Electronic Imaging 2014

Countering Anti-Forensics by Means of Data Fusion

Marco Fontani[#], Alessandro Bonchi[*], Alessandro Piva[*], Mauro Barni[°]

[*] University of Florence (IT)

[#] CNIT, University of Siena (IT)

[°] University of Siena (IT)

The Perfect Crime ?

- Creating a good forgery is easy today, yet most forgers may not know what they are leaving behind:
  - JPEG compression artifacts
  - Camera-related artifacts
  - Physical/Geometrical inconsistencies
  - Suspicious Metadata
- Creating the "perfect forgery" may not be so easy
- A smart analyst will make use of **many complementary detectors**, properly interpreting their answers (**multi-clue analysis**)

The world is full of obvious things which nobody by any change ever observes.

THE HOUND OF THE BASKERVILLES
A. Conan Doyle

Anti-Forensics & Counter-Anti-F.

- New threat: development of **Anti-Forensic** (AF) tools
  - Process the image so to remove a certain trace.
- In doing so, they are likely to **leave new artifacts in turn**

- **Counter-Anti-Forensic** (CAF) tools search for these second-round artifacts so to expose the presence of AF
- Some noticeable examples:

Anti-Forensics	Counter-Anti-Forensics
Stamm's approach for JPEG compression	Valenzise approach based on Total Variation analysis
Median filtering	Various Tools for MF detection

Our Contribution

- We recently investigated the **benefits of multi-clue analysis** in Image Forensics (AMULET project)
  - Proposed a framework based on Dempster-Shafer Theory for IF

- Now the question is: can **multi-clue analysis help against counter-forensics**?
  - By leveraging on the complementary nature of tools
  - By including CAF tools in the analyst's arsenal

Dempster-Shafer Theory

- Alternative to classical Bayesian theory
  - Good for modeling missing information
  - No need for prior probabilities
- Information is represented through *belief assignments*
- **Dempster's Combination Rule:** fuse information from multiple sources
- See the paper for more details and references

Countering Anti-Forensics by Means of Data Fusion

Marco Fontani[a], Alessandro Bonchi[b], Alessandro Piva[b] and Mauro Barni[c]
[a]CNIT, University of Siena, 53100 Siena, Italy;
[b]University of Florence, 50139 Firenze, Italy;
[c]University of Siena, 53100 Siena, Italy;

ABSTRACT

In the last years many image forensic (IF) algorithms have been proposed to reveal traces of processing or tampering. On the other hand, Anti-Forensic (AF) tools have also been developed to help the forger in removing editing footprints. Inspired by the fact that it is much harder to commit a perfect crime when the forensic analyst uses a multi-clue investigation strategy, we analyse the possibility offered by the adoption of a data fusion framework in a Counter-Anti-Forensic (CAF) scenario. We do so by adopting a theoretical framework, based on Dempster-Shafer Theory of Evidence, to synergically merge information provided by IF tools and CAF tools, whose goal is to reveal traces introduced by anti-forensic algorithms. The proposed system accounts for the non-trivial relationships between IF and CAF techniques; for example, in some cases the outputs from the former are expected to contradict the output from the latter. We evaluate the proposed method within a representative forensic task, that is splicing detection in JPEG images, with the forger trying to conceal traces using two different counter-forensic methods. Results show that decision fusion strongly limits the effectiveness of AF methods.

Keywords: Counter Forensics, Image Forensics, Data Fusion, Multi-clue decision

1. INTRODUCTION

In the last years Image Forensics (IF) has emerged as a way to investigate the processing history of digital images in a blind fashion.[1] Usually, IF tools work by searching a specific footprint that was left by processing operations as a side effect. Therefore, each IF tool usually behaves well in detecting whether a certain processing was applied. In real applications, however, there are many possible ways to tamper with an image, and the analyst does not know which forensic traces should be searched. A thorough analysis must rely on the use of many different tools, and merge their outputs as intelligently as possible. This path has been recently investigated in the IF field, and several methods are now available for data fusion.[2–4] As a new challenge to IF, anti-forensic (AF) methods are emerging, whose goal is to remove the footprints left during processing, making forensic analysis harder.[5] On the other hand, AF tools may leave their own footprints, and counter-anti-forensic (CAF) tools are being designed to detect them as well.

