# BIOMETRICS IN FORENSIC SCIENCE: CHALLENGES, LESSONS AND NEW TECHNOLOGIES

*Massimo Tistarelli*, Enrico Grosso* and Didier Meuwly***

*University of Sassari
Computer Vision Laboratory
Porto Conte Ricerche, Tramariglio, Alghero
email:tista,grosso@uniss.it ; http://visionlab.uniss.it

**Netherland Forensic Institute
The Hague, Netherlands
email:d.meuwly@nfi.minvenj.nl; http://www.forensischinstituut.nl

## ABSTRACT

Biometrics has historically found its natural mate in Forensics. The first applications found in the literature and over cited so many times, are related to biometric measurements for the identification of multiple offenders from some of their biometric and anthropometric characteristics (tenprint cards) and individualization of offender from traces found on crime-scenes (e.g. fingermarks, earmarks, bitemarks, DNA). From sir Francis Galton, to the introduction of AFIS systems in the scientific laboratories of police departments, Biometrics and Forensics have been "dating" with alternate results and outcomes. As a matter of facts there are many technologies developed under the "Biometrics umbrella" which may be optimised to better impact several Forensic scenarios and criminal investigations. At the same time, there is an almost endless list of open problems and processes in Forensics which may benefit from the introduction of tailored Biometric technologies. Joining the two disciplines, on a proper scientific ground, may only result in the success for both fields, as well as a tangible benefit for the society. A number of Forensic processes may involve Biometric-related technologies, among them: Evidence evaluation, Forensic investigation, Forensic Intelligence, Surveillance, Forensic ID management and Verification.

The COST Action IC1106 funded by the European Commission, is trying to better understand how Biometric and Forensics synergies can be exploited within a pan-European scientific alliance which extends its scope to partners from USA, China and Australia.

Several results have been already accomplished pursuing research in this direction. Notably the studies in 2D and 3D face recognition have been gradually applied to the forensic investigation process. In this paper a few solutions will be presented to match 3D face shapes along with some experimental results.

## 1. INTRODUCTION

Forensic science is defined as the body of scientific knowledge and technical methods used to solve questions related to criminal, civil and administrative law. Biometric technologies are the set of automated methods used for the recognition of individuals using their physiological and behavioral traits. Forensic biometrics can be defined as the scientific discipline that makes use of the biometric technologies for the demonstration of the existence and the investigation of infringements, the individualization of perpetrators and the description of modus operandi. These tasks are embedded in several forensic processes: forensic investigation, forensic evaluation, forensic intelligence, automated surveillance and forensic identity management.

Methods like, the forensic anthropometry (Bertillon), the forensic dactyloscopy (Galton) and "le portrait parlé" (Reiss), exploiting physiological and behavioral traits, since the end of the 19th century have been used for the identification of criminals as well as for the transmission of the information relevant for remote identification. From the 1960s the development and implementation of automatic fingerprint identification systems (AFIS) represent the first forensic deployment of biometrics, with the automation of the identity verification process [1]. This is also used for the automation of the first step of the individualization process (selection/rejection of candidates). In the 1980s the discovery of forensic DNA profiling led to identity verification process from DNA reference material and the individualization process from biological traces.

In the 1990s the development of computer science and signal processing allowed a performance breakthrough of biometric technologies, offering practical solutions for access control based on several modalities. Speaker, face and gait recognition became of interest for forensic biometrics, as a consequence of the development of mobile telecommunication and surveillance technologies (CCTV). During the same decade the first solutions integrating biometric technologies and the Bayesian inference framework were proposed for forensic individualization, with the aim of ensuring a logical and transparent approach for the evaluation of the biometric forensic evidence.

In the last decade interest has arisen in so-called soft biometric modalities, based on biometric features such as height, weight, gender, hair, skin and clothing color. This interest is mainly due to their availability of data, allowing capture without constraint that is a prerequisite in surveillance environments. However, their limited typicality enhanced the necessity to consider the fusion of several modalities. Some aspects of this technological progress are potentially interesting for forensic biometrics, for example the estimation of the body height and body weight from individuals present on still and live images. Attempts to combine several biometric modalities are not only of interest for forensic biometrics but for forensic science in general, as it is related to the combina-

tion of forensic evidence [2, 3]. The critical gap is the analysis of all the forensic processes that can integrate biometric technologies, to understand their specificities and translate them in clear needs, for the biometric community to be able to propose specific solutions.

