Chapter 17.2: Forensic Photographic and Video Analysis

“A Picture is Worth a Thousand Words” (anon).

Learning Goals and Objectives

Photographic images capture and preserve unbiased information for identification of criminals and documentation of the events that occurred during the commission of a crime. In this chapter, you will need to understand the following concepts:

- What is meant by video and photographic forensic analysis;
- What are the uses of photographic images in forensic investigations;
- What tools and methods are used to analyze photographic evidence;
- What are the limitations and challenges these analyses.

Introduction

Video and photographic devices seem to be everywhere, from cell phones and personal computers to surveillance cameras in stores, streets, and offices. Whether we are aware of it or not, we are often being watched and recorded by cameras that stand constant vigil in protecting people and property. Cameras watch for shoplifting in stores, traffic violations at road crossings, vandalism outside buildings, robberies in homes, and unauthorized entries to restricted places. Because of their prevalence, photographic devices also are increasingly capturing important forensic evidence. These images may provide dramatic records of the actions that occurred as part of a crime, leading to the identification of the criminals and tying them to their actions.

Photographic and video records have a powerful impact on people. Because of their influence, images may be altered and modified to improperly manipulate and wrongly change our understandings, beliefs, and feelings about events and people. Convincing “doctored” videos and pictures are quite easily made using readily available computer software and rapidly distributed as authentic renditions of events around the world. These manipulations may range from the subtle enhancement of the appearance of a model to blatant manipulations to add or remove people and objects from a scene.

The role of forensic photographic and video analysis spans a number of areas including image enhancement, authentication, documentation, and analysis. These topics will be briefly presented in this section.

Video Forensic Analysis

Video images captured by surveillance cameras and personal video cameras, especially phone cameras, can play an important role in an investigation and later criminal prosecution. Forensic video analysis

Figure 17.2.1. Forensic photographic analysis can provide information critical to an investigation (www.stinkyjournalism.org/latest-journalism-news-updates-139.php).
may focus on several types of inquiry useful to an investigation including:

- Recording crime scenes as part of the processing of the scene;
- Recording the events surrounding the commission of a crime;
- Documenting the authenticity of the video;
- Separating multiplexed video signals from surveillance cameras (images from many cameras recorded on one tape);
- Enhancing and clarifying video images for the identification and interpretation of events;
- Enlarging or highlighting specific areas of interest.

In previous chapters, still and video photography have been described as critical tools for documenting both the overall features of a crime scene as well as recording the close-up details of the identified pieces of evidence. The crime scene photographic record needs to be taken of the scene in as close to pristine condition as possible, before other types of forensic processing has begun. Photographic images also form a permanent record that later can be used to document the steps employed in evidence location and collection. The photographic records then become part of the evidence collected at the crime scene.

Video recordings have been shown to be faithful reporters of criminal actions. Surveillance and personal video recordings have been frequently used in court to identify perpetrators and to document beyond question the extent and sequence of their criminal actions. Often, criminals do not consider the presence of hidden cameras or the likelihood that images taken by

---

**Figure 17.2.** the process of multiplexing and de-multiplexing surveillance images. (Top) Feeds from six surveillance cameras are recorded superimposed on one recorder (bottom left) that must be de-multiplexed by software programs (bottom right) to give a viewable image (www.cognitech.com/wp-content/uploads/2011/03/TS-Brochure-Final2.jpg).

**Figure 17.2.3.** Enhancement of a dark image. (top left) original images, (top right) image brightened and amplified, and (bottom) the brightened image “denoised” through frame averaging to be able to resolve the license plate of the vehicle (www.tomshardware.com/reviews/video-forensics,996-3.html).
accomplices of their actions will make it into the hands of the police.

Video images of taken by surveillance cameras and witnesses of crimes are, unfortunately, often of very poor quality. This may arise through the use of inexpensive and poorly maintained equipment, overused tapes (sometimes recorded over hundreds of times), unsteady camera handling (phone cameras), poor lighting conditions, rapid motion action, and low-resolution images. In these instances, investigators often turn to computer enhancement techniques that can make visible and understandable obscured images in the video.

In the video enhancement process, the video is usually first digitized (if it is not already) onto a computer system. This allows specially developed software to adjust, manipulate, and enhance the images in a scientifically acceptable and court admissible manner. It is especially important during this process that a proper chain of custody be established, beginning with the original recording and including a detailed log of exactly how the images were manipulated. Many software programs automatically maintain this log, along with the original recording, for later verification in court of how the enhancements were performed.

Surveillance systems often use multiple cameras that feed into a single recorder. The recorder “multiplexes” these images onto one video recorder usually by recording just a few frames from each camera at a time or encoding superimposed images from all the cameras together (Figure 17.2.2). The resulting tape is unwatchable in the multiplexed form because of the very fast switching that happens between cameras or confusing of superimposed images such that the forensic software must first demultiplex the images — putting all the scrambled images from

---

**Figure 17.2.4.** De-blurred image from a moving vehicle make the license plate readable (www.cognitech.com/wp-content/uploads/2011/03/TS-Brochure-Final2.jpg).