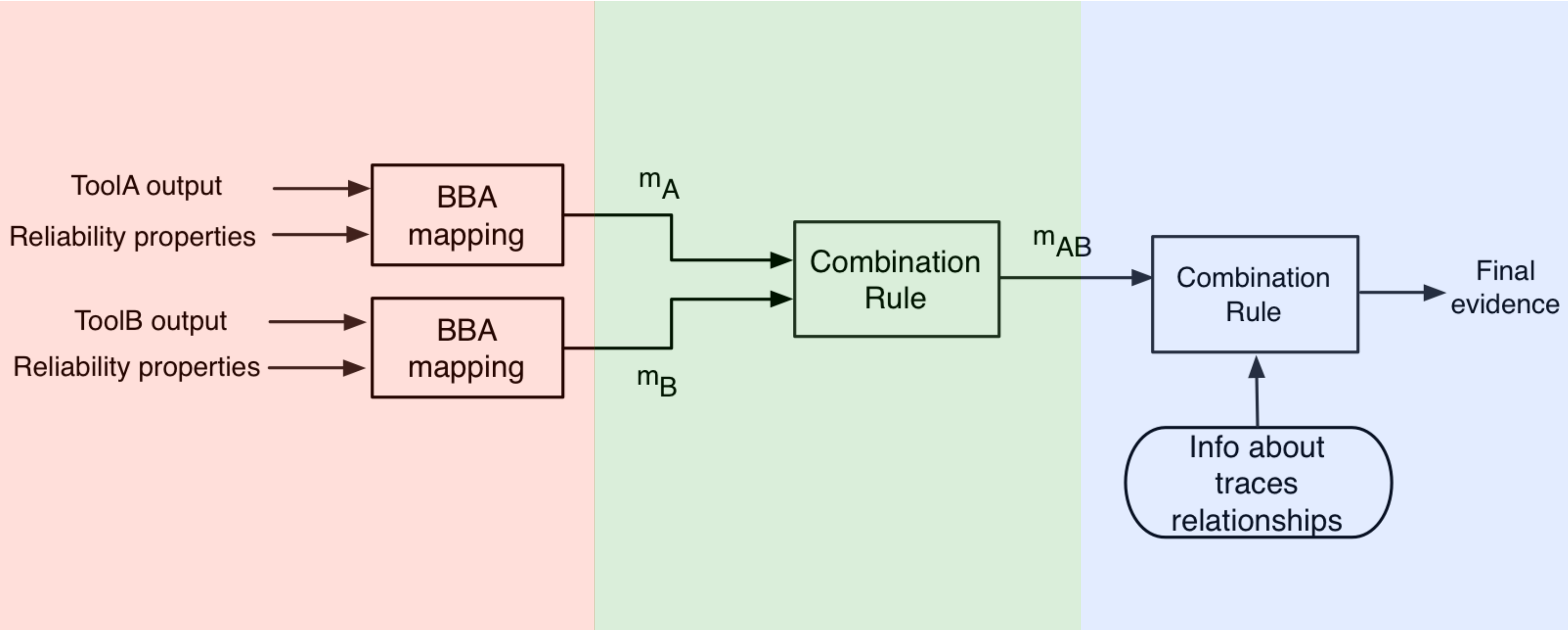
In such a scenario, the forensic analyst needs to simultaneously tackle with both the variety of detectable footprints and the presence of an adversary equipped with AF tools. If CAF tools are available to the analyst, a more robust analysis can be carried out, provided that outputs from IF tools and their CAF versions are interpreted properly, thus going back to information fusion. To the best of our knowledge, so far information fusion and CAF have been investigated only separately.

In this paper we analyse the possibility offered by the adoption of a data fusion framework in a CAF scenario. An intuitive solution could be to use all the available tools in an additive fashion ("OR" fusion rule), that means classifying the image as tampered when either an IF or a CAF tool detects the footprint it is looking for. This approach, however, does not take into account the following facts: i) IF tools may be searching for mutually

Further author information: (Send correspondence to Marco Fontani)
Marco Fontani: E-mail: marco.fontani@gmail.com
Alessandro Bonchi: E-mail: bonchi.ale@gmail.com
Alessandro Piva: E-mail: alessandro.piva@unifi.it
Mauro Barni: Email: barni@dii.unisi.it

DST framework in a nutshell 1/2

- We start from our multi-clue framework:



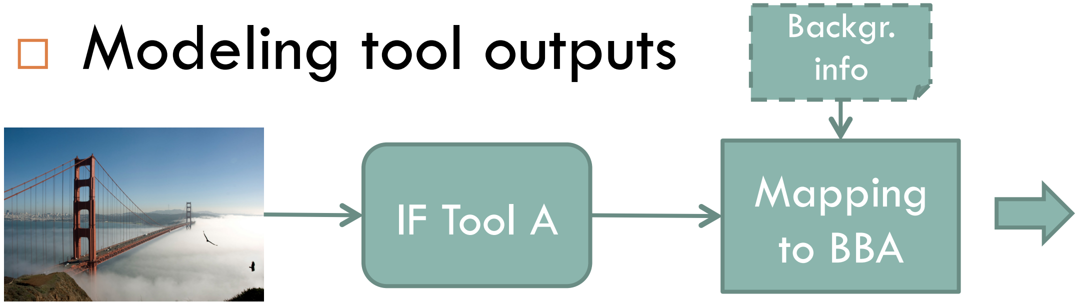
Interpretation of Tools Output (mapping to BBA)

Combine BBAs from different tools

Account for traces compatibility

DST framework in a nutshell 2/2

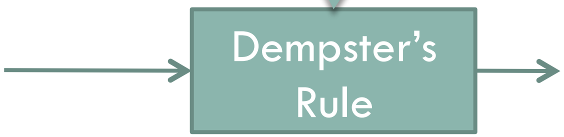
- Modeling tool outputs



$$m_A^{\Theta_\alpha}(X) = \begin{cases} 0.7 & \text{for } X = \{(t\alpha)\} \\ 0.2 & \text{for } X = \{(n\alpha)\} \\ 0.1 & \text{for } X = \{(t\alpha) \cup (n\alpha)\} \end{cases}$$

