FIDIS

Future of Identity in the Information Society

Title:	"D6.8b: Identification of images"
Editors:	Zeno Geradts (NFI), Thomas Gloe (TUD)
Reviewers:	Mark Gasson (University of Reading), Martin Meints (ICPP)
Identifier:	D6.8b
Type:	Deliverable
Version:	1.0
Date:	Wednesday, 08 April 2009
Status:	Final
Class:	Public
File:	fidis-wp6-del6.8b_identification_of_images.doc

Summary

In recent years, digital imaging systems have permeated our everyday lives. CCTV systems, mobile phones, (video) cameras, scanners and webcams can be used to record scenes that may be of forensic use later on. Questions may arise regarding the identification of persons, or alternatively, the authenticity or origin of these images or videos, especially when these images or videos are spread over the Internet. Therefore, objective methods that may answer some of these questions are investigated.

Here we investigate the feasibility of identifying the source camera used to record a video based on videos originating from *YouTube*. Also, classification of camera devices is shown to be possible to a certain extent with the help of a limited number of features and a Support Vector Machine (SVM). These methods may however fail if the images or videos were tampered with. Methods to detect these manipulations are presented, as well as an image recognition algorithm that can be used to detect known illicit images that were subject to unknown manipulations. The performance of current facial comparison techniques, by human and machine, and, aspects regarding the legal collection of electronic evidence from the Internet are also evaluated.

The FIDIS NoE receives research funding from the Community's Sixth Framework Program

Copyright Notice:

Members of the FIDIS consortium

1. Goethe University Frankfurt	Germany
2. Joint Research Centre (JRC)	Spain
3. Vrije Universiteit Brussel	Belgium
4. Unabhängiges Landeszentrum für Datenschutz (ICPP)	Germany
5. Institut Europeen D'Administration Des Affaires (INSEAD)	France
6. University of Reading	United Kingdom
7. Katholieke Universiteit Leuven	Belgium
8. Tilburg University[1]	Netherlands
9. Karlstads University	Sweden
10. Technische Universität Berlin	Germany
11. Technische Universität Dresden	Germany
12. Albert-Ludwig-University Freiburg	Germany
13. Masarykova universita v Brne (MU)	Czech Republic
14. VaF Bratislava	Slovakia
15. London School of Economics and Political Science (LSE)	United Kingdom
16. Budapest University of Technology and Economics (ISTRI)	Hungary
17. IBM Research GmbH	Switzerland
18. Centre Technique de la Gendarmerie Nationale (CTGN)	France
19. Netherlands Forensic Institute (NFI)[2]	Netherlands
20. Virtual Identity and Privacy Research Center (VIP)[3]	Switzerland
21. Europäisches Microsoft Innovations Center GmbH (EMIC)	Germany
22. Institute of Communication and Computer Systems (ICCS)	Greece
23. AXSionics AG	Switzerland
24. SIRRIX AG Security Technologies	Germany

1 Legal name: Stichting Katholieke Universiteit Brabant

2 Legal name: Ministerie Van Justitie

3 Legal name: Berner Fachhochschule

Foreword

FIDIS partners from various disciplines have contributed as authors to this document. The following list names the main contributors for the chapters of this document:

Chapter	*Contributor(s)*
2 Introduction	Joint contribution
3 Digital Image Forensics	Zeno Geradts (NFI), Wiger van Houten (NFI), Maarten van der Mark (NFI) Thomas Gloe (TUD)
4 Robust image recognition algorithm	Yves Brouze (University of Lausanne), David-Olivier Jaquet-Chiffelle (VIP)
5 Facial Comparison by Man and Machine	Arnout Ruifrok (NFI), Vicky Vassiliki (NTUA)
6 Ensuring the evidentiary value of images in criminal proceedings	Fanny Coudert, Evi Werkers (ICRI)
7 Conclusion	Joint contribution

Table of Contents

1 Executive Summary

This FIDIS D6.8b Deliverable "Identification of Images" gives an overview of current methods for the forensic analysis of digital images and discusses corresponding legal aspects. This deliverable is based on a workshop (FIDIS D6.8a) held in Dresden in 2008.

Nowadays digital imaging technologies enable acquisition and processing of digital images at very high quality and low cost. Often, digital images are used as records, for example, in the media, in scientific publications, in court, in surveillance systems or in correspondence with insurance companies. Using the acquired images, not only within these scenarios, can raise questions about the originality and authenticity of the image content. In some cases it is important to assure that an image has not undergone malicious image processing operations, for example by adding or removing individual depicted persons in a scene. Furthermore, it is known that digital images contain important information that can be used for forensic investigation into their acquisition devices and, hence, may provide indications on possible suspects or perpetrators in civil and criminal cases. Both aspects, image originality and image origin, are subsumed in the young area of research of *digital image forensics*. This deliverable discusses image source identification for all major classes of acquisition devices, including video cameras, flatbed scanners and digital cameras. The state of the literature, reviewed in this deliverable, suggests that current image forensic techniques are useful and valuable for inspecting digital images.

In addition, a robust image hashing method is described which can be used to identify different versions of the same image in very large samples of images, such as police databases. Another application of such hashes is to identify derivatives of copyrighted material on confiscated storage devices.

Facial comparison between a digital image and a database of known individuals is also an important approach to identify suspects, for example in videos of surveillance cameras or occasional snapshots of witnesses. In contrast to the commonly accepted view, experimental results summarised in this deliverable provide a warning example that the match rate of trained human investigators is not as good as expected. In fact, the performance of current state-of-the-art facial comparison algorithms using frontal images turns out to be comparable or even better than the performance of human experts.

To give a comprehensive view on automatic analysis of digital images for forensic purposes, legal aspects considering the evidentiary value of images in criminal proceedings are discussed. The scope also includes privacy and copyright issues, for example when images are to be taken from private or restricted accounts on the Internet.

2 Introduction

Through the general and wide availability of affordable digital imaging technologies their analogue counterparts are continuously replaced or introduced into the realms of everyday life. Images and videos originating from a wide range of devices can be acquired and processed in high quality and in short time with low cost. Considering the everyday use of digital images, for example, in the media, in scientific publications, in court, in surveillance systems or in correspondence with insurance companies, the question whether a digital image depicts an original unaltered scene is of high importance. Questions pertaining to the content (e.g. facial recognition), authenticity (e.g. image manipulation) as well as to the origin of an image or video (e.g. source identification) can and should be asked when there is any reason for doubt. Notably the origin or content of an image or video may easily be obfuscated when these media are uploaded, shared or manipulated on social networking sites or filesharing programs. It may be hard to trace back copies of the original file to its source, or find the original image when a number of manipulated images are available. In addition to the analysis of image and video authenticity, methods for scene analysis and especially for recognition and comparison of faces are important for the reconstruction of crime scenes.

The need for establishing reliable methods for detecting manipulations, facial recognition, and verifying the source of a digital video or image becomes apparent when these supposed digital representations of the reality are considered in a legal forensic context.

In this deliverable we intend to present some of the possibilities and limitations in answering these questions. We will not only present available techniques and methods, but as we are operating in a forensic/legal context, we will also tackle the issue of the conditions we should comply with in order to ensure the legality of the outcome.

In Chapter 3 we will address the issue of source *identification*, i.e. tracing the origin of an image or video back to the device that produced the image or video. The method used for identification to this end is largely the same as the method used for identifying the scanner that has been used to digitise an analogue image, namely the sensor noise. The latter is presented in Section 3.2, while in Section 3.3 techniques are presented for the *classification* of image sources. In Section 3.4 methods are presented to detect image manipulations. In Chapter 4 the development of a robust image recognition algorithm is discussed that is able to detect known (illicit) images even after certain manipulations have occurred such as resizing or rotation.

Analogue and digital videos from security cameras often have a limited resolution and are recorded in difficult circumstances where e.g. insufficient lighting prevents the reliable recognition of persons. Chapter 5 presents the current performance of facial comparisons done by humans and by automated systems.

Finally, Chapter 6 deals with the legal aspects when images or videos are collected from the Internet, and the collection of electronic evidence in general. In order to ensure the legality of the outcome a number of conditions should be met for the collected evidence to be admissible, e.g. the right to privacy.

3 Digital Image Forensics

This section presents methods for *image source identification* and *detection of image manipulations*.

Generally, *image source identification* tries to detect the existence of specific characteristics introduced by an image acquisition device. Figure 1 shows the source of typical device-dependent characteristics in a simplified model of a digital camera. Starting with the lens, characteristics due to aberrations like chromatic aberration [1,2] are introduced which become visible as coloured edges. Further characteristics are introduced by the sensor, namely sensor defects [3] and sensor noise [4,5]. Since most sensors cannot differentiate between different colours, most digital cameras and digital video cameras employ colour interpolation techniques, which leave characteristic dependencies between adjacent pixels [6] as another characteristic for forensic methods. Furthermore, differences in the applied compression can be evaluated [7]. Aside from the analysis of specific characteristics, it is also possible to consider the whole image acquisition process as a black box and analyse the camera response function [8] or macroscopic features of acquired images [9].

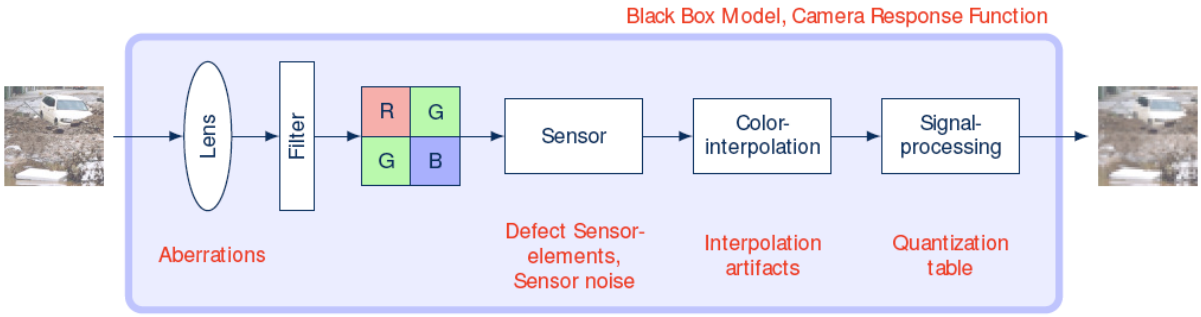

Figure 1: Optical path and subsequent signal processing pipeline in the simplified model of a digital camera. Origins of device-dependent characteristics are indicated in red.

Based on these device-dependent characteristics the task of determining the source of an image can be classified into the following subtasks: detecting the device type used (digital camera, flatbed scanner, etc.), detecting the used device model, and detecting the used device itself.

The detection of *image manipulation* tries to either unveil characteristic traces of an image processing operation or to verify specific characteristics originating in the image acquisition device (as above). In the following sections methods to detect the device used as well as the device model are exemplarily discussed. Furthermore, selected techniques for tamper detection are presented.

3.1 Video Camera device identification applied to videos obtained from YouTube

Due to the integration of image sensors in high volume electronics such as mobile phones, smartphones, notebooks and media players, (digital) photographs and videos may be taken at any time or in any circumstance for different purposes. These digital media may be

distributed over the Internet in a short time, obfuscating the source. These videos or photographs may depict illegal acts such as assault or child abuse, and the need for reliably establishing the origin becomes apparent when these videos or images are used in a forensic context.

Modern digital (photo) cameras may write EXIF (EXchangeable Image File Format) or XMP (eXtensible Metadata Platform) metadata to the image containing tags such as date and time, camera settings, or the serial number of the camera that produced the image. However, this data can be easily removed or manipulated. Therefore, even when this information is available, it is important to have alternatives available should there be any doubt concerning the image origin. Preferably, these alternatives should rely on unique identifiers. Traditionally, defective pixels could be used for this purpose, in which the positions of the defective pixels act as a fingerprint when these defects are present in the sensor [3]. These defects are present in all images obtained by a certain image sensor, and hence could be used for device identification. However, as manufacturing standards continue to increase, the presence of defects is decreasing. Furthermore, defective pixels may be corrected after image acquisition in the integrated post-processing stage in the camera, making this method largely superfluous. In the following years this method has been refined: instead of defective pixels we now look at the individual pixels that may report slightly lower or higher values than their neighbours, even when these pixels are illuminated uniformly.

The technique used to perform device identification is by extracting the seemingly invisible sensor pattern noise from images left behind by the image sensor. These patterns act as a 'fingerprint' (a device signature) and the origins of this 'noise' suggest that each sensor has its own unique pattern [4,10]. Just like in real fingerprint identification (dactyloscopy), a fingerprint from unknown origin is compared to a database of fingerprints with known origin. Likewise, the sensor pattern noise that is extracted from a questioned image can be compared with the reference patterns from a database of cameras. When two patterns show a high degree of similarity, it is an indication that both patterns have the same origin. Hence, it may be advantageous in the case of videos depicting child pornography to build a database of patterns from these videos. This may aid in establishing connections between producers of these videos.

The origin of these 'fingerprints' suggest that these patterns are unique, as they result from the non-uniform response of the pixels under a certain (constant) applied signal, due to construction and device imperfection. Specifically, when the illumination incident on a number of pixels is exactly the same for all pixels, the output signals from these pixels will be slightly different, creating a pattern with some pixels outputting systematically lower (or higher) signals. This differing sensitivity of individual pixels to the same amount of light is called the *Photo Response Non-Uniformity* (PRNU), and is the characteristic that is used for establishing the image or video origin. The PRNU is a multiplicative signal, which means the apparent non-uniformity increases (linearly) with the applied signal. In practice this means that the PRNU is more visible in bright segments of an image, and less in segments with low intensities. To a certain extent, this pattern is present in all images acquired by a certain sensor (CCD or CMOS active pixel sensors), and cannot easily be removed. These CCD and

CMOS image sensors are present in a wide range of electronic devices: mobile phones, webcams, photo- and video cameras but also in image scanners[4].

Identifying the digital source camera based on the images it produces was addressed by [4,10-14]. Different filters are available for extracting these PRNU patterns from digital images, differing in complexity and applicability. These filters work very well when they are applied to digital images, and even when they are applied to digital video. As video cameras also use CCD or CMOS chips, as in digital cameras, this is not surprising. On the other hand, video resolutions are in general much lower compared to digital cameras. Also, video files are in general heavily compressed, attenuating the sensor noise. In [14] digital camcorders are identified by using the PRNU, with videos encoded by various encoders and recorded in various resolutions. We intend to use the filter as presented by [4], and apply it to videos downloaded from *YouTube*, a popular Internet video sharing site. The difference with [14] is that the quality of the video cameras used in this paper is generally much lower, and there is additional compression by *YouTube*.

The following sections are organised as follows. In the next section we take a short look at some of the noise sources (3.1.1) after which the algorithm is explained that is used to extract the pattern noise (3.1.2). The program in which this algorithm is utilised is shown in section 3.1.3. Finally, in Section 3.1.4 we use this algorithm to extract the pattern noise from videos that were uploaded to *YouTube* in different formats and with different quality settings.

3.1.1 Sensor noise sources

Before the actual image is recorded and transferred from the digital device, various noise sources degrade the image. Some of these noise sources are temporal, some of these are spatial and others are a combination of these. For a comprehensive overview of noise sources in CCD and CMOS digital (video) cameras, see [15] and [16], and the references therein.

Temporal noise in image sensors is mainly due the (photonic) shotnoise that is inherent to the nature of light and to a lesser extent to the (thermal) dark current shotnoise due the thermal generation of charge carriers in the silicon substrate of the image sensor. As the camera has no way of differentiating the signal charge from the spurious electrons generated, these unwanted electrons are added to the output and represent a noise source. Flicker noise (1/f noise) is also a temporal noise source, in which charges are trapped in surface states and subsequently released after some time in the charge to voltage amplifier. In CMOS active pixel sensors additional sources are present due the various transistors integrated on each pixel [17,18]. As this temporal noise is a purely statistical phenomenon, averaging multiple frames will reduce the amount of temporal noise.

Some of the variations due to dark current are somewhat systematic: the spatial pattern of these variations remains constant. Because of fabrication and material properties, this 'fixed pattern noise' (FPN) is a flatfield uncertainty due to device response when the sensor is *not* illuminated. Crystal defects, impurities and dislocations present in the silicon may contribute to the size of the fixed pattern noise, as well as the detector size, non-uniform potential wells and varying oxide thickness in the case of CCD image sensors. In CMOS image sensors additional sources are present, and can be thought of as composed of a column component (shared between all pixels in a certain column) and an individual pixel component. For

[4] Scanners may also use Contact Image Sensors (CIS) in low-powered (USB) scanners, in addition to the aforementioned sensors. Scanner identification using pattern noise was previously investigated by [4] and [5]. See also §3.2.

instance, due to a variable offset in the reset transistor used to reset the photodiode to a reference value a systematic offset in the output values is present. This gives a per-pixel variation. An example of a column component is the variation of the input bias current in the bias transistor present in each column of the APS. As FPN is added to all frames or images produced by a sensor, and is independent of the illumination, it can be easily removed by subtracting a 'dark' frame from the image. It should be noted that the amount of shotnoise will increase with a factor $\sqrt{2}$ [16].

A source somewhat similar in characteristics to FPN is PRNU, the variation in pixel response when the sensor *is* illuminated. This variation comes e.g. from non-uniform sizes of the active area where photons can be absorbed. This is a linear effect. For example, when the size of the active area is increased with a factor x, the number of photons detected will also increase with factor x. This illustrates the multiplicative characteristic of the PRNU: when the illumination increases, the effect of this source increases as well. Another possibility is the presence of non-uniform potential wells giving a varying spectral response. Therefore, the PRNU is also wavelength dependent.

The multiplicative nature of the PRNU makes it more difficult to remove this type of non-uniformity, as simply subtracting a frame does not take this illumination dependent nature into account. In principle it is possible to remove the PRNU, or even add the pattern of a different camera [19]. It is also possible to reduce the PRNU inside the camera by a form of non-uniformity correction [20].

FPN together with PRNU form the pattern noise and is always present, though in varying amount due to the varying illumination between successive frames.

There are also noise sources that do not find their origin on the image sensor but are added further down the pipeline, i.e. when the digital signal is processed. The most obvious source of this type of noise is the quantisation noise introduced when the analogue information from the sensor (the potential change detected for each pixel) is digitised in the analogue-to-digital converter. Another effect that occurs in the processing stage is the demosaicing of the signal. CCD and CMOS image sensors are essentially monochrome devices, i.e. they detect the amount of light incident on each pixel but cannot distinguish the colour of the incident light. To produce colour images a Colour Filter Array is present above the image sensor, such that only one certain colour is absorbed by each pixel. As a result each pixel only records the intensity of one colour, and in this way a mosaic is obtained. To give each pixel its three common RGB values, the colour information of neighbouring pixels are interpolated. This interpolation gives small but detectable offsets, and can be seen as a noise source (see [21] and [22]). Also, dust present on the lens may contribute to the pattern noise [23], as well as possible optical interference in the lens system.

3.1.2 Extracting the PRNU pattern

As discussed, due to various random and systematic noise sources, an image is corrupted to a certain extent during acquisition. The goal of a de-noising filter is to suppress or remove this noise, without substantially affecting the (small) image details. In general, de-noising algorithms cannot discriminate between true noise and small details. It is therefore important to select an appropriate filter that leaves the image structure intact, most notably around edges where the local variance is high. For example, simple spatial filtering such as the Gaussian smoothing filter removes the noise from an image by low-pass filtering the image data, as noise is generally a high frequency effect. However, as this filter is not able to distinguish between noise and signal features, this method will also distort (blur) the edge integrity.

The noise in digital images can be considered as a non-periodic signal with sharp discontinuities. This is the reason why Fourier-based filtering is only moderately effective: the Fourier basis functions (the sine and cosine) are able to describe periodic functions (localised in frequency), but they are not localised in time. Hence a sudden change of frequency in the image data (at some instant of time) will produce a non-localised change in the time domain, as can easily be seen in the formula for the Fourier Transformation [24]:

$$\hat{f}(\omega) = \int_{-\infty}^{+\infty} f(t) e^{-i\omega t} dt$$

This expresses the conversion of a time signal *f(t)* into a frequency signal $\hat{f}(\omega)$, the Fourier transform of *f(t)*. As we integrate from $-\infty$ to $+\infty$ the resulting Fourier Transform is invariant to where (in time) a frequency change occurred. In other words, the Fourier transform extracts the frequency components of the input signal *f(t)*, but it does not tell us *where* those components occur: we lose the time information when the signal is transformed into the frequency domain. This is the reason we cannot know the exact frequency (spectral component) at a certain instance of time. As long as the signals are stationary this is no problem, but as we want to localise each discontinuity (deviating pixel) in the signal, this is a serious drawback. Non-stationary signals (i.e. the frequency changes with time) are hence not suitable for Fourier filtering, as the frequencies are not localised.

The short time Fourier transform (STFT) or windowed Fourier transform is able to ameliorate this effect somewhat by utilising a small time-window in order to find the frequency at some interval of time. In other words, we can select a small time-window *w* and find the frequency of the signal in this window, hence localising the frequency and the time:

$$STFT\{f(t)\} = \int_{-\infty}^{+\infty} f(t) w(t-\tau) e^{-i\omega t} dt$$

The narrower the window the more precise we know at which time the signal changes. The price of selecting a narrow window, however, is that we sacrifice the precision of the frequency estimation. On the other hand, in large windows the frequency can be estimated well, but we sacrifice the time resolution. Ultimately, the signal is still not fully localised in the time-frequency domain, which is essentially Heisenberg's uncertainty relation.

Concluding, in the Fourier Transform we know the exact frequencies that exist in the signal, but not at which time. By reducing the window size we gain the knowledge in which time interval a certain spectral component occurs, but simultaneously sacrifice the frequency resolution. The best we can do is finding a frequency band in a certain time interval.

To solve these problems, the wavelet transform is introduced [24,25]. The wavelet transform is very similar to the STFT, with some important differences. Instead of a window function *w* we now have a mother wavelet Ψ:

$$W\{f(\tau,s)\} = \int_{-\infty}^{+\infty} f(t) \frac{1}{\sqrt{s}} \psi^* \left(\frac{t-\tau}{s} \right) dt$$

By scaling and translating this mother wavelet different 'window' functions are obtained, the 'daughter wavelets'. This time we have an additional parameter: a translation τ and a scale *s*. By scaling the mother wavelet the wavelet is dilated or compressed (the 'window' function is resised), and by translating the wavelet the location of the window is changed. A large-scale parameter results in a slowly varying daughter wavelet, while a small scale results in a fast

varying daughter wavelet. After translating the signal from the beginning of the signal to the end of the signal the wavelet representation for this scale is obtained. The coarsest scale (large *s*, a 'window' with large support) detects low frequencies, the approximation details. On the contrary, a fine scale is sensitive to high frequencies, the detail coefficients, as can be seen from the formula. Each scale represents a different sub-band, Figure 2. The scale and translation parameters are related: when the scale parameter increases, the translation parameter is increased as well. In this way the wavelet functions are localised in space and in frequency, and solve the drawback of the (short time) Fourier Transform. Namely, the Windowed Fourier Transform only uses a single window in which the frequencies are found, while the Wavelet Transform uses variable size 'windows'. The Wavelet Transform is like the Windowed Fourier Transform with variable size window and an infinite set of basis functions. We use a large window for finding low frequency components and small windows for finding high frequency components.

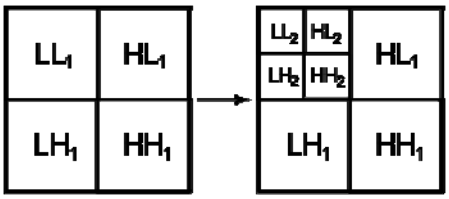

Figure 2: Sub-bands of a two dimensional wavelet transform. After the approximation and detail coefficients are calculated, the approximation details (LL1) are split up in high and low frequency sub-bands again.

By calculating the wavelet coefficients for different values of s and τ, the wavelet representation is obtained. When a wavelet coefficient is large, a lot of signal energy is located at that point, which may indicate important image features such as textures or edges. On the other hand, when a wavelet coefficient is small, the signal does not strongly correlate with the wavelet, which means a low amount of signal energy is present and indicates smooth regions.

To extract the PRNU pattern, we employ the de-noising filter as presented by Fridrich *et al.* [4], which in turn is based on the work presented in [26], in which an algorithm used for image compression is used for image de-noising[5]. A short (general) description of the used algorithm follows, and for further details the interested reader is referred to the aforementioned works. The presented algorithm is implemented using the free WaveLab package [27] in Matlab, and has been integrated in the PRNUCompare program (see section 3.1.3) [28].

[5] This connection between compression and de-noising can be seen by realising that the important signal features (high signal energy) are represented by a small number of large wavelet coefficients, while small features such as noise are represented by a large number of small wavelet coefficients. Thus, removing these small coefficients below a certain global threshold results in the removal of the noise (creating a sparse matrix), while simultaneously decreasing the amount of bits needed to represent the image. Instead of using a global threshold, a spatially adaptive threshold improves the image quality [21].

3.1.2.1 Algorithm

To perform video camera device identification, the video is first split up into individual frames using FFmpeg [29]. Calculating the wavelet coefficients for all possible values of *s* is not efficient, and we only use certain discrete values for *s* and τ for the calculation to obtain the Discrete Wavelet Transform. The image is assumed to be distorted with zero-mean WGN in the spatial domain with variance σ^2, and hence this noise is also WGN in the wavelet domain.

The input frames (images) must be dyadic (based on 2), as we generally choose base 2 (dyadic sampling) so that the coefficients for scale 2^j , j = 1 … n are computed. The translation τ depends on the scale, and can be dyadic as well. The end result is an image with the same size as the input image, composed of nested sub-matrices each representing a different detail level, as shown in Figure 2. This is done for all frames extracted from the video.

We now present the actual algorithm [4].

1. The fourth level wavelet decomposition using the Daubechies wavelet is obtained by letting a cascade of filters work on the image data, decomposing the image into an orthonormal basis (known as transform coding). The level-1 approximation coefficients are obtained by filtering the image data through a low-pass filter *g*, while the level-1 detail coefficients are obtained by filtering the image data through a high-pass filter *h*. These two filters are related, in such a way that the original signal can be obtained by applying the filters in reverse ('mirrored') order (these filters are called Quadrature Mirror Filters). By filtering the level-1 approximation coefficients (LL_1 sub-band) with the same set of filters *g* and *h*, the level-2 approximation and detail coefficients are produced (iteration), as represented in Figure 4 (See, e.g. Chapter 5 of [30]).
   Each resolution and orientation has its own sub-band, with HL_1 representing the finest details at scale 1 where the high pass filter was applied in the horizontal direction and the lowpass filter in the vertical direction. LL_4 represents the low resolution residual.

   This wavelet decomposition into different detail and approximation levels allows the image to be represented as a superposition of coarse and small details, as schematically represented in Figure 3.

2. For all pixels in each sub-band the local variance is estimated for each coefficient with a variable size square neighbourhood *N* with size $W \in (3; 5; 7; 9)$.

$$\hat{\sigma}_W^2(i,j) = \max\left(0, \frac{1}{W^2}\sum_{(i,j)\in N} LH_s^2\ (i,j) - \sigma_0^2\right)$$

   with (i, j) representing the pixel location in each sub-band. This estimates the local signal variance in each sub-band, and the minimum variance of each pixel for these varying size neighbourhoods is taken as the final estimate:

$$\hat{\sigma}^2(i,j) = \min(\sigma_{w\in W}^2(i,j))$$

3. The wavelet coefficients in the detail sub-bands can be represented by a generalised Gaussian with zero mean [31], and the image is assumed to be distorted by WGN with $N(0; \sigma_0^2)$. We currently cannot estimate this noise parameter σ_0^2 from the image itself. This σ_0^2 parameter controls how strong the noise suppression will be. When we

estimate the reference pattern as well as when we estimate the pattern noise from the (questioned) natural image, we need to set this parameter (denoted σ_{ref} and σ_{nat} respectively). Ultimately this parameter depends on the image itself (and hence also on the compression) and on the size of the noise. Ideally, the σ parameters should be spatially adaptive.
The actual de-noising step takes place in the wavelet domain by attenuating the low energy coefficients as they are likely to represent noise. This is done in all detail sub-bands (LH_s, HL_s, HH_s with s = 1 … 4) while the low resolution residual LL_4 remains unadjusted. The Wiener filter de-noises the wavelet coefficients:

$$LH_s(i,j) = LH_s(i,j)\frac{\hat{\sigma}^2(i,j)}{\hat{\sigma}^2(i,j)+\sigma_0^2}$$

This approach is intuitive because in smooth regions where the variance is small the coefficients will be adjusted strongly as a disturbance in a smooth region is likely caused by noise. On the other hand, in regions that contain a lot of details or edges, the variance will be large. Hence, these coefficients are adjusted only marginally, and blurring is avoided. This is also the reason why we select the minimum of the local variance for different sizes of the neighbourhood (step 2).

