Disclaimer:

As a condition to the use of this document and the information contained herein, the SWGIT requests notification by e-mail before or contemporaneously to the introduction of this document, or any portion thereof, as a marked exhibit offered for or moved into evidence in any judicial, administrative, legislative, or adjudicatory hearing or other proceeding (including discovery proceedings) in the United States or any foreign country. Such notification shall include: 1) the formal name of the proceeding, including docket number or similar identifier; 2) the name and location of the body conducting the hearing or proceeding; 3) the name, mailing address (if available) and contact information of the party offering or moving the document into evidence. Subsequent to the use of this document in a formal proceeding, it is requested that SWGIT be notified as to its use and the outcome of the proceeding. Notifications should be sent to: SWGIT@yahoogroups.com

Redistribution Policy:

SWGIT grants permission for redistribution and use of all publicly posted documents created by SWGIT, provided that the following conditions are met:

1. Redistributions of documents, or parts of documents, must retain the SWGIT cover page containing the disclaimer.

2. Neither the name of SWGIT, nor the names of its contributors, may be used to endorse or promote products derived from its documents.

Any reference or quote from a SWGIT document must include the version number (or create date) of the document and mention if the document is in a draft status.

Section 14

Best Practices for Image Authentication

OBJECTIVE

The objective of this document is to provide personnel with guidance regarding practices appropriate when performing image authentication as part of image analysis.

INTRODUCTION

Forensic Image Authentication is the application of image science and domain expertise to discern if a questioned image or video is an accurate representation of the original data by some defined criteria. Image Authentication is a subtask of Image Analysis, and general best practice issues are discussed in SWGIT document "*Best Practices for Forensic Image Analysis"*. This document addresses issues specific to Image Authentication. Questions involved in authentication include issues of image manipulation, image creation, and consistency with prior knowledge about the circumstances depicted.

Image Authentication must not be confused with the requirement to authenticate evidence as a precondition to admissibility in court. Likewise, authenticity differs significantly from integrity. Integrity ensures that the information presented is complete and unaltered from the time of acquisition until its final disposition. For example, the use of a hash function can verify that a copy of a digital image file is identical to the file from which it was copied, but it cannot demonstrate the veracity of the scene depicted in the image. For further information on digital image integrity, refer to SWGIT document "*Best Practices for Maintaining the Integrity of Digital Images and Digital Video"*.

The process of Image Authentication can involve several tasks. These tasks include, but are not limited to, evaluation of image structure and content. Image structure issues include discovery of artifacts consistent with image manipulation or degradation, metadata analysis, and indications of provenance. Image content issues include continuity issues, evidence of manipulation, evidence of staging, and anachronism. General principles and procedures for such evaluations are described below.

Image authentication may involve the evaluation of a number of technical issues as discussed below; the image analyst should demonstrate a command of them. Training and proficiency are discussed in the SWGDE/SWGIT document "*Guidelines & Recommendations for Training in Digital & Multimedia Evidence"*.

GENERAL CONSIDERATIONS

Provenance

In the absence of a witness who can testify to the origin of a questioned image or video, it may be possible for an examiner to authenticate such data by identifying its origin (provenance).

Metadata Analysis

Digital image files contain both pixel data and information about the structure and content of the file itself; the latter is referred to as metadata. Metadata may be useful in identifying the source and processing history of the file, but can be absent or altered.

Detection of Manipulation

For the purposes of this document, manipulation is defined as the modification of image features by direct alteration of image content at the pixel/voxel level. Detection of manipulation may involve analysis of textures within the image, shading and shadow, color balance, palette, lighting, quality of light, perspective, focus, and resolution.

Common manipulation techniques amenable to analysis involve primarily alteration and compositing. Alteration is the changing of image features through the use of artistic means. Figure 1 provides an example.