- Merging multiple tools

$$m_B^{\Theta_\alpha}(X) = \begin{cases} 0.8 & \text{for } X = \{(t\alpha)\} \\ 0.2 & \text{for } X = \{(n\alpha)\} \\ 0 & \text{for } X = \{(t\alpha) \cup (n\alpha)\} \end{cases}$$



$$m_{AB}^{\Theta_\alpha}(X) = \begin{cases} 0.8 & \text{for } X = \{(t\alpha)\} \\ 0.06 & \text{for } X = \{(n\alpha)\} \\ 0.14 & \text{for } X = \{(t\alpha) \cup (n\alpha)\} \end{cases}$$

- Introducing traces relationships

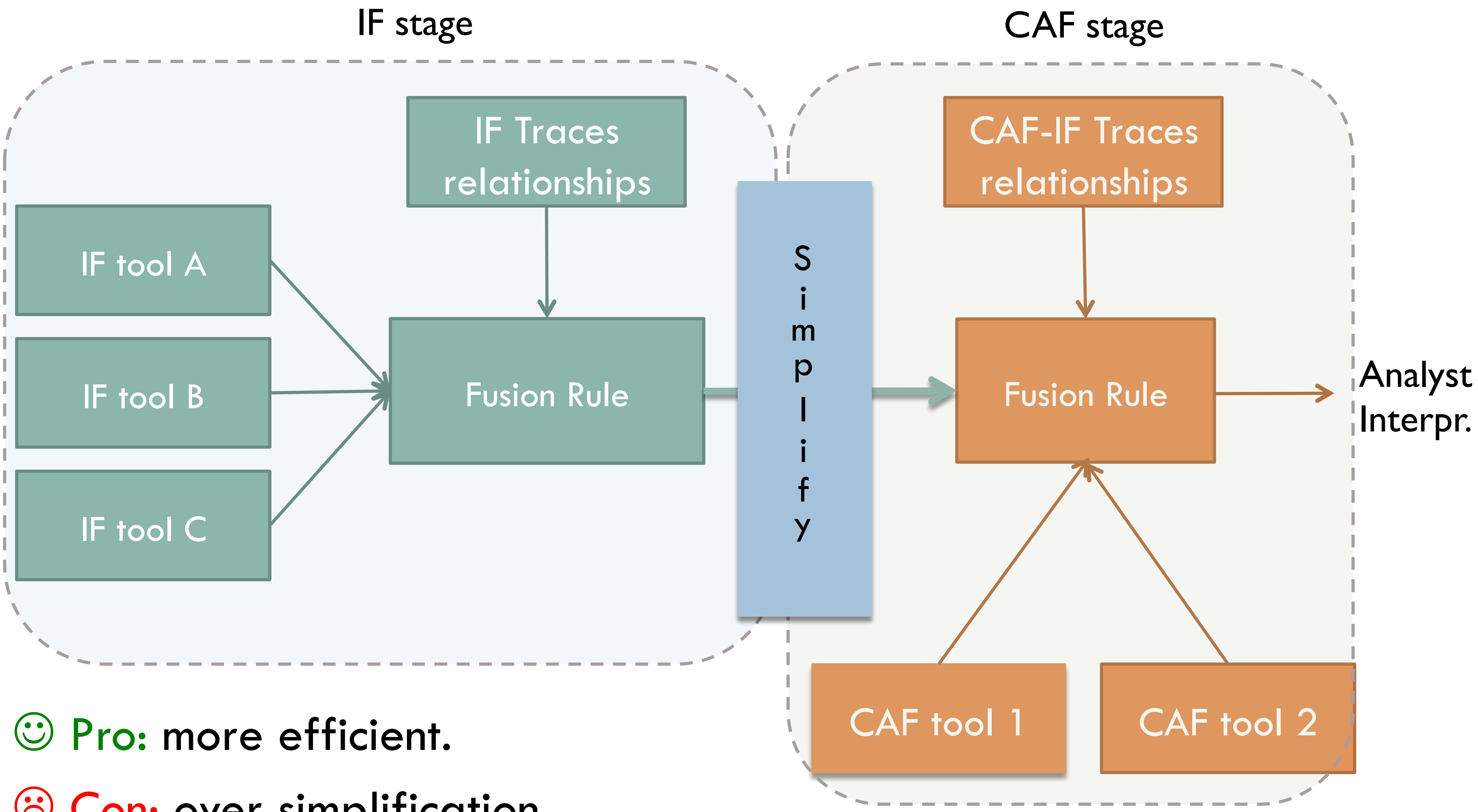
Id	α	β	Interpr.
1	0	0	Non-Tampered
2	0	1	Tampered
3	1	0	Tampered
4	1	1	-

$$m_{comp}(X) = \begin{cases} 1 & \text{for } X = \{(t\alpha, n\beta) \cup (n\alpha, t\beta) \cup (n\alpha, n\beta)\} \\ 0 & \text{for } X = \{(t\alpha, t\beta)\} \end{cases}$$

Introducing CAF tools…

- CAF tools can be modeled as standard IF tools…
- Still, some questions are in order:
- **Where** should we introduce them within the framework?
  - *Cascaded* architecture;
  - *Mixed* architecture.
- Traces of AF may have an ambiguous valence.
- How can we easily allow fusion of **subsets of tools**?