4. The above steps are repeated for all levels and colour channels. By applying the inverse discrete wavelet transform to the obtained coefficients, the de-noised image is obtained. By subtracting this de-noised image from the original input image, the estimated PRNU pattern is obtained. As a final step this pattern is zero-meaned such that the row and column averages are zero by subtracting the column averages from each pixel and subsequently subtracting the row averages from each pixel. This is done to remove artefacts from e.g. colour interpolation, as suggested in [12]. Wiener filtering of the resulting pattern in the Fourier domain, also suggested in [12], was not applied.

Figure 3: Left is the low resolution residual. The images are obtained by applying the inverse wavelet transform to the wavelet representation of different scales. Moving to the right more detail is added until the final image is obtained.

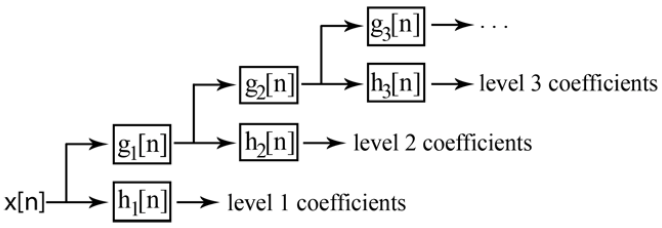

Figure 4: Iterated filterbank. The output of the lowpass filter g is the input of the next stage. See also Figure 1.

3.1.2.2 Obtaining the sensor noise patterns and detecting the origin

To determine whether a specific video V_q in question originates from a certain camera C, we first extract the individual frames I_{q_i} (i = 1 … N) from the video, and subtract the de-noised image I_{d_i} from each individual frame:

$$p_{q_i} = I_{q_i} - I_{d_i} \text{ with } I_{d_i} = F(I_{q_i})$$

and F the filter as described above. After this is done for all frames, the noise pattern is averaged:

$$p_q = \frac{1}{N}\sum_{i=1}^{N} p_{q_i}$$

In a similar manner the reference patterns p_{r_j} from different cameras with a known origin are obtained by averaging a number of these noise residuals in order to suppress the random noise contributions. However, instead of using images that contain natural content, it is preferred to use a flatfield video V_f from which individual flatfield images I_{f_i} can be extracted that have no scene content and an approximately uniform illumination:

$$p_r = \frac{1}{N}\sum_{i=1}^{N} I_{f_i} - F(I_{f_i})$$

This is done for multiple cameras, each with its own reference pattern p_{r_j}. After all the reference patterns are obtained, the final step is to measure the degree of similarity between the questioned pattern and the reference patterns. We use the total correlation (summed over all colour channels) as the similarity measure in order to find out whether a certain pattern p_q originates from a certain camera C. In order to do so, we calculate the correlation between the pattern from the questioned video p_q and the reference patterns p_{r_j}. When the correlation of p_q is highest for a certain p_{r_j}, we conclude that the video was acquired using camera j.

When obtaining flatfield videos is not feasible (e.g. the camera is not available or broken), it is also possible to use (multiple) natural videos with known origin to obtain the reference pattern.

As mentioned previously, we have to set the noise parameter to actually de-noise the image. Unfortunately, there is not one general value that works best. As this parameter controls how

strong the noise suppression in the image will be, the value for this parameter depends on the image itself. As the amount of noise left behind in the image (FPN and PRNU) depends among others on the illumination of the image, it is understandable that a fixed value works suboptimal, and that a spatially adaptive estimation of this parameter would be advantageous. This is partly realised by a stronger de-noising in the regions where the local image variance is small and vice versa. Especially as a video is generally composed of hundreds of frames, a fixed value is likely to under- or overestimate the pattern noise in the individual frames. For natural frames with a high amount of details a higher σ_{nat} is favourable, while for smooth frames a lower parameter is advantageous.

When the resolution in which the videos have been recorded are lower than the native resolution, binning may occur and attenuate the pattern noise. When this occurs, the pattern to be extracted is much weaker which influences the optimal parameter to be used. The same is expected to be true for compression, as strongly compressed videos are expected to have less of the pattern noise available in the video.

As a final remark, in smooth regions the possibility exists that a ringing effect occurs in the reconstructed image as in shown in Figure 5. This occurred for very low resolution images, such as 128x128 or lower. As these effects occur in smooth regions, it was decided for these low resolution images to only adjust the lowest scales (e.g. only the LH_s, HL_s, and HH_s with s=1…3 were adjusted for 128x128 images; for 64x64 images only the lowest two scales were adjusted (s=1,2)).

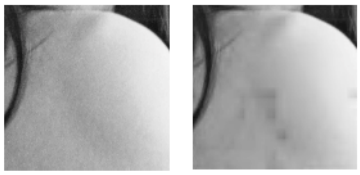

Figure 5: Example of the ringing effect. (a) the original image, (b) the de-noised image with the introduced ringing effect.

3.1.2.3 Remarks on the uniqueness of the PRNU

It was mentioned in the introduction that the sensor noise patterns from different cameras are unique, though large-scale tests have not been performed. However, it was observed that reference patterns from cameras of the same type have a slightly similar sensor noise pattern. This slight similarity was not observed when the patterns from different cameras were compared, as can be see in Figure 6. When reference patterns of dissimilar cameras are compared, the correlations are centred on 0, i.e. there is no (linear) relationship between the patterns. When patterns from the same model are compared the correlation increases, indicating partly similar patterns. Thus a thorough test should always include a large number of cameras of the same type. This does not always occur in the literature.

Indeed, when some of the artefacts introduced in the output image do not come from the CCD or CMOS sensor itself, but from some other component that is present on all cameras of a certain model and/or type, a similarity in the output can be expected.

In [21,32] and the references therein the camera class is identified by looking at traces left behind by the (proprietary) colour interpolation algorithm that is used to demosaic the colours, after the colour filter array decomposed the incoming light in RGB/CYGM[6]. In [33] different measures are used to identify the make/brand of the camera. With the use of binary similarity measures some of the artefacts from the processing stage in the camera can be detected in the 'low order bitplanes', the 6th to 8th bit (LSB). High-order wavelet statistics (HOWS), statistical measures such as the mean, variance and kurtosis of the wavelet sub-bands, can be used to find characteristic features. With these features it is possible to a certain extent to identify the make or brand of camera from which an image originates. These characteristics show that other traces left behind in the image are not unique to the individual camera. Hence, device classification shows we need to select an appropriate amount of cameras of the same type and model to compare with.

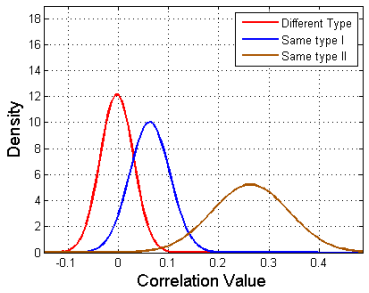

Figure 6: Correlations between the sensor patterns originating from the same make/brand and correlations between patterns originating from different makes/brands.

As the relative size of the individual components responsible for the PRNU is unknown it is possible that the components present on all cameras of the same type contribute a significant amount to the magnitude of the estimated PRNU pattern. For high quality digital cameras this is not a serious problem, as it is expected that these high quality cameras contain less systematic artefacts introduced by compression or demosaicing. In [12] these problems were circumvented by zero-meaning the estimates and Wiener filtering the image in the Fourier domain. While zero-meaning decreased the correlation between same type cameras, Wiener filtering did not have the same effect. This, combined with an imprecise extraction of the PRNU from a dark/highly detailed/compressed image may possibly result in false source identification.

3.1.3 The NFI PRNU Compare program

As mentioned in Section 3.1.2, the algorithm was initially implemented in Matlab using the freely available WaveLab package from Stanford [27]. In the spirit of the reproducible research philosophy of the authors of WaveLab, and to make the results more accessible and easy to use, we manually translated this code to Java and added it to the *NFI PRNUCompare* program. This program is open source and freely available from [28]. Extensive help is available which can be accessed with the help-button.

First, the method used to extract the PRNU patterns needs to be set. This can be done by going to *View* → *Advanced settings*. By clicking on the radio button next to *`Wavelet extraction'* the wavelet based PRNU extraction is selected, as shown in Figure 7. By clicking

[6] See also §3.3: Fusion of characteristics for image source identification (p.42)

this button one can immediately observe that some fields are greyed-out, as they do not need to be set with this method.

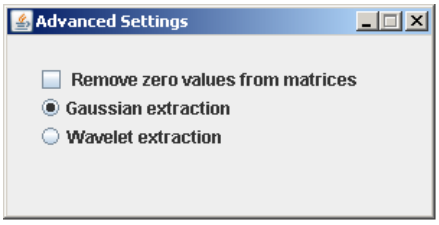

Figure 7: Selecting the method used for extracting the PRNU patterns.

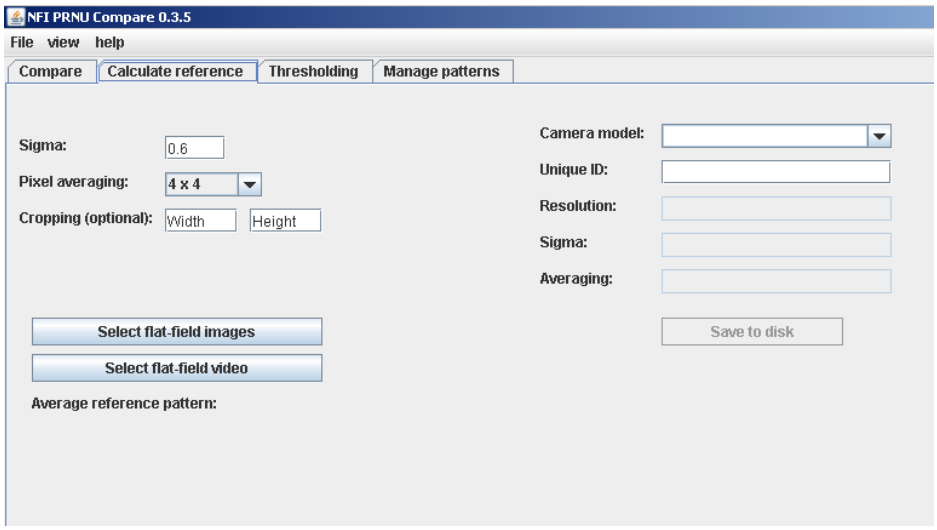

Figure 8: Main view of the Calculate reference tab.

By default, a σ-value of 5 is used to extract the PRNU from the image. Often this is a suitable value, but varying this parameter may result in a better performance. By default, the maximum dyadic image size is selected. However, it is also possible to select only a small portion of each image by entering the desired *Width* and *Height* in their respective fields. This may be of use when using high-resolution images, to speed up the process of the extraction.

To calculate the reference pattern of a certain camera, a preferably large amount of flatfield images should be acquired with the reference camera. In the case of video cameras, a preferably long flatfield video should be captured with sufficient frames. The amount of frames to be used depends on the compression, the PRNU size, etc. In general, 200 or more flatfield frames was found to be sufficient for videos. By clicking the *Select flatfield images* button, (multiple) flatfield images may be selected. When a reference pattern should be obtained from a video camera, the video file may be selected with the *Select flatfield video* button. See Figure 8.

After selecting the video or image files, the PRNU extraction starts. The average pattern found from these files is dynamically displayed in the window. A name should be given for the camera model, as well as a unique identifier, as multiple cameras of the same type may be available. As calculating reference patterns can be a lengthy process, the patterns can be saved to disk for later use.

After the patterns have been extracted from all the reference cameras we are interested in, we go to the *Compare* tab (Figure 9). Again, the σ-parameter can be set, in this case for the

natural (questioned) video or image(s). The default value of 5 is again generally adequate, but may not be optimal. After a video or (multiple) images are selected, the PRNU extraction starts. After this process has been completed, the reference camera patterns may be selected in the right part of the window. After clicking the *Compare* button, the correlation between the pattern extracted from the natural video or image and the selected reference patterns is calculated. Of course, the resolution of the reference pattern and the pattern extracted from the natural video or image need to be the same. The resulting correlations appear, and the reference camera that has the highest total correlation (summed over all colour channels) with the pattern extracted from the natural video is automatically placed on top. This should be the camera that also produced the natural video. As was mentioned previously, it is advisable to include a large amount of reference cameras of the same model and type as the questioned camera, as a higher correlation may be expected between cameras of the same type. In other words, we need to know the distribution of the correlation values between cameras of the same type. For example, when the distribution of correlation values between cameras of the same type is centred on 0, with a standard deviation of 0.01, a correlation value of 0.05 between the pattern extracted from the natural image and the questioned camera is significant. On the other hand, a correlation value of 0.05 is insignificant when the distribution of correlation values between cameras of the same type is centred on 0.03 with a 0.02 standard deviation. Finally, the results may be exported to a *.csv* file, after which they can be imported in to spreadsheet applications.

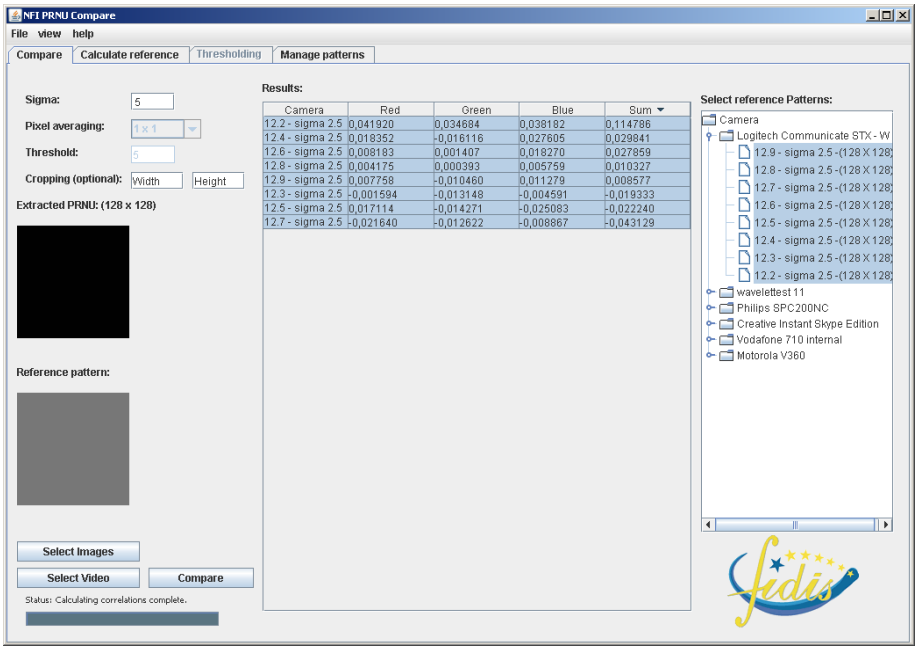

Figure 9: Main view of the Compare tab.

In the *Manage patterns* tab the PRNU patterns can be managed, for example renaming the camera model, or deleting the patterns. This application works both for videos and photos. The applicability of this application to photos has only been tested briefly, but as this algorithm was initially developed for images from digital cameras, we expect no difficulties in this respect. In principle, all results in this text should be reproducible. However, reading images in Java (especially bitmap files) leads to different pixelvalues compared to reading images in Matlab. As this happens for bitmap files (i.e. a format without compression), this may be due to a different gamma value.

3.1.4 Application to *YouTube* videos

YouTube is a website (like Dailymotion, metacafe) where users can view and share (upload) video content. Videos encoded with the most popular encoders (such as WMV, DivX, Xvid, but also the 3GP format used by mobile phones) are accepted as uploads, after which the uploaded video is converted. To compress the uploaded video *YouTube* uses the Sorenson H.263 (Sorenson Media, used in Adobe Flash .flv) codec for the maximum standard quality viewing of 320x240, while the H.264 (MPEG-4 AVC, developed by the Video Coding Experts Group VCEG in collaboration with the Moving Picture Experts Group) is used for high quality viewing and has a maximum resolution of 480x360[7]. Note that unless the video is uploaded in RAW format (which in practice will not occur often), the resulting video is doubly compressed.

Online viewing is done using a Flash videoplayer, while downloading these videos can be done using services such as *keepvid.com*. The aspect ratio of the video will generally not change (there are exceptions, see section 3.1.4.4); hence a video uploaded as 640x360 (aspect ratio 16:9) will be downloadable as 320x180 (for .flv) or as 480x270 (for .mp4). As the resolution and the visual quality of the mp4 video is higher than for the .flv video, we use the mp4 video for extracting the pattern noise though the actual bitrate in bits per pixel is lower. This results in a better performance compared to when .flv files were used. To assess the performance of the algorithm for videos that are uploaded to *YouTube*, we uploaded multiple (natural) videos encoded with different settings and from different cameras to *YouTube*. The natural videos of approximately 30 seconds were recorded using two popular video codecs, namely Xvid (version 1.1.0) and Windows Media Video 9 (version 9.0.1) in single pass setting, using the Video for Windows (VfW) or DirectShow framework. The WMV9 codec is also used in the popular Windows Live (MSN) Messenger application (see also section 3.1.4.3.2). After downloading these videos, the individual frames were extracted using the open source command-line tool FFmpeg [29].

The flatfield video was obtained by recording (without any form of compression) a flat piece of paper under various angles in order to vary the DCT coefficients in the compression blocks for the duration of approximately 30 seconds. Natural video (also approximately 30 seconds) was obtained by recording the surroundings of an office in which scenes with a high amount of details alternated smooth scenes, both with dark and well-illuminated scenes. Static shots alternated shots with fast movements, and saturation occurred frequently. All recorded videos have approximately the same content. We made no attempt to select suitable frames based on brightness or other characteristics, other than the removal of saturated frames that occurred at the start of the recording.

When the uploaded (natural) content has a resolution lower than the maximum resolution from *YouTube* (480x360), there is no change in resolution. If this is the case, the reference pattern can be obtained from the RAW video directly from the (web-)camera; this gives a better performance compared to uploading the RAW video and finding the reference pattern from the downloaded video.

However, when the resolution of the uploaded (natural) content exceeds the maximum resolution that can be obtained from *YouTube*, *YouTube* resizes the input video. As it is unknown how the resizing occurs and which artefacts are introduced by the *YouTube* compression scheme, it is necessary to upload the reference material (in native resolution) to

[7] As of 6 December 2008, it is possible to watch videos in HD quality if the source video allows it

YouTube as well. In this way the reference video undergoes the same processing as the natural video that was uploaded. In Sections 3.1.4.2 and 3.1.4.4 we will also calculate the reference patterns by resizing the native flatfield video to match the dimensions from the downloaded natural video.

Ideally, a large number of frames should be used to calculate the sensor noise patterns. To see how many frames should be averaged we calculated the Mean Square Error (MSE) with respect to the final pattern as obtained from N=450 flatfield frames for the Logitech Communicate STX webcam, see Figure 10:

$$MSE(p_{i=1}^{j}, p_{i=1}^{N}) \text{, with } p_{i=1}^{j} = \frac{1}{j}\sum p_i$$

We see that the pattern obtained converges quickly to a stable pattern, and that by averaging the patterns from approximately 200 images already a reliable estimate is found. This is not necessarily true for natural video, as the noise estimation depends on the content of the individual frames.

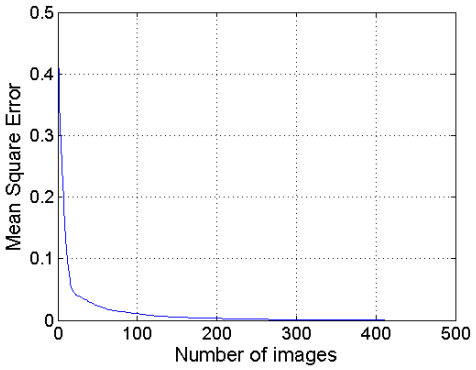

Figure 10: Mean square error of the estimated pattern noise with respect to the final estimate. We clearly see the estimated pattern converges reasonably quickly to the final pattern.

The patterns obtained from each natural video are compared with the reference patterns from all other cameras of the same type.

As explained above, the σ-parameters control the amount of noise that is extracted from each frame. To see which settings perform best, we calculate the reference patterns as well as the natural patterns (the patterns obtained from the natural video) for multiple values: σ_{nat} = 0.5:1:8.5, σ_{flat} = 0.5:1:7.5). By calculating the correlation between all these possible pairs we can find the optimum parameters. In actual casework this is not possible, as the questioned video has an unknown origin. We only report the correlation values of the matching (the natural video and reference material have the same origin) and the maximum correlation value of the mismatching pairs (the maximum correlation of the pattern from the natural video and the patterns from all other unrelated cameras), ρ_m and ρ_{mm} respectively.

3.1.4.1 Philips SPC200NC

First, it was tested if the source camera could be correctly identified from 9 Philips SPC200NC CMOS-based webcams (352x288 native resolution). For all cameras a video of approximately 30 seconds with natural content was recorded by the methods described above. These videos were directly encoded using the Xvid encoder (1.1.0) in single pass setting, with quality setting 4 (quality settings range from 1-32, with 1 the highest possible quality) set in

VirtualDub [34]. This resulted in 9 videos with an average bitrate of 475-525 kbit/s (0.15-0.18 bpp), which were subsequently uploaded to *YouTube*. After *YouTube* compressed/encoded the uploaded videos, they were downloaded as mp4 files using keepvid.com. In order to extract the patterns each frame was written to a lossless bitmap file. The amount of frames varied between 863 and 1083, due to slightly longer/shorter videos, varying amount of framedrops, etc.

The reference patterns were obtained by filming a white sheet of paper as described above, after which the reference pattern was again calculated using the individual frames. Between 898 and 1051 frames were extracted per video. To find the best parameters for σ_{flat} and σ_{nat} we calculated the noise residuals with varying parameters. The correlation between all noise residuals were calculated, and the parameters were selected that gave the most correct identifications and had on average the largest distance between the matching correlation ρ_m and the maximum correlation of the mismatching cameras ρ_{mm}. The best separation was found for $\sigma_{nat} = 6.5$, $\sigma_{flat} = 1.5$.

	cam1	cam2	cam3	cam4	cam5	cam6	cam7	cam8	cam9
ρ_m	0.0796	0.0830	0.1150	0.1939	0.1538	0.1814	0.1316	0.1347	0.1441
ρ_{mm}	0.0399	0.0350	0.0494	0.0830	0.0312	0.0238	0.0274	0.0226	0.0229

Table 1: Philips SPC200NC, 352x288, Xvid quality 4. Flatfields from RAW video. Between 863 and 1083 images used from approximately 30 seconds of natural video. σ_{nat} =6.5, σ_{flat} =1.5

	cam1	cam2	cam3	cam4	cam5	cam6	cam7	cam8	cam9
ρ_m	0.0362	0.0678	0.1021	0.1541	0.1231	0.1416	0.0903	0.0815	0.0737
ρ_{mm}	0.0317	0.0264	0.0534	0.0756	0.0339	0.0195	0.0126	0.0085	0.0107

Table 2: Philips SPC200NC, 352x288, Xvid quality 4. Flatfields from RAW video. Only 500 images used (approximately 15 seconds) of natural video. σ_{nat} =6.5, σ_{flat} =1.5

	cam1	cam2	cam3	cam4	cam5	cam6	cam7	cam8	cam9
ρ_m	0.0076	0.0503	0.0918	0.0993	0.0925	0.1165	0.0690	0.0582	0.0378
ρ_{mm}	0.0288	0.0256	0.0478	0.0563	0.0268	0.0170	0.0069	0.0326	0.0094

Table 3: Philips SPC200NC, 352x288, Xvid quality 4. Flatfields from RAW video. Only 250 images used (approximately 7.5 seconds) of natural video. σ_{nat} =6.5, σ_{flat} =1.5

	cam1	cam2	cam3	cam4	cam5	cam6	cam7	cam8	cam9
ρ_m	-0.0046	0.0332	0.0649	0.0925	0.0710	0.0923	0.0396	0.0421	0.0096
ρ_{mm}	0.0198	0.0222	0.0369	0.0321	0.0279	0.0417	0.0011	0.0348	0.0068

Table 4: Philips SPC200NC, 352x288, Xvid quality 4. Flatfields from RAW video. Only 125 images used (approximately 4 seconds) of natural video. σ_{nat} =6.5, σ_{flat} =1.5

We see all the source cameras were correctly identified based on the correlations when all the frames from the 30 second sample were used. To approximate the behaviour when a shorter sample is used, we only used the first 500 frames of each video; this corresponds to a sample of approximately 15 seconds (Table 2).

Although all cameras are correctly identified, the average distance between ρ_m and ρ_{mm} decreases. To see the behaviour when even less frames are used, we again reduce the number of frames to 250 (≈7.5 seconds), see Table 3.

The amount of wrong identifications is increased when 250 frames are used to 1/9, indicating that the noise pattern cannot be reliably estimated for this amount of natural frames. When the amount of frames is decreased even more to 125, there is again one wrong identification, but the distance between ρ_m and ρ_{mm} is again decreased (Table 4).

One may argue that it is advantageous to first upload the RAW video file to *YouTube* and subsequently download the video before the reference patterns are estimated, instead of directly extracting the patterns from the RAW video. Doing so has the advantage that both videos have the same processing history, i.e. both videos undergo the same compression. Note however that at this low resolution no resize is necessary (but see section 3.1.4.4), so the only result of undergoing the compression is that the pattern is obscured by the codec and the introduction of compression artefacts.

	cam1	cam2	cam3	cam4	cam5	cam6	cam7	cam8	cam9
ρ_m	0.0739	0.0428	0.1114	0.0028	0.0320	-0.0114	0.1654	0.0224	0.1144
ρ_{mm}	0.0028	0.0332	0.0497	0.1505	0.0841	0.0304	0.0232	0.0479	0.0172

Table 5: Philips SPC200NC, 352x288, Xvid quality 4. Flatfield images from RAW video uploaded to *YouTube*, 455-1024 images used. σ_{nat} =6.5, σ_{ref} =1.5

Indeed, using images extracted from the video that was uploaded to *YouTube* resulted in a lower identification rate: only 5 out of 9 were correctly identified. The correlations between mismatching pairs are significantly higher than when frames directly from the RAW video are used. This is not surprising since the encoding scheme from *YouTube* may introduce compression artefacts in the reference video.

3.1.4.2 Creative Live! Video IM

We recorded for each of the 6 Creative Live! Cam video IM (native resolution 640x480) a 30 second natural video with resolution 352x288, and again uploaded it to *YouTube*. Note that the recording resolution has a different aspect ratio than the native resolution, 11:9 compared to 4:3. The natural video was recorded in the WMV9 codec, with quality setting 70 (max 100). Approximately 250 frames were recorded in this time span due to the high amount of framedrops that occurred when moving scenes were recorded.

