2011 Sixth International Conference on IT Security Incident Management and IT Forensics

Forensics Investigations of Multimedia Data: A Review of the State-of-the-Art

Rainer Poisel
Institute of IT Security Research
St. Poelten University of Applied Sciences
St. Poelten, Austria
rainer.poisel@fhstp.ac.at

Simon Tjoa
Institute of IT Security Research
St. Poelten University of Applied Sciences
St. Poelten, Austria
simon.tjoa@fhstp.ac.at

Abstract

Digital forensics is one of the cornerstones to investigate criminal activities such as fraud, computer security breaches or the distribution of illegal content. The importance and relevance of this research fields attracted various research institutes leading to substantial progress in the area of digital investigations. One essential piece of evidence is multimedia data. For this reason this paper provides an overview of the state-of-the-art in the forensic investigation of multimedia data, the relationship between the various research fields and further potential research activities.

Keywords

Digital Forensics, State-of-the-Art, Multimedia Data, Survey, Source identification, Environment classification, Content classification, Content forgery, Data recovery approaches for multimedia files, Fragment Identification, Steganography and Steganalysis, Standardization

I. Introduction

Modern life is unthinkable without electronic data processing and communication. Never before, so many information processing devices (PC, laptops, smart phones or multimedia players, ...) have been used and this trend seems to continue. The fact that nearly every area of life is supported by electronic devices strongly contributes to the steadily increasing importance of digital evidence in crime investigations. According to [1] "...80 to 90 percent of cases today have some kind of digital evidence". For this reason, it is no big surprise that academic research puts a lot of efforts in the improvement of methods and practices that can support digital investigations.

One important element of electronic evidence is multimedia content. When investigating and analyzing multimedia content challenges such as the time restrictions, numerous formats or huge amount data arise. Another challenge is the highly dynamic environment with very short innovation cycles. This makes it difficult to stay up-to-date regarding the current state-of-research in the domain.

We therefore survey approaches focusing on the analysis of multimedia data. The main contribution of this paper is to provide practitioners and researchers with a state-of-the-art overview of techniques to investigate multimedia data.

The remainder of this paper is structured as followed: Section II gives an overview about state-of-the-art research within the individual areas. Subsequently, we provide related work in section III. In the last section we conclude our findings and outline our future work.

II. Identification of fields for further research

Overview for scientific research fields for digital forensics have been outlined in a couple of publications [2], [3], [4]. As mentioned before this paper keeps the classification of forensics methods on the content investigated [5]: images, audio and video content.

A. Source identification

This field tries to determine the device which has been used to create specific content. The scenario can be compared to gun identification in general forensics: bullets leave scratches on obstacles they hit and so do cameras with images they take. Lanh [3] and Sencar [2] mention the potential devices for identification:

978-0-7695-4403-8/11 $26.00 © 2011 IEEE
DOI 10.1109/IMF.2011.14

1) Digital cameras: While there are many features available for the identification of digital cameras (e. g. peculiarities of the JPEG compression, the color filter array (CFA), sensor imperfections, etc.) [3] most publications rely the sensor pattern noise (SPN) to identify the source device. SPN is usually caused by influences during the sensor production cycle: individual pixels show a different sensitivity to light because of inhomogeneity of silicon wafers. The fingerprint for an individual camera is also known as photo response non-uniformity noise (PRNU). The major problems of this approach are the contamination of SPN with details from scenes [6] and the denial of the acquisition of a clean fingerprint of the camera because of its absence. As a a solution to the contamination problem the influence of details from the scene where attenuated on sensor patterns to improve the correct rate of device linking. The main advantage of this approach is, that it is possible not only to identify "camera models of the same make, but also individual cameras of the same model" [7].

Li [8] improved the PRNU approach further by considering the CFA as well. This approach was then called colour-decoupled PRNU (CD-PRNU). In digital cameras not every color component is captured when a picture is taken. For each pixel a specific physical color is acquired. The resulting artificial color of an individual pixel is determined by interpolating its physical color and the colors of its neighbor pixels. The CFA is predefined by the manufacturer. That makes it a valuable additional source for the identifcation of the source digital camera [8].

2) Scanners: Digital cameras can be understood as a device for the reproduction of natural scenes whereas scanners are often used to capture hard-copy media. Intrinsic sensor noise features are altered by several different postprocessing operations. That makes the methods presented here applicable for the detection of content forgery of analogue images, such as scans from traditional paper checks, as well. The approach chosen by Gou et al. to identify the source device scanner took three different aspects into count: image denoising, wavelet analysis and neighborhood detection [9]. From each characterization moment-based features are extracted then to determine the source device.

3) Video cameras: For this area techniques known from the picture- and audio-domain can be transfered [5]. The sensor types used in digital cameras and camcorders are similar. That is why approaches which regard sensor pattern noise can be applied in this field as well. The vast amount of frames in video data leads to better results for source camera identificaiton compared to source digital camera identification. Houten et al. [10] showed that successful identification was even possible after uploading videos with different quality settings and unknown parameters to the YouTube platform.

B. Environment classification

The classification of the environment of digital multimedia data tries to determine the location and the local conditions of the place where the data has been taken or recorded. The context for such a classification depends on the type of media investigated.

1) Visual Data: In case of visual data, the classification of the recording environment can be divided into the two subgroups of event recognition and place instance recognition. The former has been described by Li and Fei-Fei [11]: objects in an image have been assigned semantic labels to gather information on the elements which make up the event displayed in a picture. In e. g. a rowing scene, elements such as a lake, athletes, a rowing boat, water, etc. have been identified and fed into a integrative graphical model to determine the class of sport game. A similar approach by Luo et al. [12] has been developed to perform semantic event recognition. Satellite images provided by Google Earth$^{\text{TM}}$have been gathered based on the GPS (Global Positioning System) coordinates of a tagged photograph. By using a multiclass AdaBoost engine the terrain environment could be predicted when given a satellite aerial image of the location.

Other approaches focus on place instance recognition. Wu described an approach which "mainly encodes the structural properties within an image and suppresses detailed textural information" [13], [14].

Some approaches for the classification of content in visual data incorporate the context to improve accuracy. Divvala et al. [15] use the term "context" to refer to various types of meta- and environmental-information such as the "geographic context" (GPS location, elevation or population density) or "2D Scene Gist Context" (global image statistics). This meta-information is used as an input parameter to object classification algorithms to determine the possibility of object/context combinations.

2) Audio Data: Recent research projects show that there is a close relation between environment classification and source identification for auditive information. Information that describes both the environment and the recording source is located in hidden locations which can be detected with known approaches from the field of steganalysis [16]. The following kinds of information in auditive recordings is covered in this review paper:

- the region where the recording has been taken,
- the local conditions depending on the spatial conditions and
- the recording location depending on side noises which are identified through content analyzation.

The Electrical Network Frequency (ENF) is contained in some audio recordings because of the magnetic field which is emitted by devices connected to an electrical outlet [17]. Because of the stability of the ENF signal it is possible to determine the place and the time when a recording was carried out [18]. According to resesarch results by Grigoras [19] the location can be estimated down to the "city-level" when he was able to show the differences of the ENF between locations that were approximately 400km apart from each other.

