Open Problems in Multimedia Forensics

Rimba Whidiana Ciptasari

School of Computing, Telkom University

2015

#1: COPY-MOVE FORGERIES

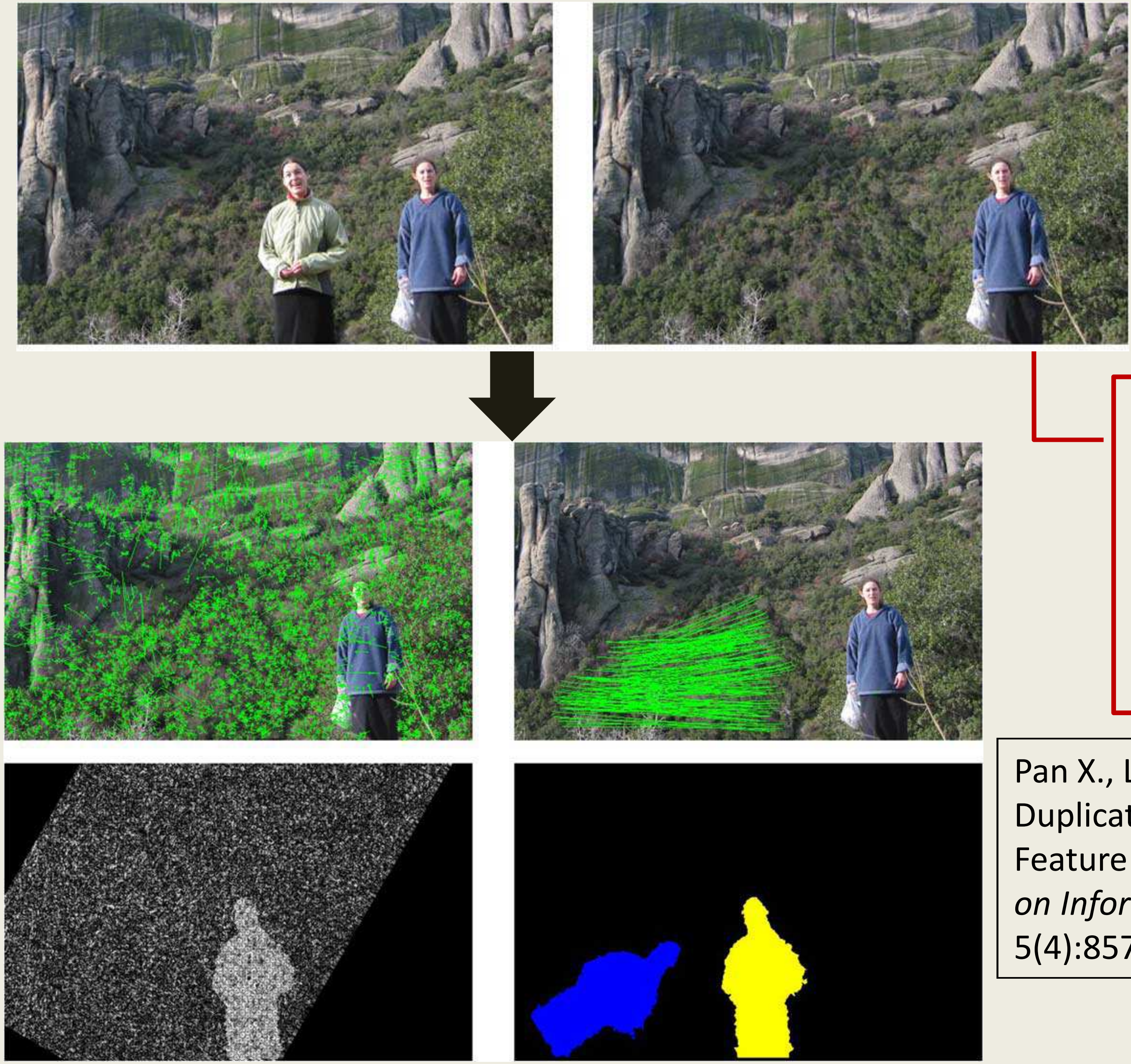
Overview

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

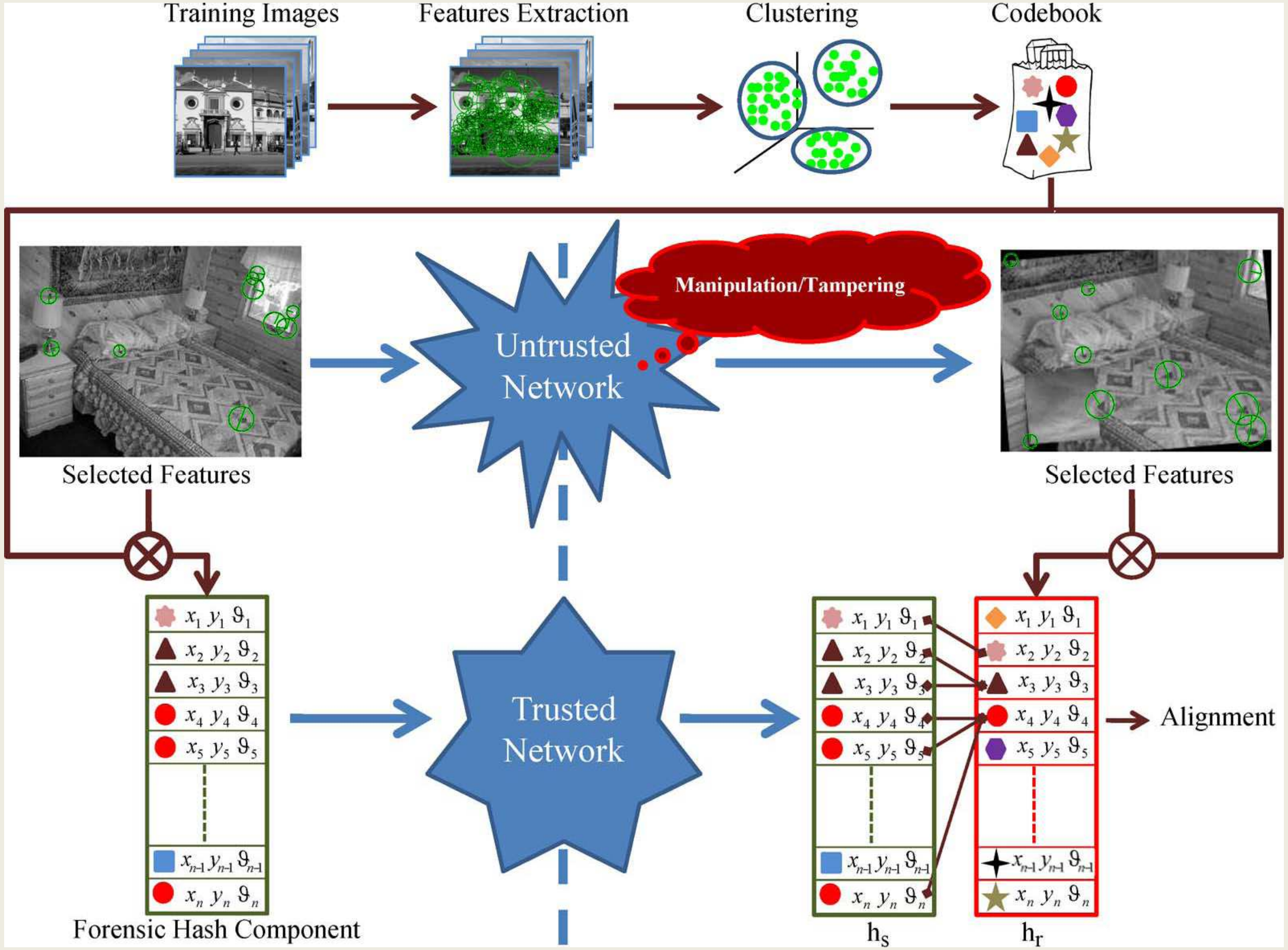


Several general techniques applied to detect geometric transformations is subjected to **duplicated regions**.

Pan X., Lyu S.(2010) "Region Duplication Detection using Image Feature Matching", *IEEE Transaction on Information Forensics and Security*, 5(4):857-867.

Existing schemes: Exposing duplicated region

Battiato S., Farinella G.M., Messina E., Puglisi G.(2012) “Robust Image Alignment for Tampering Detection”, *IEEE transaction on Information Forensics and Security*, volume 7, issue 4, pp. 1105 - 1117.



Challenge issue

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

References:

- Pan, X., and Lyu,S., ”Region Duplication Detection using Image FeatureMatching,” In: IEEE Transaction on Information Forensics and Security, 5(4):857-867, 2010.