This resulted in videos with a bitrate of approximately 180-230 kbit/s (0.13-0.16 bpp). As there was no further resizing by *YouTube*, the flatfield video was recorded without any form of compression at resolution 352x288. The best results were found using $\sigma_{nat} = 6.5$, $\sigma_{flat} = 2.5$, so that 5 out of 6 cameras were correctly identified:

	cam1	cam2	cam3	cam4	cam5	cam6
ρ_m	0.0569	0.0242	0.0381	0.0121	0.0294	0.1017
ρ_{mm}	0.0240	0.0233	0.0262	0.0533	0.0070	0.0526

Table 6: Creative Live! Natural video recorded in 352x288, wmv70. σ_{nat} =6.5, σ_{ref} =2.5

As a next step, we recorded for each of the 6 cameras a 30 second natural video in 800x600 resolution (±250 frames) encoded with the WMV9 codec at quality 60, which means that the video has been rescaled by the driver while retaining the same aspect ratio. This resulted in videos with a bitrate between 360-430 kbit/s (0.05-0.06 bpp). After uploading and subsequently downloading the natural video from *YouTube*, the noise patterns were again calculated. As we cannot be sure about the recording resolution, we also uploaded the RAW flatfield videos recorded in the native resolution (640x480). This resulted in a 100% correct identification rate:

	cam1	cam2	cam3	cam4	cam5	cam6
ρ_m	0.1222	0.1074	0.1104	0.1475	0.0627	0.2036
ρ_{mm}	0.0419	0.0276	0.0165	0.0296	0.0113	0.0321

Table 7: Creative Live! Natural video recorded in 800x600, wmv60 (Flatfields from *YouTube*) parameters: (σ_{nat} =5.5, σ_{flat} =3.5)

As we have seen in Section 3.1.4.1, uploading the flatfield video to *YouTube* resulted in a low amount of correct identifications. This is not the case for this camera (at these settings). Still, we were interested to see whether simply resizing the flatfield video from 640x480 to 480x360 without uploading the video to *YouTube* would perform better, as the additional layer of *YouTube* compression is now absent. Each individual frame was resized using the nearest neighbour algorithm as well as bilinear interpolation (Table 8 and 9, respectively). We see the distance between ρ_m and ρ_{mm} is increased, while the ρ_{mm} are more centred on zero, indicating a lower similarity between the patterns. This may be due to the introduction of certain artefacts by the *YouTube* codec, which are not present when the frames were resized using the nearest neighbour or bilinear interpolation method.

	cam1	cam2	cam3	cam4	cam5	cam6
ρ_m	0.1196	0.112	0.1137	0.1743	0.0684	0.1781
ρ_{mm}	0.0261	0.0166	-0.0008	-0.0003	0.0014	-0.0011

Table 8: Creative Live! Natural video recorded in 800x600, wmv60 (Flatfields from nearest neighbour interpolation from 640x480 to 480x360) parameters: (σ_{nat} =5.5, σ_{flat} =2.5)

	cam1	cam2	cam3	cam4	cam5	Cam6
ρ_m	0.119	0.1167	0.1105	0.176	0.0655	0.1734
ρ_{mm}	0.0263	0.0157	-0.0041	-0.002	0.0044	-0.0004

Table 9: Creative Live! Natural video recorded in 800x600, wmv60 (Flatfields from bilinear interpolation from 640x480 to 480x360) parameters: (σ_{nat} =5.5, σ_{flat} =2.5)

To see whether this is still the case when the natural videos are recorded in lower quality, we repeated the test for WMV50 and WMV40. Again, using interpolated frames results in a distribution of mismatching values that is more closely distributed around zero. When interpolated flatfield images are used, camera 5 is correctly identified. When the natural videos are encoded with WMV with quality setting 40, all cameras are again correctly identified, with the mismatching correlations closer to zero.

	Cam1	cam2	cam3	cam4	cam5	cam6
ρ_m	0.1369	0.1305	0.1022	0.0448	0.0682	0.1682
ρ_{mm}	0.0555	0.0553	0.0284	0.0303	0.0756	0.0297

Table 10: Creative Live! Natural video recorded in 800x600, wmv50 (Flatfields from *YouTube*) parameters: σ_{nat} =5.5, σ_{flat} =3.5

	Cam1	cam2	cam3	cam4	cam5	cam6
ρ_m	0.1306	0.0991	0.0612	0.0389	0.0695	0.1473
ρ_{mm}	0.0246	0.0151	0.0126	0.0344	0.0208	0.0141

Table 11: Creative Live! Natural video recorded in 800x600, wmv50 (Flatfields from bilinear interpolation from 640x480 to 480x360) parameters: σ_{nat} =6.5, σ_{flat} =2.5

	cam1	cam2	cam3	cam4	cam5	cam6
ρ_m	0.1438	0.0994	0.0529	0.0340	0.0737	0.1483
ρ_{mm}	0.0245	0.0116	0.0099	0.0335	0.0115	0.0102

Table 12: Creative Live! Natural video recorded in 800x600, wmv50 (Flatfields from nearest neighbour interpolation from 640x480 to 480x360) parameters: σ_{nat} =6.5, σ_{flat} =2.5

	cam1	cam2	cam3	cam4	cam5	cam6
ρ_m	0.1046	0.0815	0.0579	0.0526	0.0640	0.1764
ρ_{mm}	0.0145	0.0390	0.0380	0.0501	0.0193	0.0702

Table 13: Creative Live! Natural video recorded in 800x600, wmv40 (Flatfields from *YouTube*) parameters: σ_{nat} =5.5, σ_{flat} =3.5.

	cam1	cam2	cam3	cam4	cam5	cam6
ρ_m	0.0730	0.0522	0.0680	0.0462	0.0790	0.1655
ρ_{mm}	0.0147	0.0055	0.0100	0.0266	0.0053	0.0119

Table 14: Creative Live! Natural video recorded in 800x600, wmv40 (Flatfields from bilinear interpolation from 640x480 to 480x360) parameters: σ_{nat} =5.5, σ_{flat} =2.5

	cam1	cam2	cam3	cam4	cam5	cam6
ρ_m	0.0776	0.0527	0.0683	0.0481	0.0797	0.1660
ρ_{mm}	0.0147	0.0065	0.0091	0.0273	0.0053	0.0136

Table 15: Creative Live! Natural video recorded in 800x600, wmv40 (Flatfields from nearest neighbour interpolation from 640x480 to 480x360) parameters: σ_{nat} =5.5, σ_{flat} =2.5

3.1.4.3 Logitech Quickcam STX

We recorded for each of the 8 Logitech Quickcam STX cameras a 30 second sample with natural content recorded in the native resolution of 640x480 with the Xvid codec with quality setting 4, as well as a 30 second flatfield sample in the same resolution in RAW. Note that *YouTube* will resize these videos. Again, the reference patterns were obtained from uploading the RAW video to *YouTube*, as well as from the bilinear and nearest neighbour resized flatfield videos.

Regardless of the parameter settings (σ_{nat}=4.5-6.5, σ_{flat}=2.5-6.5 has the best separation), this resulted in a 100% correct classification rate:

	cam1	cam2	cam3	cam4	cam5	cam6	cam7	cam8
ρ_m	0.1836	0.3013	0.1926	0.2297	0.1731	0.1967	0.1998	0.2581
ρ_{mm}	0.0526	0.0369	0.0239	0.0362	0.0406	0.019	0.0283	0.0315

Table 16: Logitech Communicate STX – RAW from *YouTube* - σ_{nat} =4.5, σ_{flat}=3.5 (all parameters work well).

As in the previous paragraph, we resized the frames from the RAW flatfield video from 640x480 to 480x360 to match the dimensions obtained from the natural video, see Table 17 and 18.

	cam1	cam2	cam3	cam4	cam5	cam6	cam7	cam8
ρ_m	0.1334	0.2301	0.1279	0.1818	0.1596	0.1622	0.1515	0.2099
ρ_{mm}	0.0374	0.0512	-0.0009	0.0342	0.0355	0.029	0.0118	0.0421

Table 17: Logitech Communicate STX - RAW from Bilinear Resize - σ_{nat}=6.5, σ_{flat}=7.5 (all parameters work well).

	cam1	cam2	cam3	cam4	cam5	cam6	cam7	cam8
ρ_m	0.1341	0.2323	0.1287	0.1763	0.1592	0.1574	0.1547	0.2103
ρ_{mm}	0.0345	0.0542	-0.0017	0.0305	0.0364	0.0317	0.0134	0.0411

Table 18: Logitech Communicate STX - RAW from Nearest Neighbour Resize - σ_{nat}=6.5, σ_{flat}=7.5 (all parameters work well).

We repeated the experiment with the same cameras and only changed the recording resolution to 320x240. Recording in a lower than native resolution means that the pixels in the output video are binned (in this case 4 pixels are averaged to give the output of 1 pixel) which results in a strong attenuation of the PRNU, as the PRNU is a per-pixel effect. If one general set of parameters is chosen, a maximum of 6 cameras were correctly identified, as can be seen in Table 19.

	cam1	cam2	cam3	cam4	cam5	cam6	cam7	cam8
ρ_m	0.1044	0.0936	0.109	0.0153	0.0304	0.1044	0.0984	0.0334
ρ_{mm}	0.028	0.0616	0.0803	0.0407	0.0245	0.0526	0.0652	0.0648

Table 19: Logitech Communicate STX - flatfields from RAW video - σ_{nat}=3.5, σ_{flat}=5.5

3.1.4.3.1 Codec variations

For one camera we recorded video in the native resolution of 640x480, as well as the lower resolution 320x240 for two different codecs and different codec settings. In order to let the video content be the same for all videos, we first recorded the video in RAW at both resolutions, and subsequently encoded it with different codec settings in VirtualDub. For both resolutions we recorded the video in Xvid and WMV9, with different codec settings. For the Xvid codec we used quality settings q = 4n, with n = 1 … 8, while for the WMV9 codec we used quality settings q = 10n, n = 5 … 9. Note that in the case of Xvid higher q values represents higher compression, while in the case of the WMV9 codec a higher setting means higher quality. The videos were uploaded to *YouTube*, and subsequently downloaded after which the sensor pattern noise was extracted again.

For these settings we again tried to find out whether the outlined method was able to pick out the source camera; a comparison was made with the reference patterns from 7 other Logitech cameras of the same type. For the low resolution 320x240 we used the RAW video to extract the patterns, while for the high resolution it was required to resize the frames from the flatfield videos.

We see the algorithm performs very well for the 640x480 (native) resolution: the correct identification rate is 100% for all codec settings (Table 20 and 21). Also, the parameter values do not influence the identification rate, and the correct camera is identified for almost all combinations of these parameters.

setting	size (kB)	frames	duration	bitrate (kbit/s)	bpp	ρ_m	ρ_{mm}
4	4031	519	34.59	932	0.202	0.2252	0.0693
8	2008	519	34.59	464	0.101	0.2046	0.0901
12	1455	519	34.59	337	0.073	0.1957	0.0678
16	1193	519	34.59	276	0.060	0.1921	0.069
20	1036	519	34.59	240	0.052	0.1715	0.0471
24	960	519	34.59	222	0.048	0.1612	0.0679
28	889	519	34.59	206	0.045	0.1798	0.0677
32	863	519	34.59	200	0.043	0.1479	0.0579

Table 20: Logitech Communicate STX. Video recorded in 640x480 with the Xvid codec, variable quality. σ_{nat} =8.5, σ_{flat} =7.5

setting	size (kB)	frames	duration	bitrate (kbit/s)	bpp	ρ_m	ρ_{mm}
90	6401	508	34.6	1480	0.207	0.2852	0.0665
80	3013	508	34.6	697	0.103	0.2084	0.0599
70	1994	508	34.6	461	0.075	0.1972	0.0521
60	1459	508	34.6	337	0.061	0.1666	0.062
50	1210	508	34.6	280	0.053	0.1773	0.0689
40	967	508	34.6	224	0.049	0.1842	0.0586

Table 21: Logitech Communicate STX. Video recorded in 640x480 with the WMV9 codec, variable quality. σ_{nat} =8.5, σ_{flat} =5.5

When the recording resolution is set to 320x240 we see that the correct identification rate is lowered. For the Xvid codec we see this happens at the moderate quality setting of 16, while for even lower quality encodings the camera is correctly identified. This shows that video compression is not a linear process; apparently, at lower quality settings more important details are retained. For the WMV9 codec we see the correct identification rate is decreased for the lowest quality settings (Table 22 and 23).

setting	size (kB)	frames	duration	bitrate (kbit/s)	bpp	ρ_m	ρ_{mm}
4	2206	488	32.97	535	0.859	0.1173	0.0497
8	1238	488	32.97	300	0.429	0.0795	0.0852
12	949	488	32.97	230	0.311	0.1115	0.0541
16	813	488	32.97	197	0.255	0.0811	0.0608
20	750	488	32.97	182	0.221	0.1474	0.0472
24	703	488	32.97	171	0.205	0.0935	0.0684
28	675	488	32.97	164	0.190	0.1259	0.0531
32	660	488	32.97	160	0.184	0.1026	0.0381

Table 22: Logitech Communicate STX. Video recorded in 320x240 with the Xvid codec, variable quality. σ_{nat} =5.5, σ_{flat} =4.5

setting	size (kB)	frames	duration	bitrate (kbit/s)	bpp	ρ_m	ρ_{mm}
90	3023	489	32.97	734	0.859	0.0939	0.0811
80	1717	489	32.97	417	0.428	0.1107	0.0894
70	1229	489	32.97	298	0.310	0.1483	0.0823
60	953	489	32.97	231	0.254	0.1001	0.08
50	815	489	32.97	198	0.221	0.0663	0.0481
40	700	489	32.97	170	0.204	0.0592	0.074

Table 23: Logitech Communicate STX. Video recorded in 320x240 with the WMV9 codec, variable quality. σ_{nat} =6.5, σ_{flat} =7.5

3.1.4.3.2 Video extract from a Windows Live Messenger stream

Windows Live Messenger [35], formerly known as MSN Messenger (using the Microsoft Notification Protocol (MSNP)), is a popular instant messaging client, which provides webcam support as well as videochat support. Recent data of market penetration is hard to come by, but the data available from a company that provides a free mobile instant messaging application with multi-protocol support (MSN, AIM, Yahoo, ICQ, Jabber and QQ) suggests a dominant marketshare for Windows Live Messenger for countries as Canada, Mexico, Australia, as well as large parts of Western Europe and South America [36]. The actual figures may be somewhat different, especially when we consider that not all protocols and clients have reliable webcam support.

Through the use of external programs it is possible to record the video stream sent during a webcam session, often simply by capturing the screen. It is also possible to directly record the data from the stream, as is done with MSN Webcam Recorder [37] (version 1.2rc7). This program uses the WinPcap driver [38], allowing the program to directly capture the data packets from the stream.

As a final test with this webcam, we set up a webcam session between two computers with Windows Live Messenger, with one computer capturing a webcam stream of approximately two minutes sent out by the other computer. The stream was sent out as a WMV9 video at a resolution of 320x240 (selected as 'large' in the host client). After the data was recorded with the aforementioned program, it was encoded with the Xvid codec (1.2.-127) with a bitrate of 200 kbps, which resulted in 1705-1815 frames (0.17-0.18 bpp). Finally, the resulting video was uploaded to *YouTube*, where a third layer of compression was added. It has to be stressed that in practice with low bandwidth systems the framerate may be reduced significantly.

	cam1	cam2	cam3	cam4	cam5	cam6	cam7
ρ_m	0.1029	0.1361	0.0792	0.106	0.101	0.077	0.0616
ρ_{mm}	0.0421	0.0383	0.0476	0.0129	0.0459	0.0288	0.0505

Table 24: Logitech Communicate STX. Video (320x240) recorded from webcam stream from Windows Live Messenger (WMV9) and subsequently encoded with the Xvid codec. σ_{nat} =4.5, σ_{flat} =2.5

We again see the source camera is correctly identified.

3.1.4.4 Vodafone 710

The final test is for the external camera of the Vodafone 710 with a resolution of 176x144, which stores the videos in the 3GP format. This is, like the AVI file format, a container format in which H.263 or H.264 can be stored. The Vodafone 710 uses the H.263 format optimised for low-bandwidth systems. We recorded both natural and flatfield content for all 10 cameras. The natural video had a bitrate between 120 and 130 kbit/s (0.36-0.39 bpp). After uploading the source video, *YouTube* changed the aspect ratio from 11:9 to 4:3 (to 176x132)[8]. This made it necessary to also upload the flatfield videos. As with the Philips webcam (x5.1), uploading the flatfields is detrimental for the results (especially at these low resolutions), and this is also true for the Vodafone 710. Only 5 of 10 cameras were correctly identified. When the source camera is correctly identified, the distance between ρ_m and ρ_{mm} is small.

In this case, resizing the frames from the flatfield videos using either the nearest neighbour or the bilinear interpolation method does not result in an improvement: 5 or 6 cameras are still incorrectly identified. Downloading the natural videos in the H.263 format (also used by the phone to encode the video) did not improve the result.

The correct identification rate for this camera is much lower than for the other cameras. This may be due to the codec used to initially encode the source video, namely H.263. This codec uses a form of vector quantisation, and is therefore different from the discrete cosine transform used in WMV9 and Xvid.

	cam1	cam2	cam3	cam4	cam5	cam6	cam7	cam8	cam9	cam10
ρ_m	0.0106	-0.0138	0.0913	0.0632	0.0497	0.0339	0.0401	0.0069	0.0291	0.0326
ρ_{mm}	0.0340	0.0195	0.0713	0.0212	0.0385	0.0306	0.0548	0.0261	0.0558	0.0286

Table 25: Vodafone 710 (176x144, resized by *YouTube*) H.263 (no further settings possible). RAW downloaded from *YouTube*, σ_{nat} =1.5, σ_{flat} =6.5

[8] Initially it was thought that the minimum aspect ratio had to be 4:3, but the Philips webcam (352x288) also with 11:9 did not have the change of aspect ratio.

	cam1	cam2	cam3	cam4	cam5	cam6	cam7	cam8	cam9	cam10
ρ_m	0.0078	0.0234	0.0622	0.0433	0.0282	0.0145	0.0261	0.0112	0.0251	0.0095
ρ_{mm}	0.0126	0.0206	0.0373	0.0412	0.0468	0.0215	0.0269	0.0169	0.0230	0.0226

Table 26: Vodafone 710 (176x144, resized by *YouTube*) H.263 (no further settings possible). Bilinear Resized Flatfields, σ_{nat} =0.5, σ_{flat} =4.5

	cam1	cam2	cam3	cam4	cam5	cam6	cam7	cam8	cam9	cam10
ρ_m	-0.0208	0.0075	0.0961	0.0649	0.0414	0.0319	0.0421	0.0150	0.0500	0.0125
ρ_{mm}	-0.0027	0.0228	0.0773	0.0432	0.0492	0.0663	0.0314	0.0416	0.0487	0.0408

Table 27: Vodafone 710 (176x144, resized by *YouTube*) H.263 (no further settings possible). Nearest Neighbour Resized Flatfields, σ_{nat} =2.5, σ_{flat} =2.5

3.1.5 Discussion

Although the detection works well for a wide range of σ_{nat} / σ_{flat} parameters, in some cases the choice is critical. Especially for videos with low resolution the choice is important. For example, for most parameters only 2 out of 10 source cameras were correctly identified for the Vodafone 710, while for other parameters 4 were correctly identified. The same is true for the Creative Live! IM Video in 352x288 resolution: between 1 and 5 cameras were correctly identified, depending on the parameters. In actual casework it is of course impossible to find the optimal parameter for which the detection works best, as the origin is unknown. Of course, the best remedy is to have the original videos available, i.e. the videos before the additional compression at *YouTube* is applied.

It is necessary to compare the pattern extracted from the natural video with a preferably large amount of cameras of the same make and model as the suspect camera. These cameras may not always be available, especially for old (video) cameras.

With the help of the PRNU it is also possible to detect certain image manipulations. In places where the image has been adjusted, e.g. by a copy/paste operation, the PRNU has been changed locally. In other words, the correlation between this adjusted region and the original reference pattern is lower. In principle, it is even possible to detect from which camera the copied region originates, if this region is large enough.

3.1.6 Conclusion

By extracting and comparing sensor noise patterns it was shown to be possible under certain conditions to find out from which camera a certain video originates, even after it was uploaded to *YouTube* where the added layer of compression further degrades the sensor noise. Although it is certainly possible to correctly identify videos, there are some important remarks to be made. The largest problem is that we do not know in which codec settings and in which codec or resolution the original video was initially uploaded (see e.g. Tables 20-33). When the video is recorded in low resolution such that the output is binned it is especially detrimental to the PRNU and we have problems correctly identifying the source camera. Also, the video may have been encoded multiple times before it was uploaded to *YouTube*. This makes it very difficult to judge whether the pattern with the highest correlation is truly the source camera. As we have seen, the PRNU pattern is severely distorted when video is

recorded in a lower than native resolution, such as 320x240 instead of 640x480. This will especially be a problem when the native resolution is e.g. 1280x960, and the video was recorded in 640x480. Videos with this resolution will be resized by *YouTube*, and we cannot infer the recording resolution from those downloaded videos.

Another problem is that *YouTube* may change its encoding scheme from time to time, such that at the time the original (natural) video was uploaded the codec (settings) used to encode the video to H.263 or H.264 may be different compared to when the reference material is uploaded. However, as long as no spatial transformations are applied (such as changing the aspect ratio), this is no severe limitation. Also, the usual remarks regarding applicability apply: when the video is rotated, scaled or when other spatial transformations have been applied, the detection will not work unless the identical operations occur for the reference material as well. As video editing is less common than image editing, this also poses no serious limitation at the moment.

As there are a lot of parameters (duration of the video, content of the video, amount of compression, which codec was used to encode the video, which parameters should be used to extract the noise patterns, with which resolution was the video recorded, etc.) it is not possible to give a general framework to which the video should comply. However, in general, setting the parameter for extracting the PRNU pattern from natural or flatfield videos between 4 and 6, satisfactory results are obtained.

Finally, the assumption of added white Gaussian noise (be it in the wavelet or the spatial domain) is only a rough approximation to the true distribution of the PRNU. Namely, the multiplicative nature of the PRNU implies that well illuminated areas contain more pattern noise than dark areas. Either the de-noising parameter could be made spatially adaptive, or a de-noising algorithm could be used that does not make these explicit assumptions about the frequency content in the image, for example a Non-Local means approach.

We hope that providing an open source and freely available application to the public will aid law enforcement agencies in the quest of finding the source camera based on the videos it produces.

3.2 Sensor noise in flatbed scanners

Image source identification in general is based on detecting specific device-dependent characteristics of the image acquisition device. The previous section discussed the analysis of sensor noise for digital camera identification. To identify the source of digital images in general, it is necessary to understand the occurrence of device-dependent characteristics in all types of image acquisition devices including, for example, flatbed scanners and digital camcorders. Within this section, we will focus on determining the CCD-flatbed scanner that has been used to digitise an analogue image and we will take a closer look on the possibilities to use sensor noise for this task. A detailed discussion of the specific architecture of contact imaging scanners (CIS) is skipped for the sake of brevity. Generally, the presented results are expected to be similar for both scanner architectures (CCD and CIS).

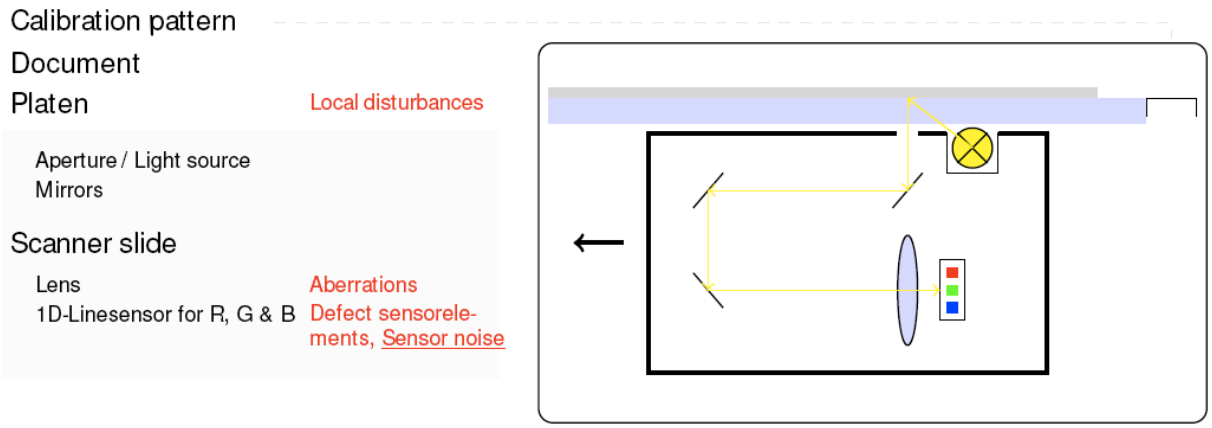

Figure 11: Optical path in a CCD-flatbed scanner and origin of different device-dependent characteristics (indicated in red).

3.2.1 Flatbed scanner architecture

The *key components* of flatbed scanners and digital cameras are very similar: Both have an optical system and use a photosensitive sensor to convert the light of a scene into a digital signal. Figure 11 shows the optical path of CCD-flatbed scanners in detail. The main components of a flatbed scanner are the platen to take the analogue document for digitisation, and the scanner slide, which includes all optical elements needed to acquire the image. In contrast to digital cameras, where an image is acquired at once, flatbed scanners move the scanner slide over the selected scan area and a one-dimensional line sensor creates a two-dimensional image by acquiring the image line by line sequentially. The line sensor consists of several sensor elements, which count the arriving photons as electrical charges. After acquiring a single line of the document, the charges are digitised and different image processing steps are done. Subsequently, the processed line images are transferred to the personal computer for composition of the complete image. In addition to the line sensor, the scanner slide includes a light source to illuminate the document, an aperture to narrow the admitted light, a lens to focus the light on the sensor and some mirrors to extend the optical path between the document and the lens. To improve the image quality, characteristics of the sensor and the optical system are estimated by scanning a white calibration pattern. The measured characteristics are used to reduce different noise sources and vignetting. For a more detailed discussion of the architecture and design of flatbed scanners, the reader is referred to the work of Vrhel *et al.* as well as to the work of Webb *et al.* [39,40].

3.2.2 Device-dependent characteristics

Some typically *device-dependent characteristics* introduced in flatbed scanners are indicated in red in Figure 11 [23]. Dust, scratches and surface defects on the platen lead to local disturbances in the acquired image, which can be hard to remove especially when located at the bottom side of the platen. Small inaccuracies of the lens and of the mirrors cause inherent aberrations in the mapping of the document to the sensor, e.g. chromatic aberration (cf. Section 3.3.2). Sensor elements can be defective or introduce sensor noise. Furthermore, mechanical distortions originating in the movement of the scanner slide during digitisation can leave analysable traces. In contrast to digital cameras (see Figure 1), the line sensor consists of separate sensor lines for each basic colour, i.e., no colour interpolation is needed and no interpolation artefacts occur. Furthermore, the final image is composited and

compressed on the attached personal computer and no special scanner-dependent JPEG-quantisation tables are used.

Device-dependent characteristics are an inherent part of each scanned image and are directly influenced by *particularities of the scanning process.* Within a forensic analysis of scanned images, it is important to consider these particularities. Usually, the document covers only a part of the platen and the user selects the area to be digitised respectively. Therefore, only a part of the device-dependent characteristics localised in the selected area can occur in the scanned image. For example, in case of sensor noise, not all CCD elements might be involved in the scanning process and thus only an incomplete noise pattern will be detectable in the final image. Contrary to digital cameras, the maximum available resolution in flatbed scanners depends on the number of sensor elements of the CCD-line sensor in horizontal direction and on the step size provided by the stepping motor in vertical direction. Due to performance and memory requirements in common office tasks, low resolutions with appropriate characteristics in reproduction are applied when scanning a document. Besides the selected scan area and the selected resolution, the calibration process inside the flatbed scanner directly influences the occurrence of sensor noise and vignetting in each scanned image [39,23].

3.2.3 Source identification of Scanned Images

Due to the similarities in the sensor technology of digital cameras and flatbed scanners, current state-of-the-art methods for image source identification of scanned images are motivated by the promising results on camera identification [4] already discussed in 3.1 and therefore, focus on *sensor noise* [23,41,42]. Within this section, a brief summary based on Ref. 23 on challenges and results of source identification in case of scanned images will be given.

