ARGO Forensic Video Analysis System	**ARGO follows the NIST SP 800-86 guidelines for examination, analysis and reporting. All embedded methods are scientifically valid and the entire workflow is automatically documented.**

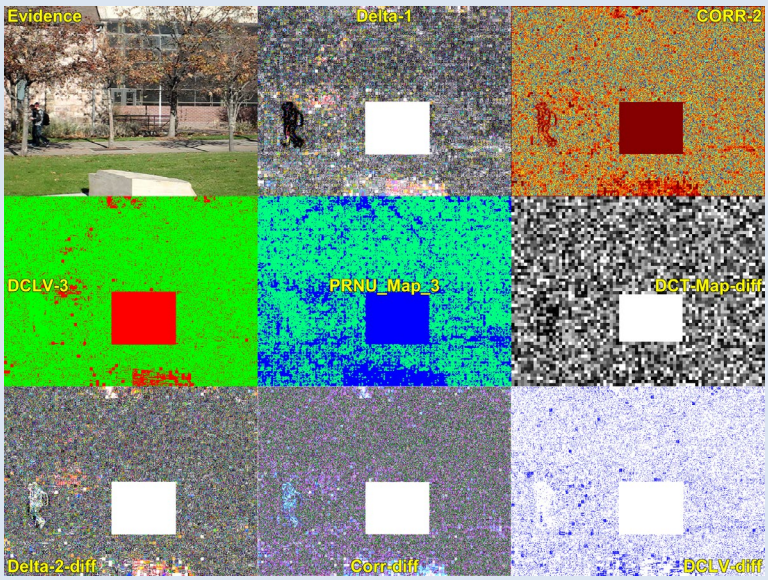
ARGO is a user-friendly software package that offers forensic video analysis and authentication techniques in an easy-to-use environment. Today, video manipulation has become much more subtle, easy, and widespread with the advent of image and video attack techniques such as green/blue screen removal, deleting or adding people and objects, and inter-frame cloning objects. Whether the video has been manipulated for publishing reasons or to obfuscate information, ARGO is the one-stop solution for the toughest video authentication challenges. ARGO follows the forensic framework and much more then described in Grigoras C., and Smith J.M. (2013) **Digital Imaging: Enhancement and Authentication** in: Siegel JA and Saukko PJ (eds.) Encyclopedia of Forensic Sciences, Second Edition, pp. 303-314. Waltham: Academic Press [*selected by Computing Reviews as a notable article of 2013*]. **Remember that video authentication is different than image authentication!**

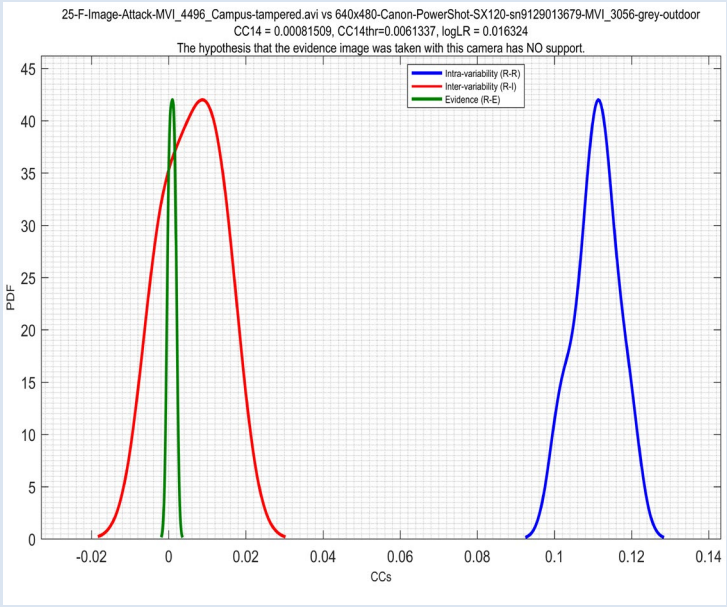
ARGO provides unique tools for:

Structure & Format	Analyze the file structure for inconsistencies or traces of hidden data
EXIF	Extracts the EXIF and Metadata
Audio channel(s)	The audio channels are automatically extracted for further FAAS analysis.
Unique Frames	Detects the unique frames of a video
MJPG Carving	The MJPG frames are automatically carved
Previous Frame Rate	Assess the previous frame rate
Copy-Paste Frames	Detect cloned frames
Copy-Paste Regions of Interest (ROI)	Detect cloned regions
Inserted Objects	Detect inserted objects
Green/Blue Screen Removal	Detect traces of Green/Blue screen removal
Diminished Reality	Detect traces of diminished reality effects
Video Content-Aware	Detect traces of video content-aware
Face Tampering	Detect traces of Face2Face, FaceSwap, DeepFake effects
Video PRNU / Residue	Computes and displays the PRNU/Residue frames, and detects traces of intra-frame and inter-frame editing
PRNU Camera	use PRNU to compare the evidence vs. a reference video; the results are reported as likelihood ratios (LR) and converted to a verbal scale
PRNU Database	use PRNU to compare the evidence vs. a database of reference videos; the results are reported as likelihood ratios (LR) and converted to a verbal scale
YouTube Download	forensic download of YouTube videos
Sort Folder	analyzes all the videos in a folder and sorts them in separate subfolders based on camera Make, Model (e.g. Canon, GoPro, Nikon, etc.), and/or editing traces

A video tampering example showing a frame from the original and tampered videos, and the tampering mask

ARGO results, the first frame of the evidence and resulted videos, and the PRNU analysis against a suspect camera





ARGO protects your files and casework according to the best practices for digital evidence labs.

ARGO also detects and extracts (based on forensic carving) the MJPG frames, and generates a Hex Analysis report for further hexadecimal investigations of the evidence video.

ARGO was successfully tested and installed on 64bit Windows XP, 7, 8, and 10. The minimum recommended configuration is i7 processor, 16GB RAM, 1 TB HDD - solid state preferred.

For a full forensic analysis of a video that contains audio as well, it is recommended to use both ARGO and FAAS.

ARGO and FAAS are available for Law Enforcements only.