Audit Log for Forensic Photography

Timothy Neville and Matthew Sorell

School of Electrical and Electronic Engineering,
University of Adelaide SA 5005, Australia
matthew.sorell@adelaide.edu.au

Abstract. We propose an architecture for an audit log system for forensic photography, which ensures that the chain of evidence of a photograph taken by a photographer at a crime scene is maintained from the point of image capture to its end application at trial. The requirements for such a system are specified and the results of experiments are presented which demonstrate the feasibility of the proposed approach.

Keywords: Digital photography, crime investigation, forensic investigation, digital negative.

1 Introduction

In legal terminology, the chain of evidence (or chain of custody) refers to "the ability to guarantee the identity and integrity of the specimen from collection through to reporting of the test results" in a Court of Law [1]. As technology continues to evolve, the ability to both maintain and break the chain of evidence has become increasingly easy. One example of this is in the area crime scene photography.

Since 1840 traditional analogue photography has involved both a negative and positive image, with the latter developed using the former [2]. While important in developing a viewable picture, the negative image, to law enforcement agencies, has also allowed the chain of evidence of a crime scene photograph to be easily secured. This is because image manipulation of a negative photograph is both relatively difficult to achieve and relatively easy to identify.

The advent of more sophisticated technology has, however, provided law enforcement with the ability to use digital cameras in the course of their investigations, and indeed the lack of technical support for film cameras is accelerating this migration. As digital forensic photographs provide investigators with high quality images with quicker access, at a cheaper cost than traditional analogue photographs, a significant benefit exists for the use of this technology. There is, however, one significant drawback to the use of digital photography: the inherent insecurity of a digital image and the ease at which the chain of evidence can be broken.

While it is unlikely that law enforcement officials would manipulate digital evidence, it is nevertheless important that a secure chain of evidence is maintained that is similar to its physical evidence counterpart. Indeed, digital photographs tendered in a speeding fine case in New South Wales were found to not include the

M. Sorell (Ed.): e-Forensics 2009, LNICST 8, pp. 142 – 152, 2009.

appropriate watermarks needed to prove authenticity and were thus deemed inaccessible as evidence [3]. Similarly, from an international point of view, the jury in the case of *State of Florida v Victor Reyes* (2003) acquitted Victor Reyes of murder after the validity of a digitally enhanced photograph was challenged by the defence attorney [4].

Current practices for the secure storage of digital data in law enforcement involve software packages such as Foray's Authenticated Digital Asset Management System used by the FBI and DEA in the United States [5]. These packages track and monitor every access to the digital data once it has been uploaded to a secure storage device. For example, a crime scene investigator takes a series of digital photographs at a crime scene then travels back to the crime lab and uploads the photographs to a secure server running data management software. Once these photographs enter the system their access can be tracked.

In the above scenario, while the photographs can be tracked once uploaded, there is no electronic confirmation that the image taken at the scene is the same as the image uploaded at the crime lab. The only assurance in the chain of evidence during this period is the integrity of the camera operator. This gap in the electronic chain of evidence is a direct consequence of digital technology. In the case of an analogue photograph a negative image is produced at the moment of capture; for a digital photograph no negative is needed, and thus no negative is produced.

2 The Need for a Digital Negative

Whilst there appears to be little demand for a digital negative by the everyday user, the aforementioned scenario indicates a need for law enforcement. One novel yet cumbersome approach suggested by Blythe and Fridrich [6] is to create a secure digital camera that takes a biometric image of the user's iris. The iris image information would then be included in the metadata of the captured photograph. While this approach identifies the person who took the photograph it still fails to secure the digital image from the time it is taken to the time it is stored on a secure storage device. This approach also renders a camera specific-approach to authentication, providing limitations on what how secure authentication process.

It is from the idea of creating a secure digital camera, that the aims of this project were developed. There is a definite need to prove, beyond a reasonable doubt, that the photograph taken at a crime scene is the same as the image uploaded at the crime lab. Following from traditional analogue photography, one approach to this would be to create a digital negative of the image at the time of capture. This image should immediately be stored securely and accessed at a later time to prove authenticity.

