Verification Application

User Manual

Rolf Fricke, Jan Thomsen, Ali Sarioglu

Condat AG, Berlin

InVID - In Video Veritas:

Verification of Social Media Video Content for the News Industry

Version: 2.3

23 April 2019

Tabel of Contents

1 Introduction 3

2 User Interface - Overview 4

3 Verification App – Detailed Feature Description 5

Registration and Login 5

A) Video Player 5

1) Verify new Video with indicated URL 5

2) Monitor Progress of the video analysis 5

3) Play/ Stop video and use further player features 6

4) Meta Data 7

5) Adjust Brightness and Contrast of the Video 7

B) Verification Services for the whole video 7

1) Assessment and notes from users 7

2) Near Duplicates 8

3) Forensic analysis of the whole video using different filters 9

4) Social Media Search for further Near Duplicates by keywords 10

5) Source information about the video provider derived from the meta data 11

6) Location/time information extracted from the video meta data 11

7) Rights information extracted from video meta data and other rights sources 12

8) Comments/Tweets related to the video from several social media channels 13

C) Video Tracks analysis on shot, subshot and frame level 13

1) Play slider and further options to play the video, frame-by-frame navigation 13

2) Shots/Subshots allow to activate a forensic analysis for subshots 14

3) Video Forensic for subshots 14

4) Reverse Image Search and Image Forensic for Keyframes and each frame during Single Step 14

5) Logos detected in the video with reference to the original Logo definition 15

6) Video Forensic Analysis results 15

7) Near Duplicates for segments of the video are shown in a list 16

8) User Comments 17

4 Details about the parallel processing of Verification Services 18

1 Introduction

The InVID Verification Application – or shorter: Verification App – supports journalists during the whole video verification workflow from analysis, validation of results until the assessment. The comfortable user interface provides features for playout, analysis of aspects concerning the whole video and for the deeper examination of relevant shots and subshots down to frame level. The InVID App supports the verification workflows according the leading best practice from https://firstdraftnews.org and the http://verificationhandbook.com .

Target Group

The Verification App addresses individuals and groups of users from the TV/Media sector such as journalists, who want to analyse and verify videos from social networks for re-use in new media productions.

Browsing Example Videos

In order to get acquainted with the Verification App we recommend to browse with a Chrome, Firefox or Safari Browser through the already processed videos. There are several examples on http://invid.condat.de such as the Pope's 'magic trick' or the eagle snatching a kid.

Login

For the analysis of new video you have to register using a social media account at http://invid.condat.de through an Internet connection allowing to play HD videos.

Video Sources

The user can analyse new videos with URLs from Youtube, Facebook or Twitter, for other videos only a partial analysis is possible.

Common Data Space

The Verification App uses a common data space, so that several users can collaboratively view, analyse and comment the same video. The videos and analysis results are permanently stored in a data base, so that the cooperative work can be interrupted and resumed.

Monitoring the Analysis of new Videos

During the analysis of new videos the Verification App calls several remote services from the InVID partners Certh, Modul, WebLyzard and ExoMakina. The parallel processing of these services, which usually need less time than the video length, can be tracked by the user through the monitoring window.

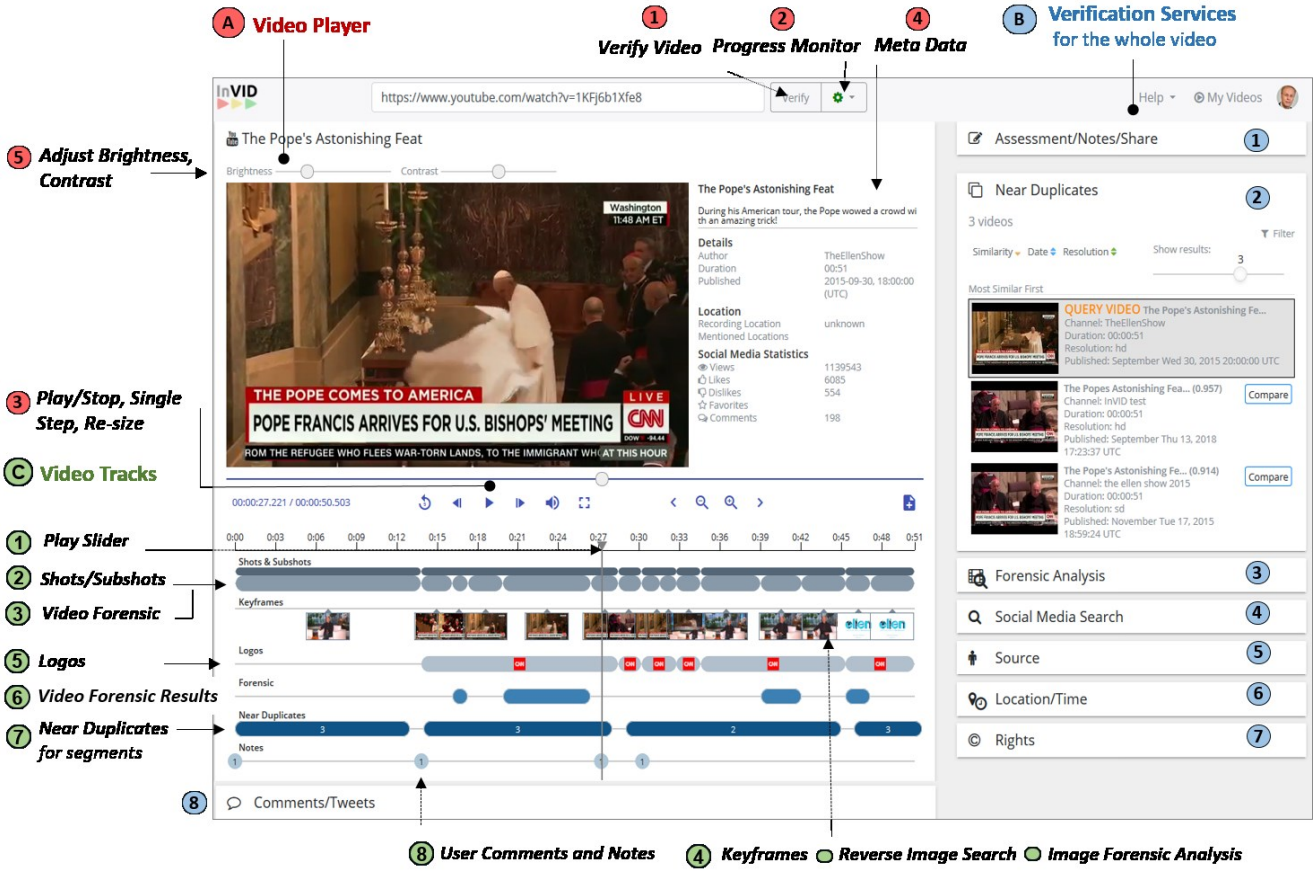
Tolerate cases where not all analysis services can be applied

