Computers in Industry 98 (2018) 34–47

Contents lists available at ScienceDirect

Computers in Industry

journal homepage: www.elsevier.com/locate/compind

Image super-resolution for outdoor digital forensics. Usability and legal aspects☆,☆☆

Salvador Villena[a], Miguel Vega[a], Javier Mateos[b], Duska Rosenberg[c], Fionn Murtagh[d], Rafael Molina[b], Aggelos K. Katsaggelos[e]

[a] Dpto. de Lenguajes y Sistemas Informáticos, Universidad de Granada, Spain
[b] Dpto. de Ciencias de la Computación e I. A., Universidad de Granada, Spain
[c] iCOM Research, Richmond, UK
[d] Centre for Mathematics and Data Science, University of Huddersfield, UK
[e] Department of Electrical Engineering and Computer Science, Northwestern University, Evanston, IL 60208-3118, USA

ARTICLE INFO

Article history:
Received 3 October 2017
Received in revised form 20 December 2017
Accepted 22 February 2018
Available online xxx

Keywords:
Super-resolution
Outdoor surveillance
Usability
Legal aspects

ABSTRACT

Digital Forensics encompasses the recovery and investigation of data, images, and recordings found in digital devices in order to provide evidence in the court of law. This paper is devoted to the assessment of digital evidence which requires not only an understanding of the scientific technique that leads to improved quality of surveillance video recordings, but also of the legal principles behind it. Emphasis is given on the special treatment of image processing in terms of its handling and explanation that would be acceptable in a court of law. In this context, we propose a variational Bayesian approach to multiple-image super-resolution based on Super-Gaussian prior models that automatically enhances the quality of outdoor video recordings and estimates all the model parameters while preserving the authenticity, credibility and reliability of video data as digital evidence. The proposed methodology is validated both quantitatively and visually on synthetic videos generated from single images and real-life videos and applied to a real-life case of damages and stealing in a private property.

1. Introduction

Digital Forensics encompasses the recovery and investigation of data, images and recordings found in digital devices in order to provide evidence in the court of law (cf. [1–6]). Digital evidence can be obtained from any devices capable of storing digital data, but there are strict national and international guidelines for its use in criminal and civil investigations as part of legal processes. The most common are the British ACPO [7] and US NIJ guidelines for the appropriate use of digital evidence [8] that includes gathering digital data, processing of digital data and the preparation of digital data to be presented in courts by both forensic and legal professionals.

Most of the Digital Forensics literature focuses on practical activities of gathering digital evidence, preparing it for presentation in courts and presenting it in court by legal professionals and expert witnesses. Issues of authenticity, reliability and credibility addressing the concerns of the legal professions have been raised and operational standards and structured processes devised in order to resolve them. They have provided regulation in digital forensic practice, but more needs to be done.

As well as being used to prove that a criminal act has been committed, digital evidence is required to aid in identification of the perpetrators, confirming alibis, identifying sources of documents and confirming their authenticity. There are, however, significant issues still to be addressed related to not only the increasing size of digital media, but also the complexity of their use. These complexities arise from an increasing number of users owning multiple devices capable of storing and sharing potential

☆ This work was supported in part by the Spanish Ministry of Economy and Competitiveness (MINECO) through projects TIN2013-43880-R and DPI2016-77869-C2-2-R, the Department of Energy under Grant DE-NA0002520, ONR award N00014-15-1-2735, NSF IDEAS program, DARPA ReImagine.
☆☆ Special thanks to Igor Borcic, lawyer, for legal advice and Dr Najah AlFaise for insightful discussions of the role of culture and religion in the status of digital evidence in legal process.

E-mail addresses: svillena@ugr.es (S. Villena), mvega@ugr.es (M. Vega), jmd@decsai.ugr.es (J. Mateos), research@icomict.org (D. Rosenberg), f.murtagh@hud.ac.uk (F. Murtagh), rms@decsai.ugr.es (R. Molina), aggk@eecs.northwestern.edu (A.K. Katsaggelos).

https://doi.org/10.1016/j.compind.2018.02.004
0166-3615/

digital evidence. In addition, the integration of digital evidence (and scientific evidence in general) is often influenced by social, cultural and religious factors that underpin legal systems in different countries (cf. [9]).

To generate those high resolution (HR) images of a scene, a general variational Bayesian approach to the super-resolution (SR) problem [10–12] is proposed. For the first time, the general modelling of Super Gaussian (SG) distributions [13] is applied to SR. SGs are priors capable of capturing the sparse distribution of edges within natural images. SG priors have been successfully applied to blind image deconvolution [14–16]. Here, they are combined with proper modelling of the observation process as well as the registration parameters in order to obtain a high quality HR image from a set of LR observations.

The rest of the paper is divided as follows. In the next section, a bibliographic study on the status of digital evidence and SR is presented. Section 3 introduces the SR problem and formulates it using the Bayesian framework. Then, in Section 4 a solution to the SR problem using variational Bayesian inference is proposed. The proposed methodology is applied, in Section 5, to the study of a real-life forensic case to help identify the culprits of damages in a property and synthetic video sequences generated from an image and a real-life video which allow to compare the resulting images both visually and numerically. Finally, Section 6 concludes the article.