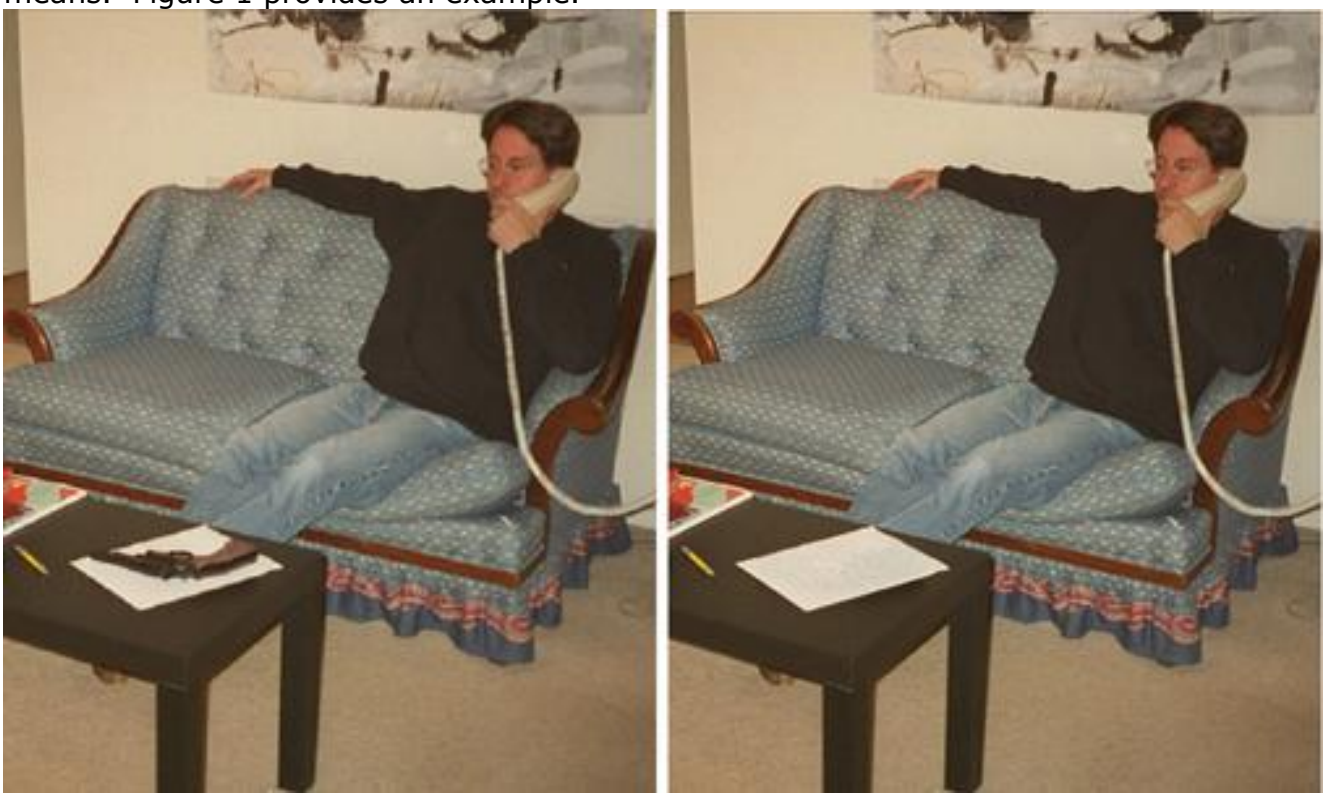

Figure 1. Left is original image. Image on right has been altered to remove weapon from table.

Compositing (also known as cut-and-paste) is the combination of elements of two or more images to form one image. Figure 2 provides an example.

These techniques are sometimes incorrectly referred to as morphing. Morphing is the automated transformation of components of one image into those of another involving a sequence of intermediate images demonstrating incremental change.

