Face Recognition: Some Challenges in Forensics

Anil K. Jain, Brendan Klare and Unsang Park
Department of Computer Science and Engineering
Michigan State University
East Lansing, MI, U.S.A
{jain, klarebre, parkunsa}@cse.msu.edu

***Abstract*—Face recognition is becoming a valuable and routine forensic tool used by criminal investigators. Compared to automated face recognition, forensic face recognition must be able to handle facial images captured under non-ideal conditions and has high liability for following legal procedures. This paper discusses recent developments in automated face recognition that impact the forensic face recognition community. Improvements in forensic face recognition through research in facial aging, facial marks, forensic sketch recognition, video, near-infrared recognition, and soft biometrics will be discussed. Finally, current limitations and future research directions for face recognition in forensics are suggested.**

Keywords- face recognition; forensics; facial marks; aging; forensic sketch; face in video; unconstrained face recognition

I. Introduction

Face recognition is the ability to establish a subject's identity based on his facial characteristics. Automatic face recognition has been extensively studied over the past two decades due to its important role in a number of application domains, including access control, visual surveillance, and de-duplication of government issued identity documents (e.g., passport and driver license), to name a few. Face recognition systems generally operate under one of two scenarios: verification or identification [1]. In a verification scenario, the similarity between two face images is measured and a determination of either match or non-match is made. In an identification scenario, the similarity between a given face image (probe) and all the face images in a large database (gallery) is computed; the top (rank-1) match is returned as the hypothesized identity of the subject. Ideally, both of these scenarios are expected to operate in a "lights out" mode, i.e., the system makes an identity decision without requiring any human interaction.

The performance of automatic face recognition techniques has been evaluated in a series of tests conducted by the National Institute of Standards and Technology (NIST) using the FERET evaluation methodology [17]. The Face Recognition Vendor Test (FRVT) and Face Recognition Grand Challenge (FRGC) have continued these benchmarks with participants from both industry and academia. In the FRVT 2002 [13], an identification accuracy of ~70% was achieved for facial images with near frontal pose and normal lighting conditions on a large gallery (121,589 face images of 37,437 subjects). The most recent test, FRVT 2006 [14], involved a verification scenario; the best performing system showed a False Reject Rate (FRR) of 0.01 at a False Accept Rate (FAR) of 0.001 for high resolution (400 pixels between eyes) or 3D images. See Fig. 1 for examples of test images used in FRVT 2006.

Despite the impressive performance of automatic face recognition systems in a controlled setting, the benchmarked error rates in FRVT do not reflect the accuracy of face recognition systems when used in certain operational and forensic scenarios where it is not possible to make restrictive assumptions about ambient illumination, subject pose, sensor resolution, and compression (see Fig. 2). Contrary to the CSI-effect [27], which gives the illusory impression to citizens about the capabilities of state of the art face recognition technology, a number of prototype deployments (e.g., the Super Bowl game in Tampa in 2001 [33] and the Meinz railway station test in Germany in 2006 [36]) did not meet the required levels of matching accuracy. On the other hand, there are a few face biometric applications successfully deployed such as Smartgate in Australia [34] and the border control system between Hong Kong and China [35]), where user's cooperation is expected under a constrained environment. In addition to the effects of these extrinsic variables on face recognition accuracy, real-world forensic scenarios exhibit intrinsic variables (e.g., facial aging, expression and cosmetic makeup) which further degrade the recognition performance and are generally not replicated in controlled studies.

Forensic science, or simply forensics, deals with the application of scientific principles to analyze data collected by law enforcement agencies. There is an increased emphasis on this field in order to prove or disprove the guilt of a suspect with high confidence under the legal system. Some examples of forensic science applications include blood spatter analysis, soil analysis, pathology, DNA identification, shoe print matching, latent fingerprint examination, and surveillance video analysis. These examples illustrate the range of data used in forensics, where one of the major goals is to establish the identity of the suspect. While fingerprint and DNA forensic identification are two of the most reliable and available identification methods in forensic science, continued progress in automated face recognition technology is necessary to improve the set of tools available to determine a person's identity, particularly from surveillance imagery.

(a) (b) (c) (d)

Figure 1. Example images used in FRVT 2006. (a) Controlled lighting, neutral expression (IPD = 400 pixels), (b) controlled lighting, smiling, (c) uncontrolled lighting, smiling (IPD = 190 pixels), and (d) 3D shape and texture. IPD stands for inter-pupillary distance.

Face recognition by humans has a long history in forensics. The first attempt to identify a subject by comparing a pair of facial photographs was reported in a British court in 1871 [11], and the first known systematic method for face recognition was developed by the French criminologist Alphonse Bertillon in 1882 [28].

