Chapter 26
Face Recognition in Forensic Science

Nicole A. Spaun

26.1 Introduction

The use of facial recognition in the field of forensic science presents a challenging set of issues. Forensic science is the use of scientific principles and methods to answer questions of interest to a legal system. Forensic science differs from the field of security; in security applications the goal is to prevent incidents from occurring, while in forensic cases typically an incident has already occurred.

Unlike security or portal scenarios where the administrators have control over the scene and the setup of cameras, in forensics the evidence and surveillance generated is completely uncontrolled by the user of the facial recognition system. Unconstrained lighting conditions, face orientation, and other factors all make the deployment of face recognition systems for surveillance a difficult task [7]. For example, surveillance cameras in places of business are generally pointed at specific locations to spot theft by criminals or employees. These locations include entry/exit doors where the opening of the door may allow the contrast of the camera to be overwhelmed or above an employee's head, where the angle will be steep and the camera is more likely to observe the top of the subject's head than the front of their face. Such conditions lead to the inability to enroll facial images or the worsening of system accuracy rates. Low system accuracy can be disastrous in legal matters. Thus, many forensic organizations have yet to embrace facial recognition as fully as users in the field of security.

N.A. Spaun (✉)
Forensic Audio, Video and Image Analysis Unit, Federal Bureau of Investigation, Quantico, VA, USA
e-mail: Nicole.Spaun@us.army.mil

Present address:
N.A. Spaun
United States Army Europe Headquarters, Heidelberg, Germany

N.A. Spaun
USAREUR, CMR 420, Box 2872, APO AE 09036, USA

S.Z. Li, A.K. Jain (eds.), *Handbook of Face Recognition*,
DOI 10.1007/978-0-85729-932-1_26,

In this chapter, we will first explain the current means of comparing faces used by forensic science laboratories. It is a nonautomated process performed by forensic examiners and has been referred to as facial "photographic comparison" [15] or forensic facial identification. Next, we will outline the innovative ways in which facial recognition systems are being used by the forensic community. Lastly, we will discuss the growing future of facial biometrics in the legal system and the increasing (not decreasing) need for human examiners to perform facial identification in combination with the automated facial recognition systems.

26.2 Characteristics of Forensic Facial Recognition

Forensic facial recognition and facial identification are distinct, separate processes. In the past facial recognition in the forensic context referred to the process of using eye-witnesses to identify a suspect from either a physical or photo line-up. In today's terminology, facial recognition is the use of an automated system to determine matches to a probe image from a gallery of images, a one-to-many search, or to verify the identity of an individual, a one-to-one check. The one-to-many process can propose suspects to be investigated or can generate candidate lists to be shown to eyewitnesses. This differs from forensic facial identification, which is a manual process where an expert performs a photographic comparison focusing on the face of an individual. According to the Scientific Working Group on Imaging Technology, photographic comparison is an assessment of the correspondence between features in images and/or known objects for the purpose of rendering an expert opinion regarding identification or elimination [15]. Within these manual comparisons, the features of the head will be analyzed and compared both morphologically and spatially. We will focus on forensic facial identification in this section and the use of automated facial recognition in the following section.

Forensic photographic comparison has a long history; documentation shows it has been in use within the US legal system since at least 1970 [4]. Specialized photographic comparisons have assisted different forensic fields: fingerprint comparisons, tire tread and tool mark analysis, footwear impressions, ballistics, etc.

The specific analysis of faces in images has been performed by forensic examiners with various backgrounds, such as image analysts, photographers, forensic artists, and forensic anthropologists. This diversity of backgrounds is due to the nature of facial identification, where one is assessing a highly three-dimensional aging anatomical feature, a face, in an image that is generally subject to varying photographic conditions including lighting and angles of view. While the backgrounds of persons performing facial identification may vary, the common approach is the application of scientific principles in the course of a visual comparison.

One way of articulating the scientific method for use in photographic comparisons was derived by R.A. Huber for questioned documents [8] and later referred to as "ACE-V": Analyze, Compare, Evaluate and Verify. When assessing a face, a forensic examiner can use this method to rigorously document facial characteristics, compare them, and form an opinion that can be verified by a similarly trained examiner.

The goal of facial identification is to determine if the questioned individual is the same individual as the known to the exclusion of all others. If so, this is called an Individualization or Identification in the forensics community. Within the biometrics community such a one-to-one comparison is called a "verification"; however in forensic science the term verification generally specifically refers to a peer review or other post-examination evaluation process. Because there are differences in terminology between the forensic and biometric communities, when using a word that has different meanings we will introduce both terms and then continue with the forensic usage for consistency. In contrast to an identification, the examination may lead to the conclusion of Exclusion or Elimination of the known individual as being the questioned individual. If an individualization or elimination cannot be made, it is reported that no definitive conclusion is possible, while listing noted similarities and/or dissimilarities.

