From single object to contextual authentication: A new challenge in multimedia forensics and beyond

Mauro Barni
University of Siena
CNIT
Outline

• Motivation
• Multimedia forensics
• Hottest challenges
• Contextual authentication
  – Motivation
  – A general framework
  – An early attempts based on image phylogeny
• Conclusions
Seeing is believing. Does it?

Photographic images have lost their innocence (if they ever had one) a long time ago.
Seeing is believing. Does it?
Seeing is believing. Does it?
Seeing is believing. Does it?

With digital photography (and videos and audios) the diffusion of fake images has bloomed.

Fake images are virtually everywhere
Gutter press

Frontal light

Side illumination
Military propaganda
Anti-regime propaganda
Even scientists
Not only photomontages

CG    CG    Real    CG    Real

CG    Real    CG    Real    Real
Not only images
Why should we care?

- Probatory value of digital images, videos, audios
- Opinion manipulation
- Social impact: undermines one of our primary source of information
- Problem worsened by diffusion of UGC paradigm

Scientific question: ultimate reliability of digital media as trustful representation of reality
Multimedia forensics

• Multimedia forensics aims at gathering information about the history of images, video and audio contents

• Basic idea: each step image life leaves peculiar traces that can be exploited to detect its presence
Digital image life cycle

Real word -> Lenses -> Optical filter -> CFA pattern -> Sensor

CCD/CMOS -> Color interpolation

In-camera software processing (white balancing; contrast; saturation; etc)

Digital image -> Out-camera processing -> Final digital image
A rich forensic toolbox

- PRNU analysis for device identification
- CFA analysis for model identification
- Double JPEG compression to retrieve image history
Double JPEG for cut & paste detection

- JPEG compression introduces blocking artifacts on an 8x8 grid
- In the case of double JPEG compression the old traces of blocking artifact are not aligned with the new compression grid
A rich forensic toolbox

- PRNU analysis for device identification
- CFA analysis for model identification
- Double JPEG compression to retrieve image history
- Resampling traces to detect cat and paste with resizing
- SIFT matching for copy-move detection
- Geometric inconsistencies
  - Shadows
  - Lights
  - Perspective
  - Motion
- ...
All that glitters ain't gold

• From the lab to real world
  – Lack of good statistical models
  – Multi-clue forensics analysis

• Counter-forensics
  – What if ...
  – Counter-counter-forensics
  – Adversarial MMF

• There’s more to authenticity than single object analysis: Contextual authentication
The importance of context (1)

• Truthfulness of multimedia contents does not depend on the content only
• The context wherein the content is used must be considered as well
• Together with its intended meaning
The importance of context
The importance of context

In the image, a group of television news organizations set up their equipment on an empty airport runway, preparing to broadcast a significant event. This scene highlights the importance of context in understanding the impact of technology and news media on public perception and behavior. The presence of multiple news outlets suggests a high level of significance associated with the event, possibly indicating a major news story or a significant global event. The context here includes the media's role in shaping public opinion and the rapid dissemination of information in today's fast-paced news cycles.
The importance of context
The importance of context

Yet, the image is authentic

Or to better say ... it has not been manipulated
The importance of context (2)

- Images do not live in isolation
- The web (and not only) forms a kind of collective background knowledge
- Image content can be checked against such a background knowledge

- Image with Bin Laden face after death
A less critical example
A framework for contextual authentication

• Foreground Context (FC): the context – document, webpage, text – wherein the content is used
  – Explicit assumptions
  – Implicit assumptions

• Background context (BC): pre-existing information about the analyzed content and the foreground context wherein the content is used

• Contextual authentication: verification of explicit and implicit assumptions deriving from the FC, by the light of content analysis and BC
Information from different sources

- Single object MM forensics
  - Information from content

  Rich features

  Contextual authentication
  - Build background context
  - Check assumptions from FC

  Background Information from the web

  Web mining and retrieval
  - Information from the web

  Semantic knowledge

  Social computing - crowdsourcing
  - Information from people
Several challenges

• Information from content
  – Strengthen forensics analysis to exit the lab
  – Multiple object, multimodal analysis

• Information from the web
  – Content-based retrieval
  – Big-data scenario

• Information from people:
  – Efficient use of social resources
  – Effective engagement of people
  – Interaction with automatic components
Several challenges

• Foreground Context definition
  – Derive all implicit and explicit assumptions linked to the foreground context
  – Bring the analysis to a sufficiently high semantic level

