## Video and Imaging, 2013-2016

Ruifrok, A.; Geradts, Z.

**Publication date**
2016
**Document Version**
Final published version
**Published in**
18th INTERPOL International Forensic Science Managers Symposium, Lyon, France


# 18th INTERPOL International Forensic Science Managers Symposium
# Lyon, France

## 11-13 October 2016
## Review Papers

**EDITED BY:**
DR. MAX M. HOUCK, FRSC
MANAGING DIRECTOR, FORENSIC & INTELLIGENCE SERVICES, LLC
ST. PETERSBURG FL USA
MAX@FORENSICINTELLIGENCE.US

# Table of Contents

Media Evidence

# Video and Imaging, 2013-2016

Arnout Ruifrok Ph.D., Netherlands Forensic Institute

Zeno Geradts Ph.D., Netherlands Forensic Institute and University of Amsterdam

Corresponding author: Zeno Geradts PhD, z.geradts@nfi.minvenj.nl

## 1. Introduction

In this review, the most important developments are presented for the following general fields of expertise: : (1) Biometric analysis of image material, (2) Detection of image manipulation, (3) Camera source identification, (4) Video image processing and Image search.

This year we have been requested to add Video to the review. Since there is clearly overlap, we have integrated this field in the review.

Working groups and organizations

The development of forensic image analysis has several international working groups:

- SWGIT: an American group that has produced a lot of guidelines and best practice manuals. http://www.swigit.org The group has terminated operations, since the new OSACs are formed http://www.nist.gov/forensics/osac.cfm . http://www.swigit.org/
- ENFSI DIWG: The ENFSI Digital Imaging Working Group that is focused on methods, techniques, education and training. http://www.enfsi.org
- LEVA : an American group focused on video processing and training: http://www.leva.org
- EESAG: an Australian-New Zealand group that proficiency tests for video and audio processing: http://www.nifs.com.au/eesag/about.html
- AGIB, A working group in Germany that is focused on facial image comparison: http://www.foto-identifikation.de/ .
- FISWG, An American group since 2009 that is focused on facial image comparison: http://www.fiswg.org
- OSAC Facial Identification Subcommittee, An American group part of the Organisation of Scientific Advice Committees, with focus on standards and guidelines related to the image-based comparisons of human facial features: http://www.nist.gov/forensics/osac/sub-face.cfm
- American Academy of Forensic Science [1] Within the American Academy of Forensic Science the Digital and Multimedia Sciences Section works in this field.

Since 2003 each year a workshop was organized on Forensic Image and Video processing with handouts on the methods for face comparison, video restoration, 3D reconstruction, length measurement, photogrammetry and image processing. Also each year a scientific session was organized on this field. More information is available on: http://www.aafs.org

## 2. ENFSI Forensic IT Working Group

The forensic IT working group of ENFSI [2], [3] deals with digital evidence as such. There exist some overlap with the Digital Imaging working group, and for that reason joint events are organized.

Since most CCTV-systems are digital nowadays, often the question of handling the CCTV system itself is a question of digital evidence. Hard drives and other digital media should be handled in a secure way with proper forensic imaging software. The working group organizes training conferences each year. More information is available from http://www.enfsi.eu/.

### 2.1 Biometric analysis of image material

Biometrics is regularly announced in news items as a panacea against terrorism, security problems, fraud, illegal migration, etcetera. Biometrics, which can be defined as the (automatic) identification or recognition of people based on physiological or behavioral characteristics, is not a single method or technique, but consists of a number of techniques, with each their own advantages and drawbacks. None of the available biometric modalities combines the properties of an ideal biometrics system. We have to acknowledge that biometrics never can be 100% accurate. However, if requirements and applications are carefully considered, biometric systems can provide an important contribution to investigation, authentication and safety.

Within the context of person identification (individualization), different processes can be defined. Within different areas of science, different terminologies are used for the same process, and sometimes the same terminologies are used for different processes. Therefore, a clear definition of the different terms as used in this text is important and made explicit here.

Recognition can be defined as the process of identifying or matching a person, his/her photograph or image with a mental image that one has previously stored in long term memory. Recognition requires observation and retention of a person's features and the process of comparison of the retained information with an external image whether it be the life person, a photograph or composite image. The word recognition is important for investigation as well as witness statements. Recognition is within the forensic community also used for the automated searching of a facial image in a biometric database (one-to-many), typically resulting in a group of facial images ranked by computer-evaluated similarity.

Identification is the most contentious term because this most often used term can mean several things in different context, like the automated searching of a facial image in a biometric database (one-to-many) in biometrics, the examination of two facial images or a live subject and a facial image (one-to-one) for the purpose of determining if they represent the same person in forensics, or the assignment of class or family name in biology and chemistry. Therefore, the authors of this paper prefer not to use the term identification unless the meaning is unambiguous within the context.

Recall is here defined as the process of retrieving descriptive information of a person from long term memory in the absence of the person, his/her photograph or other image. Recall requires observation, retention and reproduction of a person's features. Recall is essential for the production of composite images, as produced by a police artist for investigational purposes. However, these images can only be used as investigative tools, and can never be used as proof of identity.

### 2.2 Face

On top of the list of preferred, and in most travel documents required, biometric modalities is the face. The face has always been the most important personal feature on travel documents. The most important change the last decade is that the face is now also stored digitally in passport, and is optimized for automatic facial recognition. The automated systems are still very sensitive to ageing of the person depicted [Agrawal 2015, ]; The latest test results indicate that higher resolution and well controlled images may result in a 10-fold better performance than using average passport like images.

Facial image comparison is defined as the visual examination, by a human operator, of the differences and similarities between two facial images or a live subject and a facial image (one-to-one) for the purpose of determining if they represent the same person. In biometrics the one-to-one comparison is termed verification. The Facial Imaging Scientific Working (FISWG) group also uses the term Facial Identification for the same process. However, the authors of this review prefer to use the term facial image comparison, because that exactly describes the process, and cannot be confused with the use of the word identification as used in other contexts.