A typical facial comparison begins with at least two images depicting individuals for identification. In forensic science, the subject of interest is commonly referred to as the "questioned individual"; in biometrics the image of the subject to be analyzed is called the "probe". Likewise, in forensic science the suspect depicted in the image is generally called the "known individual"; in biometrics the images of the suspects or potential matches are referred to as the 'gallery'. It is common for known images in forensic cases to be controlled images, such as those from a driver's license, passport, previous arrest photograph (a.k.a. mugshot), or other official sources. Most questioned images are typically uncontrolled, obtained from surveillance images or video. The difficulty of the comparison is compounded when both the questioned and known images are uncontrolled. As an example, the case of "the ruthless care giver", a subject accused of felony embezzlement who later pled guilty, features uncontrolled known and questioned images.

Figure 26.1 depicts four known images submitted to the Federal Bureau of Investigation (FBI) for a facial identification examination. These personal photographs demonstrate several challenging elements for facial identification and recognition: the position (tilt, rotation, and pitch) of the head differs in each image, background/scene is busy and differs in each image, facial expressions differ, illumination varies, image resolution is low, and the face is obstructed by eyewear and other objects. It is worth noting, however, that the ability to resolve details on these images is considerably better than for typical surveillance video obtained in most cases. The submitted questioned images of a suspect were also highly uncontrolled and arrived as both photographs and digital video; the three best images were selected for further examination (see Fig. 26.2). There is at least 10 years in time between when the pictures were taken, possibly more. Matching uncontrolled images such as these is challenging for facial identification but virtually impossible with current facial recognition technology; this highlights the importance of having human examiners involved in the process of forensic facial comparison.

In the analysis stage of the examination, the morphology and texture of the face is reviewed. One observes and notes the characteristics of the questioned face and then for the known face(s). The traits that are used within facial comparisons, like most other forensic examinations, fall into two categories: class and individual characteristics. Class characteristics are those that place an individual within a class or

Fig. 26.1 Four known images of the subject. Images were submitted as printed photographs. Notice the variation in perspective, lighting, expression, pose, and background scene of these uncontrolled images

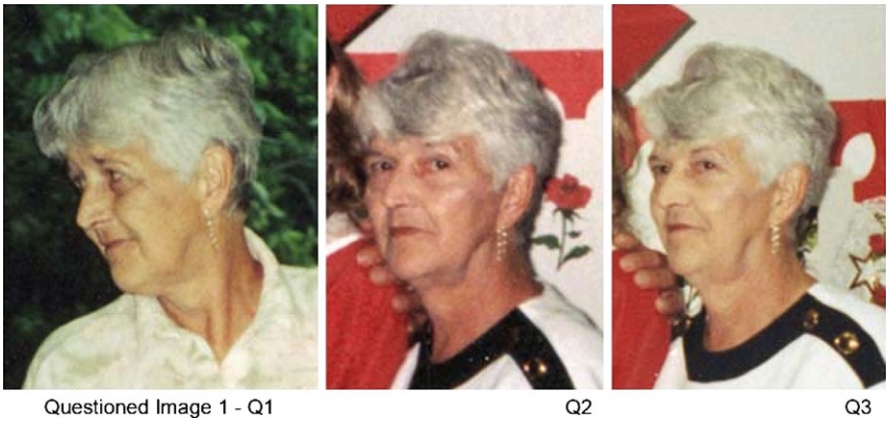

Fig. 26.2 Three questioned images of the suspect taken under uncontrolled conditions. Image Q1 is derived from digital video; Images Q2 and Q3 were submitted as printed photographs

group [17]. These general characteristics include hair color, overall facial shape, presence of facial hair, shape of the nose, presence of freckles, etc. Individual characteristics are those that are unique to the individual and/or allow for a person to be individualized [17]. These specific characteristics include number and location of facial minutiae, such as moles and blemishes, as well as scars, tattoos, chipped teeth, lip creases, wrinkles, etc. The mere presence of freckles is a class characteristic whereas, if the image is detailed enough for one to observe them, the specific number, pattern, and relative location of freckles can be an individualizing characteristic. Many individuals develop wrinkles around the eyes therefore the presence of crow's feet would be a class characteristic, however matching patterns, lengths, and locations of individual wrinkles may be unique. In order to bring out such details within the questioned and known images, the examiner may deem it beneficial to enhance all or part of the image. For example, simple contrast adjustments may bring out details in skin texture such as freckles, blemishes, and scars.