Please be aware, that sometimes services can not be applied due to specific conditions of the video, such as low resolution, missing meta data or limited access rights. Therefore we recommend the user to concentrate on the available results to verify the video.

User Interface: the Verification App offers a user interface with three main cards:

- **Video Player** to analyse new videos and play them with several options to start and stop including a frame-by-frame playout.
- **Verification Services** to analyse and assess the whole video regarding
  Near duplicates, Video Source, location/date, rights, related social media
- **Video Tracks**: visualize the video in more detail on several hierarchical levels: shots, subshots and keyframes enabling to analyse parts of the video deeper by various services.

2 User Interface - Overview



A) Video Player

1) **Verify Video** starts the analysis of the video with the indicated URL
2) **Monitor Progress** for the analysis of the new video
3) **Play, Stop, Single Step** and further player control (re-size tracks, subtitles, full screen,)
4) **Meta Data** are shown right to the video
5) **Adjust Brightness and Contrast** of the video

B) Verification Services for the whole video

1) **Assessment/Notes** from users for the video
2) **Near Duplicate** Search with function to **Compare Query Video and Near Duplicate Video**
3) **Social Media Search** for further Near Duplicates by keywords
4) **Source** information about the video provider derived from the meta data
5) **Location/time** information extracted from the video meta data
6) **Forensic** analysis of whole video with function to **Compare Query Video and Filtered Video**
7) **Rights** information extracted from the video meta data and further rights data bases
8) **Comments/Tweets** related to the video from several social media channels

C) Video Tracks analysis on shot, subshot and frame level

1) **Play slider**
2) **Shots/Subshots** divide the the video in logical units
3) **Video Forensic** for subshots analysis using specific filters (items, similarity, date, resolution)
4) **Keyframes** per subshot to activate **Reverse Image Search** or **Image Forensic Analysis**
5) **Logos** detected in the video with reference to the original Logo definition
6) **Video Forensic results** for subshots from already processed requests
7) **Near Duplicates** for segments of the video are shown in a list
8) **User Comments** can be inserted (by click in upper left corner of the Tracks card)

3 Verification App – Detailed Feature Description

Registration and Login

For the verification of new videos you need to register at http://invid.condat.de with a Chrome, Firefox or Safari browser by existing accounts from Facebook, Google or Twitter or by creating an individual account via an email address:

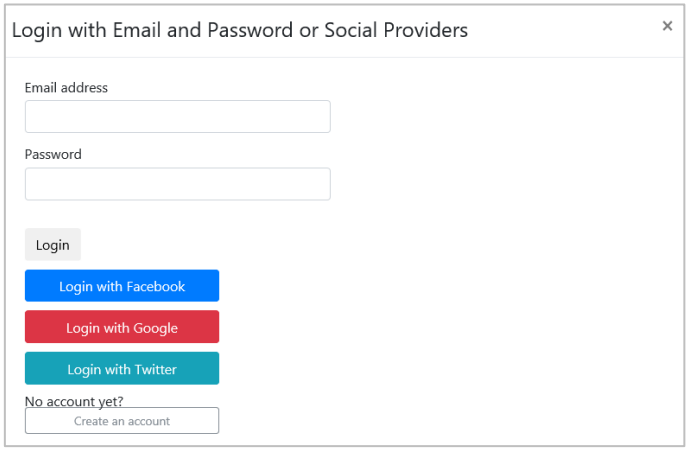


Figure 1: Registration and Login

After the Login the App starts and offers the three main cards **A) Video Player, B) Verification Service** and **C) Video Tracks** as shown in the overview on the page before. The User interface allows to flexibly open and close all main and sub-cards while preserving their content, which enables both for top-down and explorative verification workflows.

A) Video Player

1) Verify new Video with indicated URL

The user can analyse a new video for a URL from Twitter, Facebook or Youtube by clicking the “Verify” button. For some Videos an analysis is not possible (no shots, keyframes or logos are shown and error messages are displayed) if

- the URL is not publicly accessible (in particular for Facebook)
- they need a login or
- their resolution is too low, or the video file is somehow corrupted.

2) Monitor Progress of the video analysis

The analysis of new videos usually needs less time than the video length until all results are available. Therefore we recommend starting with a Youtube video not longer than 1 minute. If the analysis needs more time than expected you can click in the cogwheel to open the Progress Monitor, which shows the execution of the different services running in parallel until they are finished. If several videos are launched at a time, the requests are enqueued and the position of my video in the queue is indicated in the text below the progress bar.

