

The secret life of JPEG images

Forgery detection using compression traces

Tina Nikoukhah

Thesis defense, November 8th 2022

Supervisors



R. Grompone



M. Colom



J.-M. Morel

Thesis committee



H. Farid



L. Verdoliva



W. Puech



C. Ballester



A. Desolneux



D. Teyssou

What are the news of the day?

What are the news of the day?

Support the Guardian

Available for everyone, funded by readers

Contribute →

Subscribe →

Search jobs

Sign in

Search

International edition

The Guardian

News

Opinion

Sport

Culture

Lifestyle

More

World

UK

Coronavirus

Climate crisis

Environment

Science

Global development

Football

Tech

Business

Obituaries

Headlines

Sunday 30 October 2022

versailles

Now 18°C

18:00 16°C

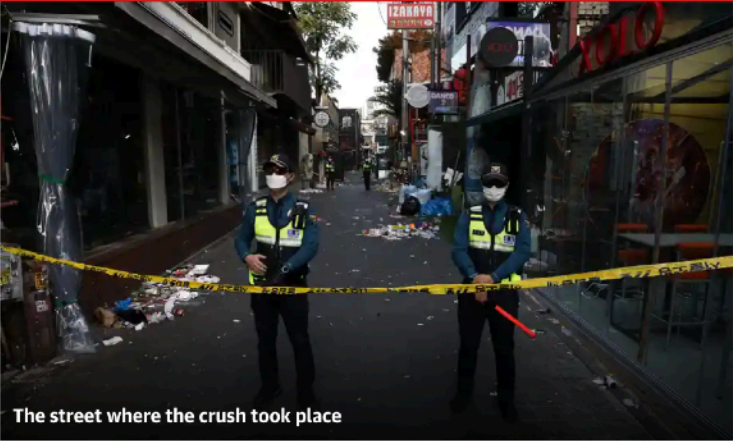
21:00 14°C

00:00 13°C

03:00 13°C

View full forecast

South Korea / At least 153 killed in crowd crush during Halloween festivities in Seoul



The street where the crush took place

Officials say 82 more injured after surge in Itaewon nightlife quarter of capital

'It was chaos' How my night out in Itaewon went from fun to horror

Halloween deaths

What we know so far about the crush in Itaewon

Itaewon crush

'Felt like an accident was bound to happen'

Brazil / Lula slight favourite to oust far-right Bolsonaro as election day arrives



Cop27 / Greenpeace accused of greenwashing Egypt's image ahead of summit



House of Lords / Tory peer apparently misled watchdog investigating his alleged misconduct



Twitter / Trolls bombard platform after Elon Musk takeover

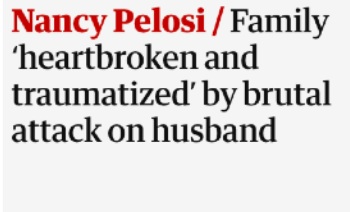


Northern Ireland / DUP 'hiding behind' protocol, ...

Live / Russia-Ukraine war: US accuses Russia of 'weaponising food' as EU urges Moscow to rejoin grain deal



Somalia / Car bombings kill at least 100 in Mogadishu, says president



Revealed / TE Lawrence felt 'bitter shame' over UK's ...



theguardian

Google News

Search for topics, locations & sources

Home

For you

Following

U.S.

World

Local

Business

Technology

Entertainment

Sports

Science

Health

Your briefing

Sunday, October 30

Yvelines 17°C

More on weather.com

Top stories



Seoul crowd crush shows gaps in Korean safety rules, experts say

15 minutes ago

CNN-News18

Seoul Halloween 2022 | Seoul Stampede Video | Seoul News Live | South Korea News | English News LIVE

2 hours ago

NBC News

Deadly Crowd Stampede Kills At Least 149 At Halloween Celebrations In Seoul

14 hours ago

Bloomberg

EXPLAINER: How And Why Do Crowd Surges Turn Deadly?

17 hours ago • Opinion

Full Coverage



Who Is the Man Accused of ...

The New York Times

Fox News

Nancy Pelosi breaks silence on husband Paul's attack: 'Heartbroken and traumatized'

12 hours ago

CNN

Pelosi says children, grandchildren are 'heartbroken and traumatized' in first comments since attack

1 hour ago

Fox News

Local news

Versailles

Cachan

7 Life Lessons At Versailles For My New High School Graduate

Aug 31

The Local France

French phrase of the Day: C'est pas Versailles ici

Jul 21

Reuters

Global CEOs to announce 6.7 billion euros of investment at Macron's Versailles summit

Jul 10

Picks for you

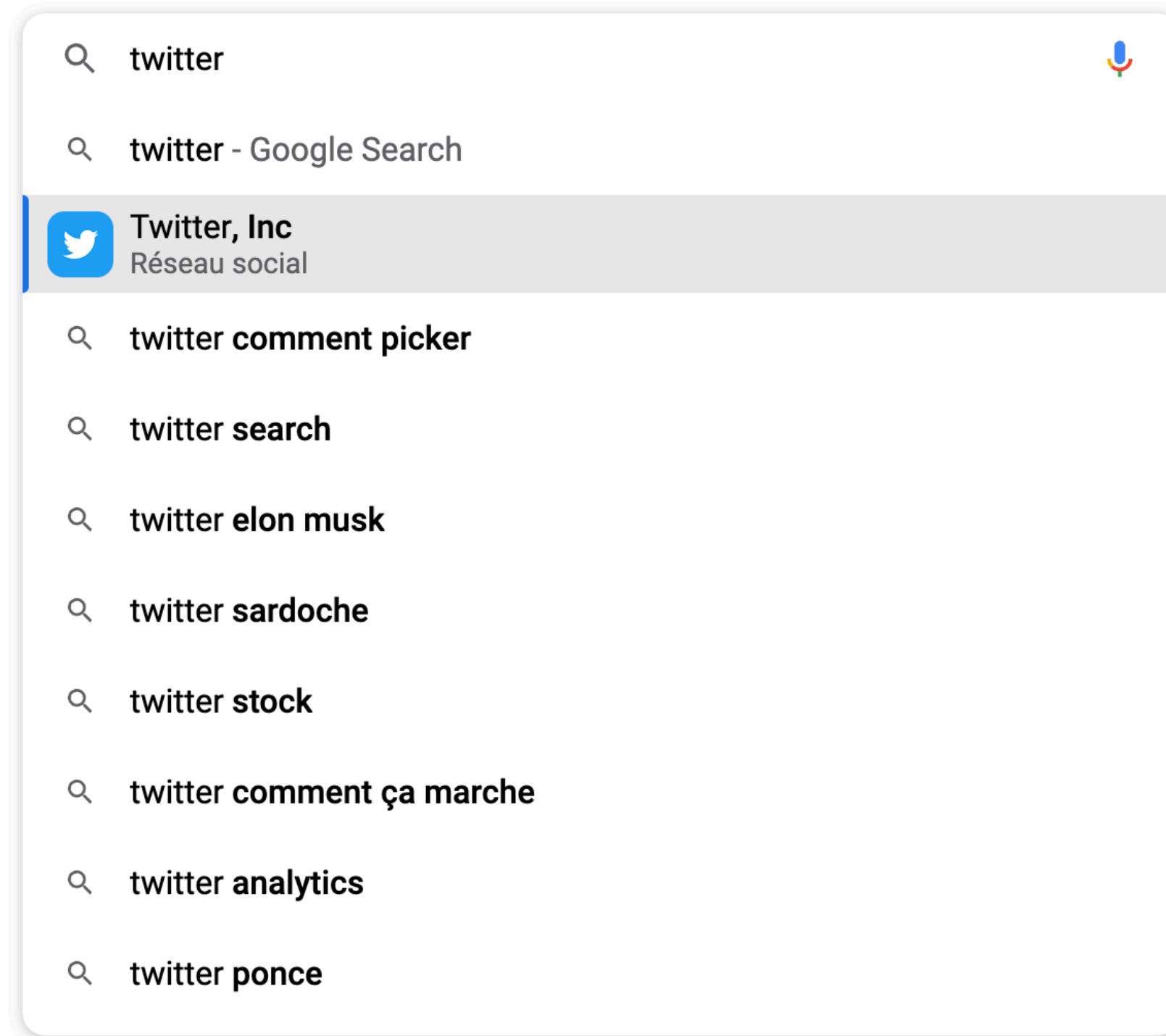
yahoo/life

This 'Friends' Co-Star Was the First to Reach Out to Matthew Perry During His Active Addiction



Google News

What are people talking about today?



twitter.com/search?q=%23TinasPhdDefense&src=recent_search_click&f=live

BookmarksInbox - tina.nikouk...BenLibrary GenesisIPOL Developmen...SciHubLa cave SlackGoogle Scholarjournals and confe...InVID Verification...ADUMOther Bookmarks



Home



Explore



Notifications



Messages



Bookmarks



Lists

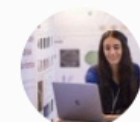


Profile



More

Tweet



Tina
@TinaNkh



#TinasPhdDefense



Top

Latest

People

Photos

Videos



Pashm @Pashm_ina · 19h

Soooo many people at #TinasPhdDefense 🤖🤖🤖



Pashm @Pashm_ina · 19h

No one showed up at #TinasPhdDefense, maybe because of the problems with the #RERB line?



Elon Musk

210K Tweets

Trending

Fake news

110K

Tweets

Trending in France

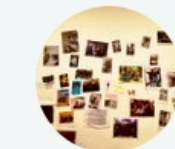
China

8,816

Tweets

Show
more

Who to follow



Planar Polarity Team
@PlanarPolarityT

Follow



MAMMOth
@mammoth_ai

Follow



Pantelis Dogoulis
@dogoulis Follows you

Follow

Show more

Terms of Service Privacy Policy Cookie Policy

Accessibility Ads info More ...

© 2022 Twitter, Inc.

Messages



Should we believe everything we see?

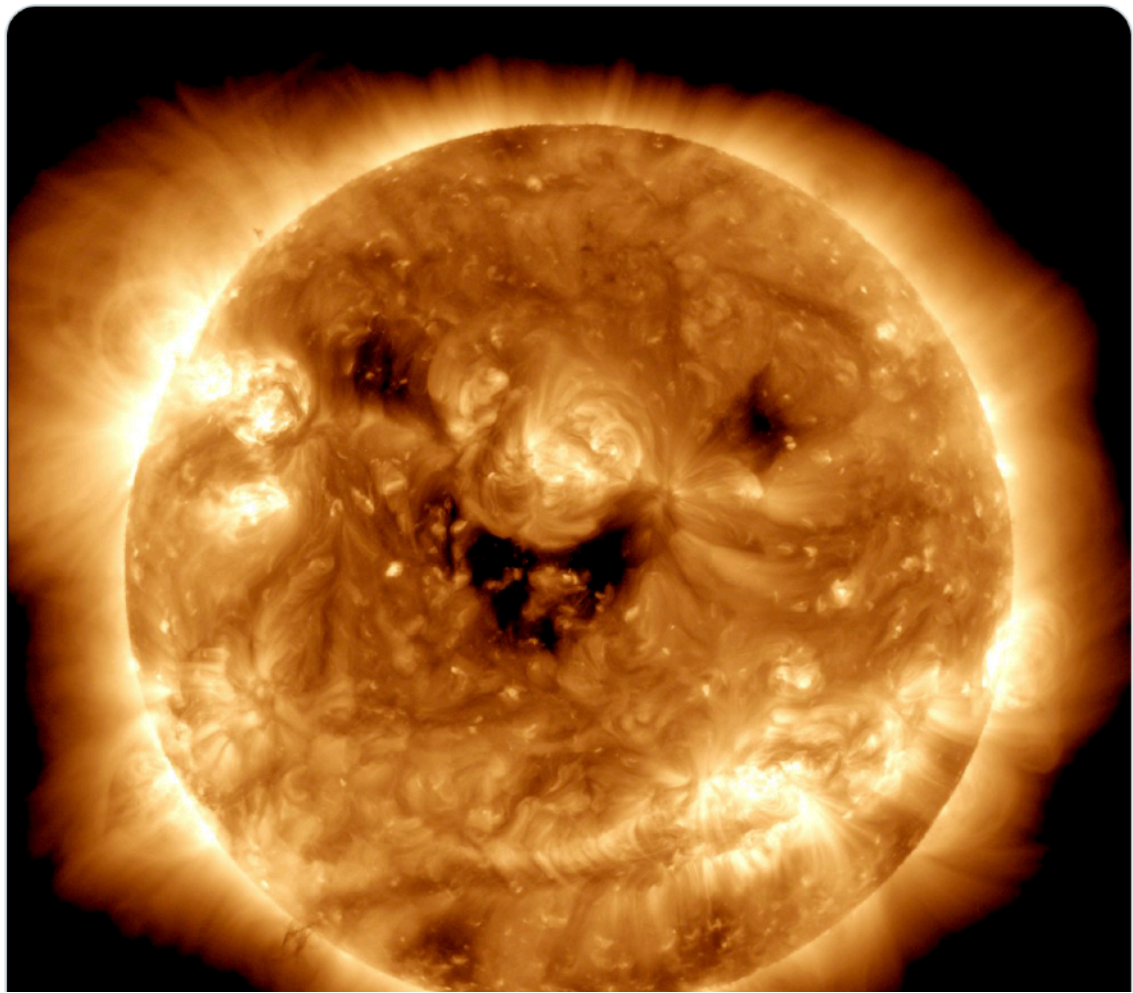


NASA Sun, Space & Scream 🍁🌌

@NASASun

Say cheese! 📸

Today, NASA’s Solar Dynamics Observatory caught the Sun "smiling." Seen in ultraviolet light, these dark patches on the Sun are known as coronal holes and are regions where fast solar wind gushes out into space.





Fascinating

@fasc1nate

High winds at the perfect time of day created a previously undocumented 2,400-foot rainbow waterfall in Yosemite National Park



From **Amazing Nature**
9:56 PM · Oct 21, 2022 · Twitter Web App



Le Média Positif 🍀

@LMPositif

🇮🇳 En Inde, dans le parc national de Keoladeo, une impressionnante photographie a été prise d’une antilope et d’une grue antigone. Une scène qui fait penser à la célèbre créature fantastique Pégase ! ❤️

📸 Jagdeep Rajput

[Translate Tweet](#)





ENS Paris-Saclay

@ENS_ParisSaclay

No one showed up at [#TinasPhdDefense](#), maybe because of the problems with the [#RERB](#) line?



4:00 PM · Nov 8, 2022 · Twitter Web App



Telegraph Breaking News

@TelegraphNews

Fake images of Parkland shooting survivor Emma Gonzalez tearing up US constitution spread on social media



telegraph.co.uk
Fake images of Parkland shooting survivor Emma Gonzalez tearing up US const...
Faked images showing the Parkland school shooting survivor Emma Gonzalez tearing up the US constitution have emerged on social media.

12:45 PM · Mar 26, 2018 · dlvr.it



Le Parisien | Paris

@LeParisien_75

VIDÉO. 76 platanes coupés à Paris, les riverains en colère: «Pour qu’un arbre pousse, il faut du temps»
[l.leparisien.fr/9R3H](#)

[Translate Tweet](#)

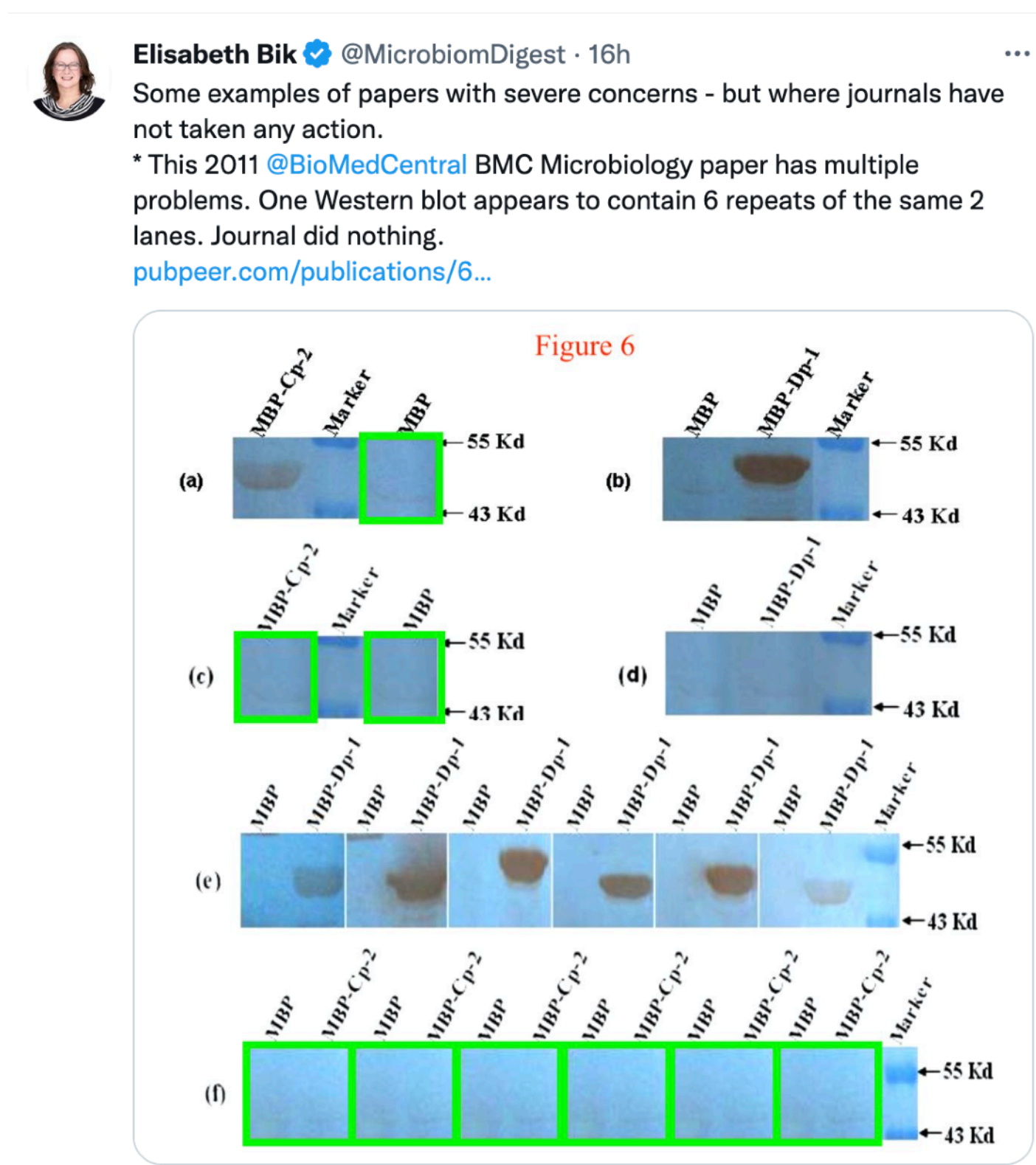


1:43 PM · Apr 28, 2022 · Nonli

Why forge an image?



fake news



scientific misconduct



fraud

Why forge an image?



aesthetic reasons



advertisement



other

Home / Twitter

twitter.com/home

Search Twitter

Home

Explore

Notifications

Messages

Bookmarks

Lists

Profile

More

Tweet

Home

What's happening?

Professor Xmonad and Hugo Travers (HugoDécrypte) follow

Mathis Hammel @MathisHammel · 23h

Après un petit changement d'algo (vitesse plus faible + compensation de l'hystérésis), je vais pouvoir m'attaquer à des dessins plus complexes 😊

Alicia Keys @aliciakeys

No one, no one, no one 🎵 #TinasPhdDefense



4:02 PM · Nov 8, 2022 ·

Tina @TinaNkh

God (Thee/Thy) @TheTweetOfGod · 1m

Oh Ye of little sanity.

Trends for you

Trending in France

#vpvcestlavie

Trending

IPOL

6,546 Tweets

Trending

#PashminaisthenewLena

12,902 Tweets

Trending in France

#TinasPhdDefense

14,082 Tweets

Trending in France

RERB en panne

2,070 Tweets

Trending

#مهسا_امینی

38,546 Tweets

Trending in France

#FemmeVieLiberté

Trending

Elon Musk

210.4K Tweets

Trending

Fake news

110K Tweets

Messages

Fake news



ENS Paris-Saclay

@ENS_ParisSaclay_ParisSaclay



No one showed up at [#TinasPhdDefense](#), maybe because of the problems with the [#RERB](#) line?



4:00 PM · Nov 8, 2022 · Twitter Web App

Disinformation: image taken out of context

 **ENS Paris-Saclay**
@ENS_ParisSaclay_ParisSaclay

...

No one showed up at [#TinasPhdDefense](#), maybe because of the problems with the [#RERB](#) line?



4:00 PM · Nov 8, 2022 · Twitter Web App

 **ENS Paris-Saclay**
@ENS_ParisSaclay

...

Rehearsal of [#TinasPhdDefense](#), sound check, video check, internet check 🙄🙄🙄



10:49 AM · Nov 1, 2022 · Twitter Web App

Original image



ENS Paris-Saclay
@ENS_ParisSaclay



Rehearsal of [#TinasPhdDefense](#), sound check, video check, internet check 🙄🙄🙄



10:49 AM · Nov 1, 2022 · Twitter Web App

Image tampering: erasing



Alicia Keys
@aliciakeys



No one, no one, no one 🎵 #TinasPhdDefense



4:02 PM · Nov 8, 2022 ·

Image tampering: duplicating



Movers
@troll



Soooo many people at [#TinasPhdDefense](#) 🤡🤡🤡



4:02 PM · Nov 8, 2022 · Twitter App

Image tampering: splicing



Pashmina fan club
@Pashm_ina



Her pets came to [#TinasPhdDefense](#) !! 🐱🐶



4:05 PM · Nov 8, 2022 · Twitter Web App

What tools do we easily have access to?

- Our eyes and brain: forgeries are made to be believable!
- The image file, but there are no EXIF metadata!
- Image reverse search on the Internet.

#TinasPhdDefense - Twitter Se x

twitter.com/Pashm_ina/status/1586428190545055744/photo/1

BookmarksInbox - tina.nikouk...BenLibrary GenesisIPOL Developmen...SciHubLa cave SlackGoogle Scholarjournals and confe...InVID Verification...ADUMOther Bookmarks

#TinasPhdDefense

3,172 Tweets

Sports · Trending



Alicia Keys

@aliciakeys

No one, no one, no one 🎵
#TinasPhdDefense

4:02 PM · Nov 8, 2022 · Twitter Web App



Tweet your reply

Reply

Open Image in New Tab

Save Image As...

Copy Image

Copy Image Address

Create QR code for this Image

Search image with Google Lens

AdGuard AdBlocker

Fake news debunker by InVID WeVerify

Windscribe - Free Proxy and Ad Blocker

Inspect

Open with assistant

Open with OCR

Image Magnifier

Image Forensic

Image Reverse Search - ALL

Image Reverse Search - DBKF (beta)

Image Reverse Search - Google

Image Reverse Search - Yandex

Image Reverse Search - Bing

Image Reverse Search - TinEye

Image Reverse Search - Baidu

Image Reverse Search - Reddit

Tina

@TinaNkh

Messa

19

What can we do?

Reconstruct the digital history of an image.