A number of Forensic processes may involve some sort of Biometric-related technology, among them:

- Evidence evaluation. Likelihood ratio-based method to quantify the evidential value of biometric traces
- Forensic investigation. List of putative sources of biometric traces from one or several combined modalities
- Forensic Intelligence. Grouping of putative sources of biometric traces on basis of one or several combined modalities
- Surveillance. Capture of biometric traces and detection of putative sources on the basis of one or several combined modalities
- Forensic ID management and ID Verification. ID infrastructure and management, ID processes (create, challenge (access control / ID verification) and end an identity)

Several results have been already accomplished pursuing research in this direction. Notably the studies in 2D and 3D face recognition are being gradually applied to the forensic investigation process. [4]

## 2. BIOMETRIC CHALLENGES IN FORENSICS

Obtaining and using biometric evidence from the multimedia content available on social networking sites is a promising forensic activity for which the forensic community lacks biometric solutions. On the other hand the biometric community has developed technologies that are still not fully implemented in all the possible forensic processes:

- Even though uniqueness is not an issue in some forensic processes [5], several law enforcement applications still require the extent to which fingerprints coded in AFIS systems are unique to individuals.
- The role of the human operator in comparing the results of automated processing of fingerprints, facial images, etc.
- Systems engineering approaches to the application of biometric recognition in a forensic context
- Coding of scars, marks and tattoos; and a quantitative assessment of their contribution to identification or verification of identity
- The role of international standards and codes of practice to support research as well as in the interchange of forensic information
- Establishing robust test procedures (on the lines of work undertaken in the testing of biometric devices, software and systems in the ISO 19795 series of standards)
- Development of privacy-enhancing techniques to reduce privacy invasion in the collection and processing of material relating to people who are only incidentally involved in a capture event (e.g. processing a video stream in a crowded public place, where many hundreds of individuals are involved).

The EU COST Action IC1106 "Integrating Biometrics and Forensics for the Digital Age" represents an ideal opportunity for the Biometric and Forensic communities to join and understand each others needs, challenges and opportunities in a realistic manner. These synergies will lead to the development of a coherent joint vision and its dissemination across disciplinary and geographical borders [6].

### 2.1 Biometric evidence for forensic evaluation and investigation

Biometric data analysis may be of pivotal importance at any stage of the course of justice, be it the very first police investigation or a court trial. In the police investigative mode, reasoning follows a process of generating likely explanations, testing these with new observations and eliminating or re-ranking the explanations. In the forensic evaluative mode for a court trial, an opinion of evidential weight, based upon case specific propositions (hypotheses) and clear conditioning information (framework of circumstances) should be provided for use as evidence in court. The main objective of this task is to establish a robust methodology for forensic automatic biometric recognition based on statistical and probabilistic methods. Such a methodology should provide guidelines for the calculation of biometric evidence value and its strength and the evaluation of this strength under operating conditions of casework. This theoretical approach and corresponding design methodology are intended to bridge the gap between forensics and biometrics. This task involves several aspects of the forensic casework process: from the collection of evidence to the evaluation of the strength of evidence, to provide a unified framework which models the assumptions, conditions, and uncertainty implicit in the casework. A complete set of interpretation methods, based on the likelihood ratio approach, needs to be defined independently of the baseline biometric recognition system [7]. It should also define the integration procedure of these interpretation methods with the state-of-the-art automatic biometric recognition algorithms.

### 2.2 Audiovisual biometrics for forensics examination

Nowadays digital evidence rather than physical evidence is increasingly getting easier to acquire from the scene of crime or cyber-crime. [1]

In fact, the Internet, computers, video surveillance cameras, mobile phones, telephone networks, social networks are all examples of methods for generating, collecting and sharing information on a massive scale. Therefore, by exploiting biometric technologies it will be possible to capture identity information from strong biometric data left on the scene of a crime, like:

- facial imaging (face, ear, iris) which can be acquired from both single images and surveillance video recordings, etc.;
- voice recording acquired from video sequences, ambient microphones, phone call recordings;
- Audio-visual recording containing lip-motion and faces;
- gait information acquired from video sequences.

In many cases, face and iris samples are not ideal since they depend on the camera position, occlusions, and the degree of cooperation of the suspected person. This information must be complemented with other sources of evidence like voice recording, lip-motion, gait information, etc.