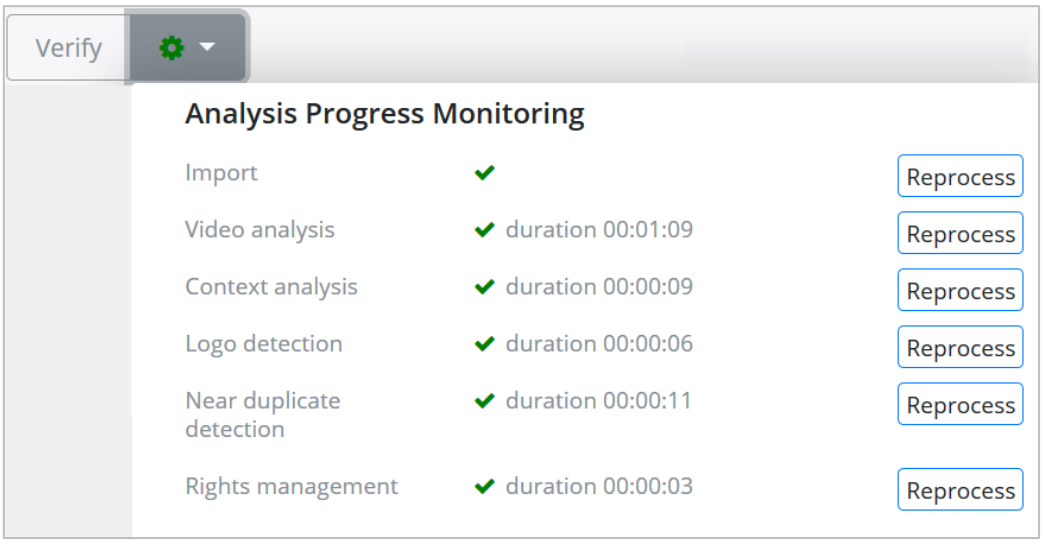


Figure 2: Progress Monitoring

3) Play/ Stop video and use further player features

The Player offers several buttons and bars similar to common video players to stop, play, single step, mute the videoor switch to full screen. The + / - buttons on the lower right side allow to resize the visible part of the tracks, which can be shifted with the < / > buttons.

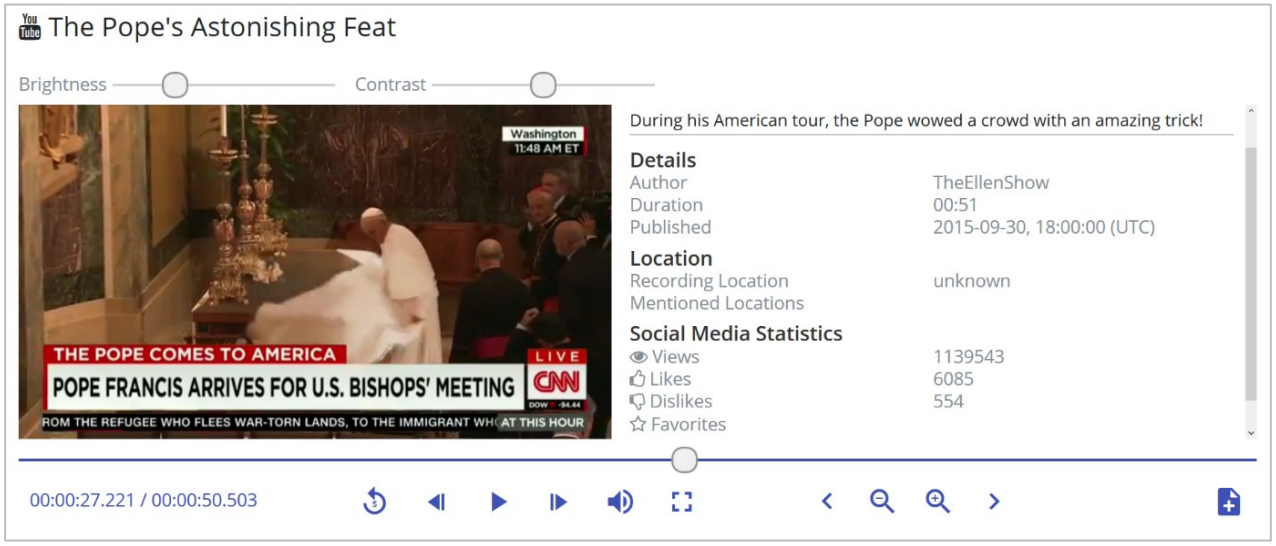


Figure 3: Player Card [1]

[1] the example video was shown in the US-based "The Ellen Show": https://youtu.be/1KFj6b1Xfe8 fabricated from the original: https://youtu.be/ABy_1sL\-R3s

4) Meta Data

Initially, the basic video metadata, such as title, duration and author are shown right to the video player. In addition, the user can display the complete set of available metadata, which are:

i) retrieved metadata via the API,
ii) enriched data coming from the InVID contextual analysis, such as the video's long description,
iii) comments that contain keywords related to verification,
iv) locations mentioned in the metadata,
v) tweets that share the input video, and
vi) the upload time of the video file.

The current version of the contextual verification service extracts context from YouTube, Twitter, and Facebook and maps them on the indicated meta data fields. Moreover, available information about the channel and the contributor of the video, such as whether the channel relates to a verified YouTube account, are displayed. Additional useful information is derived, e.g. from the extraction and display of geographical locations found in the video description.

5) Adjust Brightness and Contrast of the Video

Use the sliders to adjust brightness and contrast even when playing the video.

B) Verification Services for the whole video

The right side of the Verification Application offers verification services related to the whole video.

