Service Definitions

aletheia - An open-source toolbox for steganalysis

Function	Description	Parameters	Returns
auto	Tries different steganalysis methods.	None	- `pred_outguess [float]`: Probability Outguess - `pred_steghide [float]`: Probability Steghide - `pred_nsf5 [float]`: Probability nsF5 - `pred_juniward [float]`: Probability J-Uniward - `pred_lsbr [float]`: Estimated Payload LSBR - `pred_lsbm [float]`: Probability LSBM - `pred_steganogan [float]`: Probability SteganoGAN - `pred_uniward [float]`: Probability UNIWARD
spa	Sample Pairs Analysis.	- `treshold [float]` (optional, default: 0.05): Treshold	- `hidden_data_found [bool]`: Hidden data detected - `bitrate [float]`: Bitrate (grayscale) - `bitrate_R [float]`: Bitrate (red) - `bitrate_G [float]`: Bitrate (green) - `bitrate_B [float]`: Bitrate (blue)
rs	RS Attack.	- `treshold [float]` (optional, default: 0.05): Treshold	Same as `spa`

Function	Description	Parameters	Returns
ws	Weighted Stego Attack.	- `treshold [float]` (optional, default: 0.05): Treshold - `octave_timeout [int]` (optional, default: 20): Timeout	- `hidden_data_found [bool]`: Hidden data detected - `alpha [float]`: Alpha (grayscale) - `alpha_R [float]`: Alpha (red) - `alpha_G [float]`: Alpha (green) - `alpha_B [float]`: Alpha (blue)
triples	Triples Attack.	Same as `ws`	Same as `ws`
aump	Aump Attack.	Same as `ws`	Same as `ws`
calibration	Calibration attack on F5.	- `octave_timeout [int]` (optional, default: 20): Timeout	Same as `ws`
effnetb0_predict	Runs prediction on a pre-trained effnetb0 model.	- `model_name [string]`: Model to use	- `pred [float]`: Probability of image containing stego payload
srm	Full Spatial Rich Models feature extractor.	- `octave_timeout [int]` (optional, default: 20): Timeout	- `features [bytes]`: Extracted features as a file
srmq1	Spatial Rich Models with fixed quantization q=1c feature extractor.	Same as `srm`	Same as `srm`
scrmq1	Spatial Color Rich Models with fixed quantization q=1c feature extractor.	Same as `srm`	Same as `srm`
gfr	JPEG steganalysis with 2D Gabor Filters feature extractor.	- `quality [string]` (optional, default: auto): JPEG quality - `rotations [int]` (optional, default: 32): Rotations - `octave_timeout [int]` (optional, default: 20): Timeout	- `features [bytes]`: Extracted features as a file
dctr	JPEG Low complexity features extracted from DCT residuals feature extractor.	Same as `gfr`	Same as `gfr`

Function	Description	Parameters	Returns
chi_square	Perform Chi-Square Analysis on an image to detect potential hidden data.	- `treshold [float]` (optional, default: 0.05): Treshold	- `detected [bool]`: Hidden data detected - `chi_stat [float]`: Chi-statistic - `p_val [float]`: P-value

extractor - Functions for extracting data from images.

Function	Description	Parameters	Returns
extract_exif	Extracts all exif fields.	None	- `exif_data [dict]`: Extracted exif data as dictionary.
extract_comment	Extracts data embedded into the comment section.	None	- `data [bytes]`: Extracted data.
extract_eof	Extracts data appended to the end-of-file marker.	None	- `data [bytes]`: Extracted data.
extract_outguess	Extracts data using Outguess.	None	- `data [bytes]`: Extracted data.
extract_steghide	Extracts data using Steghide.	None	- `data [bytes]`: Extracted data.
extract_lsbsteg	Extracts data using LSB Steganography.	None	- `data [bytes]`: Extracted data.
extract_jsteg	Extracts data using JSteg.	None	- `data [bytes]`: Extracted data.
extract_lsbs	Extracts least significant bits (LSBs).	None	- `lsbs [bytes]`: Extracted LSBs.
extract_img_type	Retrieves image type based on common magic bytes.	None	- `img_type [string]`: Image type (e.g., PNG, JPG, BMP, GIF, etc.).

Function	Description	Parameters	Returns
extract_strings	Executes a string search within an image.	- `min_length [int]` (optional, default: 6): Minimum consecutive UTF-8 characters.	- `strings [list]`: List of extracted strings.
binwalk_analyze	Scans the file using Binwalk.	None	- `findings [list]`: List of findings, including offsets and descriptions.
binwalk_extract	Extracts embedded data using Binwalk.	None	- `findings [list]`: List of findings, including offsets, descriptions, and extracted data.
compare_exif	Compares EXIF fields between two images.	- `image_b [bytes]`: Image to compare with.	- `exif_diff [dict]`: Dictionary with EXIF field names as keys and differences in the form "ExifData_a:ExifData_b" as values.

util - Collection of utility functions.

Function	Description	Parameters	Returns
save_file	Saves temporary file.	- `file_name [string]` (optional): Temporary file name. - `life_span [int]` (optional, default: 10): File life span in minutes (-1 = unlimited). - `file_limit [int]` (optional, default: 100): Limit for returned file stats.	- `file_name [string]`: Temporary file name. - `expires_at [string]`: Expiration date. - `data_type [string]`: Data type. - `sha256 [string]`: Sha-256 hash. - `file_type [dict]`: File type. - `stats [dict]`: File stats.
get_last_file	Gets the last saved temporary file.	- `delete_after [bool]` (optional, default: False): Delete after retrieval. - `file_limit [int]` (optional, default: 100): Limit for returned file stats.	- `file_data [bytes]`: File data. - `stats [dict]`: File stats. - `sha256 [string]`: Sha-256 hash. - `file_type [dict]`: File type.

Function	Description	Parameters	Returns
get_file	Retrieves temporary file.	- `file_name [string]`: Name of the file to retrieve. - `delete_after [bool]` (optional, default: False): Delete after retrieval. - `file_limit [int]` (optional, default: 100): Limit for returned file stats.	Same as `get_last_file`.
get_stats	Retrieves current info of saved files.	- `file_limit [int]` (optional, default: 100): Limit for returned file stats.	- `stats [dict]`: File stats.
compare_size	Compares the size of two files.	- `file_b [bytes]`: File to compare with.	- `size_a [int]`: Size of file A. - `size_b [int]`: Size of file B. - `diff_in_bytes [int]`: Difference in bytes. - `diff_in_percentage [float]`: Difference in percentage.
get_file_type	Retrieves the type of a file based on known magic bytes.	None	- `file_type [dict]`: File type (e.g., PNG, JPEG, ZIP, etc.).
sha256	Calculates the sha-256 hash value of a file.	None	- `sha256 [string]`: Sha-256 hash.
png_to_jpg	Converts PNG to JPG.	None	- `jpg_img [bytes]`: The JPG image.
jpg_to_png	Converts JPG to PNG.	None	- `png_img [bytes]`: The PNG image.
clear_storage	Deletes all stored files from storage.	None	None

vt - A service for VirusTotal file analysis.

Function	Description	Parameters	Returns
scan_file	Scans a file using the VirusTotal API. Delay can be set to allow for better timing.	- `delay [int]` (optional): Delay for the scan (in sec). Default: 5	- `report [dict]` - `report_url [string]`

Function	Description	Parameters	Returns
get_report	Retrieves the analysis report for a file. It fetches detailed results and a URL to the report.	None	- `report [dict]` - `report_url [string]`