Friction Ridge Skin – Automated Fingerprint Identification System (AFIS)

Introduction

Definition

Automated fingerprint identification system (AFIS) is a generic term that refers to a range of computer systems and technologies developed in order to assist in establishing the identity of individuals through their fingerprints. AFISs are used for forensic and non-forensic (other government uses and commercial) applications; this article concentrates only on the forensic applications.

AFISs were originally designed to assist fingerprint practitioners in the task of verifying the identity of repetitive offenders comparing the fingerprints of suspected persons to the standard impressions stored in reference databases. Later, the AFIS became a corner stone of the forensic investigation, supporting the practitioners in the task of selecting potential offenders on the basis of the comparison of fingermarks found on crime scenes and standard impressions stored in reference databases. For this application, the systems would be better labeled as automatic fingerprint selection systems (AFSSs). More recently, the use of AFISs was extended to the forensic intelligence application, by linking cases when comparing fingermarks found on different crime scenes [1].

AFISs embed fingerprint biometric algorithms used to extract and compare features of fingerprints and fingermarks images and to compute scores representing the similarity and the typicality of two specimens [2]. AFISs are used for forensic applications by virtually all the law enforcement agencies worldwide. It is a typical example of e-government implementation with a high level of automation and a high degree of both vertical and horizontal accountabilities in the law enforcement agencies running the AFIS-driven processes [3].

In the literature, confusion exists between the term print and mark. We will use a uniform terminology: the finger dermatoglyphics and their standard rolled or flat inked or scanned impressions are named *fingerprints*, whereas the recovered or lifted traces are named *fingermarks*. *Marks* is a preferred usage in many countries to designate impressions that in other countries (primarily the United States of America and Canada) would be characterized as *latent* impressions. In criminal records, the standard impressions are collected using forms named ten-print cards (Figures 1 and 2).

Early Fingerprint Classification

At the end of the nineteenth century, William Herschel and Henry Faulds set out the principles of the forensic use of fingerprints and fingermarks: the use of fingerprints and fingerprint collections for the identification of offenders, and the use of fingermarks to establish a link between a crime scene or an object and an individual.

Juan Vucetich of Argentina introduced the first system of fingerprint classification in 1891. The development and practical application of dactyloscopy for forensic use became known in law enforcement after the publication of the first manual and a system of fingerprint classification by Francis Galton. This led to the acceptance of the use of fingerprints for forensic use in Great Britain. Then, in 1900, Edward Richard Henry modified the classification system of Galton, which became the most widely used system under the name of Galton–Henry. The volume of paper-based ten-print card collections increased progressively during the twentieth century and workability was maintained by increasing the sophistication of the classification system, leading to a trade-off between selectivity and reliability [4].

AFIS Technology

Development

The work on automation of fingerprint identification started in the 1960s with the advent of computers. Manual searching of the ten-print card collections reached its limits, in terms of workload and efficiency. The United States of America and Japan concentrated on automation of the high-volume ten-print workload, whereas France and the United