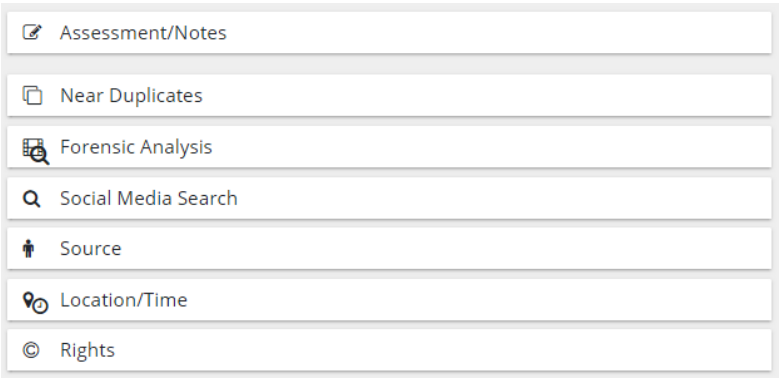


Figure 4: Verification Services for the whole video

1) Assessment and notes from users

The video can be manually assessed by the user according to the verification results. Users may add notes which are stored and shared with all other users verifiying this video.

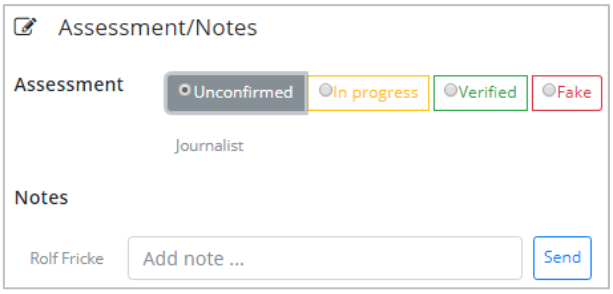


Figure 5: Assessment and notes from users

2) Near Duplicates

The near duplicate search service retrieves near duplicates of the selected video segment by querying the index of pre-analysed videos of the InVID platform. This component aims to identify whether the selected video shot or subshot is part of another video, giving the journalists a clue about its originality or reuse. The retrieved near duplicates are presented in the right card of the application. As illustrated in the Figure below, they are initially shown in descending order based on their similarity with the query video.

- **Filters**
  The user can optionally re-arrange the list based on the filters “similarity”, “date” or “resolution”, and toggle the ascending and descending order. The number of shown results can be adjusted to improve the clarity. The video currently under examination is marked with grey background to ease the verification. For example, when “date” and “earliest first” is selected, the user can directly see which videos were uploaded earlier. If one of them already contains parts of the focussed video, the latter one can apparently not be an original.

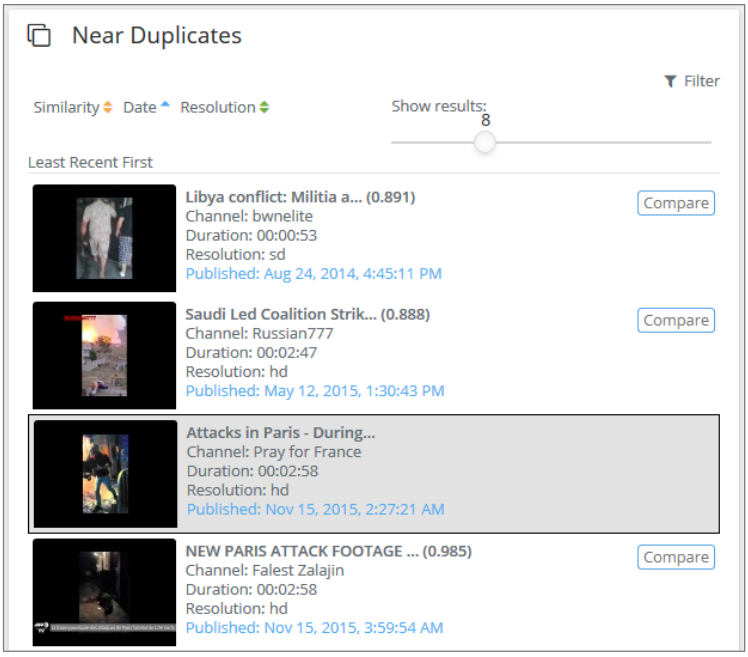


Figure 6: Near Duplicate results and filters

- **Compare Query Video and Near Duplicate Video**
  The Near Duplicate service provides a compare function, that enables the user to regard the query video and a potential near duplicate video in parallel. Both videos are displayed side by side and can be started and stoped synchronously by a single button. This allows to go manually stepwise through the videos and detect differences.

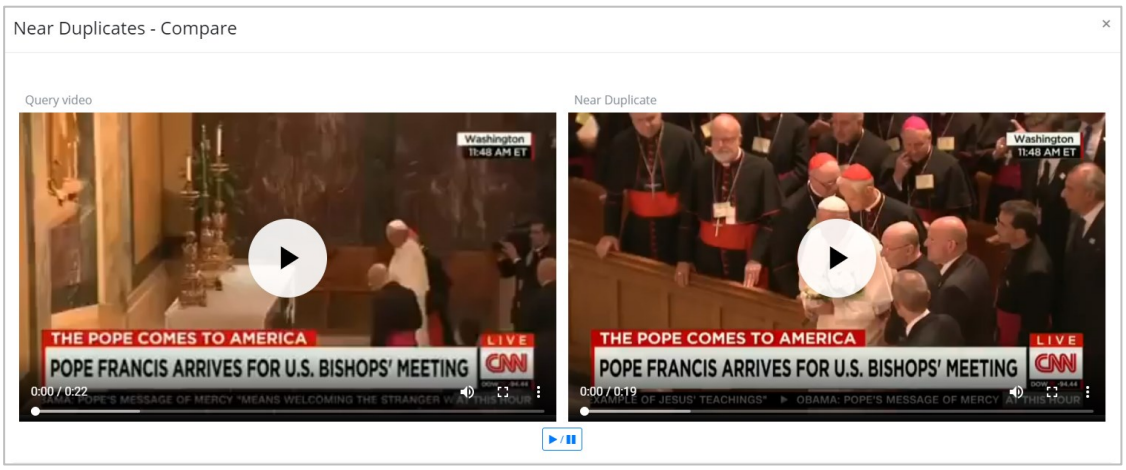


Figure 7: Compare Query Video and Near Duplicate Video

3) Forensic analysis of the whole video using different filters

The service comprises two groups of filters applied to the whole video: the tools for 1) Discovery of irregular or unnormal and for 2) visual improvement. Since these tools need some time for analysis, especially for longer videos, the user has to wait in the case that a new video is submitted to the InVID system for analysis. The user may select the appropriate filters according to type of analysis s/he wants to perform.