**Figure 17.2.5.** Mosaic method for forming a complete image of an object by piecing together images of smaller portions of the object. The image on the left was one of several of the truck that was used to create the entire picture of the vehicle (right) (www.cognitech.com/wp-content/uploads/2011/03/TS-Brochure-Final2.jpg).

---

**Figure 17.2.6.** A panorama mosaic image of the Himalayas made by overlapping five images of the mountains covering different regions (http://earthobservatory.nasa.gov/IOTD/view.php?id=4346).
one camera back into one sequence. Different security systems have varying ways of performing the multiplexing operation so that the demultiplexing operation may be a complicated process. Once completed, the demultiplexed images may allow investigators to follow a person from one camera to another camera to establish a record of their movements.

Sometimes, video images are too dark or lack sufficient contrast to be able to pick out useful information. When not enough light is present, the image from a video camera is usually filled with “noise” – random “sparkles” (sometimes called “snow”) in the picture that results from increased amplification of thermal and electronic background signals in the camera’s imaging system. Forensic video software must first be used to brighten up this type of image, but this brightening process also increases the noise levels as well. To combat this, the enhancement software frame averages several adjacent images together – “adding” together a number of sequential frames of the recording. In the frame averaging process, the random noise that changes locations from frame to frame is cancelled out while the faint images from real objects remain unchanged and are increased in signal intensity. For example, in Figure 17.2.3, the dark license plate of the auto is not even visible in the original image but, through the process of brightening and frame averaging, not only does the plate become visible but the number becomes legible.

Sometimes, video information is not legible because of blurring caused by either a rapidly moving object or by moving the camera too quickly. This often occurs because the shutter speed of the camera (the speed that the camera creates each new frame) is slower than the speed needed to resolve the moving object. To “de-blur” such images, forensic video software can determine the speed and direction that the object is moving and correct to keep a portion of the image stationary in the picture, thereby allowing frame average or similar processes to enhance the image, such as shown in Figure 17.2.4.

The images captured by a stationary camera might only record a small portion of an object of interest at a time, such as a vehicle, boat or plane moving past the camera. It is often desirable, however, to have a picture of the entire object for identification. This can be done by creating a “panorama mosaic” picture that is prepared by aligning multiple images that each captures a portion of the entire object (Figure 17.2.5). To illustrate how the process is done, Figure 17.2.6 shows how NASA has taken five separate images of the Himalaya Mountains and

---

**Keys to Video Evidence**

Managing video evidence can be challenging. Here are a few items that should be considered when using videos (adapted from [www.ncavf.com/advice/top-tips-for-security-camera-evidence](http://www.ncavf.com/advice/top-tips-for-security-camera-evidence)):

- Search for all video cameras that might have captured the event;
- Work quickly, many surveillance systems have auto-erase functions that clear tapes weekly or monthly;
- Check timing recorded on the cameras – they may be inaccurate;
- Confiscate both the recorder (tape) and the camera;
- Maintain a proper chain of custody and log of all enhancement operations for the recording;
- Use a forensic video expert to enhance and clarify video images of interest;

---

**Figure 17.2.7.** Surveillance camera image of the September 11, 2001 airplane attack on the Pentagon just after impact (www.yourdiscovery.com/photos/gallery/9-11-pentagon-attack)
overlapped them carefully to give a picture covering 130 km (80 miles) of terrain.

Reginald Denny and Video Evidence

During the 1992 Los Angeles riots, a news helicopter captured video images of a rioters pulling a helpless truck driver, Reginald Denny, from his vehicle and brutally assaulting him. While the tape horrified millions of watchers, it also provided the evidence necessary to find and convict the perpetrators.

Through forensic video enhancement techniques, the distinctive tattoo on the arm of one of the attackers was identified. This tattoo was later matched with one of the suspects that resulted in his conviction. In addition, the actions of each of the attackers was recorded throughout the attack, including striking Denny with a hammer, bricks and metal medical devices before turning to the cameras over Denny’s unconscious body.


Forensic Photographic Analysis

There are two main roles of still photography in forensic science: site/evidence documentation and photographic analysis and enhancement. In previous chapters, the key role of photography in documenting both crime scenes and individual pieces of evidence has been emphasized. These images form a permanent record of the evidence that can be revisited periodically as an investigation progresses as well as used in court to connect the evidence with the scene. The Scientific Working Group on Imaging Technology (SWGIT) provides guidelines and best practice information on photographic techniques for legal applications. As with all types of evidence, proper chain of custody procedures must be followed for each picture, including an identification number for the shot. Photographic evidence, however, has the added requirement that it must also provide information about where, the relative orientation of the photo within the crime scene, and when a picture was taken along with technical information such as shutter opening, focal length, magnification, (e.g., wide-angle v. telephoto), shutter speed, film characteristics (when film is used), and other relevant photographic information. Each photograph must also include some type of scale marker, such as a ruler or object of known dimensions (e.g., coin or similar object), that allows the observer to judge the size of the item in the image. There is clearly a very specialized area of expertise that requires significant experience and training to take valuable forensic photographic records.