Referring to Section 3.1 image source identification using sensor noise is a two-step process: First, a *reference noise pattern is calculated for each digital camera under investigation* by averaging the estimated noise[9] of a set of images with corresponding origin. Second, the *correlation coefficient is calculated as a similarity measure between the estimated noise of an image under investigation and the reference noise patterns* of probable source devices. Consequently, the highest correlation coefficient beyond a minimum threshold indicates the used digital camera for acquiring the image under investigation.

In the case of digital cameras, the image source identification scheme assumes a two-dimensional sensor noise pattern based on the image- as well as sensor-geometry. Corresponding to the image- and sensor-geometry of flatbed scanners, two different reference noise patterns are possible: a two-dimensional *array noise pattern* of the full scanable area or a one-dimensional *line noise pattern* characterising the noise of each sensor element directly. The process of calculating the two possible reference noise patterns is visualised in Figure 12. Equally to the camera identification scheme, the array noise pattern of a flatbed scanner can be calculated by averaging the estimated noise of a set of corresponding images. Subsequently, the line noise pattern can be calculated by averaging the array noise pattern within each column.

[9] To estimate the noise of an image, the authors in [4] propose to use a wavelet de-noising filter [26].

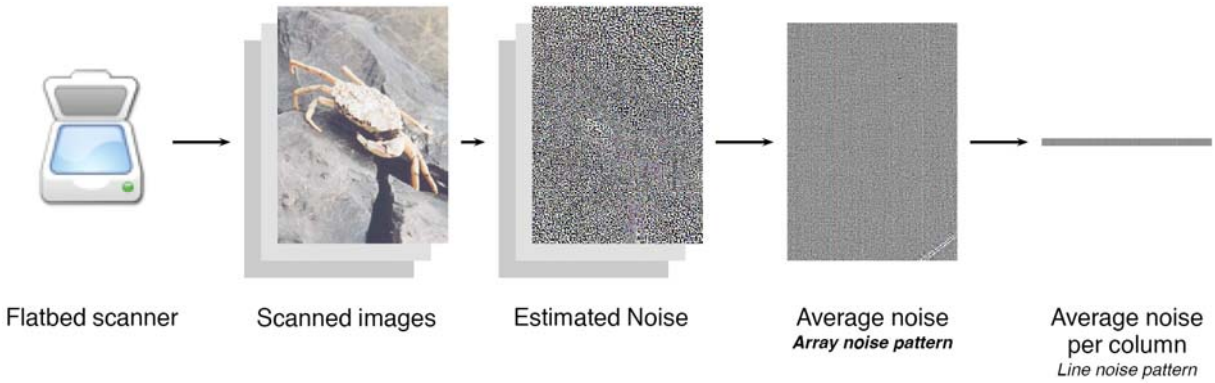

Figure 12: Calculation of reference noise patterns for flatbed scanner.

While *measuring the similarity* between an image's noise pattern and the array noise pattern is equal to the case of digital cameras, the similarity between an image's noise pattern and the line noise pattern is determined by the average of the calculated correlation coefficients between the line noise pattern and each row of the estimated noise of an image.

3.2.4 Practical results

Figure 13 depicts the results for the array noise pattern and the line noise pattern of a flatbed scanner manufactured by Hewlett Packard. Both reference noise patterns were calculated using 300 scanned images of different natural scenes and enable separation between images acquired with the corresponding flatbed scanner and images acquired with other devices.

To quantify the performance of the identification scheme, the true positive rate (TPR), indicating the number of correct identified images, in combination with a fixed false positive rate (FPR) of 0%, indicating none wrongly assigned images, were calculated. The high true positive rate (TPR) of 97% for the array noise pattern and of 96% for the line noise pattern documents the reliable use of sensor noise as device-dependent characteristic for correct source identification of scanned images. Focusing on Figure 13, a slight decrease between the average correlation of the first 300 images used to calculate the array noise pattern and the remaining images acquired with the same flatbed scanner is visible. In contrast to the array noise pattern, the average correlation remains stable over all corresponding images for the line noise pattern. Considering local disturbances like dust and scratches originating in the flatbed scanner's platen, an analysis of the array noise pattern included traces of this characteristic and probably causes of this effect. An example for the presence of a scratch in the array noise pattern and the estimated noise of a single image is illustrated in Figure 14. While the scratch is clearly distinguishable from other noise sources in the array noise pattern, it disappears in the noise pattern of one image due to object edges, scene texture and temporal noise.

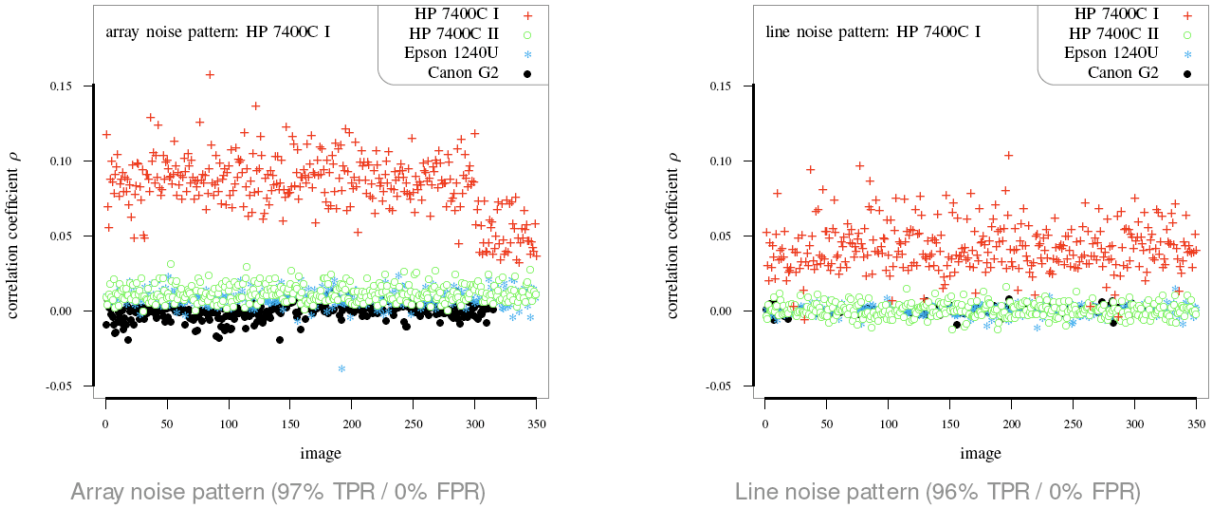

Figure 13: Identification results for HP ScanJet 7400C using 300 images of natural scenes scanned with 200dpi. The first 300 images were used to calculate the reference noise patterns. Generally, the results for both reference noise patterns are comparable.

Generally, array noise patterns have two disadvantages in comparison to the line noise pattern: they include local disturbances and calculating the similarity measure over all possible settings of scanning parameters (resolution and selected scan area) is computationally expensive due to its two-dimensional geometry. Another important problem for both reference noise patterns is the requirement to acquire approximately 300 natural images for all flatbed scanners under investigation, which is a very time consuming task. Therefore, the use of *homogenous coloured documents* in combination with a reduction of the number of scanned images was investigated to improve the generation of the reference noise patterns.

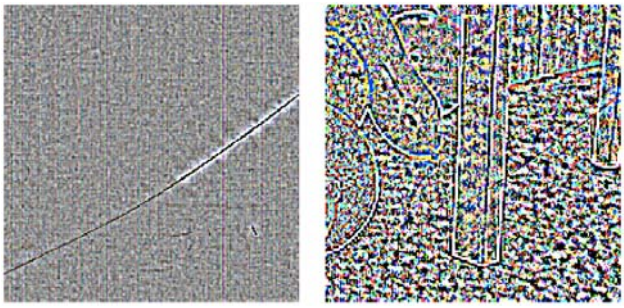

Figure 14: Presence of a scratch on the flatbed scanner's platen in the estimated sensor noise; while it is clearly visible in the array noise pattern (left image), it is occluded by object edges, scene texture and temporal noise in the estimated noise of one image (right image).

Among tests of different documents including homogenous white, black and grey coloured images, a black-white-black gradient image in combination with a line noise pattern turned out to generate the best results measured in terms of the true positive rate. Figure 15 shows the results for the HP flatbed scanner using 20 scans of the black-white-black gradient image. The extracted line noise pattern allows a true positive rate of 99% for all corresponding images, which enables a clear separation between corresponding images and images acquired with other devices. Contrary to the line noise pattern, the performance of the array noise pattern was worse for all tested homogenous documents.

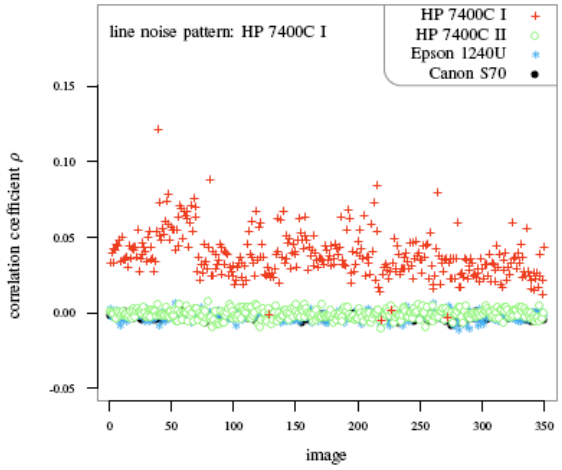

Figure 15: Identification results for HP ScanJet 7400C using 20 black-white-black gradient pictures.

3.2.5 Noise reduction in flatbed scanners

Reconsidering the calibration process inside the flatbed scanner in order to reduce noise, the dependence between scene intensity and correlation to the line noise pattern was investigated. Figure 16 depicts the average correlation for each row in the 20 black-white-black gradient images. In contrast to digital camera identification, where higher intensity results in higher correlation values, the opposite happens in the case of digital flatbed scanners. Apparently, the noise reduction due to the internal calibration process is implemented effectively in brighter areas and leaves analysable traces of sensor noise within darker areas in case of the HP 7400C flatbed scanner. Consequently, corresponding images with a low correlation in Figure 16 largely include dominant bright areas.

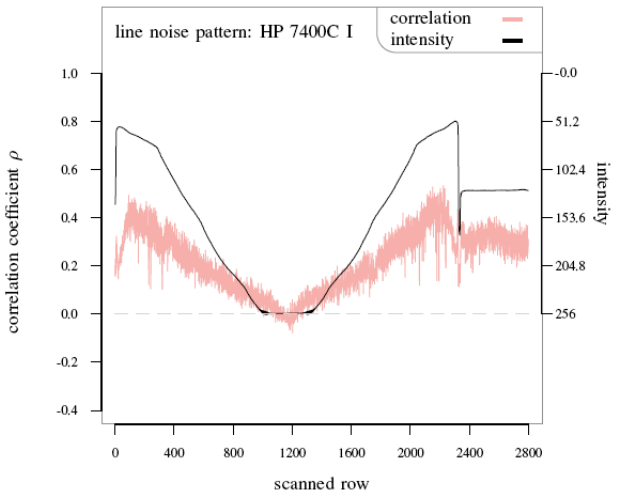

Figure 16: Relation between row intensity (grey) and average correlation (red) for 20 scanned black-white-black gradient images. Spatial noise is better detectable in dark areas.

3.2.6 Conclusion

Current work on source identification of scanned images is motivated by the work in Ref. [4] and focuses on sensor noise [23,41,42]. Reliable methods are known for different flatbed scanners and the use of a black-white-black gradient image can decrease the number of required images for the extraction of a line noise pattern while increasing the true positive rate. However, extended test sets including scanned images of one Epson Perfection 1240U

flatbed scanner showed that the implementation of noise correction methods within flatbed scanners differs between manufacturers. Figure 17 shows the identification results for the Epson Perfection 1240U using 20 black-white-black gradient images, exemplary. In contrast to the Hewlett-Packard flatbed scanner, source identification using the line noise pattern was less successful indicated by a poor true positive rate of 14%. Investigations of the estimated noise pattern suggest a more accurate implementation of noise correction methods in comparison to other flatbed scanners and therefore less analysable traces of sensor noise in images scanned with this device.

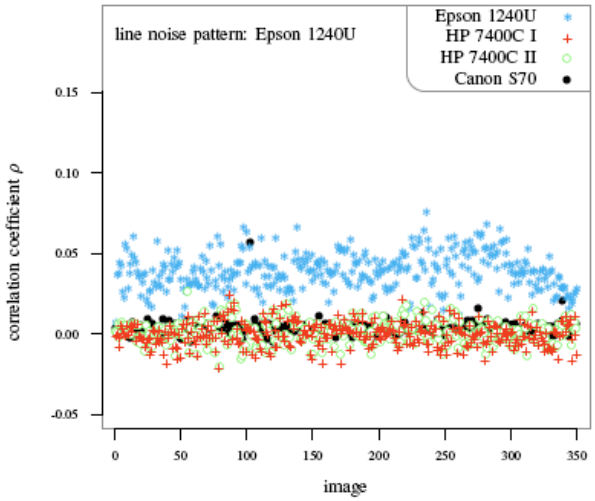

Figure 17: Identification results for Epson Perfection 1240U using 20 black-white-black gradient images.

To enable a reliable source identification of scanned images independent of the manufacturer and the implemented noise reduction processes, further research is needed to create methods that make use of other device-dependent characteristics like local disturbances or aberrations.

3.3 Fusion of characteristics for image source identification

Motivated by differences in the internal image acquisition pipeline of digital cameras, Kharrazi, Sencar and Memon proposed a set of 34 features in order to identify the camera model used for image acquisition [9]. Within this section, key ideas and the performance of the scheme are discussed. Additionally, extensions to improve correct camera model identification in case of JPEG-compression and downscaling as examples of typical image processing operations are introduced and evaluated.

The proposed features capture different characteristics of a digital camera model coarsely and can be classified into three main components: *colour features* describing the colour reproduction of a camera model, *wavelet statistics* coarsely quantifying sensor noise and *image quality metrics* measuring the sharpness and the noise in typically acquired images. As detailed earlier, Figure 18 illustrates the basis of the three components in the simplified model of a digital camera. The used optical system (lens) specifies the quality in reproduction of the scene or, more specifically, the sharpness of the acquired image, which is measured by a subset of the image quality metrics. Sensor noise is caused due to small inaccuracies during the manufacturing process and due to electrical properties of the sensor material. This noise is coarsely quantified by both wavelet statistics and image quality metrics. Generally, the manufacturers specifically fine-tune the components and algorithms used for each digital camera model to create visually pleasing images. Details on this fine-tuning are usually considered as trade secrets. The colour features characterise the camera dependent

combination of colour filter array and colour interpolation algorithm as well as the algorithms used in the internal signal-processing pipeline including, for example, its white-point correction.

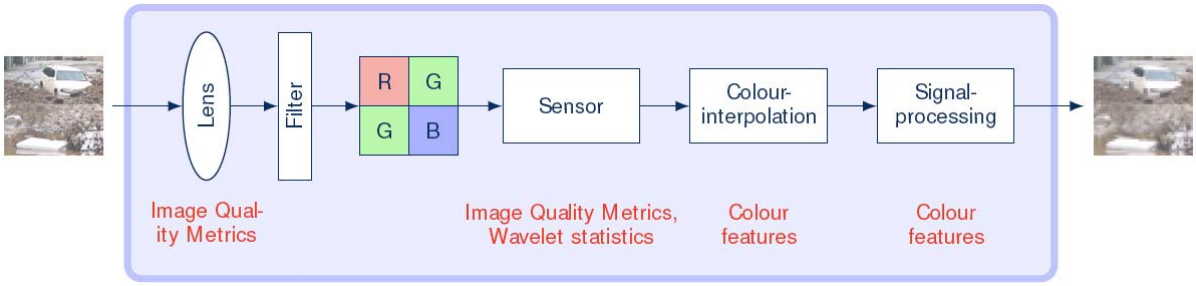

Figure 18: Basis of different device-dependent characteristics proposed by Kharrazi *et al.* [9] classified in the three main components: colour features, wavelet statistics and image quality metrics.

To determine the camera model used for acquiring an image under investigation, a machine-learning algorithm – for example a support vector machine (SVM) [43] – is trained using sets of images of each digital camera model under investigation. Afterwards the trained machine-learning algorithm (classifier) is able to determine the source camera model of an image under investigation by finding the digital camera model with closest match of feature values.

Table 28 shows typical results for correct camera model identification using the method proposed by Kharrazi *et al.* In this scenario, two different sets of cameras were used to evaluate the performance of the method: the first set of camera models includes 3 (Minolta Z1, Kodak DX6340 and Canon HV10) and the second set includes 4 different digital camera models (Minolta Z1, Canon Ixus IIs, Canon Powershot S45 and Canon Powershot S70). About 200 images of different outdoor and some indoor scenes were acquired for each digital camera model under analysis. To train the classifier independently of the scene content, each scene was photographed using each digital camera of one set. The acquired images were split in a set of training and a set of evaluation images with equal size. For unmodified or "original" digital camera images, reliable camera model identification with correct identification rates of approximately 99% are possible. In the case of further image processing, the results are different. While for additionally JPEG-compressed images with a quality factor of 75%, a reliable identification is still possible, reducing the size of an image by downscaling to a width of 1280 pixel, or applying downscaling and JPEG-compression in combination, decreases the success rates considerably (indicated by italics in Table 28).

	First set of cameras (Minolta Z1 / Kodak DX6340 / Canon HV10)	**Second set of cameras** (Minolta Z1 / Canon Ixus IIs / Canon S45 / Canon S70)
Unmodified images	99.2	99.0
JPEG-compression (75% JPEG quality)	96.1	98.6
Downscaling (1280 pixel image width)	93.1	*81.5*
Downscaling and compression	*88.3*	*66.9*

Table 28: Results for correct camera model identification of original and processed images acquired with different digital cameras with the method proposed by Kharrazi *et al.* [9].

To enable a precise camera model identification using the method proposed by Kharrazi *et al.* also for further processed images, additional features were investigated and evaluated. Note that a required property of these additional features is invariance to JPEG-compression and downscaling.

3.3.1 Additional Colour Features

Generally, colour features quantify small differences in colour reproduction of a scene by different digital camera models (exemplarily visualised in Figure 19). They typically remain stable after both JPEG-compression and downscaling. In a first step, the performance of the already known colour features was evaluated, before additional features were investigated.

Figure 19: Small differences in colour reproduction of a scene photographed with three different digital cameras (Casio EX-Z150, Nikon Coolpix S710, Samsung NV15).

To get natural looking images, white-point correction is a very important step in the signal-processing pipeline of a digital camera. The simplest model for white-point correction is based on the grey world assumption [44], where the average of each colour channels is assumed to be equal or generally speaking a grey value:

$$\mathsf{E}(\mathbf{I}_{\mathcal{R}}) = \mathsf{E}(\mathbf{I}_{\mathcal{G}}) = \mathsf{E}(\mathbf{I}_{\mathcal{B}}),$$

where $\mathrm{E}(\mathbf{I}_c)$ denotes the mean of the image $\mathbf{I}$ in colour channel c. To correct an image $\mathbf{I}$ in its colour channels (red, green and blue) using the grey world assumption the following equations are applied:

$$\widehat{\mathbf{I}}_{\mathcal{R}} = \frac{\mathsf{E}(\mathbf{I}_{\mathcal{G}})}{\mathsf{E}(\mathbf{I}_{\mathcal{R}})} \cdot \mathbf{I}_{\mathcal{R}}, \quad \widehat{\mathbf{I}}_{\mathcal{G}} = \mathbf{I}_{\mathcal{G}} \quad \text{and} \quad \widehat{\mathbf{I}}_{\mathcal{B}} = \frac{\mathsf{E}(\mathbf{I}_{\mathcal{G}})}{\mathsf{E}(\mathbf{I}_{\mathcal{B}})} \cdot \mathbf{I}_{\mathcal{B}},$$

where $\hat{\mathbf{I}}_c$ indicates the white-point corrected image.

In their original set of features, Kharrazi *et al.* use only the single mean values of the three colour channels red, green and blue. However, it is important to include the dependencies between the mean values of the colour channels. Therefore, the factors for white point correction and the difference between an original and a white-point corrected image measured by the L_1- and L_2-norm are included in the extended set of colour features.

Table 29 compares the results for correct camera model identification using the original and the extended set of colour features. With the extended set of colour features it was possible to

improve the correct identification rate considerably for two of three cameras sets (indicated by italics).

Colour features	**Set of cameras**		
	Z1 / Ixus IIs	Ixus IIs / S45	S45 / S70
Original set of colour features	76.3	66.8	69.7
Extended set of colour features	76.1	*87.9*	*95.3*

Table 29: Results for correct camera model identification using the original set of colour features and using an extended set of colour features.

3.3.2 Additional Features by Lateral Chromatic Aberration

Digital cameras need a lens (Figure 18) to project a scene on a very small sensor. A perfect projection of the scene on the sensor is virtually impossible and thus aberrations like radial lens distortion, vignetting or lateral chromatic aberration (LCA) occur. Figure 20 depicts colour fringes due to very small differences in the focal length of a lens for different wavelengths, which are known as lateral chromatic aberration.

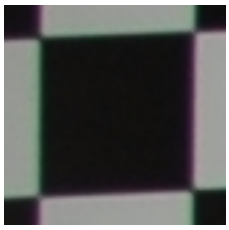

Figure 20: Visible colour fringes in an image due to lateral chromatic aberration.

A typical map indicating the misalignment between the green and red colour channel due to differences in the focal length is visualised in Figure 21 by small arrows for the digital camera Canon Powershot A640. Note that the misalignment due to LCA is radial dependent to the optical centre, which is in most cases unequal to the geometric image centre. In the case of digital camera identification, the lens used determines the occurring lateral chromatic aberration and it is different between most digital cameras models. Considering the fact that a complete reduction of all aberrations is impossible, the use of features based on LCA for camera model identification was investigated and evaluated.

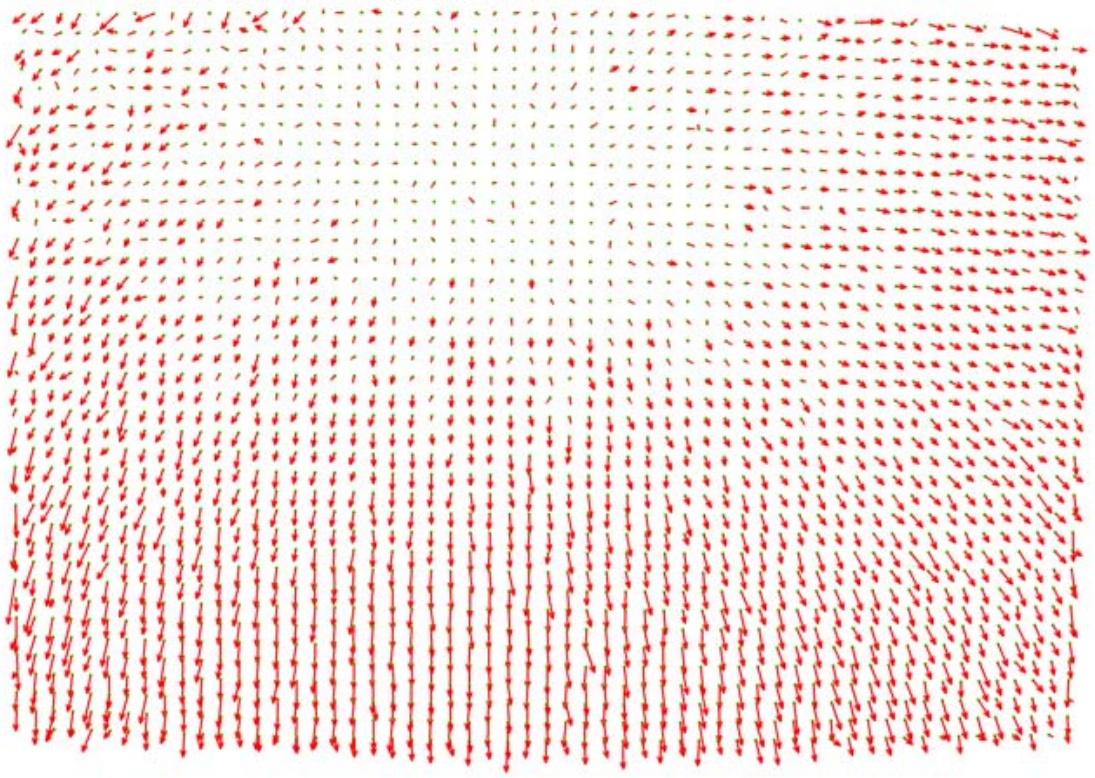

Figure 21: The arrows indicate the shift between green and red colour plane due to lateral chromatic aberration (Canon Powershot A640).

Johnson and Farid first proposed to use lateral chromatic aberration for detecting image manipulations [1]. Their scheme first estimates a LCA model globally on the whole image under investigation and then checks the consistency of the model with the local occurrence of LCA in single rectangle parts of the image. LCA is modelled as an expansion or contraction α of the red or blue colour channel relative to the green colour channel:

$$\begin{pmatrix} \hat{x}_r \\ \hat{y}_r \end{pmatrix} = \alpha_r \begin{pmatrix} x_r - \dot{x}_r \\ y_r - \dot{y}_r \end{pmatrix} + \begin{pmatrix} \dot{x}_r \\ \dot{y}_r \end{pmatrix},$$

where (x_r, y_r) with dot denotes the optical centre, (x_r, y_r) without dot denotes the original coordinates with LCA, and (x_r, y_r) with hat is the corrected coordinates without LCA.

Based on the work of Johnson *et al.* Van, Emmanuel and Kankanhalli propose to use the parameters of the LCA for source identification of images acquired with mobile phone cameras [2]. However, estimating LCA globally is computationally inefficient due to the large number of required interpolation steps during model fitting.

Borowka, Gloe and Winkler propose a computationally efficient method to estimate LCA [45]: First, the image under investigation is divided in equally sized non-overlapping image blocks and second, for each image block, the LCA is measured locally by shifting the corresponding colour planes until the similarity between the colour planes is maximised. To measure the similarity between colour planes, the correlation coefficient is calculated. Based on the estimates of LCA in each block, the global model by Johnson *et al.* and a second order polynomial is fitted. The resulting model parameters (model coefficients, optical centre) are used as features for camera model identification. Generally, not all image blocks are useful to

estimate LCA due to saturation or missing edge information. Therefore unusable blocks are ignored in the model fitting.

Table 30 shows the improved results for correct camera model identification using the set of original and proposed features in combination. In contrast to using the features proposed by Kharrazi *et al.* alone, reliable camera model identification in case of downscaling as well as downscaling and JPEG-compression in combination is now possible for the cameras under analysis.

	First set of cameras (Minolta Z1 / Kodak DX6340 / Canon HV10)	**Second set of cameras** (Minolta Z1 / Canon Ixus IIs / Canon S45 / Canon S70)
Unmodified images	99.7 (+0.5)	99.7 (+0.7)
JPEG-compression (75% JPEG quality)	98.5 (+2.4)	99.1 (+0.5)
Downscaling (1280 pixel image width)	97.6 (+4.5)	96.1 (+14.6)
Downscaling and compression	95.2 (+6.9)	88.9 (+22.0)

Table 30: Improved results for correct camera model identification using the extended feature set (the difference between original results and improved results are provided in brackets).

3.3.3 Conclusion

The scheme for camera model identification proposed by Kharrazi *et al.* works reliably for unmodified or JPEG-compressed images. The presented research results suggest that the use of additional colour features and features based on lateral chromatic aberration enables reliable identification for both downscaled as well as downscaled and JPEG-compressed images.

Within future work, the performance of the camera model identification scheme will be evaluated in a real world scenario using test sets with a large number of devices.

3.4 Methods to detect image manipulations

Image processing toolboxes such as Gimp or Photoshop enable the user to create visually pleasing manipulations, which are in most cases very difficult to detect visually. Automatic methods try to analyse image statistics in order to determine manipulated images. This section briefly introduces some important methods.

