Forensic Face Recognition: A Survey

Tauseef Ali, Raymond Veldhuis, Luuk Spreeuwers Signals and Systems Group, FEMCS, University of Twente, Enschede, The Netherlands

Abstract

Beside a few papers which focus on the forensic aspects of automatic face recognition, there is not much published about it in contrast to the literature on developing new techniques and methodologies for biometric face recognition. In this report, we review forensic facial identification which is the forensic experts' way of manual facial comparison. Then we review famous works in the domain of forensic face recognition. Some of these papers describe general trends in forensics [1], guidelines for manual forensic facial comparison and training of face examiners who will be required to verify the outcome of automatic forensic face recognition system [2]. Some proposes theoretical framework for application of face recognition technology in forensics [3] and automatic forensic facial comparison [4, 5]. Bayesian framework is discussed in detail and it is elaborated how it can be adapted to forensic face recognition. Several issues related with court admissibility and reliability of system are also discussed.

Until now, there is no operational system available which automatically compare image of a suspect with mugshot database and provide result usable in court. The fact that biometric face recognition can in most cases be used for forensic purpose is true but the issues related to integration of technology with legal system of court still remain to be solved. There is a great need for research which is multi-disciplinary in nature and which will integrate the face recognition technology with existing legal systems. In this report we present a review of the existing literature in this domain and discuss various aspects and requirements for forensic face recognition systems particularly focusing on Bayesian framework.

1. Introduction

Face recognition is one of the most important task forensic examiners carry out manually during their investigation when there is a video or image available from crime scene. Forensic examiners perform manual examination of facial images or videos for a match with huge database of mugshots. The use of automated system aimed at facial recognition will not only improve the efficiency of forensic work performed by various law enforcement agencies but will also standardize the comparison process. However, until now, there is no working face recognition system that has been accepted within the judicial system. A face recognition system must be thoroughly evaluated and verified before it can be utilized for forensic applications. Although biometric face recognition has been used for secure building access, border control, Civil ID and login verification, however, there is no such system exists which can be used for identification or verification in crime investigation such as comparison of images taken by CCTV with available database of mugshots. A state-of-the art face recognition systems such as [6, 7] can be used for this purpose however there are several issues which are specific to forensic domain need to be addressed and integrated with technology.

First and foremost, the consequences of a wrong decision made by forensic face recognition are far severe from biometric face recognition. Although a large number of biometric face recognition

systems are currently in use [8], their results are not generally robust [9]. The reason has been the enormous variability both in faces such as pose, lighting conditions, facial expression as well as in imaging systems itself such as image quality, resolution and compression.

Secondly, a score based biometric recognition system is not suitable to judicial system where the objective of the automatic system is to give a probability or degree of support for one hypothesis against the other incorporating the prior knowledge about the case in hands rather than giving a binary decision [10, 11].

Finally it should be mentioned that in forensic scenario the quality of images available for processing is generally low such as images of crime scene from CCTV. Such images are usually of low resolution as well as unrestricted pose and sometimes even images of half occluded faces. However, recognition task in forensic framework is 'offline' in contrast to biometric system where a decision is to be made in real-time, e.g., user access system at a building or border control scenario. The algorithm for forensic face recognition therefore has less time constraint and to certain extent human involvement generally does not effect the overall objective of the system.

In the context of forensic identification, a related field is forensic facial reconstruction (or approximation) which aims to reproduce lost or unknown face of an individual for the purpose of recognition or identification [12]. This is usually performed with starting with the skull of a deceased [13].

In this paper, we review existing literature on forensic face recognition. Where a paper is pure theoretical description, a short summary is presented. For experimental works, overall conclusions and results are discussed. There are only a few papers focusing on forensic application of face recognition mainly because more effort is done on the improvement of technology itself rather than its application. However, as the performance of face recognition system improves there is a great need for integration of technology with legal system and a uniform framework for application of face recognition technology in forensics.

