Video Error Level Analysis

By Doug Carner, CPP/CHS
President of Forensic Protection, Inc.

ABSTRACT:
Video content manipulation can be extremely difficult to detect. Video Error Level Analysis (VELA) can definitively identify and document video cropping and the addition, removal, relocation or alteration of an object, weapon, person, vehicle or text.

INTRODUCTION:
With rare exception, video compression is lossy(1) and thus creates an imperfect copy of the original video data. Each time a video is resaved, additional video quality losses occur, even in the absence of any editing or alterations. Furthermore, since most video CoDecs compress utilizing data from adjacent frames, and within pixel blocks, video cropping will disproportionally affect perimeter pixels.

Modern CoDec compression causes quantization data errors, often seen as visual artifacts, as the data extremes are suppressed to reduce the overall video file size. Each subsequent compression reduces the variance extremes between adjacent, and blocks of, pixels by a lesser amount. After a nearly infinite number of compressions, the minimal error level will be reached and the video may appear as a homogeneous blur(2).

If an object is added to, or relocated in, an already compressed video, it will be at the earlier stages of this process. As such, when the altered video is compressed again, any recent viewable alterations will incur larger changes in quantization data errors than the remainder of the video content. This can be visually represented by subtracting a re-compressed video from the version that you began with.

MATERIALS AND METHODS:
Start with a suspect video named "BEFORE", and then save it as “AFTER” using a h.263 CoDec. Subtract the AFTER video from the BEFORE video and the difference represents the newest quantization data errors, viewed as a nearly black video. To perform your own test:

1. Install free software: VirtualDub(3), AVISynth(4) and the XVID(5) h.263 CoDec.
2. Run VirtualDub and open (under the FILE menu) the video named "BEFORE.avi"(6). The altered object is a 4th logo moving from the upper left corner until it disappears in the lower right.
3. Under the VIDEO menu, set compression to XVID (use the "configure" button to set quantizer to 8)
4. Use the Save command (under the FILE menu) to save this video with the name "AFTER.avi".
5. Create a new text file named “TEST.avs” with the following text:

```
BEFORE=directshowsource("BEFORE.avi")
AFTER=directshowsource("AFTER.avi")
Overlay(BEFORE,AFTER,mode="Subtract")
Levels(0,5,100,0,255)
stackhorizontal(BEFORE,last)
```

6. Right click to open this file with VirtualDub, and then save the resulting video as "RESULTS.avi”.

RESULTS:
As the RESULTS video plays, the VELA value of the added (aka manipulated) fourth company logo will nearly always be larger, and appear brighter, than the original three logos. The resulting VELA view of the original three moving logos will briefly become brighter as they overlap the altered logo. This is a side effect of the CoDec's predictive frames algorithm, and this issue was intentionally encouraged to demonstrate the power of VELA, even under worse-case scenarios.

DISCUSSION:
VELA can be visually represented by subtracting a re-compressed video from the video that you began with. The resulting video will appear black with areas of brightness (luminosity) indicating the differences in error levels between both videos.

Boundaries of high contrast (for example, a bright pixel adjacent to a dark pixel) will have higher VELA values and thus appear relatively brighter in the resulting video. Points of video alteration will be depicted as pixels which are brighter than their relative contrast would suggest. If a video has been cropped to reduce the field of view, the altered perimeter edges will appear abnormally bright. These are the suspected points of manipulation.

If points of manipulation are colored differently than the underlying objects, this information can aid in fingerprinting the software that was used to alter the video. Additional clues can be deduced from analyzing the video's visual consistency (reflections, clarity, shadows, etc…), metadata, and chain of custody. Principal Component Analysis (PCA) and Wavelet analysis can further identify the exact points of manipulation. Prior writings by Doug Carner address many of these complimentary topics.

CONCLUSION:
Detecting video tampering through a visual inspection is nearly impossible, especially when the depicted objects are of varying size, color or brightness. VELA easily detects most after-the-fact changes to a video, and works on all types of digital videos, even historical recordings.

REFERENCES:
(1) "Video codecs and decompressors" (http://www.ncbi.nlm.nih.gov/pmc/articles/PMC3232547/)
(2) Dr. Neal Krawetz, "A Picture's Worth...", 2007 Black Hat conference, Caesars Palace - Las Vegas, 08/01/07 (http://blackhat.com/html/bh-usa-07/bh-usa-07-speakers.html#Krawetz).
(3) http://virtualdub.sourceforge.net/
(4) http://sourceforge.net/projects/avisynth2/ (remember to associate VirtualDub)
(5) XVID h.263 CoDec (http://xvid.org/Downloads.15.0.html)
(6) Files located at (http://ForensicProtection.com/VELA.html)

COMMENTS:
Hands-on workshops and lectures are available without charge, although the hosting venue may impose a fee. Refer to (http://ForensicProtection.com/staff.html) for a current training schedule.
Copyright Forensic Protection, Inc. All rights reserved. Document date: June 4th, 2013.