3) Video Data: can be classified by a combination of the methods used for visual and auditive data. The approaches are related to the basic types of which this kind of media is made of. Wu and Rehg [14] refer to the identifaction of video data by using methods developed for the environment classification in digital images.

C. Content classification

Storage media has been becoming steadily cheaper over the years. Hard-disks built into personal computers with capacities in the range several hundred gigabytes and up have led to an amount of information which cannot be processed manually by humans anymore. Currently the data which has to be investigated in a single case amounts to several terabytes [20]. Therefore a common problem of digital forensics investigators is the lack of time when analyzing large collections of content [21]. Even when working with techniques that are supported by automation there is still the problem of false-postivies and -negatives. Processing this reduced amount of data, humans suffer absorbability and exhaustion [22]. Type I and II errors can be led back to the lack of efficient detection algorithms [23]. Typical applications for the field of content classification could comprise the identification of almost anything, but most research results have been published in the classification of recovered video and digital image files for pornography from computer systems as well as material from surveilance cameras and evidence related to financial crime (e. g. contraband image analysis).

Castro Polastro classified digital images containing nudity by considering both file names and image analysis [24]. The algorithm proposed by [25] was implemented for the classification part of the project. Compared to former approaches the algorithm for skin detection processed images in RGB color space directly which resulted in a higher processing speed. The overall success-rate for classifying data containing nudity was 95%.

The bag-of-visual-words (BOVW) approach for the detection of nudity in images was described by Deselaers et al. [26]. This algorithm treats pictures as if they were built from discrete visual words. To classify images vocabulary has to be learnt from a task-specifical training database. Learnt vocabulary is used to represent pictures as a histogram. Then filtering rules are set up to classify the different amounts of pornography that can be seen in an image. The algorithm finally calculates a probability value to automatically classify images based on learnt data. The results generally outperformed algorithms which were based on skin detection.

Regarding the classification of video media, both keyframes as well as motion analysis is performed to classify content [21]. Keyframes are analyzed for skin regions (average skin probability, ratio of skin pixels and size of the largest skin region) which are then classified using a support vector machine (SVM). Another approach to keyframe analysis was based on the BOVW methodology. A histogram was constructed based on the count of how often visual words occured. This histogram was used as a feature vector for a SVM to support the classification of pornographic content. The motion analysis part was performed by testing three different approaches: Periodicity Detection (PER, to detect periodic motion patterns), Sliding Window Periodicity (PERWIN, to detect smaller parts where repetitive motion occurs) and Motion Histograms (MHIST, to detect where and which motion occurs).

Finally a weighted sum fusion of the classification scores was used to calculate the total probability of the content to contain pornography. Best results could be gained by combining the BOVW with the MHIST approach.

D. Content forgery

Approaches for detecting content forgery exist for the three domains of visual, auditive and video data. The following section presents the state-of-the-art in these fields.

1) Visual data: This field comprises the modification of digital images. The forgery of digital image data can be classified in seven different fields [27]:

- Copy-move forgery is also known as "cloning" because of duplicated image sections. An example has been given by the online service of the Iranian Revolutionary Guards [4]. A picture showing the launch of several Iranian missiles from the Iranian Daily Jamejam has been modified to show one non-functioning missile. The forgery was detected using Popescu et al.s approach of exposing digital forgeries [28], [29]. Bayram et al. published a survey of copy-move forgery detection techniques [30] which led to the proposal of a robust method for the detection of this kind of tampering [31]. This approach was based on several techniques. Features were extracted from image blocks by using Fourier-Mellin Transform (FMT). These features were robust to lossy JPEG compression, blurring or noise addition as well as scaling and rotation operations. Compared to approaches proposed before the authors attempted to replace lexicographic sorting with counting bloom filters which resulted in faster processing times. The results showed that the detection of image tampering was robust up to JPEG quality better than 20, rotation of less then 10 and scaling of up to 10%.

- Retouching, e. g. to make some digital images more appealing to the audience,
- filtering of unwanted parts of an image,
- partial deletion of specific objects,
- mounting and merging which is used to combine image information from different pictures. The latter is also known as "image splicing" [32].
- manipulation of luminance, color space or contrast to make showed information more appealing or spectacular and
- manipulation of the geometry to influence the relation of objects.

Different approaches for each of the presented forgery methods exist. Based on their complexity digital image tampering detection techniques can be classified into three different levels [33]:

- Low Level: Digital image pixels or DCT coefficients are used to engage statistical investigations on this level. Some image tampering approaches break up consitency between adjacent pixels which have been made consistent using gamma correction during the image acquiring process. Strongly related to source identification since SPNs are modified in case of modified images [3].
- Middle Level: Traces of tampering operations are detecting with the help of simple semantic information. Content which has been copied into the medium cause sharp edges or areas which are blured artificially. Inconsistencies in the lighting direction also count to this level of tampering detection.
- High Level: Comprises purely semantic tampering detection methods. As an example for this level a picture containing both George W. Bush and Osama bin Laden shaking hands was given. The automated identification of such a tampered image would at least require a computer to identify the characters properly as well as a mechanism to classify this combination as impossible.

The higher the level, the more complex are the methods for automated detection of image tampering. In contrast to the high level approaches, low level methods target to verify the homogeneity of the digital representation of image data.

Farid proposes in his talk [34] that producers of digital cameras develop forgery resistant devices by adding watermarking technology. Embedded secret data should also include the recording position.

2) Auditive data: Detecting the forgery of auditive data can be performed in several ways. Maher stated that "the examiner needs to perform visual, physical, electrical, and acoustical tests that include" [35]:

- a review of the documented history of the evidence,
- a properly used recording device,
- mechanisms that verify the integrity of the recording medium,
- critical listening to the entire audio recording,
- checks for continuous operation with no unexplained interrupts and
- the usage of analytical tools (e. g. spectral analysis software) to identify irregularities.

Further Maher explained that recordings of surveillance devices should be audibly marked (date, time location, identity of participants, etc.) at the beginning to able to proof continuous recording operation [36]. To verify the authenticity of auditive material it is also possible to visualize changes of background sounds in a frequency spectrum. In case foreground sounds have been edited or exchanged an alternation of the background sounds can be observed. Another approach for proofing the authenticity of auditive signals "uses the residual pickup fo eletrical power line magnetic fields by the audio recording device" [35]. A comparison of measured electrical network frequency (ENF) from an audio recording with a database of known ENF measurements can show that a recording has been taken in a specific place at a specific time [37].

Bender et al. presented several techniques for embedding information in auditive cover media [38]. Approaches which are based on the digital representation of auditive data, e. g. low-bit coding or least significant bit-coding (LSB-coding) are fragile to modification of the cover media. Therefore it can be used to detect tampering of auditive data as long as an investigator has the original information.