3.4.1 Detecting traces of re-sampling

Creating image manipulations by compositing different regions (containing a person or an object) of one or several images typically requires an adjustment in size or alignment using geometric transformations. Geometric transformations like up- or downscaling, rotating or shearing include a re-sampling step to a new image lattice, which typically involve interpolation to calculate missing intensity values.

Figure 22 gives a simple example for re-sampling in case of doubling the image size. Starting with the original image lattice (left part), a new image lattice (centre part) is created by adding

one pixel between each pair of original image pixels. Subsequently, the intensity values of the original image are transferred to their corresponding pixels in the new image lattice (for example $I_{3,3}$ equals $\hat{I}_{5,5}$), and missing intensity values are calculated by using the intensity values of all existing original pixels in direct neighbourhood (in case of linear interpolation, for example $\hat{I}_{6,7}=0.5\bullet(\hat{I}_{5,7}+\hat{I}_{7,7})$).

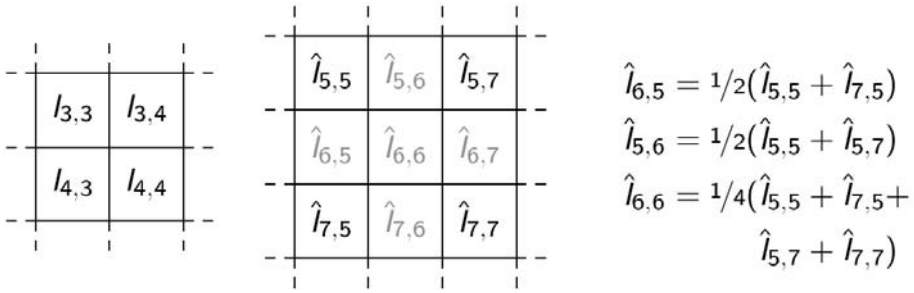

Figure 22: Example for re-sampling – doubling the image size by linear interpolation. The left image shows the original and the right image the resized image grid. Missing values for new image pixels (grey) are calculated by averaging existing intensity values of direct neighbours.

The interpolation step is part of most geometric transformations and causes systematic dependencies between adjacent pixels. Popescu and Farid propose to analyse the statistics of an image to detect these dependencies as an indicator for image manipulations [46]. Therefore, each pixel is modelled as a linear combination of its neighbouring pixels within a window of size NxN and an independent residual. Using the expectation maximisation algorithm (EM-algorithm), the scalar weights for the linear combination of neighbouring pixels and each pixels probability of being correlated with its neighbours is estimated. The probabilities of each pixel result in the so-called "p-map" which directly indicates an applied interpolation.

Figure 23 gives an example for p-maps of original and upscaled images using a factor of 105% and 120%, respectively. Dependencies between neighbours of pixels due to the re-sampling operations cause periodic patterns in the p-map and become visible as strong characteristics peaks in the p-map transformed to the frequency domain using the DFT. Considering the original image, only a low amplitude noise signal appears in the DFT of the corresponding p-map.

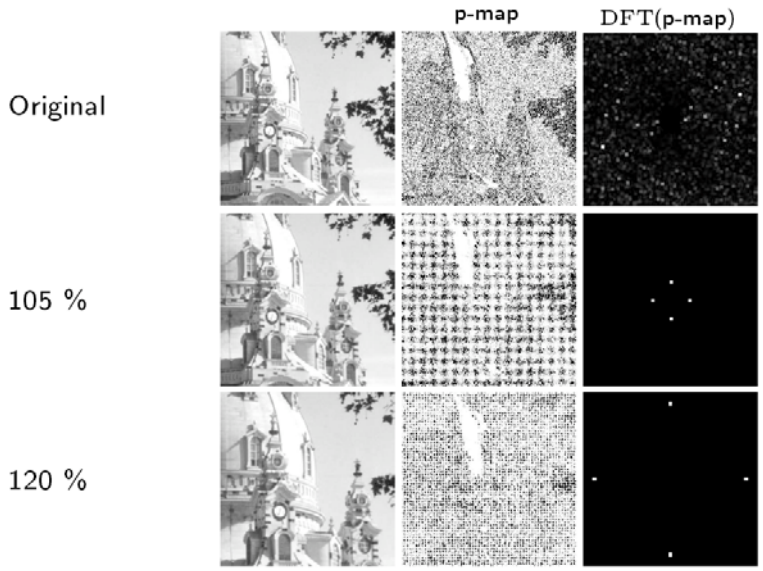

Figure 23: Dependencies between neighbours of pixels introduced due to re-sampling operations like upscaling (here 105% and 120%) cause periodic patterns in the p-map and become visible as strong characteristics peaks in the transformed p-map to the frequency domain (DFT). Note that the DFT of the p-map for an unmodified original image looks very similar to noise and includes only low amplitude signals.

The method proposed by Popescu *et al.* enables reliable detection of re-sampling operations, but is very time-consuming for large images. Kirchner proposes a modification of the algorithm by using only linear filtering instead of the EM-algorithm and demonstrates almost similar results [47]. Furthermore, an exact formulation of how a specific transformation will influence the position of characteristic peaks in the frequency domain was developed. This formulation allows for drawing conclusions on the re-sampling operation applied.

3.4.2 Analysing colour interpolation artefacts

Besides re-sampling operations, colour interpolation applied in most digital cameras includes an interpolation step to calculate missing colour values. In contrast to the strong peaks caused by re-sampling operations, colour interpolation generates peaks with lower amplitude. Popescu and Farid propose to use these artefacts as another component for image forensic toolboxes to detect manipulations [6]. A check for consistent occurrence of artefacts introduced by colour interpolation in blocks of the image enables to detection of image manipulations in digital camera images. Manipulated regions, for example by smearing a region in order to hide an object or a person like in Figure 24, include no colour interpolation artefacts and therefore are detectable. Note that manipulated image regions created by adding a copied region of a digital camera images may preserve the colour interpolation artefacts and may not be detectable with this simple approach.

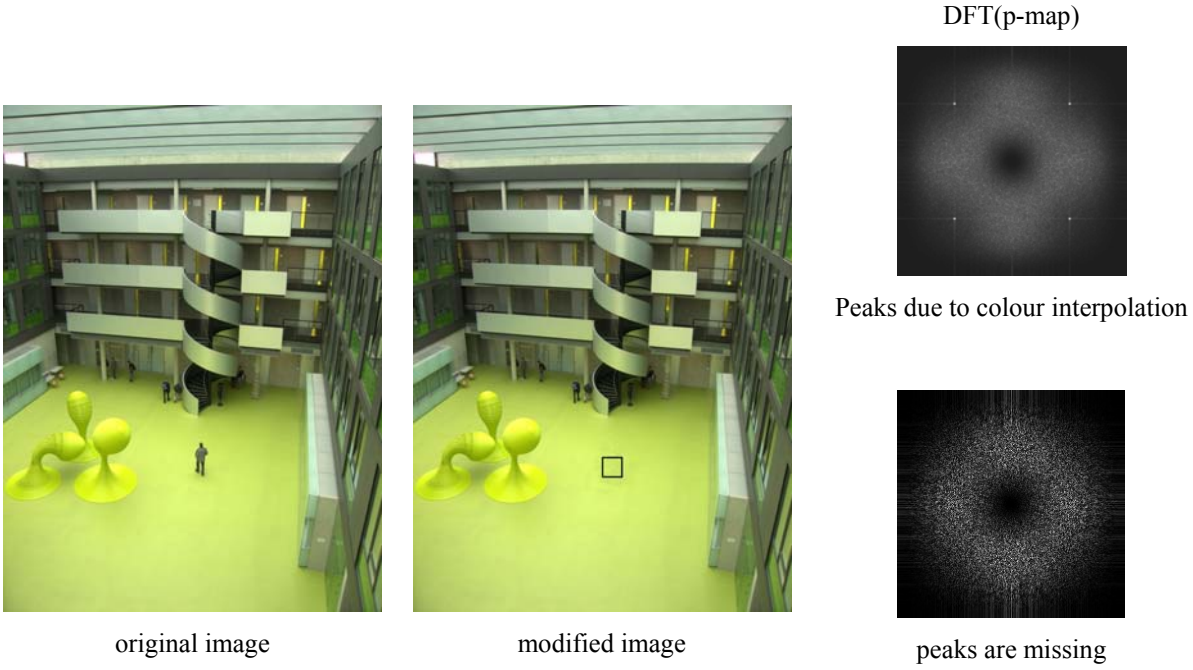

Figure 24: Modifying a digital camera image for example by smearing a region in order to hide a person removes the characteristic peaks due to colour interpolation.

3.4.3 Copy & move forgery detection

In addition to re-sampling operations, copy-and-move operations are typically applied to modify an image. Popecu and Farid propose a runtime efficient algorithm to detect duplicated image regions by calculating the similarity of overlapping blocks of an image [48]. Figure 25 shows the result of an analysis of an image showing an Iranian rocket test, which was distributed by the government of Iran. The white areas in the generated map indicate duplicated image regions.

Figure 25: Copy & move forgery.

3.4.4 Detecting inconsistencies in lighting

Another very important technique proposed by Johnson and Farid analyses the consistency of lighting in a scene [49,50]. The algorithm estimates the direction of light at the border of

objects. While the estimated light direction is similar for all parts of an unmodified image, differences may be detectable between objects of a composite image.

Figure 26 shows an example for the estimated light directions of an unmodified image and a known forgery [50]. The unmodified image was taken at a meeting of Richard Nixon and Elvis Presley and the estimated light directions are similar. On the contrary, in case of a known forgery showing John Kerry and Jane Fonda, the estimated light directions differ.

Figure 26: For unmodified images, the estimated light directions are similar within one scene (left figure showing Richard Nixon and Elvis Presley), while in case of manipulated images, inconsistencies in lighting can be detected (right figure showing John Kerry and Jane Fonda) [50].

3.4.5 Conclusion

Today's image manipulation toolboxes enable advanced users to create visually pleasing and authentic looking images. Tampering with image content introduces manipulation artefacts, like duplicated image regions, or inconsistencies in device-dependent characteristics, like disturbance of colour interpolation patterns. These and other traces form the basis for different state-of-the-art image manipulation detectors and were exemplarily discussed within this section. While the results for forgery detection are promising in laboratory tests, further investigations for their application in practice are necessary. For example, the analysis of re-sampling artefacts works very well for uncompressed images or images compressed with a high JPEG-quality factor, but the detection accuracy decreases considerably with lower JPEG-quality factors.

4 Robust image recognition algorithm

4.1 Introduction

Some existing forensic tools allow a fast recognition of known illegal pictures on a hard disk. Most of the time, these tools are based on a cryptographic one-way hash function (typically the MD5) that generates a hash value for any image. The hash value is then used to identify the image; it plays the role of a "fingerprint" for the image.

With such a method based on a cryptographic one-way hash function, a small transformation applied to an image will change its hash value drastically. We will present recent results of ongoing research the objective of which is the development of a more robust recognition algorithm. This new algorithm should be able to cope with the deformations commonly applied to images, so that the fingerprint of an original image often corresponds to the one of the transformed image. We have focused our research on the use of information contained in the histogram of an image. The algorithm consists in a series of operations on the histogram itself in order to extract relevant information that allows a robust comparison of images.

As we mentioned before, a one-way hash function, such as MD5, fails to recognise two slightly different images. In fact, even a seemingly negligible change in an image leads to a completely different hash value. For example, if only one pixel in an image is altered, the consequence is a new hash value which looks random in comparison to the original one.

Using current technology, it is now possible to apply automatically a series of treatments to a large number of images in a minimum time. Thus, it is easy to bypass the MD5 hash identification. It becomes easy for a person possessing a large collection of illegal pictures to remain completely undetected.

One-way hash functions are usually used in other contexts where they must meet certain specific characteristics. Not all these requirements are needed in the context of image recognition. For example, the one-way property: it is unfeasible to generate an image that hashes to a particular value. This characteristic is not necessary in our context because there is no reason for a person to risk being suspected of possessing illegal images. On the other hand, efficiency is an important property in our context too.

These thoughts do not question the current use of MD5 in a forensic context, because it has proven its effectiveness on many occasions. Our point is to show how to circumvent some of its potential weaknesses, in case people start to systematically modify images before storing them on their computers. To this end, we describe in the following the first version of an algorithm that calculates a robust fingerprint that most of the time allow the recognition of two slightly different images.

4.2 Algorithm

The first step of the algorithm consists of extracting the three colour layers of the image (red, green, blue). If the image is greyscale, there is only one layer. Then, we compute the histogram for each layer. Some image modifications, such as adding a border or making a rotation, have the effect of massively adding a specific colour to the image. These colours are often black or white, that is why we ignore those intensities[10] in order to obtain a histogram

10 Intensities 0, 1, 254, 255 are removed

which is less sensitive to such changes. If there is massive addition of another colour, the algorithm simply replaces it by black. For example, the figure below shows a histogram with massive presence of an intensity which is due to the addition of a specific colour border. The result is a huge peak that completely changes the appearance of the histogram. The algorithm detects the presence of such oversized peaks and replaces the corresponding intensities by black, which means that the value of this intensity will be ignored eventually.

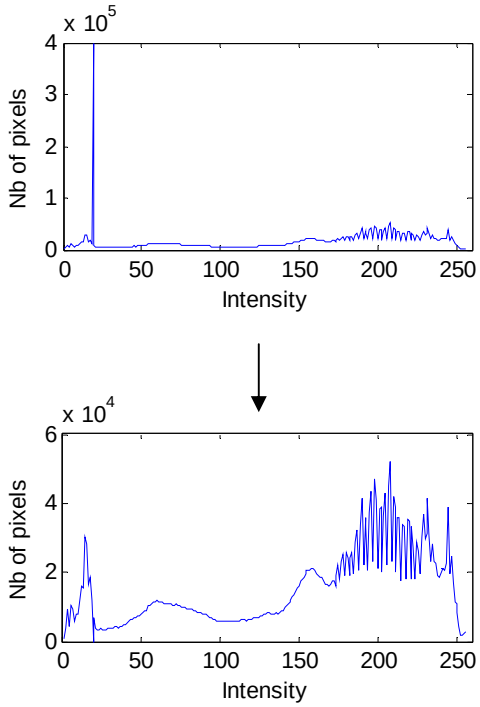

Figure 27: Suppression of oversized peaks[11]

The algorithm continues until there are no oversized peaks to remove anymore. Then, it adds up the three histograms to create a RGB histogram.

The next step consists of smoothing the curve of the histogram in order to make it more resistant to small image modifications. Each value is recomputed taking into account its neighbours. We chose to consider five neighbours on the right and five on the left. Figure 28 shows the smoothed version of the original histogram depicted in Figure 27.

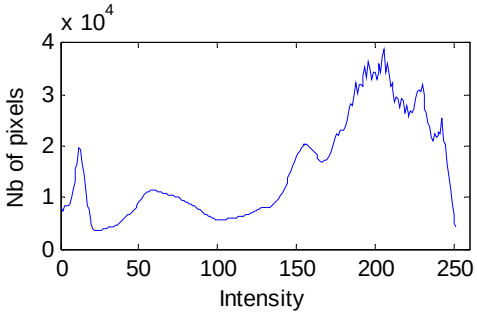

Figure 28: Smoothed histogram

[11] Peak in 0 (black) is voluntarily not represented.

At this stage, the histogram is cut in to eighteen sections, each containing fourteen values[12] of the histogram. For each section, we calculate three variables: the sum, the maximum and the minimum. We record these values in three vectors of size eighteen: the first one gathers all the sums, the second one all the maxima and the third one all the minima.

Then, we introduce the robust component of our transformation: for each of the three vectors, we calculate its corresponding "rank vector". This consists of storing the index of values sorted in increasing order. The first component of the rank vector corresponds to the index of the smallest value in the original vector; the last component of the rank vector corresponds to the index of the largest value in the original vector. As an example, we take an original vector of four values:

Index	1	2	3	4
Original vector	86	45	23	64
Rank vector	3	2	4	1

Table 31: Calculation of a rank vector

The minimum value in this original vector is 23, its third component. The index 3 is therefore the first component of the corresponding rank vector.

Rank vectors constitute the core components of our robust fingerprints. In a first implementation, an image was considered equivalent to another one when at least one of the three rank vectors of this image was identical to the corresponding rank vector of the other one. We noticed that the rank vectors of slightly modified images often tend to switch two values with respect to the rank vectors of the original image. Therefore, we decided to loosen the equivalence definition and to store not only the three basic rank vectors, but also all rank vectors that can be generated with a switch of two neighbouring components.

In doing so, we generate seventeen new rank vectors for each of the three basic rank vectors. In the end, a robust fingerprint consists of three groups of eighteen rank vectors.

4.3 Current results

We have been doing two types of tests. The first one estimates the false non-matching rate, i.e., the false rejection rate (FRR); the second one estimates the false matching rate, i.e., the false acceptance rate (FAR).

For the estimation of the FRR, we applied some basic transformations to a group of one hundred images[13] and we counted the number of modified images which did not match with the original ones anymore. The following table summarises the results:

[12] The histogram has 252 values because we removed black and white (0, 1, 254, 255). Each section has 252/18=14 values.
[13] All the tests were realised with jpeg pictures

Type of modification[14]	% FRR
Adding a black text	0
Adding a red text	1
Adding a black border	0
Adding a red border	0
Rotation of 5%	2
Adding a coloured border and a coloured text	12
Reduction of the size	10

Table 32: Results FRR

As we can see, the algorithm is generally able to link a modified image with the original one. When we combine two basic transformations, we see that the ability of the algorithm to recognise the image decreases. The results for the last modification (reduction of the size) could be explained by the fact that the jpeg lossy compression has a stronger impact on small images.

In order to estimate the FAR, we have selected several themes, and for each of them, we downloaded one hundred images from Google Image Search. We ran the algorithm on all images of each theme, and we counted the number of false matches. Table 33 summarises the results.

Although the number of tested images is relatively small[15], the results that we obtained are promising.

Theme	% FAR
Taj Mahal	0
Statue of Liberty	1
Random faces	1
Eiffel tower	2
Famous actor 1	3
Famous actor 2	0
Famous actress 1	1
Famous actress 2	2

Table 33: Results FAR

In addition, we found that each false match in the above table is due to "low key"[16] images. Indeed, such images lead more or less to rank vectors composed of the values of eighteen to

[14] Texts are added in the original pictures; pixels of the original pictures are replaced. Borders extend the original images.
[15] The algorithm is not yet optimised for analysing a large number of images
[16] Images where most of the tones occur in the shadows are called "low key"

one in decreasing order. If most of low key images lead to this type of rank vector, there is no possible discrimination between them. The simple method consisting of extending the lower part of the histogram onto a "normalised" histogram decreases the FAR for "low key" images, but seems to increase the FRR for other pictures. This is a point that needs to be studied further and improved if possible: Which normalisation is the best? Should we separately normalise each colour layer? Should it be applied to all images or only to "low-key" images? In the latter case, what is the optimal threshold for an image to be considered as a "low-key" image?

We also found that the last five components of rank vectors are very stable when an image is modified. They correspond to the intensities which are the most frequent in the image, and those intensities are less sensitive to small modifications of the image. We believe that this aspect should be developed further to try to improve the accuracy of the algorithm further.

4.4 Conclusion

The first milestone of this ongoing work was to create a proof of concept of an efficient algorithm capable of linking two slightly different images through a robust fingerprint. As we have seen, we consider that current results are promising. They confirm that we should continue our research in order to create an efficient forensic tool that could circumvent expected future behaviour of people storing illegal, slightly modified pictures that they have gathered.

5 Facial comparison by man and machine

5.1 Introduction

Due to the growing number of security cameras, the number of crimes in which facial comparison plays a role is increasing. In general, people are thought to be reasonably good at recognising faces. However, although research indicates that recognition of "familiar" faces can be extremely efficient, even with disguises and poor-quality images, this does not apply to recognition of "unfamiliar" faces [51,52]. Data on human performance are limited, especially on the performance and reproducibility of "forensic facial comparison experts". Additionally, human observers may suffer from bias during the subjective assessment of images. Automated facial comparison and recognition may provide support to the difficult task of unfamiliar face recognition. A major advantage of automated systems is that they operate objectively. However, automated facial comparison and recognition also still function far from optimally. Especially in uncontrolled circumstances, like surveillance, the performance is known to be poor, and highly dependent on pose and position, lighting and facial expression. This chapter will discuss the current status of automated biometric face comparison, compared to the performance of humans untrained and trained to perform facial comparison.

Within the context of person identification, different processes can be defined: (a) recall, 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, (b) recognition, 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 and (c) comparison, defined as the process of identifying or matching a person or his/her image with another photograph or image without the use of retained information. For comparison, as discussed here, retention and reproduction do not play a role and only the matching process is of importance.

5.2 Face comparison by man

As a measuring instrument, humans are not good at assessing facial features in which sizes and proportions play a role [53]. The evidential value of sizes and proportions in visual material is also limited because of the image distortion caused by unknown camera equipment, unknown zoom settings, and unknown pixel aspect ratios of digital cameras. Not every human observer assesses the differences in shapes of facial features in the same way either [54,55]. In addition, people are not very consistent in the assessment of similarities between pairs of photos [56]. In an experiment using credit cards with a small (2cm x 2cm) colour photo on the back of the card, it was shown that untrained people rejected 7-14% of the cards carried by legitimate holders, while 34-64% of the cards carried by a different holder were accepted, depending on the 'likeness' of the false bearer. In total only about 67% correct decisions were made [54]. In an experiment with face pictures taken under different lighting condition, shown on computer screens, an Equal Error Rate (EER) of about 8% was found when 'easy' image pairs were used, and about 15% when 'difficult' pairs were used [57].

The few experiments described above were performed using full frontal photos, examined by untrained people. Even less is known about the performance of trained people, considered by themselves or others as facial comparison experts. A small test comprising of one person who had performed as facial comparison expert witness, a comparative scientist, a scientist not

used to image comparison and a lay person, showed that, using difficult photo pairs (document quality) from different people, the lowest number of correct answers was given by the expert (11%), and the highest number by the comparative scientist (89%). The highest number of wrong answers was given by the lay person (53%) followed by the expert (37%), with both scientists giving 11% wrong answers. The expert responded the most often with 'inconclusive' (53%), while the comparative scientist and the lay person always gave a conclusive statement. These data suggest that a scientific background and training or talent to judge image material, may be helpful for performance, but certainly is no guarantee.

To further study the performance of people performing forensic facial comparison, we developed a ring test which was performed by members of the Digital Imaging Working Group of the European Network of Forensic Science Institutes (ENFSI) and other facial comparison experts. The test[17] comprised five sets with one query and seven target images, all to be compared with the query image. All images were frontal, and the image quality of the query image was 'surveillance quality'. The test was performed two times by eleven people, both resulting in 1-5 errors in four out of the five sets, errors being made by 6 out of the 11 investigators. Considering all comparisons that were made by all contributors, these tests resulted in an error rate of about 2% for these investigators, which is considerably lower than the error rates determined in the previous experiments.

5.3 Face comparison by machine

Automated facial comparison and recognition still is not functioning optimally. The best systems have a verification equal error rate (EER) of about 5%, and a false reject rate (FRR) of about 10% at a false accept rate (FAR) of 1% if "document quality" images under controlled lighting conditions are used [58]. The facial recognition systems are still sensitive to aging of the subjects: the FRR increase to about 20% at an FRR of 1% if the picture is 3 years old [59].

Looking at the performance of facial biometrics systems for investigational purposes of criminals or terrorists on a watch list (identification), the best systems find about 60% of the suspects on a list of 1000 people at a setting, resulting in 1% false alarms [59].

Note that these results are based on experiments with standardised high to medium quality pictures from collaborating subjects. The performance of biometric facial recognition systems decreases quickly with changes in pose and position, lighting, and facial expression. Tests using a well performing automated system (own experiments) resulted in an EER of 1.5% when using only frontal images. The performance dropped to an EER of 11% when using only left or right ¾ images, and it dropped to an EER of 24% when using frontal and ¾ images in combination. Surveillance images taken under uncontrolled circumstances, using standard quality cameras mostly placed in conspicuous places (high at the ceiling, low at automatic teller machines (ATMs), "hidden" at the side of entrances) and recording people who do not look into the camera, with changing expression and sometimes partly covered faces, are hardly or not at all recognised by biometric systems.

When using the above automated system, frontal surveillance images of people at about 2m distance resulted in an EER of about 12%, rising to about 40% at 4m distance.

The above mentioned performance was tested using 'document quality' frontal database images. As mentioned before, pose and position of the image largely influences the

[17] Presented at Biometrics 2008, London, 21-23 October 2008

performance of biometric systems. Using a database with images from the same angle as the test images did improve the performance of the automated system significantly.

Under uncontrolled conditions, including large illumination variations, complex and moving foreground and background, partial or total occlusions, the performance of face detection techniques is also substantially reduced with a tremendous effect on face recognition results, as the output of the first step (face detection) is one of the main inputs for the second one (face recognition). For this reason there is ongoing effort on improving background extraction and face detection techniques, but also enriching the recognition task with other bodily parts.

POLYMNIA was a system developed for the POLYMNIA project [60] under the fp6 European framework, aiming at delivering an intelligent cross-media platform for the production of custom video souvenirs for visitors to leisure and cultural heritage venues. An issue in the POLYMNIA real-time human recognition system had been the combination of face and body recognition results so as to achieve higher recognition rates for the entire system. For this reason, initially the results of the face and body recognition based on the recognition rate were ordered producing a ranking list of identified persons based on face recognition and based on body recognition. From this list only the best five results of each recognition method which exceeded an experimentally pre-defined threshold value were further used. The recognition rates of the face and body recognition were then summed up if a person could be found in both of these ranking lists. The highest sum value was then selected to select the identified person. Evaluation results showed that recognition rates of up to 90% could be reached in the POLYMNIA system. [61] When the above technique is applied in long term applications during which there can be bodily variations of the humans, it can be transferred one step earlier at the human detection step, improving significantly the results of the face detection techniques and thus providing more accurate input to the face recognition system. In [62] researchers aimed at improving face recognition by processing the colour information in the images and making an effort to find an optimal way to represent colour images for the recognition processing. The proposed models and algorithms were evaluated using the face recognition grand challenge (FRGC) database and the biometric experimentation environment (BEE) system and more specifically the FRGC Experiment 4, designed for indoor controlled single still image versus uncontrolled single still image. It should be noted that FRGC comprises one of the most comprehensive face recognition efforts and it consists of a large amount of face data and a standard evaluation system; the BEE system [63]. With the Experiment including 12776 training images, 16 028 controlled target images, and 8014 uncontrolled query images, the proposed method achieves the face verification rate (ROC III) of 78.26% at the false accept rate (FAR) of 0.1%.

5.4 Man versus machine

Current data show that when using frontal images of ‘document’ quality with changes in illumination, the performance of biometric systems is similar to or even better than the performance of untrained people [57,58]. Although there is some indication that trained people perform better, hardly any data concerning the performance of facial comparison experts are available. When the pose of the face is such that both eyes of the subject cannot be detected, the biometric systems will fail: all current systems need to locate the eyes to position the face for the comparison algorithms. As this is regularly the situation in surveillance material of crimes, currently biometric systems cannot be used for most forensic material. Current practice at the Netherlands Forensic Institute (NFI) is to make reconstruction images with suspects if possible, for manual comparison by experts. However, experience has taught

us that the suspects need to be cooperative to succeed in making useful reconstruction images. Current research is geared towards using 3D scans of the suspects, or 3D models of the perpetrators, to overcome pose and positioning issues.

5.5 Summary

The facial comparison performance of humans is not as good as we might think, certainly not 100% correct 100% of the time, even when experts are involved. The performance of current machine algorithms using frontal images can be as good as or even better than humans. However, pose and image quality are important challenges for man and machine; machine algorithms fail if the eyes are not visible. Current researches into 3D techniques to overcome pose and position issues are most promising for performance improvement.

6 Ensuring the evidentiary value of images in criminal proceedings

6.1 Introduction

The Internet is a valuable tool that many law enforcement agencies are progressively taking advantage of to find and catch criminals. Lately, the press unveiled several examples of criminal evidences being collected via the Internet and that have permitted prosecution of criminals.