Facial Reconstruction is used in two different meanings:

1. The process of reconstructing three-dimensional facial (computer) models of individuals from their 2D photographic images or video sequences.
2. The process of recreating the face of an individual (whose identity is often not known) from their skeletal remains through an amalgamation of artistry, forensic science, anthropology, osteology, and anatomy.

These two different uses of facial reconstruction may meet when three-dimensional computer models are used to recreate the face of an individual based on skeletal remains. The current review does not consider facial reconstruction as a means to recreate the face of an individual based on skeletal remains.

Facial composite is a graphical representation of an eyewitness's memory of a face, as recorded by a composite artist, also sometimes termed facial sketch. A facial composite may be based on combination of images of facial features (photo composition) as well as actual drawings by a composite artist.

### 2.3 Facial image recognition

Biometric systems that can search databases with facial images, using automatically extracted facial features, are still being developed further. Face recognition error rates have declined massively in the two decades since initial commercialization of the various technologies [4]

However, one of the complicating issues is that the images of the unknown person often differ from the target images in the database with respect to the orientation of the head, the distance to the camera, the illumination and the image resolution. Recently, increased attention has been given to the existence of quality measures for face recognition [5][6]. New approaches focus on better acquisition techniques in order to get better images, from which as many facial features as possible can be extracted for comparison to images in the database.

### 2.4 Unconstrained images

Forensic material in general is not acquired under controlled circumstances. This means that a number of confounding factors may influence the effectiveness of face recognition. A number of academic studies try to tackle the different confounding factors, like pose issues,

resolution issues, and occlusions. How different quality features may influence the performance of face recognition systems has been studied by Dutta el al [6].

Several techniques are being developed to use unconditioned images and media collections for unconstrained face recognition [7] and partially occluded faces [8]. Though issues surrounding pose, occlusion, and resolution continue to confound matchers, there have been significant advances made in face recognition technology to assist law enforcement agencies in their investigations [9]

Park et al [10] report improvements in facial image retrieval of partially occluded images (sunglasses and scarfs), resulting in more than 90% retrieval of partially occluded faces.

Peng et al [11]have reported successful face recognition using a novel method for low-resolution face recognition.

**2.5 Pose variation**

Pose is the “orientation of the face with respect to the camera, consisting of pitch, roll, and yaw”. An optimal frontal pose may be considered as 0° in all directions. Variations to the optimal pose can be due to photographing a physical subject who can move freely during the capture process, or misalignment of the camera. As images are a 2-dimensional representation of the 3-dimensional world, pose of a subject has a major influence on the image captured by a capturing device. As a result of this the appearance and position of facial features can change depending of the pose of the person and the position of the camera at the moment of capture. This is, together with inter and intra observer variability of landmark annotation, one of the main causes of the limited value of landmark measurements on photographs [12]. However, development of pose detection and automatic landmark detection has been reported to result in almost 90% identification accuracy in side view positions [13].

For predicting face recognition performance in a video, it was observed that face detection confidence and face size serve as potentially useful quality measure metrics [14].

**2.6 3-dimensional face comparison**

The most promising approach to the complicating issues of pose and illumination is the use of 3 dimensional models for pose an illumination correction. Since the previous review, there has been an increase in reports on development of methods that are based on the use of 3-dimensional computer models of faces. A number of 3d-acquisition systems are now available for the acquisition of these models. Most 3d-cameras work with a configuration of 1 or more normal digital photo cameras, a flash and the projection of a pattern on the face. These models can be used in two ways. A 3d-facial model of a suspect can be compared to a 3d-model of an unknown person, or the 3d-model of a suspect is used to compute an image that can be compared to an image of an unknown person. Since there are many sources of images and video in practice, a number of studies are focused on the (partial) reconstruction of 3d-models from 1 or more images or video streams. Van Dam et all [15] developed a model 3-D face reconstruction algorithm based on 2D landmarks. he 3D landmark reconstruction algorithm simultaneously estimates the shape, pose and position of the face, based only on the fact that all images in the sequence are recorded using a single calibrated camera.

**2.7 Deep learning**

With the further development of computer technology, neural network approaches for facial recognition have gained renewed interest. Alignment and the representation of the face by

employing explicit 3D face modelling have resulted in improved accuracy of face recognition in unconstrained environments [16][17] [18] [19]

**2.8 Facial image comparison**

The result of facial image recognition is often the selection of 1 or more target facial images that could be matched with the image of the unknown person. In practice, however, this often leads to hit lists with multiple possible matches to the query image, and the correct target not necessarily on top of the hit list. In such cases, the decision has to be made by a forensic anthropologists or forensic image analysts. Since the previous review, more studies and proficiency tests have been reported on the performance of facial image comparison by lay people and experts, showing that there is a reason for concern, and that better methods and technology are needed. A number of institutes have published documents that describe their procedures for performing facial image comparison. These procedures show that measures are being taken to limit the influence of subjective judgments and that there is a need for quantitative statistical data. The FBI has started a working group in 2009 for facial image comparison that is expected to stimulate the development of better methods and technology (FISWG).