The procedure of the comparison can be qualitative or quantitative, using relative or absolute dimensions. In a morphological comparison, the location and size of facial features is measured relatively, not absolutely. If the perspectives of the questioned and known images are similar and the position of the head is similar, the image depicting the known individual can be scaled to that of the questioned individual by using the interpupillary distance or other consistent features within the image.

An overlay of the scaled known image and the questioned image can then be made in order to determine if the relative alignment of other facial features is consistent. This overlay of images is also referred to as the superimposition method and can be performed with video editing or image processing equipment [19]. A variation of the overlay approach is a photogrammetric one: a side-by-side of the images is prepared and two sets of 3 or more parallel lines are drawn through facial features, such as the jawline, pupils, nasal bridge, on both images and compared by position [4].

For both a photogrammetric and overlay approach, the images must be of the same perspective, but the key difference is that an overlay allows one to view the length and width simultaneously although viewing the lines in the photogrammetric approach leaves more to human perception as one looks across both images. Superimposition can appear to be doctoring the evidence if not properly explained because scaling implies changing the images to effect alignment, but the method is sound. Consider that if you scale an image of Abraham Lincoln to the same eye corner-to-corner distance as that of George Washington, that scaling will not force the length of the face or shape of the jaw to match up, and rightly so because they are different individuals. Just as scaling two images of Abraham Lincoln to the same interpupillary distance will demonstrate the similar locations of facial marks and the consistent sizes of facial features because the images do depict the same individual. Therefore a superimposition can provide extremely beneficial information to determine if features appear to be the same and if the relative locations and dimensions relate.

With an overlay, the examiner can "blink" back and forth between questioned and known imagery to assist in the comparison by identifying similarities and dissimilarities. In this type of comparison, facial landmarks, standard reference marks generally defined by the underlying structure of the skull [6, 10], are used in the main as guides and are not typically measured.

26.3 Anthropometric Method

On the contrary, the anthropometric method of facial comparison relies on measurements between facial landmarks [10, 19]. The challenge with the anthropometric method, and others that are absolute measurement driven, is two-fold: they are severely affected by image perspective and are therefore fairly inaccurate in surveillance situations, where the position of the head and camera-to-subject distances are

Fig. 26.3 To make this side-by-side chart, the K4 image was scaled by the distance from the ear to the nose of the Q1 image. Of all the submitted images, these two were most similar in pose and perspective, although there is clearly a difference in the rotation of the head. An overlay of the images was attempted but proved to be unhelpful

uncontrolled [13], and also it is difficult to consistently locate the landmarks in different images by different examiners [5]. Therefore, the FBI's forensic examiners do not use an anthropometric method for facial identification and instead use a fusion of the morphological and superimposition technique. Figure 26.3 depicts two images, one questioned and one known, that are of a similar perspective. However, in this case, the images were scaled by the nose to ear distance to assist in preparing a visual aid, a side-by-side chart, instead of a direct overlay as the superimposition would be affected by the difference in position of the head. Figure 26.4 depicts additional side-by-side charts that display greater variation in perspective.

Within the comparison examination, the number and significance of corresponding features must be evaluated [17]. If there are dissimilarities, the examiner works to understand the nature of the dissimilarity. The mere presence of a dissimilarity is not necessarily a cause for exclusion as many dissimilarities can be readily explained by differences in pose, illumination, expression, and time. It is also important to note the significance of any dissimilarity. For example, a large variation in ear length between individuals in questioned and known images is more significant than a possible difference in skin-tone as the latter can potentially be explained by make-up, sun exposure, or differences in photographic conditions.

Another consideration when weighing the significance of dissimilarities is to consider the effects of time: wrinkles, transience of facial markings, and changes in weight. If a dissimilarity can be logically explained, such as the disappearance of a pimple or increase in eye wrinkles, then it can be weighted accordingly as a less substantial difference. In our example shown, similarities are noted in overall class characteristics to include shape of the head and nose and the presence and location

Fig. 26.4 Two side-by-side charts depicting image K4 for comparison to images Q2 and Q3. No superimposition of the images was attempted due to the significant differences in rotation and tilt of the head between images

of wrinkles. Figure 26.5 is the chart from Fig. 26.3 with arrows added to identify specific individualizing features: a blemish on the left cheek and the ear pattern.

