

# CSE 599B:

# Technology-Enabled Misinformation

Franziska (Franzi) Roesner

[franzi@cs.washington.edu](mailto:franzi@cs.washington.edu)

*Fall 2018*



PAUL G. ALLEN SCHOOL  
OF COMPUTER SCIENCE & ENGINEERING



UNIVERSITY of WASHINGTON

SECURITY AND PRIVACY  
RESEARCH LAB

# CSE Colloquium tomorrow (Thursday)

- Kate Starbird:  
“Muddied waters: Online Disinformation during Crisis Events”
- Please attend or watch (will send video link ASAP)
- Kate joining us for discussion next Wednesday

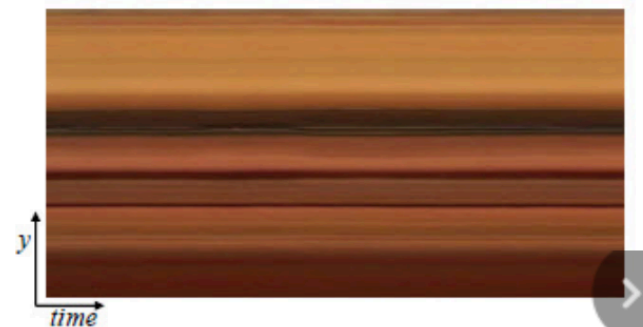
# FaceForensics: A Large-scale Video Dataset for Forgery Detection in Human Faces

Andreas Rössler<sup>1</sup>   Davide Cozzolino<sup>2</sup>   Luisa Verdoliva<sup>2</sup>   Christian Riess<sup>3</sup>  
Justus Thies<sup>1</sup>   Matthias Nießner<sup>1</sup>

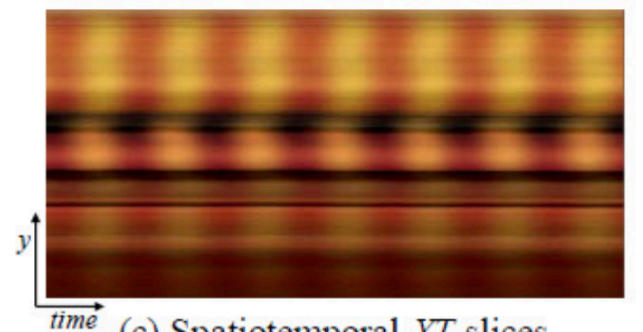
<sup>1</sup>Technical University of Munich   <sup>2</sup>University Federico II of Naples  
<sup>3</sup>University of Erlangen-Nuremberg

[Videos](#)
[Software](#)
[Publications](#)
[Applications](#)
[People](#)
[Related Work](#)
[Talks](#)


(a) Input



(b) Magnified



(c) Spatiotemporal YT slices

An example of using our Eulerian Video Magnification framework for visualizing the human pulse. (a) Four frames from the original video sequence. (b) The same four frames with the subject's pulse signal amplified. (c) A vertical scan line from the input (top) and output (bottom) videos plotted over time shows how our method amplifies the periodic color variation. In the input sequence the signal is imperceptible, but in the magnified sequence the variation is clear.

---

# In Ictu Oculi: Exposing AI Generated Fake Face Videos by Detecting Eye Blinking

Yuezun Li, Ming-Ching Chang and Siwei Lyu  
Computer Science Department, University at Albany, SUNY

---

SEEING IS NOW BELIEVING >

# Image authentication for any situation

Truepic is the leading image authentication platform for anyone looking to verify photos or videos.