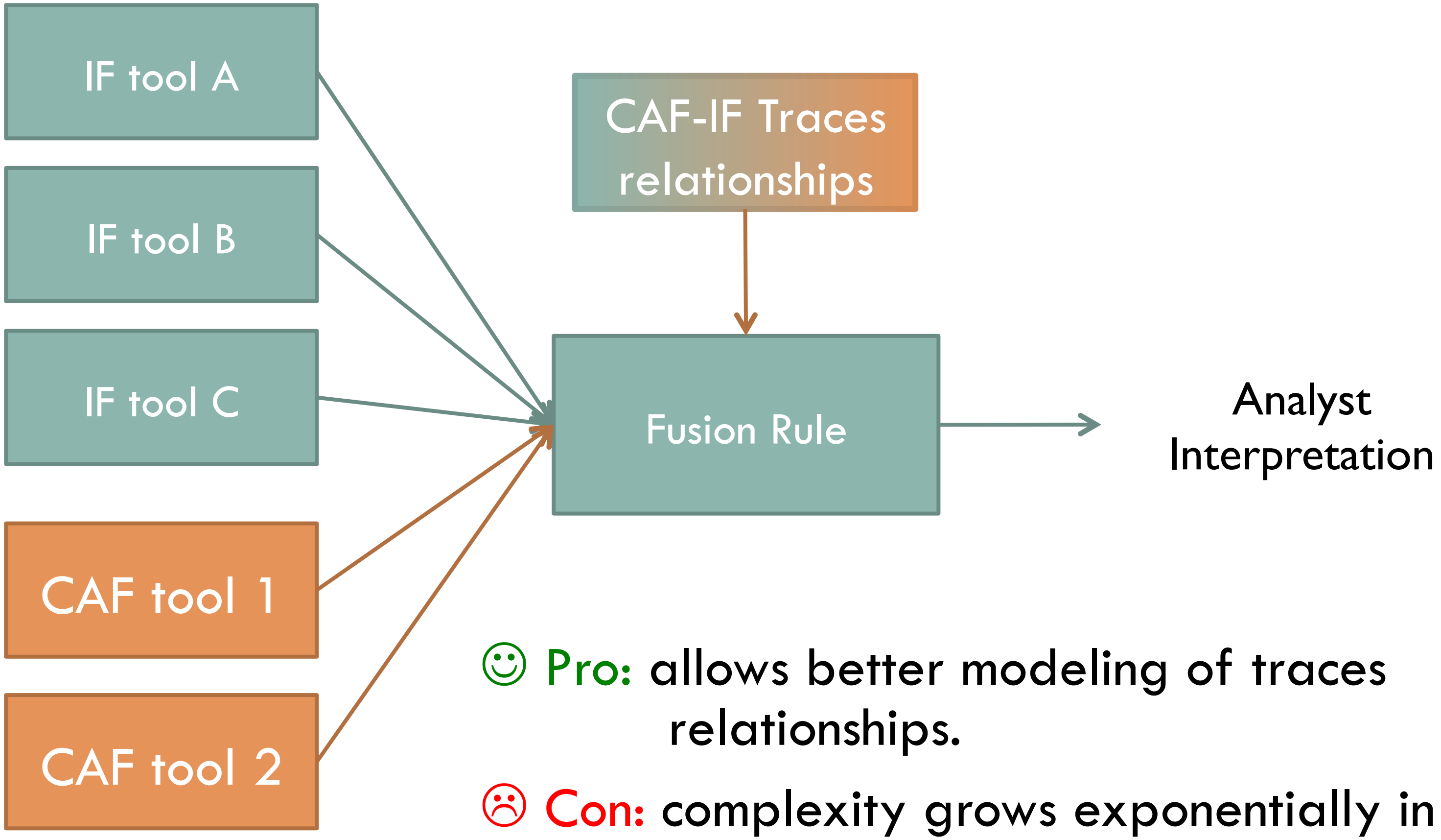
Where to introduce: *Cascade* Architecture



☺ Pro: more efficient.

☹ Con: over-simplification.

Where to introduce: *Mixed* Architecture



☺ Pro: allows better modeling of traces relationships.

☹ Con: complexity grows exponentially in the number of traces.

Ambiguous AF Traces

- It has been shown that some filtering operators can act as a good AF tool (e.g., median filtering operator).
- These operators has an **ambiguous forensic valence:**
  - they may have been used “benignly” (noise removal);
  - they may be acting as an AF attack.