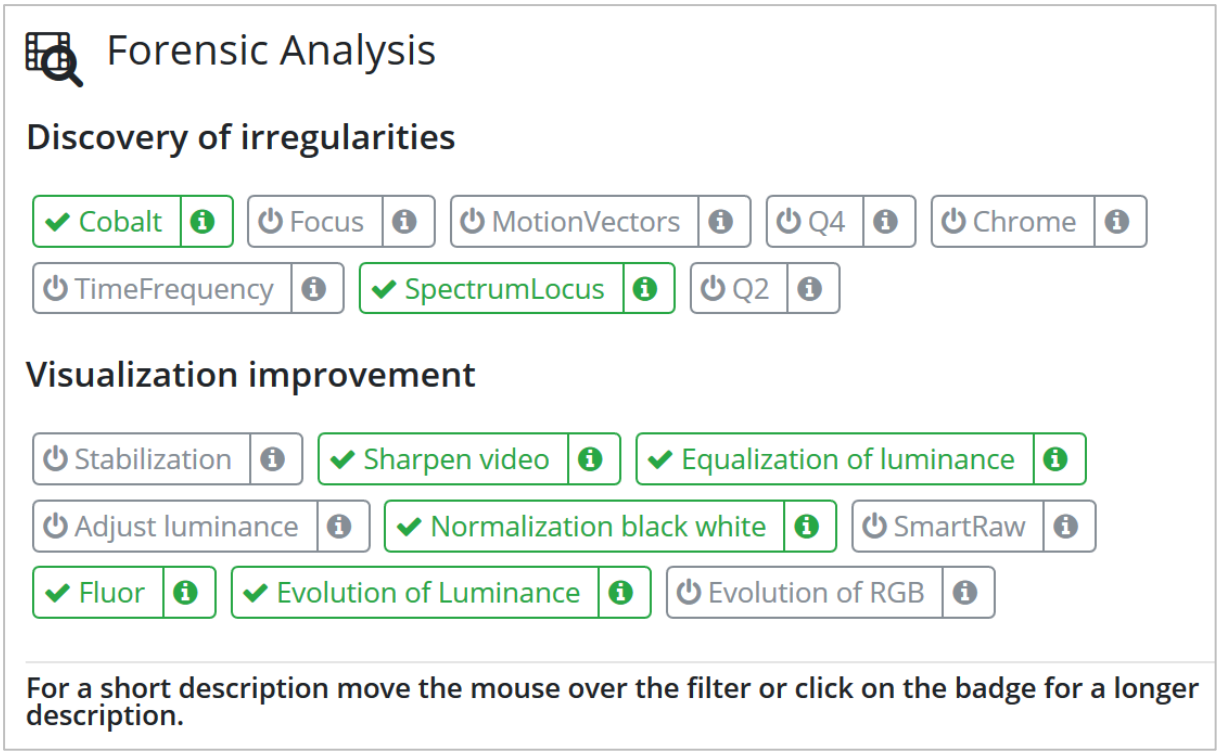


Figure 8: Invoke function of the Forensic Analysis and Visualization Improvement

- **Compare Query Video and Filtered Video**
  For each filter, the Verification App returns an output video with additional information that assists the user to identify suspicious areas, thus supporting the detection of manipulated parts of the video.

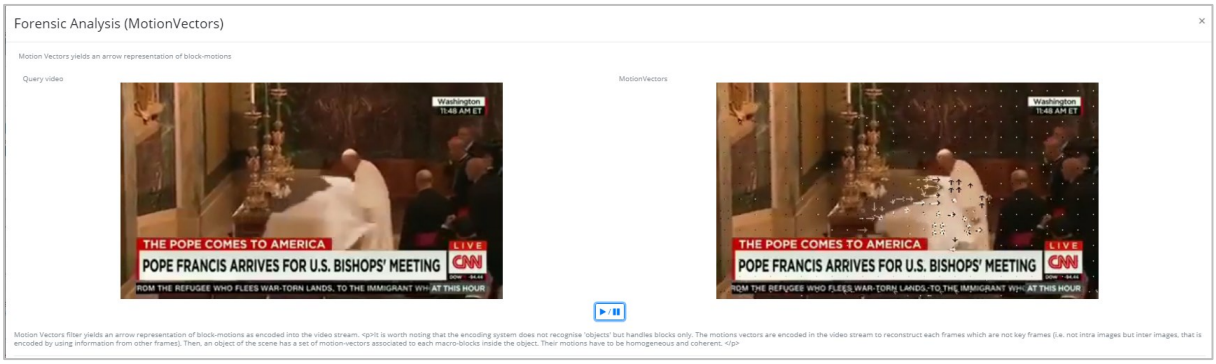


Figure 9: Compare Query Video and Filtered Video

The original video on the left and the version with marks from the selected filter on the right side can be played and stopped synchronously, which allows the user to detect irregular Subshots.

4) Social Media Search for further Near Duplicates by keywords

While the NDS retrieval is based on visual similarity, the Social Media Search for further Near Duplicates is based on keywords. This Search command line proposes keywords from the title and author, which can be eliminated by the user as well as new keywords can be added.

