Open Problems in Multimedia Forensics

Rimba Whidiana Ciptasari
School of Computing, Telkom University
2015
#1: COPY-MOVE FORGERIES
Overview

Given any two regions in an image, it is a simple matter to determine how similar they are using any standard measure of image similarity (e.g., root mean square distance). Searching all possible pairs of regions and region sizes in even a modest-sized image, however, is computationally intractable. In addition, changes in geometry or color of the cloned region further increases the complexity of the search. The complexity of the search for cloned photo with cloning (top) regions can be reduced by operating on salient image features, as and the original photo opposed to pixels.

A common form of photo manipulation is to copy and paste portions of an image to replicate an object or conceal a person in a scene, Figure 1. The presence of identical (or virtually identical) regions in an image can, therefore, be used as evidence of tampering [1].

Figure 1. An altered photo with cloning (top) and the original photo (bottom)
Existing schemes: Exposing duplicated region

Several general techniques applied to detect geometric transformations is subjected to **duplicated regions**.

Existing schemes: Exposing duplicated region

Identify the region that has undergone geometric distortions as well as their parameters (rotation degree, scaling factor).
References:


#2: EXPOSING BLENDING ARTIFACTS BASED ON INCONSISTENCY SHADOW, LIGHTING, PRINCIPAL POINT, RESAMPLING PARAMETERS, & OTHERS
To create convincing photograph forgeries, it is often necessary to re-size, rotate, or stretch portions of the images.

Such manipulations can be investigated either from statistical or camera-based parameters. Estimating these parameters and finding the differences of estimated parameters can be used as evidence of tampering.
### Existing schemes: Estimation/Case based

- **Estimation-based technique**
  - E.g., Popescu and Farid (2005): exploited expectation/maximization (EM) algorithm to **detect re-sampling's lattice** of the original image.
  - **Accuracy** greater than 97%, false positive less than 1%
  - **Disadvantage**: still, no tampering evidence for verification purpose.

#### What case

<table>
<thead>
<tr>
<th></th>
<th>x1</th>
<th>x2</th>
<th>x3</th>
<th>x4</th>
</tr>
</thead>
<tbody>
<tr>
<td>x1</td>
<td></td>
<td>x2</td>
<td></td>
<td>x4</td>
</tr>
<tr>
<td>x3</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>y1</td>
<td>y2</td>
<td>y3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>y4</td>
<td>y5</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>y7</td>
<td>y7</td>
<td>y9</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

\[
y_2 = 0.5y_1 + 0.5y_3
\]
\[
y_4 = 0.5y_1 + 0.5y_7
\]
\[
y_6 = 0.25y_1 + 0.25y_3 + 0.25y_7 + 0.25y_9
\]

JPEG compression
Resampling
Lighting
Cloning etc.

Up-sampling a 2-D image

Estimate a set of periodic samples to their neighbors

A labeled image, e.g., re-sampled

Up-sampled by 15% and then rotated by 5°
Existing schemes: Estimation/Case based

Kee et al. (2013): Combined multiple constraints from cast and attached shadows to constrain the projected location of a point light source.

O’Brien & Farid (2012): Investigated geometric inconsistencies that arise when fake reflections are inserted into a photograph.
Exploring **image blending** process and then investigate/estimate their parameters as tampering evidence.

Exploiting **probabilistic model** to identify the digital forgeries.
Another approach: Machine-learning based

- Machine learning framework
  - Chen et al. (2007), Sutthiwan et al. (2011) \(\rightarrow\) employed SVM to train image features.

- Accuracy:
  - Sutthiwan et al.: 80%
  - Chen et al.: 82%

- Disadvantage:
  - No digital tampering evidence provided for verification.
Existing schemes: Machine-learning based

- **Farid & Lyu (2003):** built a classification scheme to differentiate between natural and tampered images by computing the higher-order wavelet statistics of images.

- **Ng et al. (2004):** improved the performance of bicoherence features of (Farid, 1999) to detect image splicing.

- **Avcibas et al. (2004):** constructed a classifier by employing image quality metrics as essential features.

- **Hsu et al. (2006):** to identify the suspicious splicing areas, they computed the geometry invariants from the pixels and estimated the CRF (camera response function).