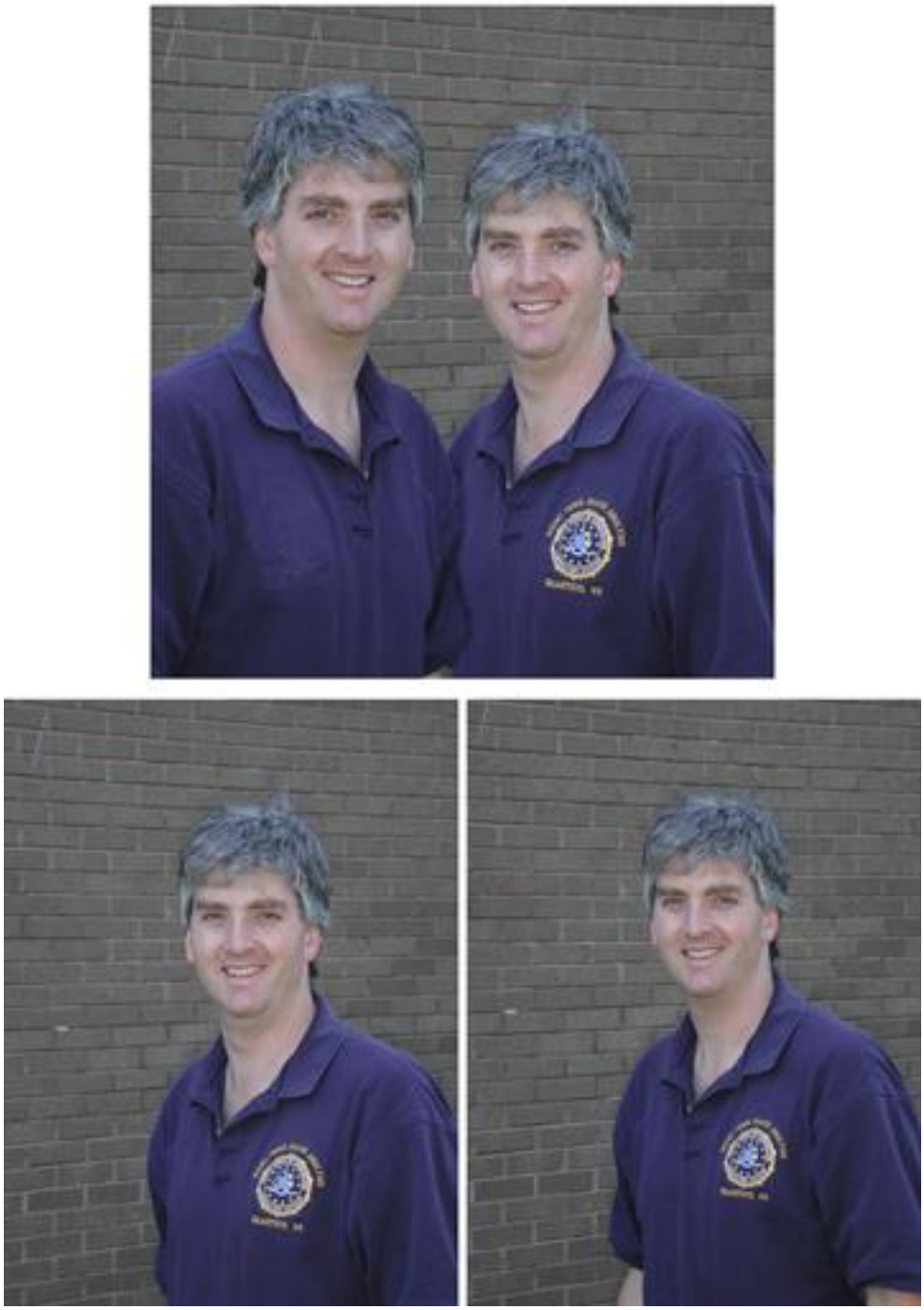

Figure 2. Top image has been created by altering bottom left image and compositing it with the bottom right image.