We propose that a digital negative need not be a secure copy of the complete digital image or digital image file, but rather a secure data structure against which an image or set of images can be audited. In the application outlined in this paper, it should be noted that once a digital file is stored in a conventional auditable logging system such as Foray, it is possible to keep track of subsequent image processing and analysis; we are concerned with ensuring that the chain of custody extends from the point at which the photograph is taken to the point at which it enters such a

conventional logging system. It is thus sufficient to consider four components of an audit trail record:

- A record of the nature of the transaction and operating-system specific parameters including the file name and its location on a memory device
- A decipherable metadata record, if possible, which allows independent matching of a file with its record
- A thumbnail or miniature version of the image, if possible, which allows visual confirmation of a file match, and
- A cryptographic hash code, to verify that an image file is a complete and untampered copy of the original file.

In order to construct a record at the front-end of the chain of evidence, it is necessary to capture the above components at the camera. We have identified two broad approaches where the image file is effectively quarantined and so the audit file can be constructed with certainty of security. The first is to embed the Audit Log System in the firmware of a Digital Still Camera; the second is to monitor and capture the required data as it is transferred to and from a memory card, provided that the camera under consideration only supports an external memory.

The first approach is impractical for the simple reason that modern Digital Still Cameras are highly optimized devices with little processing overhead available in which to consider the separate processing of an audit log record. The development of such an implementation would result in a camera with a very specific and relatively small market which would contribute prohibitively to the cost of the product to an end user.

The second approach has the advantage that it can be implemented and customized, at least in theory, for any of the finite combinations of cameras and memory devices under consideration, with the cost of development and production significantly reduced for two reasons – the one generic device (economy of scale) is not necessarily specific to just one make and model of camera (economy of scope). However an external device adds bulk to the camera, might require an independent power source, and might, if not designed properly, prevent or inhibit normal use of the camera. With these limitations in mind, we consider the requirements of our proposed system.

2.1 File Transaction Component

The file transaction component of the record includes the name of the file, the timestamps and other operating-specific parameters available to the data monitoring device. It is also important to consider the nature of the transaction, which might be, for example:

- The transfer of a file onto a memory device (writing)
- The reading of the file from a memory device (reading)
- The deletion of a file from a memory device (deletion)
- The changing of the name or other file records (renaming)

Other memory device transactions which might be of interest include identification of when a device is switched on or off, and when a memory device is swapped in or out

of a logging system. While it is desirable to maintain an associated timestamp, for a low-power unit it might not be feasible to maintain an accurate real time clock, in which case it is at least necessary to ensure that the order of transactions is accurately recorded.

2.2 Metadata Record and Thumbnail

Unlike traditional negatives, which only show a colour-inverted, snapshot of the photograph taken, a digital negative has the ability to provide greater information to the user. Images are most often stored in JPEG format [7], but other formats (particularly proprietary so-called *raw* formats) are also used. JPEG, and many of the proprietary formats, also support the Exif metadata standard [8] within the file structure, and the Exif standard is ubiquitously supported by all Digital Still Cameras the authors have examined. Metadata stored in Exif format includes the time and date at which an image was taken, the make and model of camera, and a wide range of standard camera settings. A thumbnail or miniature version of the image is often included. Proprietary extensions include specific camera parameters. The Exif data structure, which is limited in size to 64 Kilobytes, is thus a very good encapsulation of the characteristics of a digital image file, especially if it includes a thumbnail image.

2.3 Cryptographic Hash

A cryptographic hash function generates a number based on a complete file input to it, which is virtually unique to that file. Hash functions are best known for their application as a digital signature. For our proposal, a hash can be used to verify that an image file is in fact identical to the version originally written to the memory device with a very high level of confidence, without having to permanently store the complete original image.

3 Audit Log System

The proposed architecture of the Audit Log System (ALS) is given in Figure 1. The proposed system is an external device which is physically attached to the camera, interfacing to the camera through the memory device socket. A number of form factors were considered in conceiving the proposed system. It would be ideal for such a log system to be implemented in the form of a full-sized memory adaptor which accepts a micro-form memory. For example, adaptors which allow micro-SD memory devices to be used in a full-sized SD-card slot exist, and there are similar adaptors for related devices such as Sony's Memory Stick. Implementation in such a package would be ideal because the photographer would not be inconvenience by having to manage a separate device. However, our investigation of technical requirements suggests that such a package is not currently viable, although this may change in the future. In particular, we recognize the need for an independent power supply and electrical interface for accessing the audit records.