- Ryu S.J., Lee M.J., Lee H.K., ”Detection of Copy-Rotate-Move Forgery Using Zernike Moments,” In: Information Hiding Lecture Notes in Computer Science, Volume 6387, pp. 51-65, 2010.
- Solorio S.B., Nandi A.K., ”Automated detection and localisation of duplicated re- gions affected by reflection,rotation and scaling in image forensics,” In: Signal Pro- cessing, Elsevier, pp.1759-1770, 2011.
- Amerini I, Ballan L, Caldelli R, Del Bimbo A, Serra G., ”A SIFT-Based Forensic Method for Copy-Move Attack Detection and Transformation Recovery,” In: IEEE transaction on Information Forensics and Security, Volume 6, issue 3, pp. 1099 -1110, 2011.
- Battiato S., Farinella G.M., Messina E., Puglisi G., ”Robust Image Alignment for Tampering Detection,” In: IEEE transaction on Information Forensics and Secu- rity, volume 7, issue 4, pp. 1105 - 1117, 2012.
- Kakar P., Sudha N., ”Exposing Postprocessed Copy-Paste Forgeries through Transform-Invariant Features,” In: IEEE Transaction on Information Forensics and Security, Vol.7 Issue 3, pp.1018-1028, 2012.

#2: EXPOSING BLENDING ARTIFACTS BASED ON INCONSISTENCY SHADOW, LIGHTING, PRINCIPAL POINT, RESAMPLING PARAMETERS, & OTHERS

