Understanding the Provenance of Visual Disinformation Targeting Science

Walter J. Scheirer
Department of Computer Science and Engineering
University of Notre Dame
Public health counter-messaging from an unlikely source

When they're about to give you Coronavirus Vaccine

**THE CORONAVIRUS VACCINE WILL ELIMINATE CORONAVIRUS**

**JUST LIKE THE FLU VACCINE ELIMINATED THE FLU**

**IF YOU BELIEVE ONE WEEK OF THIS IS WORSE THAN THE RISK OF LIVING A LIFETIME WITH THIS, YOU'VE BEEN PHARMED LIKE A SHEEP.**
Memetic warfare

Origin of the bat soup myth: genomic link

Origins of the bat soup myth: the Huanan Seafood Wholesale Market
Origin of the bat soup myth: tabloid news

https://video.foxnews.com/v/6145888115001#sp=show-clips
Origin of the bat soup myth: Twitter disinfo.

Alleged Chinese Delicacy

Banned Anti-CPC Account

Reverse Image Search

Turns up links about Palau and somebody named Wang Mengyun?
Origin of the bat soup myth: Wang Mengyun

Origin of the bat soup myth: Palau

Photo Credit, Elizabeth Warren, Taken in 2012.
https://elizabethinpalau.wordpress.com/2012/05/20/exploring-the-island/
Limitations of determining provenance by hand

- Reverse image search only works well for duplicate and near duplicate images
- Staggering number of memes and source images
  - Every minute: 243,000 images are uploaded to Facebook
  - Every day: 500 million people use Instagram and over two billion users watch or post to YouTube
  - Every year: hundreds of billions of photos are uploaded to social media

S. Aslam, “Facebook by the Numbers: Stats, Demographics & Fun Facts,” Omnicore, 2021
S. Aslam, “Instagram by the Numbers: Stats, Demographics & Fun Facts.” Omnicore, 2021
Watching the meme landscape with AI

- Real-time processing pipeline with content flagging
- Assess meme landscape with respect to events and actors
- Scale to the order of billions of images per day
- Match composite images to other composite and donor images
Automatic Image Provenance Analysis

Provenance Analysis Pipeline

**Provenance Analysis Pipeline**

**Image Filtering**
- Database Indexing
  1. Distributed interest point selection
  2. Optimized product quantization (OPQ)
- Database
- Query
- Image Search
  3. Distributed interest point selection (over query)
  4. Approximate Nearest Neighbors (ANN) analysis
- IF re-query
- IVFADC
- RCMM rank

**Graph Construction**
- MI-based Dissimilarity Calculation
  8. Homography calculation based on GCM
  9. Mutual Information (MI) calculation of warped and color-matched patches
- Pairwise MI dissimilarity matrix
- Clustered Graph Construction
- Provenance graph

**Clustered Graph Construction**
Dynamic Spatial Verification for Large-Scale Object-Level Image Retrieval

How well does it work?

NIST Media Forensics Challenge (https://mfc.nist.gov/)
Order millions of images

<table>
<thead>
<tr>
<th></th>
<th>Recall@200</th>
<th>Node Recall</th>
<th>Link Overlap</th>
<th>Node Overlap</th>
<th>Node + Link Overlap</th>
</tr>
</thead>
<tbody>
<tr>
<td>MFC 2018</td>
<td>0.9</td>
<td>0.798</td>
<td>0.272</td>
<td>0.798</td>
<td>0.543</td>
</tr>
<tr>
<td>MFC 2019</td>
<td>0.819</td>
<td>0.693</td>
<td>0.295</td>
<td>0.703</td>
<td>0.519</td>
</tr>
<tr>
<td>MFC 2020</td>
<td>0.855</td>
<td>0.753</td>
<td>0.250</td>
<td>0.490</td>
<td>0.714</td>
</tr>
</tbody>
</table>
How about the real data?

Images from /r/photoshopbattles

<table>
<thead>
<tr>
<th>Solution</th>
<th>VO</th>
<th>EO</th>
<th>VEO</th>
</tr>
</thead>
<tbody>
<tr>
<td>GCM-SURF [38]</td>
<td>0.884</td>
<td>0.156⁺</td>
<td>0.523⁺</td>
</tr>
<tr>
<td>GCM-MSER</td>
<td>0.924</td>
<td>0.121⁺</td>
<td>0.526⁺</td>
</tr>
<tr>
<td>MI-SURF</td>
<td>0.757</td>
<td>0.037</td>
<td>0.401</td>
</tr>
<tr>
<td>MI-MSER</td>
<td>0.509</td>
<td>0.027</td>
<td>0.271</td>
</tr>
</tbody>
</table>

⁺: Values for undirected edges. In bold, the solution with the best VEO.
A Meme Analysis Engine

Motif Mining
Pipeline for Meme Genre Discovery


Case Study: 2019 Indonesian National Election

Our Approach

44,612 images from a major world event with ground-truth clusters
Unusual findings over 2 million images

A variety of messaging. Not all of it disinformation!

Advertising regularly piggybacks on significant events like elections.
Bogus Medical Supplements

- “Super Grow Up” supplement
- Promises to increase the height of adults taking it
  - Only works under the age of 40
- Website went offline in early 2020

https://www.facebook.com/Super-Grow-Up-107002714187108/
Who else is selling bogus supplements using elections as a vehicle?

https://thecounter.org/would-you-buy-supplements-from-alex-jones/
Coronavirus? There’s a cheap cure for that too...

Outstanding Challenges

Scalability

Video Processing

Graph Building

Usability for Analysts
Questions?