Image processing pipeline

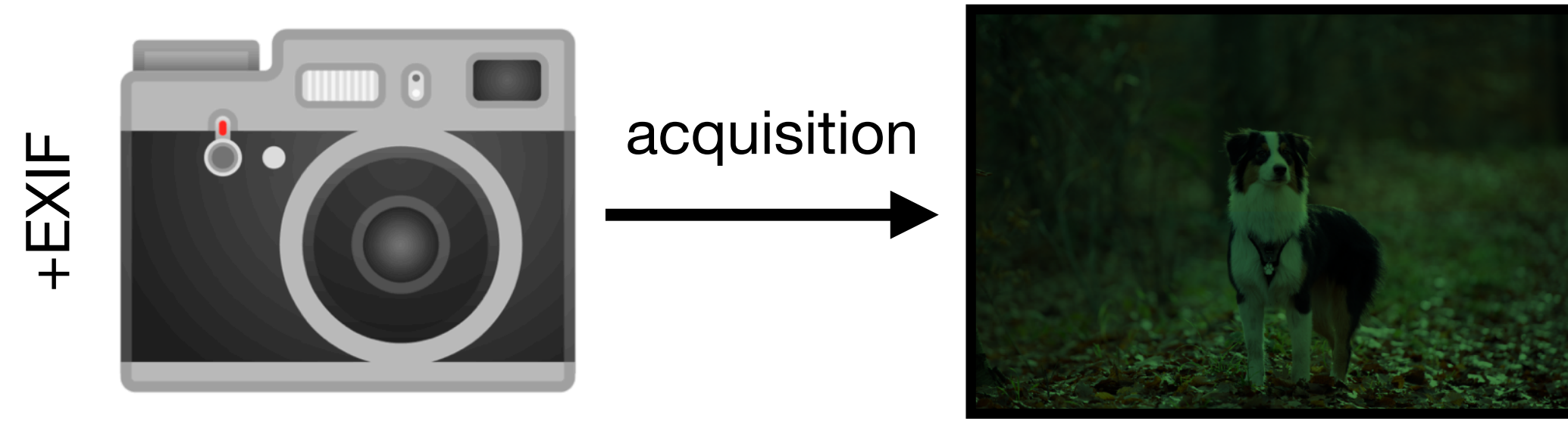


Image processing pipeline

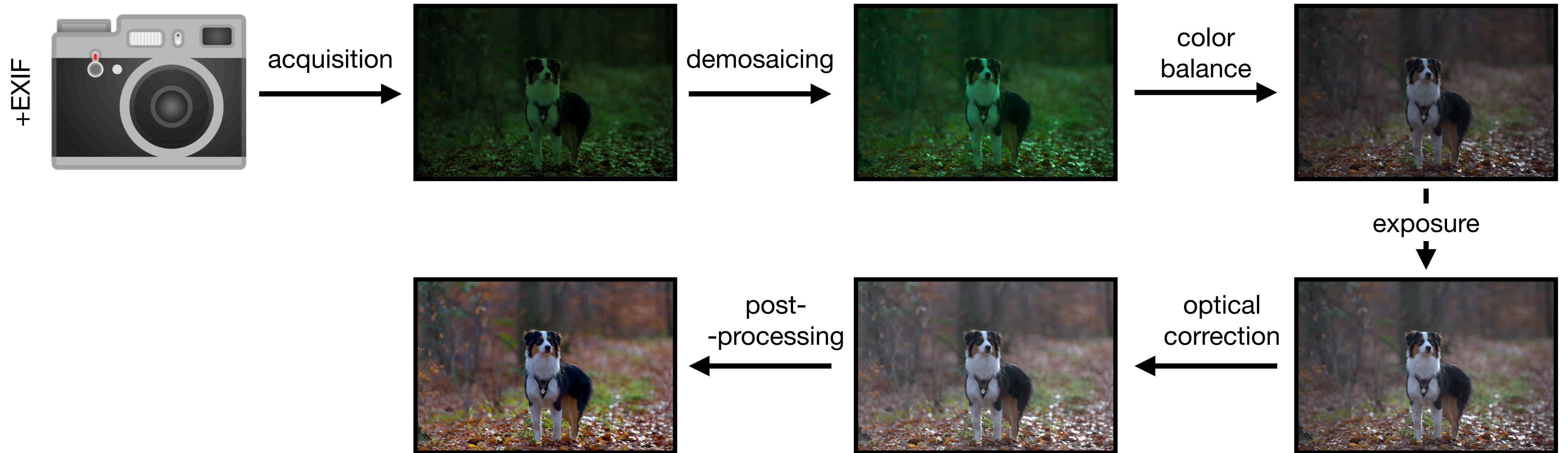


Image processing pipeline

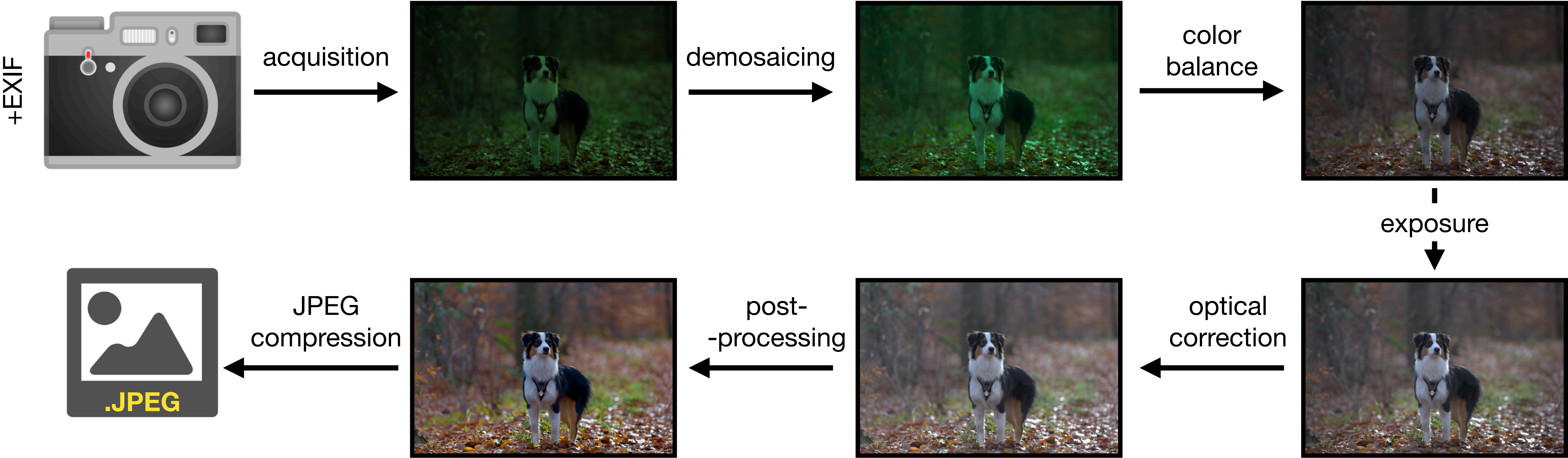


Image processing pipeline

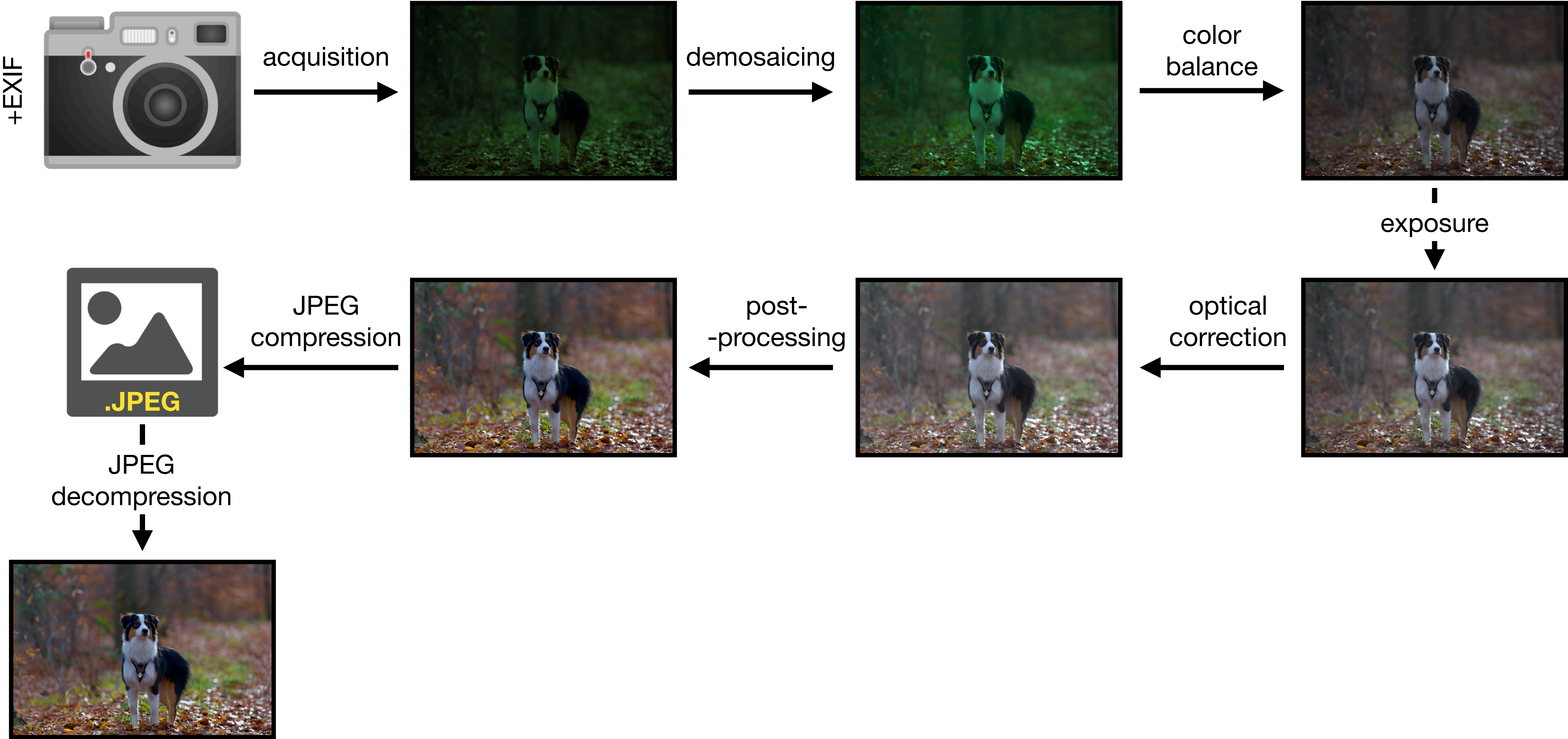


Image processing pipeline

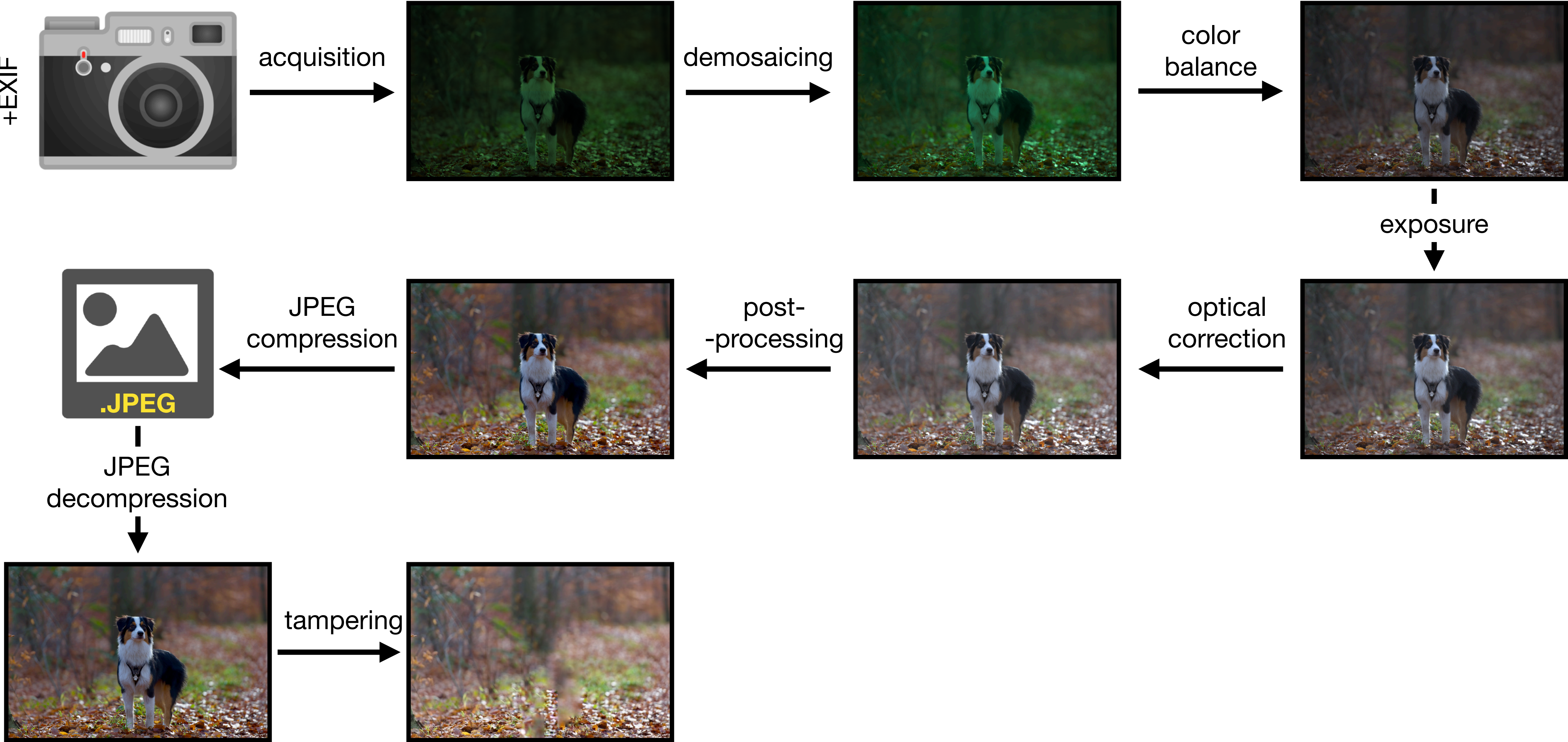
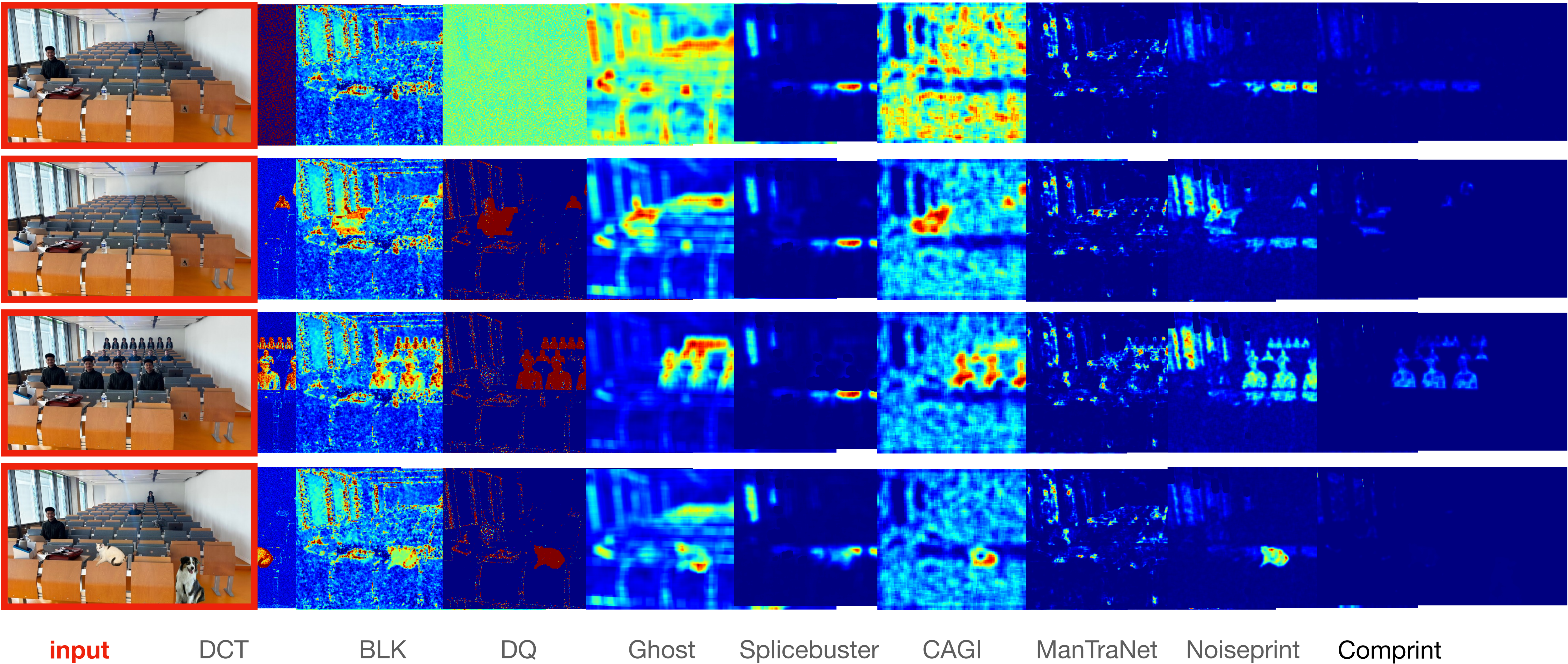


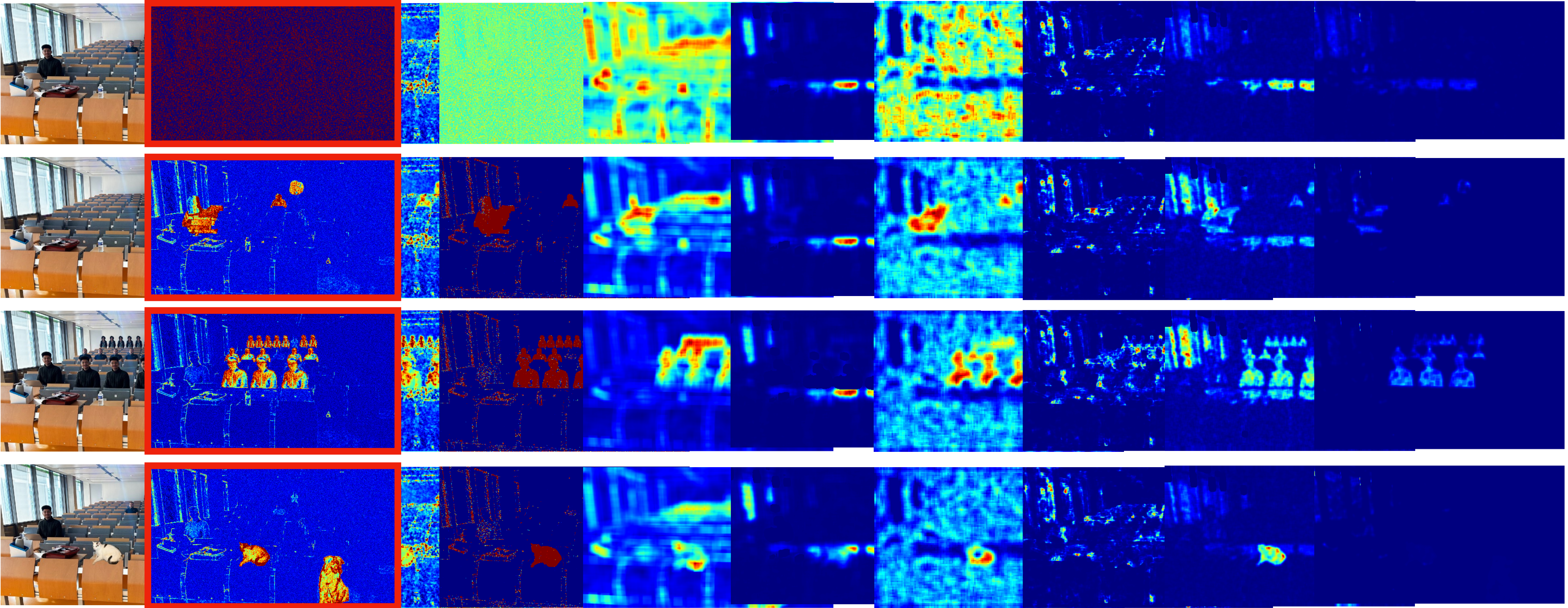
Image forensics

Image forgery detection



Markos Zampoglou, Symeon Papadopoulos, and Yiannis Kompatsiaris. "Large-scale evaluation of splicing localization algorithms for web images". In: Multimedia Tools and Applications 76.4 (2017).
Cozzolino, Davide, and Luisa Verdoliva. "Noiseprint: a CNN-based camera model fingerprint." *IEEE Transactions on Information Forensics and Security* 15 (2019): 144-159.
Mareen, Hannes, et al. "Comprint: Image Forgery Detection and Localization using Compression Fingerprints." (2022)

Image forgery detection



input **DCT** BLK DQ Ghost Splicebuster CAGI ManTraNet Noiseprint Comprint

Image forgery detection

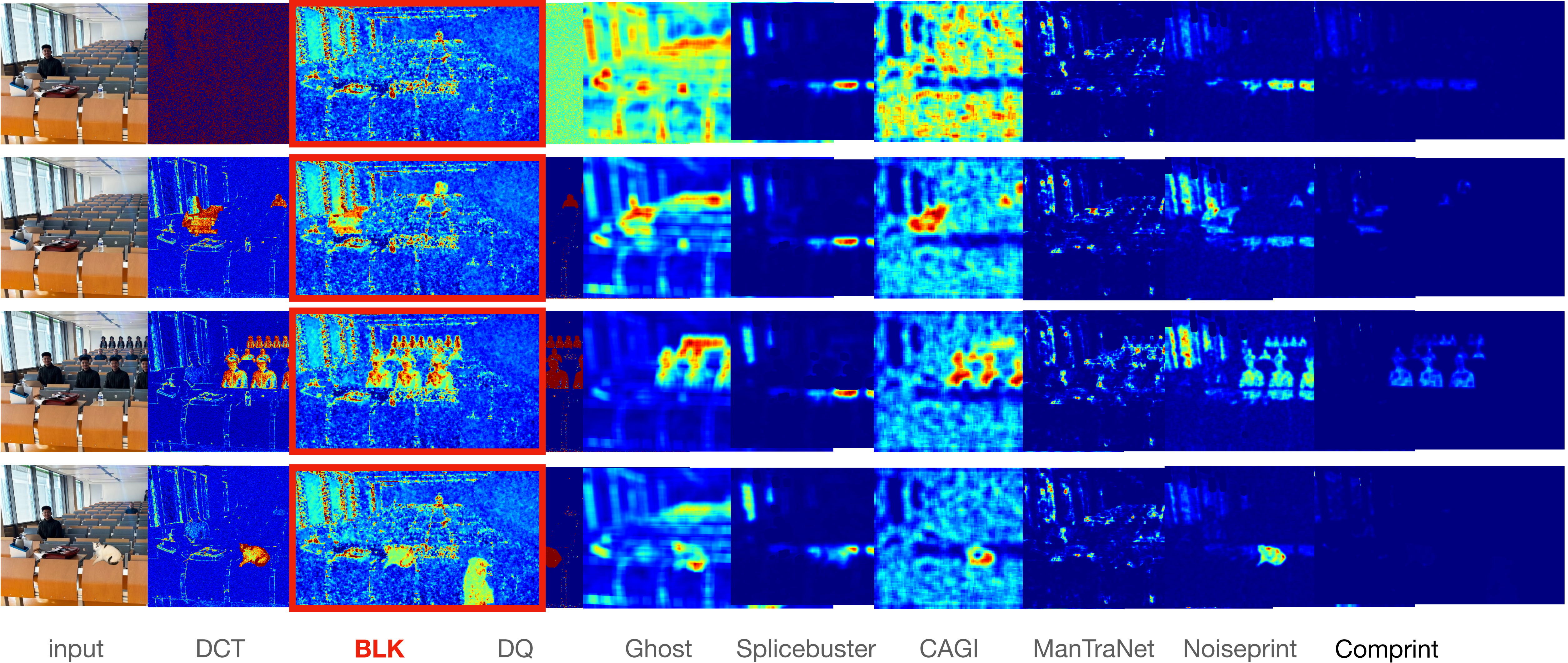


Image forgery detection

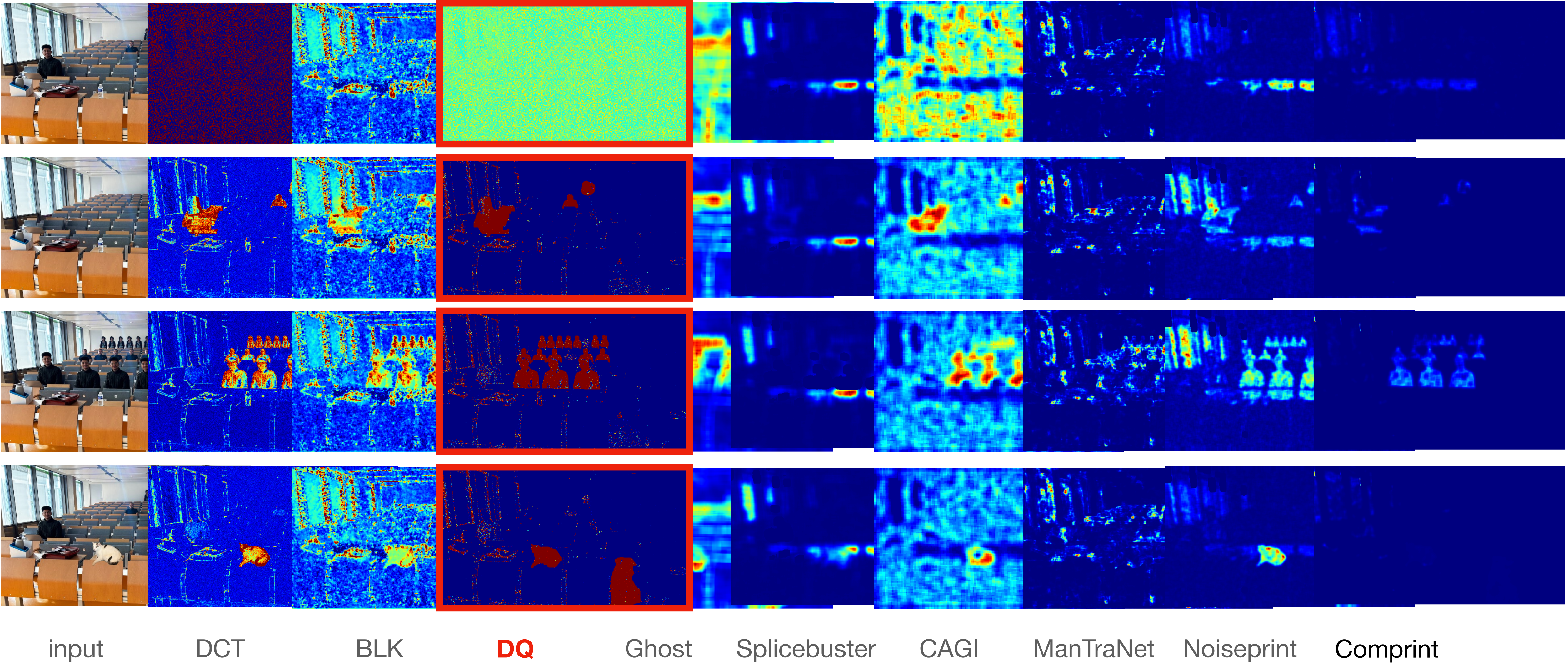


Image forgery detection

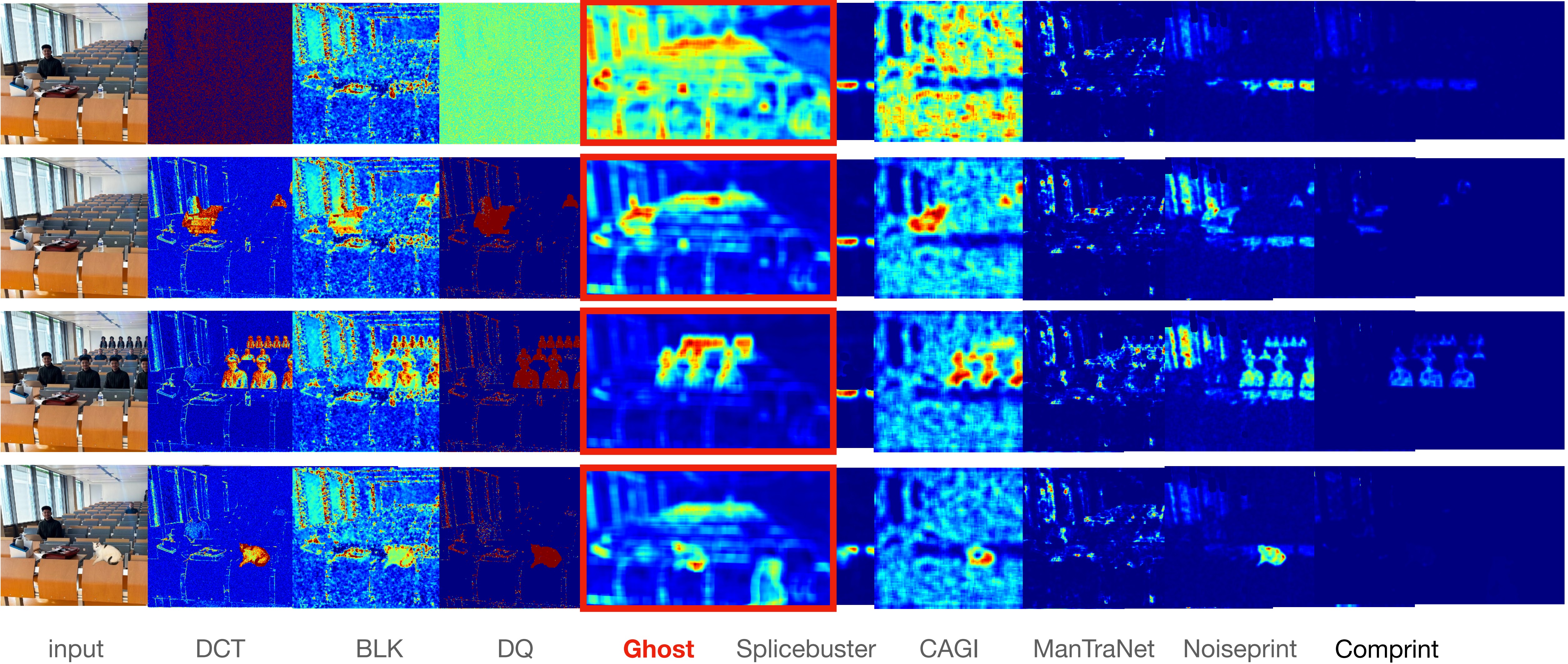
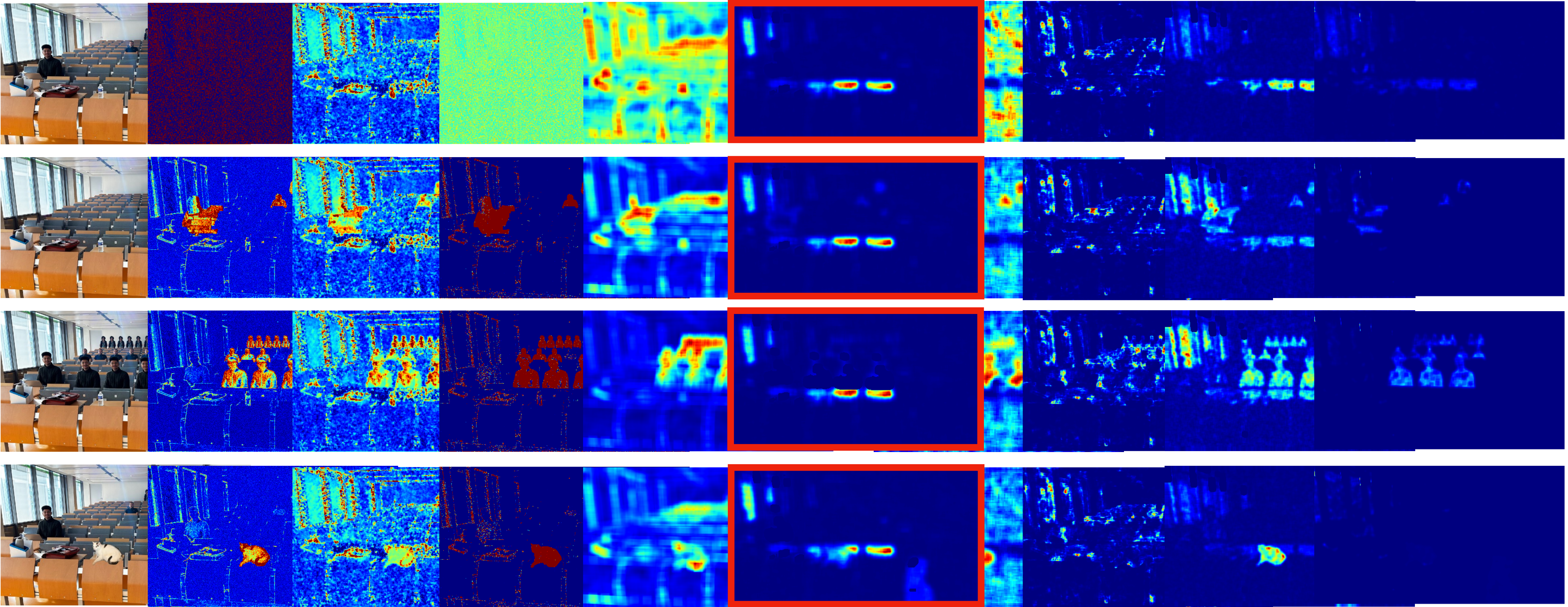