3) Video data: For the detection of tampering in video data the approaches can be classified as given in the detection of image data manipulations. Wang gave the example of a Russian talk show in which a political activist was digitally erased [39]. The forgery was detected through semantical analysis, a high level approach, by humans since the technicians neglected to erase the legs of the politic activist in one frame.

Wang presented approaches which can be compared to the detection of digital image tampering on the middle level [40]. The techniques were classified into two groups: the detection of duplicated frames and the duplication of regions across frames. For the detection of duplicated frames a correlation coefficient was introduced as a measurement of similarity. In case of stationary surveillance cameras the coefficient of sub-sequences is ignored to avoid the problem of numerous duplications due to the static scene. For the detection of region duplication a normalized cross power spectrum was presented to detect duplicated areas using phase correlation.

Low level approaches comprise the detection of video tamperings through artefacts that occur when video data is encoded more than once [41]. Another approach based on noise characteristics differentiated video material that has been taken using another camera by detecting inconsistencies of irradiance-dependent noise [42]. This technique only worked for static scenes but being able to detect moving objects has been proposed as a future research field in this publication.

With video data being a combination of visual and auditive information the approaches presented in the detection of auditive data tampering can be applied as well.

E. Data recovery approaches for multimedia files

With digital content being stored on nowadays vast number of storage devices the number of required techniques for recovering data has increased significantly. In contrast to traditional data recovery file carving is independent of system metadata. The following places are predestined for finding data using this technique:

- Unallocated-space: which is not assigned to partitions of a hard-disk [43],
- Slack-space: which "occurs when the size of a file is not a multiple of a data unit size" [43],
- Swap-space: which is used for the computer to use more random-access memory than it actualy has [44],
- Memory areas which have been marked corrupt [43],
- Computer memory: which contains the data structures of running applications and operating systems [45],
- Flash-memory: which can be found in almost all portable devices [46] and
- Host Protected Area: which can be programmed by special ATA-commands into the hard-disk controllers of personal computers [43].

Actually file carving aims to support investigators in efficient recovery from storage devices, but nevertheless it is currently necessary for humans to actively participate in the process as there is a chance for false positives to be recovered. Once the areas for hidden data are identified, the process of data recovery can be broken down into several steps [47]. The three major steps for file carving are:

- In the identification phase files have to be found in a forensic image. This comprises the classification of file fragments and the identification of file fragmentation points to put fragments back together.
- During the validation phase found files are checked if they can be decoded properly using so called validators or decoders. The main problem here is the vast amount of available file formats.
- In the last step a human expert has to validate found data based on its content. False-Positives are sorted out, e. g. bad files that are irrelevant for the investigated case.

The following sections summarize existing file carving approaches. They are sorted by the properties they consider to get back the content of files in the original order.

1) File-Signature-Based Carving: File fragments are identified by comparing byte-sequences (also refered to as magic bytes or magic numbers) contained in headers and footers with values stored in a database containing well known values for specific file types. Former file carving approaches where computationally intensive and required large amounts of memory. Scalpel [48] was introduced to overcome these limitting factors.

The operation of Scalpel is performed in two sequential passes. During the first pass the whole disk image is indexed by reading chunks of several megabytes and searching for file headers. After finding headers in a chunk, footers are identified as well and stored in a database. This database is analyzed to only contain header-footer tuples which fulfill the constraints for the maximum size of files to be recovered. The contents of the database are used to put up working queues which contain locations for the file extraction process in the second pass. During the second pass the disk image is again processed in chunks to copy recovered files to the place where recovered files are kept.

Carving files using Scalpel has further been improved [49] by removing the final step of copying recovered files. Instead a file system is developed using the FUSE [50] library. The user accesses the investigated storage area by mounting an image using the Scalpel filesystem in which the contents of the header-footer database are presented as actual files.

Further improvements for the carving of contiguous files have been categorized based on different properties for files to be recovered [51]:

- Header/footer carving: for extracting data between distinct start and end of file markers (string sequences),
- Header/maximum size carving: with additional analysis for the longest valid string sequence that still validates,
- Header/embedded length carving: which can be used for file formats that do not have distinctive footers for the end and
- File trimming: for "byte-at-a-time formats" that do not have obvious footers by trimming characters at the end until the file no longer validates.

2) Steps toward fragmented file recovery: To support the recovery of files which are fragmented into two or more fragments the "Fragment Recovery Carving" (also known as "split carving") approach has been introduced [51]. After analyzing over 350 disks Garfinkel found out that files fragmented into two pieces are the most common. He called this kind of fragmentation therefore "bifragmentation". Pal [45] summarized Garfinkel's recovery approach as "Bifragment gap carving recovery occurs by exhaustively searching all combinations of clusters between an indentified header and footer while excluding different number of clusters until a successful decoding/validation is possible".

For the recovery of bifragmented files Garfinkel introduced the fast object validation procedure. It only works for file types which have to be decoded before their content can be interpreted because the validation is based on a successful decoding procedure. This is the case for JPEG, PNG, PDF, ZIP, Microsoft Office files, etc. To find the gap between two fragments all possible combinations of clusters between found headers and footers are tried until the file can be decoded successful.

This approach has been criticized [45] because it is limited in several ways. The technique does not scale well for files fragmented with large gaps. It does not work with files which are fragmented in more than two fragments, it only works for files that have a structure and have to be decoded. Finally successful validation does not imply that a recovered file is assembled correctly, because decoders often accept files reconstructed from fragments of different files.

Pal [52] extended Garfinkel's approach for bifragmented files by utilizing a Sequential Hypothesis Test (SHT) procedure. To identify the fragmentation point of a file two hypotheses are put up: H_0 states that subsequent blocks of the currently investigated block belong in sequence to the fragment, and H_1 which states that subsequent blocks do not belong in sequence to the fragment. With H_0 being true each block is analyzed until either H_1 is achieved, the file is completely recovered or an error occured because no data-block remains or a different file type has been determined for the remaining blocks. This methodology can also be used to extend the "Parallel Unique Path" graph theoretical approach for digital images [53].

3) Graph Theoretic Carvers: File carvers assembling fragments based on graph theoretical algorithms have been proposed especially for text-based media by Shanmugasundaram [44], [54] as well as for digital images by Pal [53].

Approaches for text-based data proposed by Shanmugasundaram assign candidate probabilities for their adjacency to recovered file fragments. For text-documents these probabilities can be determined using a slinding-window algorithm which evaluates the statistics for symbol usage in a language or, for generic data, is based on statistical models used for data compression. Probabilities which have been assigned to fragments are then used to determine the permutation which maximizes the sum of candidate probabilties of adjacent fragments. This mathematical problem is equivalent to finding a maximum weight Hamiltonian path in a complete graph. Since this problem turned out to be intractable [55], heuristics have been introduced to provide the best solution. The approach proposed by Pal [53] assigns probabilities to file fragments of digital images which are then put together using different graph theoretic algorithms, e. g. an adapted version of the Shortest Path First (SPF) algorithm which yielded the best results for seven datasets of images.