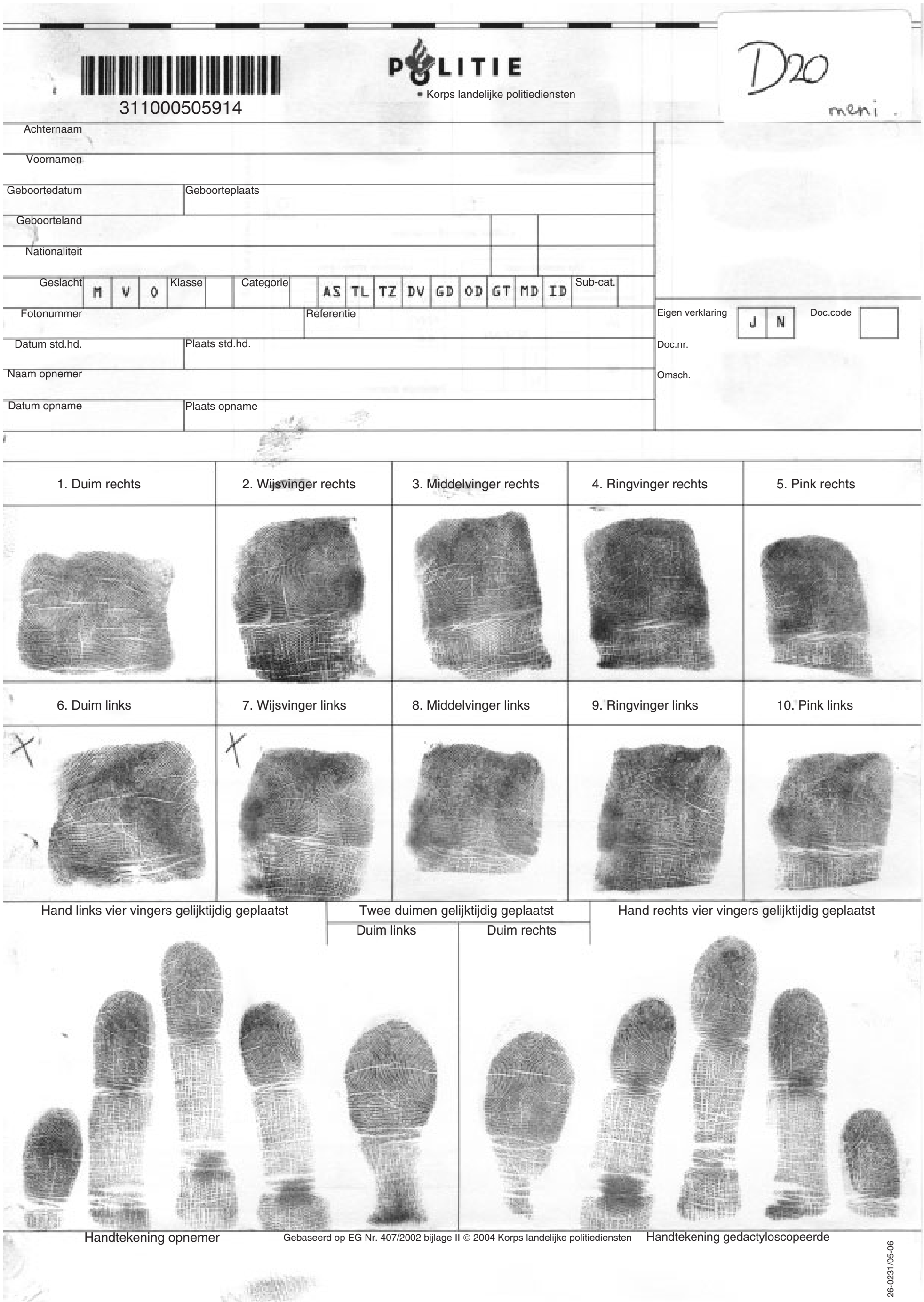

Figure 1 Example of a ten-print card

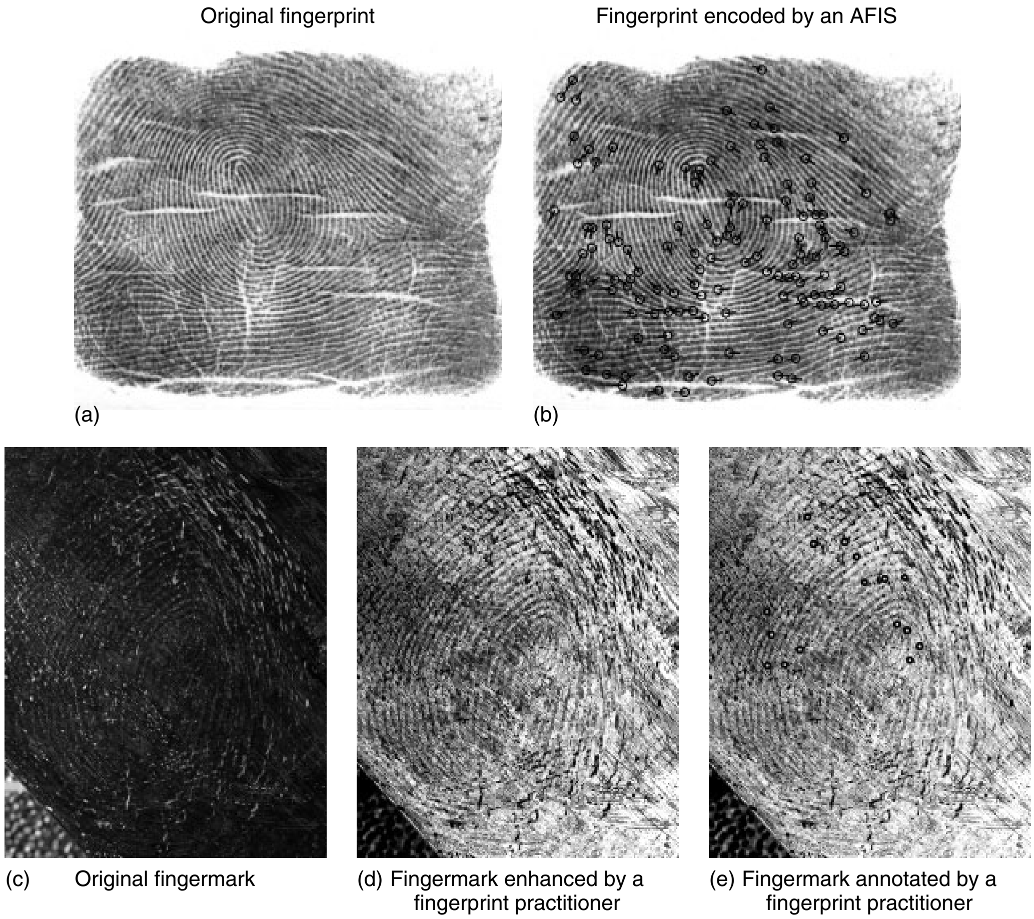

Figure 2 (a–e) Example of the encoding of a reference fingerprint and of a crime-scene fingermark from the same source

Kingdom focused more on automation of fingermark identification. After a decade of effort, digitization of the ten-print card and automatic extraction of minutiae became effective enough for the United States of America and the United Kingdom to produce automatic fingerprint reader systems. This advancement eventually permitted the digitization of the ten-print cards, thus permitting the storage of the standard impressions and the demographic data of individuals (e.g., name, citizenship, and date of birth) in a computerized database [5].

Image Capture. Currently, flatbed document scanners are used for the digitization of the ten-print cards, but the capture of standard impressions is also possible by rolling the finger friction ridge skin directly on fingerprint live-scan equipment. The imposition in controlled conditions allows for the images of the reference fingerprints to be of high quality. The fingermarks are captured from their initial support with digital cameras or scanned from analogue pictures. Their imposition in the uncontrolled conditions of the criminal activities implies that the quality of the fingermark images is impaired/limited by the possible conjunction of a complex background, a small image area, an unclear ridge structure, and large distortion. Image processing techniques are then applied to segment each fingerprint of a ten-print card as an individual image and to enhance the image parameters. Finally, the images are stored as 256 gray-level (8-bit-GS) images at a resolution of 500 or 1000 ppi (pixels per inch) and compressed at a ratio of about 1 : 15 using wavelet-based algorithms such as Wavelet Scalar Quantization (WSQ) or Joint Photographic Expert Group 2000 (JPEG2000 or JP2). The ANSI/NIST-ITL Data Format for the Interchange of Fingerprint, Facial and Other Biometric Information is used by the law enforcement agencies of more than 150 countries to exchange fingerprint data externally through Interpol, but also internally, for example, within Europe under the umbrella of the Prüm Treaty or within the Next Generation Identification Program (NGI) of the United States of America. Apart from describing how to store the fingerprint or fingermark, the most recent ANSI/NIST-ITL standard (1-2011) also describes how to store an Extended Set of (fingerprint) Features (FSA), e.g., the core and deltas of the general pattern, the incipient ridges, the creases and linear discontinuities, the ridge edge features and the pores [6].