Image forgery detection



input DCT BLK DQ Ghost **Splicebuster** CAGI ManTraNet Noiseprint Comprint

Image forgery detection

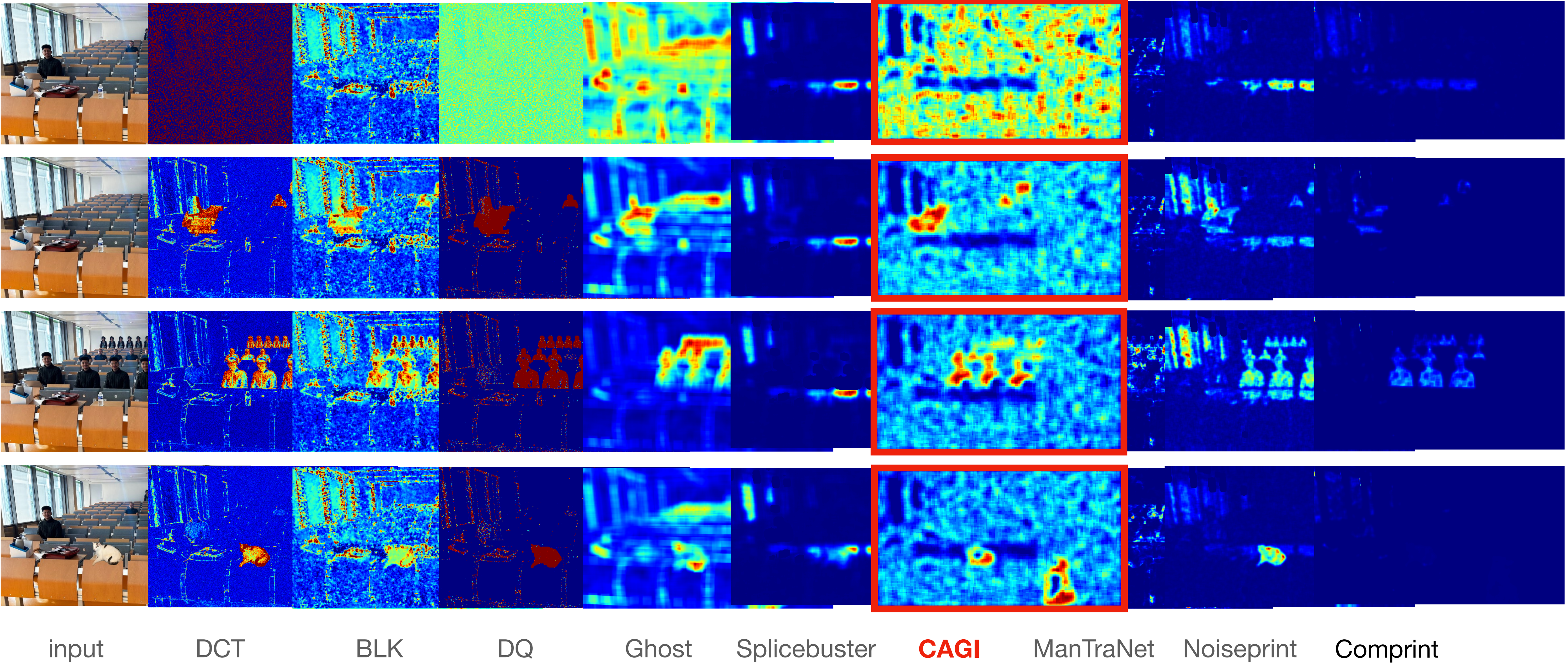


Image forgery detection

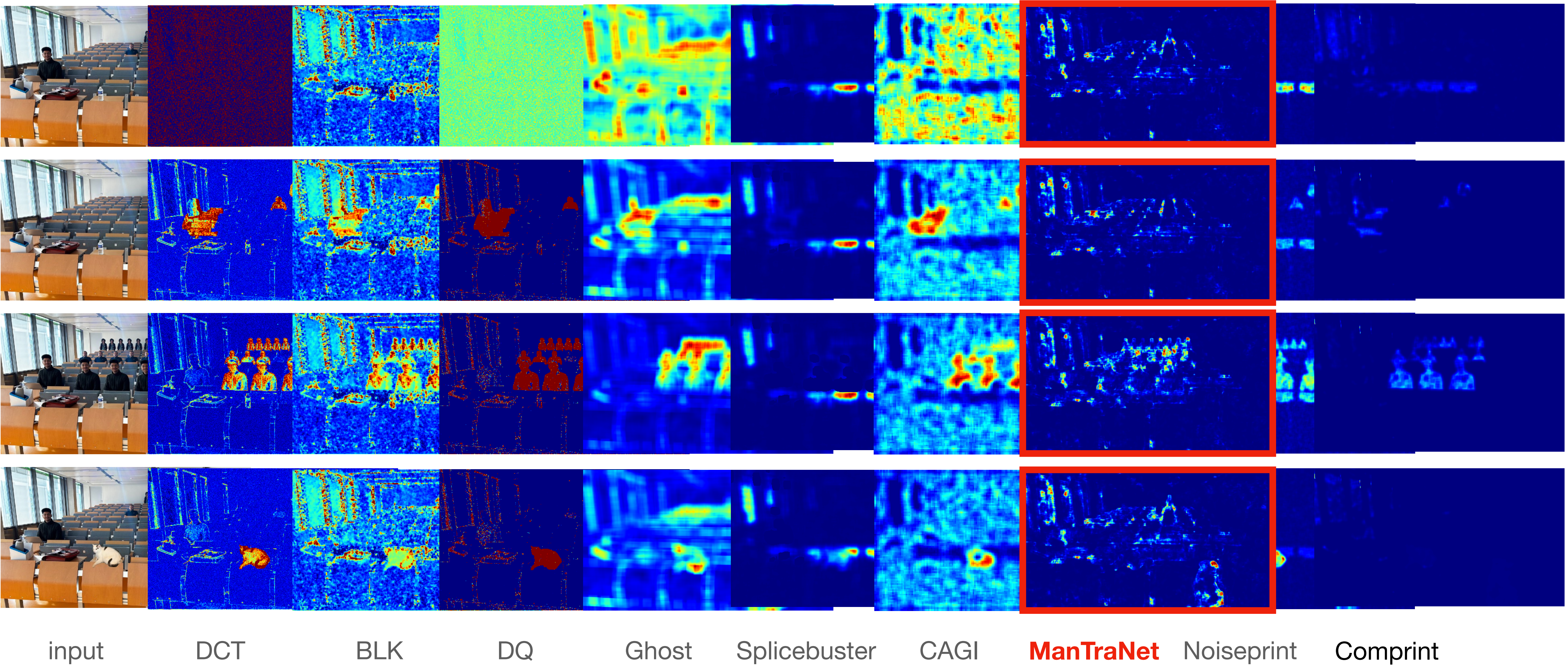


Image forgery detection

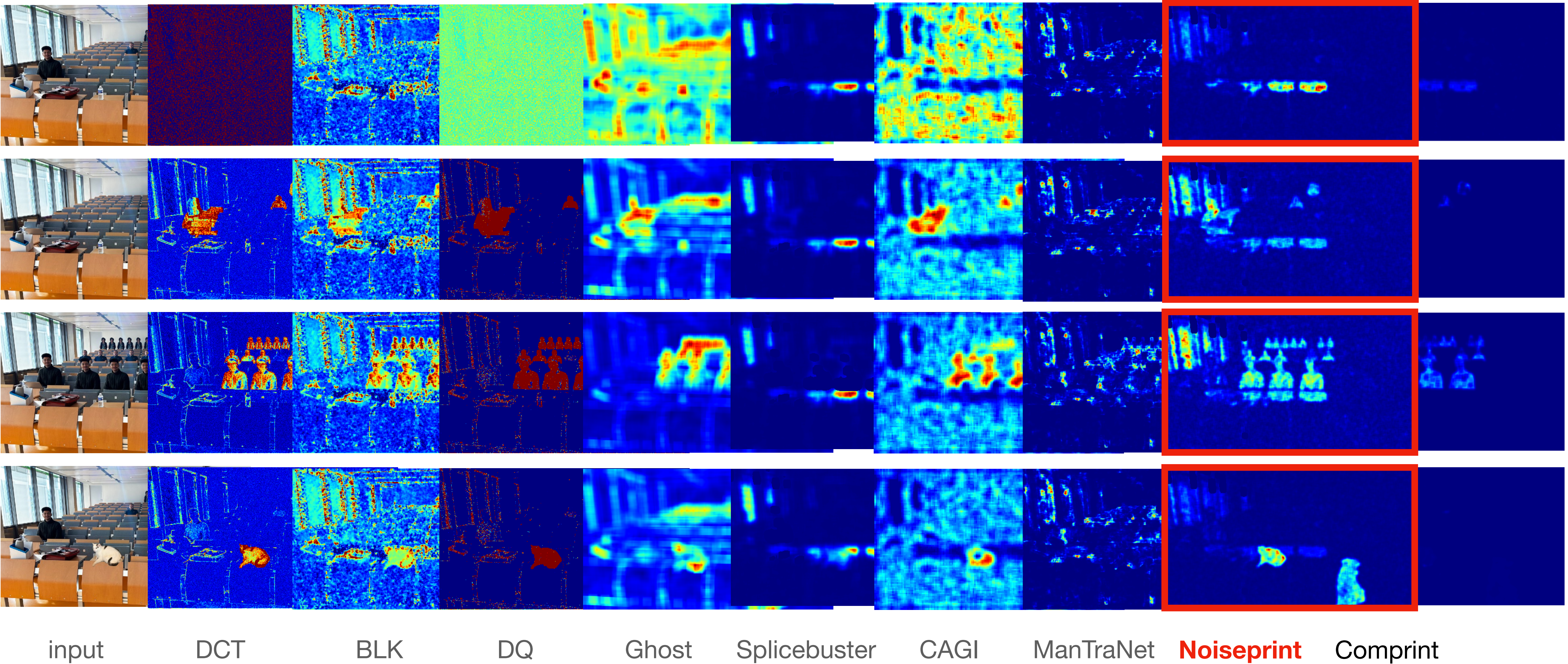
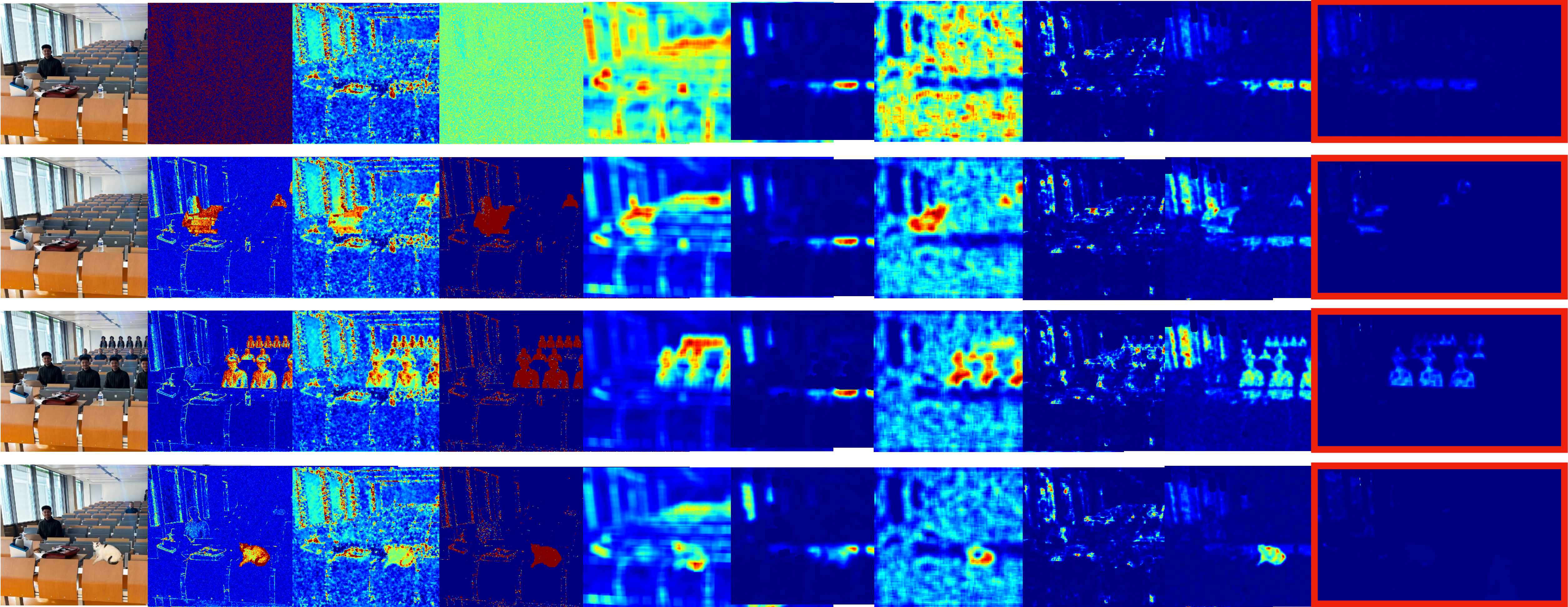


Image forgery detection

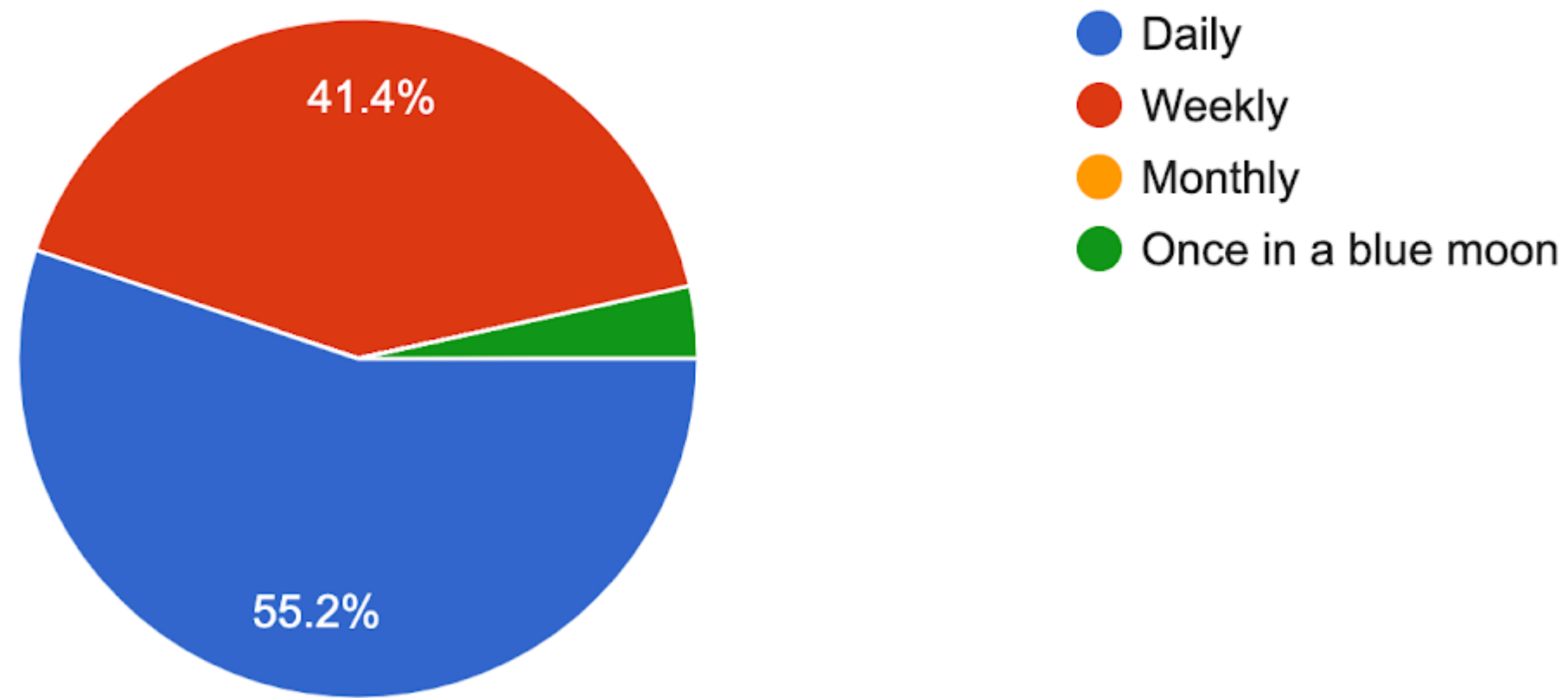


input DCT BLK DQ Ghost Splicebuster CAGI ManTraNet Noiseprint **Comprint**

Short survey among AFP fact-checkers during the Envisu4 project

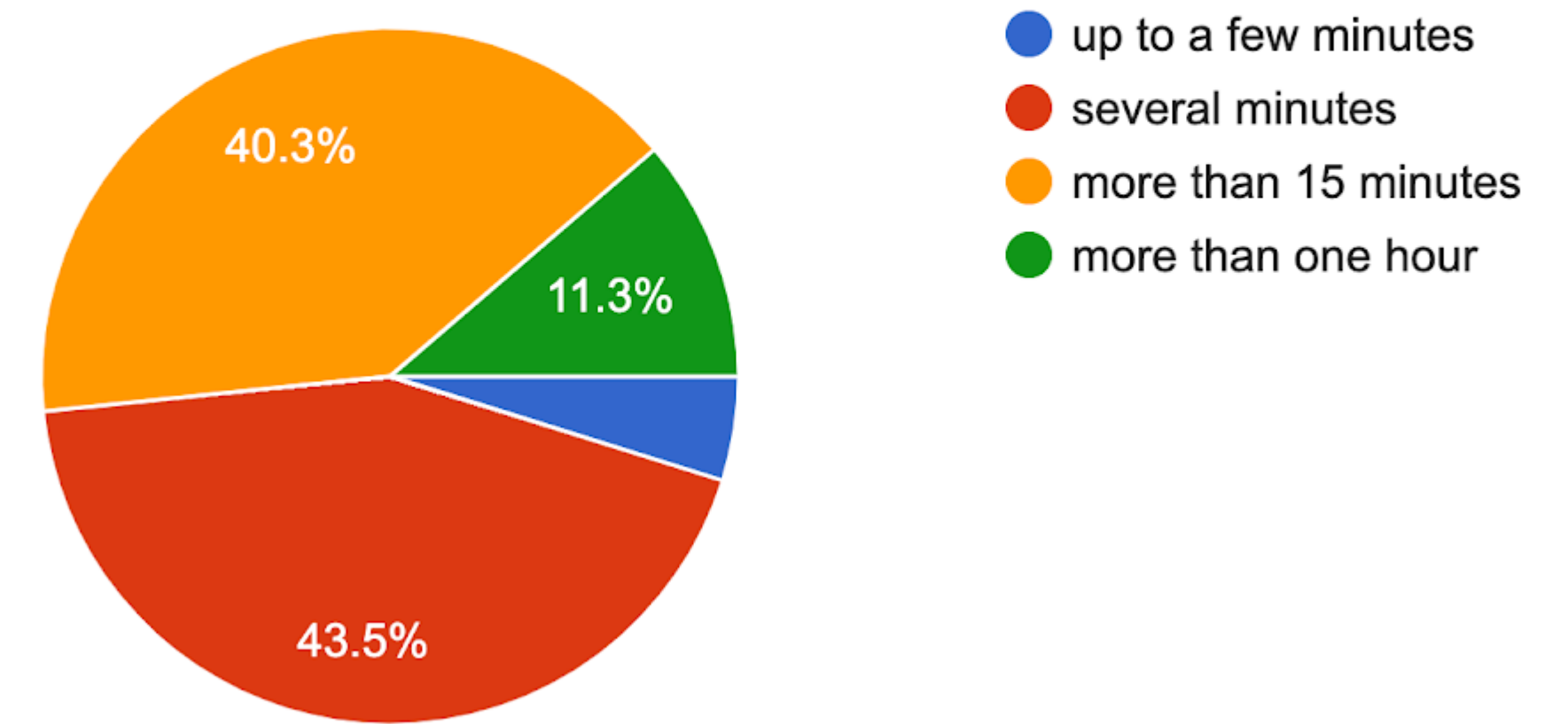
How often do you need to verify an image with respect to its authenticity ?

62 responses



How much time do you typically spend on the verification of an image ?

62 responses



- The tools are “interesting” and “attractive”, but they are also “difficult to use”.
- They wish “more explanation”, “less false positives” and “interpretability”.

"It's a bit hard to understand and therefore not as useful as it could be." - AFP journalist

What do we propose?

Automatic task-based algorithms with controlled false alarms.

Image processing pipeline

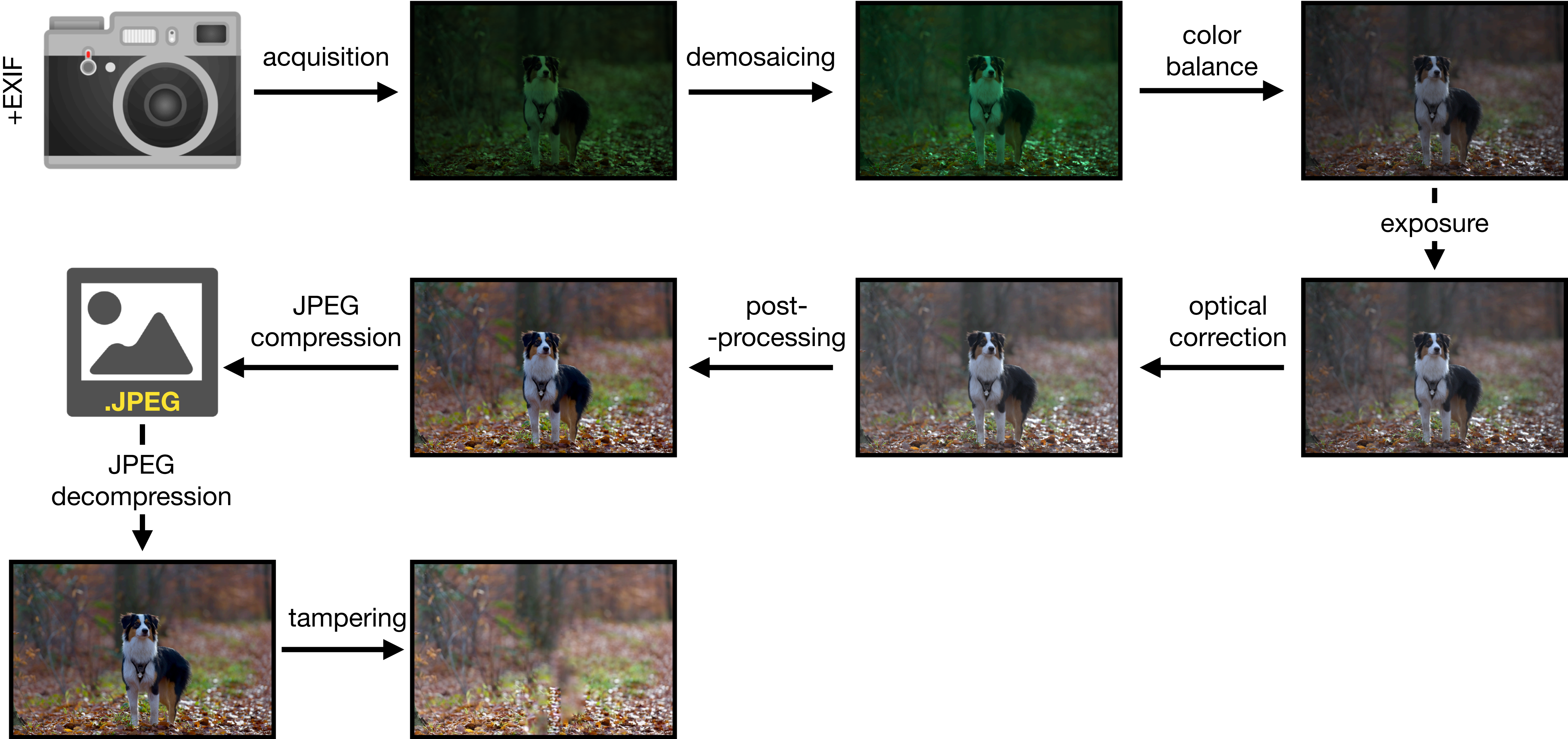


Image processing pipeline





Contribution of this thesis

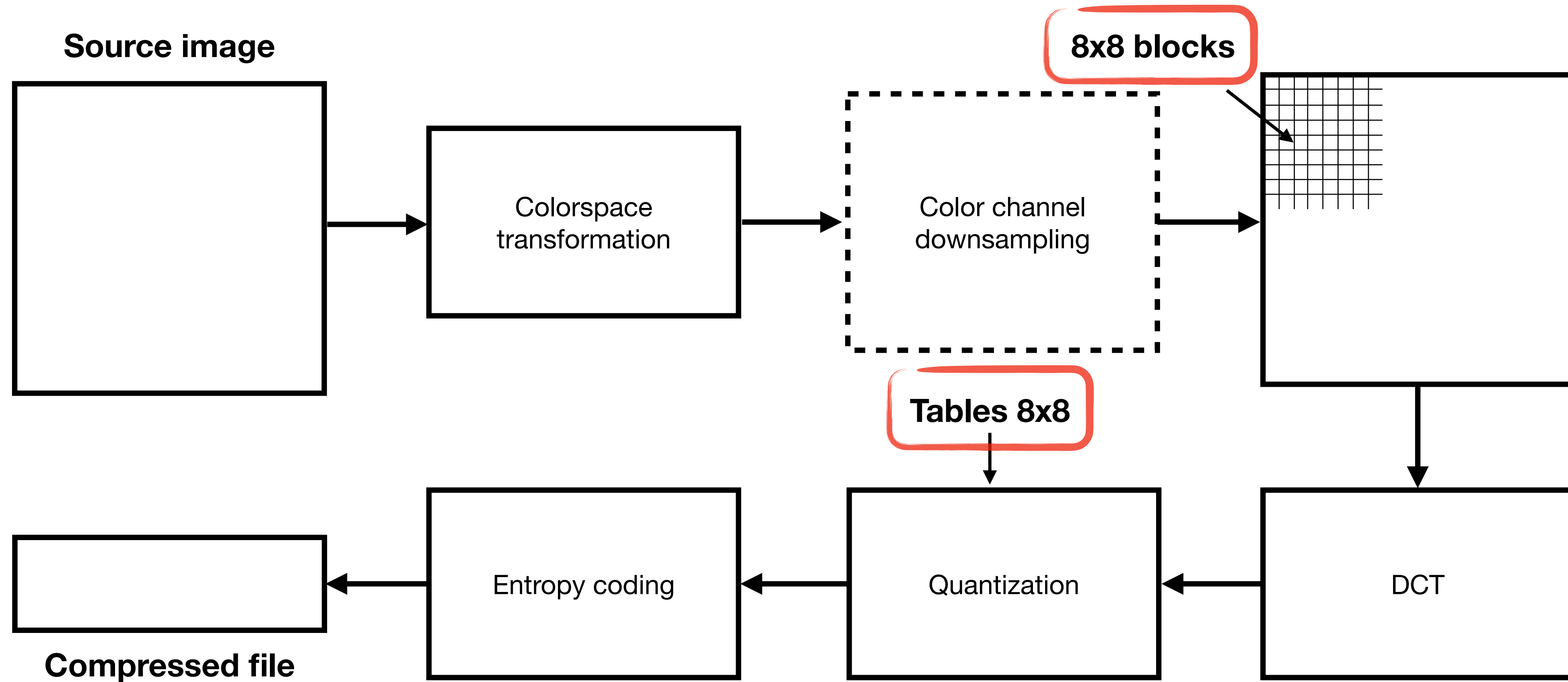
- **Local JPEG Grid Detection via Blocking Artifacts (GOD)**
Automatic JPEG grid detection with controlled false alarms, and its image forensic applications. T. Nikoukhah, R. Grompone von Gioi, M. Colom, and J.-M. Morel. IEEE Conference on Multimedia Information Processing and Retrieval (MIPR), 2018.
Local JPEG Grid Detector via Blocking Artifacts, a Forgery Detection Tool. T. Nikoukhah, M. Colom, J.-M. Morel, and R. Grompone von Gioi. Image Processing On Line, 2020.
- **Reliable Quantization Table Estimation (Qtable)**
A Reliable JPEG Quantization Table Estimator. T. Nikoukhah, M. Colom, J.-M. Morel, and R. Grompone von Gioi. Image Processing On Line, 2022.
- **Simple JPEG Grid Origin Detection (SimpleGOD)**
Détection de grille JPEG par compression simulée. T. Nikoukhah, M. Colom, J.-M. Morel, and R. Grompone von Gioi. GRETSI, 2019.
- **Local JPEG Grid Detection via the DCT zeros (ZERO)**
JPEG grid detection based on the number of DCT zeros and its application to automatic and localized forgery detection. T. Nikoukhah, J. Anger, T. Ehret, M. Colom, J.-M. Morel, and R. Grompone von Gioi. IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRw), 2019.
ZERO: a Local JPEG Grid Origin Detector Based on the Number of DCT Zeros and its Applications in Image Forensics. T. Nikoukhah, J. Anger, M. Colom, J.-M. Morel, and R. Grompone von Gioi. Image Processing On Line, 2021.
- **Non-Semantic Evaluation of Image Forensic Tools (Trace database)**
Non-Semantic Evaluation of Image Forensics Tools: Methodology and Database. Q. Bammey, T. Nikoukhah, M. Gardella, R. Grompone von Gioi, M. Colom, and J.-M. Morel. IEEE/CVF Winter Conference on Applications of Computer Vision (WACV), 2022.