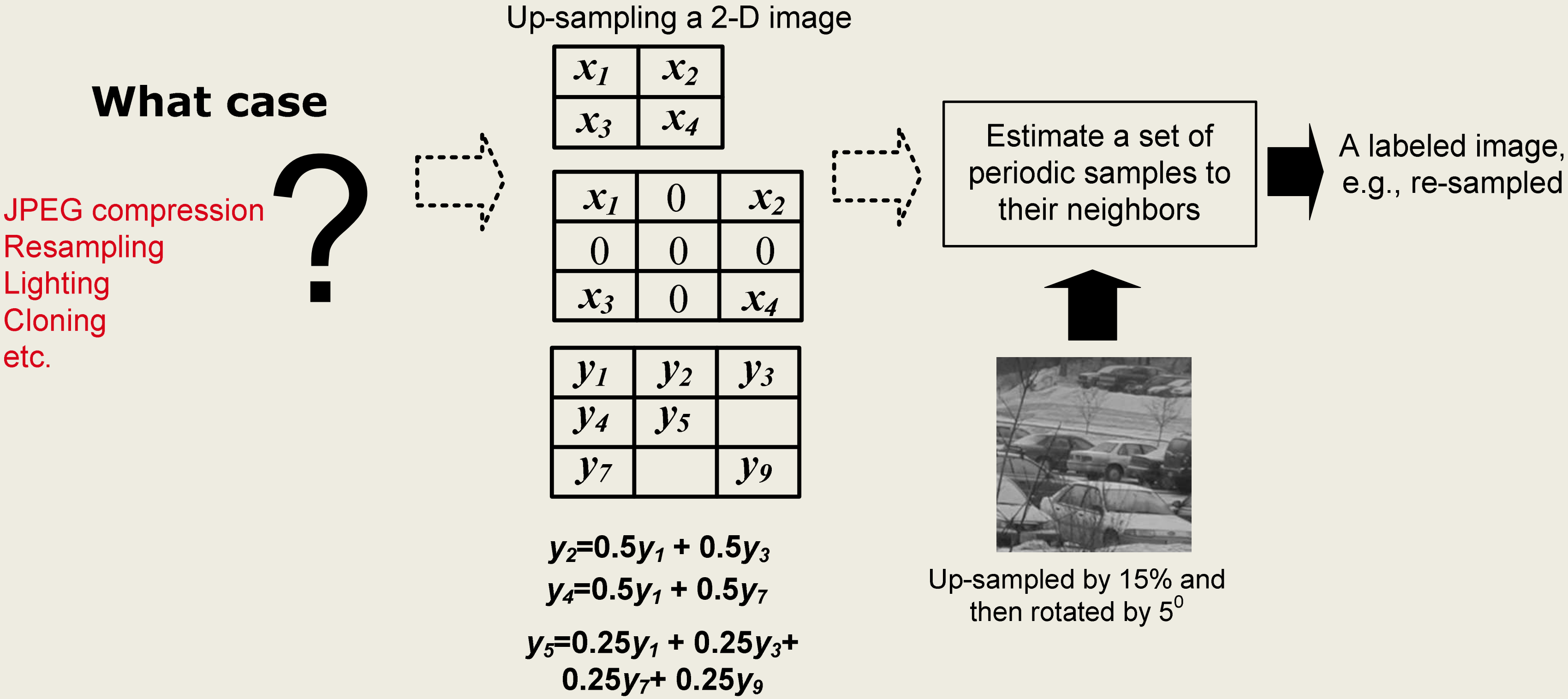
Overview

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

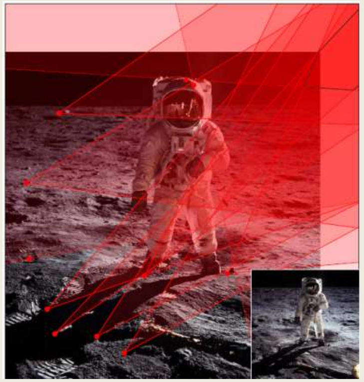
- Estimation-based technique
  - E.g., Popescu and Farid (2005): exploited expectation/maximization (EM) algorithm to **detect re-sampling's lattice** of the original image.



  - Accuracy greater than 97%, false positive less than 1%
  - **Disadvantage**: still, no tampering evidence for verification purpose.

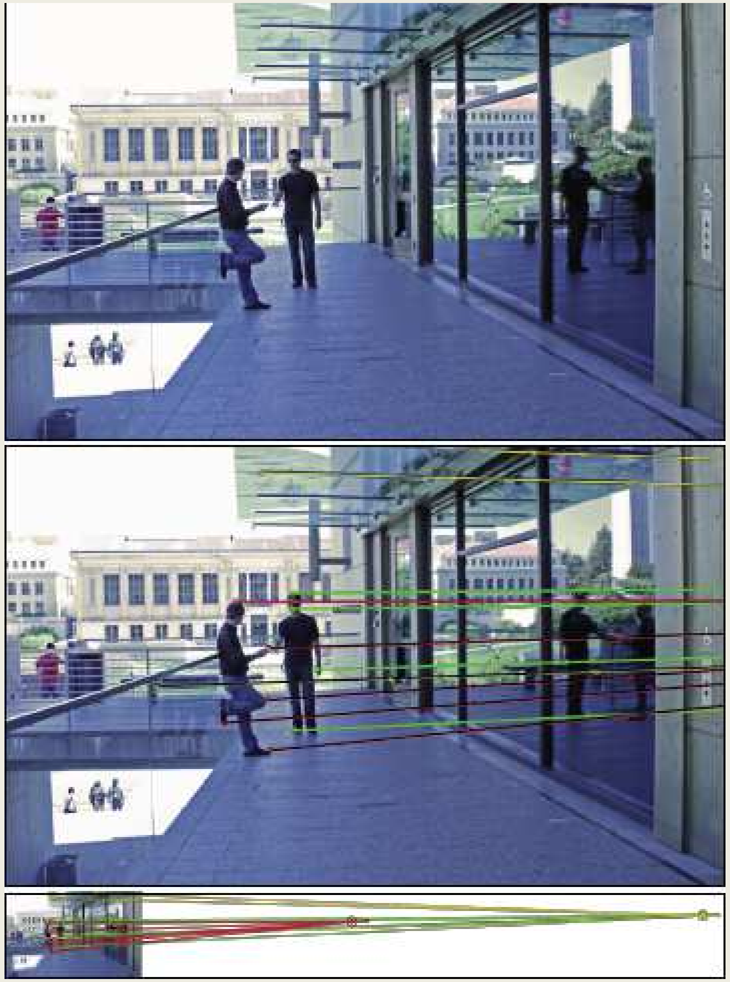
Existing schemes: Estimation/Case based

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



©NASA 1969

O'Brien & Farid (2012): Investigated geometric inconsistencies that arise when fake reflections are inserted into a photograph.