We therefore visualize the proposed system as a small form factor package similar in size to a miniaturized music player, sufficiently large to contain a rechargeable

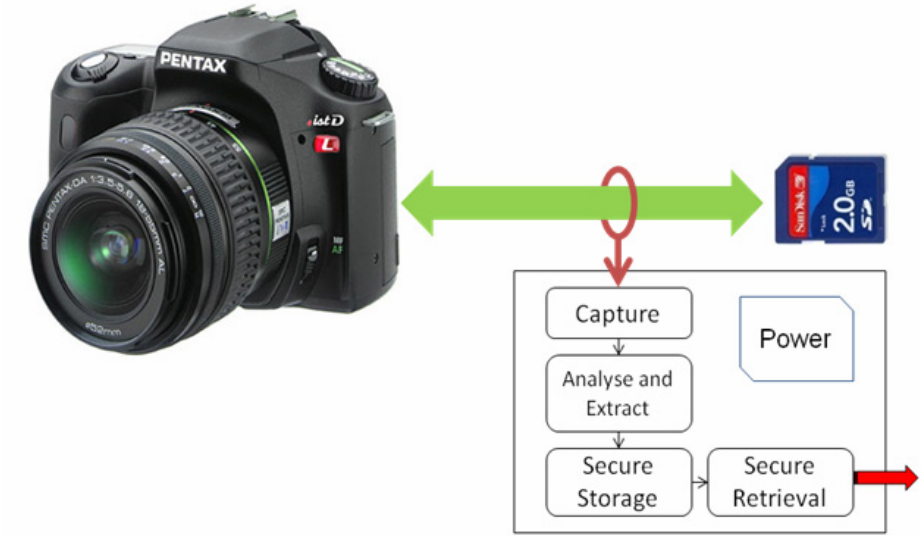

Fig. 1. System Architecture of the proposed Audit Log System

battery, electrical sockets for memory access and power, and a socket for the normal memory device such as SD-card or Memory Stick. A universal memory socket would allow the device to be used on a wider range of cameras, although multi-format support would complicate firmware. A memory plug, similar to a port extender, is relatively easy to implement. The key complication is that most cameras completely encapsulate the memory device and so minor physical modification of the camera might be necessary to allow a thin cable to extend from the memory socket to the ALS, such as drilling a small hole or cutting a slot in a panel.

It is also necessary to support an external memory plug to connect into the camera, and a means of physically securing the device to the camera. In the latter case, it would be a relatively simple matter to design the package to be screwed into the universal tripod thread, and provide a further thread for a tripod to be used.

Taking the concept further, it is necessary to consider the electronic requirements based on the proposed architecture. For the purpose of discussion of specifics, we consider the widely used SD-card memory to illustrate the challenges of implementation.

3.1 Passive Capture

The proposed system is located between the camera and the memory and interprets communications between the two devices. Both an active and a passive architecture can be considered.

An active architecture would mean that the ALS would interface directly to the camera and mimic the functions of the memory. The memory would be connected separately and in this case the ALS would mimic the role of the camera. Such an active architecture has some advantages, particularly in determining which of the two devices (the memory or the camera) is transmitting, and allows translation between memory protocols, enhancing the compatibility of an old camera with a contemporary

memory device for example. However the latter function is not critical to our consideration, and the disadvantages are manifold. These include the need to implement sophisticated mimicry and translation of operating system characteristics such as compliant communication when the external memory is full, but most critically if the ALS fails then the photographer cannot continue working.

A passive architecture on the hand means that the memory is connected directly to the camera and receives power and communication signals exactly as intended. All that is required is for the ALS to monitor the communications between the two devices and interpret events of interest for analysis and storage. There are some complications because full interpretation of the handshaking protocol between the memory and the camera is needed to determine the direction of transmission, but on the other hand there is no need to mimic communications, and if the ALS fails the photographer can continue working.

A more important consideration however is that a passive implementation does not interfere with the chain of evidence and is thus more trustworthy.