One distinct advantage that humans have over today's automated facial recognition programs is that we regard the ear as part of the face and can use it in our analysis. Automated systems for ears are being developed, generally separately from facial recognition programs, and the combination of face and ear analysis is considered multi-modal biometrics. The ear is important because researchers have noted that they have not found any ears that are alike in all parts and that the ear is also stable throughout adulthood [9, 18]. The ear itself contains approximately 16 different features that can be assessed and compared. Figure 26.6 focuses on the left ears depicted in the questioned and known images. The similarity in ear features is

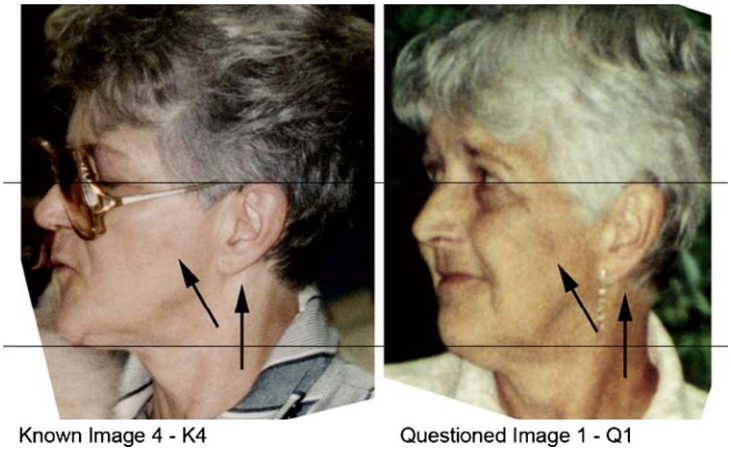

Fig. 26.5 *Arrows* have been added to the K4 and Q1 images depicted in Fig. 26.3 to indicate the most individualizing similar characteristics: a blemish on the left cheek and the pattern of the left ear

striking, to include the pattern of the crux of the helix and triangular fossa and the projection of the tragus and anti-tragus.

Based on the number and significance of the similarities in the case depicted in the figures, the known individual was identified as the questioned individual by the FBI examiner. The result was peer-reviewed by a similarly trained FBI examiner as a verification of the case results. If the examiners had a difference of opinion, the results would be discussed and then arbitrated if further disagreement existed. In this instance, the examiners readily reached the same conclusion. A similar analysis by the Oakland County Sheriff's Office in state of Michigan [1] also reached the same conclusion. The suspect was arrested in 2005 and pled guilty to 6 out of 10 charges. The facial identification examinations in this case were a critical component of the forensic investigation.

26.4 Use of Facial Recognition in Forensics

Facial recognition technology is being embraced by, and for, law enforcement world-wide. It is being used in novel ways and is pushing the limits of the technology. It is those limits of the technology, mainly the accuracy rates, which are holding back the usage of facial recognition in the legal system. This section will explore several uses of automated facial recognition systems in forensics.