© O'Brien & Farid

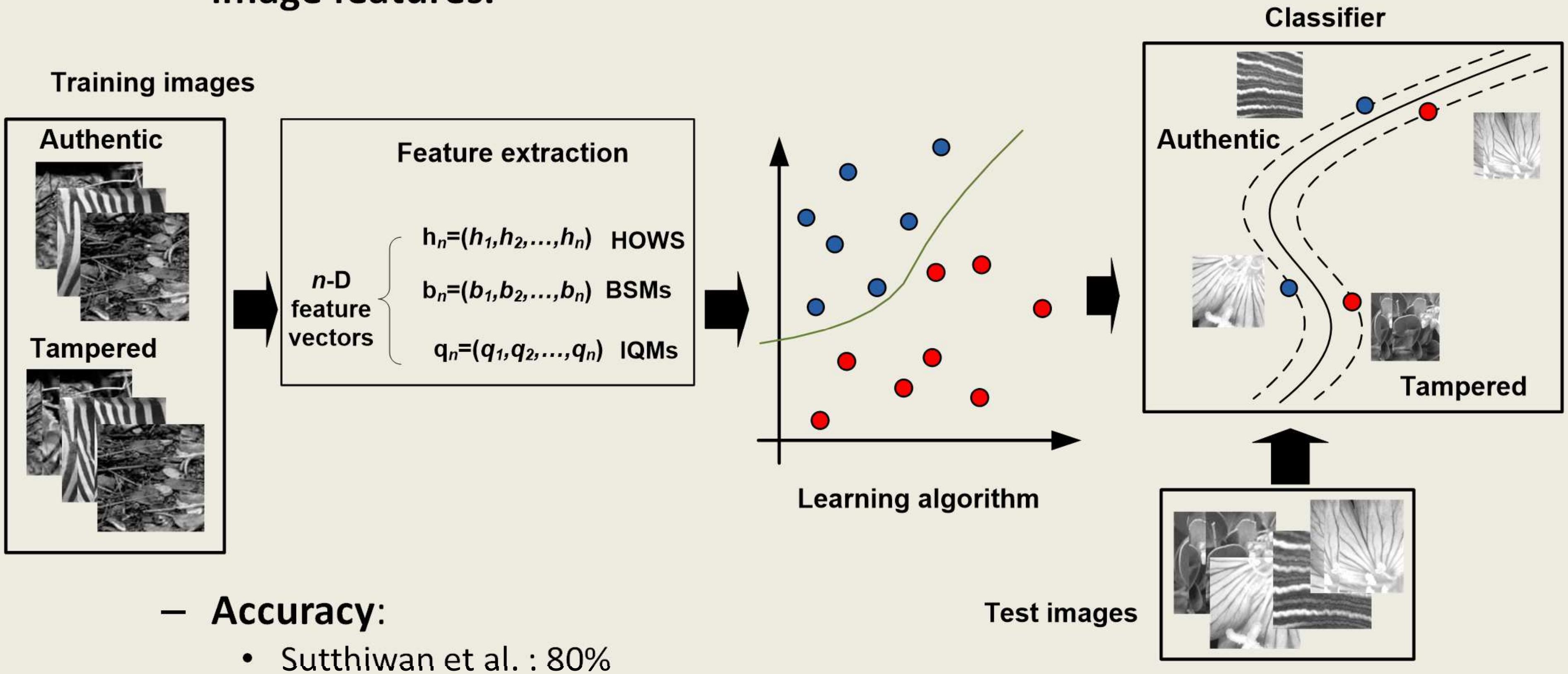
Challenge issue

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) → **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

- E. Kee and H. Farid. Digital image authentication from thumbnails. In SPIE Symposium on Electronic Imaging, San Jose, CA, 2010.

- M. Kirchner and T. Gloe. On resampling detection in re-compressed images. In IEEEWorkshop on Information Forensics and Security, pages 21-25, 2009.

- A.C. Popescu and H. Farid. Exposing digital forgeries by detecting traces of re-sampling. IEEE Transactions on Signal Processing, 53(2):758-767, 2005.

#3: EXPLOITING REFERENCE IMAGES (TARGETED OR BLIND) FOR EXPOSING TAMPERING ARTIFACTS

Motivation: Inspired by the real situation

Examples of target images

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

Image source: http://www.fourandsix.com/photo-tampering-history/.

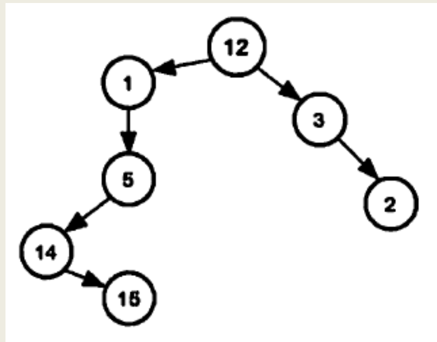
Existing schemes: Multi-images forensics

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

→ SYSTEM → Authentic/ Unauthentic (?)