In the case of SD memory, there are a total of five data lines which need to be monitored, consisting of a four-bit bus and a single bit command line, plus a clock which operates at up to a nominal speed of 25MHz (in addition to circuitry which detects whether power has been applied). The most appropriate architecture for the capture circuitry is a First-In-First-Out (FIFO) buffer which uses the SD-card clock signal to write to the memory. The subsequent analysis processor needs to be able to read data out of the FIFO buffer at a somewhat higher speed to ensure real-time analysis; alternatively a very large buffer is needed to allow more leisurely processing. The latter case is highly undesirable however because unless the command channel is interpreted with low delay, memory is wasted and may overflow during idle periods when the clock continues to cycle. It should be noted that emerging standards operate at higher clock speeds, and so it is likely that higher operating speeds will be needed to support new memory devices.

3.2 Analysis and Extraction

The ALS is not intended to store a complete record of all communications but rather a secured summary of transactions. It is therefore necessary for the ALS to interpret communications, and this function requires a combination of data communications at a reasonable speed, computationally tractable analysis, and low power embedded computing.

It would be possible in theory to implement an automatic configuration algorithm in the analysis process, so that the device would automatically determine the make and model of the camera and the memory type and behave accordingly. However, it is sufficient here to consider only the case in which a known camera communicates through a known protocol to a known memory device. In this case, the analysis processing is required to perform the following functions:

- Determine the status of the communication channel, so that the ALS is only armed when the camera is on, memory is connected and power is applied to the memory.
- Interpret file transaction instructions and parameters in order to extract the file construction parameters for the audit record

- Determine when a memory device is removed or inserted
- Interpret operating system instructions and parameters including the amount of free memory on the memory card, based only on passive capture of data communication between the camera and the memory.
- When an image file is transferred, capture the Exif metadata file component, and generate a cryptographic hash of the full image file.

It should be noted that contemporary low-powered microprocessors designed for battery-driven consumer electronics such as cameras and mobile phones, for example an ARM RISC processor, would be capable of delivering the data transfer bandwidth and processing power to meet the current and emerging technical requirements of the ALS.

3.3 Secure Storage and Secure Retrieval

We note that the security of auditable transaction records is an active area in computer security, particularly in the field of security of financial records, and propose that an off-the-shelf solution for secure storage would be sufficient to meet the requirements of the device. However, it is worth considering some of the requirements of the secured data records.

Simply put, the secure record should be relatively easy to extract, and once extracted, effectively impossible to modify without detection. The secure memory of the ALS may either be an un-erasable WORM (Write Once Read Multiple) memory, in which case the ALS has a finite life, or else a secure protocol is required to allow the secure memory to be erased and over-written.

It is worth considering that it is very much in the interest of the investigator to ensure that the chain of evidence is maintained, and in the latter case this means that such a secure protocol is supported by the investigator's requirement to retain the audit log before erasure. However, just as anyone can dispose of a film negative, it is always possible to dispose of an audit file.

There are significant disadvantages in specifying a WORM solution, notably that the device has a finite life and that such memory is becoming increasingly rare, requiring a proprietary silicon solution. For these reasons, we reject the WORM approach and advocate a secure erasure protocol.

It should also be noted that once the audit log is extracted it can be entered into a conventional digital chain-of-custody system and is then subject to conventional procedures. It is however necessary to note that a secure but conventional cryptographic communication solution is required for tamper detection, so that the chain of evidence is maintained from the ALS to the point of entry.

3.4 Power

There are two options for providing power to the ALS. Either the ALS can operate on the same power supply as the memory card, provided by the camera's battery, or it can have its own independent power supply. The use of the camera's power supply is undesirable for two key reasons. Firstly, the ALS draws additional power which reduces battery life and thus interferes with the photographer's function. Secondly, ALS processing would only be possible when the memory device is powered by the

camera, thus reducing the scope for functionality of the device such as the implementation of an internal real-time clock.