2. State-of-the-art

Many studies of digital evidence in legal practice are focused on the reliability and acceptability of digital evidence as shown by categorisations of Levels of Certainty that were devised by Casey [3]. Therefore, in order to discover, examine and provide evidence to legal enforcement in criminal events, a wide range of issues need to be addressed [4]. As digital forensics is essentially a process of applying scientific methods to the discovery, examination and provision of evidence to legal enforcement in criminal events [17], the credibility of digital evidence requires not only understanding of the scientific techniques but also understanding of the legal principles. The procedures that traditionally safeguard the integrity of evidence, including digital evidence, involve establishing that an incident has occurred, determining the nature of the incident and identifying the culprits (as far as this is possible under specific circumstances). Unlike physical evidence, digital evidence is often regarded by legal professionals as fragile, that is, it can be lost, altered, damaged, or accessed by unauthorised personnel. It is therefore of critical importance that forensic investigations safeguard its integrity by exercising evidential controls, such as maintaining the chain of custody as well as ensuring that it is gathered and protected through structured processes that are acceptable to the courts. "Tainted evidence that may have been acquired or protected without the requisite level of security may be legally inadmissible." [18]. Guidance on the process of analysing and interpreting digital evidence is also necessary as it provides the structure to the analytical and interpretational processes so that different investigators working on the same digital evidence can obtain the same results. Furthermore, any changes to the digital evidence in the process of analysis and interpretation should be traceable and justifiable in order to preserve the credibility of both the evidence and the analyst in the eyes of legal professionals. This is quite a challenge given the volume, variety and complexity of digital evidence, and raises issues of selection and use of forensic tools as well as proficiency and competency of the investigators themselves [19].

In this context, video as evidence has to be authenticated so that it is clear whether it is original or an altered copy since the nature of the alteration may render it inadmissible in court. This could happen if, for example, it cannot be proved that in spite of the alterations the video still depicts the scene of the crime and that the location, date and time when the recording was taken have remained the same as in the original. Traditional approaches of evidential control, described briefly above, may not be sufficient to guarantee the authenticity of the video as evidence [20]. However, digital systems usually provide methods for authentication such as metadata or serial numbers hidden in the video [21] as well of stronger forms of identification based on the image or video itself. Sensors imperfections and noise, photo response non-uniformity [22] or defective pixels can help to authenticate digital images and videos (see [23,24].

Nowadays, surveillance cameras are ubiquitous and their recorded videos are often used to identify the perpetrator. However, surveillance cameras usually suffer from poor quality and low resolution which prevent identification on the frames as extracted from the recorder. Image SR can help bridge the gap between poor video quality and evidence gathering [25]. The image SR problem has received a lot of attention from the image processing and computer vision research community in the past two decades (see [26–29] for a review). We can distinguish between *Multiple-Image Super-resolution (MISR)* and *Single Image Super-resolution (SISR)*. SISR [30] allows to obtain a HR image from only one observed LR image by applying, for instance, interpolation [31–34] or machine learning techniques based on LR/HR image patches [35–39], see [40] for the use of deep learning techniques in image recovery problems. However, when a video sequence or a set of LR images is available, MISR is preferred.

MISR allows to infer a spatially HR image of a scene, from multiple LR images affected by warping, blurring, and the noise inherent to the capture process [41]. Frames of a video sequence may contain many small shifted or rotated LR images of a given object, caused by the acquisition process, and the camera and/or scene motion, from which a HR image can be obtained using MISR techniques. MISR can be applied to obtain either a single HR image from a sequence of many LR images or a HR image sequence from a LR image sequence [42–45].

Although some SR algorithms with application to forensic investigation [46–51] have been proposed (see [46–51]), they are mainly formulated from an image processing point-of-view. A few briefly discuss on the use in a court of law of SR (see [25] for instance) or image enhancement techniques in general [52,53] but, to the best of our knowledge, no-one discusses in depth the forensic aspects or analyses real-life cases where SR had an important role to play.

3. Problem formulation

Let us now describe the MISR problem, i.e., the reconstruction of a HR image $\mathbf{x}$ from a sequence of L LR observed images $\mathbf{y} = \{\mathbf{y}_k\}$, $k = 1, \ldots, L$, of the same scene.

Each LR image $\mathbf{y}_k$ consists of $N = N_h \times N_v$ pixels while the size of the HR image $\mathbf{x}$ is PN, where $\sqrt{P} \in \mathbb{N}$ is the factor of increase in resolution. In this paper we adopt the matrix-vector notation, images $\mathbf{y}_k$ and $\mathbf{x}$ are arranged as $N \times 1$ and $PN \times 1$ column vectors, respectively. The imaging process, illustrated in Fig. 1, introduces warping, blurring and downsampling, which is modelled as

$$\mathbf{y}_k = \mathbf{A}\mathbf{H}_k\mathbf{C}(\mathbf{s}_k)\mathbf{x} + \mathbf{n}_k = \mathbf{B}_k(\mathbf{s}_k)\mathbf{x} + \mathbf{n}_k, \tag{1}$$

where $\mathbf{A}$ is the $N \times PN$ downsampling matrix, $\mathbf{H}_k$ is the $PN \times PN$ matrix modelling sensor integration and blurring, $\mathbf{C}(\mathbf{s}_k)$ is the $PN \times PN$ warping matrix generated by the motion vector $\mathbf{s}_k$, and $\mathbf{n}_k$ is the $N \times 1$ acquisition noise. A detailed description of the explicit form of the warping matrices $\mathbf{C}(\mathbf{s}_k)$ in Eq. (1) can be found in [11]. The effects of downsampling, blurring, and warping are combined into the $N \times PN$ system matrix $\mathbf{B}_k(\mathbf{s}_k) = \mathbf{A}\mathbf{H}_k\mathbf{C}(\mathbf{s}_k)$, from which each row maps the pixels of the HR image $\mathbf{x}$ to a given pixel in the LR image $\mathbf{y}_k$.