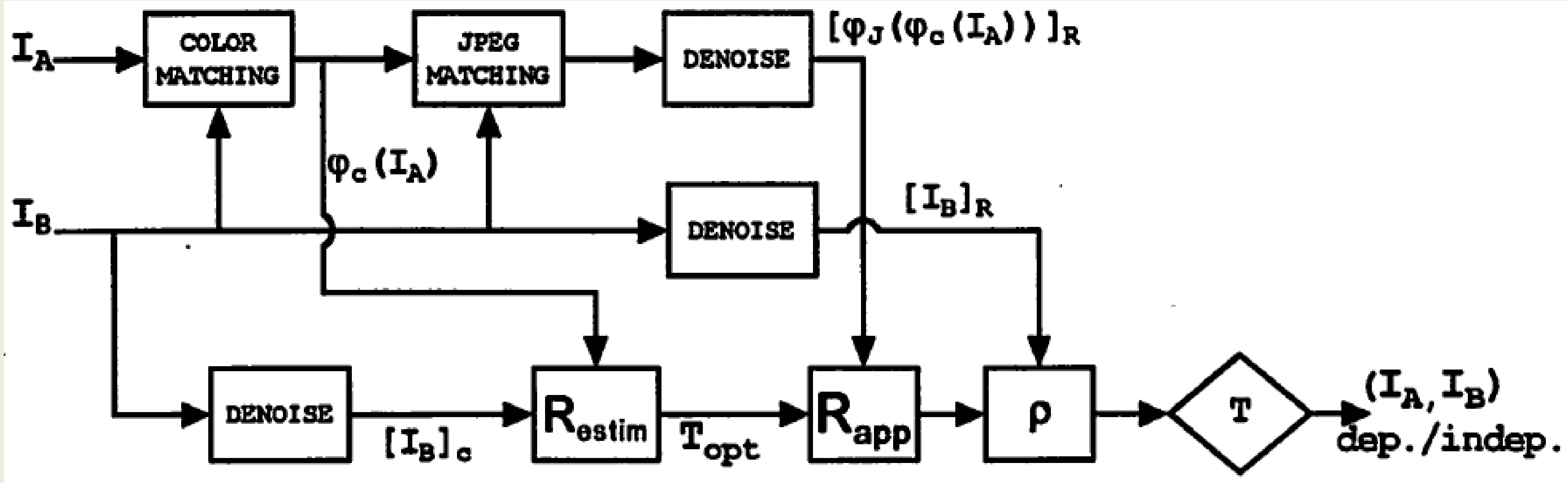
Proposed a formalization of the relationships between a group of images, and present a simple system for the detection of the dependencies between a set of images sharing similar or identical contents.

→ SYSTEM →



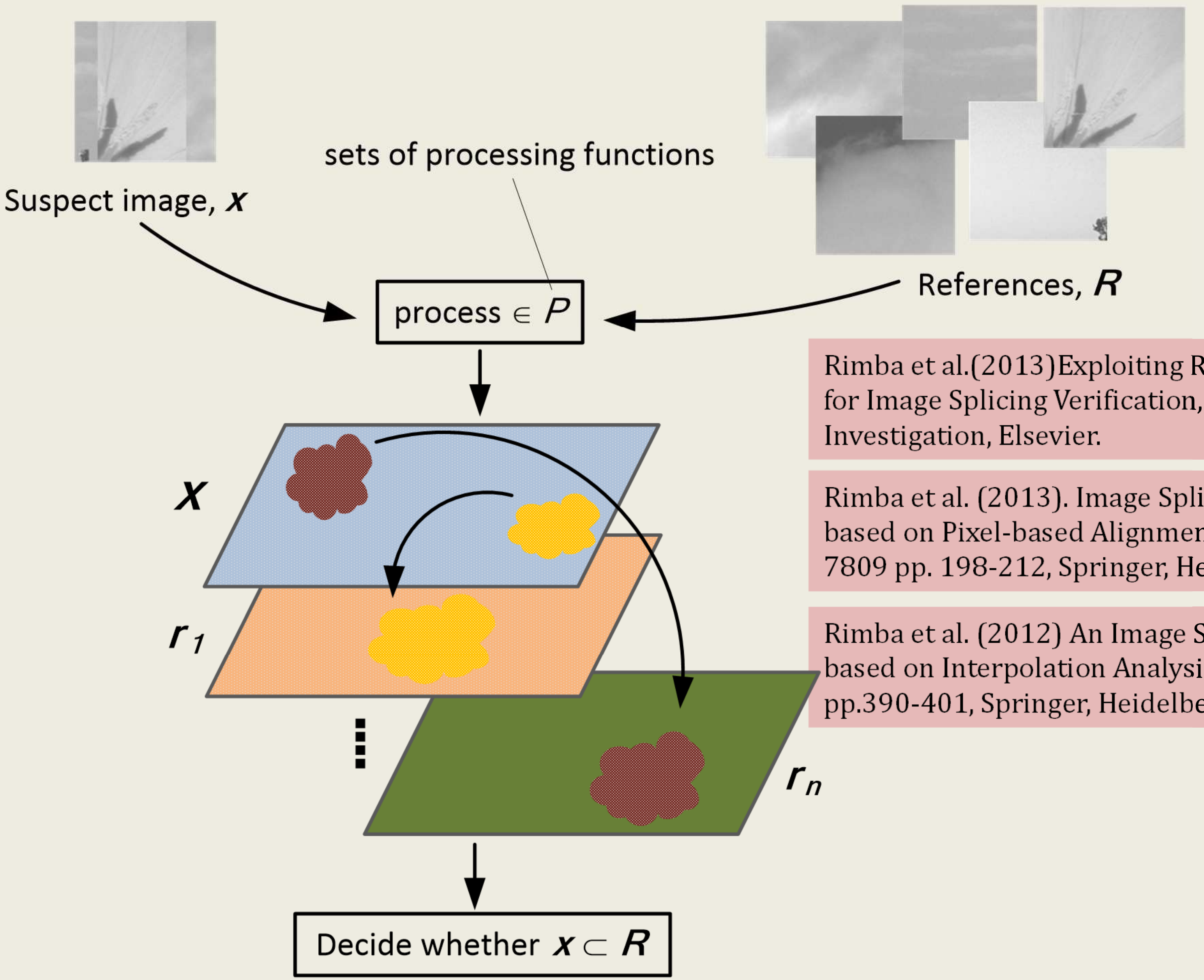
Rosa A D, Uccheddu F, Costanzo A, Piva A and Barni M (2010): Exploring image dependencies: a new challenge in image forensics. In: Proc. of SPIE-IS&T Electronic Imageing, SPIE Vol. 7541.