[1]Some of the forensic concepts developed for physical evidence may be transposed to digital evidence, some other not, due to the property of digital information. It is desirable to define the extent and limits of such a transposition. For example the question of chain of evidence is different for the physical and digital evidence.

Audio-visual speech can be also useful to determine the authenticity of a recorded media. This is a challenging task because of the enormous amount of recorder data and the non-cooperative acquisition scenario, which may reduce the recognition accuracy. Interactive multimodal biometric authentication techniques, using quality and reliability measures, offer a potential solution. In the near future, audiovisual biometrics could be regarded as the best starting point of forensic investigations, also to orient the collection of physical traces.

### 2.3 Soft biometrics for forensics examination

Soft biometrics like age, gender, ethnicity, height, weight, eye color, hair style, can not be used to authenticate individuals since they lack of sufficient permanence and distinctiveness. Nevertheless, they can be used as ancillary information to support the forensic evaluation process to either narrow down the field of search or if only partial strong biometrics data are available. Moles, freckles, birthmarks, scars, marks, and tattoos possess higher discriminative capabilities. Being permanent imprints on the body, they can be used to assist the process of people identification in forensic applications or disaster recovery. Automating the accrual of evidential value, based on soft biometrics, would provide experts a valuable tool for: supplementing the decision made from other biometrics (like face, iris, etc); improving the identification accuracy: increasing the search speed in a database with hierarchical searches; improving the strength of evidence, also when partial information is available.

### 2.4 Forensic behavioral biometrics

From a forensic perspective, it is becoming increasingly important being able to infer various aspects about criminal activities. As such, biometric data are not only usable in forensic science for inference of identity of source, but also for inference at activity level. Either single user or crowd behavioral analysis is one of these aspects. Given an audio visual or visual scene is there any unusual or abnormal event taking place in the scene? Are there any specific contexts or events that will change the behavior of the scene dynamics by triggering other events without necessarily leading to unusual events? For instance, it is expected that when a train is near its departure time, that many individuals start running to catch it. One of the major difficulties in extracting useful information from a long dynamic visual flow, is the identification of that small portion of data that contains important information. Algorithms that could automatically detect unusual events within streaming or archival audio/video would significantly improve the analysis efficiency and save valuable human attention for only the most salient content. For example, algorithms for real time scene analysis, fight scene detection, weapon detection, etc. The outcome of this research task is to associate Actions/events with a group, identifying the role of the various individuals leading up to the potentially criminal activities. In this framework special focus will be on real time analysis of the actions to detect a suspect behavior in order to prevent crime.

### 2.5 Biometric analysis of crime scene traces and their forensic interpretation

The collection of forensic traces from a crime scene involves a number of different processes which may be used for evidential purpose. Biometric technologies can be deployed to process data from:

- latent fingerprints and palmprints;
- written documents (signatures and handwriting analysis, etc.).

At the crime scene, fingerprints and palmprints can be found on many different surfaces [8]. Although fingerprints have been studied for decades, both in the forensic and in the biometric community, the progress made followed parallel and almost never convergent tracks. The potential convergence can be investigated by adopting high resolution optical capturing devices, to obtain non destructive quality measurements. For example, recovering the age of a latent fingerprint can be very important to determine if the suspect was present before or after a crime took place. [2] Moreover, the use of the *whole* electromagnetic spectrum (from infrared to X-rays) may track potential biometrics, even in a covert mode, such as latent finger and palm marks, for a subsequent forensic analysis (e.g. contaminations, DNA, etc.).

Novel means of fingerprints and palmprints visualization can be addressed. Especially when a conventional treatment is unlikely to work, such as on metal surfaces subject to extreme conditions [9]. Techniques that extend the range of treatments available for latent fingerprint visualization, all of which would extend the usefulness of an AFIS database in searching for offenders, would be very useful.

Written documents represent another source of physical evidence that is used by forensic experts and whose analysis can benefit from the studies conducted in the biometric field on both signature and handwriting analysis. The focus of this research should be on the development of pattern recognition algorithms, to complement and expedite the experts judgment. Algorithmic solutions for a semantic analysis, i.e. for extracting and representing the contextual usage meaning of words, by means of statistical processes applied to a large corpus of text, can be also exploited to infer the users identify.