Feature Extraction. In parallel to digitization, research has concentrated on classification. The first approaches translate the manual pattern classification into computer-friendly codes based on the shape of the papillary ridge flow; this shape is named general pattern and classified as first-level detail (Figure 3). This operation resulted in a potential elimination of the manual search and filing errors, but did not offset the original pattern type assignment errors [7]. Later, the fingerprint pattern classification was automated using the ridge direction extracted from the fingerprint images. However, this suffered from the same type of assignment errors [8]. A solution was found with the more precise automatic minutiae detection and the comparison of minutiae configurations. Minutiae are points of termination (ridge ending) or bifurcation of the papillary ridges; they are also named Galton points and classified as second-level detail (Figure 4).

Current AFISs use the position (x- and y-coordinates) and the tail angle (theta) of the minutiae as the core component of comparison, followed by the use of extended characteristics of the minutiae such as their basic type (ridge ending or bifurcation), the ridge count between pairs of minutiae, or the topology of the minutiae in combination with other features (Figure 3). The crucial elements in the success of this approach are the extreme typicality and robustness offered by the topology of the minutiae configurations and the development of robust image processing techniques to enhance the clarity of the papillary ridge structures.

The main stages of the feature extraction consist of an orientation field estimation, using information about local average directions of the ridges (gradient or ridge-valley algorithm), a ridge detection, using a thresholding algorithm given a gray-scale image, the ridge-valley algorithm, or a gray-level histogram decomposition, and a thinning of the ridges, by means of algorithms based on mathematical morphology [9]. These techniques allow for an accurate minutiae designation on high-quality fingerprint and fingermark images, as the ridges have well-defined frequency and orientation in local areas. They also

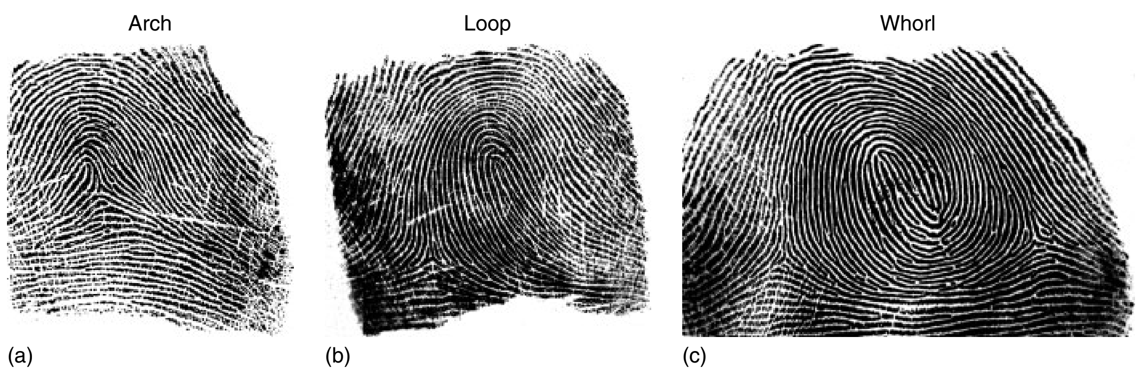

Figure 3 (a–c) Example of a general pattern (the ridges are black and the valleys are white)

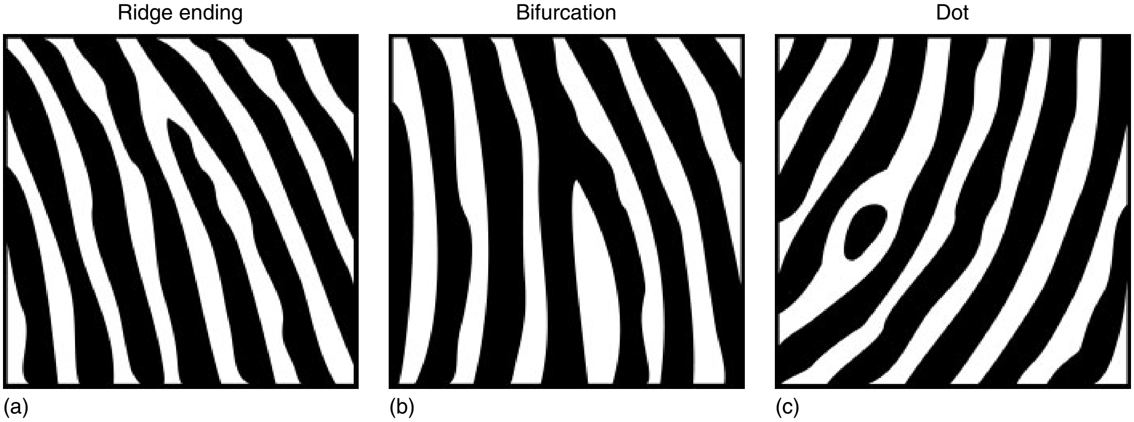

Figure 4 (a–c) Example of minutiae (the ridges are black and the valleys are white)