Such is the case for instance of a 23-year-old from Swarcliffe (UK) who was banned from Google's video sharing service *YouTube* after having posted numerous clips, most of them reportedly illegal. According to Web User News, the *YouTube* user uploaded no less than 80 videos on the website, one of them showing him '*being driven in a car at more than 140 mph.*' [64], taking narcotics, insulting people, and not paying a taxi driver. Other examples includes the release of a photographed copy of the final book of Harry Potter four days before it was released in bookstores that was made available via Bit Torrent to the fans. The editor was then threatening to identify the author of the 'crime' thanks to the metadata left by its camera.

By the same token, the information posted on online networks is increasingly being used by police officers to search for the perpetration of crimes or offences [65]. A US press release dated from 2007 describes how a 22 years-old police officer surfs social networks to find out about offences or crimes. The press release refers to a ruling of the Arizona's Pima County Superior Court where a prosecutor used pictures from a suspect's *MySpace* page as evidence after he was accused of holding up a student with a Tec-9 semiautomatic handgun in June. The 19-year-old's *MySpace* page had pictures of him holding a gun that looked a lot like a Tec-9. The suspect pleaded guilty to aggravated assault with a deadly weapon and was sentenced to five years in prison. Another police officer, who uses the sites to find information about students he is investigating, is reported to say that students are usually surprised to learn that he found incriminating photos or information online. The article concludes stressing that '*Facebook.com and MySpace.com are the newest crime-busting tools in a police officer's repertoire, particularly for campus police, who are using the sites to investigate student crimes and violations and gather information about where students live and whom they know. In some cases, the information they find is making its way into court*'. Most recently, the Belgian press unveiled recent practices of tax officers asking to be marked as 'friends' on *Facebook* accounts of the persons under investigation in order to collect information about their way of life and compare it with their tax declaration [66].

Finally, an initiative from the Greater Manchester Police force in the UK should be mentioned. As reported by *ITWorld*, this police force has created a *Facebook* application to collect leads for investigations, marking the first use of the social networking site by UK law enforcement. The application delivers a real-time feed of police news and appeals for information. Next to that content is a feature to share a particular story with other friends in a person's network, as well as post comments. A "Submit Intelligence" link takes a *Facebook* user to the police Web site where they can anonymously submit tips. Another link leads to the videos on *YouTube* featuring information on the police force, ongoing investigations and other advisories [67].

These examples show how law enforcement authorities are increasingly making use of the Internet and more specifically of online networks websites to gather relevant information for their investigations. The search for specific individuals in images posted on the Internet is moreover expected to be facilitated by specific search engines as the one launched by Viewdle.[18] Questions thus arise about the very nature of the images posted on the Internet as regards the traditional categories of criminal law and which safeguards should apply to their collection and use by law enforcement authorities. In particular, the question whether specific guarantees attached to the protection of the home or correspondence should apply to searches and seizure through private accounts should be dealt with. This chapter will first recall the general rules applying to the collection of electronic evidence before entering into the specific issues raised by the collection of images posted on the Internet for law enforcement purposes from a privacy standpoint.

This chapter will also deal with another and more specific field of digital forensics, related to image enhancement. Forensic uses of digital imaging are increasing in recent years [68]. Not only can digital images be acquired from routine crime scenes using digital cameras in order to enhance images and extract and reveal details that may not be seen in the original, but the topic of the authenticity of images, including detection of digital forgeries is becoming central. The digital image also lends itself to computer manipulation to 'enhance' the visibility of details. It is not always clear what constitutes enhancement and what may verge into the area of improper manipulation that can distort or introduce information. Some considerations will be included at the end of this chapter. The collection of images (videos or pictures) can respond to several purposes such as the identification and recognition of individuals or the evidence of facts.

6.2 Electronic evidence gathering in criminal investigations

Evidence is the means by which factual ingredients of an offence (because of which proceedings are started) or a civil litigation can be proved, in order to succeed [69]. In particular '*computers and the various media in which computer-generated information is stored, provide a unique window into company's or individual's correspondence, data, statistics… and generate, sort and store huge amounts of information, while providing a source of information that may not exist in paper form.*'[69].

In order to be able to submit an image before a Court as evidence, this image has to have all attributes of conventional evidence, meaning that it must be [70]:

- *admissible*, i.e. it must conform to legal rules to be put before a court. This relates to the validity of evidence brought before a court.
- *authentic*, i.e. it should be possible to positively tie evidentiary material to the incident.
- *complete* (as much as possible)
- *reliable*, i.e. there must be nothing about how the evidence was collected and subsequently handled that casts doubts about its authenticity and veracity.
- *believable*, i.e. understandable by a Court.

[18] This search engine aims to identify individuals whose pictures are stored on a database on any image. For more information see: www.viewdle.com

Most criminal laws in many countries are based on express provisions of specific coercive powers and differentiate the following issues: the possibilities of monitoring publicly available facts, the powers of entry and search of premises, the power of seizure and retention, the duty of witness to testify, the duty of witnesses to surrender existing means of evidence and the powers of wiretapping [69].

Two aspects will be focused on in the following two sections, namely: the powers of entry and search of premises and the power of seizure and retention. Whereas it is not possible in this deliverable to provide an analysis of the national differences about freedom or restriction of the types of proof, in particular about the manner and procedure for submitting evidence or the weight of evidence, this chapter will focus on a series of legal provisions that could influence the admissibility of the evidence when it comes to images, namely with the right to privacy, based on the case-law of the European Court of Human Rights (ECHR).

6.2.1 The Convention of Cybercrime: introduction of specific rules for the collection of electronic evidence for criminal law enforcement

The Convention on Cybercrime has tried to tackle the issue of collection of evidence in electronic form of a criminal offence and more specifically the search and seizure of stored computer data.

Article 19 is explicitly dedicated to the latter issue. The explanatory report clarifies that this article aims at modernising and harmonising domestic laws on search and seizure of stored computer data for the purposes of obtaining evidence with respect to specific criminal investigations or proceedings. The report stresses that whereas any domestic criminal procedural law includes powers for search and seizure of tangible objects, in a number of jurisdictions stored computer data *per se* will not be considered as a tangible object and therefore cannot be secured on behalf of criminal investigations and proceedings in a parallel manner as tangible objects, other than by securing the data medium upon which it is stored. The aim of Article 19 of this Convention is thus to establish an equivalent power relating to stored data.

The report furthers describes the issues raised by the search and seizures of electronic evidence. In that sense, it is stated that in the traditional search environment concerning documents or records, a search involves gathering evidence that has been recorded or registered in the past in tangible form, such as ink on paper. The investigators search or inspect such recorded data, and seize or physically take away the tangible record. The gathering of data takes place during the period of the search and in respect of data that exists at that time. The precondition for obtaining legal authority to undertake a search is the existence of grounds to believe, as prescribed by domestic law and human rights safeguards, that such data exists in a particular location and will afford evidence of a specific criminal offence.

With respect to the search for evidence, in particular computer data, in the new technological environment, many of the characteristics of a traditional search remain. For example, the gathering of the data occurs during the period of the search and in respect of data that exists at that time.

It is worth noting that this explanatory report recalls that the preconditions for obtaining legal authority to undertake a search remain the same as for the collection of 'material' evidence. The degree of belief required for obtaining legal authorisation to search is not any different whether the data is in tangible form or in electronic form. Likewise, the belief and the search

are in respect of data that already exists and that will afford evidence of a specific offence. The concern of the Convention is not thus to draw new safeguards with regard to the characteristics of the search warrant but rather to ensure that the required procedural provisions are introduced in the legislations of the Contracting States tending to ensure that computer data can be obtained in a manner that is equally effective as a search and seizure of a tangible data carrier.

It follows that whereas Contracting Parties are compelled to adapt their legal framework to enable or facilitate the collection of electronic evidence, in particular of stored data (Article 19) but also for the real-time collection of computer data (Article 21) either directly or via the intervention of Internet Service Providers, these new powers and procedures granted to law enforcement authorities should remain subject to the safeguards provided for under domestic law, in particular with regard to the protection of human rights and liberties, including those defined by the European Convention on Human Rights (Article 15.1). The explanatory report specifies that the powers and procedures shall incorporate the principle of proportionality. Proportionality shall be implemented by each Party in accordance with relevant principles of its domestic law. For European countries, this will be derived from the principles of the European Convention on Human Rights, its applicable jurisprudence and national legislation and jurisprudence. The power or procedure shall be proportional to the nature and circumstances of the offence. Finally, such safeguards and conditions should moreover, as appropriate in view of the nature of the procedure and power concerned, *inter alia*, include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure (Article 15.2).

This is particularly relevant with regard to the conditions surrounding search warrants. When interfering into fundamental rights, such as the right to privacy, such warrants usually have to be issued by a judicial authority which will have to make the balance between the different interests at stake and provide for specific and limited authorisation to the police. These guarantees act as safeguards against abuses. It is thus necessary to define whether and how such safeguards could be applicable to the collection of information on the Internet for evidentiary purposes.

6.2.2 Searches and seizures and the right to privacy

The start of a criminal investigation is often linked to restriction in the exercise of rights guaranteed by Article 8 of the European Convention on Human Rights. Such interferences should be based on one of the derogations admitted under this article, i.e. on the need and prevention of crimes and offences and the investigation of authors' identity and facts. Specific procedural safeguards, such as the supervision by a judge and the limitation of the warrant issued should be present.

6.2.2.1 Admitted interferences into the right to privacy

Article 8 of the European Convention on Human Rights states that:

> *'1. Everyone has the right to respect for his private and family life, his home and his correspondence'.*

Limited derogations are admitted to these rights as defined by the Convention under Article 8.2 that stipulates that:

> *'2. There shall be no interference by a public authority with the exercise of this right except such as in accordance with the law and is necessary in a democratic society in*

> *the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedom of others.'*

It is thus first necessary to define when a search will interfere with the rights protected under Article 8.1 before assessing whether it falls under one of the derogations of Article 8.2. To that effect, an overview of the relevant case-law of the ECHR appears to be sufficient for the purpose of this deliverable.

When it comes to searches and the documents seizures that go with it, all the rights guaranteed under Article 8.1, except the right to family life, can be challenged (ECHR, Funke, 1993 §48 [71]). The Court has adopted a broad concept of the right to privacy and has extended accordingly its scope of protection. The mere consultation of files by itself - without any seizure - qualify as an interference (ECHR, Niemietz, 1992, §11 and 32 [72]). With regard to the interpretation of 'home', the Court does not only include private but also professional premises within the scope of the protection. The correspondence protected is not limited to private document exchanges (ECHR, Niemietz, 1992, §32 [72]) and includes commercial correspondences as well (ECHR, Miailhe, 1993, §28 [73]). In that sense it is worth noting that the text of Article 8.1 ECHR does not limit the protection to private correspondence but includes any type of 'correspondence'.

Once the practice of search and seizure is identified as interference into the right to privacy, the law enforcement authority should base such intrusion on a legitimate ground. With regard to the justification of the interference, the Court accepts multiple grounds: Prevention of crimes in order to identify the author of a criminal act (ECHR, Niemietz, 1992, §36 [72]), protection of right of others when the search seeks to grasp the results of an infringement to copyrights (ECHR, Chappell, 1989, §51[74]), or to protect the economic wellness of the country when collecting evidences of fiscal, customs or change-control offences (ECHR, Funke, 1993, §52 [71]). The searches and seizures within a criminal investigation are thus largely covered by the derogation of Article 8.2 ECHR.

The Court will then check whether adequate safeguards surround the search. Such safeguards should be sufficient as to prevent abuses and to ensure that they are strictly proportionate to the goal foreseen (ECHR, Funke, 1993, §57 [71]). The Court identifies such safeguards in the concretion of the search mandate issued and the presence of an advisor or at least an independent observer (ECHR, Chappell, 1989, §§59-66 [74] for compliance with such requirement; ECHR, Niemietz, 1992, §37 [72] for a case where such safeguards were lacking). The mandate should have a judicial nature, in other case, the administrative authorities would have the power to assess by themselves the opportunity, number, duration and scope of searches which would annul other safeguards that could be established (ECHR, Funke, 1993 [71]; *ECHR,* Crémieux, *1993 [75];* ECHR, Miailhe, 1993, [73]). The lack of judicial mandate is considered as the determinant cause of the insufficiency of safeguards (ECHR, Funke, 1993§57 [71]) and of the excessive nature of the search (ECHR, Miailhe, 1993, §39 [73]).

6.2.2.2 Consequence of a breach of Article 8 of the European Convention on Human Rights on the admissibility of the evidence before Criminal Courts

If the evidence were to be collected in violation of the right to privacy and thus of the provisions of Article 8 of the European Convention on Human Rights, it raises the question whether this would lead to its discarding during the trial.

As mentioned in [69], *'in order to avoid polluting the evidence, the gathering, conservation, communication and presentation of the evidence must fulfil legal requirements with regard to the admissibility of the evidence'*. Infringing these requirements would compromise the evidence eventually leading to it being discarded. He also points out that on the one hand, issues related to the admissibility of evidence should be distinguished from question relating to the relevance of the proofs, and on the other hand that inadmissible evidences could be more prejudicial for the whole judicial process insofar as they can pollute subsequent actions than no evidence at all.

In [69] O. Leroux distinguishes Common Law from continental law systems. In the former, such as the English system, *'the violation of evidence rules does not prevent the accusation from producing the litigious proof; but the court retains the discretionary ability to accept it or to refuse it'*. On the contrary, in continental law systems such as French inspired ones (e.g. Belgian and Italian) *'inadmissible evidence must be declared null and void; the nullity of subsequent procedure could be implied from inadmissible evidence'*.

In criminal cases, continental countries operate according to the principle of free introduction and free evaluation of evidence. It means that in such cases, every means of proof is in principle permitted as far as it is gathered according to specific rules and respecting general principles of law [69].

However, Common and Continental Law had brought their positions closer. In the UK, as stressed in [76], since the enactment of the Police and Criminal Evidence Act (PACE) in 1984, the legal nature of the evidence seems to rely on the one of the fairness of the procedure and the moral correction in the seeking of evidence. Continental penal law seems also reluctant to discard evidence, despite being inadmissible, during criminal procedures. In that sense, the example of the turnaround of Belgian jurisprudence in that matter provides an interesting illustration.

The Belgian Supreme Court had first decided in a ruling of 1987 that evidences obtained unlawfully should not be taken into consideration either directly or indirectly by the judge [77]. However, the situation radically changed in 2003 [78]. In a ruling of 14 October, the Court considered that the fact that evidence had been obtained unlawfully, had as sole consequence that the judge could not take it into consideration either directly or indirectly in the following cases:

- When the respect of certain formal conditions were sanctioned with nullity by the law,
- When the unlawful actions had put at stake the reliability of the evidence,
- When the use of such evidence would be contrary to the right to a fair trial.

The Court had further specified in a ruling of 23 March of 2004 the criteria that should be used to assess the infringement into the right to a fair trial as protected by Article 6 of the European Convention on Human Rights:

- When the police or judicial authority intended to commit the unlawful act,
- When the seriousness of the offence (of police officer) outweighs the seriousness of the offence,
- When the unlawful evidence is only concerned with a material aspect of the offence.

Fairness in the collection of the evidence and thus a strict compliance with the right to due process as contained in Article 6 of the European Convention on Human Rights[19] seems to be of first importance in order to assess the admissibility of the evidence.

In that sense, the ECHR had to deal with the unlawful installation by the police of tapping devices and the registration of voices of suspects in a police cell (ECHR, *P.G. & J.H.,* . 2001 [79]). The Court decided that despite the fact that Article 6 of the European Convention on Human Rights did not contain rules regarding the unlawful obtaining of evidence, which is left to national authorities, this article does imply that the trial should be conducted in a fair way including the previous phase of collection of evidence. The Court referred to previous case-law (e.g. [ECHR, Schenk, 1988 [80]; ECHR, Khan, 2000 [81]) and it recalled that the procedure should be contradictory. To assess the fairness of the trial, the defence should have been given at any moment the right to contest the authenticity and the use of evidence. When making the balance, the Court also takes into account whether it is the only evidence which is put forward. These requirements intend to ensure equality of arms.

An application of this jurisprudence into Belgian case-law can be found in a judgement of the Supreme Court of 8 November 2005. The case was dealing with the interference into the right to privacy of an individual suspected by the police of having committed a road offence. For the sake of a TV program, cameramen of the production team had taken a place in a police car and filmed an individual caught perpetrating a road offence on his way home. The images had been broadcasted on TV. The lower Courts had found a violation of the right to privacy of the individual as the evidence had been collected via the cameras of incompetent third parties (the cameramen). The Supreme Court confirmed the judgements of the lower Courts and ruled that Article 8.2 of the European Convention on Human Rights had been violated. The evidence collected in an unlawful way were compromising the right to a fair trial, namely because of the excessive nature of the interference into the right to privacy with regard to the nature of the offence.

---

[19] Article 6 ECHR states that : '1. In the determination of his civil rights and obligations or of any criminal charge against him, everyone is entitled to a fair and public hearing within a reasonable time by an independent and impartial tribunal established by law. Judgement shall be pronounced publicly by the press and public may be excluded from all or part of the trial in the interest of morals, public order or national security in a democratic society, where the interests of juveniles or the protection of the private life of the parties so require, or the extent strictly necessary in the opinion of the court in special circumstances where publicity would prejudice the interests of justice.
2. Everyone charged with a criminal offence shall be presumed innocent until proved guilty according to law.
3. Everyone charged with a criminal offence has the following minimum rights:
(a) to be informed promptly, in a language which he understands and in detail, of the nature and cause of the accusation against him;
(b) to have adequate time and the facilities for the preparation of his defence;
(c) to defend himself in person or through legal assistance of his own choosing or, if he has not sufficient means to pay for legal assistance, to be given it free when the interests of justice so require;
(d) to examine or have examined witnesses against him and to obtain the attendance and examination of witnesses on his behalf under the same conditions as witnesses against him;
(e) to have the free assistance of an interpreter if he cannot understand or speak the language used in court.

The incorporation of the European Convention on Human Rights into national laws has finally led to some recognition that the acquisition of 'intangible' information may fall within the purview of Article 8 and that any prosecution that relies upon such evidence might be challenged under Article 6, should there be an unreasonable interference with privacy rights [82]. This will however be done on a case-by-case basis by every national judge. In case the judge admits the evidence despite the breach in the fundamental rights of the 'victim', (s)he could however seek remedy in suing the errant official agent on the basis of infringement to its privacy rights.

However, as rightly stressed by A. Ashworth [83], on the one hand, *'if the purpose of the Convention is to guarantee individuals protection from having their rights breached, it is surely appropriate that they should not be placed at a disadvantage in consequence of that breach; on the other hand one might argue that the proper way to deal with such breaches is to allow the defendant a remedy in damages against the errant official, and to prosecute that official if an offence was committed, rather than to upset a trial where the reliability of the evidence is not in question'*. But then, *'what moral standing would a court have if it proceeds to a conviction on the basis of evidence obtained by a violation of a right that it purported to recognise as fundamental?'*

Moreover, the lawfulness of the interference by the police into the individual privacy right would appear conditioned to the suspect to be eventually convicted. In the case where the suspect is cleared from charges, this interference would no longer be justified, putting the police in a delicate position. Van Der Hulst [84] points out this risk in its analysis of the ruling of the ECHR in the Lüdi case (ECHR, Lüdi, 1992 [85], where a suspect of drugs traffic subject to covered surveillance was claiming that this actuation were infringing his right to privacy. The Court maintained that *'the applicant must therefore have been aware from then on that he was engaged in a criminal act punishable under Article 19 of the Drugs Law and that consequently he was running the risk of encountering an undercover police officer whose task would in fact be to expose him.'* Van Der Hulst however stresses that *'this reasoning starts from the hypothesis that there was an offence. If this reasoning had not subsequently been confirmed, the result would be that the undercover operation constituted unwarranted interference with the private life of the person who was its subject. Consequently, the basis on which the infiltration was founded remains uncertain until the criminal activity is proven.'* Van Der Hulst concludes that the police cannot operate on such a basis because the lawfulness of their actuation would depend upon the (uncertain) fact that the investigation would ultimately produce a conviction. He advocates for a reasoning that would consider undercover operations (as dealt with by the case), which by its nature involves personal contacts between individuals, as affecting the right to respect for private life and that it must then be legitimised within the meaning of paragraph 2 of Article 8.

6.3 Evidence gathering on the Internet: privacy issues

Whereas there is little doubt that images posted on the Internet that are freely available could only expect limited protection under Article 8 of the European Convention on Human Rights, although it does not mean that there will be no protection at all, this statement is not that clear when it comes to searching users' private accounts protected by passwords or whose access is restricted to a definite number of individuals.

However, even in the former case, it should be recalled that individuals are granted some protection to their right of privacy even in public places. As an example, in *Peck vs. United Kingdom [86]*, the ECHR ruled that individuals do not lose their right to privacy when they

are being monitored in public spaces for law enforcement purposes. In that case, the CCTV Council disclosed the footage to the public as stills of the man carrying a knife and apprehended by the police in "CCTV News", without the Council having obtained the applicant's consent or masking his identity. This man presented as a dangerous criminal and detected as such by the CCTV observer was actually trying to commit suicide. The Court considered that particular scrutiny and care was needed given the crime prevention objective and context of the disclosures. This case shows that even if public safety may prevail on the right to privacy under certain circumstances, especially where individuals could have lower expectations of privacy, they are still entitled to be adequately protected. In that sense, some provisions of the data protection legislation may put some limits to the searching of images posted on the Internet by the police.

6.3.1 Collection of publicly available information from the Internet

The Internet is a great source of information, in most cases publicly accessible. However, publicly accessible does not necessarily mean that the information can be collected and used for any kind of purposes. One of the most significant barriers resides in the application of privacy protection to any information that could qualify a person. To that effect, it is interesting to mention a decision of the Italian Data Protection Authority in the case Peppermint [87]. A copyright society had commissioned a private company to monitor peer-to-peer networks with the purpose of identifying IP addresses of users who upload or download protected works to further prosecuting these users. The processing of IP addresses by the private company was deemed unlawful by the Italian Data Protection Authority, because it could not be based on any of the legitimate grounds listed by the Italian Data Protection Act. More specifically, the Italian Data Protection Authority considered that the IP addresses collected from the P2P software had been disclosed by the Internet user for the specific purpose of exchanging files and thus any re-use of these data for any other purposes should be based on one of the grounds listed by the Italian Data Protection Act. This case refers to the collection of personal data by private parties in order to file a judicial complaint in a civil procedure. The context is thus different from the subject of this deliverable focused on criminal procedures and the collection of personal data from the Internet by law enforcement authorities. It however provides a good example of how data protection legislations could limit the possibility to collect information relevant to judicial investigations.

In the case of a criminal investigation, the context of posting and of the collection will obviously respond to different purposes. When using information collected from the Internet, several aspects should be taken into account: the existence of a legitimate ground, the relevance of the information collected for the purpose of the processing, the limited period of storage and the rights of third parties to privacy.

6.3.1.1 Applicability of data protection legislation to the collection of images

Even if the provisions of the EU Directive 95/46/EC are not applicable to the processing carried out for purposes of criminal investigations, they remain subject to the broader provisions of the Council of Europe Convention n°108 (hereinafter termed 'CoE Convention') and to the Recommendation R 15 (87) regulating the use of personal data in the police sector. In that sense, it should be noted that when implementing the EU Directive 95/46/EC, EU Members States have adopted new data protection legislations, or adapted their pre-existing legislations based on the CoE Convention to comply with the Directive. This had an influence on a series of data protection provisions and concepts. This section will thus

detail the provisions of CoE Convention and Directive 95/46/EC to clarify the concepts and anticipate the content of national legislations in the field.

The CoE Convention purports to secure individuals respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him ('data protection'). This Convention establishes a series of data protection principles which have inspired most of European data protection systems. The EU Directive 95/46/EC outcomes the CoE Convention and is intended to ensure the free movement of personal data between Member States through the harmonisation of national provisions on the protection of individuals with regard to the processing of such data. Recital 11 clearly links both norms and states that *'whereas the principles of the protection of the rights and freedom of individuals, notably the right to privacy, which are contained in this Directive, give substance to and amplify those contained in the CoE Convention.'*

With regard to images, the interpretation of the Consultative Committee of the CoE Convention on the images collected via video surveillance should be mentioned. This Committee has considered that the data and information collected via surveillance are subject to the Convention insofar as they relate to an individual that is identified or identifiable by reference to other information, irrespective of whether such information concerns linguistic data, static or dynamic images or sound. It is sufficient for voices and images to provide information on an individual by making him/her identifiable even though indirectly. The Consultative Committee has considered the digital processing of voices and images to always represent 'automatic processing', whereas the analogue processing should only be regarded as such if voices and images undergo automatic processing in order to identify data subjects or else contribute to their identification [88].

Directive 95/46/EC issued later took into consideration the developments of the techniques used to capture, transmit, manipulate, record, store or communicate sound and image data relating to natural persons and explicitly stated that the Directive is applicable to such data (Recital 14). As a consequence, as highlighted by WP29 [89], images are acknowledged as personal data to the extent that the individuals are recognisable [90]:

- even if the images are used within the framework of a closed circuit system, even if they are not associated with a person's particulars,
- even if they do not concern individuals whose faces have been filmed, though they contain other information such as, for instance, car plate numbers or PIN numbers as acquired in connection with the surveillance of automatic cash dispensers,
- irrespective of the media used for the processing, the technique used, the type of equipment, the features applying to image acquisition and the communication tools used.

6.3.1.2 The purpose specification principle

The principle of finality implies that personal data should be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. The purpose specification principle participates from the principle of forseeability.[20] This

[20] See in that sense, Opinion of the General Advocate J.Kokott, 18 July 2007, ECJ Case C-275-06, point 53: "It must therefore, in accordance with the requirement of foreseeability, be formulated with sufficient precision to enable the citizen to adjust his conduct accordingly. The requirement of foreseeability has found particular

means that personal data can not be processed for purposes beyond the reasonable expectations of the data subject (further processing of personal data can only be slightly but never substantially different from the original processing) [91].

Data protection legislations identify data processing according to their purposes. In that sense, in the PNR case, dealing with the transfer of personal data by Air companies to the US Bureau of Customs and Border Protection, the ECJ distinguished between the activities of collection of data for commercial purposes and the further processing based on public safety needs and considered them as two different data processing, calling for two different legal bases.

The collection of personal data, such as images or video posted online, for the sake of a criminal investigation constitutes a re-use of personal data and thus should be grounded on a new and specific legal basis. Requiring the consent of the person is obviously excluded. Within a criminal investigation, the collection of the images should be based on a legal mandate. It is thus possible that additional requirements come from this legal authorisation tending to limit the power of police.

6.3.1.3 Existence of a legitimate ground

Personal data should be obtained and processed lawfully. It follows that the processing should be compliant with the applicable laws as regards this specific processing. Specific focus should be put on the competences allocated to the controller (i.e. the law enforcement authority empowered by the law) and the persons allowed to access to the personal data.

Directive 95/46/EC states that a processing, in order to be lawful, must be in addition carried out on one of the grounds listed by Article 7 (Recital 30). These grounds cannot be expanded by national laws. It follows that processing not based on any of these grounds will be unlawful. The pre-requisites set up to ensure the legality of the processing *'recognise that the processing of any personal data about another is a trespass into the informational privacy of that person and must therefore either be accepted by the individual (consent) or justified on some basis'*[92].

It should be noted that, contrary to the doctrine of self-determination, Article 7 does not overemphasise the importance of consent: all grounds for lawful processing mentioned in Article 7 have the same status [93]. The processing can be based on either of the grounds detailed below:

- Unambiguous consent of the data subject (Article 7.a). The data subject's consent means any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed. (Article 3 h).
- Processing can be run without the consent of the data subject:
    - *when it is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed*. This ground is the one more likely to be used for criminal investigations. The extent of the collection of

expression in data protection law in the criterion – expressly mentioned in Article 8(2) of the Charter – of purpose limitation. Pursuant to the specific embodiment of the purpose limitation criterion in Article 6(1)(b) of Directive 95/46, personal data may be collected only for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes."

information and their processing will thus usually depend on the content of the national legislation.