The first paper on automatic face recognition appeared in 1966 by Bledsoe et al. [29]. The project was called “man-machine” because a set of facial features are extracted from the photographs by a human. These features are then fed to a computer to conduct automated matching. From the set of feature points (such as the center of pupils, inside and outside corners of eyes, point of widows peak, etc) a list of 20 distances were computed and used to measure the similarity between face images. The man-machine system was able to consistently outperform humans based on a database of over 2,000 photographs. Goldstein and Harmon [37] also used 22 descriptive features (morphological descriptions of the face, hair, eyebrows, etc.) to identify people based on face images. These features are provided to a set of trained jurors as well as computers to conduct identification tasks. They concluded that six different features are required to identify a person in a database of 255 subjects, and predicted that 14 features are required to identify a person in a gallery of 4×10^6 faces.

The first fully automatic face identification system was developed by Kanade [38] using a set of facial parameters based on local histograms of gray scale pixel values. It was not until much later that many other automated face recognition systems were introduced. The Principal Component Analysis (PCA) method was first applied on face images by Sirovich [40] for image compression, then by Turk and Pentland [41] for identification. The ordered set of eigenvectors corresponds to a set of basis images that characterizes the variation between face images. PCA based approaches greatly reduced the computational burden and inspired more active research in face recognition. Another popular face recognition method is Linear Discriminant Analysis (LDA) [26], which is based on the Fisher's Liner Discriminant Analysis. The use of separate class labels for each subject in LDA provided better identification accuracy over PCA. Some other well known methods include Elastic Bunch Graph Matching (EBGM) [25] and Local Binary Pattern (LBP) [43] based feature representation. Table 1 shows a summary of representative works in face recognition.

(a) (b) (c) (d) (e)

Figure 2. Examples of face images commonly encountered in forensic applications. (a) A mug shot, (b) an image of a deceased subject (John Dillinger), (c) a sketch, (d) a video frame, and (e) a near infrared (NIR) image

Table 1. Summary of representative works in the history of automated face recognition research.

	Approach	*Database*	*Identi-fication Accuracy*
Bledsoe et al. [29]	20 features such as width of mouth, width of eyes, etc. (first semi-automatic method.)	N/A*	N/A*
Goldstein and Harmon [37]	22 features including simple morphological description about face, hair, eyebrows, etc. (semi-automatic)	255 images of 7 subjects	53 %
Kanade [38]	Local histogram (first fully automatic method)	20 images of 20 subjects	75 %
Turk and Pentland [41]	Principal component analysis (PCA or Eigenface)	21,500 images of 16 subjects	100 %
Belhumeur et al. [26]	Linear Discriminant Analysis (LDA)	160 images of 16 subjects (Yale DB)	99.4 %
Ahonen et al. [43]	Local Binary Patterns (LBP)	1,196 Subjects (FERET DB)	97 %

* We were unable to obtain a copy of this paper. The information about this paper was found at http://en.wikipedia.org/wiki/Facial_recognition_system

While a majority of the face gallery images used in the forensics domain are mug shots (frontal pose and normal illumination with minimal expression), probe face images are often captured at different pose, illumination, resolution, and modality (e.g., infrared, 3D image, etc.). For example, face images captured by surveillance cameras play a similar role as latent fingerprints, where the images present different degrees of difficulty in identification depending on motion blur, pose, and occlusion. With the rapid growth in the number of surveillance cameras worldwide (see Fig. 3), the progression of accurate and robust face identification techniques in videos is of utmost importance to law enforcement agencies. Images appearing in faxed, printed, and scanned documents are also often considered in forensics domain [49].

Forensic face recognition departs from automated face recognition in that it generally includes a human in the loop

(a) (b)

Figure 3. Surveillance cameras on the streets in China. There are about 400,000 surveillance cameras in Beijing alone that provide 100% coverage of public places (schools, hospitals, subways, etc.).

(Fig. 4). Many factors contribute to this requirement, such as low quality probe images, the use of metadata (demographics) to improve the chance of a successful match, and the need to present sound evidence in courts of law. The typical forensic face recognition scenario begins with a large gallery of face images, such as mug shot images and driver license photographs. For example, the face recognition system at the Pinellas County Sherriff's Office has a database of over 6 million face images [3], which is populated by both mug shot images (captured at the time of arrest) and Florida Department of Motor Vehicles (DMV) images [2]. An automatic face recognition system is needed to search queries against such a large gallery database. Given that the queries in the forensic scenarios are often captured under non-ideal situations (e.g., off-pose and low resolution CCTV frames, images captured from an ATM, a forensic sketch, or an image from a social networking site), the most similar *N* subjects (top N ranks) retrieved from the automatic system are considered "soft" suspects, which are then manually examined by forensic experts to determine the correct match. The manual inspection procedure needs to be standardized to minimize the subjective decisions. The National Academies report on "Identifying the Needs of the Forensic Sciences Community" made thirteen specific recommendations [12], which also emphasize the need for standardization of the inspection and interpretation of forensic evidence and performance measurement.

Note that a high match score between two face images alone may not be sufficient for a conviction in criminal court. Instead, investigators use the face recognition to identify a set of candidates; additional cues or supporting evidence from other sources is used to find the most likely suspect to the crime.