Contribution of this thesis

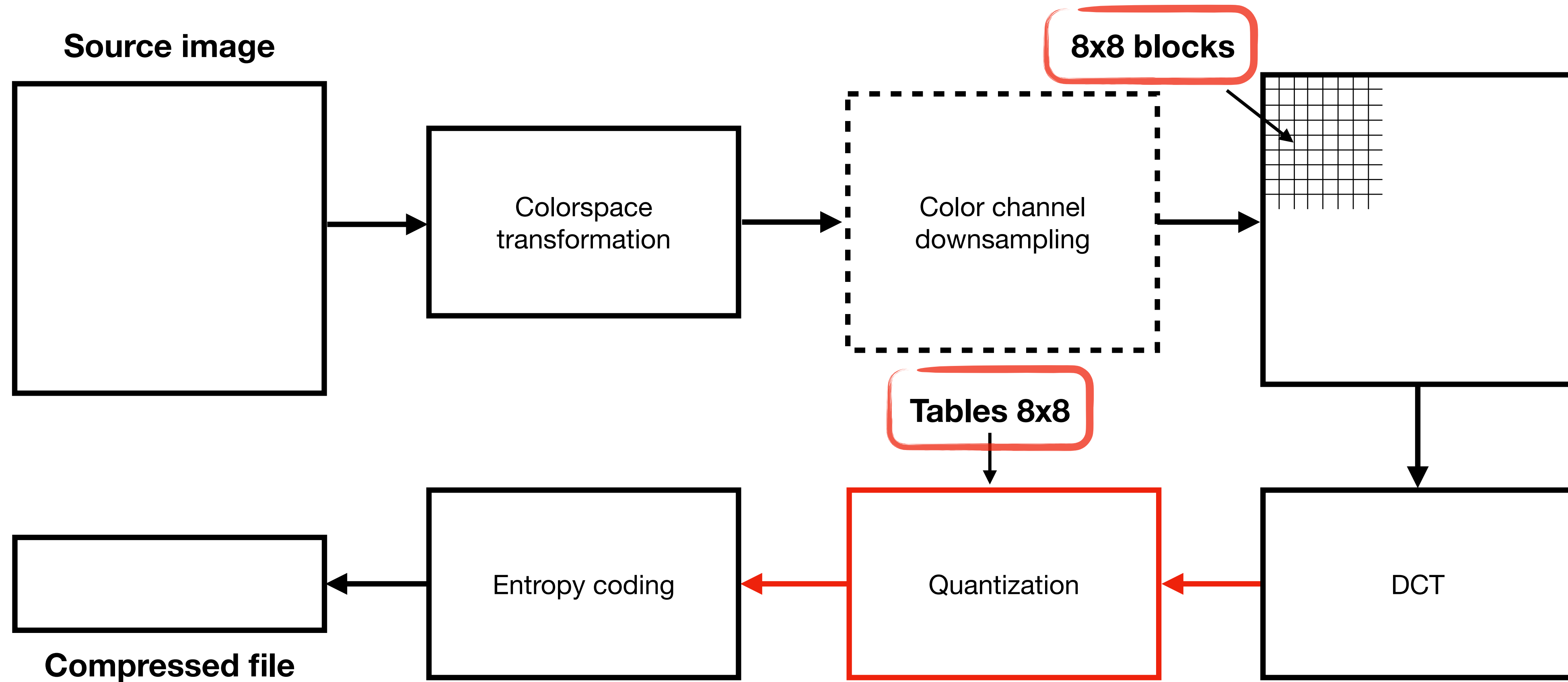
- Local JPEG Grid Detection via Blocking Artifacts (GOD)
Automatic JPEG grid detection with controlled false alarms, and its image forensic applications. T. Nikoukhah, R. Grompone von Gioi, M. Colom, and J.-M. Morel. IEEE Conference on Multimedia Information Processing and Retrieval (MIPR), 2018.
Local JPEG Grid Detector via Blocking Artifacts, a Forgery Detection Tool. T. Nikoukhah, M. Colom, J.-M. Morel, and R. Grompone von Gioi. Image Processing On Line, 2020.
- Reliable Quantization Table Estimation (Qtable)
A Reliable JPEG Quantization Table Estimator. T. Nikoukhah, M. Colom, J.-M. Morel, and R. Grompone von Gioi. Image Processing On Line, 2022.
- Simple JPEG Grid Origin Detection (SimpleGOD)
Détection de grille JPEG par compression simulée. T. Nikoukhah, M. Colom, J.-M. Morel, and R. Grompone von Gioi. GRETSI, 2019.
- Local JPEG Grid Detection via the DCT zeros (ZERO)
JPEG grid detection based on the number of DCT zeros and its application to automatic and localized forgery detection. T. Nikoukhah, J. Anger, T. Ehret, M. Colom, J.-M. Morel, and R. Grompone von Gioi. IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRw), 2019.
ZERO: a Local JPEG Grid Origin Detector Based on the Number of DCT Zeros and its Applications in Image Forensics. T. Nikoukhah, J. Anger, M. Colom, J.-M. Morel, and R. Grompone von Gioi. Image Processing On Line, 2021.
- Non-Semantic Evaluation of Image Forensic Tools (Trace database)
Non-Semantic Evaluation of Image Forensics Tools: Methodology and Database. Q. Bammey, T. Nikoukhah, M. Gardella, R. Grompone von Gioi, M. Colom, and J.-M. Morel. IEEE/CVF Winter Conference on Applications of Computer Vision (WACV), 2022.



JPEG compression pipeline



JPEG compression pipeline



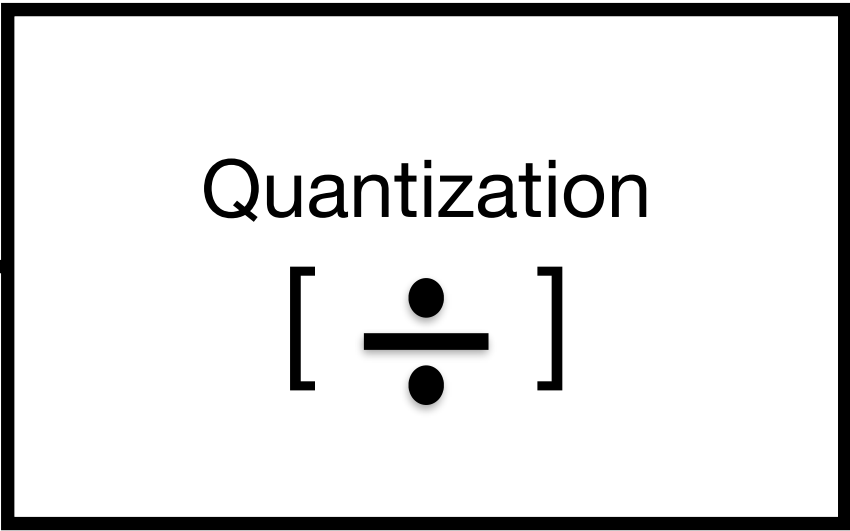
JPEG compression pipeline

Quantization table

16	11	10	16	24	40	51	61
12	12	14	19	26	58	60	55
14	13	16	24	40	57	69	56
14	17	22	29	51	87	80	62
18	22	37	56	68	109	103	77
24	35	55	64	81	104	113	92
49	64	78	87	103	121	120	101
72	92	95	98	112	100	103	99

6	-3	-6	2	2	-1	0	0
0	-3	4	1	1	0	0	0
-3	1	5	-1	-1	0	0	0
-4	1	2	-1	0	0	0	0
1	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0

Quantized DCT coefficients



102	-33	-58	35	58	-51	15	-12
5	-34	49	18	27	1	-5	3
-46	14	80	-35	-50	19	7	-18
-53	21	34	-20	2	34	36	12
9	-2	9	-5	-32	-15	45	37
-8	15	-16	7	-8	11	4	7
19	-28	-2	-26	-2	7	-44	-21
18	25	-12	-44	35	48	-37	-3

DCT coefficients

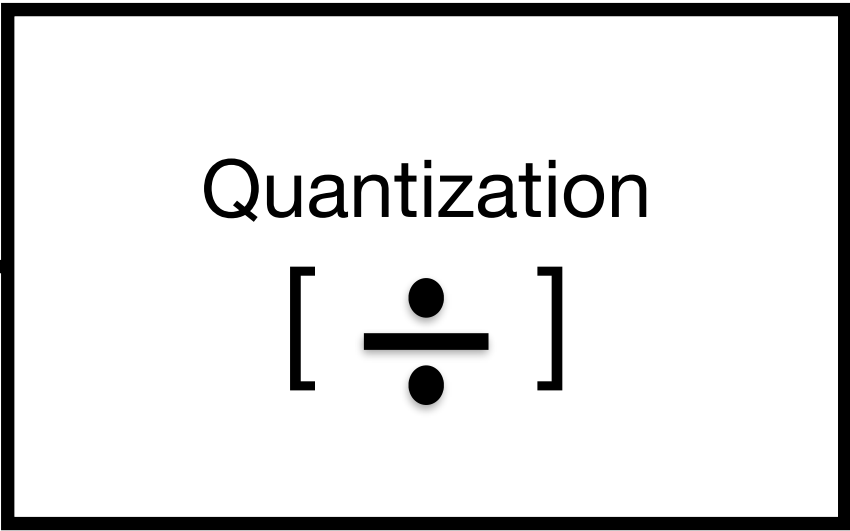
JPEG compression pipeline

Quantization table

16	11	10	16	24	40	51	61
12	12	14	19	26	58	60	55
14	13	16	24	40	57	69	56
14	17	22	29	51	87	80	62
18	22	37	56	68	109	103	77
24	35	55	64	81	104	113	92
49	64	78	87	103	121	120	101
72	92	95	98	112	100	103	99

6	-3	-6	2	2	1	0	0
0	-3	4	1	1	0	0	0
-3	1	5	-1	-1	0	0	0
-4	1	2	-1	0	0	0	0
1	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0

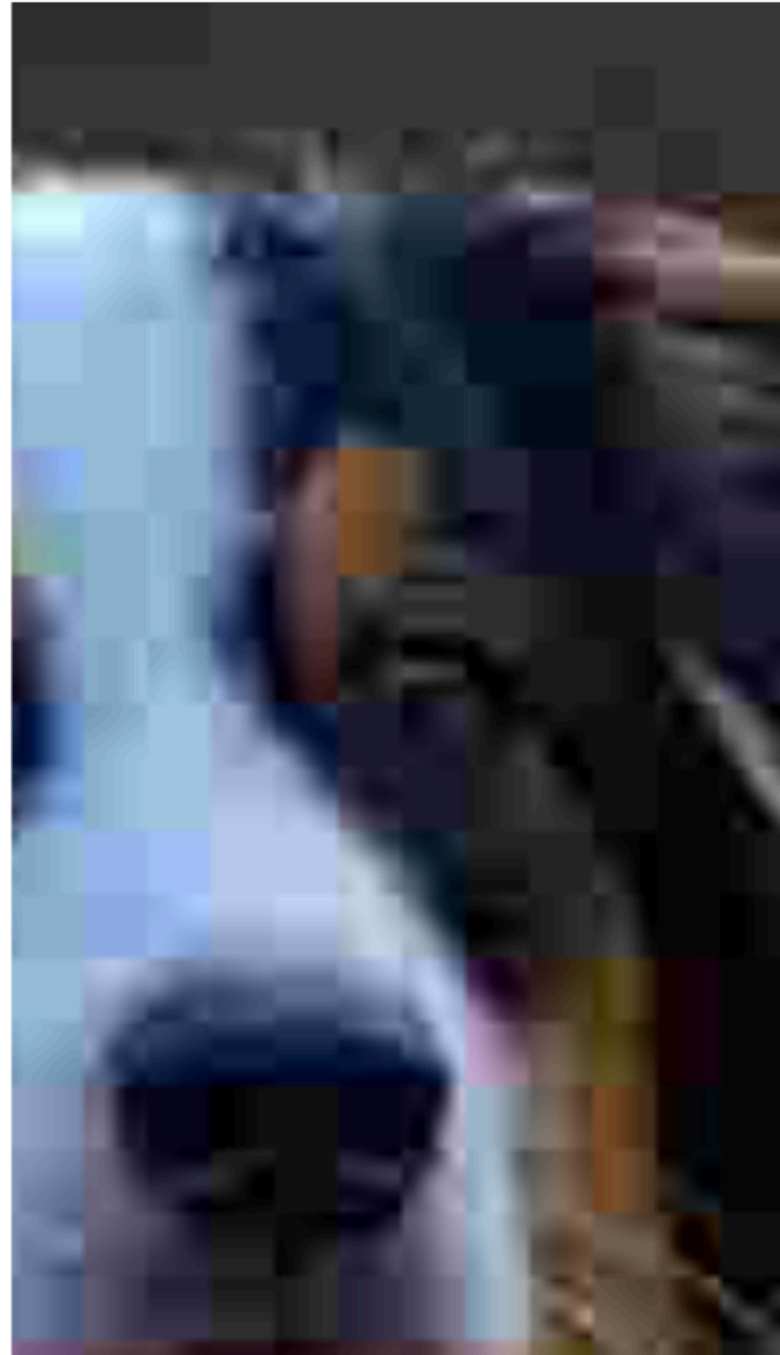
Quantized DCT coefficients



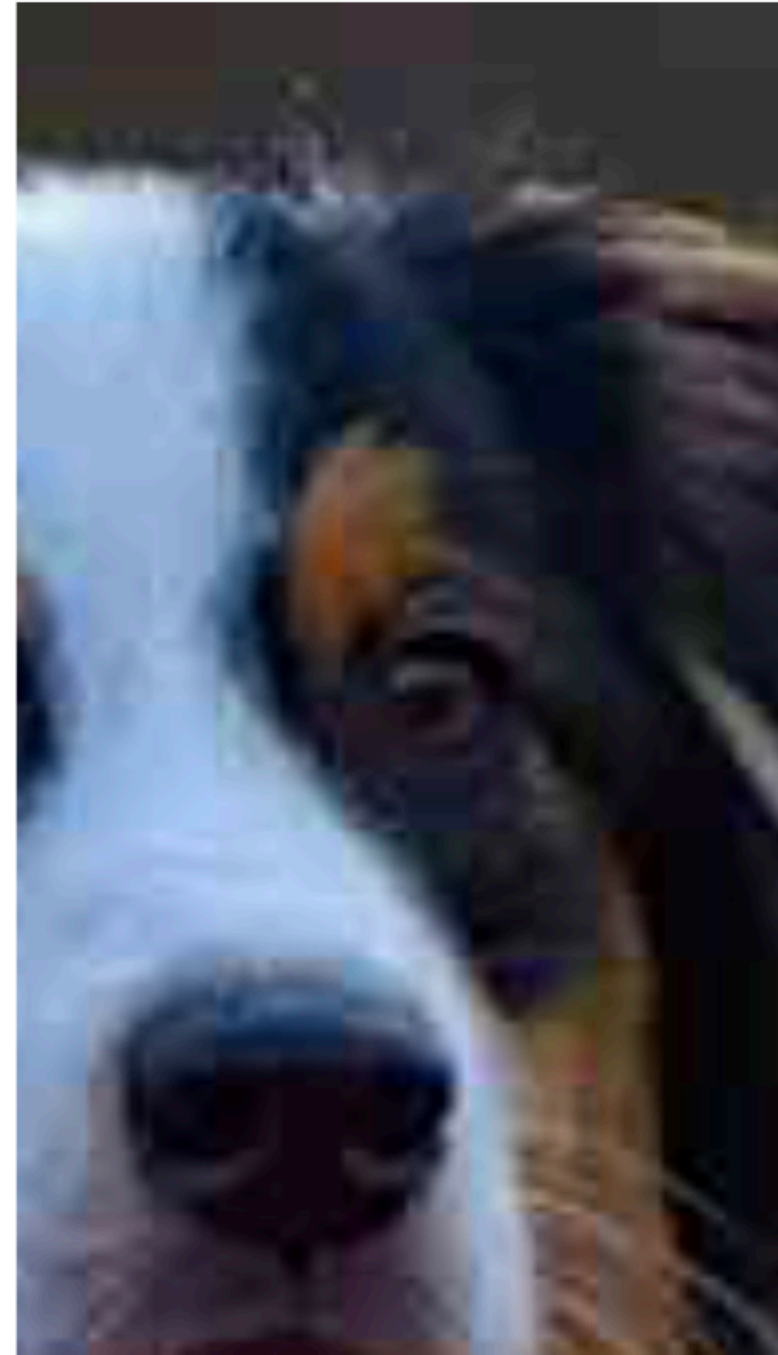
102	-33	-58	35	58	-51	15	-12
5	-34	49	18	27	1	-5	3
-46	14	80	-35	-50	19	7	-18
-53	21	34	-20	2	34	36	12
9	-2	9	-5	-32	-15	45	37
-8	15	-16	7	-8	11	4	7
19	-28	-2	-26	-2	7	-44	-21
18	25	-12	-44	35	48	-37	-3