- *when the processing is necessary in order to protect the vital interests of the data subject*. This ground should be interpreted narrowly in the sense that the processing can only be based on this ground whenever it is essential for the life of the data subject and it is a matter of life and death.
- *when it is based on the pursuit of the data controller's or the data recipient's legitimate interest*, provided this is not incompatible with the interests or the fundamental rights and liberties of the data subject. The difficult interpretation of this provision is realised by national data protection authorities and national courts on a case-by-case basis.
- *when it is necessary for the performance of a contract* to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.
- *when it is necessary for compliance with a legal obligation* to which the controller is subject.

6.3.1.4 Information to the data subject

The rights described in this section aims at *'making people aware of basic details of the processing of personal data on themselves'*. The information right guarantees the transparency of the processing as regards the data subject and empowers him to exercise his right of access.

The CoE Convention had already stated that any person shall be enabled to establish the existence of an automated personal data file, its main purposes, as well as the identity and habitual residence or principal place of business of the controller of the file. The Directive goes one step further and requires that when the data are collected or, when the data are not obtained from the data subject, at the time of the undertaking or no later than the time when the data are first disclosed, the controller should provide a series of information to the data subject which is defined by the Directive:

- the identity of the controller and of his representative, if any,
- the purposes of the processing for which the data are intended,
- any further information insofar as it is necessary having regard to the specific circumstances in which the data are collected, to guarantee fair processing in respect of the data subject, such as:
  - i. the recipients or categories of recipients of the data,
  - ii. whether replies to the questions are obligatory or voluntary, as well as the possible consequences of failure to reply,
  - iii. the existence of the right of access to and the right to rectify the data concerning him.

Principle 2.2 of the Recommendation R 15 (87) stipulates that *'where data concerning an individual have been collected and stored [by the police] without his knowledge, and unless the data are deleted, he should be informed, where practicable, that information is held about him as soon as the object of the police activities is no longer likely to be prejudiced'*.

The information to the data subject within a criminal investigation is thus subject to the need for secrecy of police activities and thus can be postponed until the investigation will not be prejudiced.

6.3.1.5 Relevance of the information collected (data minimisation principle)

The information collected should be proportionate to the objectives pursued, i.e. it should be strictly necessary for the criminal investigation and relevant to the establishment of the facts and the definition of the author of the crime.

The data to be processed should be adequate, relevant and not excessive in relation with the purpose of the processing (Article 6.c). The data minimisation principle acts here as a second barrier in order to limit the collection of data which would not be strictly necessary for the provision of the service. Principle 2 of the Recommendation R (87)15 regulating the use of personal data in the police sector states that the collection of personal data for police purposes should be limited to such an extent as is necessary for the prevention of a real danger or the suppression of a specific criminal offence. Furthermore, in accordance with Article 5 of the CoE personal data undergoing automatic processing shall be stored for specified and legitimate purposes and not used in a way incompatible with those purposes.

Another important issue resides in the relevance of the personal data processed. The Council of Europe pointed out the fact that *'sometimes, the police in order to do their work properly have to collect vast amounts of data either by downloading computers during searches in premises, by intercepting communications or by searching the emails of criminals. The storage can only be justified for the time needed to find out that they are really unrelated, unless other compatible use or other use explicitly permitted by law come in view'*[94]. In the *Campbell* case (1984) [95], the ECHR judged that *'the existence of facts or information (should) satisfy an objective observer'* that there is reasonable cause to use such data for the purpose of combating crime.

6.3.1.6 Limited period of storage

Personal data should be preserved in a form which permits the identification of the data subjects for no longer than is required for the purpose for which those data are stored. This obligation is difficult to apply in the specific case of criminal investigations. The definition of the period of storage will depend on the purpose of the processing as well as on the status of the data subject (i.e., whether the data subject is a victim, a suspect, a convict, a witness, etc.). The Council of Europe advocates for the deletion to occur after some years after the last time any relevant data has been added to the record. After this period a periodic review could be realised (as done in Article 112 of the Schengen Agreement) and, if there are no reasonable grounds to justify further storage then deletion should be the rule.

The recent *Marper* Case (2008) [96] has given valuable input to the divergences existing about the possibility to store personal data of suspects. The Council of Europe had noted to this regard that *'there was divergence with regard to the necessity of deleting such data in cases of acquittal by lack of evidence though the suspicion remains. But it is less questionable when somebody's innocence has been established. The conservation of personal data related to persons other than the suspect or the convicted person should be deleted, their further use would be deemed incompatible, unless a legal basis exists to ground such conservation or processing.'* This case moreover provides a good illustration of how the right to privacy will limit the information that can be collected and stored for purposes of criminal investigations. In this case, the ECHR had to know about the collection of fingerprints, cellular samples and

DNA profiles related to suspected persons but not convicted of offences into a centralised database held by the UK government. The ECHR judged that the blanket retention introduced in the UK legislation on fingerprints, cellular samples and DNA profiles of *'persons suspected but not convicted of offences fails to strike a fair balance between the competing public and private interests and that the respondent State has overstepped any acceptable margin of appreciation in this regard'*. The Court concluded that this processing of personal data constitutes a disproportionate interference with the applicants' right to respect for private life and cannot be regarded as necessary in a democratic society and is thus deemed excessive.

6.3.1.7 Rights of others

Finally, the collection of images could interfere not only on the right to privacy of the suspected individuals of wrongdoing but also on third parties not related to the case that appear on the images collected.

The processing of third parties' personal data will fall under the same principles: their processing should be necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed, the data processed should be strictly necessary for the purposes of the criminal investigation, they should be informed of such processing whenever such obligation is not overridden by the need to preserve the secrecy of the investigation, and they should be deleted insofar as they are no longer necessary for the purposes of the processing.

6.3.2 Collection of images from users' private accounts

During the course of an investigation, it may be necessary to access a private user account in order to obtain relevant information. To that effect, the police will need to obtain a production order, as defined in Article 18 of the Cybercrime Convention, in order to require or access such information at the Service Provider hosting the account.

If the user's account were to be protected under the provisions of Article 8 ECHR, the production order would have to abide by the more restrictive rules of criminal law procedure concerning searches and seizures interfering into the right to privacy. More restrictive rules apply to the interference into home or correspondence. It is thus necessary to define if the access to a user's private account could benefit from the protection of Article 8 ECHR of 'home' or 'correspondence'.

6.3.2.1 User's private account

A user's private account is a space on a server owned by a third party put at the disposal of the user for its use according to the conditions of utilisation specified in the contract linking both parties. As a way of example, in the case of *Facebook*, the user is given the possibility to use a series of applications directed to the communication of information, irrespective of the format (data, images, videos, music), to other individuals that (s)he has previously authorised. First and most common use of such platforms is for private purposes (although increasingly used for business purposes), to share information and exchange with friends and acquaintances. Possibilities exist to select to whom the information displayed is made available. Other websites of information sharing such as *Flickr* also enable the user to share his/her photos and videos with other users (s)he would have invited previously. As mentioned above, the development of those websites has taken such dimensions that police officers are searching them in order to gather evidence of crimes and offences for further prosecution.

6.3.2.2 Users' private account as private spaces

In the above mentioned definition, it should be noted that users' private accounts are used for developing their social life with their inner circle (of friends) but also with other persons that may be less close but who are still identified and known by the user and thus can hardly be acknowledge as 'public'.

The concept of private life as developed by the case-law of the ECHR is a general one which covers the more specific concepts of home life and correspondence. Article 8-I ECHR covers more than 'the right to be left alone'. It also encompasses the moral and physical integrity of the person, his personal identity, individual space, the storage and distribution of his personal data, his sexual activities and the social ties between individuals [97]. It is thus very likely that a user's private account would fall under this definition and be granted protection.

To that effect, it is interesting to bring forth a recent German ruling about covert online surveillance. The German Constitutional Court published on 27 February 2008 a landmark ruling about the constitutionality of secret online searches of computers by government agencies. As mentioned by EDRI-Gram, *'the decision constitutes a new "basic right to the confidentiality and integrity of information-technological systems" as derived from the German Constitution.'*[98].

It is further reported that the Court bases the need for protection on the relevance of the use of information-technological systems for the expression of personality (Persönlichkeitsentfaltung) and on the dangers for personality that are connected to this use. In these cases, the individual is depending upon the state respecting the justifiable expectations for the integrity and confidentiality of such systems with a view to the unrestricted expression of personality.

Information-technical systems that are protected under the new basic right are all systems that *'alone or in their technical interconnectedness can contain personal data of the affected person in a scope and multiplicity such that access to the system makes it possible to get insight into relevant parts of the conduct of life of a person or even gather a meaningful picture of the personality.'* This includes laptops, PDAs and mobile phones.

The decision also gives very strict exceptions for breaking this basic right. Only if there are "factual indications for a concrete danger" in a specific case for the life, body and freedom of persons or for the foundations of the state or the existence of humans, government agencies may use these measures after approval by a judge. They do not, however, need a sufficient probability that the danger will materialise in the near future. Covert online searches can therefore not be used for normal criminal investigations or general intelligence work.

If these rare conditions are met, secret online searches may only be used if there are steps taken to protect the core area of the private conduct of life, which includes communication and information about inner feelings or deep relationships.

This judgement shows that the information stored on personal devices or spaces accessible from the Internet is worthy of protection under the right to privacy insofar users' private accounts *'contain personal data of the affected person in a scope and multiplicity such that access to the system makes it possible to get insight into relevant parts of the conduct of life of a person or even gather a meaningful picture of the personality'*.

6.3.2.3 User's private accounts as 'home'

Search warrants are subject to strict conditions when it comes to searching private premises. In these cases, the warrant should usually be issued by a judicial authority in order to limit abuses. The judge granting the search warrant is expected to carry out a delicate balancing between the right to privacy and the public interest lying in crime enforcement. It should thus be defined whether the search of a user's private account should be subject to the strict conditions applying to the search of private premises. To that effect, it is necessary to analyse how the concept of 'home' is understood by the jurisprudence of the ECHR.

In the *Hatton* Case (2003), the Court gave the following definition of home: *'A home will usually be the place, the physically defined area, where private and family life develops. The individual has a right to respect for his home, meaning not just the right to the actual physical area, but also to the quiet enjoyment of that area. Breaches of the right to respect of the home are not confined to concrete or physical breaches, such as unauthorised entry into a person's home, but also include those that are not concrete or physical, such as noise, emissions, smells or other forms of interference. A serious breach may result in the breach of a person's right to respect for his home if it prevents him from enjoying the amenities of his home.'* [99] In *Niemietz (1992) [72]*, the Court argued that *'as regards the word 'home', appearing in the English text of Article 8, the Court observes that in certain Contracting States, notably Germany, it has been accepted as extended to business premises. Such an interpretation is, moreover, fully consonant with the French text, since the word 'domicile', has a broader connotation than the word 'home' and may extend, for example, to a professional person's office. In this context also, it may not always be possible to draw precise distinctions, since activities which are related to a profession or a business may well be conducted by a person's private residence and activities which are not so related may well be carried on in an office or commercial premises. A narrow interpretation of the words 'home' and 'domicile' could therefore give rise to the same risk of inequality of treatment as a narrow interpretation of the notion of 'private life''.*

The ECHR case-law thus defines 'home' as a premises where the individual carries out activities related to his private life, understood as individual space or where the individual ties social links with other individuals. The individual thus does not need to own the premises to benefit from the protection. Users' private accounts on social networks indeed provides an individual space, whose access is restricted to the other persons the individual had specifically authorised, where an individual ties social links with others. However, this space fails to meet what seems to be one essential component, namely the 'physical' element. It is thus highly uncertain whether a virtual space could qualify as 'home', even if it meets all other characteristics.

6.3.2.4 Users' private account as correspondence

Another possibility consists in acknowledging that the information disclosed under a user's private account as communication, in such case the access to such information would qualify as search of private correspondence. If such would be the case, the search warrant would then need to comply with the specific requirements relative to the interception of communications.

In the *Liberty* case (2008) [100], the Court ruled that 'telephone, facsimile and e-mail communications are covered by the notions of "private life" and "correspondence" within the meaning of Article 8' [see also ECHR, Weber and sarabia, 2006 101]). The Court recalls its findings in previous cases to the effect that the mere existence of legislation which allows a

system for the secret monitoring of communications entails a threat of surveillance for all those to whom the legislation may be applied. This threat necessarily strikes at freedom of communication between users of the telecommunications services and thereby amounts in itself to an interference with the exercise of the applicants' rights under Article 8, irrespective of any measures actually taken against them (ECHR, Weber and Saravia, 2008 § 78 [101]).

It is worth noting that the word 'correspondence' is not qualified by the adjective 'private'. It follows that correspondence of a mixed nature should benefit from the protection of Article 8. To that effect, the Court noted in *Niemietz* (§32 of [72]) that it 'has already held that, in the context of correspondence in the form of telephone calls, no such qualification is to be made (ECHR, Huvig, 1989) [102]. Again, in a number of cases relating to correspondence with a lawyer (see, for example, ECHR, Schönenberger and Durmaz, 1988 [103], and ECHR, Campbell, 1984 [95]), the Court did not even advert to the possibility that Article 8 might be inapplicable on the grounds that the correspondence was of a professional nature.

In Weber and sarabia (2006) [101], the Court has defined the guarantees that should surround measures of secret surveillance of communications. The law must indicate the scope of any such discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity to give the individual adequate protection against arbitrary interference (see also ECHR, Malone, 1983 [104], ECHR, Leander, 1987 [105], ECHR, Huvig, 1989 [102]). In its case-law on secret measures of surveillance, the Court has developed the following minimum safeguards that should be set out in statute law in order to avoid abuses of power: a) the nature of the offences which may give rise to an interception order; b) a definition of the categories of people liable to have their telephones tapped; c) a limit on the duration of telephone tapping; d) the procedure to be followed for examining, using and storing the data obtained; e) the precautions to be taken when communicating the data to other parties; and f) the circumstances in which recordings may or must be erased or the tapes destroyed (see, *inter alia*, ECHR, Huvig, § 34, p.56 of [102]; ECHR, Amann, 2000 § 76 [106]; ECHR, Valenzuela Contreras § 46, pp. 1924-25 of [107]; and ECHR, Prado Bugallo, 108, § 30 [108]).
It thus makes no doubt that if user's private account were to qualify as 'correspondence', it would be protected under Article 8 ECHR. But can a website used to communicate with a selected amount of persons qualify as such? The jurisprudence usually acknowledges the character of correspondence to letters, phone conversation and to emails, and in France, for example, electronic exchanges will qualify as correspondence provided that the recipients are defined [109]. Whereas traditionally the correspondence takes place between only one sender and one recipient, technological means allow one sender to emit a message to several recipients. A communication does not moreover terminate with the action of sending but can be protected once stored. We could thus make an analogy between the letters stored at the recipient's place and the information stored on the website. In the light of these considerations, it would appear more likely that a user's private account would qualify as communication rather than 'home'.

6.4 Other legal aspects of images: a personality right, copyrighted object and the consequences of manipulation

Since digitisation and the emergence of the virtual and interactive Internet, nearly everyone has worldwide access to information and is able to distribute information on a global scale, without having to rely on a publishing or broadcasting intermediaries. The usage of mobile phones and/or digital cameras by amateurs has become commonplace. All that is needed to

publish content on the Internet is Internet access. The fact that you can even act anonymously or under a pseudonym lowers the threshold for many people to publish something on the Internet, which in turn leads to an enormous increase of user-generated content.

In the last part of this report we will make some observations on the current problems that arise when pictures are taken and uploaded without authorisation of the image right holder even though this is required. The problem seems to accumulate within the "sharing" culture where people tend to share pictures with specific other persons or the entire Internet. We take a closer took into the legal status of the portrayed person (the image right holder), the legal status of the photographer being the author. We end by saying a few words on the effect of manipulation of images.

6.4.1 The right to protect your image on the Internet

In some European continental countries like France and Belgium natural persons can invoke a separate "image right" (droit de l'image / portretrecht), which because of its close connection to someone's person and personality is qualified as a "personality right" (droit de personnalité / persoonlijkheidsrecht).

It includes that a person's authorisation should always be obtained when a person is recognisable in an image, whatever the type / carrier of the image or the means used to make the picture. The authorisation should be obtained for both the making of the image and any further use of it, also online [110-113] e.g. when sharing it via public or private photo albums on Flickr.com or via social networks like *Facebook*. The authorisation can be given either orally or by a written statement, but there are no specific formal conditions.

However, the authorisation should be certain, unambiguous and specific. The specific character refers to the fact that the authorisation should only include specifically determined uses of an image, or that the authorisation is at least restricted in time and/or referring to defined types of usage. A "general" authorisation should have a conditional and temporary character. An authorisation can also be given for the use within a specific context. Whether these conditions are fulfilled or not, will depend on the concrete circumstances.

The authorisation can be given tacitly or explicitly. As a general rule, it should be given explicitly. An implicit authorisation will always be the exception to the rule and should be interpreted restrictively. An implicit authorisation can be derived from the concrete circumstances. Courts and legal scholars tend to explain it in such a way that it only extends to the images and goals for which the authorisation was given in the first place. The authorisation cannot be explained in such a way that it would extend to other goals or images for which authorisation was given. The question rises whether friends can expect from one another these days that when they allow that their picture is being taken, they implicitly give the authorisation to their friend that he can publish the picture online and share it with a number of friends or even the entire world?

An authorisation to publish an image can always be withdrawn. It will be the other parties' concern to prove that she has obtained the authorisation to publish the image. However there are (reasonable) exceptions, namely when the person has been photographed in a public space (unless the image is focused on the individual [114]), when the person is a public figure, when the pictures were taken within his or her professional activities (a model, a athlete, an artist), a parody, a photograph of a crowd or a group of persons whereby the individual persons loses its personal character, in other words, whereby the "individual" loses its personal character.

Bearing the previous paragraphs in mind, we can say that a lot depends on the context in which a picture is taken. In our opinion sharing pictures of a party or holiday with friends is something that is socially expected. However, sharing it with all the friends of your friends or everyone via *Facebook* or via open access on Flickr.com, does require another explicit authorisation of the person whose image was taken. After all, what one does in his or her private time, is not necessarily something he wants to share with people outside his closed circle of family and friends.

Though both *Facebook* and *Flickr* provide settings to ensure that an album is only shared with a selected group of friends, users tend to be unaware of this tool and share their albums with hundreds, even thousands of people. By doing this, they seem to neglect the fact that the publication of these pictures can have considerably prejudicial consequences for the persons on who the camera was focused. One of the most common problems is that persons get photographed in a rather compromising situation (e.g. drunken state) which casts doubt upon his professional capabilities (e.g. a police officer, a minster).

More and more problems arise between on the one hand the freedom of (creative) expression and copyright of the photographer and on the other hand, the right to privacy and more specifically, the image right of the person portrayed.

6.4.2 Copyright of the photographer

The image right is in fact a restriction on the freedom of expression of the photographer to create an image. However, when he has obtained the authorisation of the portrayed person, he is free to make the picture the way he prefers. When the photograph is considered to be original (the result of the intellectual efforts of a natural person and bearing the stamp of his personality) it is automatically protected by copyright. The author need not undertake action. The notion "originality" is interpreted quite broadly. The artistic or aesthetic character of the picture is of no importance at all, but what makes the photograph original is the setting, the perspective, the light used, the development of the photograph etc. In other words, photographs which portray a person can be very plain, unoriginal and therefore not copyrighted, e.g. pictures taken for a person's ID card tend to be unoriginal since they do not bear any personal stamp of the photographer. That stamp is entirely missing when the person for example decided to let his picture be taken by an automatic passport booth, the necessary intervention of a human being lacking there entirely. However, a picture taken by a friend of a person and posted online, even when originating from the hand of an amateur, can always qualify for copyright protection. If that is the case, the author's license is needed whenever the picture is reproduced (copied in either way: analogue, digitally, partly or as a whole, temporary or permanently), communicated or made available to the public (via wires or wireless, via cable, satellite, TV, Internet, mobile).

In sum, any usage of a photograph requires not only the authorisation of the person who is portrayed, but also the license of the photographer. Yet there are some exceptions to this rule, as adopted by Member States following the implementation of Directive 2001/29/EC on several aspects of copyright and related rights [115]. However, no harmonisation with regard to the exceptions was established since Member States were left free to choose which exceptions they wanted to implement, except for one mandatory exception, namely: '*Temporary acts of reproduction which are transient or incidental and an integral and essential part of a technological process and whose sole purpose is to enable: (a) a transmission in a network between third parties by an intermediary, or (b) a lawful use of a work or other subject-matter to be made, and which have no independent economic*

significance' (Article 5.1.). It is doubtful whether reproductions in the course of manipulation of images for forensic purposes fall under the scope of this exception given the fact that the manipulation will lead to a new established work and is not a mere copy of the image. Moreover, the manipulated image will have a permanent and not a temporary character. There is one very interesting exception which would allow investigative officers the '*use for the purposes of public security or to ensure the proper performance or reporting of administrative, parliamentary or judicial proceedings'* (Article 5.3 e). When the image would be protected by technological protection measures, right holders should take measures to enable the use foreseen by the exception for public authorities. If the right holder does not act voluntarily, the member state should take appropriate measures (Article 6.4.). However, as already stated before, the implementation of this exception was not mandatory so whether or not she can be invoked depends from one county to another.

We should also remark that the liberty of a photographer is also protected by the universally protected right to express one's opinion and to receive or impart information and ideas, which is an essential foundation of a democratic society and one of the basic conditions for each person's self-fulfilment. As a human right it has been legally recognised in many national constitutions and several international treaties with regard to human rights. Article 10 of the European Convention on Human Rights provides the broadest, most modern and media neutral definition. This fundamental right can be invoked by every person, whether natural or legal and regardless of his or her quality. In principle, every expression of an opinion including is legally protected, irrespective of its informative, artistic or commercial nature, news value or quality [116]. The information or expression can also be in the form of a picture [117]. Pictures taken by professional journalists, photographers who are published in a newspaper, or photos made by hobbyists shared on *Flickr.com* or *Facebook*, they all qualify for protection by Article 10 ECHR.

A picture may be a mere representation of reality as such and intrinsically be the reporting of a current news event (information). However, often a picture is not just a mere objective reproduction of reality, but a personal expression by the maker, emphasised by the way of shooting the picture, the perspective, the setting of the scene, the colours used, etc. (*expression*). Especially when the photographer intervenes throughout the making process and also manipulates the original version by use of software program tools (e.g. Photoshop, used both by professionals and amateurs) we can soon speak of a personal expression, which may also lead to copyright protection (*infra*).

A picture taken by a journalist and published in a newspaper, or taken by an amateur and posted on his weblog, or via a sharing website such as *Facebook* is principally legally protected. Case law of the European Court of Human Rights points out that some content is however more protected than others. Commercial information like advertisements is not protected as much as pictures which can be qualified as political speech. Furthermore, Article 10 covers the means of dissemination (print, television, radio, Internet) [118] since any restriction imposed on the means necessarily interferes with the right to receive and impart information [119]. Given the fact that the Internet has become the ultimate communication tool for traditional as well as new media players in the digital information society we can assume the European Court of Human Rights will recognise the protection of this distribution tool as well. When exercising the right to freedom of expression and making photographs, the maker of the photograph should always bear in mind the possible rights and interests of others (being the persons portrayed on the picture) that may conflict with his "expression".

Article 10 § 2 ECHR. stipulates, freedom of expression can be subject to restrictions, limitations or other formalities under the following three conditions (Article 10, §2). *First*, the restriction has to be "*prescribed by law"*. One of the requirements flowing from this expression is that the regulation must be adequately foreseeable, *i.e.* it must be formulated with sufficient precision to reasonably foresee the consequences which a given action may entail. *Second*, the restriction must have a *"legitimate aim"*. The grounds upon which a restriction is allowed, are enumerated exhaustively in Article 10, §2 ECHR.[21] and are interpreted in a restrictive way by the European Court. *Third*, the restriction has to be *"necessary in a democratic society"*, which implies the existence of a "*pressing social need"*. Although a certain margin of appreciation is left to the states, the European Court of Human Rights will always take the end decision and evaluate whether the measure at stake was *"proportionate to the legitimate aims pursued"* and whether the reasons brought forward by the national authorities to justify it are *"relevant and sufficient"*. To find out whether that is indeed the case, the Court evaluates interferences in the light of the case as a whole, including the content of statements that were made, the consequences of a publication, the intentions of the author, *etcetera*.

When investigative authorities want to use images from *Facebook* and *Flickr* for example to identify crime suspects which can be qualified as protection of public safety, there clearly is "a public authority" involved. In the following paragraph we will discuss the difficulties arising from the usage of images as evidence material to identify persons. In principle the European Convention on Human Rights does not protect against interferences by private parties (the horizontal effect). At this point in time it is unclear whether *Facebook* can be qualified as a mere neutral technological intermediary or as an editor. Given the legal uncertainty regarding their liability, social network providers like *Facebook* increasingly take measures to prevent pictures being used in a malicious way. There is a growing conscience that users must be made aware of the problems that may rise and that their right to privacy as well as those of others should always be kept in mind. Nonetheless, social network providers increasingly have to intervene to remove illegal pictures showing illegal content (like child pornography) and shut down or block accounts of persons who got in the spotlights of the press e.g. for accusation of facts, leading to fierce reactions by other users of the network that are not in keeping with the policy of *Facebook* and violate the rights of the targeted person.

6.4.3 Manipulation of images: does the end justify the means?

In order to identify suspects of a crime the use of images poses technological as well as legal challenges. We distinguish the usage of two sorts of images. *First*, images retrieved from cameras used in public or private places. *Second*, images traced by police forces on the Internet on websites where photographs are commonly shared such as Flickr.com, YouTube.com and *Facebook*.

The original images we described above are often not of such a good quality that a person can be identified at first sight. Especially when these pictures originate from video cameras, they usually are of poor quality for numerous reasons: no colours, time lapses, not enough pixels, overexposed images etc [120]. As a consequence they often need editing in order to use them for identification purposes. Moreover, the looks of persons can change considerably by means

[21] "National security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary."

of simple attributes like sunglasses, a different haircut, a beard or moustache, coloured contact lenses, make-up and plastic surgery. But what the human eye might not recognise can be caught by technologies that go beyond human capabilities. The question is: how far can you go? Where does the manipulation of images begin and where should it end in order that the evidence remains lawful before court? Are technologies in their current state trustworthy enough to rely upon to identify a person?

Much depends on the context in which the manipulation has taken place and the aim of the manipulation. Not every manipulation is under false pretences and unjustified. The aim may be inspired by artistic aspirations (*supra*), to improve the quality, to improve certain details. Photos are adapted on a daily basis for glossy magazines, to get the picture in the right size in a newspaper. Manipulation of images can be carried out in the process of identifying a person in the course of an investigation. These are all justified interventions which are part of the right to creativity and freedom of expression of the photographer. The use of digital technologies clearly facilitated the manipulation of images.[22] The bigger the efforts to identify a person by editing a picture, the more suspicions of malicious manipulation may grow.

A photographer presenting an image within a certain context should keep that context in mind as well: a journalist has to provide trustworthy information upon which the audience can rely. A caricaturist should present things in a way that it is clear the image is a caricature and not the original picture. Transparency is the key to prevent misapprehensions.

Intentional misrepresentations of reality and deceiving the audience is a problem of all times, not only in the sphere of photography, but also in that of the written press, audiovisual media etc. Contrary to texts - and although misrepresentations of reality by manipulated images or videos already gave rise to scandals several times already - the truthfulness or original / clean character of images and videos is rarely called into question by the audience, especially when it concerns “shocking” news events or when they can solve or serve the identification of a person within an investigation. It is clear that such acts cannot possibly be justified on the grounds of the fundamental freedom of creativity and expression.