### 2.6 Combination of multimodal biometrics with other forensic evidence

Data fusion may involve the same biometric trait, acquired from different devices, or different traits from different sources. For example, the same walking individual can be acquired by different surveillance cameras placed in different locations. On the other hand, several data like gait, face, ear, voice, can be acquired from the same video. This data needs to be properly represented, with feature extraction techniques, and fused. In the forensic community, little or no effort has been devoted to the multimodal integration and fusion of data from multiple sensory channels. On the contrary, multimodal data fusion has been extensively studied by the biometrics community. This may resort in a multidisciplinary approach where techniques for effective evidential evaluation, based on fragmentary evidence, object and behavior recognition, are concurring to provide a robust support for the case, in agreement with the appropriate privacy/legal requirements and recommendations. Soft biometrics may be also exploited, together with other sources of evidence, to provide support to the hypothesis of criminal behaviour.

[2] Research on datation in forensic science exists (in the fingerprint field and others) and has proven extremely difficult as the environmental parameters are unknown.

### 2.7 Ethical and societal implications of emerging forensic biometrics

It is of crucial importance for law enforcement practices to accomplish with key democratic principles and fundamental human rights. Three main areas of intervention should be considered:

- Impact on Fundamental Rights: according to the Strategy for the effective implementation of the Charter of Fundamental Rights by the European Union (COM(2010) 573 final, the Charter Strategy) adopted by the Commission on 19 October 2010, all EU policies should be assessed against their impact on fundamental rights. This holds true in particular for RTD policies and technologies concerning justice and law enforcement.
- Impact on Privacy and Data Protection: the likely impact of new and emerging biometrics on privacy and data protection should be assessed and specific guidance issued. In particular, the possibility to adopt a privacy by design approach to forensic biometrics, should be explored. Policy issues concerning international biometric data sharing for forensic purposes and the establishment of crossborder biometric forensic databanks, are also relevant.
- Impact on vulnerable and disadvantaged groups: the risk that the implementation of new forensic biometrics may produce discrimination against ethnical and religious minorities, low income or geographically dispersed populations, children and minors, persons with disabilities and aging population, should be carefully assessed and minimized.

This process may result in increasing the understanding of non-technical challenges of emerging forensics biometrics among the international scientific community and in strengthening the Biometric-Forensic EU COST IC1106 network.

## 3. 3D TO 2D FACE RECOGNITION

The analysis of 3D face data is very promising in improving the identification performances of individuals. 3D acquisition systems are also becoming affordable, user friendly and easy to install in different environments. For these reasons it is envisaged that, in the near future, 3D face acquisition and matching can be successfully employed in forensic applications as well.

There are different scenarios where three-dimensional data can be acquired and used to to provide forensic evidential value to face images in criminal investigations:

- (3D to 3D) The conventional face mug shots taken from arrested criminals are substituted with a full 3D representation of the face. A 3D face can be obtained from a video acquired by a surveillance camera in the crime scene. The degree of similarity of two 3D faces is computed to accrue evidence for a potential suspect.
- (3D to 2D) As in the previous case, a 3D face representation is available from a list of suspects, but only a 2D face image is available from the crime scene. The 3D face representation is used to generate a synthetic 2D view of the face and perform the matching with the face image taken from the crime scene.

In order to perform the 3D to 2D matching a number of salient features are extracted from the two face images. The similarity is determined by comparing the two feature-based representations.

## 4. PATTERN MATCHING ALGORITHM

3D face data is acquired for enrolment while 2D face images are used for identification. This is the case of convicted criminals whose 3D faces were acquired and stored, while 2D snapshots or a video clip is available from the crime scene. In this case the police officer should be able to identify the criminal whose face is depicted in the captured image or video. In most cases identification from images taken from a surveillance camera is quite difficult because the face is often rotated with respect to the camera. Having 3D face data allows to re-project face images with any orientation and use these images to perform the matching.

To perform the matching a series of 2D views were first produced, corresponding to 9 different head orientations, spaced 30 degrees along the horizontal and vertical axes. The 2D projections and the test images are aligned and scaled according to the positions of the eyes and the mouth. To ensure the proper scale and position on the 2D image plane a simple planar affine transformation is adopted. The image brightness is also normalized with a multi-window histogram equalization technique. Finally all 2D projections of all subjects are matched against the probe 2D face image.