• Background context
  – Definition of proper models
  – Semantic analysis
  – Data deluge
Image phylogeny: a first small step

Image phylogeny: a first small step
More formally

- **Foreground Context assumption**
  - The image content has not been manipulated
  - that is: the objects and people shown in the picture correspond to the real world scene the picture refers to
  - that is: no copy-move, no photo-montage
Information from the web

- Background information from the web is limited to the collection of near duplicate images
- A search for near duplicates is run
Information from people

- Suspect objects are identified through crowdsourcing (very limited amount of semantic information)
Alternatively: information from content

• A conventional single image forensic analysis could be run to identify suspect areas

• Change detection techniques could also be used to identify possibly tampered areas
Information from the web (again)

- A web search is carried out looking for near duplicates of suspect regions
Background context model

- The model for background context corresponds to an image phylogeny graph with multiple parents.
Construction of the graph (1/3)

- Evaluate the dis-similarity between each pair of images
  \[
d(I_A \rightarrow I_B) = \min_{T \in C}[dist(I_B, T(I_A))]
  \]

- Evaluate the similarity between random part of images
  \[
  I = [I_C, I_R], \quad \text{e.g. } I_R = I - \text{denoise}(I)
  \]
  \[
  sim(I_A \rightarrow I_B) = corr(I_A, R, T(I_B)R)
  \]
  \[
  T = \arg\min_{T \in C}[dist(I_B, C, T(I_A, C))]
  \]
  \[
  sim(I_A \rightarrow I_B) = corr(I_A, R, T(I_B)R)
  \]
Construction of the graph (2/3)

• Given the dissimilarity matrix build a Image Phylogeny Forest

<table>
<thead>
<tr>
<th></th>
<th>I_1</th>
<th>I_2</th>
<th>I_3</th>
<th>I_4</th>
</tr>
</thead>
<tbody>
<tr>
<td>I_1</td>
<td>-</td>
<td>1.81</td>
<td>2.98</td>
<td>3.85</td>
</tr>
<tr>
<td>I_2</td>
<td>2.71</td>
<td>-</td>
<td>1.88</td>
<td>2.74</td>
</tr>
<tr>
<td>I_3</td>
<td>3.98</td>
<td>2.56</td>
<td>-</td>
<td>2.50</td>
</tr>
<tr>
<td>I_4</td>
<td>22.43</td>
<td>19.62</td>
<td>19.44</td>
<td>-</td>
</tr>
</tbody>
</table>

• Minimum spanning tree (Kruskal, optimum branching)
• Tree clustering based on edge weights variance thresholding
Construction of the graph (3/3)

- Identification of multiple parents and FC assumption verification
Construction of the graph (3/3)

- Focus on root of to-be-authenticated image tree: for all the other trees look for original background image

Similarity check (possibly on random part only)

Is background host?
Construction of the graph (3/3)

• Focus on root of to-be-authenticated image tree: for all the other trees look for original suspect region

Is suspect region host?

Similarity check (possibly on random part only)
Example

Suspect image is not authentic, since it does not satisfy the FC assumption by the light of BC information.
Discussion: an over-over-simplified case

• Trivial FC assumption
• Simple model for background context
  – Yet it gives richer information than needed
• Low semantic level
• Very simply composition
  – Only one copied-region
  – Assume search is nearly perfect
  – Assume thresholds always work
• Very high complexity
  – Does not scale to big data
• It shows potentiality (and challenges) of multiple-object contextual investigation
Conclusions

• Diffusion of MM content and popularity of UGC paradigm
• Importance of web for information exchange, collective awareness, opinion formation
• Increasing pervasiveness of social networks

Call for

• Means to authenticate MM contents (and not only) by taking into account the digital ecosystem wherein the contents are produced, used and diffused
Conclusions

• Multimedia forensics represents a first partial answer

• Several challenges ahead of MMF
  – Application in realistic environments
  – Multiclue analysis
  – Adversarial version of the problem
  – Contextual authentication

• MM forensics, web mining, content-based retrieval, social computing: synergistic effort to reach the next level of web dependability
Credits

- VIPP group: http://clem.dii.unisi.it/~vipp/
- University of Siena - CNIT
- US air force (EOARD)
  - AMULET

- European Projects:
  - REWIND: http://www.rewindproject.eu
  - REVerse engineering of audio-VIual coNTent Data
  - maven: http://www.maven-project.eu
  - Management and Authenticity Verification of multimedia contENts
Thank you for your attention