In summary, the following characteristics distinguish forensic face recognition from automatic face recognition:

1. Probe image quality is non-ideal (e.g. partial face, off-pose, high compression, and low resolution)

2. Top N matches are examined, as opposed to a rank-1 match

This paper is meant to increase the awareness and understanding of important challenges in forensic face

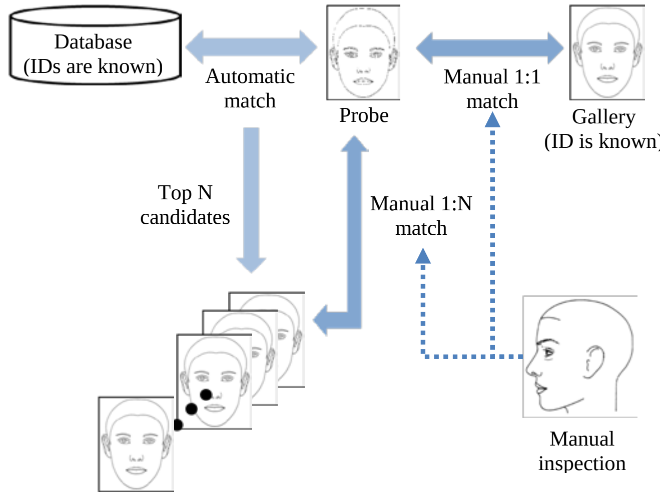


Figure 4. Schematic of forensic face recognition process. While the inspection procedure is fully manual when comparing two images, it is semiautomatic in searching a large database. In many scenarios, forensic face recognition is not yet fully automatic.

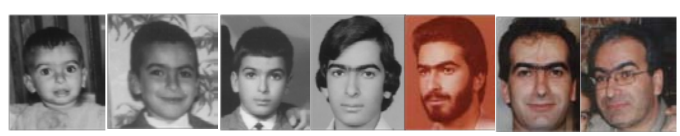
recognition. We provide some of the major research topics in forensic face recognition, including age invariant face recognition, facial mark based matching and retrieval, matching forensic sketches to mug shots, face recognition in surveillance videos (CCTV, ATM feed, etc.), and matching near infrared images to photographs.

II. Forensic Face Recognition Challenges

This section will discuss advances in several face recognition research areas of importance to forensic face recognition. The choice of these specific problems is influenced by our own ongoing research.

A. Facial Aging

Many face recognition scenarios exhibit a significant age difference between the probe and gallery images of a subject. As the age between a probe and a gallery image of the same subject increases, the accuracy of state of the art face



Age 2 5 10 16 19 29 40

(a) Images of a subject from the FG-NET database [7]

Age 25 36 40 43 48

(b) Images of a subject from the MORPH database [35]

Figure 5. Change in facial appearance due to aging.

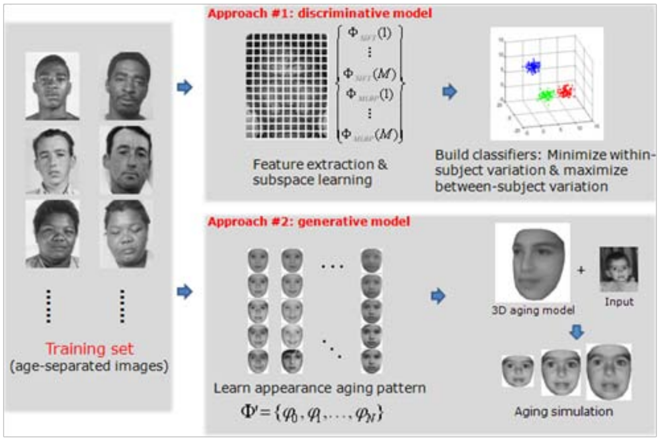


Figure 6. Schematic of discriminative and generative aging models.

recognition systems generally decreases. Some face recognition applications where such age differences are encountered include 1) identifying missing children and 2) detecting if a user/suspect is present in a database (law enforcement or DMV databases).

Facial aging is a complex process that affects both the shape and texture (e.g., skin tone or wrinkles) of a face. This aging process also appears in different manifestations in different age groups. While facial aging is mostly represented by facial growth in younger age groups (≤18 years), it is mostly characterized by relatively large texture changes and minor shape changes (e.g., due to change in subject's weight or stiffness of skin) in older age groups (>18 years). Fig. 5 shows aging variations of two subjects in the FG-NET [7] and MORPH [31] databases. As expected, the facial appearance changes more drastically at younger ages. In addition to facial aging, there are other factors that influence facial appearance as well (e.g. pose, lighting, expression, occlusion) which makes it difficult to study the aging pattern using these two public domain longitudinal face databases.