became outstandingly efficient on low-quality fingerprint and fingermark images. In the Netherlands, for example, more than 60% of the pairing of fingermarks and reference fingerprints is obtained using automatic encoding only. However, the technology still does not equal the ability of human friction ridge examiners for the last 40% of the cases.

Feature Comparison. Numerous methods have been developed to compare automatically fingermark and fingerprint images; however, they can be classified into two approaches: the correlation-based and the structural feature-based comparisons. The correlation-based comparison relies on global pattern matching; it consists in using translation and rotation to find the best superposition to compute the maximum correlation between two images. The structural feature-based comparison is based on the matching of extracted features; it consists in searching alignment between minutiae extracted from a fingermark and a fingerprint image and in finding the maximum number of minutiae pairing. The structural feature-based approach is more robust but requires more computation than the correlation-based comparison. In general, the result of the comparison is expressed as a score, which is a scalar number representing the similarity and the typicality of a fingermark and a fingerprint as a distance measure or a proximity index [10].

Forensic AFIS systems exploit these two approaches to optimize their performance, but the problem remains complex. This difficulty is mainly due to the uncontrolled conditions of production of fingermarks during criminal activity and the large variability of different impressions of the same finger, named within-finger variability. The main factors responsible for this within-finger variability are the ridge skin condition, the transfer of information with loss from a complete three-dimensional pattern to a partial two-dimensional pattern and the nonlinear distortions of the papillary ridges. These distortions result from the skin plasticity and from the movement of the finger during the production of the fingermark. These factors do not significantly affect the topological relationships of the papillary ridges and of the minutiae configurations, but they modify the shape of the papillary ridge flow and the absolute distance between any pair of minutiae. The key to fingerprint features comparison is to exploit the topological stability of the minutiae configurations despite the factors responsible for the within-finger variability.

The performance of the technology is significantly lower for the fingermarks comparison than for the plain or rolled fingerprints comparison because of the increased within-variability of the fingermarks and the limitation induced by quality of their images. The performance is often improved by conducting searches by multiple practitioners each performing several attempts varying the encoding of the fingermark [11]. Nevertheless, the current sophistication of the algorithms allows for the state-of-the-art AFIS technologies to reach a false rejection rate

(FRR) lower than 2% and a false acceptance rate (FAR) of 0.0001% in a task of identity verification comparing 500 ppi images of inked rolled fingerprints and partial not heavily distorted fingermarks containing 15 paired minutiae. Recent NIST benchmark tests of the different biometric fingerprint technology providers show that using 1000 ppi instead of 500 ppi images increases the performance modestly for most technologies. In addition, when some hits are gained with the increase in resolution, some others are lost [12].

Forensic Applications of AFIS

AFISs were originally designed to assist fingerprint practitioners in the forensic identification application. This application facilitates the practitioner to compare the ten fingerprints of a suspected person to all the standard impressions of the reference database to verify if he or she is already present in the database and, if present, to verify the demographic data. For this application, the fingerprint biometric technology has achieved enough maturity to offer an identity verification process that is virtually error-free from the technological point of view, although enrolment and clerical mistakes in the database or in the running of the process can never be excluded.

Such a degree of performance has materialized in a high level of automation of the forensic identification process, changing the human-technological interaction. The technology has grown from an assisting role to a leading role, letting a verifier role to the practitioner or taking over completely the human role in a fully automatic identification process, known as *lights out search*.