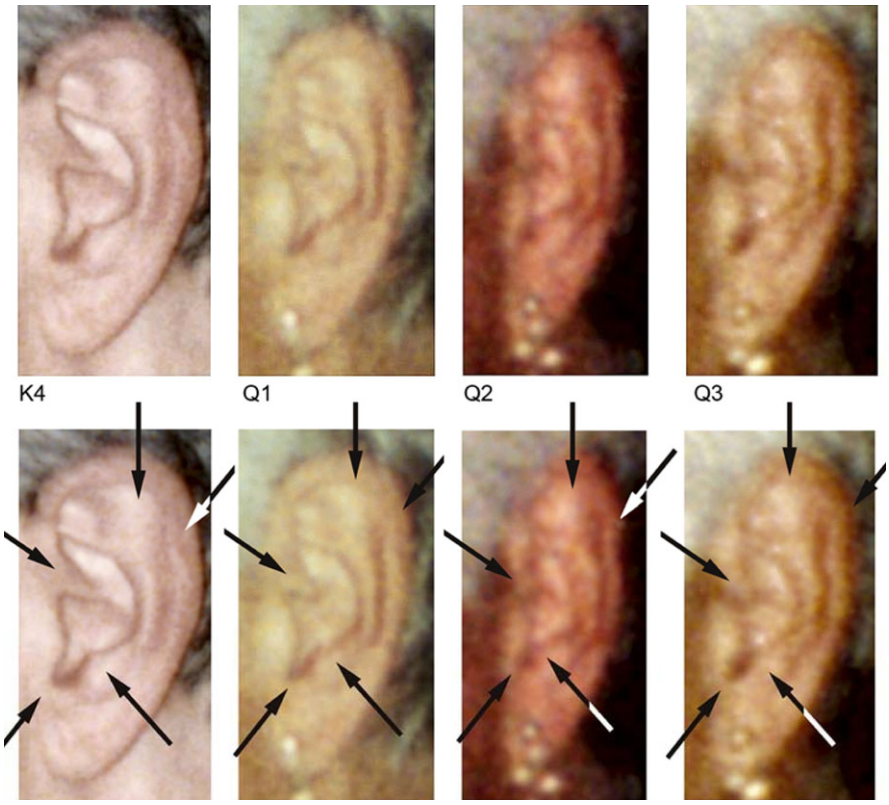

Fig. 26.6 *Top*. Enlargements of the left ear depicted in the fourth known image, K4, and the three questioned images, Q1–Q3. *Bottom*. Arrows added to indicate similarities in the pattern of the crux of the helix, Darwin's point, triangular fossa into the antihelix, tragus, and intertragic notch

26.4.1 Department of Motor Vehicles

When most people think of their state's department of motor vehicles (DMV) they think of long lines and unflattering photographs. However, when it comes to facial recognition, those photographs are showing their worth. Facial biometrics is a natural fit in a DMV environment because the photographs are controlled, taken under consistent circumstances. Many states are now on the fore-front of fraud and identity-theft detection by using automated facial recognition systems. West Virginia was the first state to use an automated facial recognition system in the late 1990s; by 2009, more than 30 states were using facial recognition systems in their driver's licensing procedures.

Most DMV fraud occurs when people use different spellings of their names, use aliases, and show false documents. Previously these cases of fraud would have involved numerous hours of investigation by state DMVs and police departments.

The investigation time has been decreased by facial image screening measures that start when a person tries to apply for a license.

Presently in many states in the US, an individual's photograph is taken for the driver's license and later fed into a facial recognition system. If there is supposed to be an existing license photo on file and the submitted photograph is not matched to it that could be a sign of identity theft where either the first or second photograph is of an imposter. Likewise, if there is a facial match found, then the biographical information is checked to determine whether this is the same individual applying for a license renewal or if there is deception in the biographical information and the person is seeking to obtain an illegal license bearing fake information or a stolen identity.

As an example, the North Carolina Division of Motor Vehicles has used facial recognition in their licensing procedures since 2005. Their Viisage (now part of L-1 Identity Solutions) system has successfully detected fraud, such as one man with nine license pictures and social security numbers, a woman with 11 different identities, and a 15-year old who had posed twice to get fake IDs to get into bars [3]. Additionally, the successes from the DMV's use of facial recognition have been publicized, providing a deterrent to other individuals contemplating fraud. The use of biometric systems has changed the way DMVs operate. In Indiana and several other states, individuals are now asked to assume a neutral expression, instead of a smile, to better control variability between images and enhance the matching accuracy of their automated systems [3]; the state of Virginia even adopted such a policy in 2009 in anticipation of having a facial recognition system in use in the future. The Oregon, Nevada, Wisconsin and other DMVs no longer issue same day license cards in order to allow their investigators time to review the biometric data before sending the license to the customer.

In a revolutionary shift, a new contract for the North Carolina DMV with the MorphoTrak-Safran Group (formerly Sagem Morpho) outlines plans to begin capturing facial images in 3-D for better facial matching. Because a driving license agency generally has the largest repository of images of state residents, DMV facial databases have always been an asset to police looking for photos of their suspects. Now a DMV's biometric system is also proving to be a boon. Nevada police were able to arrest a fugitive with an outstanding felony warrant for sexual assault after his identity fraud was detected with their facial recognition system. In North Carolina, the DMV has welcomed the FBI into their facilities to use their automated system to check for the FBI's wanted individuals. The NC DMV has generated successes for both the North Carolina law enforcement and the FBI, demonstrating the benefit of cross-agency cooperation in forensic facial recognition.

26.4.2 Police Agencies

The archetypal application of automated facial recognition in forensics is to enable law enforcement to take images obtained from surveillance or Closed Circuit

Television (CCTV) and query a database as a means of identifying the subjects depicted [20]. Using automated biometrics for the development of suspects is nothing new to forensics: fingerprint and DNA results are frequently used to narrow down a suspect pool or identify unknown subjects. However the unconstrained lighting, perspective of the face, obstructions to the face (e.g., hats, glasses), generally poor resolution, and other factors affecting common CCTV imagery severely affects current facial recognition technology. This leads to accuracy rates well below 90%; while that may sound fair for a small database, most law enforcement agencies will be sieving databases of at least several hundred thousand people, if not millions.

