the interest rose for soft biometric modalities such as body measurements (height, width, weight) and proportions, gender, hair, skin colour and clothing characteristics. This interest was mainly motivated by the possibility of capturing these features in unconstraint environments. However, the limited distinctiveness and

permanence of these features enhanced the necessity to consider a multimodal approach [JDN04].

In the current decade the development of new biometric modalities can be expected, for instance modalities exploiting spectroscopic properties of the biological tissues outside of the visible range or being spin-offs of the unprecedented development of mobile communication technology. Their potential for forensic biometrics will be investigated.

3 Data and modalities

In the forensic context a reference sample is sometimes named control material or known item, when a test sample collected on a crime scene is often denoted as crime scene sample, trace material, questioned 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.

Some biometric traces and marks are captured physically (biological traces, fingermarks, earmarks, bitemarks, lipmarks), other digitally (face, voice, body measurements, gait). Some attributes closely related to the human body like 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 a modality over time determines the obsolescence of the case related data for investigation, from lifetime for fingerprint and DNA, to some months or years for face and speaker recognition.

In order to be of forensic interest, the biometric modality has to be available as a trace and needs to be distinctive. On a crime-scene, fingermarks and biological 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 this modality is only privileged if no other option is available, due to the its poor distinctiveness [Al08]. The modality also needs to be stable and robust to the forensic conditions. Face recognition is commonly exploited for forensic investigation, but suffers from severe limitations. The facial features can change significantly over even short periods of time and the unconstrained video captures constituting the main part of the trace material can loose a substantial part of the distinctiveness of the modality.

The overall performance of a biometric technology is largely influenced by the quality of the input data conditioned by the acquisition and environmental conditions. These factors are common in all biometric deployments, but forensic processes tend to maximize their variability [DC08].

4 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 forensic biometric application relies on the integrity of the identity management used by the criminal justice chain [Me10]. The identity infrastructure in place needs to able to create, challenge and end biometric identities reliably. For example, before the use of biometric solutions in the Dutch prisons, some individuals were serving sentences, 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 the same along the whole criminal justice chain, from the arrest to the detention to serve the sentence [PG11].

4.1 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 relates to a known number of individuals from a defined group, like an aircraft crash with a passenger list. Open disasters like traffic accidents, natural disasters, technical accidents (fires, explosions), 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) [In09]. 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) 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 likelihood ratio inference model applies to assess the evidential value of the biometric features [Bu11, BTM12].

4.2 Forensic investigation

Biometric technology contributes to forensic investigation in associating traces to persons present in a database, producing ranklists and selecting subsets of persons from which the trace may originate. For instance an automatic fingerprint identification system or a computerized forensic DNA database are 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 methods at present. The importance of the human-based phase increases with the complexity of the trace, e.g. superimposed fingermarks or biological traces containing partial DNA profiles from more than one contributor. This combined combined approach (automated and human-based) can be described as an open-set selection (M from N+1).

4.3 Forensic intelligence

Biometric technology is used for forensic intelligence to associate traces from different cases, producing ranklists 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 [RWM06]. For instance the information system (IS) of Europol will integrate in the near future forensic intelligence capabilities for the DNA, fingerprint and face modalities [Eu11].

4.4 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 (*Hp*) is supported by the prosecution and states that the trace material originates from the suspected person. The second hypothesis (*Hd*) is supported by the defence and states that the trace material originates from another indivual, 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 defence 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 [DC08]. The result is expressed as a likelihood ratio, calculated as follows:

$$\underbrace{\frac{\Pr(H_p \mid E, I)}{\Pr(H_d \mid E, I)}}_{\textbf{Posterior probability ratio}} = \underbrace{\frac{\Pr(E \mid H_p, I)}{\Pr(E \mid H_d, I)}}_{\textbf{Likelihood ratio}} \cdot \underbrace{\frac{\Pr(H_p, I)}{\Pr(H_d, I)}}_{\textbf{Prior probability ratio}}$$

The posterior probability ratio is calculated as the multiplication of the prior probability ratio by the likelihood ratio. The role of the forensic practitioner is limited to the assessment of the likelihood ratio. To provide the prior probability ratio and to make decisions on basis of the posterior probability ratio is the duty of the court. This approach is considered as logical and balanced [Ev98] and the *LR* can be seen as the metric describing the evidential value [Go91].