In the 1990s, the improvement of both the fingerprint biometric and the computer technologies made the semiautomatic processing of fingermarks possible. Allying the manual minutiae extraction of the practitioners to the automatic comparison of the AFIS allowed for the partial automation of the forensic investigation and intelligence applications using fingermarks. For forensic investigation, the selection of a short list of potential offenders could be produced automatically, based on the comparison of fingermarks found on crime scenes to the standard impressions stored in reference databases. For forensic intelligence, links between digitized fingermarks could be generated automatically.

Nevertheless, the fingerprint biometric technology maintains an assisting role in the forensic investigation and intelligence applications. The practitioner retains the leading role for the selection of candidates from a short list of potential sources in the investigation process and for the validation of the links between fingermarks in the intelligence process.

In the 2000s, the improvement of the computer mass storage, in terms of size and affordability, initiated the digitization of the complete ten-print cards (flat and rolled fingerprints as well as palmprints) and the possibility to digitize several ten-print cards for one individual. It has allowed for an extension of the forensic investigation and forensic intelligence process based on the use of palmmarks, which represent up to 30% of the marks recovered on crime scenes. In most countries, the development of large-scale palmprint databases remains an ongoing process; in the United States of America, for example, it will be fully implemented in the NGI Program that will incrementally replace the integrated automated fingerprint identification system (IAFIS) capabilities [11].

Despite its obvious progress, the implementation of technology in operational systems is largely perceived as a black box by the practitioners, because of the fact that they cannot always explain and follow the systems' results [3].

Future Challenges for AFIS Technology in Forensic Science

Automation and Transparency. Minutiae designation on low-quality fingerprint and fingermark images remains a computer-assisted process, combining the outstanding but subjective human pattern recognition ability and the more objective but also more limited computer ability. Both the human inconsistencies and the limits of the computer applications affect the performance of the feature extraction and, consequently, the performance of the forensic investigation intelligence processes based on the use of finger- and palmmarks. Thus, a feature extraction process at once reliable and completely automated is desirable. Steps in this direction can be done not only by refining the minutiae extraction process but also by enriching the feature vector with other available, measurable, discriminatory, permanent, and robust features such as the generalization of the use of the number of ridges between the minutiae.

Fingerprint practitioners need a better understanding of the functioning of the fingerprint technology implemented in the AFISs in order to operate the AFIS in a more transparent manner. In the absence of an authoritative source to help them interpret the results of the AFISs, they can only speculate about how the core algorithms are designed and what could influence their output. This is not without raising difficulties for the practitioners to be accountable for results driven by the technology [3].

Scalability, Interoperability, and Multimodality. The scalability of the paper-based ten-print collections was limited by the necessary trade-off between selectivity and reliability imposed by manual classification systems, and the coexistence of several systems around the world limited their interoperability at an international level. The implementation of AFISs solved the problem of scalability for the national fingerprint databases, but the interoperability problem remains as the first generations of AFIS incorporate feature vectors that are encoded using proprietary formats. Currently, the problem of interoperability between different types of AFISs is on the way to be solved partially by the widespread use of the ANSI-NIST biometric exchange file format, but the predominant use of proprietary formats for the feature vectors remains. This improvement opens a new opportunity in terms of scalability, with the possibility to extend the interoperability of the AFISs at a global level and to integrate the AFIS functionality into a broader platform for multimodal biometric identification, for example, including facial recognition, speech, and DNA. However, this opportunity also raises the challenge of merging the results from the different biometric modalities using fusion strategies adapted to the different forensic applications: forensic identification (decision), forensic investigation and intelligence (selection), and forensic evaluation (description) [1].

Forensic Fingermark Processes. In the forensic investigation and intelligence processes, the short lists of potential sources still predominantly a fixed size based on the rank information provided by the AFISs. The efficiency of these processes would be largely benefit from the lists of variable size, combining the information of the rank and score value to output a description of the strength of the link made between the fingermark and the reference fingerprint.

Forensic evaluation of fingermarks and fingerprints consists mainly in the inference of identity of the source of a fingermark and a fingerprint. Currently, this task remains mainly performed by friction ridge examiners. They apply the analysis, comparison, evaluation, verification (ACE-V) procedure and, in some countries, a numerical standard, to substantiate three types of qualitative opinions: identification, exclusion, or inconclusive. As their evaluation is deterministic, friction ridge examiners also make an implicit use of their own subjective probabilities of the rarity of the features used for identification. They refine these subjective probabilities through training and experience [13].