The rest of the paper is organized as follows: In section 2, we discuss the techniques and methodologies used by forensic examiners for purpose of facial comparison. Section 3 presents a literature review of forensic face recognition. In section 4 we briefly discuss Bayesian framework and how it can be applied for forensic face recognition. Section 5 discusses reliability and court admissibility issues associated with forensic face recognition. Section 6 present conclusions and some future research directions in forensic face recognition domain.

2. Forensic Facial Identification

Facial identification refers to manual examination of two face images or a live subject and a facial image to determine whether they are same persons or not. Facial identification methods can generally be classified into the following four categories.

Holistic Comparison: In this approach faces are compared by considering the whole face simultaneously.

Morphological Analysis: In this approach individual features of face are compared and classified.

Photo-anthropometry: This approach (sometimes referred to as photogrammetry) is based on the spatial measurements of facial features as well as distances and angles between facial landmarks.

Superimposition: In this approach, scaled version of one image is overlaid onto another. The two images must be taken from same angle.

The choice of specific approach is usually dependant on the face images to be compared and generally combinations of these methods are applied to reach a conclusion.

Beside the above general categorization of facial comparison approaches, currently there is no standard procedure and agreed upon guidelines among forensic researchers. The process is very subjective and opinion of one forensic examiner may vary from other.

2.1 Working Groups

There are several working groups active in this area whose aim is to standardize the procedure as well as the proper training of facial comparison experts. One of the best effort toward developing standards and guidelines for forensic facial identification is currently carried out by Facial Identification Scientific Working Group (FISWG) [14]. It works under Federal Bureau of Investigation (FBI) Biometric Center of Excellence (BCOE). FISWG focusing exclusively on facial identification and develop consensus, standards, guidelines, and best practices for facial comparison. Currently they have developed drafts of several useful documents in this regard which include a description of facial comparison, facial identification practitioner code of ethics, training the experts to perform facial comparison. These documents are available for public review and comments [14]. Some other workgroups active in developing standards and guidelines for forensic facial comparison includes International association for identification [15] and European network of forensic science institutes (ENFSI) [16]. The standardization of the process of facial comparison and specific guidelines which are agreed upon by forensic community is still an unsolved problem.

2.2 Forensic Examiner's (Manual) Facial Comparison

In this section we briefly review the forensic expert's way of facial comparison. The discussion is based on the guidelines set forward by the workgroup on face comparison at Netherlands Forensic Institute (NFI) [17, 18] which is a member of ENSFI [6]. The facial comparison is based on morphological-anthropological features. In most cases it is tried to obtain pictures to be in same posture. The comparison mainly focuses on:

- Relative distance among different relevant features
- Contour of cheek- and chin-lines
- Shape of mouth, eyes, nose, ears etc
- Lines, moles, wrinkles, and scars etc in face

When comparing faces manually, it should be noted that differences can be invisible due to underexposure, overexposure, resolution too low, out-of-focus and distortions in imaging process. Furthermore, similar features can result in different depictions due camera position compared to head, insufficient resolution, difference in focusing of two images, and distortion in imaging process.

Due to aforementioned effects which usually make the comparison process difficult, the anthropological facial features are visually compared and classified as: Similar in details, Similar, No observation, Different, Different in details. Apparent similarities and differences are further evaluated by classifying features as: weakly discriminating, moderately discriminating, and strongly discriminating. Conclusion based on this comparison process is a form of support for either of the hypothesis and can be stated as "no support", "limited support", "moderate support", "strong support", and "very strong support". The process is subjective to great extent and conclusion of one expert can be different than other.

There is a great need to automate the process since it will not only improve the speed of comparison but also it will help standardize the process.

3. Literature Review

In this section we briefly review existing literature on forensic face recognition. Our review is specifically focused on works which are discussing forensic aspects and applications of the technology in hand rather than techniques for biometric face recognition where there are already good surveys available [8, 19].