Li, Park, and Jain [32] proposed both discriminative and generative aging models for age invariant face recognition. The generative model learns the parametric aging model in the 3D domain to generate synthetic images and reduce the age gap between probe and gallery. The generative 3D aging modeling technique uses a pose correction method and aging model in the 3D domain. 3D modeling is well suited to capture the aging patterns due to the 3D nature of aging. Because no 3D aging database is currently available, the proposed 3D aging model was built using a 2D face aging database. The discriminative model learns the salient features to better recognize the face images across age gaps. Fig. 6 shows the schematic of both generative and discriminative aging modeling methods. Fig. 7 shows example matching results where aging modeling improved the matching accuracy of a leading face recognition engine, FaceVACS [21]. A face recognition test with 10,000 images of 10,000 subjects from MORPH database in probe and gallery showed approximately

Figure 7. Example of face recognition in the presence of aging where a commercial matcher fails but the proposed aging model succeeds [36]. The top row shows the gallery images, and the bottom row shows the probe images of the same subjects.

(a) (b) (c)

Figure 8. Example face images with distinctive facial marks. (a) Large birth mark, (b) scar, and (c) tear drop tattoo.

8% improvement in rank-1 identification accuracy by using the proposed aging models [32].

B. Facial Marks

Local facial mark features such scars, moles, and freckles play an important role for matching face images in forensic applications (see Fig. 8) [22]. The explicit use of face marks has become valuable due to the availability of higher resolution sensors, compatibility with manual identification, and the growing size of face image databases. Local facial mark features provide a unique capability to investigate, annotate, and exploit face images in forensic applications by improving both the accuracy and the matching speed of face-recognition systems. This information is also necessary for forensic experts to give testimony in courts of law where they are expected to conclusively identify suspects [23].

Most of the current photo-based identifications in law enforcement units and related security organizations involve a manual verification stage. The identification information is often provided by a victim or witness in terms of verbal descriptions and hand-drawn sketches [6]. Spaun [22] [23] describes the facial examination process carried out in the law enforcement agencies (the five-step manual examination procedure is referred to as ACE-V [24]), where one of the major steps is to identify the "class" and "individual"

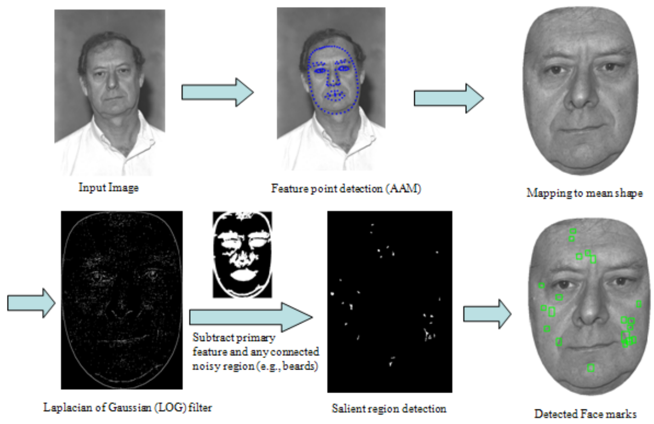


Figure 9. Schematic of automatic mark detection process [5].

characteristics. The class information includes overall facial shape, hair color, presence of facial hair, shape of the nose, presence of freckles, etc. The individual characteristics include the number and locations of freckles, scars, tattoos, chipped teeth, lip creases, number and location of wrinkles, etc., in a face. An automatic procedure for this examination will not only reduce the time-consuming and subjective manual process, but is likely to be more consistent and accurate. Further, it is expected that the computer-aided automatic feature extraction and representation will help standardize the examination process and make the process more efficient.

Conventional face-recognition systems typically encode the face images by utilizing either local or global texture features. However, these techniques do not explicitly utilize local marks (e.g., scars and moles) and usually expect the input to be a full face image. To fill this void, Park and Jain proposed the automatic facial mark detection process shown in Fig. 9 [5].

Face mark patterns have been shown to be reliable when used as a soft biometric [5]. Park and Jain developed a framework for text query retrieval of subjects using face marks [5]. Textual queries allow investigators to retrieve a list of subjects who contain some combination of face marks, such as “Mole on Left Cheek” AND “Scar on Forehead”.

A face mark retrieval system is not expected to identify a subject alone. Instead, it can be used to filter a candidate population. A witness can provide the information that a suspect has a mole on his left cheek and a scar on his forehead. Even in scenarios where no probe face image exists, this information can still be leveraged in an automated fashion to (for example) retrieve a list of felons who meet this criterion. Coupled with additional demographic information that may be available (gender, age, height, etc.), investigators may be left with only a few dozen individuals to investigate.

In addition to permitting face retrieval without a face image, Fig. 10 shows a few example image pairs where the explicit use of facial marks improved the matching accuracy (when fused with a commercial matcher). The first and second rows in Fig. 10 show example images that did not match at rank-1, but when fused with face mark match scores they improved to rank-1 matches. The third and fourth rows show facial images of identical twins that were incorrectly matched at rank-1 unless face marks were used. Face marks are critical in the identification of identical twins [9]. The use of facial mark improved the rank-1 identification accuracy of FaceVACS by about 0.5% based on 213 images of 213 subjects as probes and 10,213 images of 10,213 subjects in the gallery [5].