- Possible approach: model **inconsistencies** in the presence of AF traces
  - Full frame filtering ➔ ok
  - Filter not applied to the whole image ➔ suspect

Disabling Tools

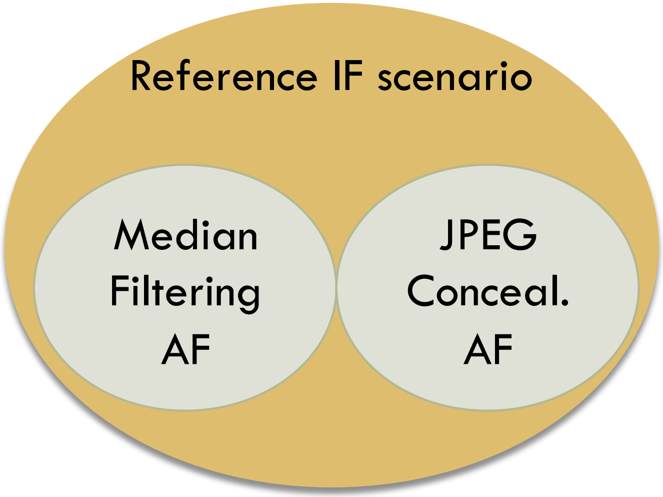
- It may happen that a tool cannot be used on an image (e.g., due to image format, size etc.)
- Can the analyst adapt the framework "on-the-fly"?
- With DS Theory, **yes!**
- Just exploiting the neutral element of Combination Rule:

$$m_U^{\Theta_\alpha}(X) = \begin{cases} 0 & \text{for } X = \{(t\alpha)\} \\ 0 & \text{for } X = \{(n\alpha)\} \\ 1 & \text{for } X = \{(t\alpha) \cup (n\alpha)\} \end{cases}$$

- **Notice:** doing the same with machine-learning techniques would not be so easy.

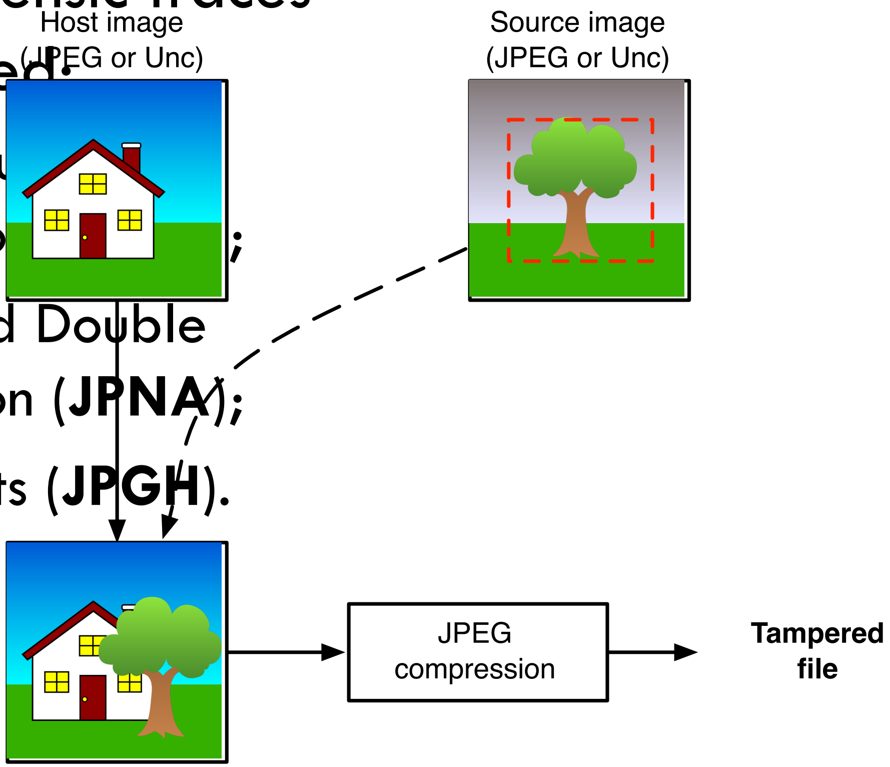
Case Studies

- We consider the **forgery detection** image forensic task:
  - given an image and a suspect region, determine whether it has been pasted or not.
- We choose a reference IF forensic scenario:
  - a set of possible tampering procedures;
  - a set of IF tools searching for different traces.
- Then, we consider two different case studies:
  - AF based on median filtering;
  - AF based on JPEG concealment.



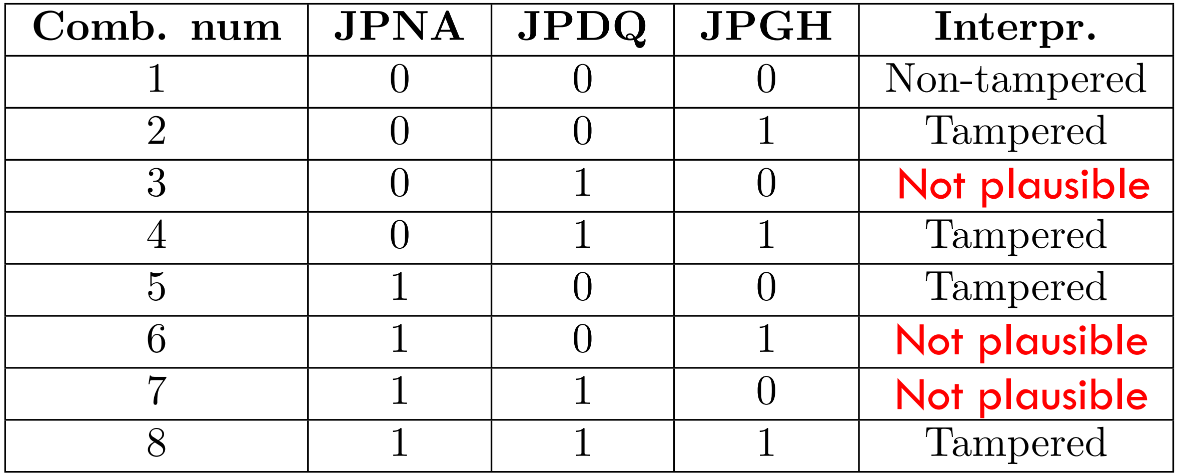
Case Studies: reference scenario

- □ Let us focus on the following forgery scenario:
- □ Different forensic traces are introduced:
  - Aligned Dou Quantizatio ;
  - Not-Aligned Double Quantization (**JPNA**);
  - JPEG Ghosts (**JPGH**).