While it is technically feasible to manipulate an image, particularly a single still image, in a manner that is not detectable by subsequent analysis using currently available tools and techniques, such manipulations involve a number of practical issues. These issues include, but are not limited to:

- Access to the image;
- The skill level of the artist necessary to perform the manipulation;
- The time necessary to create the manipulation;
- The availability of software and hardware necessary to perform the manipulation;
- The level of fine detail in the image; and
- The complexity of the image content, such as physical interaction of people with one another and the environment.

For instance, changing the color of a fountain pen in an image may be easy for an unskilled artist to achieve, but it would be a much greater artistic and technical challenge to alter an image of a nude adult to appear to be a young child. Accordingly, the complex manipulations necessary in the latter case might be easier to detect compared to a simple color change.

The presence of a manipulation does not necessarily mean that the events depicted in an image did not occur or that the individuals depicted are not real or were not there at the time. There are multiple examples in known child pornography images in which the face of an adult has been altered to obscure identity. Likewise, there are other real child pornography images in which parts of the background have been obscured to prevent observers from determining information such as the location or date of the image.

Detection of Image Creation
This is the creation of image content entirely through artistic means. One example is the creation of virtual humans using 3D modeling software (e.g. "computer-generated" or "CG" humans). Detection of such creation involves the discovery of unrealistic components and features within the image, including subsurface scattering of light in the skin, depth of field, textures, movement and physics.

Detection of Staging
Staging is the physical alteration of the scene prior to image acquisition. Detecting this may require coordination with scene investigators, correlation of image features with the real features at the scene, or comparison with other images of the scene or subject.

Continuity Issues
Continuity involves temporal inconsistencies in moving images, or inconsistencies of content within the scene in a still image. Examples include "cut edits" in a video sequence and anachronism. Anachronism is image content incongruous for the date represented in the image. Similar analysis is done to detect incongruities of place and situation. Provenance issues involve the time, place, and manner of image creation. For instance, a photograph purporting to be an original of Abraham Lincoln recorded on modern film would be suspect.

Image Processing

Image processing is often not necessary for image authentication. For instance, a picture supposed to be taken in Paris that shows the Washington monument in the background will be suspect by inspection. Detection of incongruous textural features, however, may require substantial image processing. Image Processing is discussed in SWGIT document *"Recommendations and Guidelines for the Use of Digital Image Processing in the Criminal Justice System"*.

Report

Image authentication conclusions can rarely, if ever, be reported in terms of a numerical probability. It is sometimes possible to definitively detect manipulation or rule out authenticity. It is further possible to determine positive evidence for authenticity according to a set of criteria. Those criteria should be delineated in the report.

SPECIFIC CONSIDERATIONS

In today's forensic context, certain authentication tasks are particularly common. The application of the general authentication considerations to some of these specific areas warrants discussion.

Child Pornography

Over the past decade, there has been a heightened public awareness of the exploitation of children and of child pornography, leading to an increased case load for many agencies.

A common assertion regarding purported child pornography is that the image does not depict the actual abuse of a child. Instead, there may be multiple claims:

- The image is that of an adult that has been manipulated to appear to be that of a child;
- A non-sexually explicit photograph of a child has been altered to appear to be a sexually explicit photograph; or
- The image was created through artistic means without the exploitation of real children (e.g. "computer generated" children).

The best way to authenticate child pornography is to identify the victims in the image. Investigators do this through the use of known victim databases and direct contact with victims and people who know the victims. If authentication cannot be done in this manner, then further forensic analysis may be necessary.

Detection of Manipulation

Common manipulations encountered by the analyst include cut-and-paste and removal or reduction of secondary sexual characteristics using so-called "airbrushing" and "cloning" tools, among others. Artifacts of such manipulation may include inconsistencies in lighting and shadows, inconsistencies and discontinuities in color and texture, differing resolutions within an image, changes in compression and noise artifacts, and repetition

of textures and features. Subject matter experts may be able to observe such artifacts directly through visual inspection or by utilizing image processing techniques.