DCT coefficients

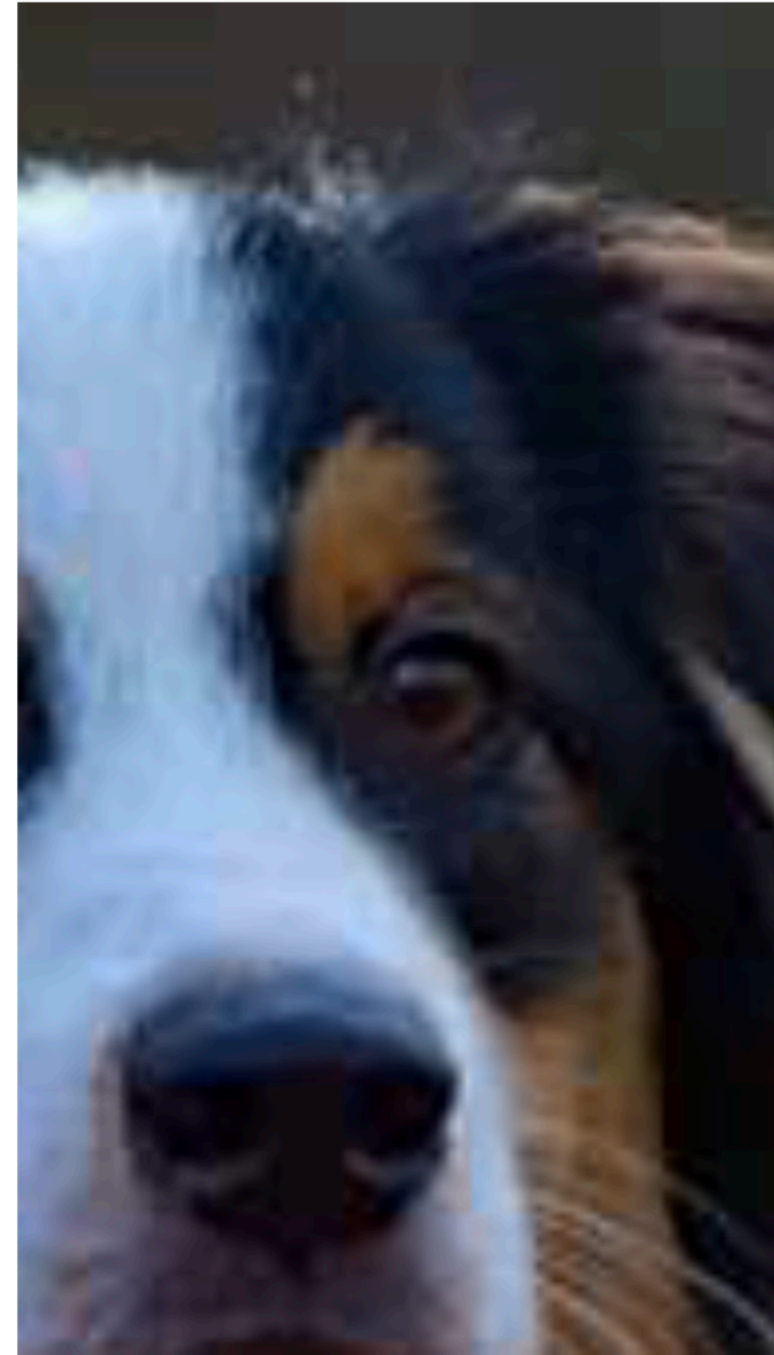
JPEG compression quality



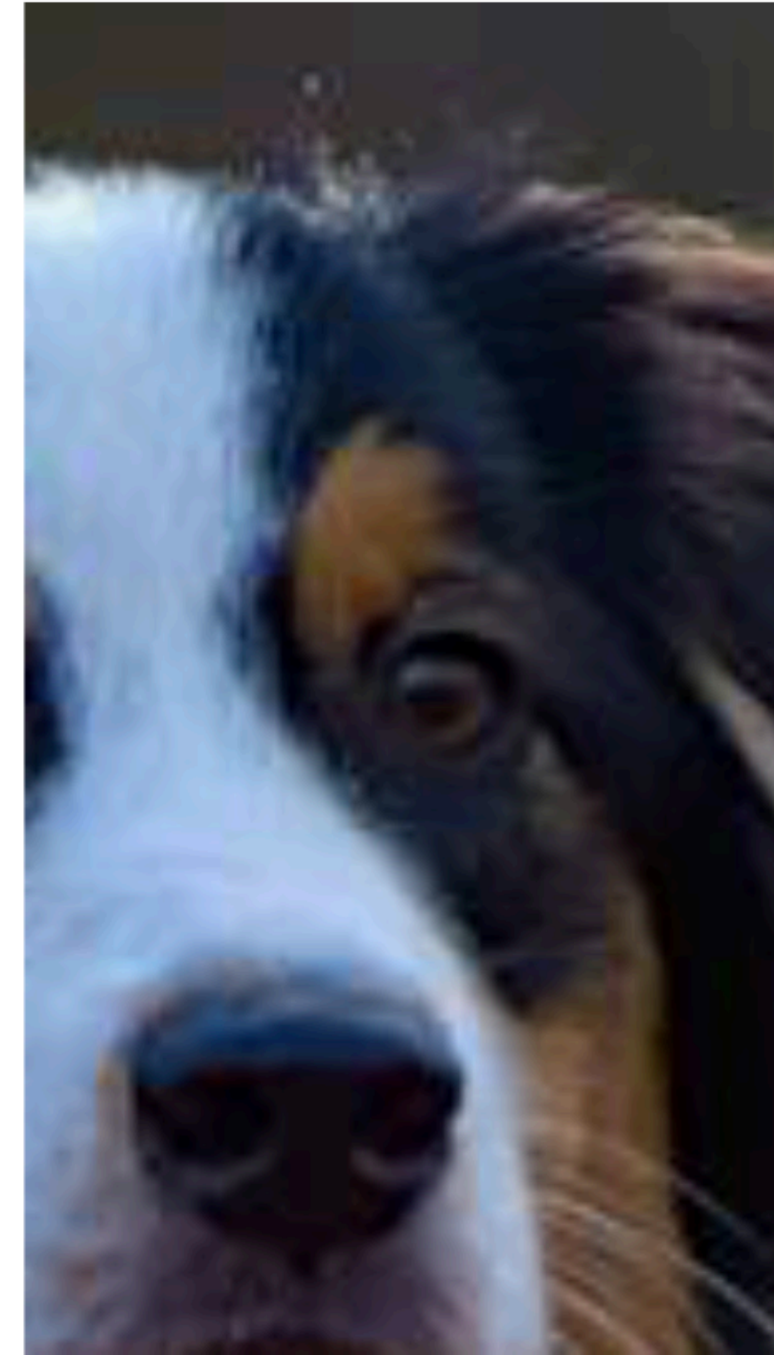
Q10 :
398Ko



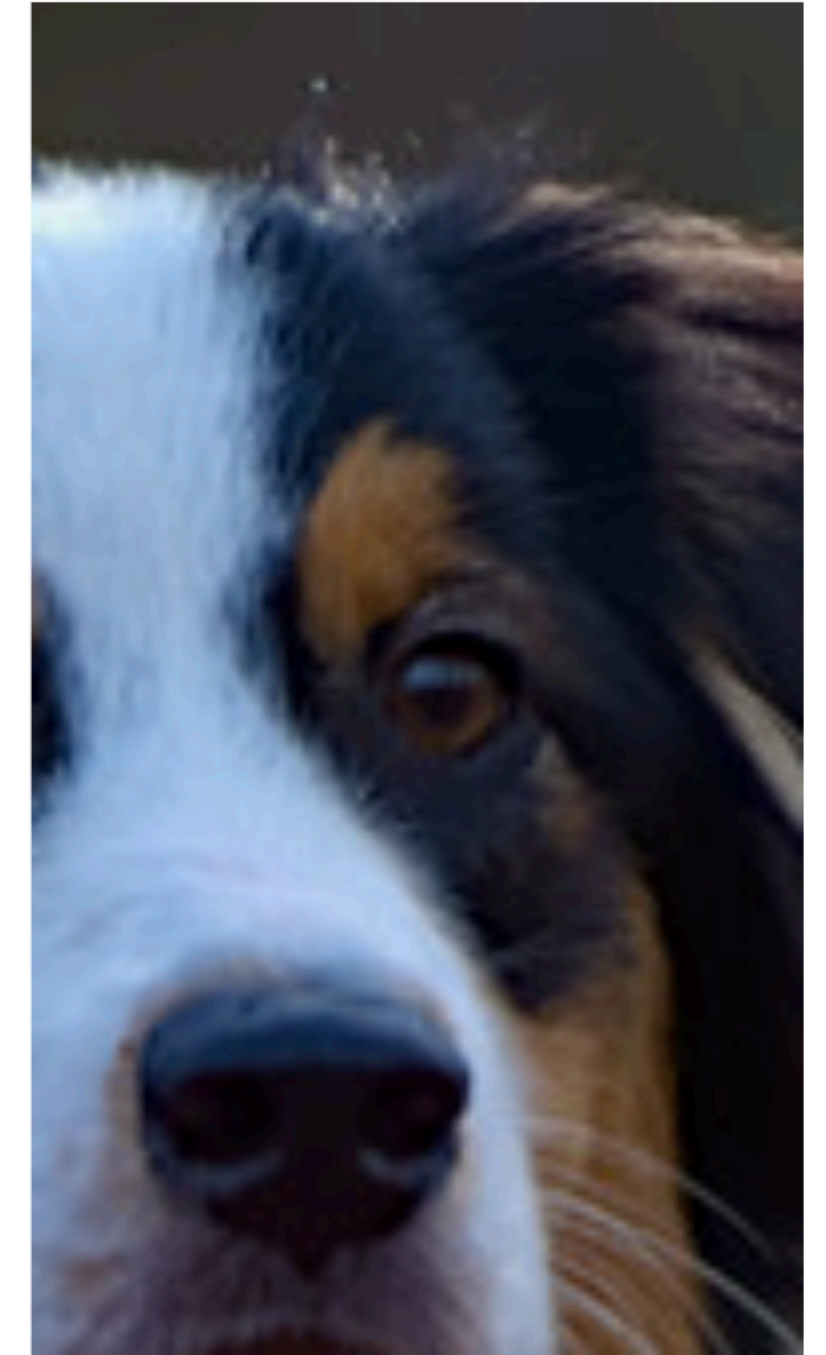
Q30 :
793Ko



Q50 :
1,2Mo



Q70 :
2,0Mo

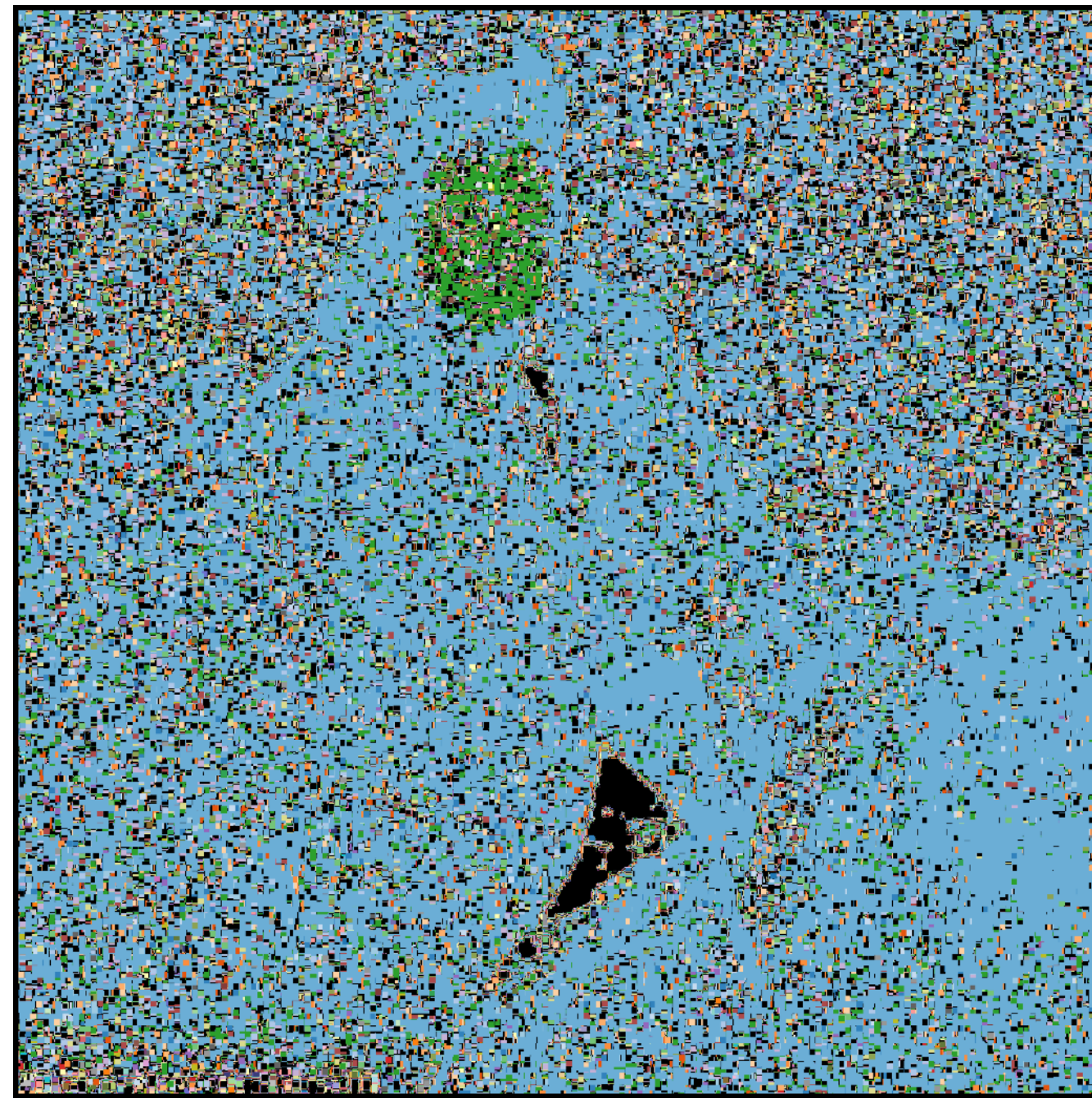


Q90 :
5,3Mo

ZERO



Forged image from @GuillaumeTC



Intermediate step



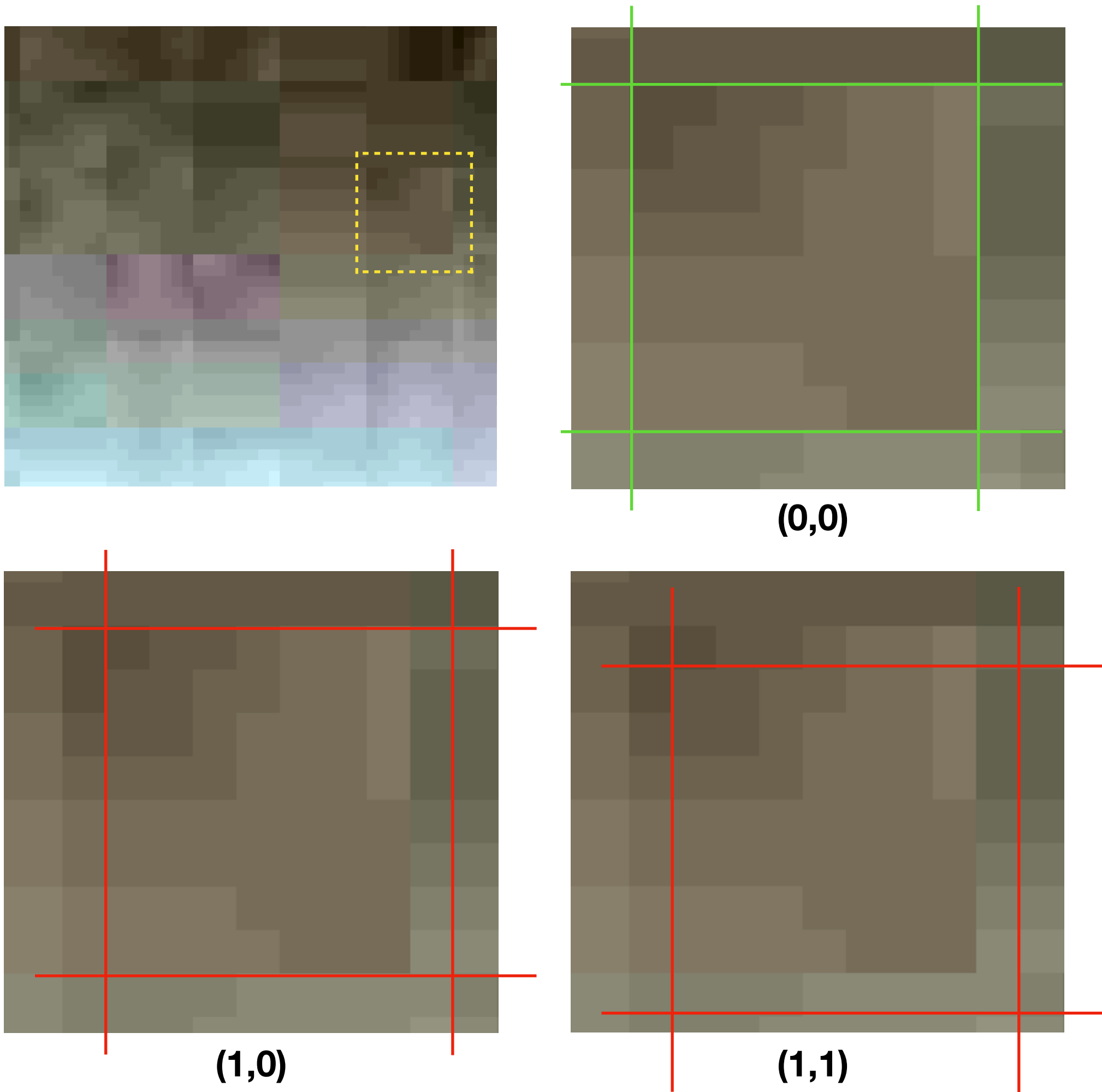
Detection result

ZERO

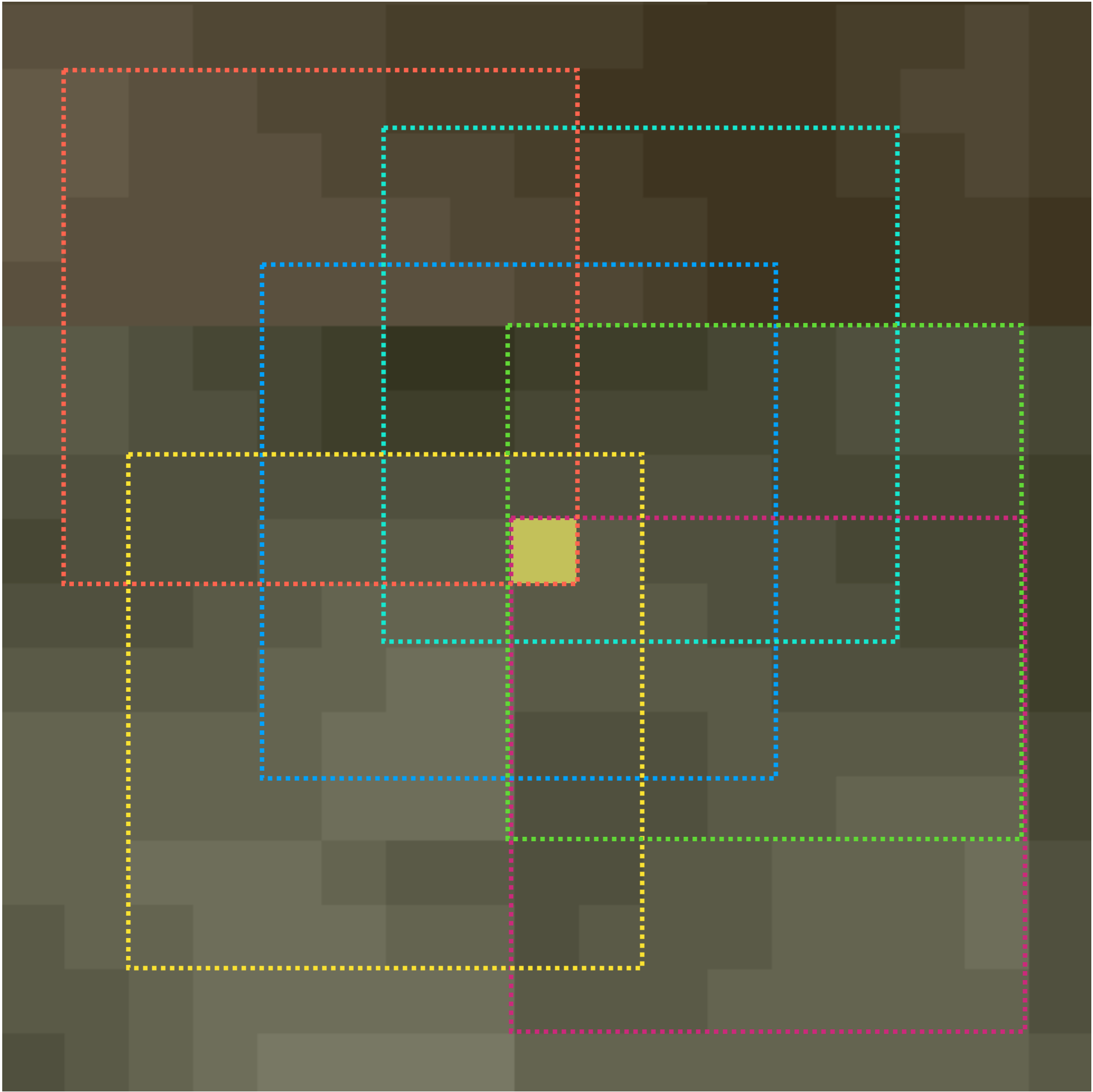
- Has the image undergone JPEG compression?
- What is the grid origin?
- Are there any anomalies in the JPEG grid of the image?

JPEG blocking artifact

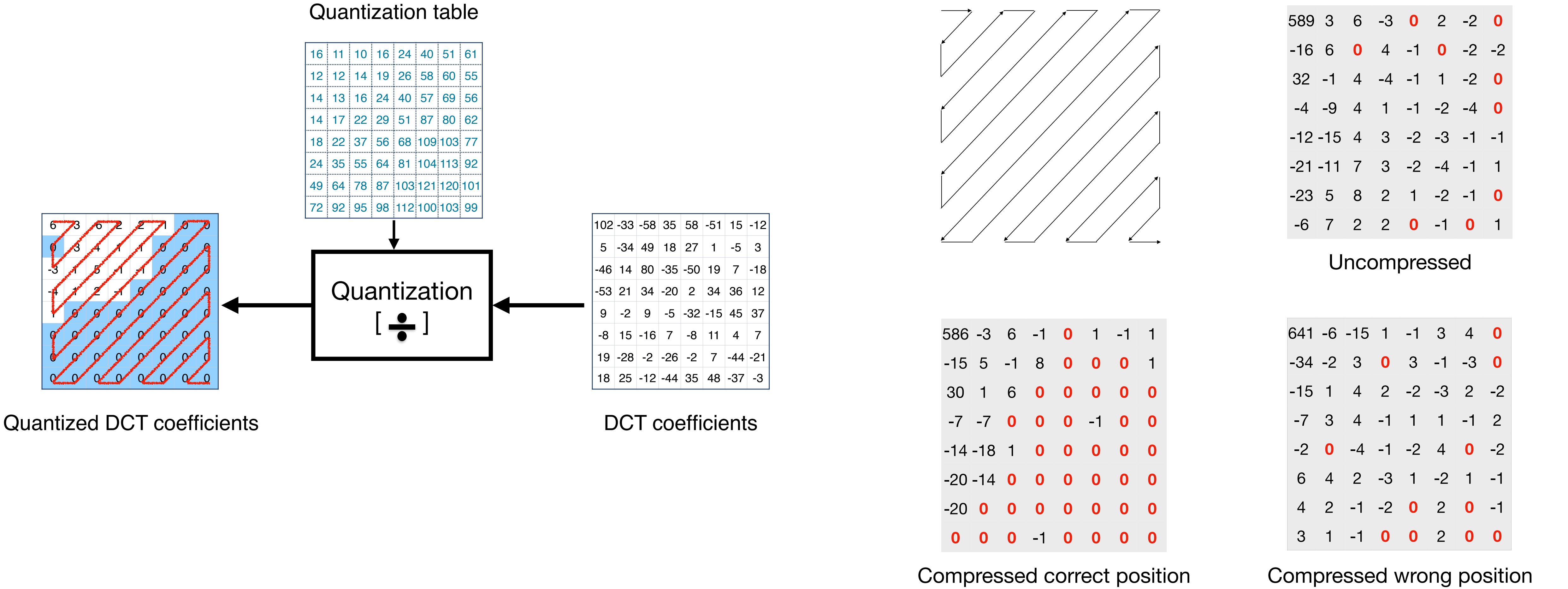
JPEG grid origin



Each pixel votes for a grid origin



JPEG compression puts values to zero



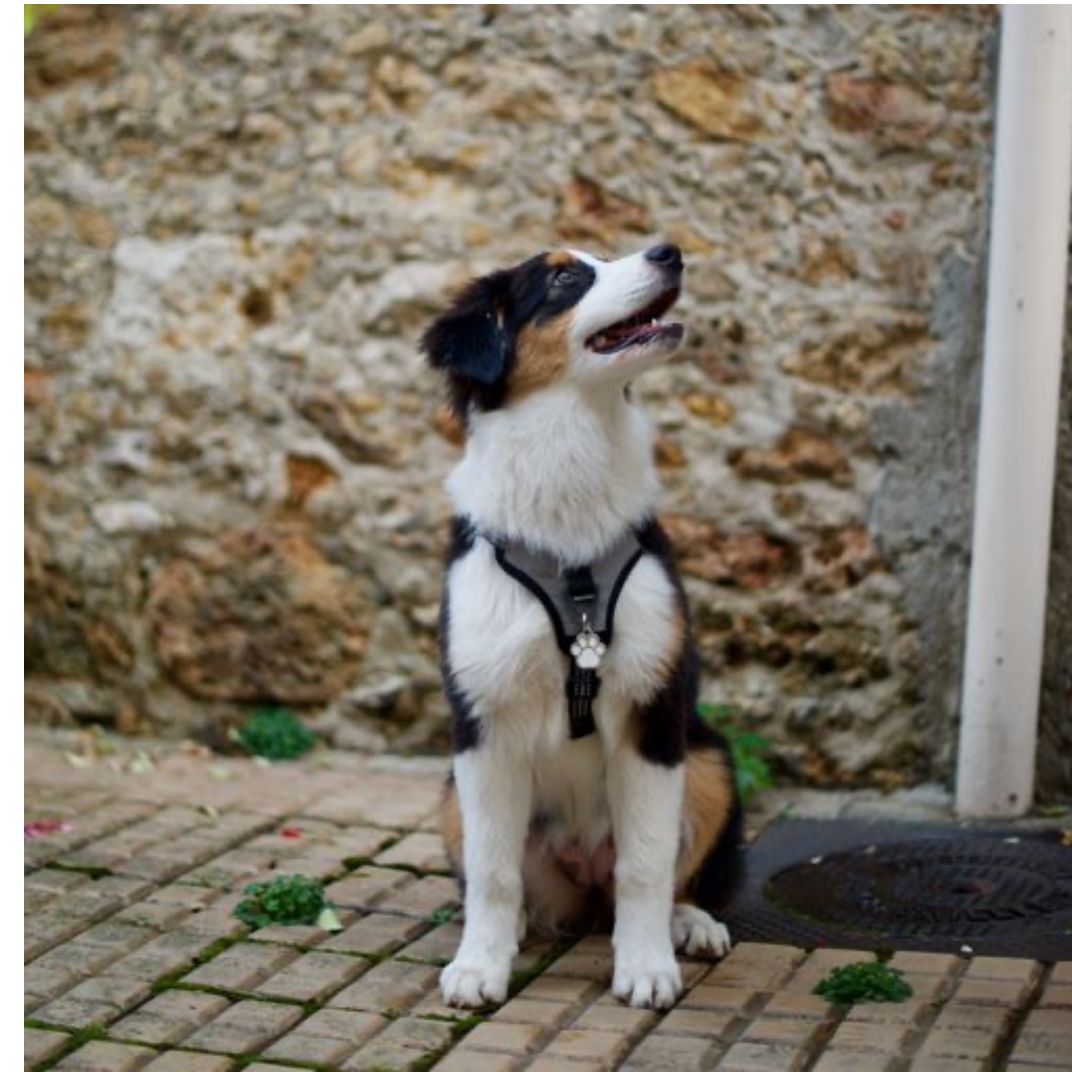
Uncompressed



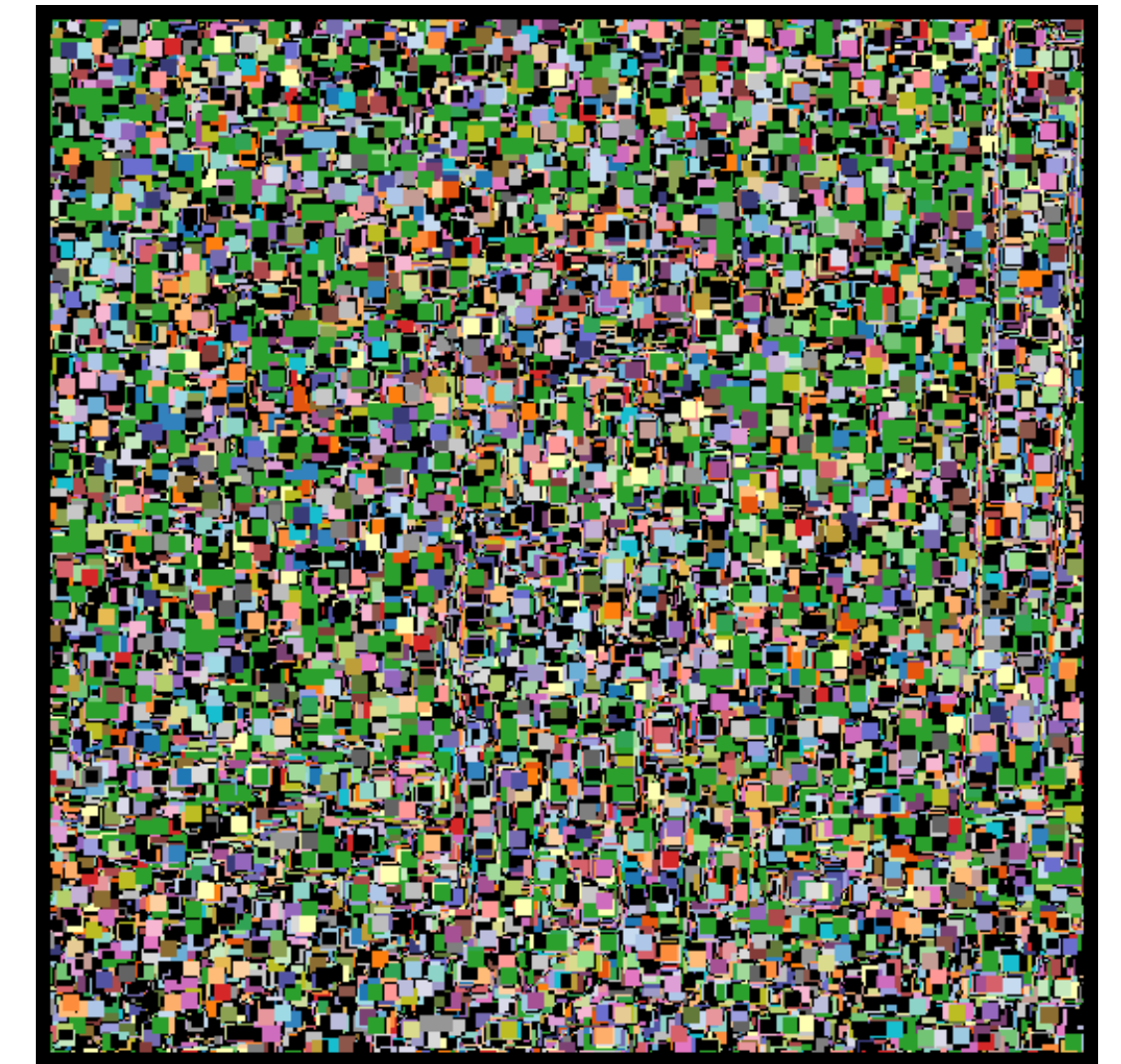
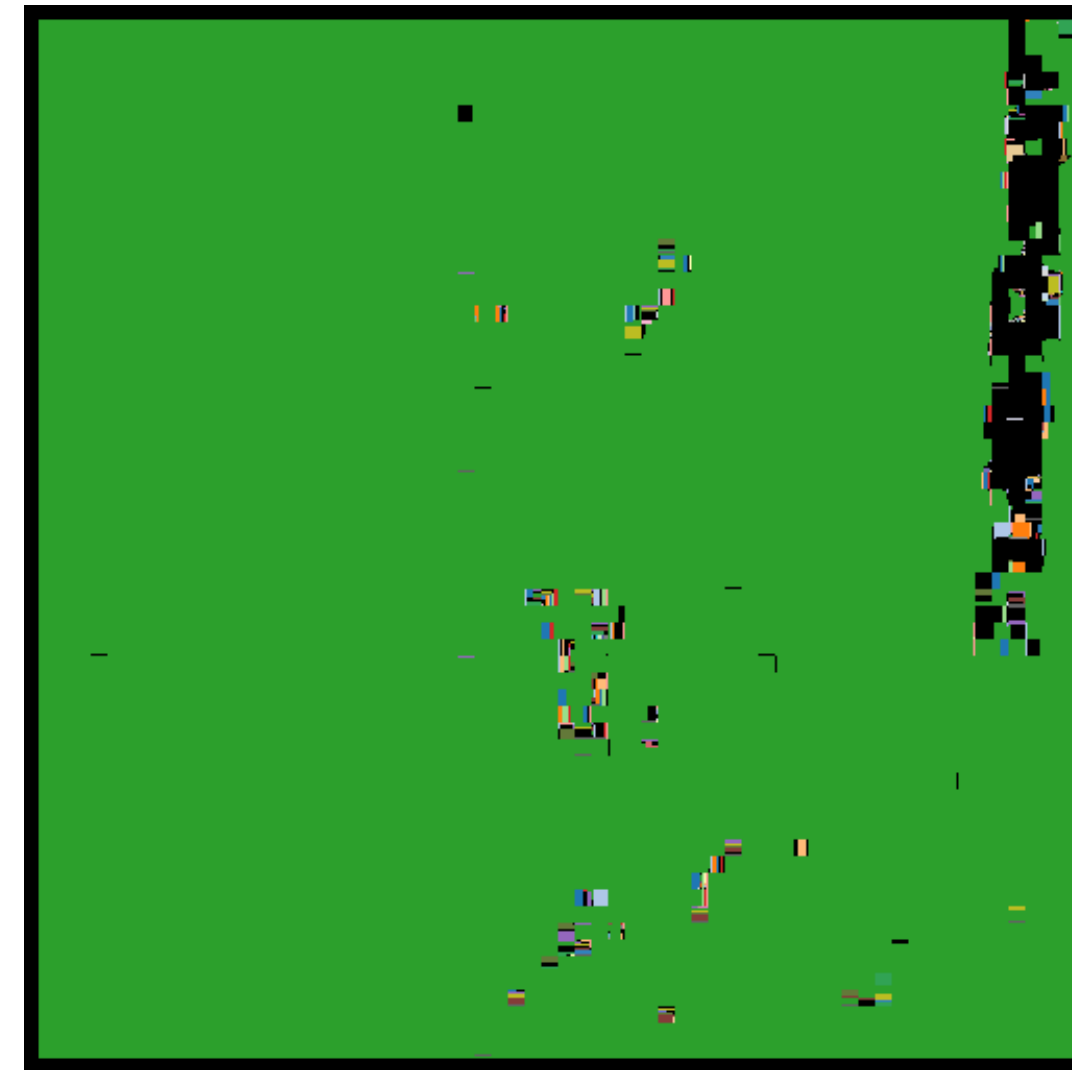
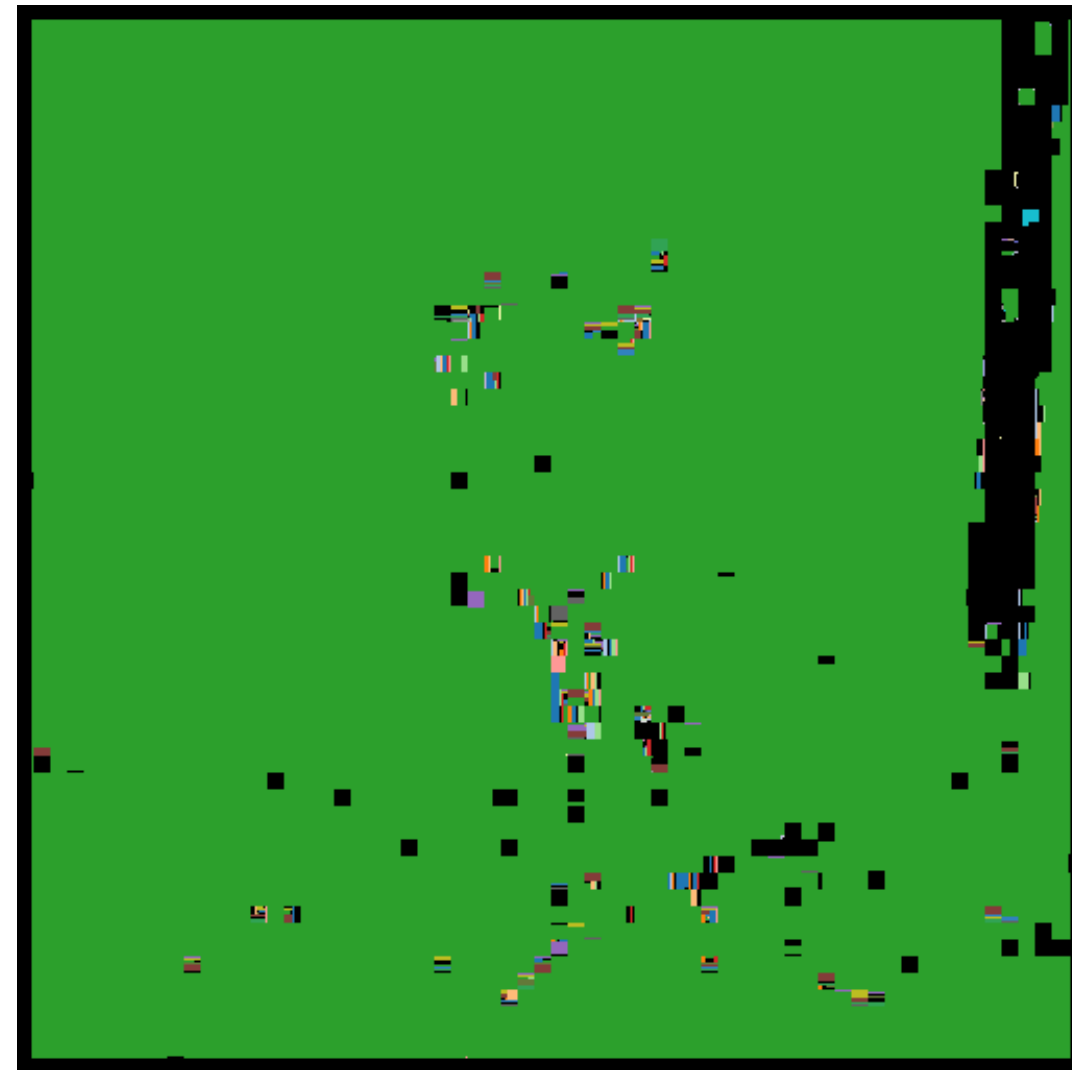
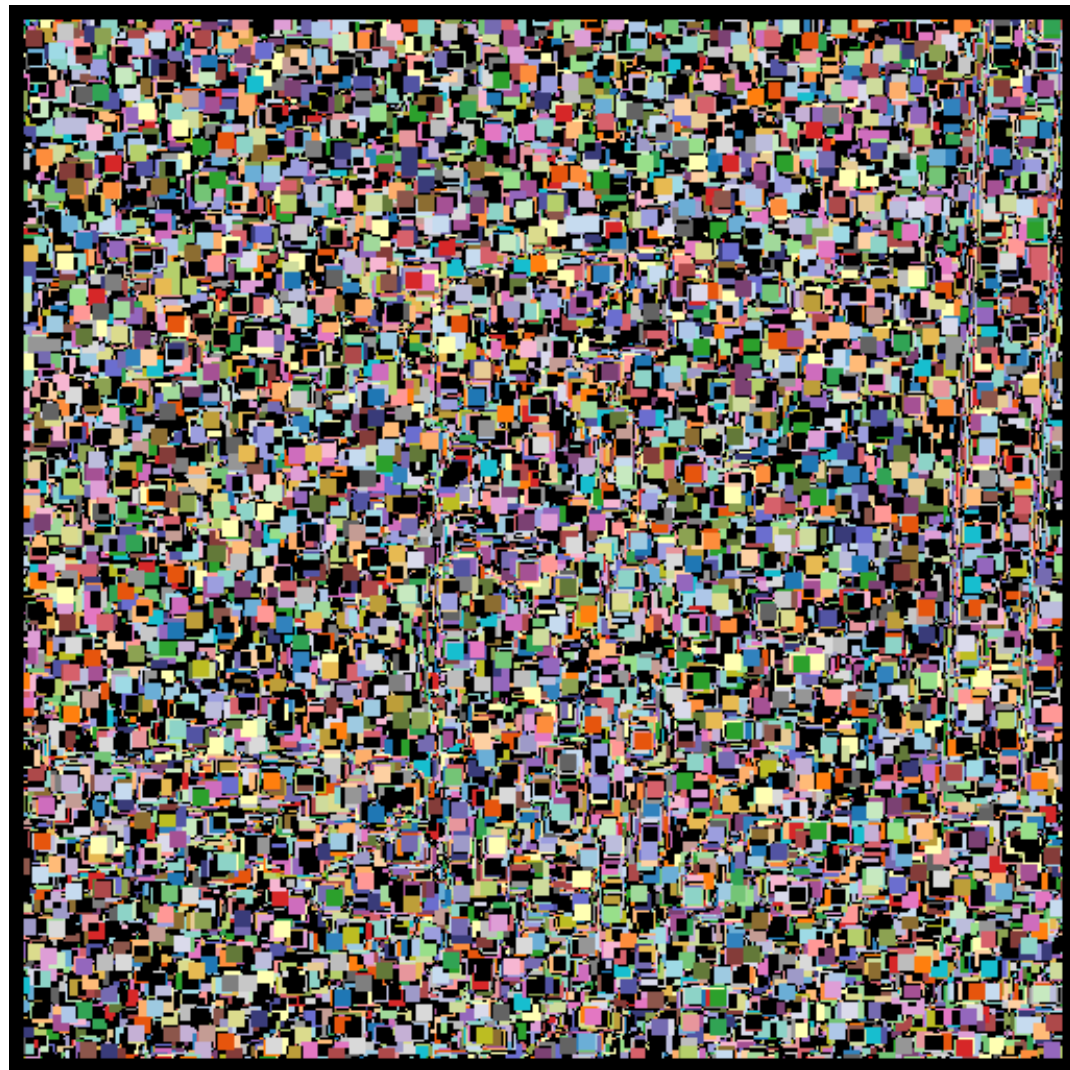
Compressed (Q=50)