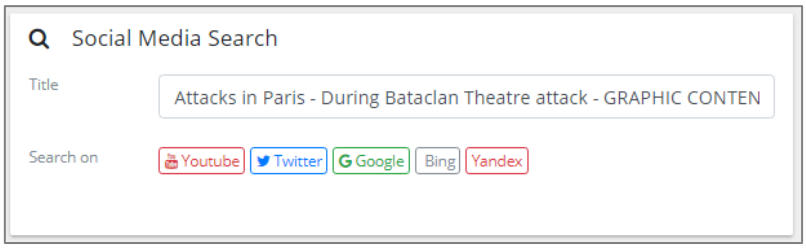


Figure 10: Social Media Search

5) Source information about the video provider derived from the meta data

In the “Source” card all available information about the publishing source is displayed. This information is aggregated from the contextual analysis, as well as the rights management service. In some cases a mapping of meta data required for some sources, e.g. for YouTube videos, if only channel information is available, it will be mapped onto the source.

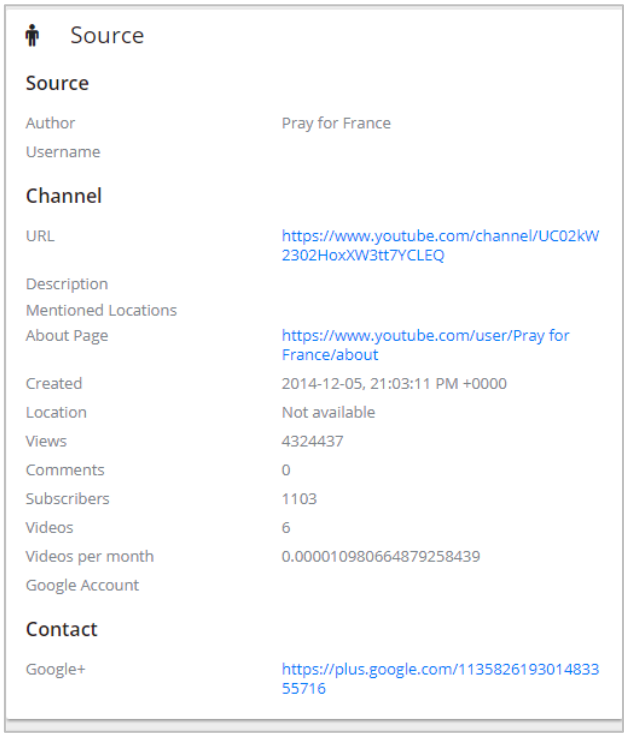


Figure 11: Information about the “Source”

6) Location/time information extracted from the video meta data

When present, publishing time and locations mentioned in the description are shown; as well as recording time/recording location (which is very rarely available).

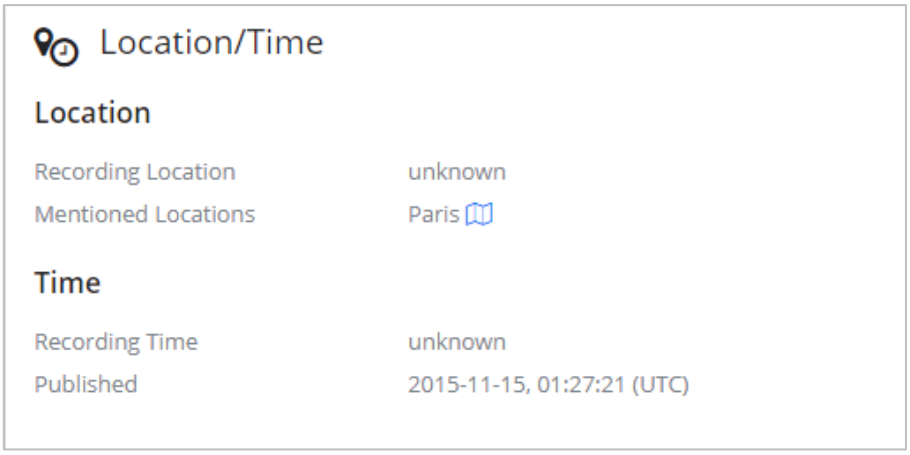


Figure 12: The “Location/Time”

7) Rights information extracted from video meta data and other rights sources

The rights and license management information is retrieved from the rights management component. The first version of the Verification Application returns the license of the video (currently YouTube and Facebook are supported, if it is licensed using the Creative Commons CC-BY license or the Standard YouTube license based on YouTube Terms of Service, in case of YouTube videos).