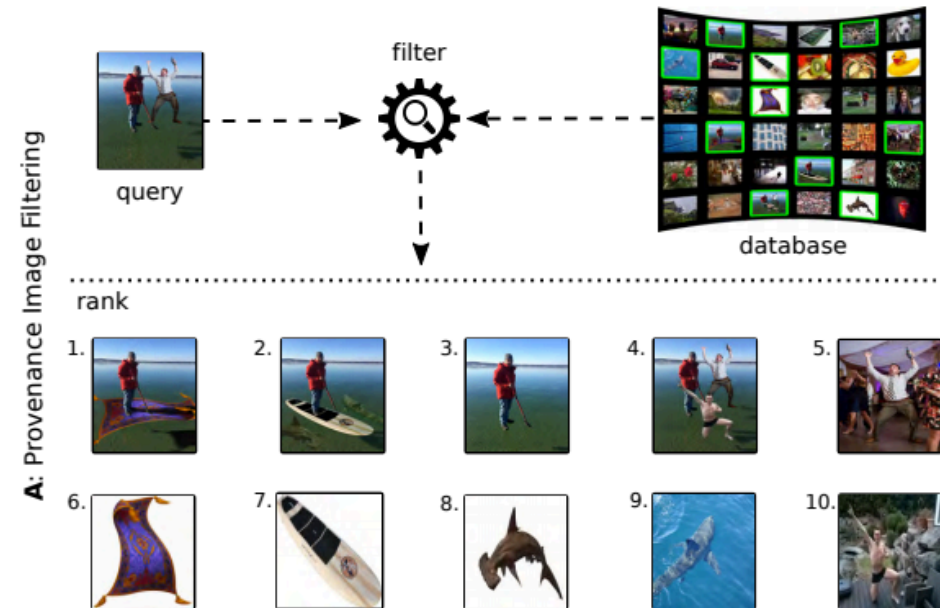
**Proof Mode**  
**Verified Visuals** with **Your Smartphone**