4) Approaches based on JPEG-Specifics: The number of different graphics formats used in web-content is low. With the JPEG-format being one among these lots of related work in this field concentrated on this format. Karresand et al. propsed a method which uses the so called restart markers (RST) of the JPEG file format to reassemble non-differential Huffman entropy coded baseline sequential Discrete Cosine Transform (DCT) JPEG image fragments [56]. With restart markers being used the scan is interrupted at regular intervals by a specific bit pattern. Further raw pixels of an image are grouped into 8x8 pixel blocks which are transformed into the frequency domain using Discrete Cosine Transformation (DCT). Most important item here is the first which represents the zero frequency DC coefficient.

The data between RST markers is called Minimum Coding Unit (MCU) and it is the smallest part of an image which can be decoded if it is intact. Luminance DC values in all restart intervals are used to form DC value chains. The DC component chains are then analyzed using a sliding window approach to identify the order of fragments of a specific image.

Enhancements using different aspects, e. g. by considering the Define Huffman Table (DHT) segment, of the JPEG-format have been proposed [57], [58].

5) SmartCarving: Reassembling objects out of their fragments which are randomly mixed with fragments from other files is a problem that can be found in many different disciplines. To overcome the lack of research in the field of digital forensics Pal et al. [59] proposed a generic approach for images which comprises the following three steps for a document reassembly process (see figure 1):

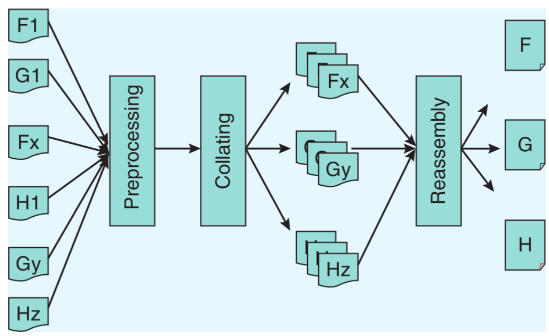

Figure 1. The three components of SmartCarving [45]

- Preprocessing: During this step investigated data is prepared to be usable by forensics investigation methods. This comprises the decryption of encrypted devices, as well as the removal of all known clusters base on file system metadata.
- Collating: The identification of fragments is performed during the second phase. After their identification fragments are collected in groups of the same type to be assembled into their original files in subsequent steps.
- Reassembling: Finally the fragments recovered in the previous phases are reassembled to their original files. It is therefore necessary to find the fragmentation points for each unrecovered file. In case of incorrect reassembly recent tools, e.g. [60], present the investigator a small number of potential orderings during manual inspection of recovered data.

As SmartCarving consideres file-system meta-data as well as different approaches to file fragment identification and file fragment reassembly it can also be understood as a combination of approaches presented in previous sections of this chapter.

F. Fragment identification

Classifying fragments determined during a recovery is an essential step for finding the parts of a whole file. Up to now different approaches have been worked out. Early approaches consulted "magic numbers" which could be found in files from the same type. This worked out fine for whole files or fragments which contained these magic numbers coincidently. Therefore approaches dealing with statistical evaluation of the content of fragments have been developed [61], [62], [63]. The results of a classification where quite modest and have therefore been criticized [64]: 78% of executables and only 18% of zip-files could be identified. On the other hand this approach worked well for html- and jpeg files with more than 98% success rates. Roussev and Garfinkel therefore recommended specific approaches depending on the content/file type which should be recovered [64].

G. Steganography and Steganalysis

While cryptography focuses primary on the protection of private information by rendering a message inapprehensible to outsiders, steganography conceals the existence of secret information at all [65].

Bender et al. [38] outlined different approaches for hiding information in both visual and auditive cover media. For auditive information four different techniques are described:

- Low-bit coding (also referred to as "LSB-hiding"): hides information in data structures such as the digital representation of digital audio. In this case only the least significant bits (hence the name "LSB-hiding") are used to minimize the effect of changing information.

- Echo hiding: an echo is introduced into the host audio signal. The secret information is then represented by the variation of three different parameters (offset, decay rate and the initial amplitude).
- Phase coding: hides information "...by substituting the phase of an initial audio segment with a reference phase that represents the data." [38]
- Spread spectrum: hides the secret signal by multiplying it by a chip, so that it is spread over the frequency spectrum.

Digital image steganography can be classified into different categories: "...spatial domain, frequency domain and adaptive methods" [66]. Algorithms used in audio steganography can be transformed into the image domain. However the parameters specific to the cover media have to be adapted.

On the other hand steganalysis refers to "...the detection of embedded information" [67] which has been hidden by using steganography techniques. In other words it is "the goal ...to detect embedded data present in the cover medium" [91]. Therefore steganalysis can be understood as a countermeassure to steganography [68]. Nissar and Mir categorize steganalysis techniques into signature based and statistical based approaches which are further split up into two classes: "specific" and "universal" techniques [65].

For further details we refer the interested reader to [65], [69] , [66], [70], [71] and [72].

H. Standardization

In the context of forensics, standards ensure accurate and reliable results [73]. Wiles et al. [73] classify standards into two groups: "paper standards" and "material standards". The former relates to the description of sets of procedures for performing specific activities and the latter refers to actual tools which can be used when conducting procedures. In the following an overview of the situation in both the USA and the UK is given.

In the United States of America the American Society of Crime Lab Directors/Laboratory Accreditation Board (ASCLD/LAB) utilizes appropriate controls and standard samples to ensure the validity of results [74]. Since 2003 the ASCLD/LAB considered digital evidence in its roster of accredited disciplines. Therefore the analysis of digital evidence is subject to the same controls and standard samples as other analyses.

Regarding the situation in the United Kingdom, Ramsthaler et al. [27] mention an early approach to the standardization of the forensics process (1999). Since then the process of the British Standards Institution has been revised in both 2004 and 2008 [75]. In this document guidance is given for the electronic creation, storage and the retrieval of information. A further approach to standardize the forensic process is outlined in the ACPO good practice guide for computer based electronic evidence [76].

Besides of that standards independent of a specific country have been defined as well. For example ISO 17025:2005 [77] specifies general requirements for carrying out tests and/or calibrations, as well as sampling. The Internet Engineering Task Force (IETF) is responsible for the development and the promotion of recommendations in the field of Internet technology in cooperation with other standards bodies such as the ISO/IEC. Some of their Request For Comments (RFCs) propose standardized procedures in the context of digital forensics:

- Fraser [78] published RFC2196 as a guide for the development of "computer security policies and procedures for sites that have systems on the Internet". Besides the response to security incidents a broad range of technical system and network security topics is presented.
- RFC 2350 [79] gives "general Internet community's expectations of Computer Security Incident Response Teams (CSIRTs)". As an answer to the needs of CSIRTs formal templates and filled out examples are presented.
- Shirey [80] proposed the "Internet Security Glossary" in RFC 2828. This publication was intended to standardize definitions of terms mentioned in the context of Internet security related documents.
- Brezinski [81] proposed RFC 3227. In this document "Guidelines for Evidence Collection and Archiving" were presented to system administrators to standardize the collection and archiving of evidence which is relevant in case of a security incident.