3.1 Forensic Biometrics from Images and Videos at Federal Bureau of Investigation [1]:

This paper gives a description of FBI's Forensic Audio, Video and Image Analysis Unit (FAVIAU) forensic recognition activities that they perform manually. Types of manual tasks include voice comparison, facial comparison, height determination, and other side by side image comparisons. FAVIAU is keenly interested in development and evaluation of the statistics of personnel individualization and of biometric systems. Two types of examinations that involve biometrics are photographic comparisons and photogrammetry [20]. Currently, in both of these types of cases, the forensic examinations are performed manually.

Photographic comparisons mean one-to-one comparisons of person in question and known. The characteristics used to carry out photographic comparisons can broadly be categorized as class and individual characteristics [21]. Class characteristics such as hair color, overall facial shape, presence of facial hair, shape of nose, presence of freckles, etc places an individual within a class or group. Individual characteristics such as number and location of freckles and scars, tattoos, number and position of wrinkles etc are unique to individual and can be used to individualize a person.

Photogrammetry [20] determines the spatial measurements of objects using photographic images. It is usually used to determine the height of a questioned individual or to determine the length of a weapon used in the crime.

The author further discusses some current and past research projects in forensic recognition field and point out some future research avenues which are more general to forensic recognition and not specific to forensic face recognition.

3.2 Facial Comparison by Subject Matter Expert: Their Role in Biometrics and Their Training [2]:

This paper describes the need for facial comparison experts which will be needed to verify the results of future forensic face recognition systems. It emphasizes on the systematic training of individuals who will be working in association with these systems. In any automated face recognition system, the ultimate judgment is the manual verification of the outcome of the system. In case of fingerprint technology, there are a lots of experts available working in association with the automated process. While compared to the fingerprint technology, face recognition is still immature and need even more manual attention so more and more expert need to be trained for the future automatic face recognition systems. This is more important in forensic scenario where the implication of incorrect decision is severe and final outcome must be verified by expert. Furthermore, comparison of images taken under controlled condition such as passport photos or photos for arrest records requires less expertise compared to images taken under uncontrolled conditions such as snapshots and images from surveillance camera. The experts also need a little bit training in legal issues because they will be working in justice system and will present their conclusion in court. The facial image examiners should be trained in mainly three areas:

First, general knowledge about the automatic system which include history of personnel identification, current methods in biometrics, underlying principles of the general field of photographic comparison [21], and know-how of basic imaging science and image processing is required.

Secondly, more specific knowledge regarding the properties of face such as aging process, temporary changes (e.g., makeup and hair change), permanent changes (e.g., formation of scars, loss of hair,

cosmetic or plastic surgery), structure of bones and muscles, specific facial expression and their corresponding internal muscle group, comparison of ears and iris is also needed.

Finally, the facial examiner should have a general understanding of the judicial system, should be aware of the implications of their testimony, admissibility issues of facial comparison in court, and should be trained in how to present their comparison process in court and to a layman.

3.3 Forensic Individualization from Biometric Data [3]:

This paper review several basic concepts of forensic science and proposes a general forensic face recognition framework based on Bayesian likelihood ratio approach. Although this work is a comprehensive review of forensic concepts, and provides a general description of the system, there is no experimental work described to prove the effectiveness of proposed framework.

In forensic literature there is confusion between the terms identification and individualization. When the class of individual entities is determined to be the source, it is called identification or classification. When a particular individual is determined to be the source, it is called individualization. In the former case, the identity is called qualitative identity while in the later case the identity is called numerical identity.

In forensic science, the individualization process is usually considered as a process of rigorous deductive reasoning, as a syllogism constituted of a major premise, a minor premise, and a conclusion. The major premise here in forensic face recognition context is the general principle of uniqueness applied to source face and trace face. Since it is based on inductive reasoning which cannot be considered as a rigorous reasoning as what is true for one instance is not necessarily true for all. While the demarcation criteria of empirical falsifiability reject the uniqueness of properties used for individualization from face, however it does not implies that face recognition cannot be used in forensic individualization rather it just put a limit on the certainty depending on the quality of the images and method used.