Detection of Image Creation

It is increasingly practical to render virtual people, but some aspects of the human body remain a challenge for artists. Unrealistic features may be observed in:

- Skin tones & textures
- Skeletal structure
- Flesh & muscle movement
- Body-to-object contact
- Skin-to-skin contact
- Skin creases
- Hair
- Ears
- Eyes
- Reaction of subjects/objects to gravity and physics.

Continuity Issues

Human beings move in a manner that is generally continuous and fluid. A recording of this movement in a sequence of images should reflect this continuity. Lapses in continuity of motion may indicate image manipulation or fabrication.

Provenance may be important. Many images encountered in child pornography are part of a series of images depicting the same individuals and/or scene. When a single image can be demonstrated to be part of a series (including video), the existence of the series supports its authenticity because of the difficulty of creating consistent, undetectable manipulations. Additionally, metadata may link an image to a specific camera, date and time, or author/creator.

The relationship between historical print media and computer imagery is of particular importance in the evaluation of child pornography. There were times and places in which child pornography was legal. These images were frequently published in magazines dedicated to child pornography. This era was prior to the advent of commercially available consumer-level digital image processing. This has specific implications:

- During this period, it was practical and cost-effective to create pornography using real children in real sexual acts.

- The technology of the period did not allow sophisticated digital image manipulation.

The practical implication of this for modern investigation is that when images dating from that period are encountered, their provenance argues for authenticity.

Child Pornography Case Workflow Example

A workflow example is included below:

A local police agency submits 20 digital images depicting child pornography. The request is to determine if the individuals and events depicted in the imagery are real or the result of manipulation or fabrication.

Following the workflow delineated in SWGIT's "*Best Practices for Forensic Image Analysis"* the agency proceeds:

1. The agency reviews the request and:
   a. determines that they do this type of analysis,
   b. determines that all necessary items to support the requested exam have been submitted,
   c. determines that they have the necessary expertise, materials, and resources to perform the analysis, and
   d. the analysis is assigned to an analyst.

2. The analyst obtains the imagery. The analyst contacts the investigating agency and verifies that the images are original images.

3. The analyst triages the images.
   a. The images are viewed to see if the subject is a known victim. The subject has not previously been noted, and is considered a new victim.
   b. The images are prioritized to establish the order in which they will be analyzed. The analyst also evaluates the images as a group for comparison with respect to continuity and similar issues.

4. Initial image processing is determined to be unnecessary in this case.

5. The images are examined to determine if there is evidence of manipulation. The agency maintains a list of features that are evaluated for such determination. A checklist of these features is used to streamline the note-taking process. Noting a feature that bears further inspection in one image, the analyst uses image processing to enhance the feature of interest. Upon this inspection, the feature is found to represent artifacts explainable as the result of the photographic process. The examiner notes this and continues with the examination.

6. Having found no unexplainable artifacts, consideration is given to the number of images depicting the same individual and/or location, as well as the level of detail. This image set consists of highly detailed views of the same victim in a number of poses taken in what appears to be one location. This is considered strong support of authenticity.

7. The analyst writes the report.

Execution Videos

In the current geopolitical and technological environment, videos purporting to depict the execution of individuals are common. In some cases, determining the authenticity of these videos is operationally important.

A common assertion regarding purported execution videos is that the images do not depict an actual execution.

The best way to authenticate an execution video is to examine the putative victim. If this is not possible, forensic image analysis may be necessary. In contrast to child pornography, in which image manipulation and continuity are of primary importance, the evaluation of execution videos often involves the detection of staging and computer-generated special effects.

Detection of Manipulation

Cases have been observed in which documentation (e.g., a newspaper) is composited into the video to falsify the date. Instances have also been observed in which blood, wounds, and smoke have been artistically inserted.