Case Studies: reference scenario (c.)

- Not all the combinations of traces are plausible:



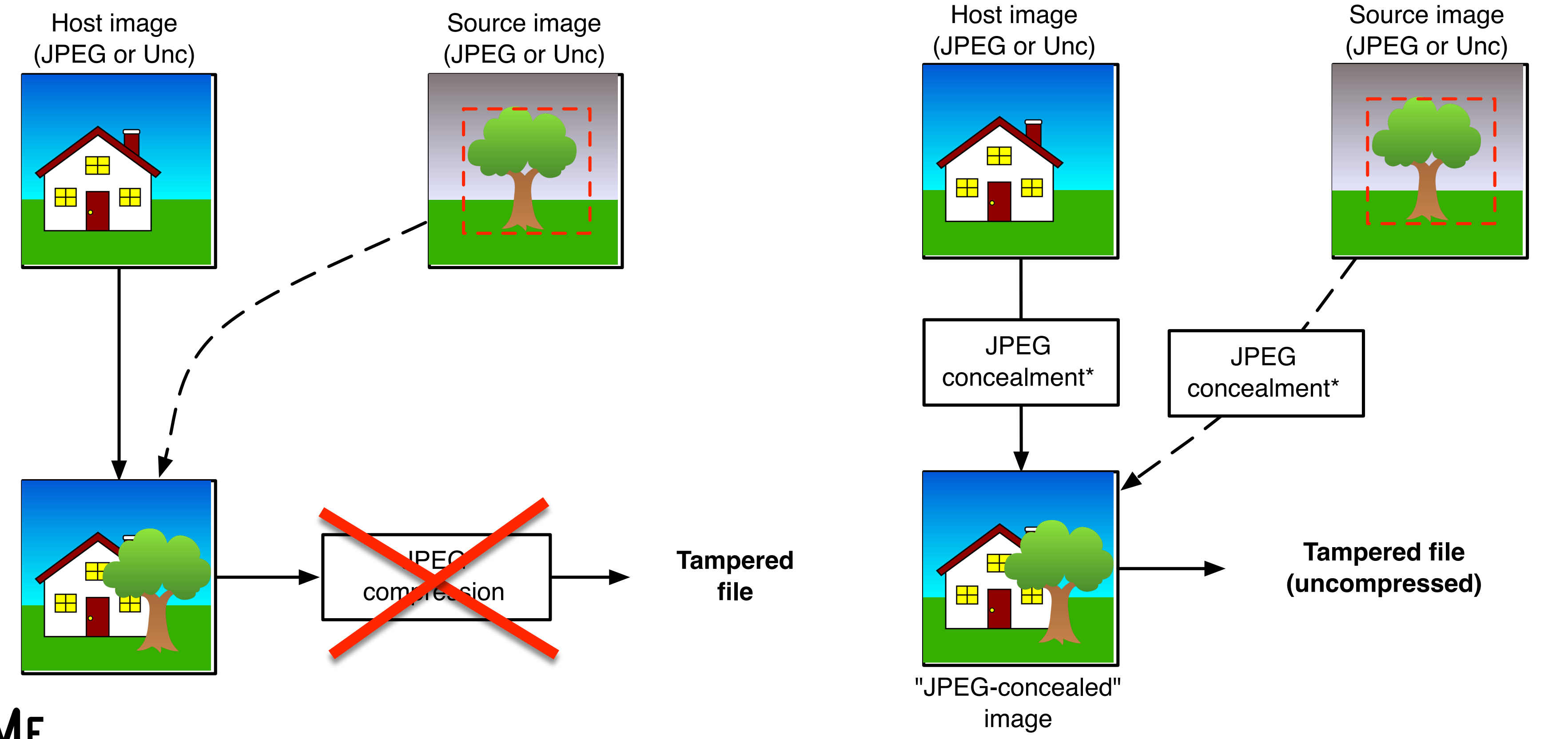
Comb. num	JPNA	JPDQ	JPGH	Interpr.
1	0	0	0	Non-tampered
2	0	0	1	Tampered
3	0	1	0	Not plausible
4	0	1	1	Tampered
5	1	0	0	Tampered
6	1	0	1	Not plausible
7	1	1	0	Not plausible
8	1	1	1	Tampered

- We provide the analyst five IF tools:

JPDQ	JPNA	JPGH
Lin et al.	Luo et al.	Farid
Bianchi et al.	Bianchi et al.	