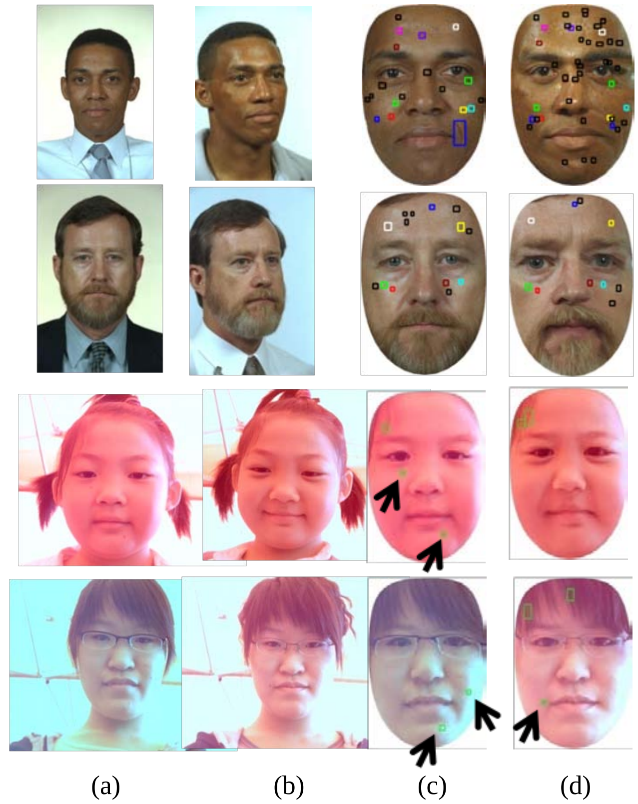


Figure 10. Example image pairs where facial marks helped to improve the matching performance. (a) (b) Probe and gallery images for the first two rows and two images of identical twins for the third and fourth rows. (c) (d) Facial mark detection results from (a) and (b).

C. Forensic Sketch Recognition

When no photograph of a suspect is available, a forensic sketch is often generated. Forensic sketches are an artist rendition of a person’s facial appearance that is derived from an eye witness description. Forensic sketches have a long history of use, where traditionally they have been disseminated to media outlets and law enforcement agencies in the hopes that someone will recognize the person in the sketch. Forensic sketches can be misleading due to errors in witness memory recall that cause inaccuracies in the sketch drawn by a forensics artist. Because a significant amount of time is needed to generate a single forensic sketch, they generally represent culprits who committed the most heinous crimes (e.g. murder

Figure 11. Examples of failed matches in forensic sketch recognition [6].

and rape). Thus, the ability to match forensic sketches to mug shot databases is of great importance.

Commercial face recognition systems are not designed to match forensic sketches against face photographs. To fill this gap, Klare, Li, and Jain [6] developed a framework for matching forensic sketches to photographs. Using a forensic sketch, the proposed system allows investigators to match the sketch against large face databases. The method from [6] encodes the structure of both sketches and photographs using local binary patterns [15] and SIFT feature descriptors [16]. Each of these two feature descriptors has the desirable property of having little variation in both sketch and photo modalities. With sketch and photos represented using feature descriptors, multiple linear discriminant subspaces are learned on vertical slices of face image patches in a framework called Local Feature-based Discriminant Analysis (LFDA). LFDA demonstrated substantial improvements over a commercial recognition system [6]. For example, when using 49 probe subjects and 10,159 gallery subjects, the rank-50 accuracy of LFDA with race and gender filtering was 44.9%. This is compared to a rank-50 accuracy of 26.53% for FaceVACS with race and gender filtering. The use of specially designed sketch recognition systems such as LFDA is necessary to maximize the capabilities of forensic sketch recognition.

A major difficulty in forensic sketch recognition is a witness's inability to correctly remember the appearance of the subject. Fig. 11 shows two examples where the top retrieved photograph (second column) is incorrect, but more closely resembles the subject in the sketch (first column) than the true photo of the subject (third column). Even though this problem also extends beyond automated sketch recognition (i.e., humans must also overcome these same noises), it demonstrates the difficulty of forensic sketch recognition. Thus, investigators must proceed carefully when examining retrieved images from a forensic sketch recognition system.

D. Face Recognition in Video

Face recognition in video has gained importance due to the widespread deployment of surveillance cameras. The ability to automatically recognize faces in video streams will facilitate a method of human identification using the existing networks of surveillance cameras. However, face images in video often contain non-frontal poses of the face and undergo severe lighting changes. Fig. 12 (a) shows example frames captured in a video stream. The multiple frames captured from the same subject and provided by a video stream enables the user to selectively use face images in a good quality (e.g., frontal pose or neutral expression). The temporal information such as the dynamic facial expression changes can also be used in face recognition [48]. Since most of the face images captured from conventional surveillance cameras appear at low resolution, the pair of static and PTZ camera systems are used in tandem. Fig. 12 (b) shows both global and close-up view images captured by a pair of static and PTZ camera system developed for the face recognition at a distance [44]. The static camera alerts the PTZ camera of the presence of a subject, and PTZ camera then acquires a higher quality face image of the subject.