The face matching algorithm is based on the comparison of the Scale Invariant Feature Transform (SIFT) feature sets extracted from the probe and gallery (3D projected) images [20]. One of the interesting features of the SIFT approach is the capability to capture the main gray-level features of an object's view by means of local patterns extracted from a scale-space decomposition of the image.

In order to perform the matching the SIFT features are first extracted from the gray scale images [21]. The matching score is computed, as proposed in [20], by counting the number of most similar SIFT features in the probe and gallery images. As several views are projected for each subject it is expected that the 2D projection corresponding to the closest head orientation of the probe image produces the smallest matching score.

Several tests were performed to determine the expected performances of the proposed biometric technology as a potential forensic application. Six out of the total nine 2D projected images of one subject are shown in figure 1. In figure 2 the test and probe image, with the same head orientation and registered with the extracted SIFT features are shown. The genuine and impostor score distributions, obtained by performing a complete matching test on the acquired dataset, are shown in figure 3. The equal error rate computed from the two distributions is equal to 4%. [3]

## 5. CONCLUSION

Biometrics and Forensics have an undiscussed strong potential for mutual cross-fertilization. Several forensic processes may be automated and rationalized by the introduction of

[3]It is worth noting that even though the EER provides a good performance indication for the technology evaluation, in the forensic evaluation scenario, some more appropriate metrics have been developed, such as [22]:

- Tippet plot, rates of misleading evidence (RMEP, RMED);
- Empirical Cross Entropy (ECE) and Cost Log Likelihood Ratio (Cllr);

biometric classification algorithms. Several forensic traces and sources of evidence in criminal cases may be better analyzed and represented by means of feature extraction techniques. Different traces and evidence sources could be more efficiently combined by means of multibiometric techniques. Some examples of how biometrics may complement forensic science have been discussed. Practical implementations and further studies are the subject of a newly started pan-European network (EU COST Action IC1106) aiming to the development of a task force to properly address and solve these as well as other emerging issues in forensic biometrics.

Face-based identification has been extensively used in forensic applications. Generally 2D face images are captured both from convicted criminals and in the crime scene. We argue that 2D face images do not convey enough information to perform automatically a reliable matching of a probe and gallery pair. Extremely different acquisition conditions between the enrollment set-up and the crime scene make it difficult to compare images from the same subject. While mug shots are taken from criminals with a camera directly looking at the subject's face, the pictures taken from the crime scene generally originate from surveillance cameras looking at faces from above. A viable solution is to exploit the information content of a full 3D face, at least for the enrollment phase.

In this paper a forensic scenario has been considered where a 3D face representation is available from a list of suspects, but only a 2D face image is available from the crime scene. The 3D face representation of the suspect is used to generate a synthetic 2D view of the face and perform the matching with the face image taken from the crime scene. 3D to 2D experiments are presented producing promising results. Improvements are expected by increasing the number of synthetic head pose variations in the training set.

## REFERENCES


[1] D. Maltoni, D. Maio, A.K. Jain and S. Prabhakar. Handbook of Fingerprint Recognition. *2nd Edition*, Springer, 2009.

[2] A. Ross, K. Nandakumar and A.K. Jain. Handbook of Multibiometrics. Springer, 2006.

[3] M. Tistarelli, R. Chellappa and S.Z. Li. Handbook of Remote Biometrics. Springer, 2009.

[4] D. Meuwly, and R. Veldhuis. Forensic biometrics: From two communities to one discipline. *Proc. of the International Conference of the Biometrics Special Interest Group (BIOSIG)*, IEEE, 2012.

[5] S.A. Cole. Forensics without uniqueness, conclusions without individualization: the new epistemology of forensic identification. *Law, Probability and Risk*, 8(3):233–255 2009.

[6] The Proposers of the COST Action IC1106. Integrating Biometrics and Forensics for the Digital Age. *Memorandum of Understanding* of the European Commission, 2012.

[7] C. Neumann, I.W. Evett, and J. Skerett. Quantifying the weight of Evidence from a forensic fingerprint comparison, a new paradigm. *J. R. Statist. Soc. A*, 175(2):1–26, 2012.

[8] C. Champod, C. Lennard, P. Margot, and M. Stoilovic. Fingerprints and other ridge skin impressions. CRC Press, 2004.