It is therefore necessary to specify the use of a separate power supply. However this raises other concerns. Firstly, batteries have a finite size placing a limit on the size and form factor of the ALS. Secondly, a simple mechanism for either charging an internal rechargeable battery, or changing out disposable batteries, becomes a requirement, further complicated by the desirability to have identical batteries to the camera to reduce the amount of equipment required by the photographer. Thirdly, it needs to be recognized that the ALS power can fail independently of the camera, and in this case the camera needs to continue to operate. This latter point is another strong argument in favour of a passive capture implementation, since active intervention would prevent the camera from working.

4 Proof-of-Concept Demonstration

In order to develop the ALS concept the transfer of data between a digital camera and an SD Card needed to be understood. Four basic experiments were conducted to show that this was not the case. As the basic function of the ALS is to monitor the copying of files from one device to another, the experiments conducted were limited to this one mode of operation.

The aims of the experiments were to demonstrate that it is possible to monitor communications between a Digital Still Camera and an SD-Card memory, and in particular to show that a JPEG image file could be detected and reconstructed from the data captured during file transfer.

4.1 Equipment

The experiments required the following equipment:

- SD Extender Card, providing direct access to signals between the SD Card and the SD Card port in a camera or computer.
- Commercial Logic Analyser – Combined with the SD Extender Card, the logic analyser allows the data flow to be captured and examined
- SD Card Reader – in this case integrated within a laptop computer
- Digital Still Camera – A digital camera with an easily accessible SD port.

4.2 Results

Early experiments showed that the command line structure for a SD card copy operation is a series of write block and write multiple block operations. Each write command (a series of file setup instructions) is preceded by a status check which checks the current status of the SD Card, while the write multiple blocks (the file payload transfer) is followed by a stop command. Although the information gained from this experiment was minimal, it did show that the command line of an SD Card is independent of the SD Card's data lines. The communications during the setup of a

file transfer onto the memory were interpreted according to the SD card standard, demonstrating that it is possible to interpret file transaction information which can usefully be included in an audit record.

Having confirmed that the communication standard was being interpreted correctly, we implemented a post-capture analysis program in Matlab to automatically detect and extract a JPEG image. This was relatively simple to implement, noting that a JPEG image, according to the standard, starts with the byte sequence FF D8. Similarly, it is relatively easy to identify the Exif metadata sequence, which begins with FF E1. While there were some complications during capture, due primarily to the limitation of operating the available logic analyser at a fixed clock rate and with limited memory, it was possible to capture a significant proportion of the JPEG image by triggering the storage of the logic levels once FF D8 was detected on the data lines.

Figure 2 demonstrates that it is possible to recover the JPEG image file from the data lines captured during the file transfer process. This experiment was done using a file transferred from a laptop rather than a camera for simplicity.

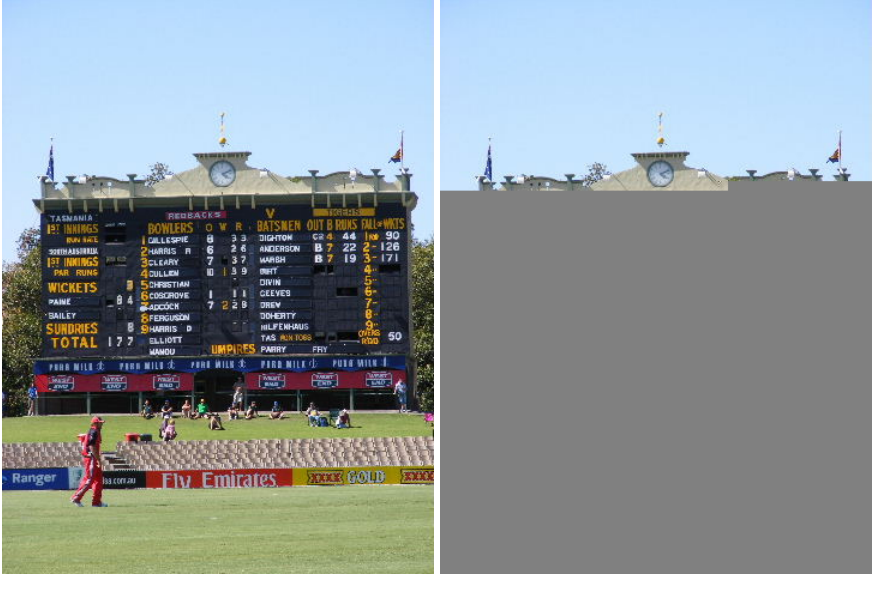

Fig. 2. The original image (left) was transferred from a laptop to an SD memory card. Although incomplete, it can be clearly seen that a significant proportion of the file was captured and reconstructed, resulting in a useable JPEG image fragment.