Compressed (Q=80)



Compressed (Q=99)



Each color represents a vote. Black corresponds to a non-valid vote, in case of a tie for example.

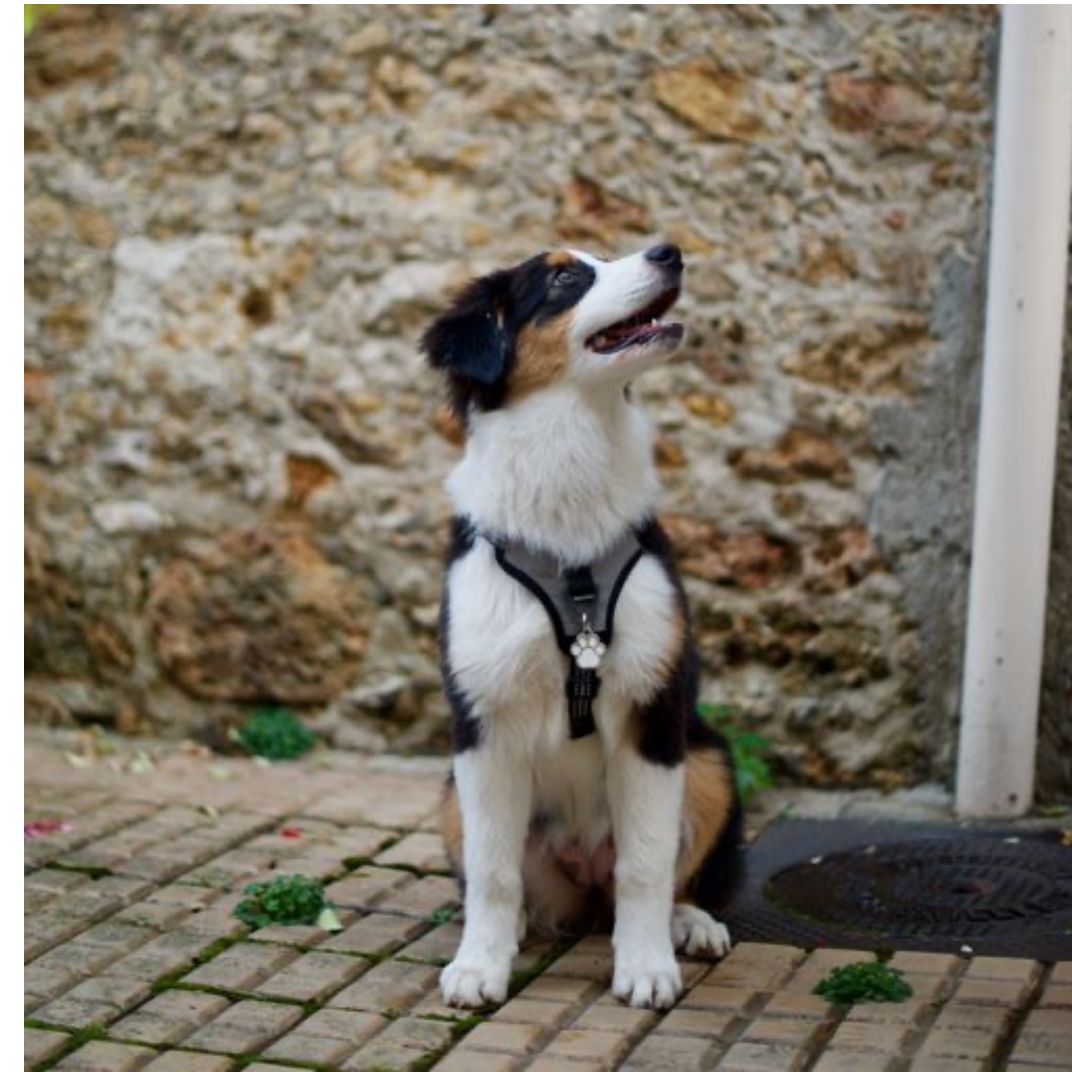
Uncompressed



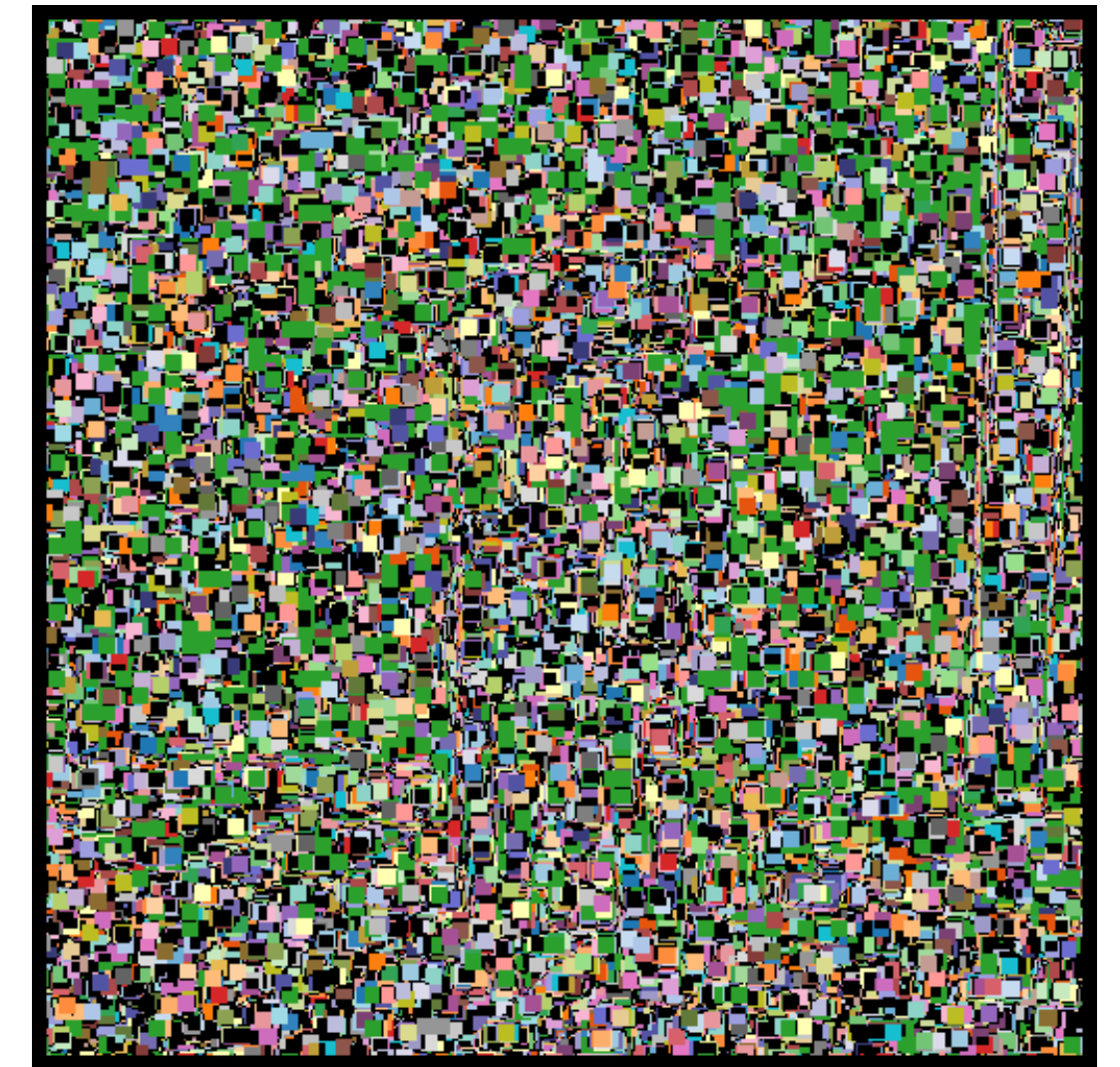
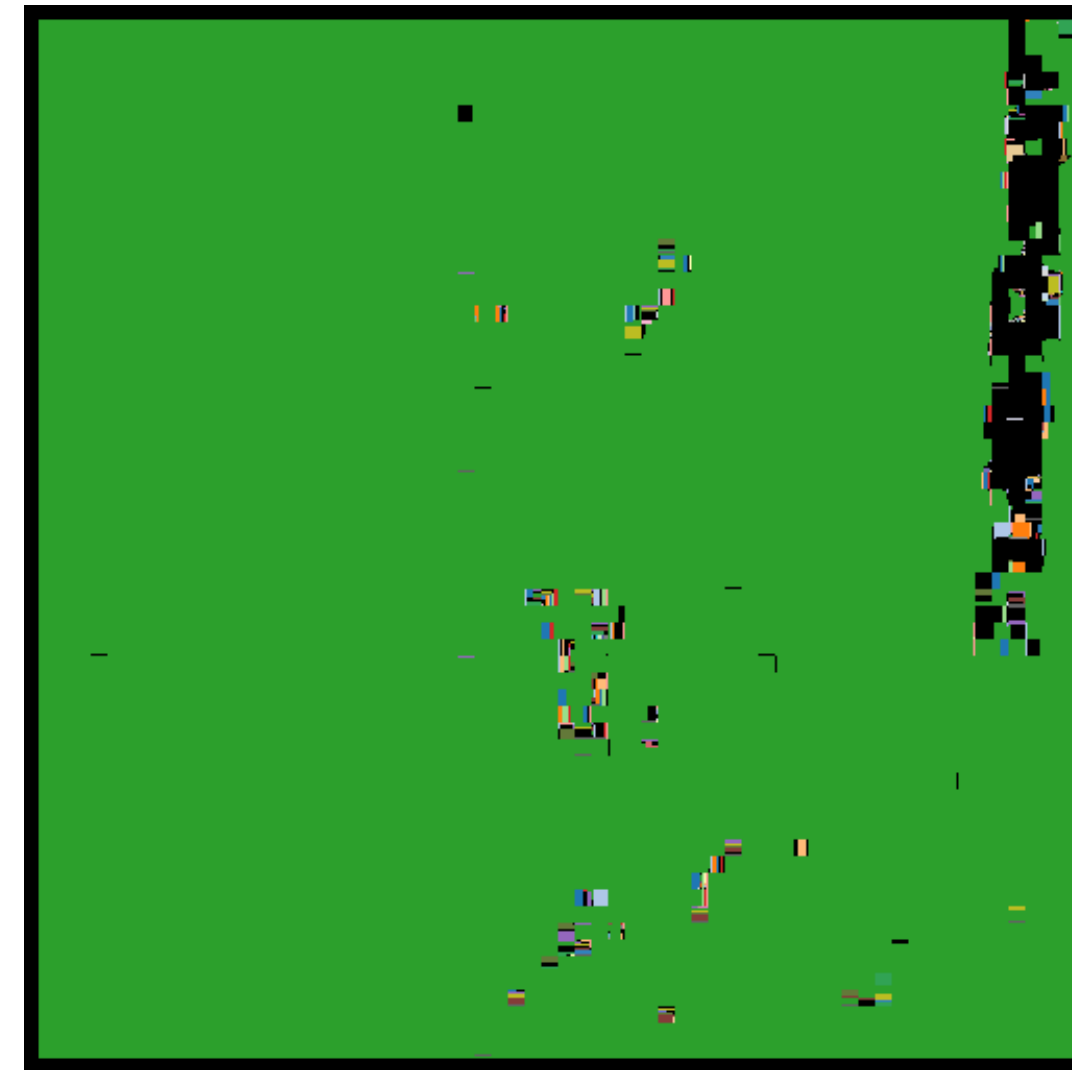
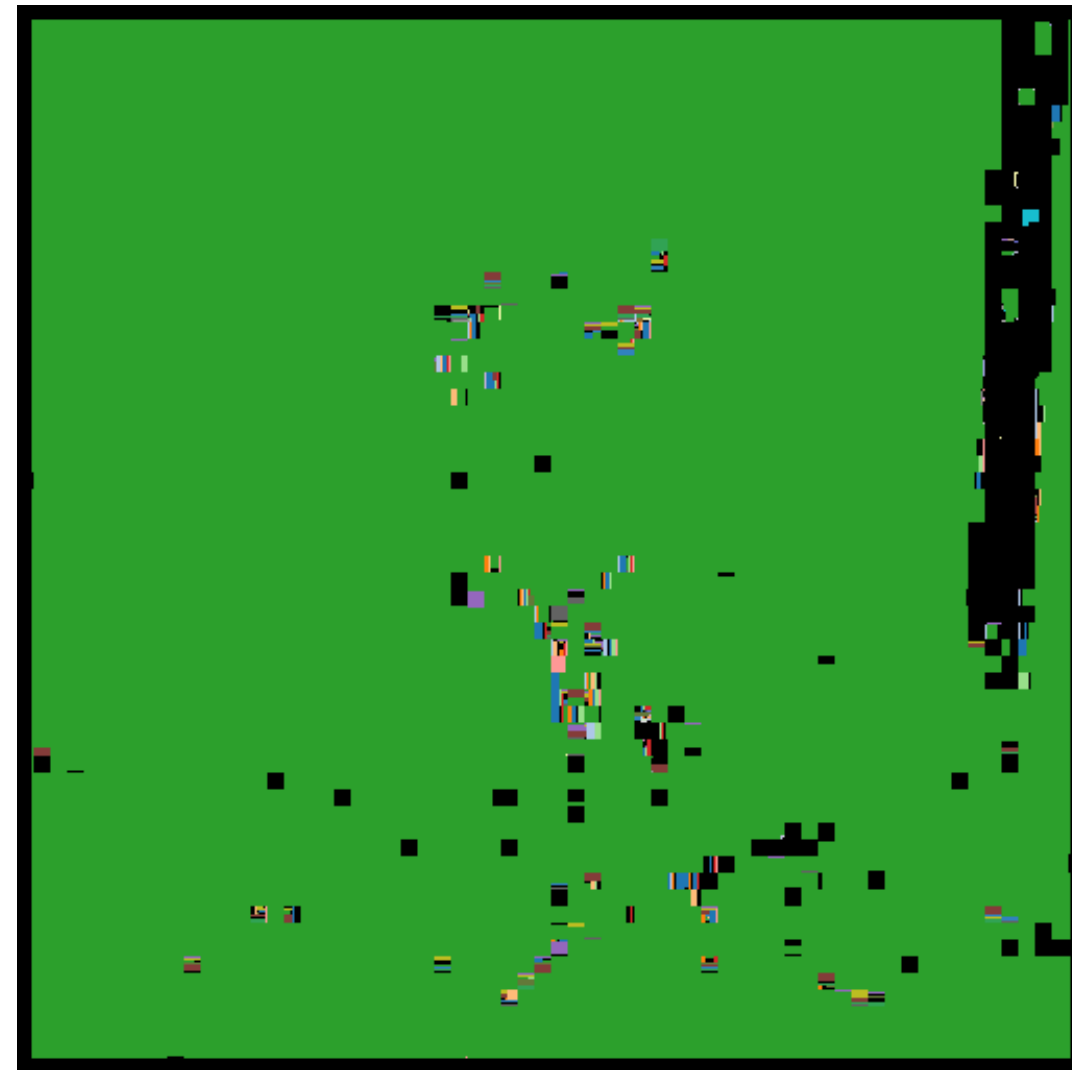
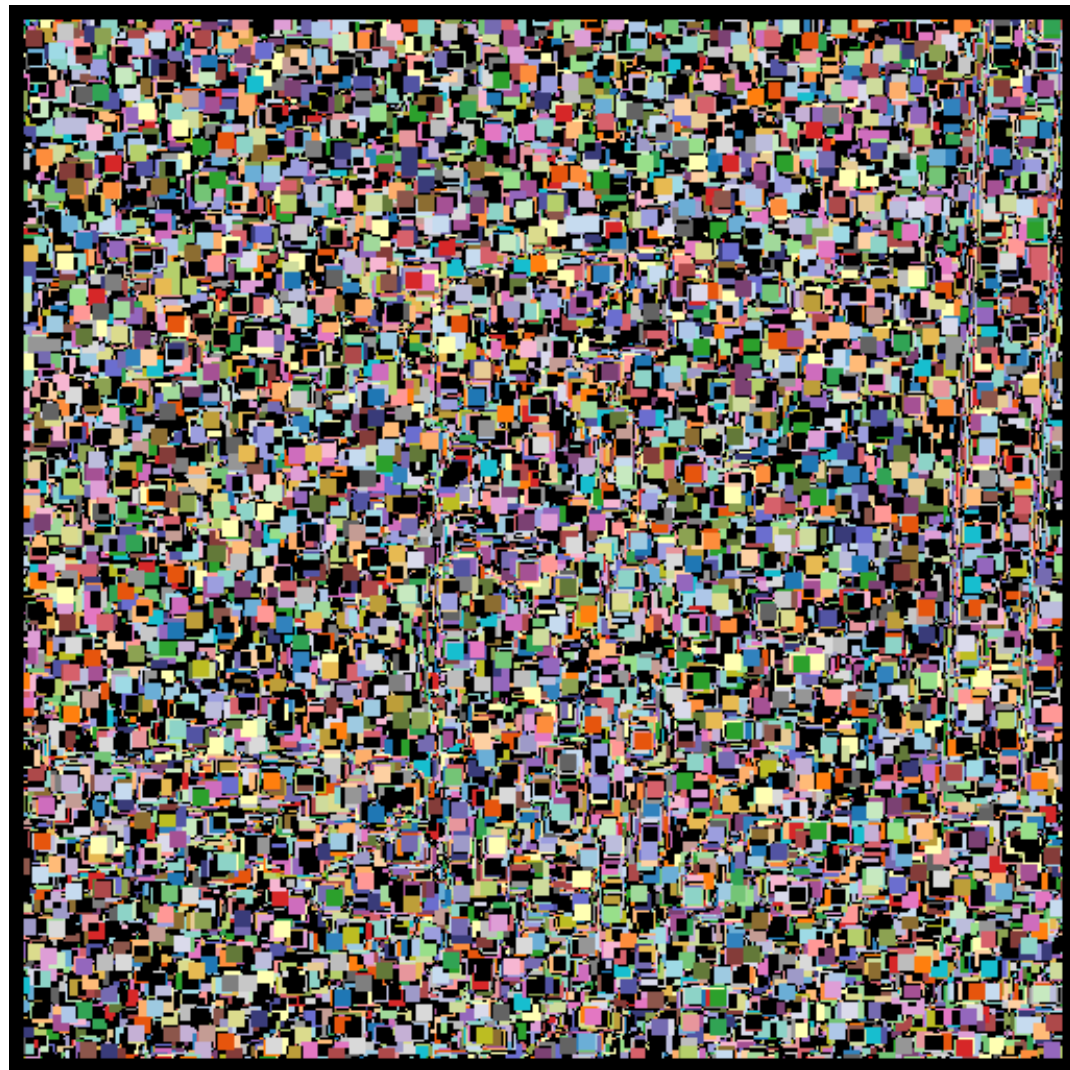
Compressed (Q=50)



Compressed (Q=80)

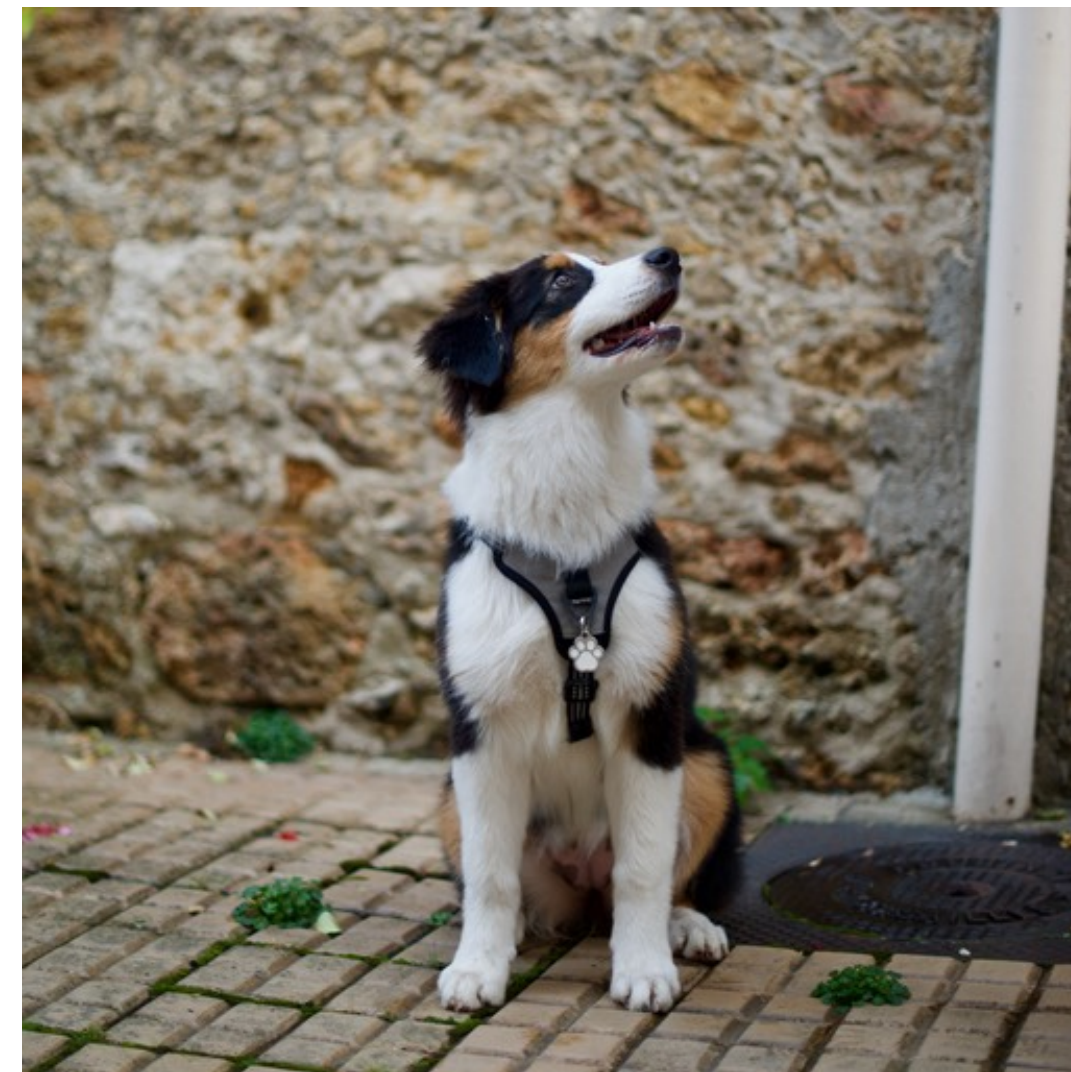


Compressed (Q=99)