A biometric *LR*-based system is a software system that combines the use of biometric databases, technologies and the likelihood ratio 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 variability [Me06]. Such an automatic approach complements the human-based approach using knowledge and experience to assign personal probabilities. The strength of a *LR*-based system is to provide statistical probabilities on the set of distinctive features that can be extracted automatically. The strength of human beings is to also consider features that cannot be handled yet by the biometric technology, like 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 [SK05], 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 USA [DC08]. The *LR* approach is considered as promising in forensic biometrics. It has been firstly implemented for the DNA modality [Ev98], followed by *LR*-based systems developed for the speaker recognition modality [GR06] and more recently for the fingerprint modality [NES12]. In this respect, forensic biometrics can be considered as a forerunner in the "forensic identification science paradigm shift" [SK05].

5 Improving the current applications

5.1 Modalities

Despite the widely spreaded usage of the biometric technologies within forensic science, some biometric modalities have escaped to catch the attention of the biometric community, probably due to the fact that they are only exploited for specific forensic purposes. For instance the size and shape of hard tissues (soft bones, bones and teeth) and the results of dentistry and surgery on these tissues are exploited by forensic anthropologists, mainly for *post-mortem* 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 fingermarks and biological traces, earmarks and footwear marks are collected in high volume crime and workable for forensic investigation, intelligence and individualization purpose. But contrarily to the fingermark and DNA modalities, 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 *de facto* the possibility to build forensic biometric systems based on these modalities [RWM06].

5.2 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 semi-automatic 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 fingermarks and fingerprints focuses on the minutiae (position and angle), but a systematic use of the extended fingerprint feature set (EFS) as defined in the ANSI/NIST ITL-1 2011 standard may improve the performance [IHK11]. In the same

way the automatic processing of higher-level speaker dependent features from speech samples of forensic quality may be beneficial [GR12].

5.3 Data and testing

Biometric data intrinsically involve some privacy issues, meaning that their use for research implies 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 the technological development 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 [Le06, Kr09].
The limitation of access to real forensic data for research purpose is a reality, but improvement is possible in line with the new EU open data strategy "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. 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 a coordination action to feed the most relevant results to standardization bodies, in order to improve international standardization. The EU project "Biometric Evaluation And Testing" [Be12], develops such an approach, but not for forensic biometrics.

5.4 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 curve-DET). But 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 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

[Hi10]. 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 [SK05]. Outside of the DNA modality, 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 exist on the use of Tippett plots [MD01] and the measure of the rates of misleading evidence in favour of *Hp* and *Hd* [Ne06] to measure the performance of such systems and on the use of the cost log likelihood ratio (C_{llr}) 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 [RC07]. The way to evaluate some other aspects of *LR*-based systems, like their robustness, coherence and generalisation 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 (SVM), fuzzy clustering, radial basis neural networks or even to fuse information between different levels [SVN07]. 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 [AF09]. The solution currently explored by the forensic community relies on the use Bayesian Networks, but despite providing logic and transparency to the process, its complexity is a major obstacle to its implementation [Ta06].

5.5 Challenges

The table 1 summarizes a series of current challenges for a set of biometric modalities relevant for the 4 forensic applications defined *supra*. The level of these challenges depends mainly on the availability of the modality and on the maturity of the technology; they are at a much lower level for the soft biometric modalities than for the fingerprint modality. For forensic identification the challenge focuses on the development of reference databases and on their management, increasing the integrity, quality and interoperability of the data. For forensic investigation and intelligence, the challenge focuses on the automation of the processes, on the improvement of the performance for real trace samples, generally of low quality, and on the scalability of the technology for large databases. For forensic evaluation the challenge focuses not only on the development of semi-automatic methods based on the likelihood ratio framework, but also on the integration of expert-based and semi-automatic methods into hybrid methods.

<table>
<tr><th rowspan="2">Forensic application</th><th colspan="5">Biometric modality</th></tr>
<tr><th>Finger</th><th>Face</th><th>Speaker</th><th>Gait</th><th>Soft modalities</th></tr>
<tr><td rowspan="2">Forensic identification</td><td>Improve the databases integrity and the quality of reference samples</td><td colspan="2" rowspan="2">Develop the concept of forensic face/speaker database</td><td colspan="2" rowspan="2">Not relevant regarding the weak distinctiveness of these modalities</td></tr>
<tr><td>Improve interoperability</td></tr>
<tr><td rowspan="3">Forensic investigation and intelligence</td><td rowspan="3">Improve technology scalability (databases > 10^6 fingerprints)
Improve performance for very partial fingermarks (5 - 8 minutiae)</td><td colspan="3">Improve technology scalability</td><td rowspan="3">Evaluate the possibilities to combine the modalities, considering their availability and dependence</td></tr>
<tr><td colspan="3">Diminish the constraints on the trace sample:</td></tr>
<tr><td>Position, lighting, aging</td><td>Noise, channel, aging</td><td>Location, clothing</td></tr>
<tr><td rowspan="3">Forensic evaluation</td><td colspan="3">Build, validate and calibrate semi-automatic LR-based methods</td><td rowspan="3">Explore the possibility to develop semi-automatic LR-based methods</td><td rowspan="3">Early developments: try to combine information from several soft modalities</td></tr>
<tr><td colspan="3">Improve and harmonize expert-based protocols</td></tr>
<tr><td colspan="3">Develop hybrid LR-based methods (expert-based and semi-automatic)</td></tr>
</table>