When can a manipulation be defined as “malicious”? A lot depends on the intentions of the manipulator. If it is clear his intentions are to give a false impression, to transform and use images in a way to influence and provide disinformation to the public, the manipulation qualifies as “malicious”[121]. The first victim of such a manipulation is of course the holder of the image right. The second victim is clearly the audience, followed by investigative authorities who should always stay cautious for usage of manipulated image material.

Thus, in order to prevent false accusations of manipulations accurate protocols should be drafted, defining how to deal with image data to ensure the integrity of the “manipulation” process. This includes: storage of the original image data, description of the steps taken (description of the manipulation) and the parameter standards used, resulting in the image that is being used as evidence.

6.5 Conclusion

The use of images stored on electronic devices for evidentiary purposes within criminal investigations raises a number of legal questions relating to their collection and further

[22] See Section 3.4 where methods are described such that common manipulations can be detected.

processing (with the possibility of enhancing and modifying the image to obtain relevant information).

There is no doubt that traditional rules applying to searches and seizures remain fully applicable to the collection of images stored electronically, despite their volatility. The Council of Europe Convention has set up the general principles to that effect, looking for equivalent rules irrespective of the means on which the information is stored. The application of the traditional rules are however more uncertain when it comes to the collection of images from the Internet. The collection of images made publicly accessible by the author (e.g. on sites such as *YouTube*) are however subject to data protection rules which call, among others, for the collection to be based on a legitimate purpose and relevant to achieve such purpose. It follows that the images collected by the police within a criminal investigation should be based on a legal mandate and be strictly relevant for the case.

The collection of images from personal users' accounts appears to be however more problematical. We contend in this deliverable that users' personal account whose access is limited to a defined number of individuals should be entitled to the protection under the right of privacy, as defined by Article 8 of the European Convention of Human Rights. However, it is more doubtful whether private accounts could benefit from the guarantees that protect the home because it fails to meet one essential element, namely the physical one. It seems more likely that the information displayed on such accounts could qualify as interference into correspondence and thus require meeting the requirements set up by the legislation to that effect. However, no jurisprudence exists on this specific and delicate issue, it is thus necessary to wait for further case-law.

Needless to say that procedural rules or rules of evidence must always be taken into account by the investigative authorities as well. Evidence cannot be obtained by committing a crime (e.g. breaking into someone's account intentionally without authorisation), provoking suspects etc. but has to be assembled in a "loyal" fashion. This is confirmed by ample case-law by the European Court for Human Rights regarding the right to fair trial (including the equality of arms principle in penal cases) [122]. The use of images retrieved from the Internet also raises fundamental problems in terms of the image (personality) right of persons who are targeted. Moreover it increased the conflict between the person who is portrayed and the interests of the photographer, who can invoke his right of expression and his copyright. All these legal conflicts have accumulated in a context where photographs are shared by numerous persons and start living their own life. Internet users seem hardly aware of the fact that authorisation is required both for the making and sharing of photographs, because technology does not require it. The law however, does. On the other hand, there is no such thing as an "absolute" right. Like other fundamental rights, image rights have to be weighted against the right to make pictures of persons to communicate information of general interest to the public or to express an opinion.

Another aspect discussed concerns the editing of original images in order to use them for identification purposes. Clearly, manipulation – despite its rather negative connotation – is not necessarily illegal and can be justifiable provided that there is no intentional misrepresentation of reality to deceive the public and is carried out in a "loyal fashion". Therefore the usage of protocols, defining how to deal with image data to ensure the integrity of the "manipulation" process, should be encouraged.

7 Conclusion

We have seen the feasibility of identifying source (video) cameras based on the videos (and in general the images) it produces, even when multiple layers of compression are added from e.g. *YouTube* or MSN (Section 3.1). In the same context, classifying the source camera according to type and/or model was found to be possible in Section 3.3. Each technique presented in the aforementioned chapters and sections has its own limitations based on the assumptions it makes. Therefore, a layered approach with a wide variety of methods is advantageous to achieve the best possible results. In other words, device classification is not superseded by device identification; rather, it supplements it. This synergy of techniques is perhaps the cornerstone of reliable forensic identification. Moreover, in 3.2 methods were presented for identifying the source scanner based on the scanned images it produces.

However, the wide availability of digital imaging techniques is not limited to physical electronics. Software solutions for manipulating images are readily available, making it necessary again to be able to detect and identify these manipulations when these images are used in a legal context. To this end, methods to detect image manipulations were presented in Section 3.4

With the technique presented in Section 3.1 it is in principle possible to link images or videos to a common source camera. This may be interesting for law enforcement agencies in the case of e.g. child pornography, so multiple videos can be identified as coming from a limited amount of cameras. This technique fails, however, when spatial transformations are applied to these images or videos. In Chapter 4 a technique was presented that allows the recognition of images even after they have been modified. Hence, if a large database of illicit images is available, a robust fingerprint can be calculated that is (to a certain extent) able to recognise the images even after manipulations have occurred. This may be of interest to automatically classify large amounts of images when the individual assessment is not feasible, e.g. when scanning a suspect's hard drive.

On a whole different level, facial recognition performance by automated systems as well as by manual comparison is limited (Chapter 5). Especially in the case of videos obtained from CCTV cameras or in general videos with low resolution or poorly illuminated scenes, unfamiliar or unknown faces are badly recognised, by both recognition methods. Hence, the evidentiary value of these videos is lower than what is commonly expected. Expectations from law enforcement agencies often have to be debilitated due to the limitations from scientific research. The old adage 'seeing is believing' should in a certain sense perhaps be loosened. Especially when CCTV systems with low resolution and frame rates are installed in areas with insufficient lighting, the conclusions based on this type of evidence may be far from convincing. Other biometric measures such as length measurements based on the images from these videos also possess wide margins of error. This situation is likely to improve with the advent of higher resolution cameras. However, even then the recognition is complicated by simple counter measures such as wearing balaclavas, baseball caps or in general changing the appearance before or after the act. 3D techniques are expected to alleviate some of the issues like pose and position problems.

In Chapter 6, examples were given to show that social networking sites prove to be a valuable source for intelligence gathering. Certain legal questions arise when this electronic information is collected by law enforcement agencies, most notably from a privacy point of view. Hence, the admissibility of potential evidence is brought into question. When the collection of images or videos that are publicly accessible are necessary in a criminal

investigation and are based on a legal mandate, and the collection is strictly relevant for the case at hand, there should be no problem. However, when information is gathered from private accounts additional considerations need to be taken into account, e.g. regarding the nature of the communication or the conditions that should be met for warranted searches and seizures. Private accounts are contended to enjoy the same privileges as private correspondence. A lack of jurisprudence in this area provides room for interpretation. Finally, electronic information may be used in other ways than was originally intended by the author, e.g. by enhancing or authenticating digital images. This may be the case when videos or images from CCTV systems are considered. In order for the enhancement of images or videos to be permissible, the steps taken to do so should be repeatable and as transparent as possible. This stipulates the development of objective algorithms that can automatically identify or classify image or video data.

8 Annex 1: References

[1] M. K. Johnson and H. Farid. Exposing digital forgeries through chromatic aberration. In *MM&Sec'06, Proceedings of the Multimedia and Security Workshop 2006, September 26-27, 2006, Geneva, Switzerland*, pages 48–55, 2006.

[2] L. T. Van, S. Emmanuel, and M. S. Kankanhalli. Identifying source cell phone using chromatic aberration. In *Proceedings of the 2007 IEEE International Conference on Multimedia and EXPO (ICME 2007)*, pages 883–886, 2007.

[3] Z. J. Geradts, J. Bijhold, M. Kieft, K. Kurosawa, K. Kuroki, and N. Saitoh. Methods for identification of images acquired with digital cameras. In S. K. Bramble, E. M. Carapezza, and L. I. Rudin, editors, *Proceedings of SPIE: Enabling Technologies for Law Enforcement and Security*, volume 4232, pages 505–512, 2001.

[4] J. Lukáš, J. Fridrich, and M. Goljan. Determining digital image origin using sensor imperfections. In A. Said and J. G. Apostolopoulus, editors, *Proceedings of SPIE: Image and Video Communications and Processing*, volume 5685, pages 249–260, 2005.

[5] M. Chen, J. Fridrich, and M. Goljan. Digital imaging sensor identification (further study). In E. J. Delp and P. W. Wong, editors, *Proceedings of SPIE: Security and Watermarking of Multimedia Content IX*, volume 6505, page 65050P, 2007.

[6] A. C. Popescu and H. Farid. Exposing digital forgeries in color filter array interpolated images. *IEEE Transactions on Signal Processing*, 53(10):3948–3959, 2005.

[7] H. Farid. Digital image ballistics from jpeg quantization: A followup study. Technical Report TR2008-638, Department of Computer Science, Dartmouth College, Hanover, NH, USA, 2008.

[8] Z. Lin, R. Wang, X. Tang, and H.-Y. Shum. Detecting doctored images using camera response normality and consistency. In Proceedings *of the 2005 IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR 2005)*, volume 1, pages 1087–1092, 2005.

[9] M. Kharrazi, H. T. Sencar, and N. Memon. Blind source camera identification. In *Proceedings of the 2004 IEEE International Conference on Image Processing (ICIP 2004)*, pages 709–712, 2004.

[10] J. Lukáš, J. Fridrich, and M. Goljan. Digital camera identification from sensor noise. *IEEE Transactions on Information Forensics and Security*, 1(2):205–214, 2006.

[11] M. Chen, J. Fridrich, M. Goljan, and J. Lukáš. Determining image origin and integrity using sensor noise. *IEEE Transactions on Information Forensics and Security*, 3(1):74–90, March 2008.

[12] M. Chen, J. Fridrich, and M. Goljan. Digital imaging sensor identification (further study). In E. J. Delp and P. W. Wong, editors, *Proceedings of SPIE: Security and Watermarking of Multimedia Content IX*, volume 6505, page 65050P, 2007.

[13] E.J. Alles, Z.J.M.H. Geradts and C.J. Veenman, Source Camera Identification for Low Resolution Heavily Compressed Images. *International Conference on Computational Sciences and Its Applications*, 2008. ICCSA 2008, pp. 557-567

[14] M. Chen, J. Fridrich, M. Goljan, and J. Lukáš. Source digital camcorder identification using sensor photo-response non-uniformity. In E. J. Delp and P. W. Wong, editors,

Proceedings of SPIE: Security and Watermarking of Multimedia Content IX, volume 6505, page 65051G, 2007.

[15] K. Irie, A. E. McKinnon, K. Unsworth, and I. M. Woodhead. A model for measurement of noise in ccd digital-video cameras. *Measurement Science and Technology*, 19(4):1–5, April 2008.

[16] G.C. Holst and T.S. Lomheim, CMOS / CCD Sensors and Camera Systems - JCD Publishing and SPIE Press, 2007

[17] H. Tian, B.A. Fowler and A.E. Gamal, Analysis of Temporal Noise in CMOS APS - *Proc. SPIE* Vol. 3649, p. 177-185 (1999), Sensors, Cameras, and Systems for Scientific/Industrial Applications

[18] K. Salama and A. El Gamal, Analysis of active pixel sensor readout circuit - *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, pp. 941-945 (2003)

[19] T. Gloe, M. Kirchner, A. Winkler, and R. Böhme. Can we trust digital image forensics? In *Multimedia '07: Proceedings of the 15th international conference on Multimedia*, September 24–29, 2007, Augsburg, Germany, pages 78–86, New York, NY, USA, 2007. ACM Press.

[20] A. Ferrero, J. Campos and A. Pons, Correction of Photoresponse Nonuniformity for Matrix Detectors Based on Prior Compensation for Their Nonlinear Behavior – *Applied Optics*, Vol. 45, No. 11, 10 April 2006.

[21] S. Bayram, H. T. Sencar, N. Memon, and I. Avcibas. Source camera identification based on CFA interpolation. In *Proceedings of the 2005 IEEE International Conference on Image Processing* (ICIP 2005), volume 3, pages III–69–72, 2005.

[22] Y. Long and Y. Huang. Image based source camera identification using demosaicking. In *Proceedings of the 8th IEEE Workshop on Multimedia Signal Processing*, pages 419–424, 2006.

[23] T. Gloe, E. Franz, and A. Winkler. Forensics for flatbed scanners. In E. J. Delp and P. W. Wong, editors, *Proceedings of SPIE-IS&T Electronic Imaging: Security, Steganography, and Watermarking of Multimedia Contents IX*, volume 6505, page 65051I, 2007.

[24] G. Kaiser, A friendly guide to wavelets - Birkhauser Boston Inc (1994), ISBN: 978-0-8176-3711-8

[24] D.L. Donoho and I.M. Johnstone, Ideal Spatial Adaptation by Wavelet Shrinkage - *Biometrika*, Volume 81, pp. 425-455 (1994)

[25] G. Kaiser, A friendly guide to wavelets - Birkhauser Boston Inc (1994), ISBN: 978-0-8176-3711-8

[26] M. K. Mihçak, I. Kozintsev, K. Ramchandran, and P. Moulin. Low-complexity image de-noising based on statistical modeling of wavelet coefficients. *IEEE Signal Processing Letters*, 6(12):300–303, December 1999.

[27] D. Donoho, A. Maleki, M. Shahram, WaveLab 850, homepage:

http://www-stat.stanford.edu/~wavelab/

[28] Maarten van der Mark, Wiger van Houten, Zeno Geradts, NFI PRNUCompare program, homepage: http://sourceforge.net/projects/prnucompare/

[29] FFmpeg, Program to record, convert and stream audio and video, homepage: http://ffmpeg.org

[30] S. Mallat, A wavelet tour of signal processing - Academic Press, second edition, 1999

[31] S.G. Chang, B. Yu and M. Vetterli, Adaptive Wavelet Thresholding for Image Denoising and Compression - *IEEE Transactions on Image Processing*, Volume 9, pp. 1532-1546 (2000)

[32] S. Bayram, H. T. Sencar, and N. Memon. Improvements on source camera-model identification based on cfa. In *Proceedings of the WG 11.9 International Conference on Digital Forensics*, 2006.

[33] O. Çeliktutan, I. Avcibas, and B. Sankur. Blind identification of cellular phone cameras. In E. J. Delp and P. W. Wong, editors, *Proceedings of SPIE: Security and Watermarking of Multimedia Content IX*, volume 6505, page 65051H, 2007.

[34] VirtualDub, A free video capture and AVI/MPEG-1 processing utility, homepage: http://www.virtualdub.org/

[35] Windows Live Messenger homepage: http://get.live.com/messenger/

[36] Worldwide Instant Messaging Market Share – July 2008 http://billionsconnected.com/blog/2008/08/global-im-market-share-imusage/

[37] MSN Webcam Recorder homepage: http://ml20rc.msnfanatic.com/

[38] WinPcap: The Windows Packet Capture Library, homepage: http://www.winpcap.org/

[39] S. L. Webb, K. J. Youngers, M. J. Steinle, and J. A. Eccher. Design of a 600-pixel-per-inch, 30-bit color scanner. *Hewlett-Packard Journal*, (Article 8):1–10, February 1997.

[40] M. Vrhel, E. Saber, and H. J. Trussell. Color image generation and display technologies. *IEEE Signal Processing Magazine*, 22(1):23–33, January 2005.

[41] H. Gou, A. Swaminathan, and M. Wu. Robust scanner identification based on noise features. In E. J. Delp and P. W. Wong, editors, *Proceedings of SPIE: Security and Watermarking of Multimedia Content IX*, volume 6505, page 65050S, 2007.

[42] N. Khanna, A. K. Mikkikineni, G. T.-C. Chiu, J. P. Allebach, and E. J. Delp. Scanner identification using sensor pattern noise. In E. J. Delp and P. W. Wong, editors, *Proceedings of SPIE: Security and Watermarking of Multimedia Content IX*, volume 6505, page 65051K, 2007.

[43] C. Burger. A Tutorial on Support Vector Machines for Pattern Recognition. *Data Minining and Knowledge Discovery* 2, pages 121–167, 1998.

[44] J. Adams, K. Parulski, and K. Spaulding. Color processing in digital cameras. *IEEE Micro*, 18(6):20–30, 1998.

[45] T. Gloe, K. Borowka, and A. Winkler. Chromatic aberration for digital image forensics. Submitted to MM&Sec'09, *Proceedings of the Multimedia and Security Workshop 2009*, 2009

[46] A. C. Popescu and H. Farid. Exposing digital forgeries in color filter array interpolated images. *IEEE Transactions on Signal Processing*, 53(10):3948–3959, 2005.

[47] M. Kirchner. Fast and reliable resampling detection by spectral analysis of fixed linear predictor residue. In *MM&Sec'08, Proceedings of the Multimedia and Security Workshop 2008*, September 22-23, 2008, Oxford, United Kingdom, pages 11–20, 2008.

[48] A. C. Popescu and H. Farid. Exposing digital forgeries by detecting duplicated image regions. Technical Report TR2004-515, Department of Computer Science, Dartmouth College, Hanover, NH, USA, 2004.

[49] M. K. Johnson and H. Farid. Exposing digital forgeries in complex lighting environments. *IEEE Transactions on Information Forensics and Security*, 2(3):450–461, 2007.

[50] M. K. Johnson and H. Farid. Exposing digital forgeries by detecting inconsistencies in lighting. In *MM&Sec'05, Proceedings of the Multimedia and Security Workshop 2005*, August 1-2, 2005, New York, NY, USA, pages 1–10, 2005.

[51] Bruce, V., Henderson, Z. & Burton, A.M. (2001). Matching identities of familiar and unfamiliar faces caught on CCTV images, *Journal of Experimental Psychology*. Applied 7, 207–218.

[52] Hancock, P.J.B., Bruce, V. & Burton, A.M. (2000). Recognition of unfamiliar faces, Trends in Cognitive Sciences 4, 330–337.

[53] Vanezis, P., Lu, D., Cockburn, J., Gonzalez, A., McCombe, G., Trujillo, O. & Vanezis, M. (1996). Morphological classification of facial features in adult Caucasian males based on an assessment of photographs of 50 subjects, Journal of Forensic Sciences 41, 786–791.

[54] Kemp, R., Towell, N. & Pike, G. (1997). When seeing should not be believing: photographs, credit cards and fraud, *Applied Cognitive Psychology* 11, 211–222.

[55] Henderson, Z., Bruce, V. & Burton, A.M. (2001). Matching faces of robbers captured on video, *Applied Cognitive Psychology* 15, 445–464.

[56] Scheuchenpflug, R. (1999). Predicting face similarity judgments with a computational model of face space, *Acta Psychologica* 100, 229–242.

[57] Face recognition algorithms surpass humans matching faces over changes in illumination. O'Toole, A.J., Phillips, P.J., Jiang, F., Ayyad, J., Penard, N. (2007) *IEEE: Trans. Patt. Anal. Mach. Intell*. 29, 1642-1646.

[58] Phillips, P.J., Scruggs, W.T., O'Toole, A.J., Flynn, P.J., Bowyer, K.W., Schott, C.L. & Sharpe, M. (2007). FRVT2006 and ICE 2006 Large-Scale Results. http://www.frvt.org/FRVT2006/docs/FRVT2006andICE2006LargeScaleReport.pdf

[59] Phillips, J.P., Grother, P., Michaels, R.J., Blackburn, D.M., Tabassi, E. & Bone, M. (2003). Face recognition vendor test 2002. http://www.frvt.org/DLs/FRVT_2002_Evaluation_Report.pdf

[60] Polymnia project (2006). http://polymnia.pc.unicatt.it/

[61] Andreas Kriechbaum, Werner Bailer, Helmut Neuschmied, and Georg Thallinger, 'Using the MPEG-7 colour structure descriptor for human identification in the POLYMNIA system', *Proceedings of I-KNOW*, pages 585-591, Graz, AT, Sept. 2006

[62] J. Yang and C. Liu: 'Color Image Discriminant Models and Algorithms for Face Recognition', *IEEE Transactions on Neural Networks*, vol. 19, no. 12, pp. 2088–2098, 2008.

[63] P. J. Phillips, P. J. Flynn, T. Scruggs, K. W. Bowyer, J. Chang, K. Hoffman, J. Marques, J. Min, and W. Worek, 'Overview of the face recognition grand challenge,' in *Proc. IEEE Conf. Comput. Vis. Pattern Recognit.*, 2005, vol. 1, pp. 947–954.

[64] Press release, Leeds 'Criminal' Finally Banned by YouTube, http://news.softpedia.com/news/Leeds-Criminal-Finally-Banned-by-YouTube-86427.shtml

[65] Press release, Officers increasingly using online social networks for Intel, 3 October 2007, http://www.policeone.com/investigations/articles/1360141/

[66] Press Release, De Belastingcontroleur, uw Facebook-vriend, *De Standaard*, 13 December 2008.

[67] Press release, British Police use Facebook to gather evidence, *ITworld*, 18 April 2008, http://www.itworld.com/police-use-facebook-to-collect-evidence-080418

[68] Considerations extracted from J.C. Russ, Forensic uses of digital imaging, CRC Press LLC, 2001.

[69] O. Leroux, Legal admissibility of electronic evidence, *International Review of Law Computers & Technology*, Volume 18, n°2, pp.193-220, July 2004.

[70] D. Brezinski and T. Killalea, Guidelines for evidence collection and archiving, *The Internet Society*, February 2002, available online at: http://www.ietf.org/rfc/rfc3227.txt

[71] ECHR, 25 February 1993, no. 10828/84, Funke v. France.

[72] ECHR, 16 December 1992, no. 13710/88, . Niemietz v. Germany.

[73] ECHR, 25 February 1993, n° 12661/87, Miailhe v. France.

[74] ECHR, 30 March 1989, n° 10461/83, Chappell v. United Kingdom.

[75] ECHR, 25 February 1993, n° 11471/85, Crémieux v. France.

[76] J. Pradel, Droit Pénale comparé, Précis Dalloz, 3rd ed., 2008, p.296

[77] Cass. 16 June 1987, Pas. 1987-I, n°627.

[78] Cass. 14 October 2003, Antigone, RCJB, 2004, pp.405 and following, note F. Kuby.

[79] ECHR, 25 September 2001, n° 44787/98, P.G & J.H.

[80] ECHR, 12 July 1988, n° 10862/84, Schenk v. Suisse.

[81] ECHR, 12 May 2000, no 35394/97, Khan v. Royaume-Uni,

[82] S. Shaoe, Search and surveillance, Ashgate, 2000.

[83] A. Ashworth, Human Rights, Serious crime and criminal procedure, Sweet & Maxwell, 2002, p.36

[84] Van Der Huslt J., ECHR and Criminal proceedings: the impact of the Convention on Human Rights on criminal proceedings in the European Union, 2002, p.445.

[85] ECHR, 15 June 1992, n° 12433/86, Lüdi v. Switzerland.

[86] ECHR, 28 January 2003, no. 44647/98, Peck v. United Kingdom.

[87] Garante per la protezione dei dati personali, Internet-Caso Peppermint : illecito « spiare » gli utenti che scambiano file musicali e giochi- 28 febbraio 2008, Divieto del Garante 28, Bollettino del. N.92/febbraio 2008.

[88] G. Butarrelli, Protection of personal data with regard to surveillance and Guiding principles for the protection of individuals with regard to the collection and processing of data by means of video surveillance, Report commissioned by the Council of Europe, 2000, p. 8, available on-line at: http://www.coe.int/t/e/legal_affairs/legal_co%2Doperation/data_protection/documents/reports_and_studies_by_experts/Y-Report_Buttarelli_2000.asp#TopOfPage (last access on 13th June 2007).

[89] Article 29 Data Protection Working Party, Opinion 4/2004 on the processing of personal data by means of videosurveillance, WP89, 11 February 2004, p.15

[90] Article 29 Data Protection Working Party, Opinion 4/2007 on the concept of personal data, WP136, 20 June 2007.

[91] L.A. Bygrave, Data Protection Law: approaching its rationale, logic and limits, Kluwer Law international, 2002.

[92] R. Jay, A. Hamilton, Data Protection Law and Practice, Thomson, Sweet and Maxwell, 2003, 2nd edition, p.178.

[93] Büllesbach A., Poullet Y., Prins C. (ed.), Concise European IT Law, Kluwer Law International, 2006, p.47.

[94] Council of Europe, Second evaluation report of the relevance of recommendation N°.R(87) 15 regulating the use of personal data in the police sector, Council of Europe, 1998).

[95] ECHR, 28 June 1984, n° 7819/77, 7878/77 , Campbell and Fell v. United Kingdom.

[96] ECHR, 4 December 2008, n° 30562/04, S. and Marper v. the United Kingdom

[97] Van Der Hulst J., ECHR and Criminal proceedings: the impact of the Convention on Human Rights on criminal proceedings in the European Union, 2002

[98] Germany: New Basic Right To Privacy Of Computer Systems, EDRI-gram - Number 6.4, 27 February 2008, http://www.edri.org/edrigram/number6.4/germany-constitutional-searches

[99] ECHR, 7 of August 2003, n° 36022/97, Hatton and others v. United Kingdom, §96;

[100] ECHR, 1st July 2008, n° 58243/00, Liberty and others v. United Kingdom, §56

[101] ECHR, 29 June 2006, no. 54934/00, Weber and Saravia v. Germany § 77,

[102] ECHR, 16 March 1989, n° 11105/84, Huvig v. France p. 41

[103] ECHR, 20 June 1988, n° 11368/85, Schönenberger and Durmaz v. Switzerland

[104] ECHR, 16 May 1983, n° 8691/79, Malone v. United Kingdom.

[105] ECHR, 26 March 1987, n° 9248/81, Leander v. Sweden

[106] ECHR, 16 February 2000, n° 27798/95, Amann v. Switzerland.

[107] ECHR, 30 July 1998, n° 27671/95, Valenzuela Contreras v. Spain

[108] ECHR, 18 February 2003, no. 58496/00, Prado Bugallo v. Spain, § 30,

[109] Cass. Crim. 25 October 2000, *Bulletin criminel* 2000 n°317, p. 318.

[110] C.A. Thijm, 'Oppassen met mobiele kiek', http://www.solv.nl/index.php?blz=3&nid=2807

[111] Pas de diffusion en ligne de photos de défilés de mode sans autorisation », 26/01/2007, http://www.legalis.net

[112] TGI Paris 18/09/2006, http://www.legalis.net

[113] CA Lyon 27 janvier 2005, http://www.juriscom.net

[114] Aanbeveling nr. 2/2007 van 28 november 2007 inzake verspreiding van beeldmateriaal (A/2007/033) ; BELGA News, 'Klasfoto's mogen niet zomaar op het Internet verschijnen', De Standaard, 18 December 2008.

[115] Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society, O.J. L. 22/06/2001, 1-19.

[116] Committee of Ministers, Declaration on the freedom of expression and information, 29 April 1982, 70th Session.

[117] C. Ruet, 'L'expression par l'image au regard de l'article 10 de la Convention Européenne des droits de l'homme in (ed.) P. Bloch, Image et droit, l'Harmattan, Paris, 2002, 33

[118] 'Regardless of frontiers', Association Ekin v. France, 17 July 2001, Recueil/Reports 2001, § 62.

[119] Autronic AG v. Switzerland, 22 May 1990, Publ. Eur. Court H.R, Series A, Vol. 178, § 47; Murphy v. Ireland, 10 July 2003, Recueil/Reports 2003, § 61.

[120] L. Van Gool, 'Forensische beeldverwerking' in W. Van de Voorde, J. Goethals en M. Nieuwdorp (eds.) Multidisciplinair onderzoek. Juridische en wetenschappelijke aspecten, Politeia, 2003, 227-230

[121] I. De Lemberterie et X. Strubel, « L'image manipulée » in (ed.) P. Bloch, Image et droit, l'Harmattan, Paris, 2002, 335-337

[122] J. Vande Lanotte en Y. Haeck, Handboek EVRM Deel 2 artikelsgewijze commentaar Vol. 1, 463

General references (Chapter 6):

L.E. Pettitti, E. Decaux, P.H. Imbert (eds), *La Convention Européenne des Droits de l'Homme, Commentaire article par article*, Economica, 1999.

Van Alsenoy B., *Legal Requirements for Privacy Evidences based on Log Views*, in FIDIS D14.6, 2009.