To describe the likelihood ratio approach based on Bayes theorem, two mutually exclusive hypothesis, prosecution hypothesis (H_p) and defense hypothesis (H_d), can be defined as the set of all possible hypothesis for inference of identity of source of a trace. Let *I* represent the background information about the case in hand and *E* is the evidence. The likelihood ratios approach calls for computation E, between-source variability (BSV) and within-source variability (WSV). Fig.1 and 2 illustrates a simplified version of incorporating likelihood ratio approach in forensic individualization described by the author [3]. A detail description of Bayesian framework and its application to forensic face recognition is presented in section 3.



Fig.1: Evaluation of the evidence in Bayesian framework



Fig.2: Evaluation of the likelihood ratio

3.4 Automatic Forensic Face Recognition from Digital Images [4]:

This paper describes a small scale experimental work carried out by Forensic Science Service (UK) which explores the performance of an existing face recognition system [22] in forensic domain. The paper investigates the application of Bayesian framework in forensic facial comparison and decision making. Experiments are carried out using Image Metrics OptasiaTM [22] which is a software package implementing face recognition system. The paper disregards the technique used by the software and focus only on the forensic aspects of the system.

The approach of the software used for experiments is very simple. Active shape and appearance model [23] is used by the software for automatic face recognition. Given the model is based on a database of n facial images, when a query image is input to the system, it results in n probabilities. Query images of persons included in database are presented to the system and all the n recognition probabilities are computed. The author carries out three tests for evaluation. Firstly, they used same images as those in database for benchmark testing. This test provides a benchmark for maximum performance of the technique. Twenty pictures chosen at random from the database are used as query images and a recognition probability of greater than 95 percent was obtained. The recognition probability sharply falls down after the nearest match.

Secondly for feasibility testing, query images are of persons contained in database but exhibiting face as well as image variability. Pictures of five volunteers are captured with varied facial and imaging conditions for the purpose of feasibility test. In this experiment, pose has the strongest effect on recognition performance followed by other factors.

Finally, for evaluation testing, five people in database are photographed under similar conditions to those in database to estimate WSV and BSV of the database. Evaluation test provide just a preliminary assessment of the expected value or performance of the system in forensics domain. WSV is estimated using a set Q of 10 images of each of 5 volunteers. These pictures are taken under similar conditions to those used in database. The matching score for set Q is then compared to all of the rest of images in database to obtain between-source variability for these identities. Based on the matching scores, WSV and BSV, likelihood ratios are computed for those five subjects.

The paper provides enough details about their experiments however it can be extended to include specific example images pair with their WSV and BSV shown and analyzed. Some details as how many images are used to measure the BSW, why 10 images are used for computing WSV are not included. It is not demonstrated as how the WSV is related to the population size in their experiments.

3.5 Face Matching and Retrieval Using Soft Biometrics [5]:

Although this work does not directly focus the forensic aspects of face recognition, however the techniques and methodology proposed in this work seems very attractive in forensic applications of face recognition. Soft biometrics (ethnicity, gender and facial marks) when combined with a traditional face recognition system such as [24, 25] can improve the recognition accuracy as well as the ease of use and interpretation of outcome in forensic domain.

The author first detects facial landmarks using AAM [23]. Using the landmarks primary facial features are extracted and excluded in subsequent facial marks detection process. First, face image is mapped to the mean shape to simplify the subsequent process. Laplacian of Gaussian (LoG) operator is utilized to detect facial marks. Each detected facial mark is classified in hierarchical fashion as linear vs. all and circular vs. irregular. Furthermore, each mark is also classified on basis of its morphology as dark vs. light. This way each of the facial mark can be classified as mole, freckle, scar etc.