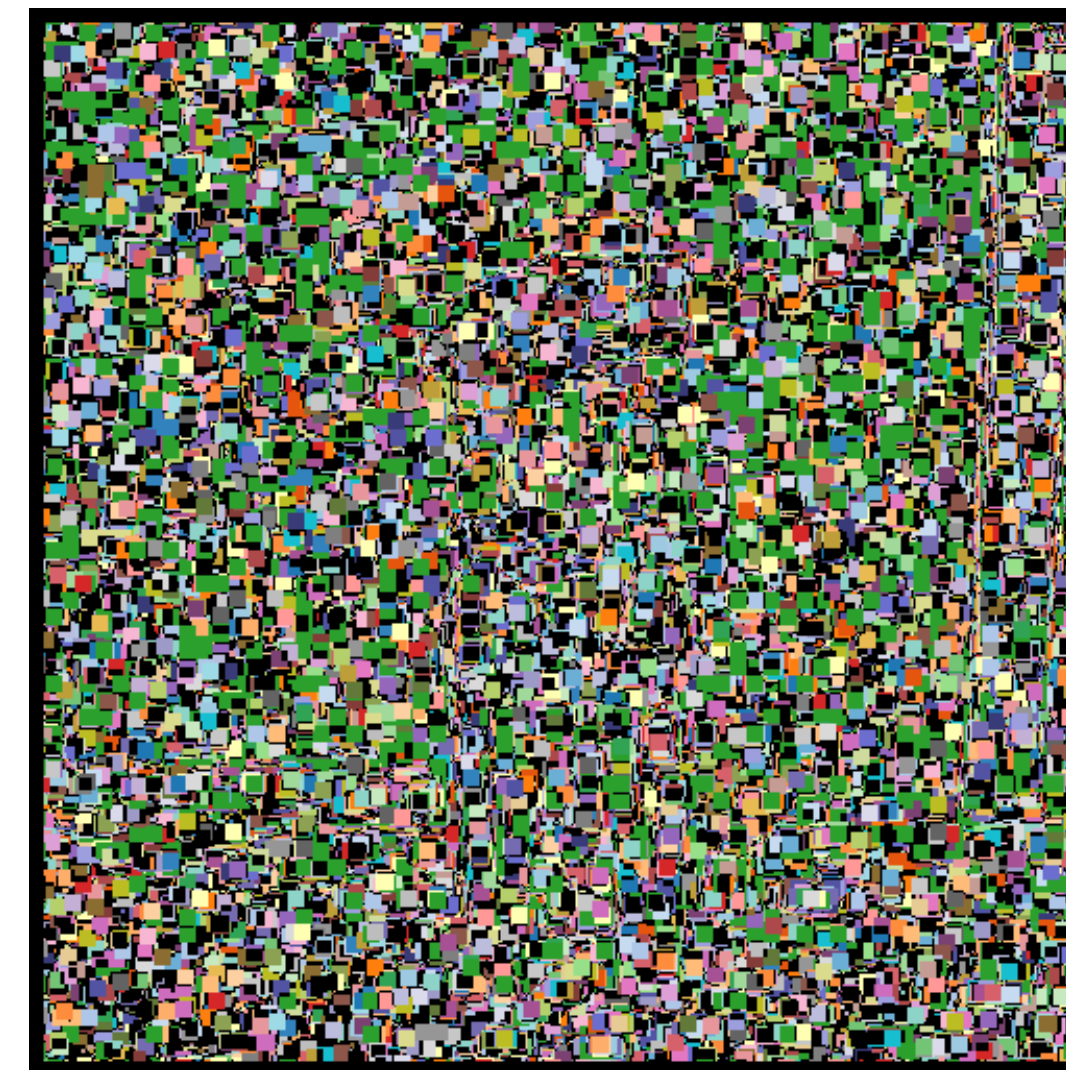
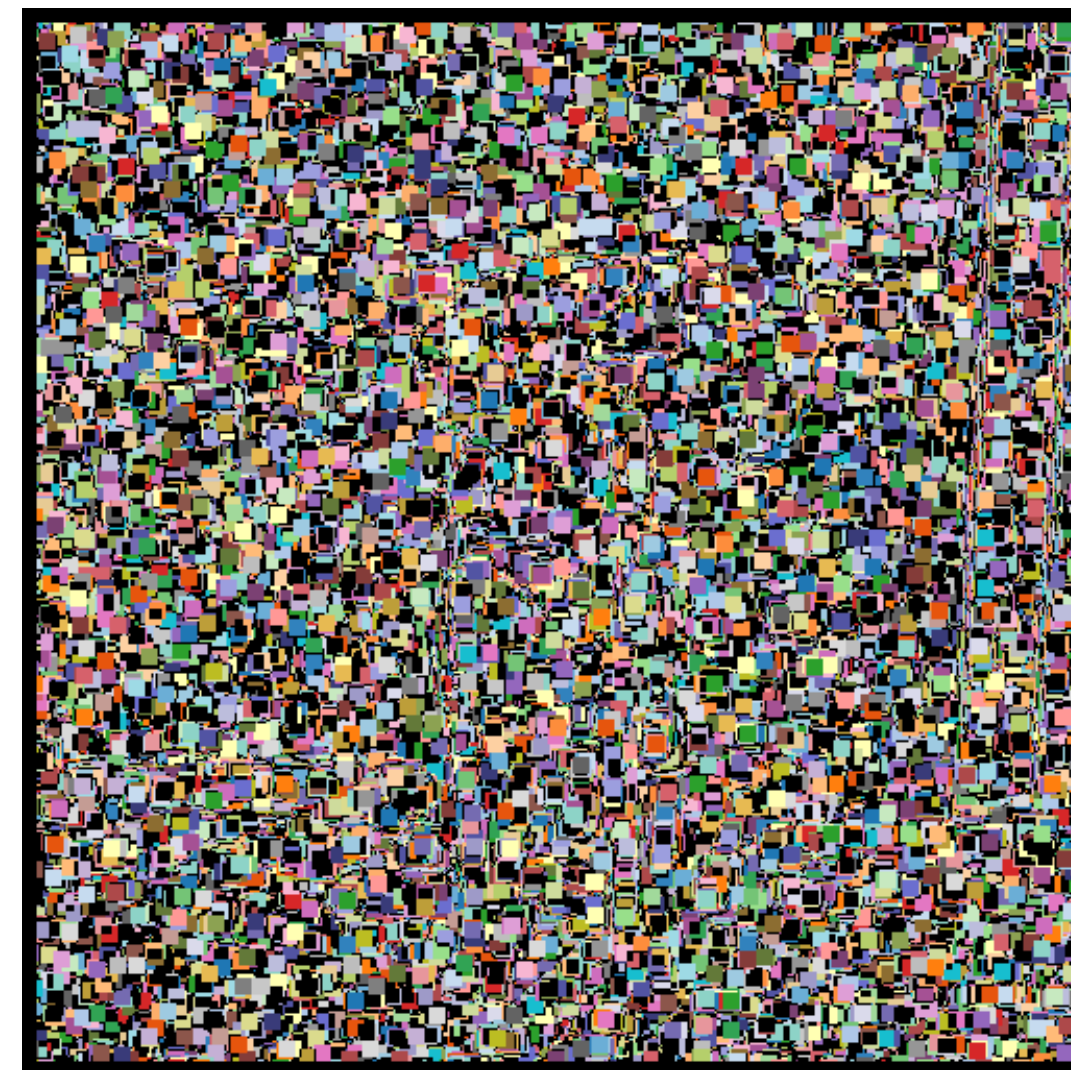
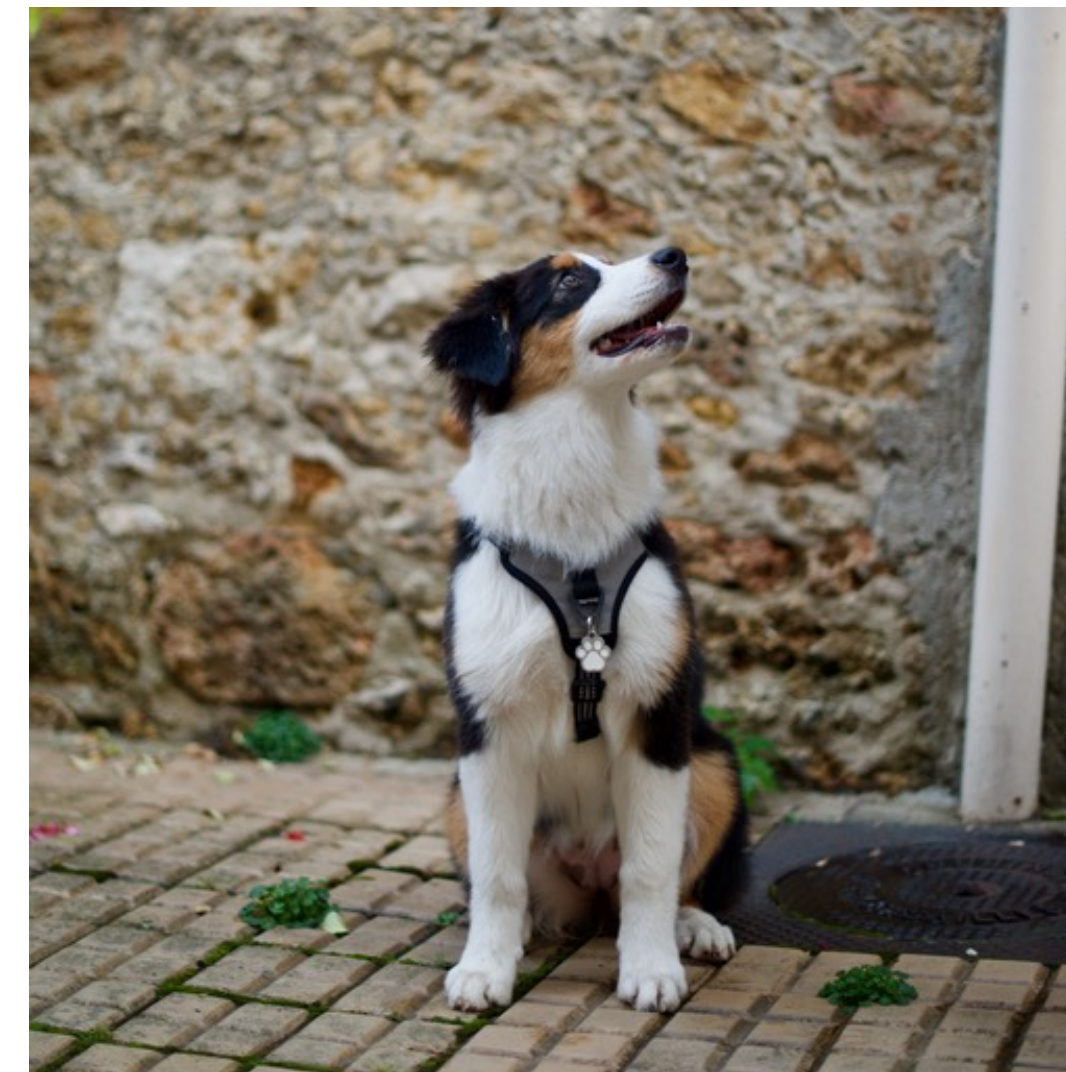


Each color represents a vote. Black corresponds to a non-valid vote, in case of a tie for example.

Uncompressed



Compressed (Q=99)



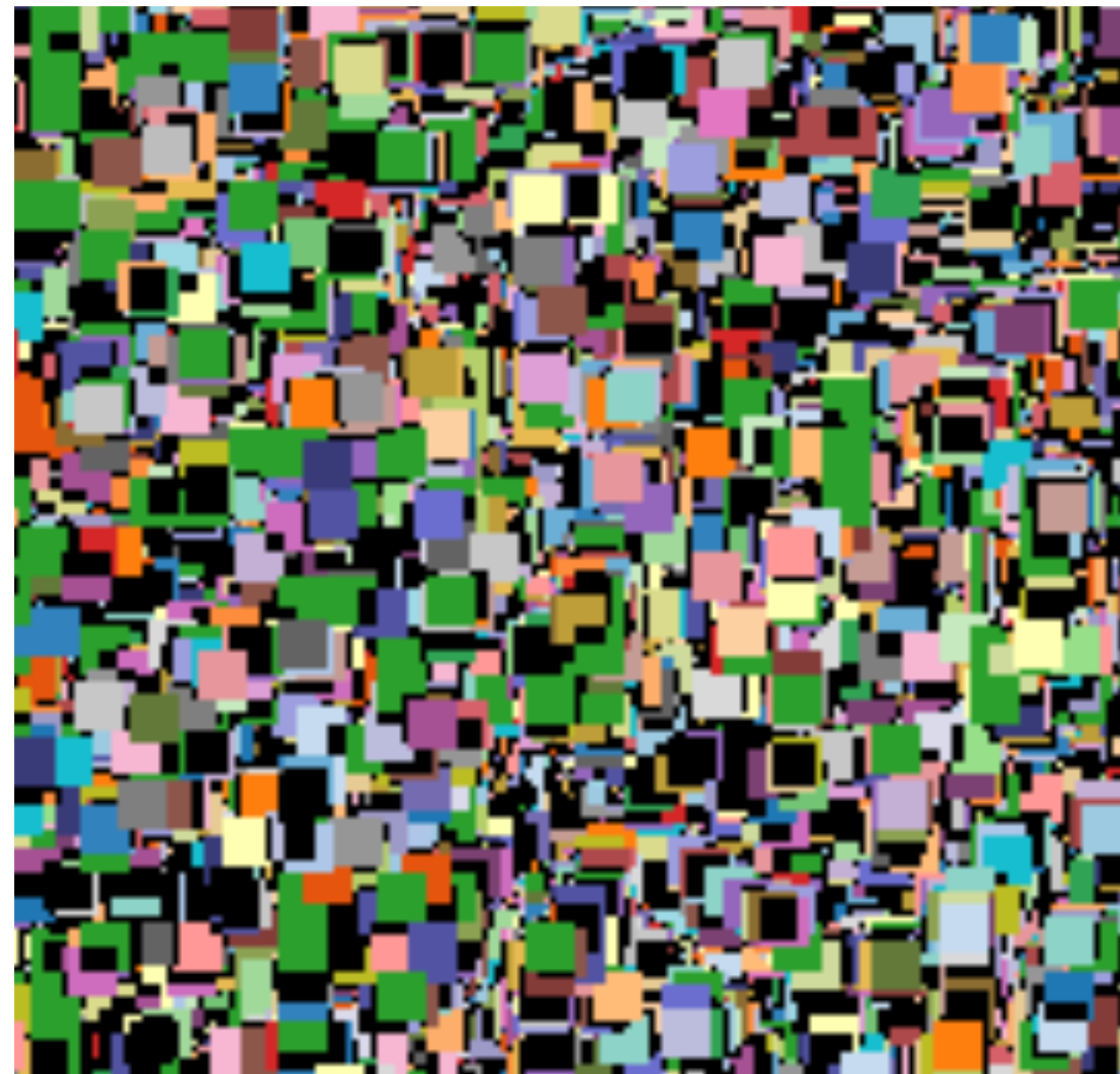
Each color represents a vote. Black corresponds to a non-valid vote, in case of a tie for example.

How to decide?

A contrario validation

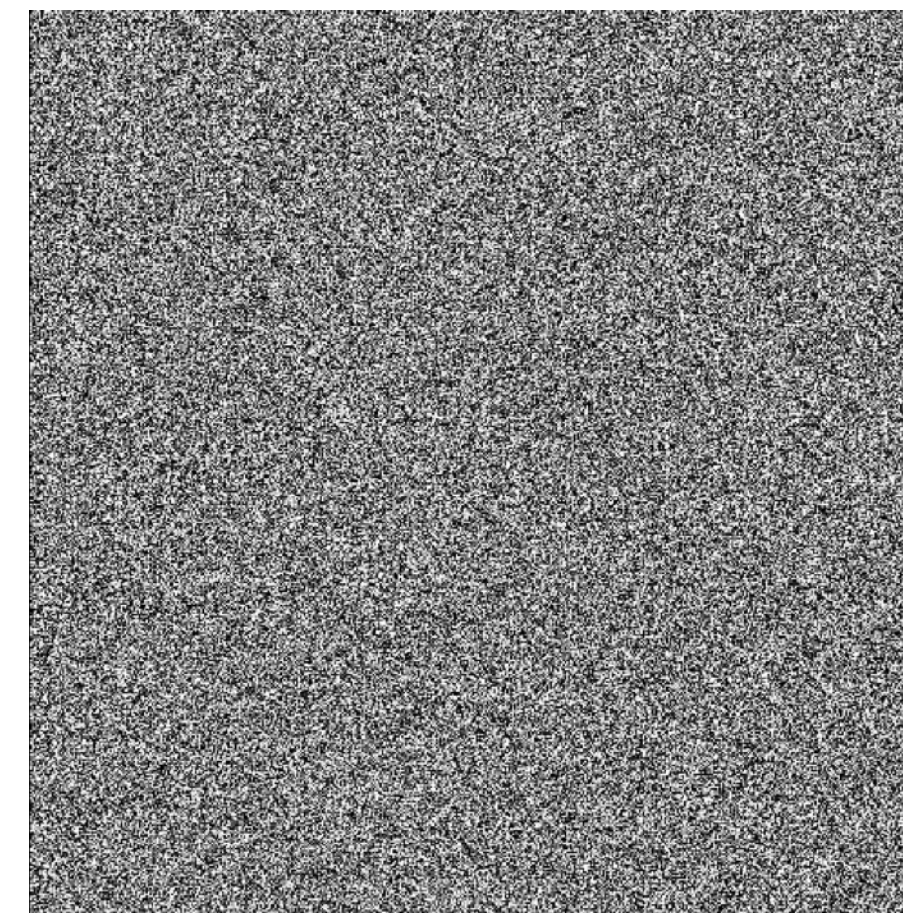
Given a window of an image, is the most voted grid significant?

We need to assess the probability that a given grid origin gets a larger number of votes purely by chance.

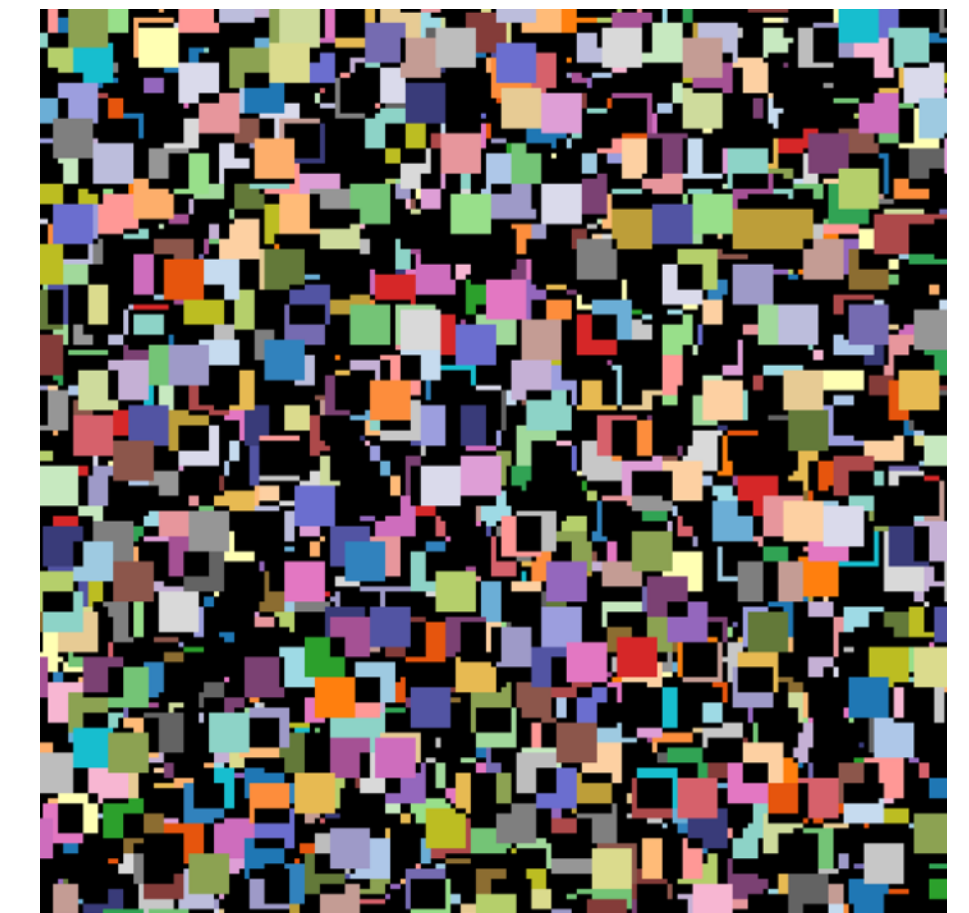


For who did this window vote?
Is the vote significant?

Laplace's principle of indifference: In absence of JPEG compression, each of the 64 blocks containing a given pixel would have the same chance of being the one with the largest number of zeros.



Noise



Vote map

Votes are correlated within a distance of 8 pixels, and uncorrelated for pixels at distance larger than 8.

We define a stochastic null model H_0 for votes at distance 8 in which votes are independent and uniformly distributed among all the 64 grid origins.

A contrario validation

Given a window w , k votes are counted for a candidate grid origin among n votes. Under H_0 , votes for the grid g become a Bernoulli random variable K with probability $p = 1/64$.

$$P(K \geq k) = \mathcal{B}(n, k, p) = \sum_{j=k}^n \binom{n}{j} p^j (1-p)^{n-j}$$

Following the *a contrario* methodology, the multiplicity of tests N_T is taken into account, where $N_T = XY \cdot XY \cdot 64 \cdot 64$.

Then, the Number of False Alarms (NFA) is defined as

$$\text{NFA}(g, w) = N_T P(K \geq k)$$

A JPEG grid is detected when $\text{NFA} < 1$.