In forensic research, the inference of identity of the source of a fingermark and a fingerprint is also envisaged, combining statistical models, digitized fingerprint and fingermark databases, and a scientific methodology; namely the likelihood ratio approach based on Bayes' theorem. This new approach aims to offer a uniform framework and a transparent methodology to friction ridge examiners, and to assist them in producing a logical, testable, and quantitative evaluation of fingerprint evidence [14]. Prototypes for forensic fingermark evaluation exist and some rely on fingerprint biometric technology. However, their validation, including criteria about the robustness of the underlying assumptions and criteria about the precision, the accuracy, and the calibration of the results, is a critical step before their acceptance by the fingerprint scientific and legal communities [4].

References

[1] Meuwly, D. & Veldhuis, R.G.F. (2012). Forensic Biometrics: From two communities to One Discipline, *Proceedings of the BIOSIG 2012*, International Conference of the Biometrics Special Interest Group. 207–218.

[2] Whither Biometrics Committee National Research Council (2010). *Biometric Recognition: Challenges and Opportunities*, J.N. Pato & L.I. Millett, eds, The National Academies Press, Washington, DC.

[3] Smith, M.L., Noorman, M.E. & Martin, A.K. (2010). Automating the Public Sector and Organizing Accountabilities, *Communications of the Association for Information Systems* **26**(1).

[4] Neumann, C. (2012). Statistics and probabilities as a means to support fingerprint examination, in *Lee and Gaensslen's Advances in Fingerprint Technology*, R. Ramotowski, ed, CRC Press Llc, Boca-Raton, pp. 419–466.

[5] Berry, J. & Stoney, D.A. (2001). History and development of fingerprinting, in *Advances in Fingerprint Technology*, H.C. Lee & R.E. Gaensslen, eds, CRC Press, Boca Raton, pp. 1–40.

[6] Wing, B.J. (2013). The ANSI/NIST–ITL standard update for 2011 (data format for the interchange of fingerprint, facial and other biometric information), *International Journal of Biometrics* **5**(1), 20–29.

[7] Allen, R., Sankar, P. & Prabhakar, S. (2005). Fingerprint identification technology, in *Biometric Systems: Technology, Design and Performance Evaluation*, J.L. Wayman, A. Jain, D. Maltoni & D. Maio, eds, Springer-Verlag, London, pp. 21–61.

[8] Moore, R.T. (1991). Automatic fingerprint identification systems, in *Advances in Fingerprint Technology*, H.C. Lee & R.E. Gaensslen, eds, Elsevier Science Publishing Co., Inc, New York, pp. 163–191.

[9] Yager, N. & Amin, A. (2004). Fingerprint verification based on minutiae features a review, *Pattern Analysis and Application* **17**, 94–113.

[10] Uchida, K. (2005). Fingerprint identification, *NEC Journal of Advanced Technology* **2**(1), 20–27.

[11] Moses, K.R., Higgins, P., McCabe, M., Prabhakar, S. & Swann, S. (2010). Fingerprint Sourcebook-Chapter 6: automated fingerprint identification system (AFIS), *National Institute of Justice/NCJRS* **225326**, pp. 6-1–6-33.

[12] Indovina, M., Dvornychenko, V.N., Tabasse, E., Quinn, G., Grother, P., Garris, M. & Meagher, S. (2009). *Elft Phase II – An Evaluation of Automated Latent Fingerprint Identification Technologies*, National Institute of Standards and Technology, Gaithersburg, MD.

[13] Langenburg, G.M., (2012). A Critical Analysis and Study of the ACE-V Process, PhD thesis, University of Lausanne, Switzerland, pp. 355.

[14] Neumann, C., Evett, I.W. & Skerrett, J. (2012). Quantifying the weight of evidence from a forensic fingerprint comparison a new paradigm, *Journal of the Royal Statistical Society: Series A (Statistics in Society)* **175**(2), 371–415.

Didier Meuwly