The need for standardization and certification has already been expressed several times. Meyers and Rogers [82] mentioned the fields in which standardized procedures are needed: search and seizure, expert qualifications as well as analysis and preservation. For clarification US federal and state court cases were analyzed with regard to their lack of standardization and certification. Slay et al. [83] previews the development of digital forensics models, procedures and standards to lay a foundation for the discipline. In their document mainly the procedures for digital forensics investigations but no specific standard is given.

Garfinkel et al. [84] states that there have been some advances in the field of common file formats, schemas and ontologies but there has only been little actual standardization. Regarding the standardization of forensic data sets - corpora - for research purposes Garfinkel et al. [85] published a paper to clear the dilemma at least in this context. Beebe et al. [86] concretizes the issue in "The Band" as well as in "The Unaddressed". Regarding the response to incidents and the collection of evidence data the digital forensic community has almost "hyper-formalized" processes and approaches, but actually there is no single, universal standard for this subfield of digital forensics. Further the small amount of widespread knowledge is heavily focused on the investigation of computers with Windows, and to a lesser extent Linux based, operating-systems installed.

III. Related Work

Different reviews of the state-of-the-art for general digital forensics have been given recently. While some focus on general research agendas [84], [87] , [86] others focus on education [88] or on both fields [89].

Digital forensics is no longer a niche discipline [86]: "It is now mainstream knowledge that the footprints that the digital footprints that remain after interactions with computers and networks are significant and probative. Even popular crime shows and novels regularly incorporate digital evidence in their story lines." The effort spent up to now on research in this area is therefore vast. With the term of digital forensics existing since the late 1980s [84] it has undergone many different definitions. Further many research subfields which are also covered by the definition of digital forensics have been developed. Böhme et al. classified the term of forensics into digital and analog forensics with the latter being subclassified into the terms "Multimedia Forensics" and "Computer Forensics" [4]. The motivation of the publication [4] was the clarification of the blurred definition of computer forensics. The latter deals with information with no or only little interpretation compared to methods covered by multimedia forensics. Further it is often difficult to study these two different fields separately. E. g. if a police search results in a hard disk image with digital images, the photographs can be found using computer forensics methods. Further investigations regarding the camera model which has been used to take the pictures are performed techniques from the field of multimedia forensics.

As mentioned by Nance [87] "digital forensics is a largely practitioner-driven field". Therefore new developments can be understood as a reaction to a class of incidents or to a specific incident. Garfinkel [84] stated that the Golden Age which lasted from the years 1999 to 2007 was marked by a rapid growth in digital forensics research and professionalization. According to the Digital Forensics Association [90] there are 15 certification programs, 16 bachelor programs and 13 masters degree programs. Further the Golden Age was characterized by relatively few different file formats of forensic interest, the widespread use of Windows XP, examinations which had to be performed on single computers and a low number of different standardized interfaces for storage devices.

Among others, the challenges which have to be faced by multimedia data forensics now can be summarized [84], [87]:

- The growing size of storage devices which results in insufficient time to create a forensic image or to process all data.
- The increasing number of different hardware interfaces results in devices that cannot be removed or imaged readily.
- The number of different operating systems and file formats has increased vastly. Therefore the cost for developing digital forensics tools has increased because of increased complexity of data exploitation tools.
- Data structures are split into elements to be stored on different devices and places. This can be seen as a result of cloud computing.

IV. Discussion and Conclusion

Nowadays, through the widespread usage of electronic devices, digital forensics gets increasingly more important. The crimes investigated range from fraud and computer security breaches to distribution of illegal content. One essential piece of electronic evidence is multimedia data. The main challenges arising when analyzing this kind of data are the limited amount of time to investigate content, the huge amount of data and different multimedia codecs and formats.

In order to face this challenges state-of-the-art research results for investigating multimedia data have been presented. Figure 2 summarizes the outcome by providing an schematic overview of presented fields of research as a UML-diagram. The relations between the different fields are either displayed as composition or as inheritance. In the case of inheritance, the parent field of research is fundamental to more specialized fields of research.

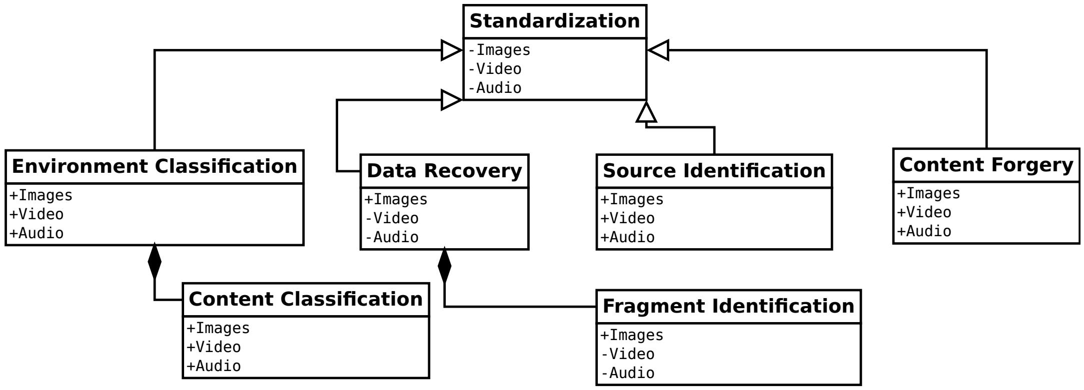

Figure 2. Relationship between identified fields of research

Standardization is the key element for all research areas in order to best support collaboration as well as usage by practitioners and researchers. Therefore all elements are connected to this entity. The attributes of shown classes refer to the type of media investigated. The availability of techniques for the investigation of certain types of media is displayed through the visibility of the attribute. Public visibility refers to research being performed in the field to which it refers and private visibility can be understood as a field for future research.

The new challenges of the highly dynamic field of multimedia data investigations have been addressed by the scientific community, leading to substantial research results as presented in this paper. However, there are still many unresolved challenges. The recovery of video files from their fragments turns out to be uncharted beside a vast amount of research being performed on file carving for digital images. Therefore our next step is going to be the development of a method for video fragment carving.

REFERENCES

[1] K. Medaris and R. Mislan. (2008, April) Expert: Digital evidence just as important as dna in solving crimes. [Online]. Available: http://news.uns.purdue.edu/x/2008a/080425T-MislanPhones.html

[2] N. D. M. Sencar, H. T., "Overview of state-of-the-art in digital image forensics," in *WSPC - Proceedings*, September 2007.

[3] T. V. Lanh, K.-S. Chong, S. Emmanuel, and M. S. Kankanhalli, "A survey on digital camera image forensic methods," in *ICME*, 2007, pp. 16–19.

[4] R. Böhme, F. C. Freiling, T. Gloe, and M. Kirchner, "Multimedia forensics is not computer forensics," in *IWCF*, 2009, pp. 90–103.