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 ϕ_g.
R_{app} applies such transformation to $[\phi_J(\phi_c(I_A))]_R$.
ρ computes the correlation coefficient between the registered randomness and $[I_B]_R$.
T indicates the comparison of ρ against the decision threshold.

Existing scheme: Exploiting reference images

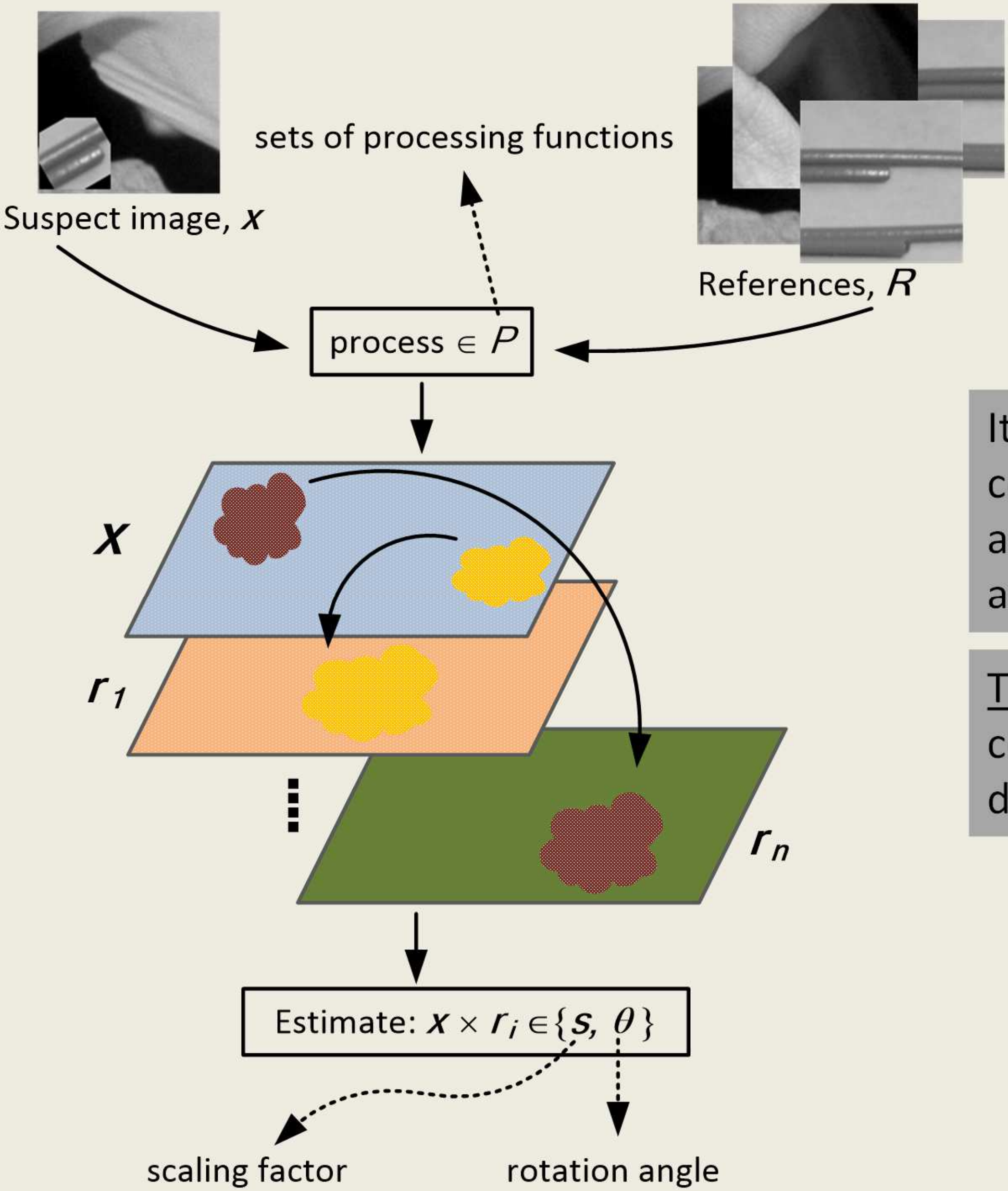


Rimba et al.(2013)Exploiting Reference Images for Image Splicing Verification, Digital Investigation, Elsevier.

Rimba et al. (2013). Image Splicing Verification based on Pixel-based Alignment Method, LNCS 7809 pp. 198-212, Springer, Heidelberg.