The time spent reviewing the incorrectly selected images can be a drain on police resources and the false reject rate could be an even larger concern. Yet the use of facial biometrics to develop a list of leads for police to then investigate is a more manageable task for today's technology. Many smaller police agencies are taking up the challenge and pioneering facial recognition systems for development of suspects in their investigations. We will next outline police use cases by exploring as examples of two police agencies that have been using facial recognition biometrics for several years and a third who are rolling out a ground-breaking new system.

In Washington State, the Pierce County Sheriff's Department has been using automated facial recognition since 2008. The county, which includes the city of Tacoma, was part of a pilot study by Sagem Morpho Inc (now known as Morpho) to use their MorphoFace Investigate (MFI) software in a forensic setting. Crimes like Automated Teller Machine (ATM) robbery, or identity theft using an ATM, have always been a challenge for biometrics because of the sheer volume of innocent fingerprints on the machine. Within the first six months of using facial biometric technology, Pierce County had already matched photos from ATM machines that were robbed with a suspect who was in their database; the suspect was charged with 11 crimes and pleaded guilty. Their database is primarily made up of booking photographs from people previously entered into the county's penal system. During the booking process, the identity of people was previously validated solely by their fingerprints. The photographs taken are now fed into the MFI software for a secondary validation; repeat offenders offer a chance to test the system by matching the new booking photograph to their previous arrest photos. The output of the system is reviewed by a human examiner, who makes the final determination. As a forensic service, officials began using the software to revisit cold cases by selecting good surveillance images and comparing them against the database. This technique is now also in use for active cases when suitable images are available.

Besides using forensic facial recognition at the station, it can be used by law enforcement in the field as well. In Florida, the Pinellas County Sheriff's Office pioneered a system that deputies can operate from their patrol cars. In place since 2002, the facial recognition system developed by Viisage (now L-1 Identity Solutions) has lead to over 500 arrests and assisted in identifying countless other individuals. At the station, the system resembles that used by Pierce County: booking photographs are taken and submitted to the system to verify the identity of the arrestee. Later, if the person is not charged with a crime, their photograph is expunged from the system. The database contains over 8.3 million arrest photos, including records from

several other sheriff's departments throughout Florida, the state Department of Corrections, and access to driver's license photographs from several Florida counties. It is not uncommon for other law enforcement agencies to send their own questioned images to the Pinellas County Sheriff's Office for facial recognition searches.

The novel aspect of the Pinellas County Sheriff's Office system is its mobile application. Installed in more than 170 patrol cars, the mobile system includes a standard digital camera. When a deputy encounters an individual who either does not have a driver's license or ID, or the deputy has reason to doubt the validity of the document, the deputy requests to take a photograph of the individual. An obvious advantage of this system is that the public are generally more willing to allow themselves to be photographed than fingerprinted. The image is uploaded into the automated system at the in-car terminal. Within seconds, the software provides a gallery of images and biographical data as potential matches to the law enforcement officer. The deputy then decides if the person resembles a photograph in the gallery. If the match is to the identity verbally provided by the individual, the deputy can now be confident about the identity even without the individual having their driver's license present. If the match is to an individual with an outstanding warrant, the deputy can bring the person to the station for further identity verification by fingerprint.

The success of their program using off-the-shelf cameras has garnered additional attention and funding from agencies to include the Departments of Defense, Justice, and Homeland Security for Pinellas County Sheriff's Office to expand their mobile facial recognition system. Mobile facial recognition applications for law enforcement are increasing in usage as they are ideal for both officers in the field and detectives at the station.

One such break-through system in Massachusetts is using an application for the iPhone. The police in the city of Brockton are using a system developed by BI2 called MORIS: Mobile Offender Recognition and Identification System. While the technology is not new, the application of it over the iPhone is recently developed. The multi-modal wireless application is using face now with iris and fingerprint under development. The iPhone is used to take a photograph of an individual and then wirelessly upload it into a secure network where it is analyzed by facial recognition software. If a match is made, the officer's phone then receives the additional images and biographic information about the individual. The Massachusetts Sheriff's Association has plans to use the technology in thirty-two police departments and sheriff's offices throughout the state. As with the mobile system used in Pinellas County Florida, the speed and ease-of-use of this technology are likely to entice other law enforcement agencies to adopt similar systems.