Human and computer performance has been systematically compared as part of face recognition competitions, with results being reported for both still and video imagery. Analysis of cross-modal performance shows that for matching frontal faces in still images, algorithms are consistently superior to humans. For video and difficult still face pairs, humans are superior [20]

People doing facial image comparison can be found in four different kinds of professions: forensic photographers, forensic anthropologists, video investigators and imaging scientists. Knowledge of anatomy and physiology of the face is needed to get a good interpretation of differences and similarities in facial features. Similarities or differences in such images can often be explained by differences in the imaging conditions, pointing to the importance of knowledge about optics. Small facial details can be distorted, and artifacts looking like small details introduced due to noise, pixel sampling and compression, requiring knowledge about image processing for the proper interpretation of observations. Changes in image quality, pose and position, lighting and facial expression greatly influence the comparison process. Therefore, it is strongly recommended that one acquire reference images of the suspect and a number of other people with the same video camera in the same situation under similar lighting conditions. While the techniques of facial image comparison are generally accepted within their practitioner communities, they are not tested, and their error rates are unknown. On that basis, the methods of facial image comparison would appear not to meet the anticipated standards [21]

It is well-established that matching images of unfamiliar faces is rather error prone. Experimental studies on face matching underestimate its difficulty in real-world situations. Photographs of *unfamiliar* faces seem to be unreliable proofs of identity, especially if the ID documents do not use very recent images of the holders [22]

Existing scientific knowledge of face matching accuracy is based almost exclusively, on people without formal training. Human performance curtails accuracy of face recognition systems, potentially reducing benchmark estimates by 50% in operational settings. Mere practice does not attenuate these limits [23], and some training methods may be inadequate [24]. However, large individual differences have been reported, suggesting that improvements in performance could be made by emphasizing personnel selection [25] White et al [26] also have shown that forensic facial examiners outperformed untrained participants and computer algorithms on challenging face matching tests, thereby providing

the first evidence that these examiners are experts at this task. Notably, computationally fusing responses of multiple experts produced near perfect performance.

### 2.9 Eyewitness identification / Facial composites

In most of the criminal investigations of a crime, one of the first steps is to interview eyewitnesses. In these interviews the witnesses are asked to provide a description of the perpetrators. For investigational purposes this description may be made into an image by a (police) sketch artist. The sketch artist can also help the witness to recall the face of the perpetrator by showing multiples examples of facial features. Instead of sketches, it is also possible to create photo compositions using examples from databases with facial images. As not always images of perpetrators are available, matching of composite sketches with facial photographs (e.g. mugshots) is of interest. Matching performance of composite or forensics sketches against photo galleries are promising but still considerably lower than photo matching performance of commercially available systems [27][28]

### 2.10 Other biometrics

#### 2.10.1 Ear

Even though current ear detection and recognition systems have reached a certain level of maturity, their success is limited to controlled indoor conditions. In addition to variation in illumination, other open research problems include occlusion due to hair, ear symmetry, earprint forensics, ear classification, and ear individuality [29]. The experimental results show that ear recognition may achieve an average rank-one recognition accuracy of more than 95% [30] Current studies are directed towards more robust automated methods for ear detection, landmark localization and ear recognition using 2D and 3D techniques [31], [32] [33].

#### 2.10.2 Body geometry and gait

With the standardisation of photographs, identification primarily occurs from the face. However, results consistently show that less body measurements are needed to find no duplicates when compared to the face. With the combination of eight body measurements, it is possible to achieve results comparable with fingerprint analysis [34]. Thicker garments produce higher inaccuracies in landmark localisation, but errors decrease as placement is repeated. Overall, comparison to truth reveals that on average statures can be predicted with accuracy in excess of 95% [35]

Also lower leg shape, sometimes the only body part consistently depicted in images, has been reported as “an effective biometric trait” [36]. Recent studies have shown that when face identification fails, people rely on the body but are unaware of doing so [37] Bouchrika et al [38] reported a method to extract gait features for different camera viewpoints achieving an identity recognition rate of 73.6 % processed for 2270 video sequences. Furthermore, experimental results confirmed the potential of the proposed method for identity tracking in real surveillance systems to recognize walking individuals across different views with an average recognition rate of 92.5 % for cross-camera matching for two different non-overlapping views.

Yang [39] describes a method for height estimations on eye measurement through a gate cycle.

#### 2.10.3 Soft biometrics

Soft biometric information extracted from a human body (e.g., height, gender, skin color, hair color, and so on) is ancillary information easily distinguished at a distance but it is not fully distinctive by itself in recognition tasks. However, this soft information can be explicitly fused

with biometric recognition systems to improve the overall recognition when confronting high variability conditions. The use of soft biometric traits is able to improve the performance of face recognition based on sparse representation on real and ideal scenarios by adaptive fusion rules [24]. Depending of the acquisition distance, the discriminative power of the facial regions can change. This results in some cases in better performance than achieved for the full face [40]

Soft biometrics introduce a possibility to automatically search databases based on biometric features obtained from verbal descriptions, resulting in more than 95% identification accuracy [41].

### 2.10.4 Liveness detection

Spoofing is the act of masquerading as a valid user by falsifying data to gain an illegitimate access. Vulnerability of recognition systems to spoofing attacks (presentation attacks) is still an open security issue in biometrics domain and among all biometric traits. Galbally [42] propose a technique using 25 general image quality features extracted from one image (i.e., the same acquired for authentication purposes) to distinguish between legitimate and impostor samples. The experimental results, obtained on publicly available data sets of fingerprint, iris, and 2D face, show that the proposed method is highly competitive compared with other state-of-the-art approaches and that the analysis of the general image quality of real biometric samples reveals highly valuable information that may be very efficiently used to discriminate them from fake traits. Erdogmus et al [43] studied detection problem of more complex 3D attack types using various texture based countermeasures.

## 3. Detection of image and video manipulation

Image and video files are changed for numerous reasons with and without a criminal intent. Images are scaled, cropped, rotated and compressed to make them fit for a document or a website. Contrast or colors are changed to enhance the visibility of details. This processing is often referred to as manipulation. However, manipulation could also refer to modification of an image with a criminal intent. One type of modification is a change of the visual content by hiding or inserting visual information in the original image. The other modification is non visual addition of information, like a text message in an image that is published on a website as a means of communication between persons. This modification is referred to as steganography.

A number of clues can be used for detection of manipulation by visual inspection, like discrepancies in lighting, brightness levels, color distributions, edges, noise patterns and compression artifacts in the transitions between the tampered and original parts of the questioned image. Visual inspection could be not feasible anymore when it is not known which region in an image is being questioned.  A lot of research was focused on automated detection of regions in an image that might have been tampered with . However, most of the methods that have been published do only produce indications of regions in an image that require inspection by an examiner. The SWGIT group has published a document on detection of manipulation http://www.swigit.org .

