FIAS Forensic Image Analysis System	**FIAS 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.**

FIAS is a user-friendly software package that offers forensic image analysis and authentication techniques in an easy-to-use environment. Today, image manipulation has become much more subtle, easy, and widespread with the advent of software image editing adjustments such as adding layers, removing content, and cloning objects. Whether the image has been manipulated for publishing reasons or to obfuscate information, FIAS is the one-stop solution for the toughest image authentication challenges. FIAS follows the forensic framework 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 computing article of 2013*].

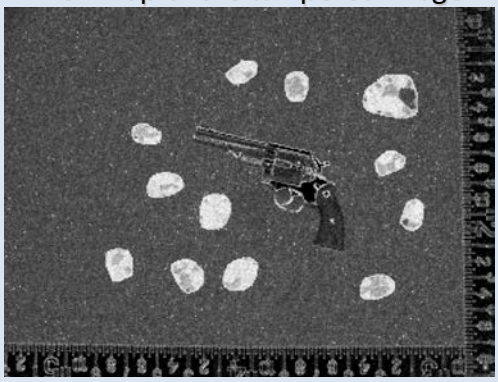
FIAS provides tools for global, local, and PRNU analysis:

Structure	analyzes the file structure for inconsistencies or traces of hidden data
EXIF	extracts the EXIF and Metadata, and displays the map for the GPS coordinates
JPG QT	extracts and compares the JPG quantization tables against reference databases
JPG DCT	extracts and plots the JPG Discrete Cosine Transform (DCT) AC and DC coefficients
CLA	analyzes the compression level of the evidence image
CFA	displays the Color Filter Array analysis of the evidence image
G/B Screen	detects traces of green/blue screen image processing
Color Spaces	splits the evidence image in the main color space layers (e.g. RGB, CMYK, HSL)
DCT Map	computes and displays the Discrete Cosine Transform Map
CL Map	computes and displays the Compression Level Map
CFA Map	computes and displays the Color Filter Array Map
Differential Map	computes and displays the Differential Map
ELA, Adaptive ELA, Smart ELA, JPG Ghost	use classic, adaptive and smart error level analysis to detect traces of local manipulation and to investigate the compression history of the evidence file
Correlation Map	uses pixel level correlation to detect traces of local editing
Blocking Artifacts	uses probability map and block level algorithms to detect traces of manipulation
ADJPEG & NADJPEG	use (Non-)Aligned-Double-JPEG algorithms to detect traces of local editing

Original image

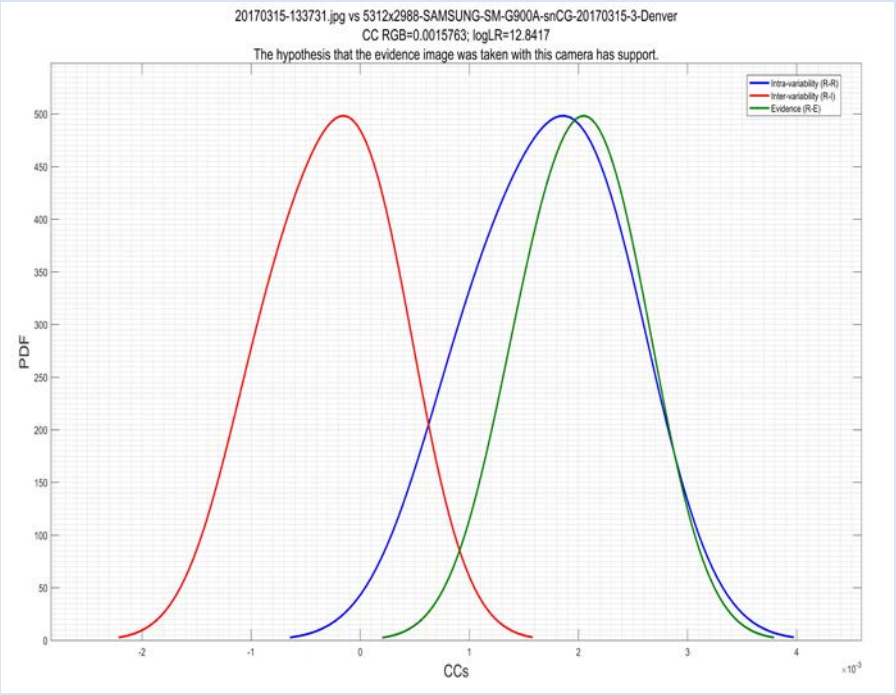
Tampered image

DCT Map of the tampered image



Forensic Media Services, Ltd, Denver, CO, USA 💻 www.mda4n6.com ✉ info@mda4n6.com ☎ (+1) 303-903-9959
Forensic Science Center, Bucharest, Romania 💻 www.forensicav.ro ✉ catalin@forensicav.ro ☎ (+1) 720-412-3340

Histogram Equalization	applies histogram equalization per each layer
High Pass	applies a high pass filter on the evidence image
PRNU / Residue	allows user to extract and analyze several PRNU (Photo Response Non-Uniformity) or Residue maps
Clone Fusion	use different algorithms to detect traces of clone stamp or copy/paste/move
PRNU Camera	use PRNU to compare the evidence vs. a set of reference images; the results are reported as likelihood ratios (LR) and converted to a verbal scale
Δ	computes and displays the mathematical difference, correlation and mean quadratic difference between evidence and a same size reference image
File Batch	allows users to batch process a file; the results are automatically saved in a ZIP file
Σ	averages all the image files from a provided folder
Sort Folder	analyzes all the images in a folder and sorts them in separate subfolders based on Make, Model, and editing traces
Folder Batch	processes the entire evidence images folder
>> Folder Batch	allows users a fast analysis by running only Structure, EXIF, JPG QT, JPG DCT and G/B Screen on the evidence images folder
Archive Case	creates a ZIP file containing the evidence and all the analysis results, and its HASH report. Archive Case works automatically during a File or Folder Batch session



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

FIAS detects and extracts (based on forensic carving) the Thumbnail and Preview JPGs, and generates a Hex Analysis report for further hexadecimal investigations of the evidence file.

FIAS was successfully tested and installed on 64bit Windows XP, 7, 8, and 10. The minimum recommended configuration is i7 processor, 16GB RAM, 512 GB HDD - solid state preferred.
FIAS is available for Law Enforcements only.

Forensic Media Services, Ltd, Denver, CO, USA 💻 www.mda4n6.com ✉ info@mda4n6.com ☎ (+1) 303-903-9959
Forensic Science Center, Bucharest, Romania 💻 www.forensicav.ro ✉ catalin@forensicav.ro ☎ (+1) 720-412-3340