26.5 Future Perspectives

The automation of facial analysis in forensic science is as inevitable as it was for fingerprint analysis. However, while the idea of a lights-out facial recognition system is appealing, the reality is that there are too many external variables, such as lighting

conditions, and internal variables, such as aging, to allow the use of an automated facial recognition system as the final evaluator for identifying faces in the immediate future. Just as latent print examiners use an automated system to develop or narrow a suspect list and then perform the manual analysis to make the final conclusion, humans will need to be in the facial analysis process as well [16]. Therefore, the near future of facial comparisons involves the fusion between automated systems performing facial recognition and humans verifying the results through facial identification.

Studies have shown that the combination of algorithms and humans yields accuracy rates that surpass those for either solely algorithm or human facial evaluations [14]. In addition, most algorithms in use today rely on measurements between facial landmarks and dimensions of facial features; human methods are more textural, focusing on facial minutiae such as blemishes and wrinkles. Thus, using a fusion of human examiners and algorithms provides a more diverse approach overall until a lights out system can be created.

Because the goal of forensic examinations is successful crime-solving and prosecutions, facial identification must maintain standards that continue its acceptance within the judicial system. A hindrance to both forensic facial identification and automated facial recognition is the paucity of robust statistics for the size and spacing of facial features/landmarks and the frequency of occurrence of facial minutiae. Examiners provide opinion conclusions at this time without quantitative support, other than being 100% positive of their conclusion that it is, or is not, the same individual.

According to Evison and Vorder Bruegge [4], what is lacking is a quantitative means of establishing a match between two facial images, and in the event of a match, there is no process by which to estimate the frequency of any given face shape in the general population. A statistical foundation would allow the examiner to give DNA-like results.

A qualitative conclusion could be supported by a statistical deduction, such as only a given percentage of the population has both a certain interpupillary distance and a blemish on their left cheek, therefore limiting the possible number of people that the questioned image may depict. Furthermore, currently a percentage match score presented by automated facial recognition is a factor of the system's algorithm. If it means anything at all, it is a measure of certainty in the match by the system; this is the equivalent of an eyewitness saying they are 75% sure that the image depicts the person they observed at the crime scene. It would be a great benefit in forensic usage if the score presented was rooted in measurable physical characteristics instead, such that a result of 91 would actually mean that the person is within the 91st percentile of the population who have certain facial statistics and therefore only 9% of the population could be the depicted person. While not definitive, it would be a significant improvement over the current result scores presented by automated systems.

Inevitably, as facial recognition algorithms improve, the number of applications that need human evaluation should decrease in the future. By incorporating the methods that human examiners use into algorithms, Jain and Park [11] have shown that algorithms to detect and compare facial minutiae can be used in tandem with

standard facial recognition systems to improve the overall accuracy rates of the automated system. In other approaches, system designers are experimenting with 3-D facial recognition to improve accuracy. The critical difference between 3-D facial technology in security and forensic applications is that one can obtain both questioned and known imagery in 3-D for access control or document checks but in a forensic instance there is little chance of capturing 3-D questioned images. Therefore in a forensic capacity, the possibility of generating 3-D models from 2-D images is more promising. Multiple known images of varying perspective are taken and can be fused to produce a 3-D model of a face that can be positioned to match the perspective of the face in an uncontrolled questioned image, such as a frame of CCTV video [2, 12].

Facial recognition algorithms combined with face finding software also provides a powerful tool for future forensics. The push for advanced software that can find, track, and extract "faces in the wild" (e.g., from video or the Internet) comes from the commercial sector as much as the government sector. For example, the Picasa photo-album program by search engine giant Google includes facial recognition technology to sort and label personal photos by the faces they contain. Similarly, law enforcement agencies are interested in using the same type of programs in an array of applications.

The FBI is interested in locating faces of potential suspects during computer forensic examinations of seized computers and mobile phones; such technology will greatly benefit gang related and organized crime or terrorism cases where the network of individuals is as important as the initial subject. The National Institute of Justice is assisting the National Center for Missing and Exploited Children (NCMEC) in using face finding software to search the Internet for missing or abducted children in a program similar to the ChildBase system used by the National Criminal Intelligence Service in the United Kingdom to identify child pornography on the Internet. In London, where there is one CCTV camera per 14 people, the Metropolitan Police Service is looking to use such programs to sort through the ubiquitous video to track criminals in both post-event, forensic situations and real-time scenarios.