Case Study: JPEG concealment

- □ The attacker now produces **uncompressed images**
- □ Two approaches considered:



Host image (JPEG or Unc)

Source image (JPEG or Unc)

~~JPEG compression~~

Tampered file

Host image (JPEG or Unc)

Source image (JPEG or Unc)

JPEG concealment*

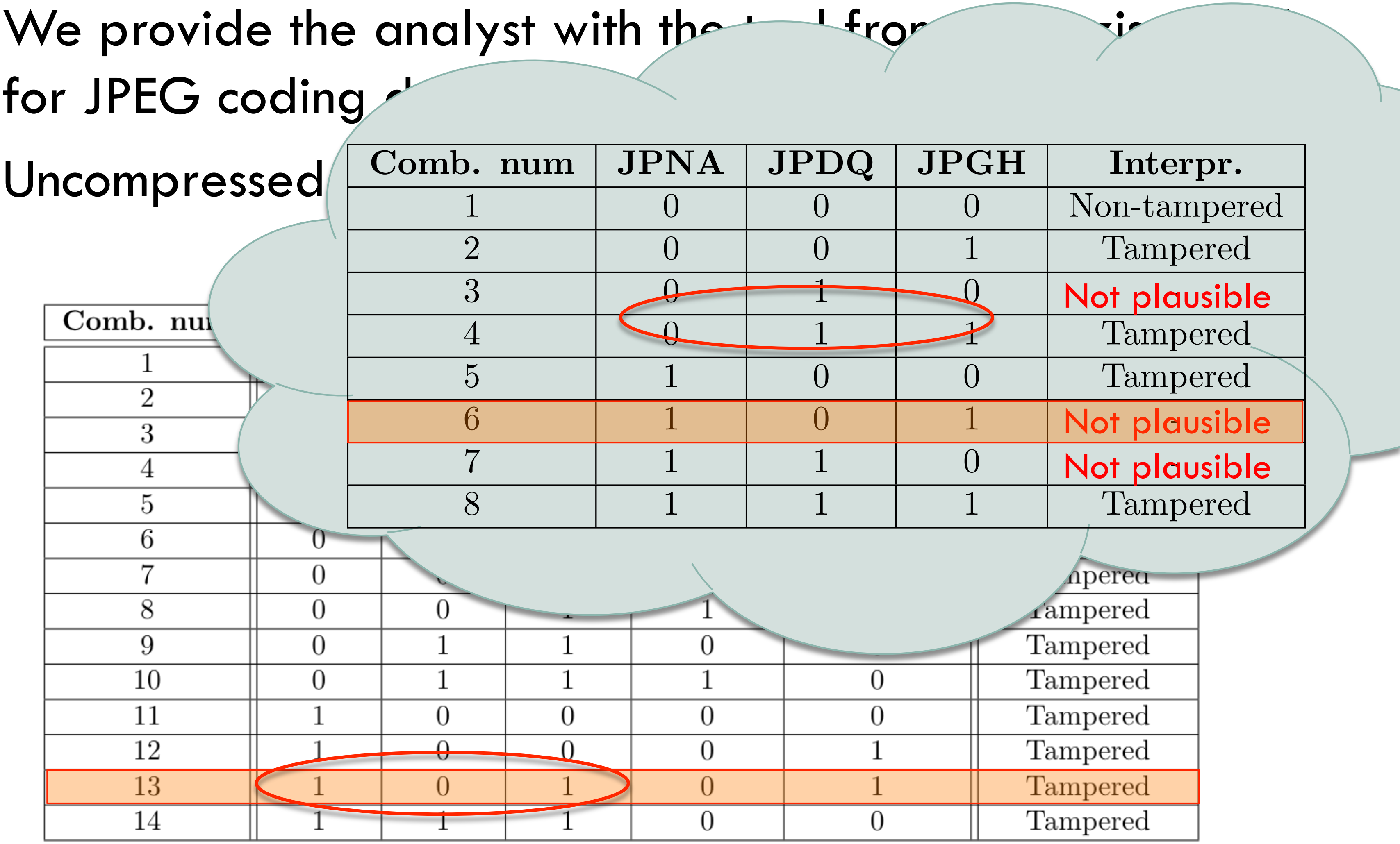
JPEG concealment*

"JPEG-concealed" image

Tampered file (uncompressed)