Rimba et al. (2012) An Image Splicing Detection based on Interpolation Analysis, LNCS 7674, pp.390-401, Springer, Heidelberg.

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.

Challenge issues

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-STEGANALYSIS

Definition

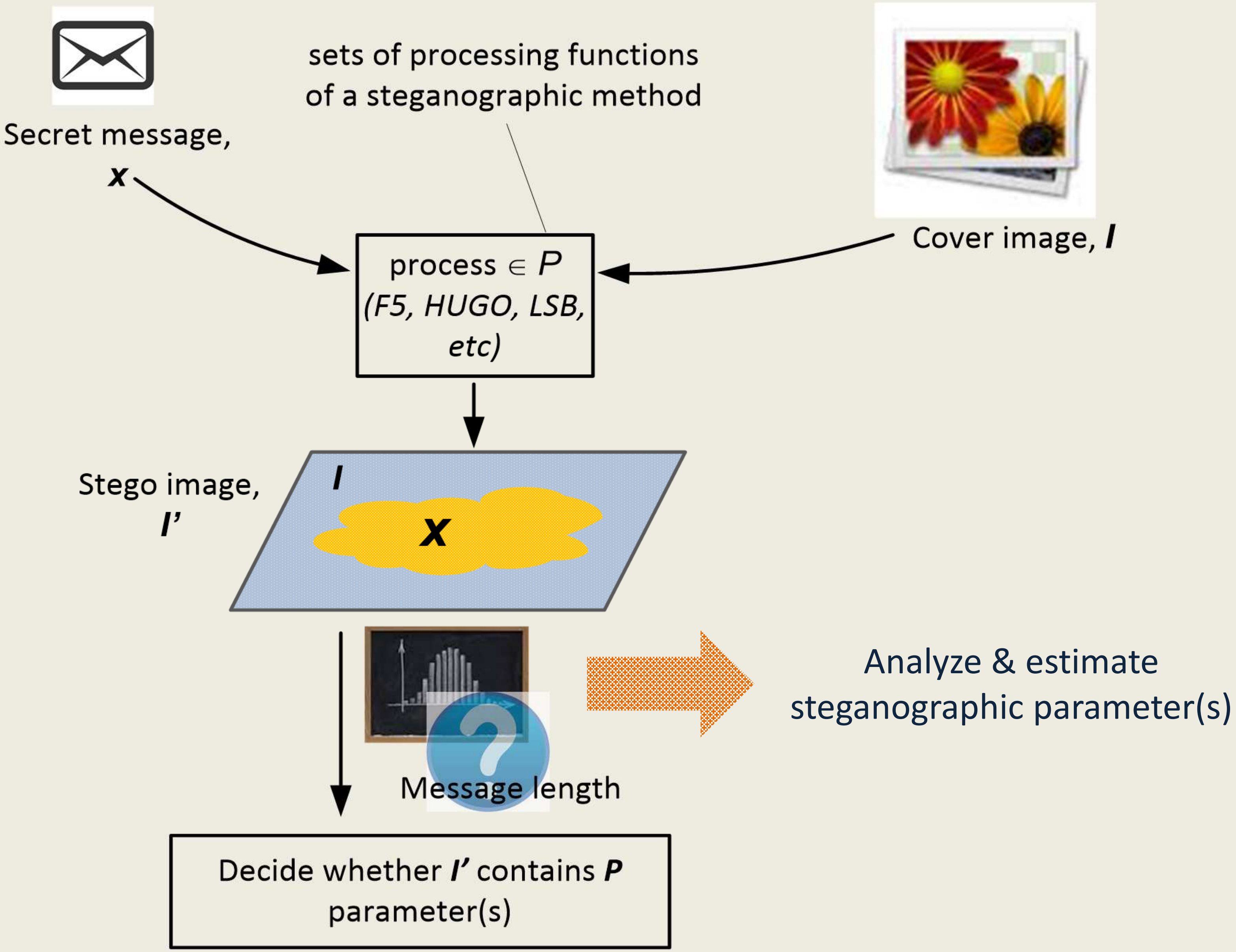
Steganalysis is the art of discovering hidden data in cover objects.

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.*)

*) Fridrich J, Goljan M, Hogea D. *Steganalysis of JPEG Images: Breaking the F5 Algorithm.* International Conference on Information Hiding. LNCS Springer vol. 2578, 2003, pp. 310 – 323.

Steganalysis general system



Challenge issue

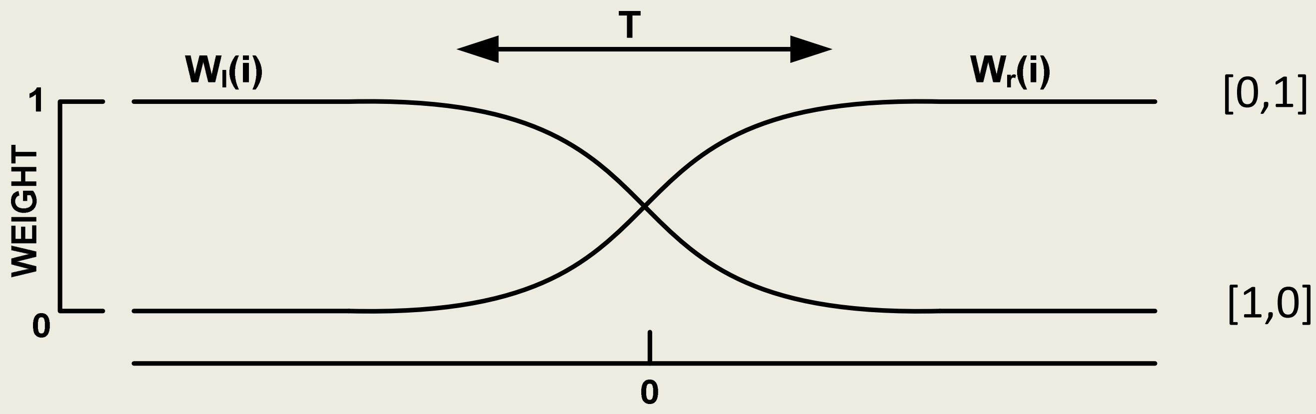
Targeted & Blind Steganalysis: to uncover steganography parameters from known methods, such as F5, Jsteg, HUGO, & LSB as well as unknown methods using probabilistic model.