[9] M. Tahtouh, J. Kalman, C. Roux, C. Lennard, and B. Reedy. The Detection and Enhancement of Latent Fingermarks Using Infrared Chemical Imaging. *J. Forensic Sci.*, 1(1):1–9, 2005.

[10] A.F. Abate, M. Nappi, D. Riccio, and G. Sabatino. 2D and 3D face recognition: A survey. *Pattern Recognition Letters*, 28:1885–1906, 2007.

[11] P. Besl and N. McKay. A method for registration of 3-D shapes. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 14(2):239–256, 1992.

[12] A.M. Bronstein, M.M. Bronstein, and R. Kimmel. Three-dimensional face recognition. *Int. Journal of Computer Vision*, 64(1):5–30, 2005.

[13] M.I. Cadoni, M. Bicego, E. Grosso. "3D Face Recognition Using Joint Differential Invariants" *Proc. of the 3rd Int.l Conference on Biometrics ICB09*, pp. 11–25, June 2009.

[14] I. Mpiperis, S. Malassiotis, and M.G. Strintzis. 3-D face recognition with the geodesic polar representation. *IEEE Transactions on Information Forensics and Security*, 2(3 Part 2):537–547, 2007.

[15] F.R. Al-Osaimi, M. Bennamoun, and A. Mian. Integration of local and global geometrical cues for 3D face recognition. *Pattern Recognition*, 41(2):1030–1040, 2008.

[16] A. Colombo, C. Cusano, and R. Schettini. 3D face detection using curvature analysis. *Pattern Recognition*, 39(3):444–455, 2006.

[17] C. BenAbdelkader and P.A. Griffin. Comparing and combining depth and texture cues for face recognition. *Image and Vision Computing*, 23(3):339–352, 2005.

[18] C. Beumier and M. Acheroy. Face verification from 3D and grey level cues. *Pattern Recognition Letters*, 22:1321–1329, 2001.

[19] K. Bowyer, K. Chang, and P. Flynn. A survey of approaches and challenges in 3D and multi-modal 3D + 2D face recognition. *Computer Vision and Image Understanding*, 101:1–15, 2006.

[20] D. Lowe. Distinctive image features from scale-invariant keypoints. *Int. Journal of Computer Vision*, 60(2):91–110, 2004.

[21] M. Bicego, A. Lagorio, E. Grosso and M. Tistarelli. On the use of SIFT features for face authentication. *Proc. of Int Workshop on Biometrics, in association with CVPR 2006*, 2006.

[22] D. Ramos. Forensic Evaluation of the Evidence Using Automatic Speaker Recognition Systems. *EURASIP Library of Phd Theses*, Universidad Autonoma de Madrid, November 2007.

Figure 1: Sample 2D images obtained by projecting the 3D texture mapped model.

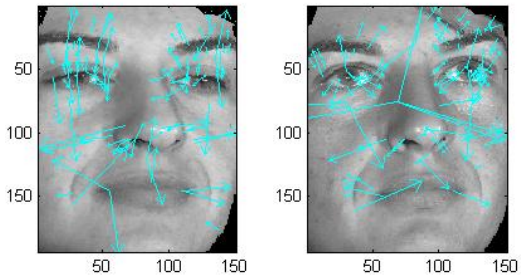


Figure 2: (left) SIFT computed from a 2D test face image. (right) SIFT extracted from the corresponding pose-projected 3D face from training.

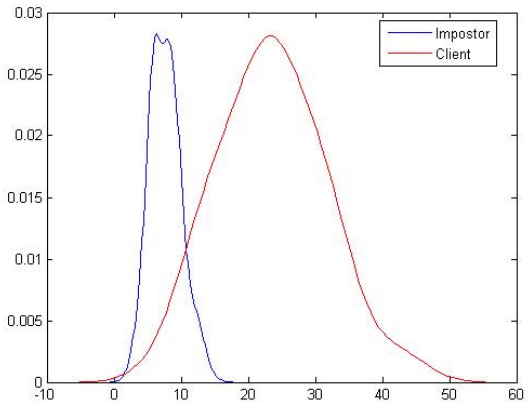


Figure 3: Impostor and client score distribution computed with the 3D to 2D matching using the SIFT features and using the global distance of the features. In forensic science these distributions are often termed "*between-source* variability of the features for the relevant population" and the "*within-source* variability of the features for the suspected person".