A special type of detection is based on the indication of ‘resampling’ [44]–[47]. When a part of an image is pasted into another image, it is often necessary to apply rotation and resizing to make them visually fit. This resizing causes a special relationship between color values in the resized region that could be detected.

Double compression detection in JPEGS [48]–[53] is also widely researched, as well as using the Photo Response Non Uniformity (PRNU) for detection [54]

Another type of image tampering is referred to as ‘copy-paste’ forgery [[46]–[54]]. Objects or persons that are visible against a background with a specific texture, like blue air, green grass, trees, etc. are hidden by pasting a copy of a region in the image with the same texture over them. Detection of this type of tampering looks like a simple straightforward process. All regions in an image have to be compared to each other in order to find regions that are copies. However, the challenge is to limit the number of comparisons and to find a computationally efficient method. This is a requirement when a large amount of images has to be checked. A relatively large number of methods have been proposed in the literature for this task. Also a method with support vector machines (SVM) for object based manipulation by the contour in a video file is proposed, with an accuracy from 70 to 95 % claimed by the authors [55]

A related problem is the detection of illegal copies of image and video files. One technique for protection of original image and video files is the use of watermarking. A watermark is in most cases a hidden mark in the image that will get lost in most common copy processes. Although watermarking is already an old technique there is a lot of research going on [[56]–[74]]. Furthermore on authenticity a survey is published for video[75].

The number of papers published on these topics show that the problem of reliably detecting image tampering has not been solved yet. There are now a number of software packages available that offer a number of methods that can be tried on a questioned image, however interpretation of the results by an expert remains important.

Also anti forensics methods are described based on methods that are published, to prevent tampering from being detected. [76]–[83]

## 4. Camera identification of images and video

In criminal investigations of child porn production and distribution, identification of the source of a digital image has become very important, because a specific camera, (or a cell phone camera, a webcam, or a flatbed scanner) could be linked to a suspect using other types of evidence. Identification of images that might have a common source can also be helpful in these investigations. The developments that have been started in the period of the previous review have not been stopped and have lead to a number of new methods and software packages. The most used method is based on the estimation of a specific type of fixed pattern noise in an image that is caused by PRNU - *Photo Response Non Uniformity[84]* . The method is also useful in other cases such as murder and fraud to find a links between a camera and images that have been taken [85], [86]

For identification of a specific camera as the source of a specific image, the PRNU patterns have to be estimated from reference images from the camera and the noise that can be filtered out from this specific image. These patterns have to be compared and a similarity measure is used as a measure for the strength of the evidence that the camera is the source. Common practice is to compare the PRNU pattern of a specific image with the PRNU patterns from a large number of camera’s. The quality of the estimation of the PRNU pattern from an image depends heavily on the image content and this can be taken into account. However, if there are more images available from the same, unknown source, e.g. the frames in a video file, much better estimations of the PRNU pattern can be obtained by averaging techniques. However several methods are presented to improve the calculation speed as well as clustering images if the camera is not available. Also the use of GPUs is discussed within these methods ([86]–[89].

Other sources of fixed pattern noise [90]–[92] that have been investigated are based on detection of image artifacts from differences in image processing in the camera chips. If the camera does not work also switching the camera module appears to work for finding a link between the camera module and the images taken[93]

In the forensic practice of a case in which a specific camera has to be identified, a collection of similar cameras from the same brand and type are needed for validation of the results. For using PRNU as evidence, the analyst has to interpret the comparison results. The ENFSI working group for Digital Imaging has conducted two proficiency tests to find out what different experts might report to the court about camera identification. In the practice of investigation of large amounts of images, PRNU is also useful to get indications of possibly common sources. A number of studies have been found on the implementation of this application .

## 5. Video Image processing and Image Search

The ENFSI worked on a proficiency test of image processing, S-Five https://s-five.eu/ . The project was for Standardization of Forensic Image and Video Enhancement, and resulted in a best practice manual for processing these. Also a test set with a collaborative exercise and the use of different software products and algorithms have shown that different results are obtained in image enhancement depending on the blur function ([94]–[96].

Several approaches have been published [97] , where also attention is given on logging and archiving processes.

A methodology to event reconstruction has been published by Quentin [98]. They proposed a systematic approach to using trace images in the framework of an investigation. The method is cyclic and iterative. In other publications [99], [100], Quentin provided solutions for image classification, by adding ssytematic description of image content to metadata as well as timeline chronological reconstruction. For 3D reconstruction using image from fixed and mobile cameras, photogrammetry is proposed.

Several software products have been developed for searching in large amounts of images and video and using similarity detection of images. The software appears to be useful in practice for searching large amounts of image databases, and big multimedia analysis [101]–[103]. The development of deep learning methods.

The development and implementation of deep learning methods

The LASIE project of FP7 funded by the European Commission has published an overview of methods for image search in relation to big data http://www.lasie-project.eu/wp-content/uploads/2015/05/LASIE_D6.1.pdf

Forensic video analysis is also assisted by algorithms, which is published for example by Geronimo [104] on retrieving certain actions, such as walking or fighting and the search for specific persons. Also relevance feedback is important for semi supervised search [105]

The recent deployment of very large scale camera networks with fixed and moving surveillance cameras has led to a novel field of object tracking. Hsu [106]proposes vehicle matching and tracking cross camera by affine and scale invariant feature transform.

### 5.1 Video games forensics

Another field which is approaching is video games forensics[107]. An investigator might not expect video games and their data files are used as a crime or hide data.

### 5.2 Video carving

Within the field of video carving several approaches have been made. The software defraser which is partly open source as published by the Netherlands Forensic Institute at https://sourceforge.net/projects/defraser/ . Since video file formats define only a limited number of mandatory features, they leave room for interpretation. Differences in file structures appear to be available [108].

## 6. References


[1] M. . Houck, “American Academy of Forensic Sciences (AAFS),” in *Encyclopedia of Forensic Sciences*, Elsevier, 2013, pp. 196–196.