- **Dong et al. (2009):** analyzed the spliced artifact on image run-length representation and edge statistics.
References


#3: EXPLOITING REFERENCE IMAGES (TARGETED OR BLIND) FOR EXPOSING TAMPERING ARTIFACTS
Motivation: Inspired by the real situation

Criminal acts, e.g. terrorism. To confirm the authenticity, the officer may need other related images to the suspected person.

Examples of target images

Existing schemes: Multi-images forensics

All the instruments developed so far focus on the analysis of single image.

Proposed a formalization of the relationships between a group of images, and present a simple system for the detection of the dependencies between a set of images sharing similar or identical contents.

Existing schemes: Multi-images forensics

An overview of the general architecture of the system to understand whether $I_B$ could have been generated from $I_A$.

$R_{estim}$ indicates the registration process performed on image contents to estimate the best parameters of $\phi_g$.

$R_{app}$ applies such transformation to $[\phi_j(\phi_c(I_A))]_R$.

$\rho$ computes the correlation coefficient between the registered randomness and $[I_B]_R$.

$T$ indicates the comparison of $\rho$ against the decision threshold.
Existing scheme: Exploiting reference images

Suspect image, $x$

sets of processing functions

References, $R$

process $\in P$

Decide whether $x \subset R$


Open problem: Understanding Geometrical Distortions through Reference Images

It is required an appropriate method to construct features that are invariant and/or sensitive to rotation, translation, and scaling.

The trace transform offers the option to construct features from an image with desirable properties.
Exploiting **probabilistic model** to identify the digital forgeries through blind reference images.

Exploiting **semantic forensics** to expose digital through targeted reference images.
#4: ACTIVE APPROACH FORENSICS: IMAGE TARGETED-STEGRANALYSIS
**Steganalysis** is the art of discovering hidden data in cover objects.

As in cryptanalysis, it is assumed that the steganographic method is publicly known with the exception of a secret key.

The method is secure if the stego-images do not contain any detectable artifacts due to message embedding. (*)

Steganalysis general system

- Secret message, $x$
- Cover image, $I$
- Process $\in P$ (F5, HUGO, LSB, etc)
- Stego image, $I'$
- Message length
- Decide whether $I'$ contains $P$ parameter(s)
- Analyze & estimate steganographic parameter(s)
Challenge issue

Targeted & Blind Steganalysis: to uncover steganography parameters from known methods, such as F5, Jsteg, HUGO, & LSB as well as unknown methods using probabilistic model.
References


#5 SINGLE AUTHENTICATION: EXPOSING TAMPERING ARTIFACTS OF SPLINED IMAGE
Weighted Average Splining

Parameter estimation of weighted average splining

\[ F(i) = W_l(i)F_l(i) + W_r(i)F_r(i) \]
Proposed idea: transition zone modeling

Construct model of these transition zones

By exposing the weighting function model, it can be used as evidence of digital tampering

Predicted weighting coefficients

<table>
<thead>
<tr>
<th>1</th>
<th>1</th>
<th>0.900826</th>
<th>0.887931</th>
<th>0.876812</th>
<th>0.864516</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>0.897638</td>
<td>0.889655</td>
<td>0.873418</td>
<td>0.863946</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>0.902778</td>
<td>0.886076</td>
<td>0.876712</td>
<td>0.859155</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>0.89726</td>
<td>0.889706</td>
<td>0.87218</td>
<td>0.858209</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>0.9</td>
<td>0.889706</td>
<td>0.871212</td>
<td>0.861538</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>0.896825</td>
<td>0.890625</td>
<td>0.874016</td>
<td>0.865079</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>0.901515</td>
<td>0.883721</td>
<td>0.873016</td>
<td>0.864</td>
</tr>
</tbody>
</table>
RESEARCH ROADMAP
2014 - 2015
• Exposing geometrical distortion by exploiting probabilistic model (blind references)

2016 - 2018
• Single authentication: Exposing Tampering Artifacts of Splined Image

2018 - 2019
• Semantic forensics: Exploiting Targeted References In Exposing Geometrical Distortions

2019 - 2021
• Multimedia forensics over active approaches: targeted and blind steganalysis

2020
• Exploring Counter-forensics
• Writing book reference
• Forensics tool design (integration & deployment)
Welcome for discussion

Contact:
rimbawh@telkomuniversity.ac.id
rimbawh@gmail.com