[5] J. Fürch and J. Meyer, "Digitale multimediaforensik," TU-Darmstadt, Tech. Rep., 2010.

[6] C.-T. Li, "Source camera linking using enhanced sensor pattern noise extracted from images," in *Proc. the 3rd International Conference on Imaging for Crime Detection and Prevention (ICDP-09)*, 2009.

[7] ——, "Source camera identification using enhanced sensor pattern noise," *IEEE Transactions on Information Forensics and Security*, vol. 5, no. 2, pp. 280–287, 2010.

[8] Y. Li, C.-T. Li, "Digital camera identification using colour-decoupled photo response non-uniformity noise pattern," in *Proceedings of 2010 IEEE International Symposium on Circuits and Systems (ISCAS)*, 2010.

[9] H. Gou, A. Swaminathan, and M. Wu, "Intrinsic sensor noise features for forensic analysis on scanners and scanned images," *Trans. Info. For. Sec.*, vol. 4, pp. 476–491, September 2009. [Online]. Available: http://portal.acm.org/citation.cfm?id=1651180.1651198

[10] W. van Houten and Z. Geradts, "Source video camera identification for multiply compressed videos originating from youtube," *Digital Investigation*, vol. 6, no. 1-2, pp. 48–60, 2009.

[11] L.-J. Li and L. Fei-Fei, "What, where and who? classifying events by scene and object recognition," *Computer Vision, IEEE International Conference on*, vol. 0, pp. 1–8, 2007.

[12] J. Luo, W. Hao, D. McIntyre, D. Joshi, and J. Yu, "Recognizing picture-taking environment from satellite images: A feasibility study," in *ICPR*, 2008, pp. 1–4.

[13] J. Wu and J. M. Rehg, "Where am i: Place instance and category recognition using spatial pact," *Computer Vision and Pattern Recognition, IEEE Computer Society Conference on*, vol. 0, pp. 1–8, 2008.

[14] ——, "Centrist: A visual descriptor for scene categorization," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 99, no. PrePrints, pp. 1–14, 2010.

[15] S. Divvala, D. Hoiem, J. Hays, A. Efros, and M. Hebert, "An empirical study of context in object detection," *Computer Vision and Pattern Recognition, IEEE Computer Society Conference on*, vol. 0, pp. 1271–1278, 2009.

[16] C. Kraetzer, A. Oermann, J. Dittmann, and A. Lang, "Digital audio forensics: a first practical evaluation on microphone and environment classification," in *Proceedings of the 9th workshop on Multimedia & security*, ser. MM&Sec '07. New York, NY, USA: ACM, 2007, pp. 63–74. [Online]. Available: http://doi.acm.org/10.1145/1288869.1288879

[17] E. B. Brixen, "Enf; quantification of the magnetic field," in *Audio Engineering Society Conference: 33rd International Conference: Audio Forensics-Theory and Practice*, 6 2008. [Online]. Available: http://www.aes.org/e-lib/browse.cfm?elib=14412

[18] D. P. N. Rodríguez, J. A. Apolinário, and L. W. P. Biscainho, "Audio authenticity: detecting enf discontinuity with high precision phase analysis," *Trans. Info. For. Sec.*, vol. 5, pp. 534–543, September 2010. [Online]. Available: http://dx.doi.org/10.1109/TIFS.2010.2051270

[19] C. Grigoras, "Digital audio recording analysis the electric network frequency criterion," Diamond Cut Productions, Inc., Tech. Rep. Application Notes, AN-4, 2003.

[20] Name Unknown, "Polizei zerschlägt Kinderporno-Ring mit 2360 Verdächtigen," http://www.spiegel.de/panorama/justiz/0,1518,464920,00.html, February 2007, [Online; Status 25/08/2010].

[21] C. Jansohn, A. Ulges, and T. M. Breuel, "Detecting pornographic video content by combining image features with motion information," in *ACM Multimedia*, 2009, pp. 601–604.

[22] A. van den Hengel, R. Hill, H. Detmold, and A. Dick, "Searching in space and time: a system for forensic analysis of large video repositories," in *Proceedings of the 1st international conference on Forensic applications and techniques in telecommunications, information, and multimedia and workshop*, ser. e-Forensics '08. ICST, Brussels, Belgium, Belgium: ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), 2008, pp. 4:1–4:6. [Online]. Available: http://portal.acm.org/citation.cfm?id=1363217.1363223

[23] L. Huston, R. Sukthankar, J. Campbell, and P. Pillai, "Forensic video reconstruction," in *Proceedings of the ACM 2nd international workshop on Video surveillance & sensor networks*, ser. VSSN '04. New York, NY, USA: ACM, 2004, pp. 20–28. [Online]. Available: http://doi.acm.org/10.1145/1026799.1026805

[24] M. de Castro Polastro and P. M. da Silva Eleuterio, "Nudetective: A forensic tool to help combat child pornography through automatic nudity detection," in *DEXA Workshops*, 2010, pp. 349–353.

[25] R. Ap-apid, "An algorithm for nudity detection," in *Proceedings of the 5th Philippine Computer Science Congress*, 2005.

[26] T. Deselaers, L. Pimenidis, and H. Ney, "Bag-of-visual-words models for adult image classification and filtering," in *ICPR*, 2008, pp. 1–4.

[27] F. Ramsthaler, M. Kettner, S. Potente, A. Gehl, K. Kreutz, and M. Verhoff, "Original oder manipuliert?" *Rechtsmedizin*, vol. 20, pp. 385–392, 2010, 10.1007/s00194-010-0669-1.

[28] A. C. Popescu and H. Farid, "Exposing digital forgeries by detecting duplicated image regions," Dartmouth College, Computer Science, Tech. Rep. TR2004-515, 2004.

[29] B. L. Shivakumar, "Detecting copy-move forgery in digital images: A survey and analysis of current methods," *Global Journal of Computer Science and Technology*, vol. 10, pp. 61–65, 2010.

[30] S. Bayram, H. T. Sencar, and N. Memon, "A survey of copy-move forgery detection techniques," in *IEEE Western New York Image Processing Workshop*, 2008.

[31] S. Bayram, H. Taha Sencar, and N. Memon, "An efficient and robust method for detecting copy-move forgery," in *Proceedings of the 2009 IEEE International Conference on Acoustics, Speech and Signal Processing*, ser. ICASSP '09. Washington, DC, USA: IEEE Computer Society, 2009, pp. 1053–1056. [Online]. Available: http://dx.doi.org/10.1109/ICASSP.2009.4959768

[32] B. Mahdian and S. Saic, "A bibliography on blind methods for identifying image forgery," *Signal Processing: Image Communication*, vol. 25, no. 6, pp. 389 – 399, 2010. [Online]. Available: http://www.sciencedirect.com/science/article/B6V08-505N6XX-1/2/da59292ef818716646092b465521f7bc

[33] W. Wang, J. Dong, and T. Tan, “A survey of passive image tampering detection,” in *Digital Watermarking*, ser. Lecture Notes in Computer Science, A. Ho, Y. Shi, H. Kim, and M. Barni, Eds. Springer Berlin / Heidelberg, 2009, vol. 5703, pp. 308–322.