There is also interest in using facial recognition technology to update more traditional police procedures. Rather than manually developing photo arrays to present to eye witnesses for review, police could use forensic facial recognition software to create arrays of individuals who are more similar in appearance to reduce bias and increase accuracy. Facial recognition technology is already being used to improve the performance of facial composite software used by forensic artists to develop images from eyewitness accounts, yet future uses could entail using automated facial one-to-many matching of sketches and composites against law enforcement databases to develop suspects [21].

26.6 Conclusions

It is clear that forensic science will benefit from improvements in facial recognition technology and increased usage thereof. Of course, the ultimate goal for facial

recognition in forensic science is for the advances it will bring in policing and security to lead to less forensics being needed due to fewer criminals in our neighborhoods. Until then, the combination of automated facial recognition to develop leads and forensic examiners performing facial identification will be a great step up from existing purely manual processes.

References

1. Bailey, B.A.M.: When to call a forensic artist. Evidence Technology Magazine Online. Technical note (2009). http://www.evidencemagazine.com/index.php/?option=comcontent&task=view&id=164
2. Bowyer, K.W., Chang, K., Flynn, P.: A survey of approaches and challenges in 3D and multimodal 3D + 2D face recognition. Comput. Vis. Image Underst. **101**(1), 1–15 (2006)
3. Browder, C.: DMV technology cracks down on fraud. WRAL.com. News article (2008). http://www.wral.com/news/local/story/4158631/
4. Evison, M., Vorder Bruegge, R.W.: The Magna Database: A database of three-dimensional facial images for research in human identification and recognition. Forensic Sci. Commun. **10**(2) (2008)
5. Evison, M.P., Vorder Bruegge, R.W.: Computer-Aided Forensic Facial Comparison. CRC Press, Boca Raton (2010)
6. Farkas, L.G., Munro, I.R. (eds.): Anthropometric Facial Proportions in Medicine. Charles C Thomas, Springfield (1987)
7. Huang, T., Xiong, Z., Zhang, Z.: Face recognition applications. In: Li, S.Z., Jain, A.K. (eds.) Handbook of Face Recognition. Springer, New York (2005)
8. Huber, R.A.: Expert witnesses. Crim. Law Q. **2**, 276–296 (1959)
9. Iannarelli, A.V.: The Iannarelli System of Ear Identification. Foundation Press, Brooklyn (1964)
10. Iscan, M.Y., Helmer, R.P. (eds.): Forensic Analysis of the Skull. Wiley-Liss, New York (1993)
11. Jain, A.K., Park, U.: Facial marks: Soft biometric for face recognition. In: Proceedings IEEE International Conference on Image Processing, pp. 37–40 (2009)
12. Jingu, H., Savvides, M.: In between 3D active appearance models and 3D morphable models. In: IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshop, pp. 20–26 (2009)
13. Kleinberg, K., Pharm, B., Vanezis, P., Burton, A.M.: Failure of anthropometry as a facial identification technique using high-quality photographs. J. Forensic Sci. **4**, 779–783 (2007)
14. O'Toole, A.J., Abdi, H., Jiang, F., Phillips, P.J.: Fusing face-verification algorithms and humans. IEEE Trans. Syst. Man Cybern. B **37**(5) (2007)
15. Scientific Working Group on Imaging Technologies, Best practices for forensic image analysis. Forensic Sci. Commun. (2005). http://www.fbi.gov/hq/lab/fsc/backissu/oct2005/standards/200510standards01.htm
16. Spaun, N.A.: Facial comparison by subject matter experts: Their role in biometrics and their training. In: Tistarelli, M., Nixon, M.S. (eds.) Advances in Biometrics. LNCS, vol. 5558, pp. 161–168. Springer, Berlin (2009)
17. Tuthill, H., George, G.: Individualization: Principles and Procedures in Criminalistics, 2nd edn. Lightning Powder, Jacksonville (2002)
18. van der Lugt, C.: Earprint Identification. Elsevier, Amsterdam (2001)
19. Vanezis, P., Brierley, C.: Facial image comparison of crime suspects using video superimposition. Sci. Justice **36**, 27–34 (1996)

20. Vorder Bruegge, R.W., Musheno, T.: Some cautions regarding the application of biometric analysis and computer-aided facial recognition in law enforcement. In: Proceedings of the American Defense Preparedness Association's 12th Annual Joint Government-Industry Security Technology Symposium and Exhibition, p. 8 (1996)
21. Zhang, Y., McCullough, C., Sullins, J.R., Ross, C.R.: Human and computer evaluations of face sketches with implications for forensic investigations. In: Proceedings of 2nd International Conference on Biometrics: Theory, Applications, and Systems (BTAS), pp. 475–485 (2008)