It is worth making the observation that experimental results using a Digital Still Camera were disappointing, but for interesting reasons. It was possible to trigger the logic analyser when the start of the JPEG image was detected, but after writing some Exif metadata to the file, there was a significant delay before the rest of the file was transferred. This delay meant that the logic analyser's memory was exhausted before any further data was transferred. However this delay does demonstrate that the

implementation of the camera's file compression and transfer firmware is such that the camera transfers what it is able to construct directly to the external memory as soon as it is composed, rather than constructing the entire JPEG image file and transferring as a single operation. While the latter approach would be more efficient, due to the external memory being powered for a shorter period, there is also a need for larger internal memory in the camera which increases costs, albeit marginally. The implications for implementation of the ALS are similarly important, because it is clearly necessary for the data capture system to either capture a very large amount of data and then process it, requiring a large FIFO memory, or a sufficiently large FIFO buffer to allow the ALS's microprocessor to transfer and analyse communications without overflow.

5 Future-Proofing and Extensions

An important issue the ALS shall need to consider through its development is the ability to implement future proofing functionality to its design. As storage technology continues to evolve, memories will become larger and different standards will be introduced. One example of this is the new High Capacity Secure Digital Card (HCSD Card) which operates at four times the speed and has a greater storage capacity when compared to current SD Cards. While not all digital cameras have the ability to use HDSD Cards, new digital cameras will be able to utilise this new standard. Thus, the ALS design must take this into consideration.

Furthermore, while the experiments conducted examined the copying of an image from one device to the SD Card, the ALS can be extended to monitor the removal of images from the SD Card and also the copying of images from a SD Card to another device. These uses allow the ALS to be designed not just for a digital camera but also for other devices that require data monitoring.

The main purpose of the ALS is to preserve the chain of evidence of a digital image from the moment it is taken at crime scenes. However, the ALS could also be implemented in other law enforcement activities. One particular operation could be to track the photographs, or even video, taken at surveillance location. By recording the time, date and thumbnail of every photograph taken, the ALS can prove timeline of the photographs for investigators in court.

6 Conclusions

The Audit Log System for digital forensics is one solution to creating a digital negative. With the creation of a digital negative the chain of evidence of digital images can be strengthened, providing an extra layer of authenticity to evidence tendered in court. From a theoretical standpoint, the ALS idea can be achieved; with experimentation showing that the SD Card protocol is workable, with images able to be recreated. From this understanding, the design can be taken further to include hardware design, power and packaging.

References

[1] West Midland Toxicology Laboratory: Chain of Custody (June 21, 2003), http://www.toxlab.co.uk/coc.htm (accessed, March 2008)
[2] National Geographic: History of Photography, http://photography.nationalgeographic.com/photography/photographers/photography-timeline.html (accessed, September 2008)
[3] Pelly, M., Norrie, J.: Speedcam slip puts $100m fines in doubt. Sydney Morning Herald (March 26, 2006), http://www.smh.com.au/news/national/speedcam-slip-may-cost-100m/2006/03/23/1142703456320.html (accessed, March 2008)
[4] Bergstein, B.: Digital Photos Pose Issues in Court. CRN -Channel Web (February 8, 2004), http://www.crn.com/digital-home/18831429 (accessed, March 2008)
[5] Foray Technology: Foray Technology - Clients (2008), http://www.foray.com/company/clients.php (accessed, September 2008)
[6] Blythe, P., Fridrich, J.: Secure Digital Camera. Digital Forensic Research Workshop (2004)
[7] ITU: CCITT T.81 information technology – Digital compression and coding of continuous-tone still images – Requirements and guidelines. International Telecommunications Union (1993)
[8] JEITA: JEITA CP-3451 Exchangeable image file format for digital still cameras: Exif Version 2.2. Japan Electronics and Information Technology Industries Association (2002)