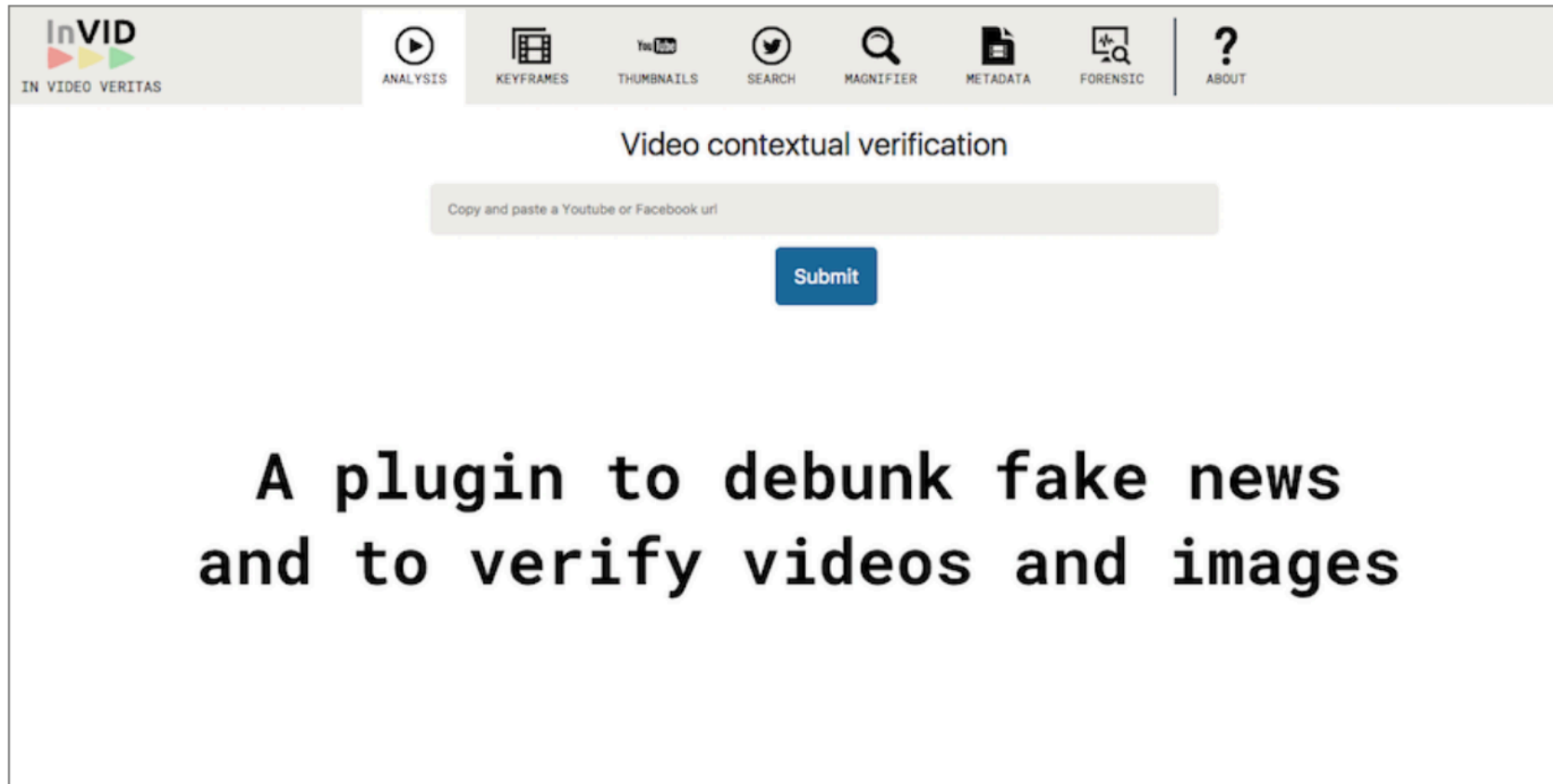
# Image Provenance Analysis at Scale

Daniel Moreira, Aparna Bharati, *Student Member, IEEE*, Joel Brogan, *Student Member, IEEE*,  
Allan Pinto, *Student Member, IEEE*, Michael Parowski, Kevin W. Bowyer, *Fellow, IEEE*,  
Patrick J. Flynn, *Fellow, IEEE*, Anderson Rocha, *Senior Member, IEEE*,  
and Walter J. Scheirer, *Senior Member, IEEE*

**Abstract**—Prior art has shown it is possible to estimate, through image processing and computer vision techniques, the types and parameters of transformations that have been applied to the content of individual images to obtain new images. Given a large corpus of images and a query image, an interesting further step is to retrieve the set of original images whose content is present in the query image, as well as the detailed sequences of transformations that yield the query image given the original images. This is a problem that recently has received the name of image provenance analysis. In these times of public media manipulation (*e.g.*, fake news and meme sharing), obtaining the history of image transformations is relevant for fact checking and authorship verification, among many other applications. This article presents an end-to-end processing pipeline for image provenance analysis, which works at real-world scale. It employs a cutting-edge image filtering solution that is custom tailored for



# InVID Verification Plugin



The screenshot shows the InVID Verification Plugin interface. At the top is a navigation bar with the InVID logo (three colored triangles) and the tagline 'IN VIDEO VERITAS'. To the right of the logo are several icons representing different verification features: ANALYSIS (play button), KEYFRAMES (film strip), THUMBNAILS (YouTube logo), SEARCH (Twitter logo), MAGNIFIER (magnifying glass), METADATA (document icon), FORENSIC (microscope icon), and ABOUT (question mark icon). Below the navigation bar, the text 'Video contextual verification' is centered. Underneath this is a light gray input box with the placeholder text 'Copy and paste a Youtube or Facebook url'. Below the input box is a blue 'Submit' button. At the bottom of the interface, the text 'A plugin to debunk fake news and to verify videos and images' is displayed in a large, bold, black, monospaced font.



Reality Defender is intelligent software built to run alongside digital experiences (such as browsing the web) to detect potentially fake media. Similar to virus protection, it scans every image, video, and other media that a user encounters for known fakes, allows reporting of suspected fakes, and runs new media through various AI-driven analysis techniques to detect signs of alteration or artificial generation.