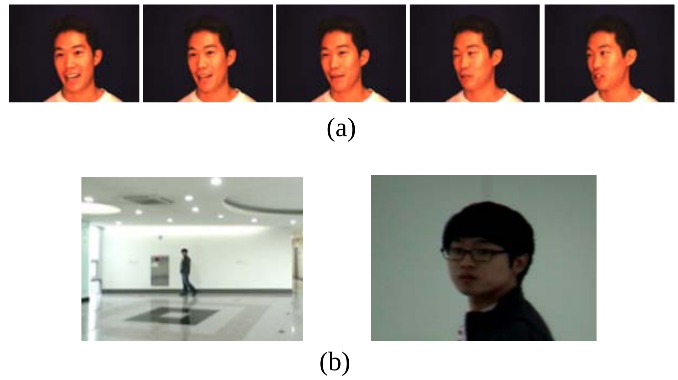


Figure 12. Example face images in video. (a) Five consecutive frames in a video. (b) Global and close-up views captured by a pair of static and PTZ cameras

Volker and Blanz [30] proposed a well known view-synthesis method, the 3D morphable model, which synthesizes the 3D face model from a 2D image. This method only requires a single image at an arbitrary pose, but the fitting process takes a few minutes and requires manual initial alignment. Park and Jain [4] used the structure-from-motion method which utilizes facial landmarks obtained from video sequences to infer the 3-D face shape. The use of 3D modeling and a PTZ camera improved the rank-1 identification accuracy by about 40% and 98%, respectively. The 3D modeling face recognition experiments used the Face In Action (FIA) database with 221 subjects, and the PTZ camera experiments used a combination of a private database and the MORPH database with 20 probe subjects and 10,020 gallery subjects.

E. Near-Infrared Face Recognition

The use of near-infrared (NIR) face images has been proposed as a method for overcoming the impact of varying illumination [45] [46]. Similar to sketch recognition, most applications of near-infrared face recognition are in a heterogeneous face recognition scenario, where the gallery

Figure 13. Near infrared face images (first row), and the corresponding photographs (second row). Near infrared face images have ideal properties for acquiring face images in surveillance scenarios. Images are from [47].

images are standard photographs. An example of face images acquired in NIR and visible (VIS) spectrums can be found in Fig. 13.

Klare and Jain [45] proposed a feature-based framework for matching NIR face probe images to visible gallery images. Both NIR and VIS face images were represented using SIFT and LBP descriptors. A random subspace framework was used with a sparse representation matcher. Using the public HFB dataset [47], Klare and Jain's proposed method when combined with a commercial matcher, FaceVACS [21], achieved a true accept rates of ~94% at a false accept rate of 1.0%.

Given the strong accuracies of matching NIR and VIS face images, surveillance systems should also consider the use of NIR cameras to compensate for illumination issues. Because the human eye is not sensitive to NIR illumination, NIR camera systems can covertly utilize directed NIR illumination without alerting subjects. This advantage allows the illumination to be tailored for improved face recognition in a particular environment.

F. *Soft Biometrics*

Systems designed to leverage soft biometrics that may be determined using face images are another useful tool in forensic face recognition. Soft biometric demographic information (such as race, gender, and general age) can usually be determined from low quality face images. The explicit use of this information in difficult recognition scenarios has been shown to improve face recognition accuracies [5] [6] [9].

III. Summary and Future Work

Despite the host of tools highlighted in the previous section, many limitations still exist in forensic face recognition.

A. *Individuality Models*

Face recognition systems return a match score between two face images indicating their level of similarity. Often these scores are normalized to the range [0,1], making them analogous to a probability of a true match. However, these match scores do not truly measure such a probability because no face individuality models have been developed.

Spaun [22] mentioned how the lack of face individuality models limits legal testimony to being opinion-based. A recent study on forensic facial comparison similarly mentioned this shortcoming [8]. Klare and Jain [9] proposed an organization of the salient information contained in facial photographs into three feature levels (analogous to the three levels in fingerprint features). By organizing the information contained in facial images, the taxonomy of facial features facilitates future studies of facial individuality.

Despite initial efforts in [5] [8] [9], we are still far removed from having a valid individuality model. Until such an individuality model is developed and accepted in a peer reviewed setting, the automated face recognition results have limited use as evidence in court. Thus, the substantial activity in face recognition research is greatly limited by a relatively non-existent amount of research in facial individuality studies. It is critical for this gap to be closed.

B. *Component-based Recognition*

Face recognition systems are generally designed to match images of full faces. Forensic scenarios exist in which a component-based recognition system would be useful. Such a system would receive as input a specific sub-region of the face containing components such as a nose, mouth, or eyebrows. However, with the exception of perioccular recognition systems [10], few advances have been made in component based recognition.