[2] M. . Houck, “European Network of Forensic Science Institutes (ENFSI),” in *Encyclopedia of Forensic Sciences*, Elsevier, 2013, pp. 199–199.

[3] Z. Geradts, “ENFSI Forensic IT Working group,” *Digital Investigation*, vol. 8, Nov. 2011.

[4] P. Grother, “Face Recognition Vendor Test (FRVT), NIST Interagency Report 8009.” 26-May-2014.

[5] P. J. Phillips, J. R. Beveridge, D. S. Bolme, B. A. Draper, G. H. Given, Y. M. Lui, S. Cheng, M. N. Teli, and H. Zhang, “On the existence of face quality measures,” in *2013 IEEE Sixth International Conference on Biometrics: Theory, Applications and Systems (BTAS)*, 2013, pp. 1–8.

[6] A. Dutta, “Predicting performance of a face recognition system based on image quality.” University of Twente, Enschede, The Netherlands, 24-Apr-2015.

[7] L. Best-Rowden, H. Han, C. Otto, B. F. Klare, and A. K. Jain, “Unconstrained Face Recognition: Identifying a Person of Interest From a Media Collection,” *IEEE Transactions on Information Forensics and Security*, vol. 9, Dec. 2014.

[8] F. JuefeiXu, D. K. Pal, and K. Singh, “A preliminary investigation on the sensitivity of COTS face recognition systems to forensic analyststyle face processing for occlusions,” *Conference on Computer Vision and Pattern Recognition Workshops IEEE Computer Society Conference on Computer Vision and Pattern Recognition. Workshops*. 01-Jun-2015.

[9] J. C. Klontz and A. K. Jain, “A Case Study of Automated Face Recognition: The Boston Marathon Bombings Suspects,” *Computer*, vol. 46, Nov. 2013.

[10] S. Park, H. Lee, J.-H. Yoo, G. Kim, and S. Kim, “Partially Occluded Facial Image Retrieval Based on a Similarity Measurement,” *Mathematical Problems in Engineering*, vol. 2015, 2015.

[11] Y. Peng, L. . Spreeuwers, and R. N. . Veldhuis, “Likelihood ratio based mixed resolution facial comparison,” in *3rd International Workshop on Biometrics and Forensics (IWBF 2015)*, 2015, pp. 1–5.

[12] M. Cummaudo, M. Guerzoni, L. Marasciuolo, D. Gibelli, A. Cigada, Z. Obertovà, M. Ratnayake, P. Poppa, P. Gabriel, S. Ritz-Timme, and C. Cattaneo, “Pitfalls at the root of facial assessment on photographs: a quantitative study of accuracy in positioning facial landmarks.,” *International journal of legal medicine*, vol. 127, pp. 699–706, May 2013.

[13] P. Santemiz, O. Aran, M. Saraclar, and L. Akarun, “Automatic sign segmentation from continuous signing via multiple sequence alignment,” in *2009 IEEE 12th International Conference on Computer Vision Workshops, ICCV Workshops*, 2009, pp. 2001–2008.

[14] Y. Lee, P. J. Phillips, J. J. Filliben, and J. R. Beveridge, “Identifying Face Quality and Factor Measures for Video.” NISTIR 8004, 2014.

[15] C. van Dam and R. Veldhuis, Eds., “Landmarkbased modelfree 3D face shape reconstruction from video sequences,” *Proceedings of the 2nd International Business and System Conference BSC 2013*. 01-Sep-2013.

[16] Y. Taigman, M. Yang, M. Ranzato, and L. Wolf, “Deepface: Closing the gap to human-level performance in face verification,” in *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, 2013, pp. 1701–1708.

[17] Y. Taigman, M. A. Ranzato, T. Aviv, and M. Park, “DeepFace: Closing the Gap to Human-Level Performance in Face Verification,” *Conference on Computer Vision and Pattern Recognition (CVPR)*. Columbus, pp. 1–8, 2014.

[18] F. Schroff, D. Kalenichenko, and J. Philbin, “Facenet: A unified embedding for face recognition and clustering,” *arXiv preprint arXiv: 1503.03832*, 2015.

[19] E. Zhou and Z. Cao, Eds., “Naive-Deep Face Recognition: Touching the Limit of LFW Benchmark or Not?,” *arXiv: 1501.04690*. 2015.

[20] P. J. Phillips and A. J. O’Toole, “Comparison of Human and Computer Performance Across Face Recognition Experiments,” *Image and Vision Computing*, Dec. 2013.

[21] X. Mallett and M. P. Evison, “Forensic facial comparison: issues of admissibility in the development of novel analytical technique.,” *Journal of forensic sciences*, vol. 58, pp. 859–865, Jul. 2013.

[22] A. M. Megreya, A. Sandford, and A. M. Burton, “Matching Face Images Taken on the Same Day or Months Apart: the Limitations of Photo ID: Matching face images,” *Applied Cognitive Psychology*, p. n/a–n/a, Oct. 2013.

[23] D. White, J. D. Dunn, A. C. Schmid, and R. I. Kemp, “Error Rates in Users of Automatic Face Recognition Software.,” *PloS one*, vol. 10, Oct. 2015.

[24] P. Tome, J. Fierrez, R. Vera-Rodriguez, and M. Nixon, “Soft Biometrics and Their Application in Person Recognition at a Distance,” *IEEE Transactions on Information Forensics and Security*, pp. 1–1, 2014.

[25] D. White, R. I. Kemp, R. Jenkins, M. Matheson, and A. M. Burton, “Passport officers’ errors in face matching.,” *PloS one*, vol. 9, Aug. 2014.

[26] D. White, P. J. Phillips, C. A. Hahn, M. Hill, and A. J. O'Toole, "Perceptual expertise in forensic facial image comparison.," *Proceedings. Biological sciences / The Royal Society*, vol. 282, Sep. 2015.