Table 1: Challenges of different biometric modalities regarding the forensic applications

5.6 Implementation

At local and national level, numerous biometric solutions are implemented within law enforcement but the forensic biometrics field remains a fragmented reality. For instance, countless face recognition products have been acquired locally, tested and implemented independently along the last decade to support forensic investigation and intelligence, despite known poor results [Br02], confirmed again for the UK riots of 2011 [Fi11]. Research and development provides solutions to improve the capture of biometric data, like intelligent cameras that can automatically detect, zoom in and follow faces. But organisational aspects like complying with minimal quality requirements and technical standards are necessary to stimulate the implementation of new technology.

AFIS systems and computerized DNA databases are at best operable at national level. But ensuring their interoperability at a larger scale, like 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. Both technological and organisational dimensions prove to be difficult on a local scale and barely manageable on national and European scales. The cause has to be found in the number of parties increasing greatly and in the differences of culture, legislation and IT infrastructure" [PG11].

6 Development of new applications

The current forensic research mainly focuses on identification, individualization and association at source level, trying to answer to the question: who is the origin of a trace? Less attention has been given to reconstruction at activity level, trying to answer to the questions: how and when the trace was made? But analysing and interpretating the position of fingermarks, the quantity of DNA, the movement of a body or the expression of a face to an activity is of great forensic interest. Exploiting properties of biometric traces to date is a similar challenge, and spectroscopic properties of physical traces outside of the visible range may contribute to it.

The flaws of the identity management infrastructures and processes offer a new role to play for forensic biometrics: contribute to investigate identity fraud and find remedies against it. The role is not limited to criminal cases like the substitution of convicted persons in prison, but also extends to civil cases like family relatedness claims (paternity, lineage) or administrative cases like 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.

7. 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 models, the relevant technology and the relevant evaluation framework. But 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 fight against crime and criminal activities. It also emphasises 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

[AF09] AFSP, *Standards for the formulation of evaluative forensic science expert opinion.* Science and Justice, 2009(49): p. 161-164.

[Al08] Alberink, I., *Obtaining confidence intervals and Likelihood Ratios for body height estimations in images*. Forensic Science International, 2008(177): p. 228-237.

[Be12] Available from: www.beat-eu.org, consulted 07.07.2012.

[Be86] Bertillon, A., *De l'identification par les signalements anthropométriques*. Reprinted from Archives d'anthropologie criminelle et des sciences pénales. 1886, Paris: Masson.

[Br02] Brooks, M.A., *Face-off.* New Scientist, 2002. **175** (2399).

[BS01] Berry, J. and D.A. Stoney, *History and Development of Fingerprinting*, in *Advances in Fingerprint Technology*, H.C. Lee and R.E. Gaensslen, Editors. 2001, CRC Press: Boca Raton. p. 1-40.

[BTM12] Biedermann, A., F. Taroni, and P. Margot, *Reply to Budowle, Ge, Chakraborty and Gill-King: use of prior odds for missing persons identification.* Investigative Genetics, 2012. **3**: p. 1-2.

[Bu11] Budowle, B., et al., *Use of prior odds for missing persons identification.* Investigative Genetics, 2011. **2**(1-6).

[CM00] Champod, C. and D. Meuwly, *The Inference of Identity in Forensic Speaker Recognition.* Speech Com., 2000. **31**(2-3): p. 193-203.

[Co98] Cook, R., et al., *A model for case assessment and interpretation.* Science & Justice, 1998. **38**(3): p. 151-156.

[DC08] Dessimoz, D. and C. Champod, *Linkages between biometrics and forensic science*, in *Handbook of Biometrics*, A. Jain, F. P, and A. Ross, Editors. 2008, Springer: New York. p. 425-459.

[Eu11] Europol, *Europol Information Management: Products and Services*, 2011, Europol: The Hague. p. 23.

[Ev98] Evett, I., *Toward a uniform framework for reporting opinions in forensic science casework.* Science & Justice, 1998. **38**(3): p. 198 - 202.

[Fi11] Firth, N., *Face recognition technology fails to find UK rioters.* New Scientist, 2011(2826).

[Ga92] Galton, F., *Finger Prints.* Macmillian and Compagny, London, 1892 [Reprinted Da Capo Press, New York, 1965], 1892.