A component-based COTS FR system would ideally have the following functionality to augment forensic capabilities. Given a probe face (partial or complete), matching and retrieval would be performed per facial components (eyes, nose, mouth, chin, and eyebrows). While such a system would have limited benefit in standard face recognition scenarios, it would be of great value to forensic investigators. Allowing investigators to specify a specific region of the face prevents incomplete, noisy, and missing regions from degrading the accuracy.

Pericoluar recognition systems have quickly established a reputation of acceptable accuracy, though their motivation was primarily in leveraging additional information captured from iris recognition systems. Fully understanding the utility of other facial components from a forensic standpoint could lead to other similarly impressive results. Further, a better understanding of component-based face recognition should facilitate the study of individuality models.

IV. Conclusions

This paper highlights some of the problems and challenges in the field of forensic face recognition. Contrary to standard automated face recognition, forensic face recognition offers a set of tools that can help investigators narrow the identity of a subject, but not fully perform the identification. A host of research has improved the abilities of forensic face recognition by studying facial aging, facial marks, sketch to photo matching, video based face recognition, and NIR image to photo match. However, many open problems related to forensic face recognition still exist, and need to receive more attention in academic research.

REFERENCES

[1] A. K. Jain, P. Flynn, A. Ross (Eds), Handbook of Biometrics, Springer, 2007

[2] S.Z. Li and A.K. Jain (eds.), Handbook of Face Recognition, Springer, 2005

[3] Pinellas County Sheriff's Office, "Agency's Use Of Driver Licenses In Facial Recognition Is First In The Nation," The Star, Vol. 21, No. 3. 2009.

[4] U. Park and A.K.Jain, "3D Model-Based Face Recognition in Video," Proc. Int. Conference on Biometrics (ICB), 2007.

[5] U. Park and A. K. Jain, "Face Matching and Retrieval Using Soft Biometrics," IEEE Trans. on IFS, Vol. 5, No. 3, pp. 406-415, 2010

[6] B. Klare, Z. Li, and A. K. Jain, "Matching Forensic Sketches to Mugshot Photos," IEEE Trans. on PAMI, 2011. To appear.

[7] FG-NET Aging Database, http://www.fgnet.rsunit.com, 2010.

[8] M. P. Evison and R.W. Vorder Bruegge (Eds.), Computer-aided Forensic Facial Comparison. CRC Press, 2010, ch. 1,10.

[9] B. Klare and A. K. Jain, "On a Taxonomy of Facial Features," Proc. Biometrics: Theory, Applications and Systems (BTAS), 2010.

[10] U. Park, R. Jillela, A. Ross, and A. K. Jain, "Periocular Biometrics in the Visible Spectrum," IEEE Trans. on IFS, 2011. To appear.

[11] G. Porter and G. Doran, "An Anatomical and Photographic Technique for Forensic Facial Identification," Forensic Science International, Vol. 114, pp. 97–105, 2000.

[12] National Research Council, "Committee on Identifying the Needs of the Forensic Sciences Community," 2009.

[13] P. J. Phillips, P. Grother, R. J. Micheals, D. M. Blackburn, E. Tabassi and M. Bone, "Face Recognition Vendor Test 2002: Evaluation Report," Tech. Report NISTIR 6965, NIST, 2003

[14] P. J. Phillips, W. T. Scruggs, A. J. O'Toole, P. J. Flynn, K. W. Bowyer, C. L. Schott and M. Sharpe "Face Recognition Vendor Test 2006: FRVT 2006 and ICE 2006 Large-Scale Results," Tech. Report NISTIR 7408, NIST, 2007

[15] T. Ojala, M. Pietikainen, and T. Maenpaa,, "Multiresolution Gray-Scale and Rotation Invariant Texture Classification with Local Binary Patterns," IEEE Trans. on PAMI, vol. 24, no. 7, pp. 971-987, July 2002

[16] D. Lowe, "Distinctive Image Features from Scale-Invariant Keypoints," Int'l J. Computer Vision, vol. 60, no. 2, pp. 91-110, 2004.

[17] P.J. Phillips, H. Moon, S. Rizvi, and P. Rauss, "The FERET Evaluation Methodology for Face-Recognition Algorithms," IEEE Trans. on PAMI, vol. 22, no. 10, pp. 1090-1104, Oct. 2000.

[18] L. Gibson, Forensic Art Essentials. Elsevier, 2008.

[19] H. Ling, S. Soatto, N. Ramanathan, and D. Jacobs, "A Study of Face Recognition as People Age," Proc. IEEE Int'l Conf. Computer Vision, pp. 1-8, 2007.

[20] N. Ramanathan and R. Chellappa, "Face Verification Across Age Progression," Proc. IEEE CS Conf. Computer Vision and Pattern Recognition, vol. 2, pp. 462-469, 2005.

[21] FaceVACS Software Developer Kit, Cognitec Systems GmbH, http://www.cognitec-systems.de, 2010.