Case Study: analyst's countermeasures

- We provide the analyst with the t l fro zi for JPEG coding
- Uncompressed



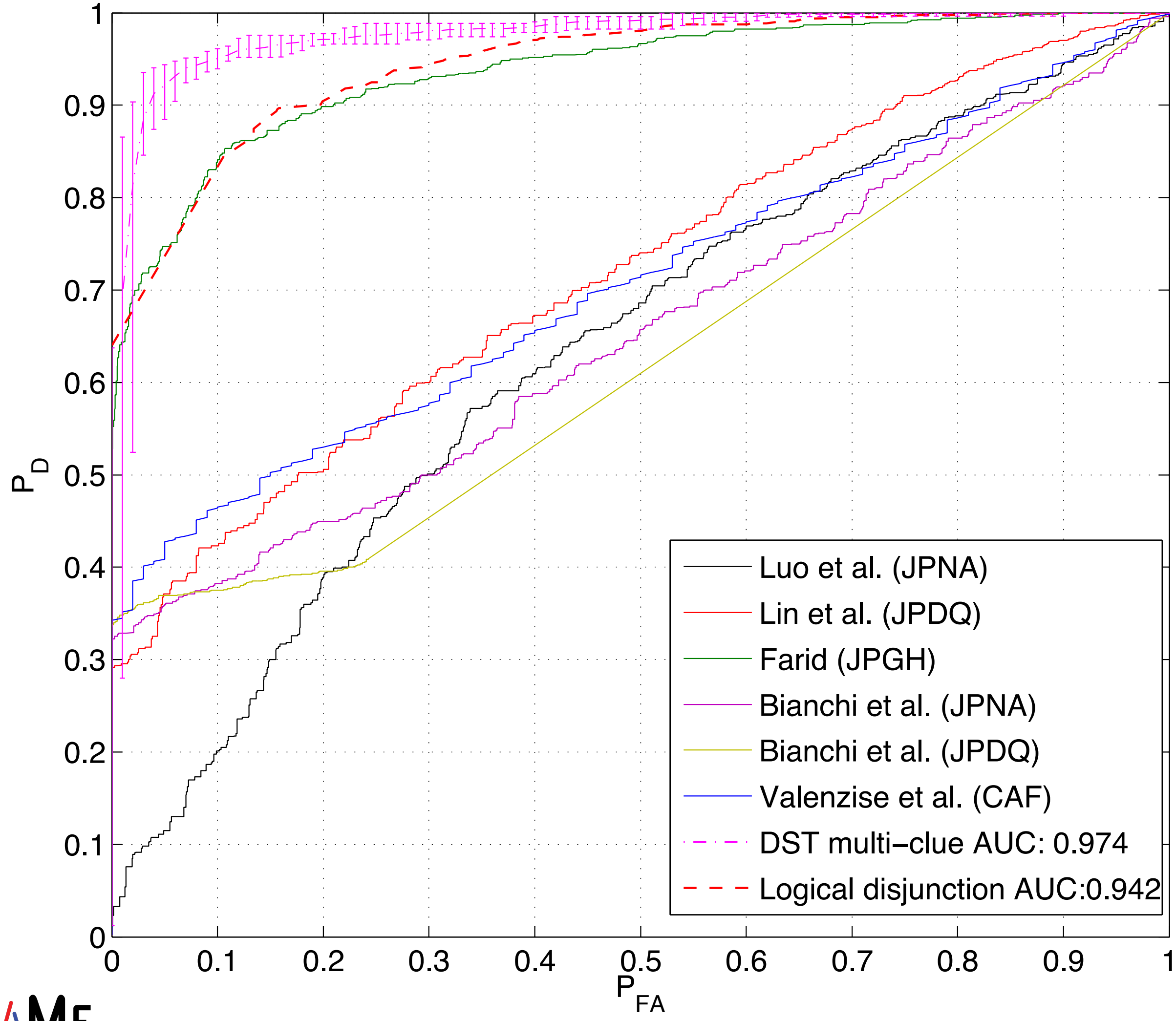
Comb. num	JPNA	JPDQ	JPGH	Interpr.
1	0	0	0	Non-tampered
2	0	0	1	Tampered
3	0	1	0	Not plausible
4	0	1	1	Tampered
5	1	0	0	Tampered
6	1	0	1	Not plausible
7	1	1	0	Not plausible
8	1	1	1	Tampered

Comb. nu						
1						
2						
3						
4						
5						
6	0					
7	0	0				npered
8	0	0	1	1		Tampered
9	0	1	1	0		Tampered
10	0	1	1	1	0	Tampered
11	1	0	0	0	0	Tampered
12	1	0	0	0	1	Tampered
13	1	0	1	0	1	Tampered
14	1	1	1	0	0	Tampered

Case study: experimental results

- Generated a dataset of:
  - 2000 untouched JPEG images
  - 500x4 tampered JPEG images (no AF)
  - 500x4 tampered images without final compression
  - 500x4 tampered images with AF
- Run all tools on every image.
- Merged outputs using:
  - DST-based fusion
  - Logical disjunction (“OR”) rule

Case study: experimental results



1. JPGH resists well to AF
2. Simple decision fusion doesn't help
3. DST-based fusion helps

Concluding Remarks

- Multi-clue analysis helps in presence of AF techniques, because:
  - the adversary may conceal only some IF traces;
  - AF tool for trace X may improve the detectability of Y;
  - the analyst can include CAF tools in the framework.
- Future work:
  - Explore wider variety of traces;
  - Compare with more complex fusion rules.

Acknowledgments

AMULET

A Multi-Clue Approach
to Image Forensics

SEVENTH FRAMEWORK
PROGRAMME

REWIND

REVerse engineering of
audio-Visual coNtend Data

AMULET

SEVENTH FRAMEWORK PROGRAMME

REWIND

SAME
SECURITY AND MULTIMEDIA GROUP

cnit

UNIVERSITÀ
DEGLI STUDI
FIRENZE

Thanks for your attention! Questions?

Countering Anti-Forensics by Means of Data Fusion

Marco Fontani, Alessandro Bonchi, Alessandro Piva, Mauro Barni