Although the demonstrated performance of their proposed approach of facial marks detection is not robust, nevertheless, facial marks give a more descriptive representation of facial recognition accuracy compared to the numerical values obtained from traditional face recognition systems. This representation will be particularly useful in forensic application. In such approach semantic based queries can be issued to retrieve a particular image from database. Furthermore, it can be particularly useful to follow research in this direction for facial comparison of half occluded images which are quite common from a surveillance camera and also can be applied to differentiate between identical twins as they may have different facial marks beside very similar facial structure. Demonstrated experimental results based on FERET [26] database and a mugshot database show that using the soft biometric in combination with existing face recognition technology can improve the overall performance of the system and is more useful to forensic applications.

4. Bayesian Framework for Forensic Face Recognition

The aim of a forensic biometric system is to report a meaningful value or expression in court to assess the strength of forensic evidence. However, the system should not overpass the role of judicial system. The output of a biometric system cannot be used directly in forensic applications as discussed in detail in previous literature on forensic speaker recognition [10, 11, 27]. Systems using a threshold to decide between two classes are not acceptable in forensic domain [27]. For the purpose of forensic applications, the likelihood ratio framework is agreed upon standard way to report evidence value from a biometric system. This framework is discussed in some details in speaker recognition domain and the theory here benefits from the literature of forensic speaker recognition [10, 11]. However, unlike forensic speaker recognition and there is an utmost need for a reliable facial comparison and recognition systems which can assist law enforcement agencies in investigation and can be used in courts. Some of the papers focusing the forensic aspects of face recognition are discussed and reviewed in section 3.

The Bayesian framework is a logical approach and can be applied to any biometric system without change in the underlying theory. The likelihood ratio (LR) assessed from a score based biometric system can be used directly in court. While in commercial biometric system, the objective is to make decision in binary form, in forensic applications, the objective is to find the degree of support for one hypothesis against the other. Using the Bayes theorem

(likelihood ratio approach), given the prior probabilities, the posterior probabilities can be calculated as:

$$\frac{\Pr(H_p|E,I)}{\Pr(H_d|E,I)} = \frac{\Pr(E|H_p,I)}{\Pr(E|H_d,I)} \times \frac{\Pr(H_p|I)}{\Pr(H_d|I)}$$
(1)

where as defined previously H_p and H_d are the prosecution and defense hypothesis respectively and *E* represent forensic information (evidence) while *I* is background information on the case in hand. The prosecution hypothesis H_p states that the suspect is the source of the questioned face while the defense hypothesis H_d states that someone else in the relevant population is the source.

Equation 1 gives the posterior odds required by judicial systems given the prior odds (background knowledge on the case) and likelihood ratio of the evidence E. The likelihood ratio

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

gives a measure of degree of support for one hypothesis against the other, taking into consideration the circumstances of the case (background information I), and the result of the analysis of the questioned face. It calculates the conditional probability of observing a particular value of evidence with respect to two competing hypotheses [28]. The numerator of LR calls for the computation of WSV while denominator requires BSV to be calculated. This fact is further illustrated in fig. 3.



Fig. 3: The solid curve shows the distribution of H_p scores while the dotted curve represents the distribution of H_d scores. LR is calculated by dividing the height of H_p by H_d at point E.

The task of a forensic scientist is to evaluate the LR which is then incorporated into the framework by judicial system to reach a conclusion. For the purpose of implementation using a score based biometric face recognition system, we compute the LR as follows:

• *E*, a score obtained by comparing questioned (trace) face and suspect face.

- A distribution of matching scores when comparing faces of suspect taken under similar conditions (control database) to that of questioned face. The computed WSV is then used to estimate the numerator, $Pr(E|H_p, I)$ of the likelihood ratio.
- A distribution of matching score when comparing faces of relevant population taken under similar conditions (relevant population database) to that of questioned face. The computed BSV is then used to estimate the denominator, $Pr(E|H_d, I)$ of likelihood ratio.

Figs 4, 5 and 6 further illustrate the procedure to compute BSV, WSV and LR. Note that in case where questioned face is compared to suspect face, the recognition score is called evidence.