References

- Chandramouli, R. and Memon, N.: Analysis of LSB Based Image Steganography Techniques. Proceedings of ICIP 2001
- Fridrich, J., Goljan, M., and Du, R.: Reliable Detection of LSB Steganography in Grayscale and Color Images. Proc. of ACM: Special Session on Multimedia Security and Watermarking. Ottawa, Canada (2001) 27–30
- Fridrich, J., Goljan, M., and Du, R.: Detecting LSB Steganography in Color and Grayscale Images. Magazine of IEEE Multimedia: Special Issue on Security, Vol. Oct-Dec (2001) 22– 28
- Fridrich, J., Goljan, M., and Du, R.: Steganalysis Based on JPEG Compatibility. Proc. SPIE Multimedia Systems and Applications IV, Vol. 4518. Denver, Colorado (2001) 275–280

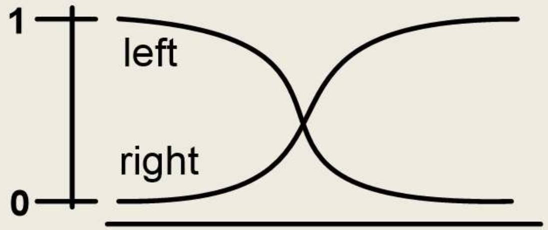
#5 SINGLE AUTHENTICATION:
EXPOSING TAMPERING ARTIFACTS OF SPLINED IMAGE

Weighted Average Splining

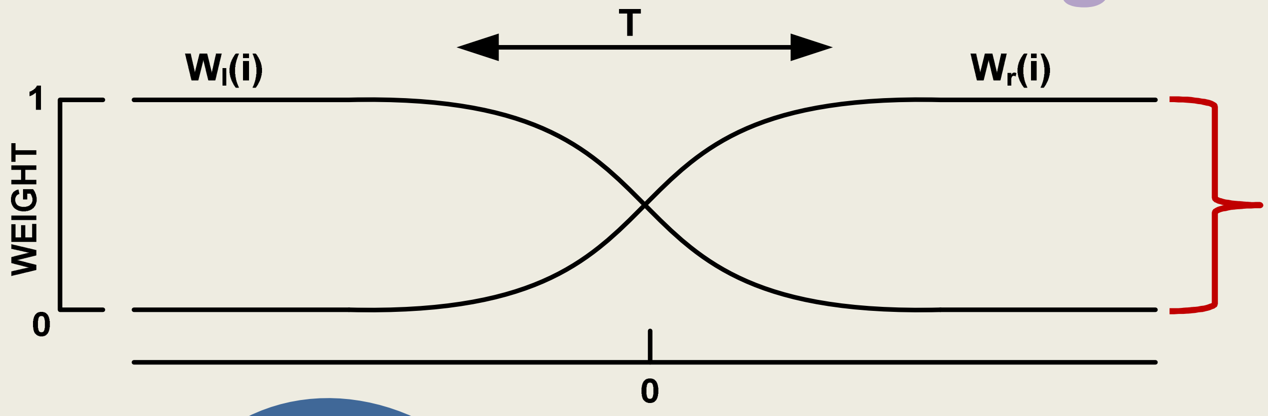


Parameter estimation of
weighted average splining

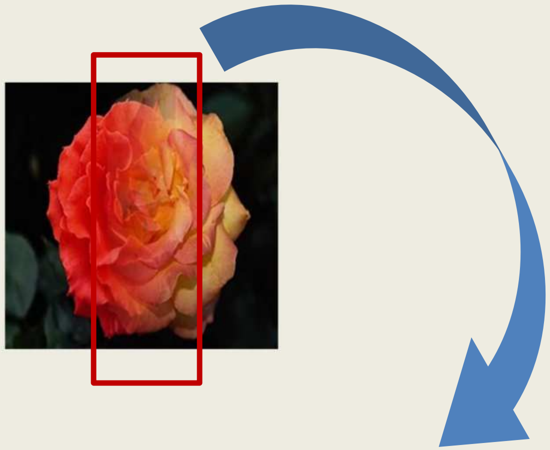
$$F(i) = W_l(i)F_l(i) + W_r(i)F_r(i)$$



Proposed idea: transition zone modeling



Construct model of these transition zones



Predicted weighting coefficients

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

1	1	0.900826	0.887931	0.876812	0.864516
1	1	0.897638	0.889655	0.873418	0.863946
1	1	0.902778	0.886076	0.876712	0.859155
1	1	0.89726	0.889706	0.87218	0.858209
1	1	0.9	0.889706	0.871212	0.861538
1	1	0.896825	0.890625	0.874016	0.865079
1	1	0.901515	0.883721	0.873016	0.864

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