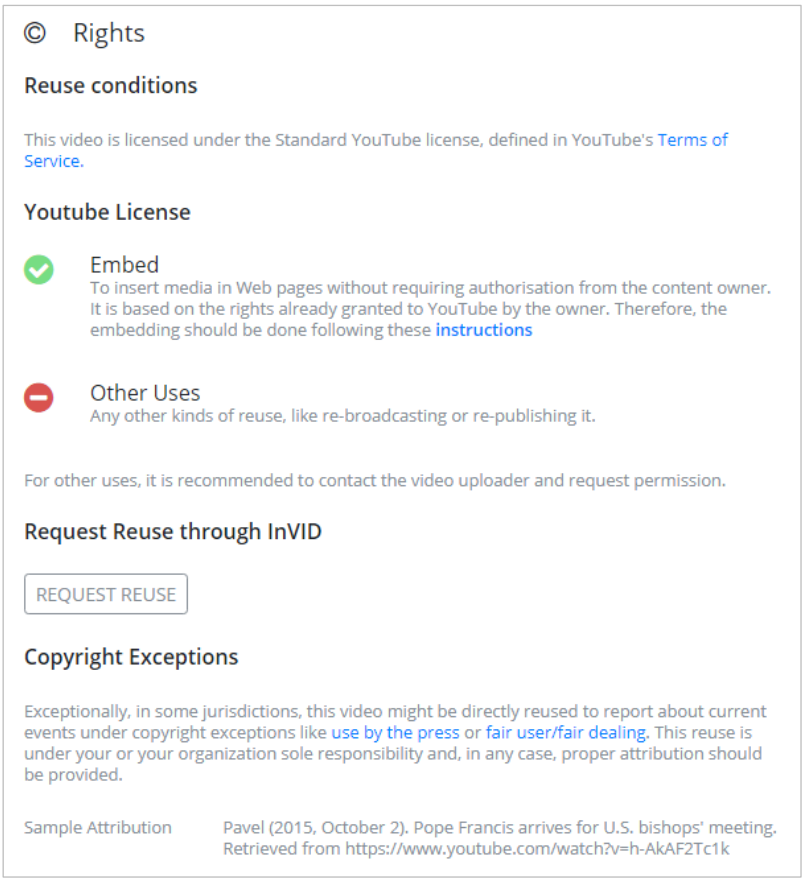


Figure 13: Retrieved rights information about a YouTube video

In addition, the rights management provides a default attribution message that is also available through the Verification App. The rights management component also facilitates with the

“Request Reuse” button to contact the content uploader and assists negotiations of reuse conditions, if the uploader is also the content owner. In upcoming versions of the Rights Module, it will also deliver detailed information about reuse terms if an agreement has been reached, and the user logged in to the Verification Application can benefit from it.

8) Comments/Tweets related to the video from several social media channels

The information gathered from several social media channels is shown in 3 groups: all comments, only verification related comments and tweets.

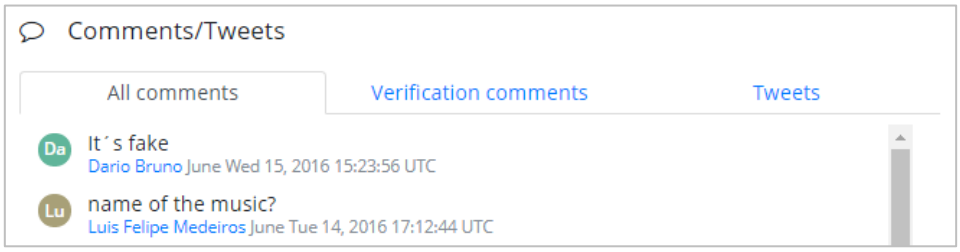


Figure 14: Comments/Tweets related to the video

C) Video Tracks analysis on shot, subshot and frame level

The video tracks card visualizes different types of timeline-based information of the video and enables to invoke further analysis and forensic services for shots, subshots and frames.

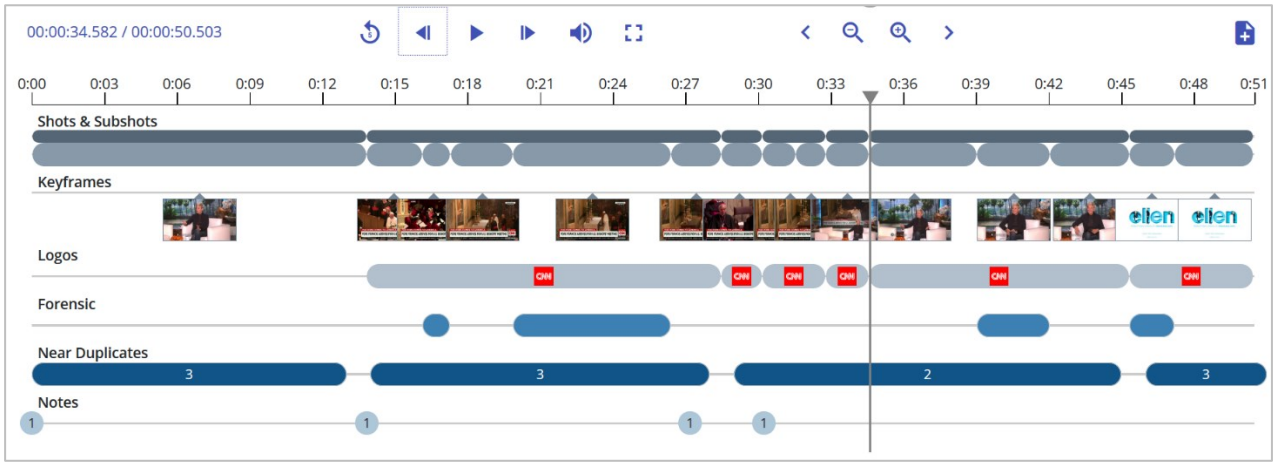


Figure 15: Video Tracks analysis

The timeline can be zoomed in and out by the buttons +/- (in the upper bar of the card) and the visible segment can be shifted by the buttons: < / >.

1) Play slider and further options to play the video, frame-by-frame navigation

The video can be played by i) the button in the lower left of the player ii) positioning the slider in the timeline or iii) click in particular shots and subshots of the video.

Additionally, a frame-by-frame navigation is available by using the arrows <- / -> on the left side of the Video Track card.

2) Shots/Subshots allow to activate a forensic analysis for subshots

This track shows the shots of the video in the upper grey line. The shots are automatically split in smaller units based on visual criteria – the Subshots – which are displayed below each shot. For each subshot the user can invoke a forensic analysis with the most promising filters. Explanations about the use of each filter are provided to the users, enabling them to select the most appropriate filter(s) according to the current/respective use case.

3) Video Forensic for subshots

The Video Forensic analysis is performed by the tools of ExoMakina running at their remote servers. Since the forensic analysis is a heavily computational-intensive process that may cause significant waiting times, the focus on smaller parts of the video and concentration on few filters could significantly reduce the needed time for analysis, allow the user to get the analysis results in a reasonable time. The forensic service displays the resulting video fragment in a separate track below, which contains hints within its frames that help the user to find manipulations in the video.