Fig 6: Estimation of LR

5. Reliability and Court Admissibility Issues

The reliability of forensic face recognition is more critical compared to biometric face recognition where an incorrect decision results in denial of access for a person to a building, login restriction etc whose consequences are usually not very serious. In such systems, a second trial can let the user to be successful. However in forensic case, the consequences are more severe as an incorrect decision can convict a person criminal while being innocent. While it is agreed by researchers that such system must be assisted by a human expert for verification purpose [2] however the reliability of the system itself is very important as it will reduce the manual effort and help standardize the process of facial comparison. In order to assess the reliability of forensic face recognition system, several factors such as lighting conditions, facial expression, and pose etc which are widely explored in biometric domain should be considered here as well. When using Bayesian framework, other factors such as the number of images used to compute BSV and WSV must also be taken into consideration. Beside the database size, it should be ensured that the database must have enough variations both in imaging system (such as lighting conditions, image quality etc) and facial expression (such as pose, facial expression etc). Bayesian framework is the most logical framework however standard must be defined as for computation of BSV and WSV. Particularly, the distribution of H_p and H_d scores are probability density functions and its estimation is sensitive to mathematical modeling. Therefore different modeling method can lead to different likelihood ratio values.

As a general rule, in order for the evidence extracted from forensic face recognition to be admissible in court of law, the employed technology must be thoroughly tested and evaluated. In United States this was ensure by application of '*Frye rule*'. It states that the judges should be acting as 'gatekeeper' to asses if the technology on which the evidence is based is generally accepted in relevant scientific community or not. Nowadays, in United States, mostly a revised version of '*Frye rule*' called '*Daubert*' is in practice. It ensures that, in addition to general acceptance of the technology, whether the employed technology is tested and can be challenged in some objective way, the technology or theory must be peer-reviewed, description of the error rate of the technology, existence and maintenance of standards and controls.

In European judicial system, there is no specific admissibility rule described regarding the scientific evidence. The judges are responsible to perform free evaluation of the scientific evidence pertaining to the case in hand.

6. Conclusions

Although there is a lot of research going on focusing on the development of new techniques and methodologies to bring improvement in current state-of-the-art face recognition systems performance however, less effort is devoted to integrating face recognition technology with legal system of court and justice. Beside a few papers there is not much published as to how the face recognition system can be adopted for forensic purpose. The output of a biometric face recognition system is not suitable for use in forensic application and the output of conventional score based biometric system must be processed so that it is more useful and acceptable by the court. Although the likelihood ratio value is subjective since it is dependent on the databases used for WSV and BSV as well as the modeling method of their distribution however it provide the most logical framework for judicial system to incorporate biometric evidence and background information on the case to reach conclusion. There is an urgent need for 'tuning' and integration of face recognition systems or development of new system which can fulfill the requirements of law enforcement agencies and legal system of court and justice.

One possible approach would be to build system which exactly mimics the forensic examiners way of facial comparison rather than the prevailing techniques in biometric domain. This approach also needs to be incorporated into Bayesian framework as any other face recognition system.