[Go91] Good, I.J., *Weight of evidence and the Bayesian likelihood ratio*, in *The Use of Statistics in Forensic Science*, C.G.G. Aitken and D.A. Stoney, Editors. 1991, Ellis Horwood: Chichester, UK. p. 85–106.

[GR06] Gonzalez-Rodriguez, J., et al., *Robust estimation, interpretation and assessment of likelihood ratios in forensic speaker recognition.* Computer Speech and Language, 2006. **20**: p. 331-355.

[GR12] Gonzalez-Rodriguez, J., et al. *A Linguistically-Motivated Speaker Recognition Front-End through Session Variability Compensated Trajectories in Phone Units*. in *IDASSP 2012*. 2012. Kyoto.

[Hi10] Hicks, T., et al., *Use of DNA profiles for investigation using a simulated national DNA database: Part I. Partial SGM Plus1 profiles.* Forens. Sci. Int.: Genetics, 2010. **4**: p. 232-238.

[IHK11] Indovina, M., R.A. Hicklin, and G.I. Kiebuzinski, *ELFT-EFS Evaluation of Latent Fingerprint Technologies: Extended Feature [Sets Evaluation #1]*, 2011, U.S. Department of Commerce, National Institute of Standards and Technology: Washington DC.

[In09] Interpol, *Disaster Victims Identification Guide*, 2009, Interpol: Lyon. p. 55.

[IR98] Inman, K. and N. Rudin, *The origin of evidence.* Forens. Sci. Int., 2002. **126**: p. 11-16.

[JDN04] Jain, A., S. Dass, and K. Nandakumar, *Soft Biometric Traits for Personal Recognition Systems*, in *Biometric Authentication*, D. Zhang and A. Jain, Editors. 2004, Springer Verlag: Heidelberg. p. 1-40.

[Kr09] Krane, D., et al., *Time for DNAdisclosure.* Science, 2009. **326**(18 December): p. 1631-1633.

[Le06] Van Leeuwen, D., et al., *NIST and NFI-TNO evaluations of automatic speaker recognition.* Comp. Speech and Lang., 2006. **20**: p. 128–158.

[MD01] Meuwly, D. and A. Drygajlo. *Forensic Speaker Recognition Based on a Bayesian Framework and Gaussian Mixture Modelling (GMM)*. in *2001, A Speech Odyssey – The Speaker Recognition Workshop*. 2001. Crete.

[Me06] Meuwly, D., *Forensic Individualization from Biometric Data.* Science and Justice, 2006. **46**(4): p. 205-213.

[Me10] Meuwly, D., *ID management in 2020*, 2010, ID.academy: The Hague. p. 21.

[Mn11] Mnookin, J.L., et al., *The Need for a Research Culture in The Forensic Sciences.* UCLA L. Rev., 2011. **58**: p. 725-801.

[Ne06] Neumann, C., et al., *Computation of Likelihood Ratios in Fingerprint Identification for Configurations of Three Minutiae.* J. For. Sci., 2006. **51**(6): p. 1255–1266.

[NES12] Neumann, C., I.W. Evett, and J. Skerett, *Quantifying the weight of evidence from a forensic fingerprint comparison: a new paradig.* J. R. Statist. Soc. A, 2012. **175**(2): p. 1-26.

[PG11] Plomp, M.G.A. and J.H.A.M. Grijpink. *Combating Identity Fraud in the Public Domain: Information Strategies for Healthcare and Criminal Justice.* in *Proceedings of the 11th European Conference on e-Government*. 2011. Ljubljana, Slovenia: Academic Conferences International (ACI).

[RC07] Ramos-Castro, D., *Forensic evaluation of the evidence using automatic speaker recognition systems*, 2007, Universidad Autónoma de Madrid: Madrid, Spain. p. 169.

[Re05] Reiss, R.A., *Manuel du portrait parlé.* 1905, Lausanne: Th. Sack.

[RWM06] Ribaux, O., S.J. Walsh, and P. Margot, *The contribution of forensic science to crime analysis and investigation: Forensic intelligence.* Forensic Science International, 2006(156): p. 171-181.

[SK05] Saks, M. and J. Koehler, *The coming paradigm shift in forensic identification science.* Science, 2005(309): p. 892–895.

[SVN07] Singh, R., M. Vatza, and A. Noore, *Intelligent biometric information fusion using support vector machine*, in *Soft computing in image processing: recent advances* 2007, Springer-Verlag: Heidelberg. p. 325 – 349.

[Ta06] Taroni, F., et al., *Bayesian networks and probabilistic inference in forensic science.* 2006, London: Wiley.

[Wh10] Whither Biometrics Committee of98 National Research Council, *Biometric Recognition: Challenges and Opportunities*, ed. J.N. Pato and L.I. Millett. 2010: The National Academies Press.