[27] B. F. Klare, K. Bonnen, and A. K. Jain with Hu Han, "Matching Composite Sketches to Face Photos: A Component-Based Approach," *IEEE Transactions on Information Forensics and Security*, vol. 8, Jan. 2013.

[28] S. J. Klum, H. Han, B. F. Klare, and A. K. Jain, "The FaceSketchID System: Matching Facial Composites to Mugshots," *IEEE Transactions on Information Forensics and Security*, vol. 9, Dec. 2014.

[29] A. Abaza, A. Ross, C. Hebert, M. A. F. Harrison, and M. S. Nixon, "A survey on ear biometrics," *ACM Computing Surveys*, vol. 45, Feb. 2013.

[30] A. Kumar and C. Wu, "Automated human identification using ear imaging," *Pattern Recognition*, vol. 45, Mar. 2012.

[31] A. Pflug and C. Busch, "Ear biometrics: a survey of detection, feature extraction and recognition methods," *IET Biometrics*, vol. 1, 2012.

[32] A. Pflug, J. Wagner, C. Rathgeb, and C. Busch, "Impact of severe signal degradation on ear recognition performance," in *2014 37th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, 2014, pp. 1342–1347.

[33] J. Lei, X. You, and M. Abdel-Mottaleb, "Automatic Ear Landmark Localization, Segmentation, and Pose Classification in Range Images," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, pp. 1–12, 2015.

[34] T. Lucas and M. Henneberg, "Comparing the face to the body, which is better for identification?," *International journal of legal medicine*, vol. 130, pp. 533–540, Mar. 2016.

[35] T. Scoleri, T. Lucas, and M. Henneberg, "Effects of garments on photoanthropometry of body parts: application to stature estimation.," *Forensic science international*, vol. 237, pp. 148.e1–148.e12, Apr. 2014.

[36] M. R. Islam, F. K.-S. Chan, and A. W.-K. Kong, "A Preliminary Study of Lower Leg Geometry as a Soft Biometric Trait for Forensic Investigation," in *2014 22nd International Conference on Pattern Recognition*, 2014, pp. 427–431.

[37] A. Rice, P. J. Phillips, V. Natu, X. An, and A. J. O'Toole, "Unaware person recognition from the body when face identification fails.," *Psychological science*, vol. 24, pp. 2235–2243, Nov. 2013.

[38] I. Bouchrika, J. N. Carter, and M. S. Nixon, "Towards automated visual surveillance using gait for identity recognition and tracking across multiple non-intersecting cameras," *Multimedia Tools and Applications*, Nov. 2014.

[39] S. X. M. Yang, P. K. Larsen, T. Alkjær, B. Juul-Kristensen, E. B. Simonsen, and N. Lynnerup, “Height estimations based on eye measurements throughout a gait cycle.,” *Forensic science international*, vol. 236, pp. 170–174, Mar. 2014.

[40] P. Tome, R. Vera-Rodriguez, J. Fierrez, and J. Ortega-Garcia, “Facial soft biometric features for forensic face recognition.,” *Forensic science international*, vol. 257, pp. 271–284, Dec. 2015.

[41] D. A. Reid and M. S. Nixon, “Human identification using facial comparative descriptions,” in *2013 International Conference on Biometrics (ICB)*, 2013, pp. 1–7.

[42] J. Galbally, S. Marcel, and J. Fierrez, “Image Quality Assessment for Fake Biometric Detection: Application to Iris, Fingerprint, and Face Recognition.,” *IEEE transactions on image processing: a publication of the IEEE Signal Processing Society*, vol. 23, pp. 710–724, Feb. 2014.

[43] N. Erdogmus and S. Marcel, “Spoofing Face Recognition With 3D Masks,” *IEEE Transactions on Information Forensics and Security*, vol. 9, Jul. 2014.

[44] J.-I. Kim and T. Kim, “Comparison of Computer Vision and Photogrammetric Approaches for Epipolar Resampling of Image Sequence.,” *Sensors (Basel, Switzerland)*, vol. 16, Mar. 2016.

[45] X. Kang, G. Lin, E. Zhang, and Y. Chen, “On the reliability of forensic schemes using resampling for image copy-move forgery,” *International Journal of Electronic Security and Digital Forensics*, vol. 5, 2013.

[46] P. Menzel, “Constrained indicator data resampling — A parameter constrained irregular resampling method for scattered point data,” *GEOPHYSICS*, vol. 81, Mar. 2016.

[47] J. M. Watson, “Resampling withTinkerPlots: Resampling withTinkerPlots,” *Teaching Statistics*, vol. 35, Mar. 2013.

[48] M. Qiao, A. H. Sung, and Q. Liu, “Improved detection of MP3 double compression using content-independent features,” in *2013 IEEE International Conference on Signal Processing, Communication and Computing (ICSPCC 2013)*, 2013, pp. 1–4.

[49] X. Jiang, W. Wang, T. Sun, Y. Q. Shi, and S. Wang, “Detection of Double Compression in MPEG-4 Videos Based on Markov Statistics,” *IEEE Signal Processing Letters*, vol. 20, May 2013.

[50] W. Wang, X. Jiang, and T. Sun, “Exposing Double MPEG Compression Based on First Digit Features: Exposing Double MPEG Compression Based on First Digit Features,” *Journal of Electronics & Information Technology*, vol. 34, Jul. 2013.

[51] Q. Liu, P. A. Cooper, L. Chen, H. Cho, Z. Chen, M. Qiao, Y. Su, M. Wei, and A. H. Sung, “Detection of JPEG double compression and identification of smartphone image source and post-capture manipulation,” *Applied Intelligence*, vol. 39, Mar. 2013.

[52] J. XU, Y. SU, and Q. LIU, “DETECTION OF DOUBLE MPEG-2 COMPRESSION BASED ON DISTRIBUTIONS OF DCT COEFFICIENTS,” *International Journal of Pattern Recognition and Artificial Intelligence*, vol. 27, Feb. 2013.