References

- 1. N. A. Spaun, "Forensic biometrics from images and video at the Federal Bureau of Investigation," in *Proc. BTAS*, pp. 1–3, 2007.
- 2. N. A. Spaun, "Facial comparisons by subject matter experts: Their role in biometrics and their training," in *Proc. ICB*, pp. 161–168, 2009.
- 3. D.Meuwly, "Forensic individualization from biometric data", *science&justice*, vol. 46, no. 4, pp. 205-213, 2006.
- 4. C Peacock, A Goode and A Brett, "Automatic Forensic Face Recognition from Digital Images", *science&justice* vol. 44, no.1, pp. 29-34, 2004.
- 5. U. Park and A. K. Jain, "Face Matching and Retrieval Using Soft Biometrics", *IEEE trans. On Information Forensic and Security (TIFS)* vol.5, no. 3, pp. 406-415, 2010.
- 6. L. Wiskott, J.-M. Fellous, N. Kruger, and C. von der Malsburg, "Face recognition by elastic bunch graph matching," *IEEE Trans. PAMI*, vol. 19, no. 7, pp. 775–779, 1997.
- 7. F. Wang, J. Wang, C. Zhang, and J. T. Kwok, "Face recognition using spectral features," *Pattern Recognition*, vol. 40, no. 10, pp. 2786–2797, 2007.
- 8. W. Zhao, R. Chellappa, P. J. Phillips, and A. Rosenfeld, "Face recognition: A literature survey," *ACM Comput. Survev.*, vol. 35, no. 4, pp. 399–458, 2003.
- 9. P. Jonathon Phillips et. al, "FRVT 2006 and ICE 2006 Large-Scale Experimental Results", IEEE Trans. on PAMI, vol. 32, no. 5, 2010.
- 10. Champod, C., and Meuwly, D., "The inference of identity in forensic speaker recognition", *Speech Communication*, 31, pp. 193-203, 2000.
- 11. Gonzalez-Rodriguez, J., Fierrez-Aguilar, J., and Ortega-Garcia, J., "Forensic Identification Reporting Using Automatic Speaker Recognition Systems. *Proc. ICASSP*, 2003.
- M. Y. Aulsebrook, W. A. Iscan, J. H. Slabbert, and B. P. Superimposition and reconstruction in forensic facial identification: a survey. *Forensic Science International*, 75(2-3):101–102, October 1995.
- 13. C.M. Wilkinson and R.A.H. Neave, "Skull re-assembly and the implications for forensic facial reconstruction", *Science & Justice* 41 (3) (2001), 233-234.
- 14. Facial Identification Scientific Working Group, http://www.fiswg.org/
- 15. International Association for Identification, http://www.theiai.org/
- 16. European Network of Forensic Science Institutes, http://www.enfsi.eu/

- 17. Netherlands Forensic Institute (NFI), http://www.forensicinstitute.nl/
- 18. "General method of facial comparison", *Addendum #:1*, internal document, Netherlands Forensic Institute.
- 19. A. Samal and P. A. Iyengar, "Automatic recognition and analysis of human faces and facial expressions: A survey," *Pattern Recognit.*, vol. 25, pp. 65–77, 1992.
- D. Alspaugh, "A brief history of photogrammetry," in Manual of Photogrammetry, 5th ed., J.C. McGlone, Ed. Bethesda, MD: American Society for Photogrammetry and Remote Sensing, pp. 1-12, 2004.
- 21. H. Tuthill and G. George, Individualization: Principles and Procedures in Criminalistics, 2nd Ed., Jacksonville, FL: Lightning Powder Company, pp. 1-73, 2002.
- 22. Image Metrices OptasiaTM Operating Instructions, 2002, www.image-metrics.com
- 23. Cootes TF, Edwards GJ, and Taylor CJ. Active Appearance Models. *IEEE PAMI*, vol. 23, no.6, pp. 681-685, 2001.
- 24. M. Turk, A. Pentland, Eigenfaces for recognition, J. Cogn. Neurosci, vol. 3, no.1, pp. 71-86, 1991.
- 25. FaceVACS Software Developer Kit, Cognitec Systems GmbH, <u>http://www.cognitec-systems.de</u>.
- 26. J. Phillips, H. Wechsler, J. S. Huang, and P.J. Rauss, "The feret database and evaluation procedure for face recognition algorithms," *Image and Vision Computing*, vol. 16, no.5, pp. 295-306, 1998.
- 27. C.G.G. "Aitken, Statistics and evaluation of evidence for forensic scientists", *John Wiley & Sons*, 1997.
- 28. Botti, F., et al., An Interpretation Framework for the Evaluation of Evidence in Forensic Automatic Speaker Recognition with Limited Suspect Data. *Proc. ODYSSEY*, pp. 63-68, 2004.