[34] H. Farid, “Nist colloquium series: Digital forensics,” October 2008, [Online; Status 16/01/2010].

[35] R. Maher, “Overview of audio forensics,” in *Intelligent Multimedia Analysis for Security Applications*, ser. Studies in Computational Intelligence, H. Sencar, S. Velastin, N. Nikolaidis, and S. Lian, Eds. Springer Berlin / Heidelberg, 2010, vol. 282, pp. 127–144.

[36] ——, “Audio forensic examination: authenticity, enhancement, and interpretation,” in *IEEE Signal Processing Magazine*, vol. 26, no. 2, 2009, pp. 84–94.

[37] C. Grigoras, “Applications of enf analysis in forensic authentication of digital audio and video recordings,” *Journal of Audio Engineering Society*, vol. 57, no. 9, pp. 643–661, 2009.

[38] W. Bender, D. Gruhl, N. Morimoto, and A. Lu, “Techniques for data hiding,” *IBM Syst. J.*, vol. 35, pp. 313–336, September 1996.

[39] W. Wang, “Digital video forensics,” Ph.D. dissertation, Dartmouth College, Hanover, NH, USA, 2009, adviser-Farid, Hany.

[40] W. Wang and H. Farid, “Exposing digital forgeries in video by detecting duplication,” in *Proceedings of the 9th workshop on Multimedia & security*, ser. MM&Sec ’07. New York, NY, USA: ACM, 2007, pp. 35–42. [Online]. Available: http://doi.acm.org/10.1145/1288869.1288876

[41] ——, “Exposing digital forgeries in video by detecting double quantization,” in *Proceedings of the 11th ACM workshop on Multimedia and security*, ser. MM&Sec ’09. New York, NY, USA: ACM, 2009, pp. 39–48. [Online]. Available: http://doi.acm.org/10.1145/1597817.1597826

[42] M. Kobayashi, T. Okabe, and Y. Sato, “Detecting video forgeries based on noise characteristics,” in *Advances in Image and Video Technology*, ser. Lecture Notes in Computer Science, T. Wada, F. Huang, and S. Lin, Eds. Springer Berlin / Heidelberg, 2009, vol. 5414, pp. 306–317.

[43] B. Carrier, *File System Forensic Analysis*. Addison-Wesley Professional, 2005.

[44] K. Shanmugasundaram and N. Memon, “Automatic reassembly of document fragments via data compression,” in *Digital Forensics Research Workshop*, August 2002.

[45] N. D. M. Anandabrata Pal, “The evolution of file carving,” *IEEE Signal Processing Magazine*, vol. March 2009, pp. 59 – 71, 03 2009.

[46] D. Billard and R. Hauri, “Making sense of unstructured flash-memory dumps,” in *SAC*, 2010, pp. 1579–1583.

[47] O. Avni and T. Knierim, “Carving und semantische analyse in der digitalen forensik,” Fraunhofer IGD, Tech. Rep., 2010.

[48] G. G. R. III and V. Roussev, “Scalpel: A frugal, high performance file carver,” in *DFRWS*, 2005.

[49] G. G. R. III, V. Roussev, and L. Marziale, “In-place file carving,” in *IFIP Int. Conf. Digital Forensics*, 2007, pp. 217–230.

[50] “Fuse: Filesystem in userspace,” http://fuse.sourceforge.net, [Online; Status 22/10/2010].

[51] S. L. Garfinkel, “Carving contiguous and fragmented files with fast object validation,” *Digital Investigation*, vol. 4, no. Supplement 1, pp. 2 – 12, 2007. [Online]. Available: http://www.sciencedirect.com/science/article/B7CW4-4P06CJD-1/2/48c9cdedb7d3e76b5880b58c871110be

[52] A. Pal, H. T. Sencar, and N. Memon, “Detecting file fragmentation point using sequential hypothesis testing,” *Digital Investigation*, vol. 5, no. Supplement 1, pp. S2 – S13, 2008, the Proceedings of the Eighth Annual DFRWS Conference. [Online]. Available: http://www.sciencedirect.com/science/article/B7CW4-4T5SYCF-3/2/3ce3ceeea25479675b0156d1cfc5ae6b

[53] A. Pal and N. D. Memon, “Automated reassembly of file fragmented images using greedy algorithms,” *IEEE Transactions on Image Processing*, vol. 15, no. 2, pp. 385–393, 2006.

[54] K. Shanmugasundaram and N. Memon, “Automatic reassembly of document fragments via context based statistical models,” in *Context Based Statistical Models ACSAC, 2003*, 2003, pp. 152–159.

[55] T. H. Cormen, C. E. Leiserson, R. L. Rivest, and C. Stein, *Introduction to Algorithms*. MIT Press, 2001.

[56] M. Karresand and N. Shahmehri, “Reassembly of fragmented jpeg images containing restart markers,” *Computer Network Defense, European Conference on*, vol. 0, pp. 25–32, 2008.

[57] K. Mohamad and M. Deris, "Fragmentation point detection of jpeg images at dht using validator," in *Future Generation Information Technology*, ser. Lecture Notes in Computer Science, Y.-h. Lee, T.-h. Kim, W.-c. Fang, and D. Slezak, Eds. Springer Berlin / Heidelberg, 2009, vol. 5899, pp. 173–180.

[58] H. T. Sencar and N. Memon, "Identification and recovery of jpeg files with missing fragments," *Digital Investigation*, vol. 6, no. Supplement 1, pp. S88 – S98, 2009, the Proceedings of the Ninth Annual DFRWS Conference. [Online]. Available: http://www.sciencedirect.com/science/article/B7CW4-4X1HY5C-D/2/7b6b8f0c39bb4f301335cb3a5e6ca946

[59] *Automated reassembly of fragmented images*, vol. 1, 2003. [Online]. Available: http://isis.poly.edu/kulesh/research/pubs/icassp-2003.pdf

[60] "Adroit photo forensics 2010," http://digital-assembly.com, [Online; Status 22/10/2010].

[61] M. McDaniel and M. H. Heydari, "Content based file type detection algorithms," in *HICSS '03: Proceedings of the 36th Annual Hawaii International Conference on System Sciences (HICSS'03) - Track 9*. Washington, DC, USA: IEEE Computer Society, 2003, p. 332.1.

[62] C. J. Veenman, "Statistical disk cluster classification for file carving," *Information Assurance and Security, International Symposium on*, vol. 0, pp. 393–398, 2007.

[63] S. Garfinkel, A. Nelson, D. White, and V. Roussev, "Using purpose-built functions and block hashes to enable small block and sub-file forensics," *Digital Investigation*, vol. 7, no. Supplement 1, pp. S13 – S23, 2010, the Proceedings of the Tenth Annual DFRWS Conference. [Online]. Available: http://www.sciencedirect.com/science/article/B7CW4-50NX65H-4/2/992954f303e13b95b4d06dde70d19cc9

[64] V. Roussev and S. L. Garfinkel, "File fragment classification-the case for specialized approaches," in *SADFE*, 2009, pp. 3–14.