[22] N. A. Spaun, "Forensic Biometrics from Images and Video at the Federal Bureau of Investigation," in Proc. BTAS, 2007, pp. 1–3.

[23] N. A. Spaun, "Facial Comparisons by Subject Matter Experts: Their Role in Biometrics and Their Training," in Proc. ICB, 2009, pp. 161–168.

[24] H. Tuthill and G. George, Individualization: Principles and Procedures in Criminalistics. Florida: Lightning Powder Company, Inc., 2002.

[25] L. Wiskott, J.-M. Fellous, N. Kruger, and C. von der Malsburg, "Face Recognition by Elastic Bunch Graph Matching," IEEE Trans. on PAMI, vol. 19, no. 7, pp. 775–779, Jul. 1997.

[26] P. N. Belhumeur, J. P. Hespanha, and D. J. Kriegman, "Eigenfaces vs. Fisherfaces: Recognition Using Class Specific Linear Projection," IEEE Trans. on PAMI, vol. 19, no. 7, pp. 711–720, Jul. 1997.

[27] M. M. Houck, "CSI: The Reality," Scientific American, pp. 85-89, June 2006.

[28] A. Bertillon, Signaletic Instructions including the theory and practice of Anthropometrical Identification, R.W. McClaughry Translation. The Werner Company, 1896.

[29] W. W. Bledsoe, "Man-machine Facial Recognition," Tech. Report. PRI: 22, Panoramic Res. Inc., Palo Alto, CA, 1966.

[30] V. Blanz and T. Vetter, "Face Recognition Based on Fitting a 3D Morphable Model," IEEE Trans. on PAMI, pp. 1063-1074, September, 2003

[31] K. Ricanek Jr and T. Tesafaye, "Morph: A Longitudinal Image Database of Normal Adult Age-Progression," in Int. Conf. Automatic Face and Gesture Recognition, pp. 341-345, 2006.

[32] Z. Li, U. Park, and A. K. Jain, "A Discriminative Model for Age Invariant Face Recognition," IEEE Trans. on IFS, Under review.

[33] J. Bonner, "Looking for Faces in the Super Bowl Crowd," Access Control & Security Systems Magazine, 2001.

[34] Smartgate, http://www.customs.gov.au/site/page5552.asp

[35] Chinese/Hong Kong border automated with biometrics, Biometric Technology Today, vol. 15, no. 5, pp. 3, 2007.

[36] J. S. Dempsey and L. S. Forst, An Introduction to Policing (5th ed.), Delmar-Cengage Learning Publishers, NY, 2010.

[37] A. J. Goldstein and L. D. Harmon, "Identification of Human Faces," Proceedings of IEEE, vol. 59, no. 5, pp. 748–760, 1971.

[38] T. Kanade, "Picture Processing System by Computer Complex and Recognition of Human faces,"Ph.D. dissertation, Kyoto University, 1973..

[39] R. Brunelli and T. Poggio, "Face Recognition: Features versus Templates," IEEE Trans. on PAMI, vol. 15, no. 10, pp. 1042–1052, 1993.

[40] L. Sirovich and M. Kirby, "Low-dimensional Procedure for the Characterization of Human Faces," Journal of Optical Society of America, A, vol. 4, no. 3, pp. 519–524, 1987.

[41] M. Turk and A. Pentland, "Eigenfaces for Recognition," Cognitive Neuroscience, vol. 3, pp. 72–86, 1991.

[42] P. N. Belhumeur, J. P. Hespanha, and D. J. Kriegman, "Eigenfaces vs. Fsherfaces: Recognition Using Class Specific Linear Projection," IEEE Trans. on PAMI, vol. 19, no. 7, pp. 711–720, 1997.

[43] T. Ahonen, A. Hadid, and M. Pietikainen, "Face Description with Local Binary Patterns: Application to Face Recognition," IEEE Trans. on PAMI, vol.28, no.12, pp.2037-2041, 2006.

[44] H.-C. Choi, U. Park, and A. K. Jain, "PTZ Camera Assisted Face Acquisition, Tracking & Recognition," Biometrics: Theory, Applications and Systems (BTAS), 2010

[45] B. Klare and A. K. Jain, "Heterogeneous Face Recognition: Matching NIR to Visible Light Images", in Proc. ICPR, 2010.

[46] S. Liao, D. Yi, Z. Lei, R. Qin, and S. Li. "Heterogeneous face recognition from local structures of normalized appearance," In Proc. 3rd ICB, 2009.

[47] S. Li, Z. Lei, and M. Ao. "The HFB face database for heterogeneous face biometrics research," In Proc. CVPRW, 2009.

[48] N. Ye and T. Sim, "Towards general motion-based face recognition," In Proc. CVPR, pp. 2598 - 2605, 2010.

[49] Thirimachos Bourlai, Arun Ross, and Anil K. Jain, "Restoring Degraded Face Images: A Case Study in Matching Faxed, Printed and Scanned Photos," IEEE Trans. on IFS, 2011. To appear.