In addition to the inconsistencies noted in the discussion of child pornography, artifacts seen in fake execution videos include the geometric artifacts of the modeling of special effects, such as globular smoke, reflecting the underlying geometric model used for the special effect.

Detection of Image Creation

Execution videos that are completely generated without the involvement of real people have yet to be demonstrated as forensically important. The same questions of realism that were discussed for child pornography would pertain.

Detection of Staging

Indicators of staging include inconsistencies on the scene, unusual objects or arrangements of objects in the scene, and unnatural body movement or position. For example, in a staged hanging the examination of the folds in the clothing might reveal an underlying scaffolding holding the body erect. This would suggest that the individual had been killed earlier and the execution was staged on a corpse. There have been cases in which a corpse was posed to make it appear that the subject was still alive for the purposes of extortion.

Subject matter expertise is often critical when looking for staging – it may be important to have extensive knowledge of uniforms, weapons, anatomy, physiology, or other disciplines in order to reach an accurate conclusion. In some staged executions, blood substitutes such as colored syrup or water do not display appropriate viscosity or bloodstain pattern behavior. In the recent Iraq conflict, the news media reported on a picture of a purported American hostage accompanied by death threats, which turned out to be a posed scene using a toy action figure.

Detection of staging was accomplished through recognition of the action figure, the lack of standard insignia and ID on the uniform, inauthentic appearance of a toy weapon, and the presence of WWII-vintage hand grenades on the victim's vest (an anachronism).

Continuity Issues

The basic principles of continuity assessment apply, as described previously. In the case of execution videos, a common finding is the presence of multiple "takes," in which the scene is replayed for varying camera angles and perspectives. In a well-known case evaluated by multiple offices, frame-by-frame evaluation revealed that a gunshot entrance wound changed location on the body slightly over time. Analysis of optical flow or visual discontinuities may reveal editing.

Consultation with specialists in the analysis of other media, such as audio, may be appropriate.

The Conspiracy Theory Defense

A common issue at trial is that someone has changed a scene or surveillance photograph for the purpose of misrepresentation. While, by definition, it is not possible to prove a negative (one cannot prove that there are no unicorns, only that no one has ever proven they exist), it is possible to demonstrate that it is unlikely. The previous discussions focused more on searching for evidence of manipulation, while this task is oriented more towards providing a measure of the difficulty in achieving an indiscernible manipulation.

It should be noted that crime scene photographers can assist in the process of refuting charges of scene alteration by taking photographs of the same objects or parts of a scene from more than one angle. As noted elsewhere, the process of creating multiple altered images of the same person, object, or scene is more difficult than creating a single altered image. This is due to the fact that the three dimensional properties of people and objects, as well as the manner in which they interact with a scene's lighting, are complex and difficult to recreate artificially in a consistent fashion in multiple images. Having multiple image of the same object from different viewpoints would thus undercut claims that an object was inserted into an image after the fact. Likewise, having multiple images which show the same empty location from multiple viewpoints can contradict arguments that an object had been digitally removed from a crime scene image.

Given that an analysis for a supposed modification provides no positive evidence for it, important considerations for a negative conclusion include:

- The artifacts that would likely be produced and the techniques necessary to remove them;
- The practical limitations of the algorithmic technique supposedly employed;
- The time and expertise necessary to achieve the supposed modification, given the opportunity; and

- The resources (hardware, software, training) that would be required and their availability at the time of the supposed modification.

To illustrate with an example, consider an allegation of prisoner abuse recorded by video taken by a participant. The video had been downloaded onto a laptop computer and had been in his possession for two days. The defense claimed that the owner of the laptop computer had inserted images of the defendant into the video. Analysis of the video revealed no evidence of manipulation. Computer forensic analysis revealed that no software had been added or removed from the computer during the time period in question and that the laptop computer contained only a common media player and editing software that allowed editing clips. Modification of individual frames was not possible using this software. Therefore, modification of the sort claimed by the defense would not have been possible with the resources and time available.