[65] A. Nissar and A. Mir, "Classification of steganalysis techniques: A study," *Digital Signal Processing*, vol. 20, no. 6, pp. 1758 – 1770, 2010.

[66] A. Cheddad, J. Condell, K. Curran, and P. M. Kevitt, "Digital image steganography: Survey and analysis of current methods," *Signal Processing*, vol. 90, no. 3, pp. 727 – 752, 2010.

[67] H. Wang and S. Wang, "Cyber warfare: steganography vs. steganalysis," *Commun. ACM*, vol. 47, pp. 76–82, October 2004.

[68] S. Lyu and H. Farid, "Steganalysis using higher-order image statistics," *IEEE Transactions on Information Forensics and Security*, vol. 1, no. 1, pp. 111–119, 2006.

[69] N. Meghanathan and L. Nayak, "A review of the audio and video steganalysis algorithms," in *Proceedings of the 48th Annual Southeast Regional Conference*, ser. ACM SE 10. New York, NY, USA: ACM, 2010, pp. 81:1–81:5.

[70] R. Chandramouli and K. P. Subbalakshmi, "Current trends in steganalysis: a critical survey," in *ICARCV*, 2004, pp. 964–967.

[71] B. Li, J. He, J. Huang, and Y. Q. Shi, "A survey on image steganography and steganalysis," *Journal of Information Hiding and Multimedia Signal Processing*, vol. 2, no. 2, pp. 142–172, 2011.

[72] I. K. Maitra, S. Nag, B. Datta, and S. K. Bandyopadhyay, "Digital steganalysis: Review on recent approaches," *Journal of Global Research in Computer Science*, vol. 2, pp. 1–5, 2011.

[73] J. Wiles, T. Alexander, S. Ashlock, S. Ballou, L. Depew, G. Dominguez, A. Ehuan, R. Green, J. Long, K. Reis, A. Schroader, K. Schuler, and E. Thompson, "Murder and money: The story of standards, accreditation, and certification in computer forensics," in *Techno Security's Guide to E-Discovery and Digital Forensics*. Burlington: Syngress, 2007, pp. 261 – 276. [Online]. Available: http://www.sciencedirect.com/science/article/B8KKC-4S03888-H/2/a095905e619b02e15115dad5e8541783

[74] ASCLD. (2011, 03) Ascld (american society of crime lab directors/laboratory). [Online]. Available: http://www.ascld.org/

[75] A. Shipman and B. S. Institution, *Evidential Weight and Legal Admissibility of Information Stored Electronically. Code of Practice for the Implementation of BS 10008.* British Standards Institution, 2008. [Online]. Available: http://shop.bsigroup.com/ProductDetail/?pid=000000000030186227

[76] A. of Chief Police Officers (ACPO), "Good practice guide for computer-based electronic evidence," http://7safe.com/electronic_evidence/index.html.

[77] *ISO/IEC 17025:2005 - General requirements for the competence of testing and calibration laboratories*, International Organization for Standardization (ISO) / International Electrotechnical Commission (IEC) Std., 2005.

[78] B. Fraser, “Site Security Handbook,” RFC 2196 (Informational), Internet Engineering Task Force, Sep. 1997. [Online]. Available: http://www.ietf.org/rfc/rfc2196.txt

[79] N. Brownlee and E. Guttman, “Expectations for Computer Security Incident Response,” RFC 2350 (Best Current Practice), Internet Engineering Task Force, Jun. 1998. [Online]. Available: http://www.ietf.org/rfc/rfc2350.txt

[80] R. Shirey, “Internet Security Glossary,” RFC 2828 (Informational), Internet Engineering Task Force, May 2000, obsoleted by RFC 4949. [Online]. Available: http://www.ietf.org/rfc/rfc2828.txt

[81] D. Brezinski and T. Killalea, “Guidelines for Evidence Collection and Archiving,” RFC 3227 (Best Current Practice), Internet Engineering Task Force, Feb. 2002. [Online]. Available: http://www.ietf.org/rfc/rfc3227.txt

[82] M. Meyers and M. Rogers, “Computer forensics: The need for standardization and certification,” *IJDE*, vol. 3, no. 2, p. , 2004.

[83] J. Slay, Y.-C. Lin, B. Turnbull, J. Beckett, and P. Lin, “Towards a formalization of digital forensics,” in *Advances in Digital Forensics V*, ser. IFIP Advances in Information and Communication Technology, G. Peterson and S. Shenoi, Eds. Springer Boston, 2009, vol. 306, pp. 37–47.

[84] S. L. Garfinkel, “Digital forensics research: The next 10 years,” *Digital Investigation*, vol. 7, no. Supplement 1, pp. S64 – S73, 2010, the Proceedings of the Tenth Annual DFRWS Conference. [Online]. Available: http://www.sciencedirect.com/science/article/B7CW4-50NX65H-B/2/19b42d7f2ccc4be6794c5a1330a551bb

[85] S. Garfinkel, P. Farrell, V. Roussev, and G. Dinolt, “Bringing science to digital forensics with standardized forensic corpora,” *Digital Investigation*, vol. 6, no. Supplement 1, pp. S2 – S11, 2009, the Proceedings of the Ninth Annual DFRWS Conference. [Online]. Available: http://www.sciencedirect.com/science/article/B7CW4-4X1HY5C-3/2/090ebc16025d598c775d87c8abbb7ae5

[86] N. Beebe, “Digital forensic research: The good, the bad and the unaddressed,” in *Advances in Digital Forensics V*, ser. IFIP Advances in Information and Communication Technology, G. Peterson and S. Shenoi, Eds. Springer Boston, 2009, vol. 306, pp. 17–36, 10.1007/978-3-642-04155-6_2;.

[87] K. Nance, B. Hay, and M. Bishop, “Digital forensics: Defining a research agenda,” *Hawaii International Conference on System Sciences*, vol. 0, pp. 1–6, 2009.

[88] K. Nance, H. Armstrong, and C. J. Armstrong, “Digital forensics: Defining an education agenda,” in *HICSS*, 2010, pp. 1–10.

[89] M. Pollitt, K. L. Nance, B. Hay, R. C. Dodge, P. Craiger, P. Burke, C. Marberry, and B. Brubaker, “Virtualization and digital forensics: A research and education agenda,” *J. Digital Forensic Practice*, vol. 2, no. 2, pp. 62–73, 2008.

[90] Digital Forensics Association, “Formal education: College education in digital forensics,” http://www.digitalforensicsassociation.org/formal-education/, 2010, [Online; Status 02/11/2010].

[91] M. Nutzinger and R. Poisel, “Software architecture for real-time steganography in auditive media,” in *IEEE International Conference on Computational Technologies in Electrical and Electronics Engineering*, Irkutsk Listvyanka, Russia, 2010, pp. 100–105.