[53] P. He, X. Jiang, T. Sun, and S. Wang, “Double compression detection based on local motion vector field analysis in static-background videos,” *Journal of Visual Communication and Image Representation*, vol. 35, Feb. 2016.

[54] G. Chierchia, G. Poggi, C. Sansone, and L. Verdoliva, “PRNU-based forgery detection with regularity constraints and global optimization,” in *2013 IEEE 15th International Workshop on Multimedia Signal Processing (MMSP)*, 2013, pp. 236–241.

[55] C. Richao, Y. Gaobo, and Z. Ningbo, “Detection of object-based manipulation by the statistical features of object contour.,” *Forensic science international*, vol. 236, pp. 164–169, Mar. 2014.

[56] S. Chikane, S. K, and R. Talwar, “An Improved Image Watermarking based on LPM and AQIM,” *International Journal of Computer Applications*, vol. 134, Jan. 2016.

[57] S. Kaur and R. Talwar, “Attack Resistant Digital Image Watermarking using Complex Wavelet Transform,” *International Journal of Computer Applications*, vol. 134, Jan. 2016.

[58] M. Mardanpour and M. A. Z. Chahooki, “Robust transparent image watermarking with Shearlet transform and bidiagonal singular value decomposition,” *AEU - International Journal of Electronics and Communications*, Mar. 2016.

[59] S. Khandare and U. Shrawankar, “Image Bit Depth Plane Digital Watermarking for Secured Classified Image Data Transmission,” *Procedia Computer Science*, vol. 78, 2016.

[60] X. CHENG, Y. HOU, J. CHENG, and X. PU, “Image zero-watermarking algorithm against geometric attacks based on Tchebichef moments: Image zero-watermarking algorithm against geometric attacks based on Tchebichef moments,” *Journal of Computer Applications*, vol. 33, Sep. 2013.

[61] S. Ranjbar, F. Zargari, and M. Ghanbari, “A highly robust two-stage Contourlet-based digital image watermarking method,” *Signal Processing: Image Communication*, Jul. 2013.

[62] B. Sridhar and C. Arun, “A wavelet based image watermarking technique using image sharing method,” in *Information Communication and Embedded Systems (ICICES), 2013 International Conference on*, 2013, pp. 629–633.

[63] A. Mehto and N. Mehra, “Adaptive Lossless Medical Image Watermarking Algorithm Based on DCT & DWT,” *Procedia Computer Science*, vol. 78, 2016.

[64] M. Botta, D. Cavagnino, and V. Pomponiu, “A modular framework for color image watermarking,” *Signal Processing*, vol. 119, Feb. 2016.

[65] R. Jin and J. Kim, “A Robust Watermarking Scheme for City Image,” *International Journal of Security and Its Applications*, vol. 10, Jan. 2016.

[66] A. J. Zargar and A. K. Singh, “Robust and imperceptible image watermarking in DWT-BTC domain,” *International Journal of Electronic Security and Digital Forensics*, vol. 8, 2016.

[67] C. Agarwal, A. Mishra, and A. Sharma, “Gray-scale image watermarking using GA-BPN hybrid network,” *Journal of Visual Communication and Image Representation*, vol. 24, Oct. 2013.

[68] M. Zareian and H. R. Tohidypour, “Robust quantisation index modulation-based approach for image watermarking,” *IET Image Processing*, vol. 7, Jul. 2013.

[69] H. B. Golestani and M. Ghanbari, “Minimisation of image watermarking side effects through subjective optimisation,” *IET Image Processing*, vol. 7, Nov. 2013.

[70] M. LIU, Z. CHEN, and X. DENG, “Image tamper detection scheme based on chaotic system and fragile watermarking: Image tamper detection scheme based on chaotic system and fragile watermarking,” *Journal of Computer Applications*, vol. 33, Oct. 2013.

[71] S. CHEN and Y. FENG, “Image watermarking algorithm based on quaternion and singular value decomposition: Image watermarking algorithm based on quaternion and singular value decomposition,” *Journal of Computer Applications*, vol. 33, Oct. 2013.

[72] Ε. Τσουγένης, “Intelligent image watermarking methods by the use of moment functions.” Δημοκρίτειο Πανεπιστήμιο Θράκης (ΔΠΘ), Σχολή Πολυτεχνική, Τμήμα Μηχανικών Παραγωγής και Διοίκησης, 01-Sep-2013.

[73] J. Chourasia, “Identification and authentication using visual cryptography based fingerprint watermarking over natural image,” pp. 1–6, 2013.

[74] Y. Guo, O. C. Au, J. Zhou, K. Tang, and X. Fan, “Halftone image watermarking via optimization,” *Signal Processing: Image Communication*, vol. 41, Feb. 2016.

[75] S. U. S, R. R. S, and M. R. Mathews, “A Survey on Digital Video Authentication Methods,” *International Journal of Computer Trends and Technology*, vol. 22, Apr. 2015.

[76] S. M.S and V. D, “Image Compression Using Anti-Forensics Method,” International Journal of Computer Science, Engineering and Applications, vol. 3, Feb. 2013.

[77] W. Fan, K. Wang, F. Cayre, and Z. Xiong, “JPEG anti-forensics using non-parametric DCT quantization noise estimation and natural image statistics,” in *Proceedings of the first ACM workshop on Information hiding and multimedia security - IH&MMSec ’13*, 2013, pp. 117–117.

[78] A. Piva, “An Overview on Image Forensics,” *ISRN Signal Processing*, vol. 2013, 2013.

[79] G. Valenzise, M. Tagliasacchi, and S. Tubaro, “Revealing the Traces of JPEG Compression Anti-Forensics,” *IEEE Transactions on Information Forensics and Security*, vol. 8, Feb. 2013.

[80] R. Böhme and M. Kirchner, “Counter-Forensics: Attacking Image Forensics,” in *Digital Image Forensics*, Springer New York, 2013, pp. 327–366.

[81] M. Raggo and C. Hosmer, “Forensics and Anti-Forensics,” in *Data Hiding*, Elsevier, 2013, pp. 193–211.