4) Reverse Image Search and Image Forensic for Keyframes and each frame during Single Step

The app offers one or more representative key frames per subshot which were predetermined by the video fragmentation and annotation service. They enable the user to get a fast overview over the content. For the key frames and each frame shown in the single step mode, the user can invoke the functions reverse image search and image forensic offered in a separate window. In single step mode, choose a frame and pop up the window by mouse-over the video:

Figure 16: Launch “Reverse Image Search” and “Image Forensic Analysis” for current frame

- **Reverse Image Search** to find other already existing similar images on the Web by selecting one of the available search engines (Google, Bing, Yandex, Baidoo, etc.).

- **Image Forensic analysis** using the services from the EU project Reveal [2]. The user can select one of the available forensic filters, based on guidelines about the use and the findings of each filter. The Image Verification analysis component requires some time for processing and then presents the resulting filtered image with the outcomes of the analysis:

5) Logos detected in the video with reference to the original Logo definition

All logos detected in the video based on a database with logos will be indicated in a separate track. The Logos can be of particular organisations or groups of interest (e.g. military organizations, non-governmental organizations, etc.). The search is based on a list of manually indexed logos, which can be extended by the journalists due to the need to recognize newly appearing groups of people in crisis zones or other areas of interest. In the logo-focusing track displays for each detected logo the officially registered one in large format and a reference to the Wikipedia entry for the associated organisation.

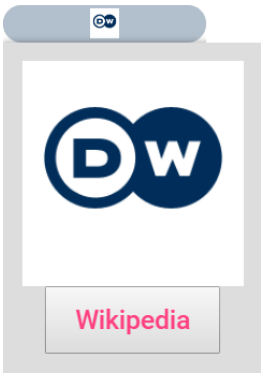


Figure 17: The detected logos within the frames of the video are presented in a separate track

6) Video Forensic Analysis results

The results from previously processed video forensic analysis requests for subshots are displayed in a separate track. The user can play the resulting video for the subshot which contains the derived marks or information of the selected filter.

[2] https://revealproject.eu/

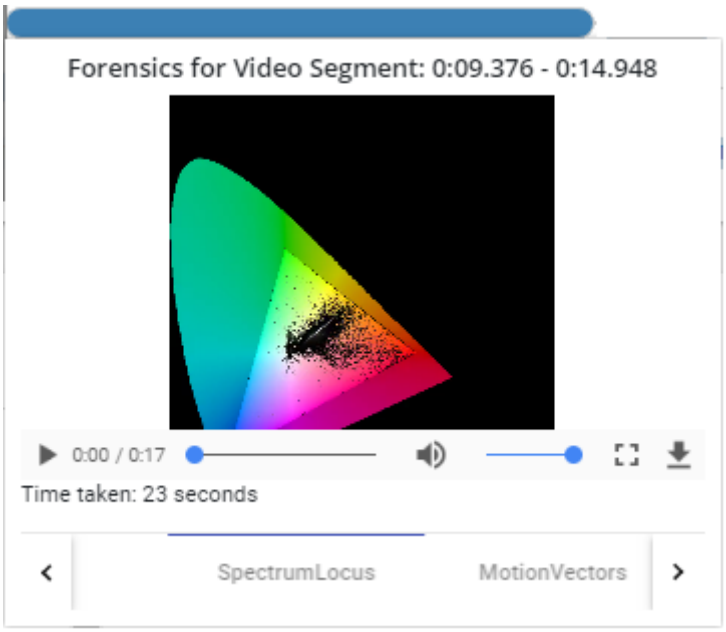


Figure 18: A forensic filter

7) Near Duplicates for segments of the video are shown in a list

The App provides Near Duplicates for smaller segments of the video. The segmentation, which is different from the shot/subshot division, was calculated during the initial video analysis. The Near Duplicates for each segment are shown in a list, which allows the user to examine and play them in order to verify whether one of them is a Near Duplicate of the focussed video. The Near duplicate search on the video-segment-level is an important feature due to the fact that often only particular parts of a video are being reused in other videos. A near duplicate search for the entire video in such cases, will return a low levels of similarity and might lead to misleading conclusions regarding the reuse of the query video. Generally, if A is the original video and B is a video to which we compare it to, then there are two cases: a) A is a part of B, b) B is a part of A.

Figure 19: Near Duplicates for segments

8) User Comments

The comments can be inserted by clicking the symbol in the upper left corner of the Video Tracks card. Each comment is associated with the time line of the video enabling several users to discuss aspects related to certain subshots.

4 Details about the parallel processing of Verification Services

When pushing the Verify Button the analysis process is performed almost automatically in the background. After the import and local caching of video the Player will be available after some seconds and all analysis processes, except Logo detection, are started in parallel. The analysis can be tracked by the Progress Monitor (click in the green wheel). The already available results will be displayed during the analysis and the can be used with the offered functions:

- The **Video analysis** covers the generation of shots/subshots and keyframes. This step is performed sequentially, for all users. If more videos are analysed at the same time by yourself or by other users, they are enqueued. You can identify your queue position in the Progress Monitor.
- The **Logo detection** is always performed *after* successful completion of the video analysis
- The **Contextual Analysis** begins with getting metadata and then gathers related social media comments. If a video has a lot of tweets and retweets the processing can take quite long, independently of the video length (sometimes up to 30 minutes)
- The **Near duplicate detection** is processed for the whole video as well as on parts in a 3-step-process: first near duplicates are searched with a similarity factor or 0.8. If no or only one video is found, the search is repeated with a factor of 0.7, and then with 0.6 if still no video is found. After that, no more near duplicate search is triggered and in that case it might happen that near duplicate search does not return any results.
- The **Rights Checking** the information about the source and copyright conditions.