[82] H. Zeng, X. Kang, and A. Peng, “A Multi-purpose Countermeasure against Image Anti-forensics using Autoregressive Model,” *Neurocomputing*, Jan. 2016.

[83] A. Thangarajah, “Attack Graphs with Anti-Forensics Tool - in Forensics Examination,” in *International Conference on Computer Research and Development, 5th (ICCRD 2013)*, ASME Press, 2013.

[84] L.-H. Chan, N.-F. Law, and W.-C. Siu, “A confidence map and pixel-based weighted correlation for PRNU-based camera identification,” *Digital Investigation*, vol. 10, Oct. 2013.

[85] D. Rublev, V. Fedorov, and O. Makarevich, “Digital camera identification system,” in Proceedings of the 6th International Conference on Security of Information and Networks - SIN ’13, 2013, pp. 297–300.

[86] M. Goljan and J. Fridrich, “Sensor fingerprint digests for fast camera identification from geometrically distorted images,” 2013, p. 86650B–86650B.

[87] F. Gisolf, P. Barens, E. Snel, A. Malgoezar, M. Vos, A. Mieremet, and Z. Geradts, “Common source identification of images in large databases.,” *Forensic science international*, vol. 244, pp. 222–230, Nov. 2014.

[88] A. R. Soobhany, K. P. Lam, P. Fletcher, and D. Collins, “Source identification of camera phones using SVD,” in *2013 IEEE International Conference on Image Processing*, 2013, pp. 4497–4501.

[89] A. J. Cooper, “Improved photo response non-uniformity (PRNU) based source camera identification.,” *Forensic science international*, vol. 226, pp. 132–141, Mar. 2013.

[90] Na Zhang and Haiyong Zheng, “The techniques of fixed pattern noise reduction for high speed digital CMOS image sensor,” in *2013 International Conference on Optoelectronics and Microelectronics (ICOM)*, 2013, pp. 211–214.

[91] Y. Tang and S. N. Srihari, “Likelihood ratio estimation in forensic identification using similarity and rarity,” *Pattern Recognition*, 2013.

[92] D. Das and S. Collins, “Fixed-Pattern-Noise Correction for an Integrating Wide-Dynamic-Range CMOS Image Sensor,” *IEEE Transactions on Electron Devices*, vol. 60, Jan. 2013.

[93] F. Gisolf, Z. Geradts, D. Verhoeven, and C. Klaver, “The effects of switching the camera module from BlackBerry Curve 9360 devices,” *Digital Investigation*, vol. 10, Jun. 2013.

[94] V. Conotter, P. Comesana, and F. Perez-Gonzalez, “Forensic analysis of full-frame linearly filtered JPEG images,” in *2013 IEEE International Conference on Image Processing*, 2013, pp. 4517–4521.

[95] J. Fan, T. Chen, and A. C. Kot, “EXIF-white balance recognition for image forensic analysis,” *Multidimensional Systems and Signal Processing*, Jan. 2016.

[96] Z. Geradts, “Image Processing and Analysis,” in *Wiley Encyclopedia of Forensic Science*, John Wiley & Sons, Ltd, 2013.

[97] J. Kamenicky, M. Bartos, J. Flusser, B. Mahdian, J. Kotera, A. Novozamsky, S. Saic, F. Sroubek, M. Sorel, A. Zita, B. Zitova, Z. Sima, P. Svarc, and J. Horinek, “SWNAME: Forensic analysis and restoration of image and video data,” *Forensic Science International*, Apr. 2016.

[98] Q. Milliet, O. Delémont, E. Sapin, and P. Margot, “A methodology to event reconstruction from trace images.,” *Science & justice : journal of the Forensic Science Society*, vol. 55, pp. 107–117, Mar. 2015.

[99] Q. Milliet, O. Delémont, and P. Margot, “A forensic science perspective on the role of images in crime investigation and reconstruction.,” *Science & justice : journal of the Forensic Science Society*, vol. 54, pp. 470–480, Dec. 2014.

[100] Q. Milliet, M. Jendly, and O. Delémont, “An innovative and shared methodology for event reconstruction using images in forensic science.,” *Forensic science international*, vol. 254, pp. 172–179, Sep. 2015.

[101] Z.-J. Zha, L. Yang, and M. Wang, Eds., “Visual Query Suggestion for Internet Image Search,” in *Internet Multimedia Search and Mining*, BENTHAM SCIENCE PUBLISHERS, 2013, pp. 415–433.

[102] M. M. Fouad, “Content-based Search for Image Retrieval,” International Journal of Image, Graphics and Signal Processing, vol. 5, Sep. 2013.

[103] M. J. Metternich and M. Worring, “Track based relevance feedback for tracing persons in surveillance videos,” *Computer Vision and Image Understanding*, vol. 117, Mar. 2013.

[104] Y. J. Ren, L. O’Gorman, L. J. Wu, F. Chang, T. L. Wood, and J. R. Zhang, “Authenticating Lossy Surveillance Video,” *IEEE Transactions on Information Forensics and Security*, vol. 8, Oct. 2013.

[105] D. Coppi, S. Calderara, and R. Cucchiara, “Active query process for digital video surveillance forensic applications,” *Signal, Image and Video Processing*, vol. 9, Jun. 2013.

[106] H.-Y. Mark Liao with Chao-Yung Hsu and Li-Wei Kang, “Cross-camera vehicle tracking via affine invariant object matching for video forensics applications,” in *2013 IEEE International Conference on Multimedia and Expo (ICME)*, 2013, pp. 1–6.

[107] M. Ebrahimi, Lei Chen, “Emerging cyberworld attack vectors: Modification, customization, secretive communications, and digital forensics in PC video games,” in *2014*

*International Conference on Computing, Networking and Communications (ICNC)*, 2014, pp. 939–944.

[108] T. Gloe, A. Fischer, and M. Kirchner, “Forensic analysis of video file formats,” *Digital Investigation*, vol. 11, May 2014.