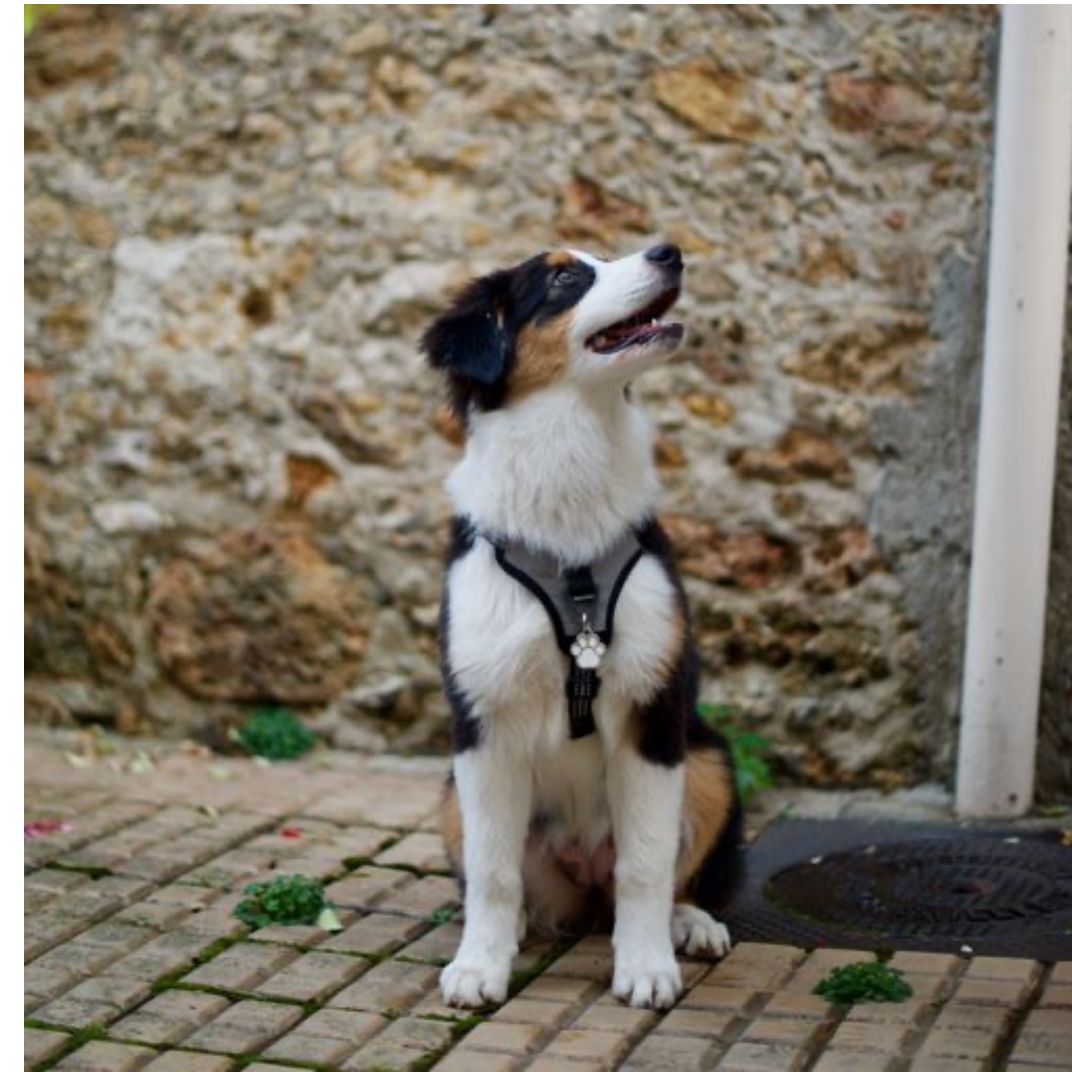
Uncompressed



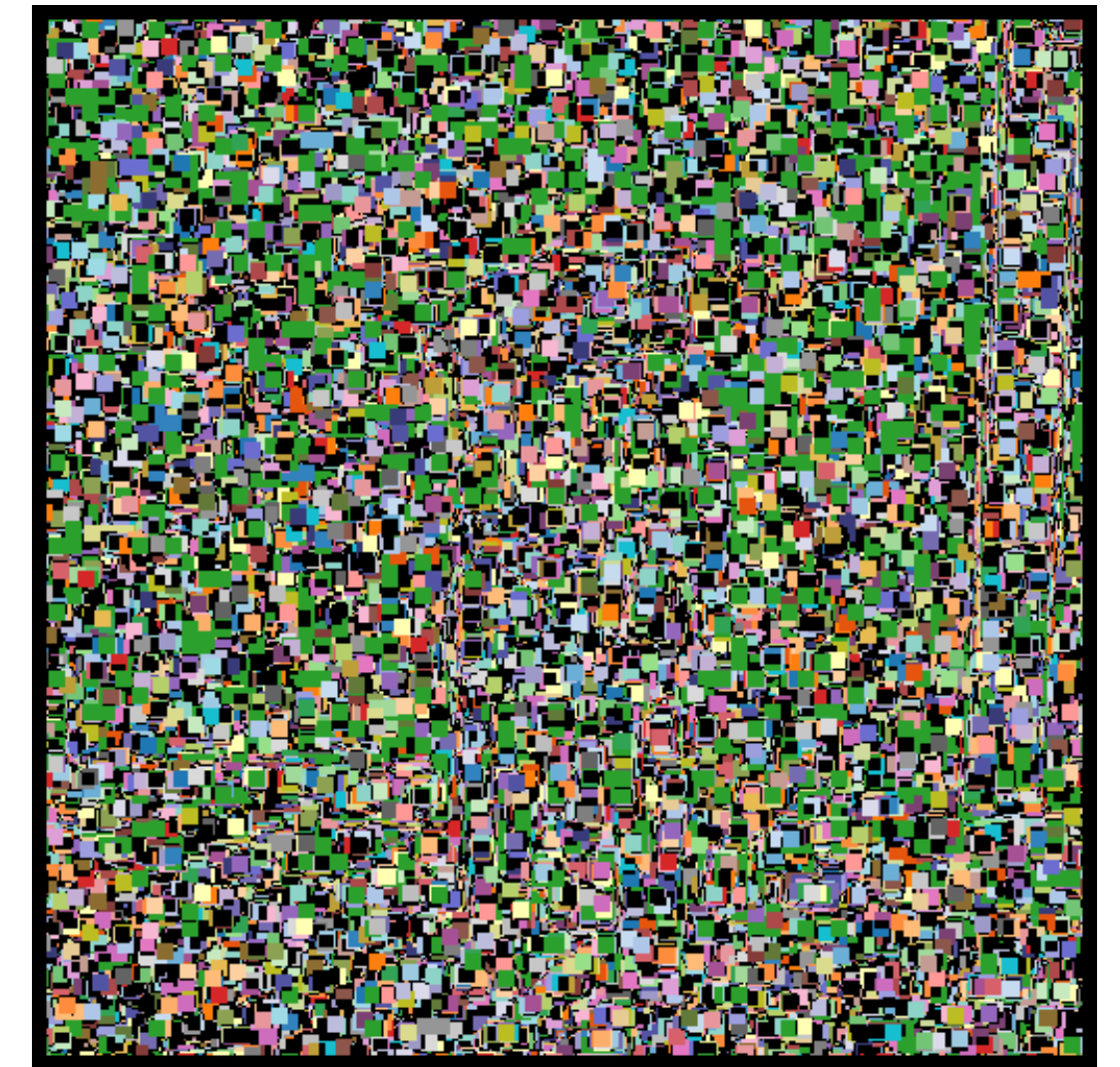
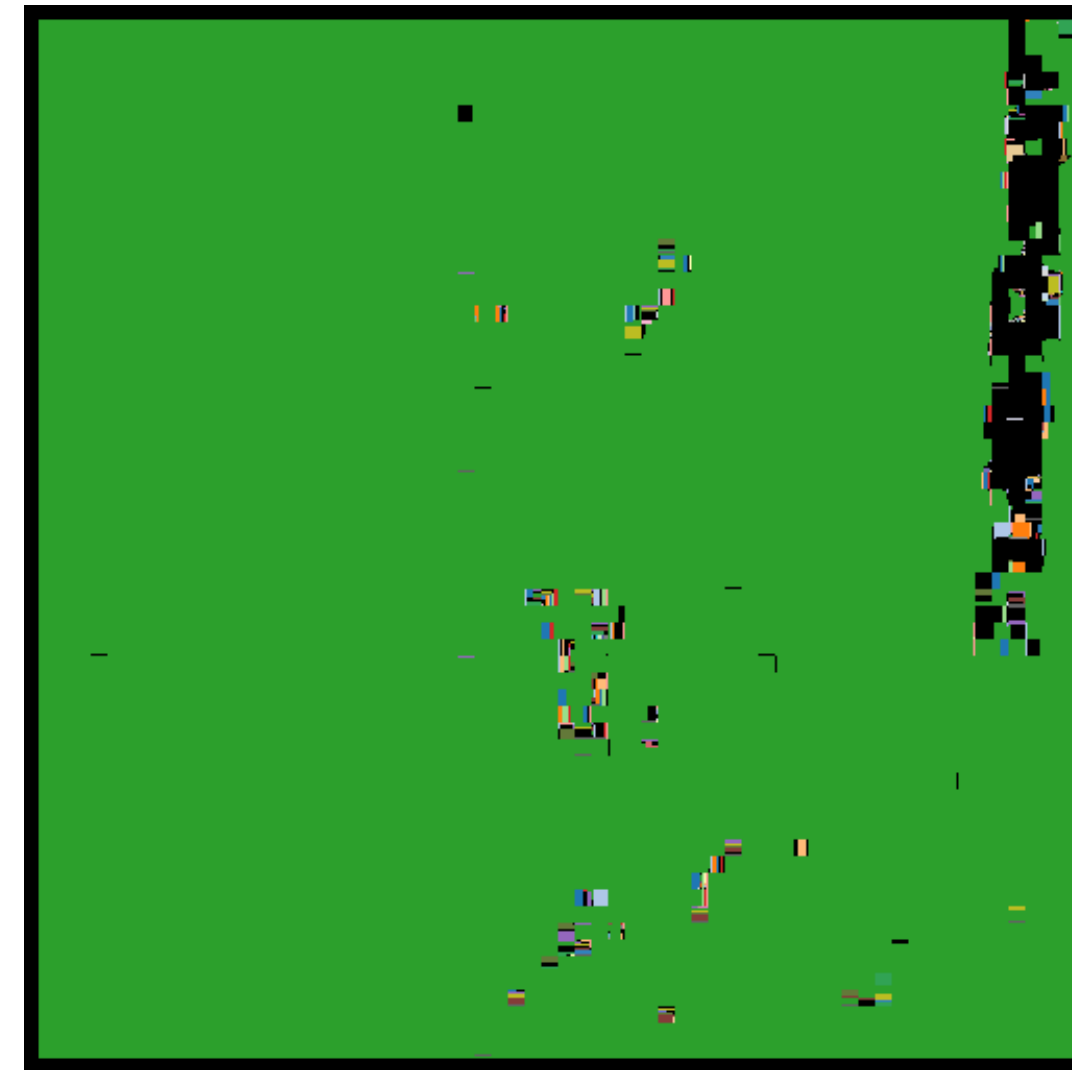
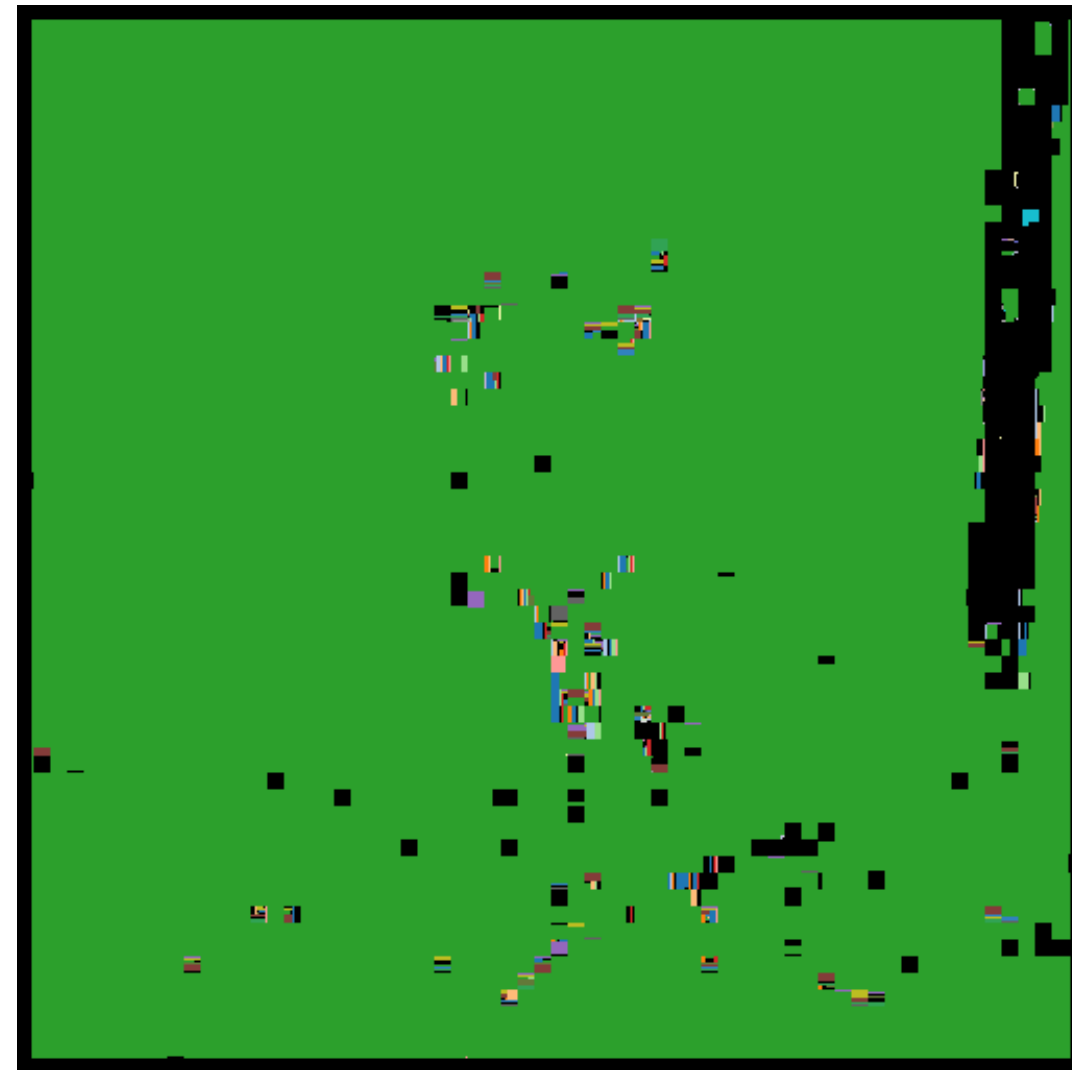
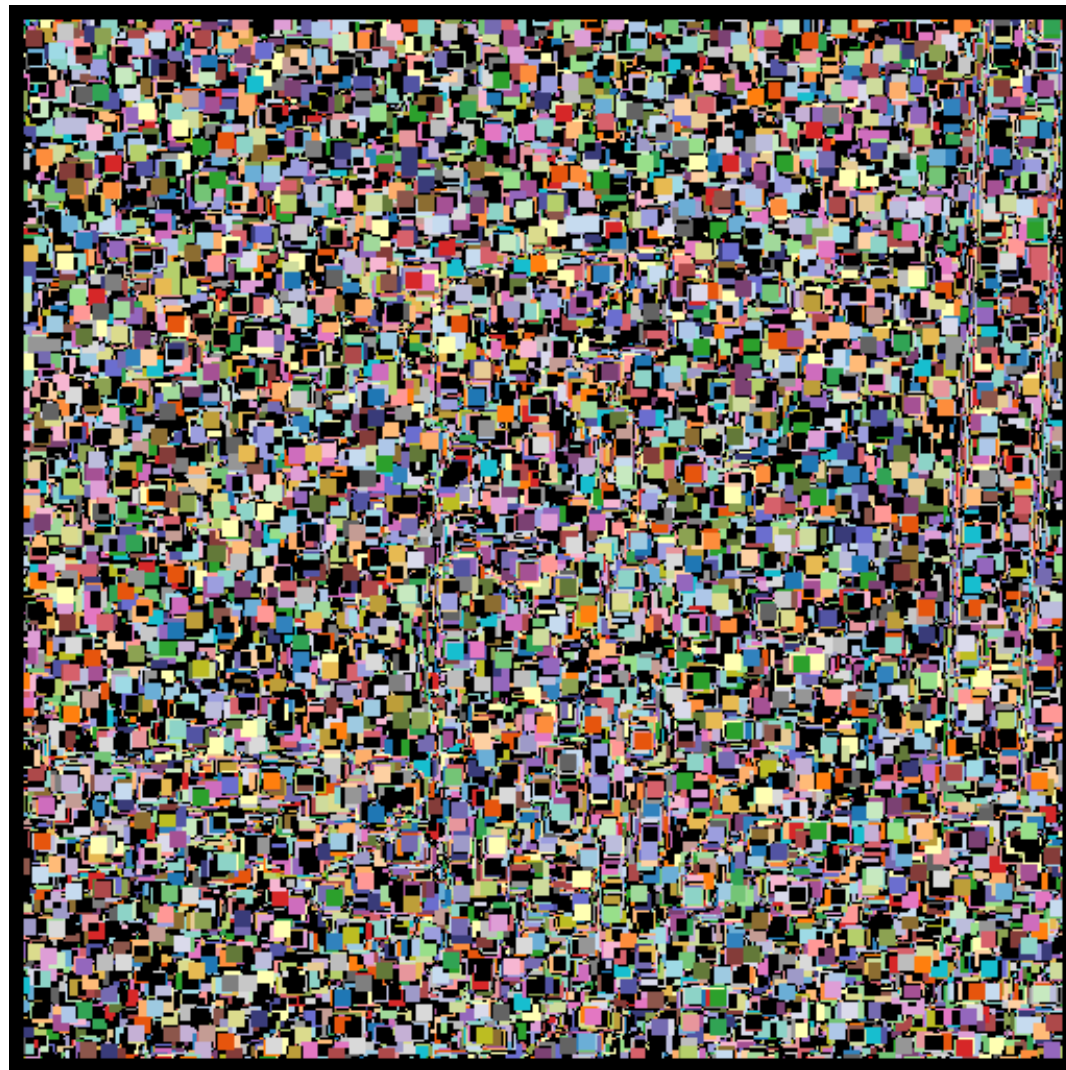
Compressed (Q=50)



Compressed (Q=80)



Compressed (Q=99)



Each color represents a vote. Black corresponds to a non-valid vote, in case of a tie for example.

Uncompressed



Compressed (Q=50)



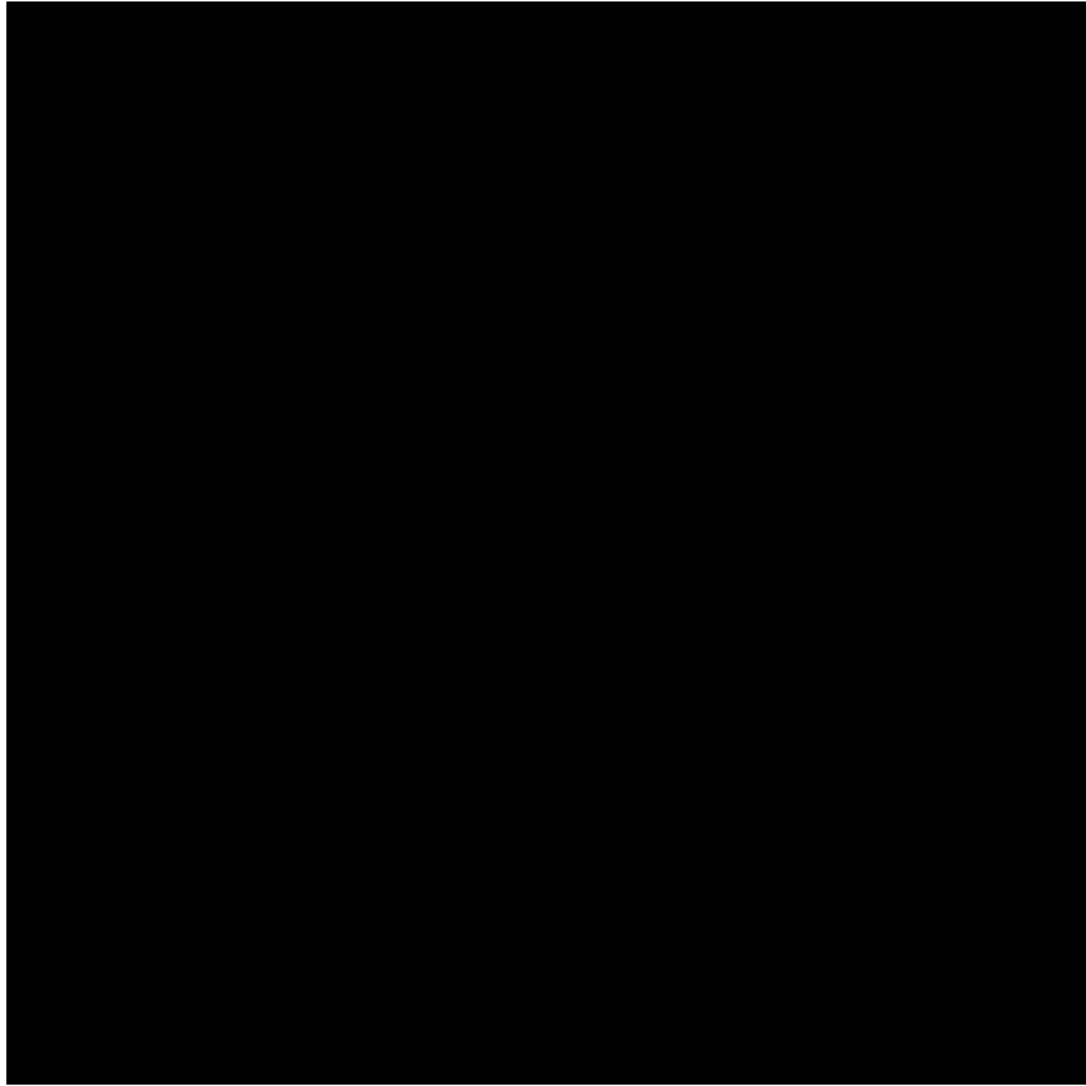
Compressed (Q=80)



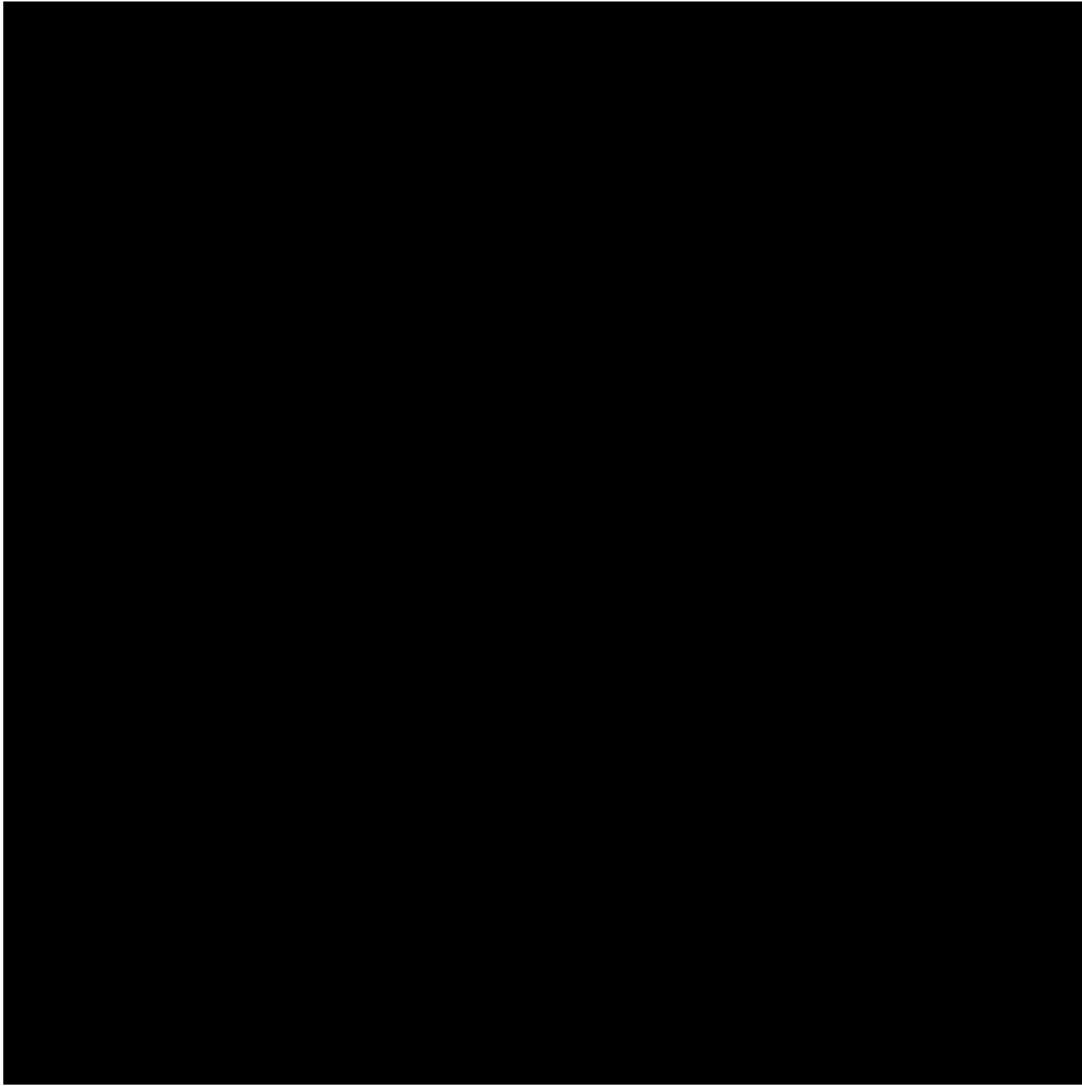
Compressed (Q=99)



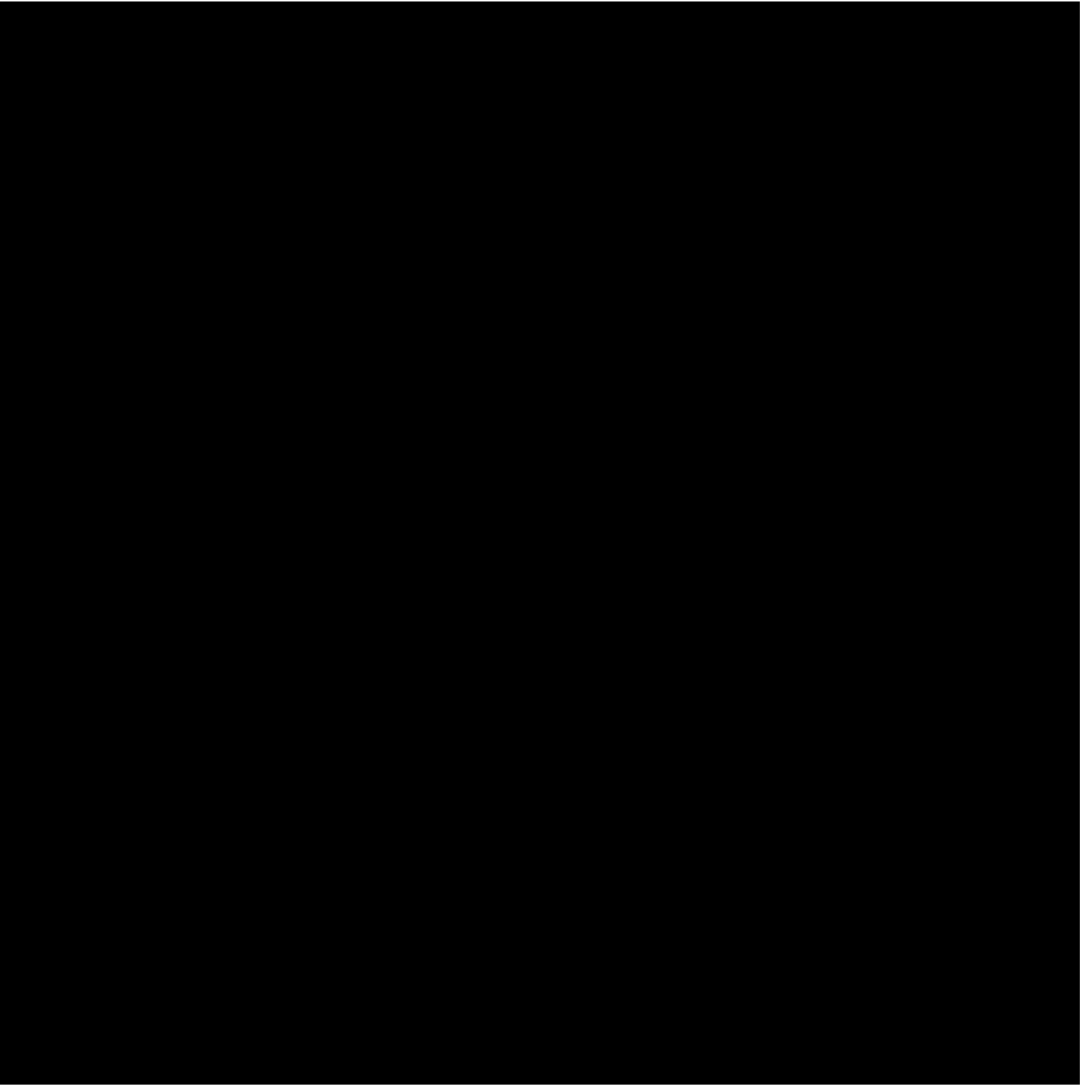
NO JPEG TRACES
DETECTED



JPEG image with origin (0,0)



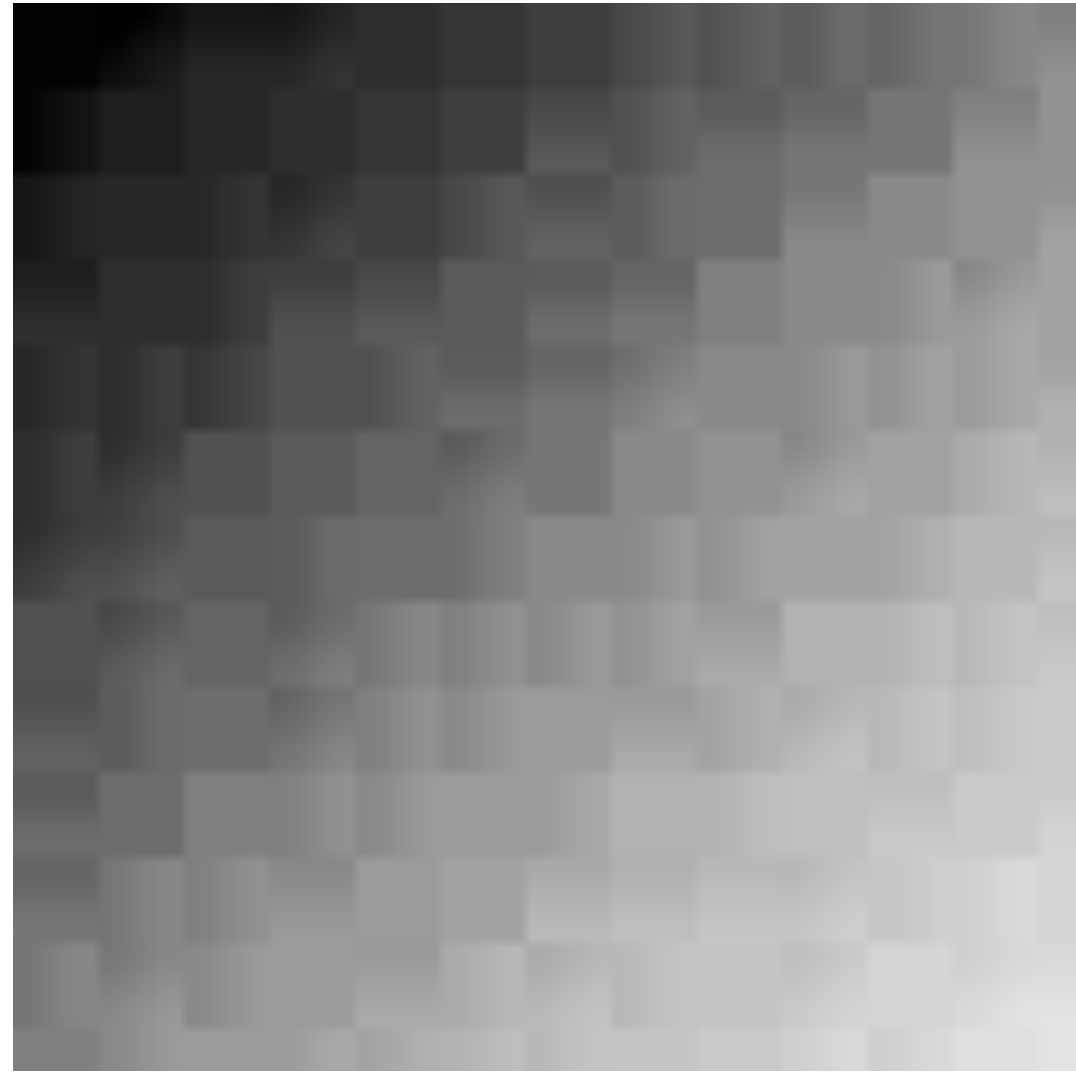
JPEG image with origin (0,0)



JPEG image with origin (0,0)

How to detect forgeries?

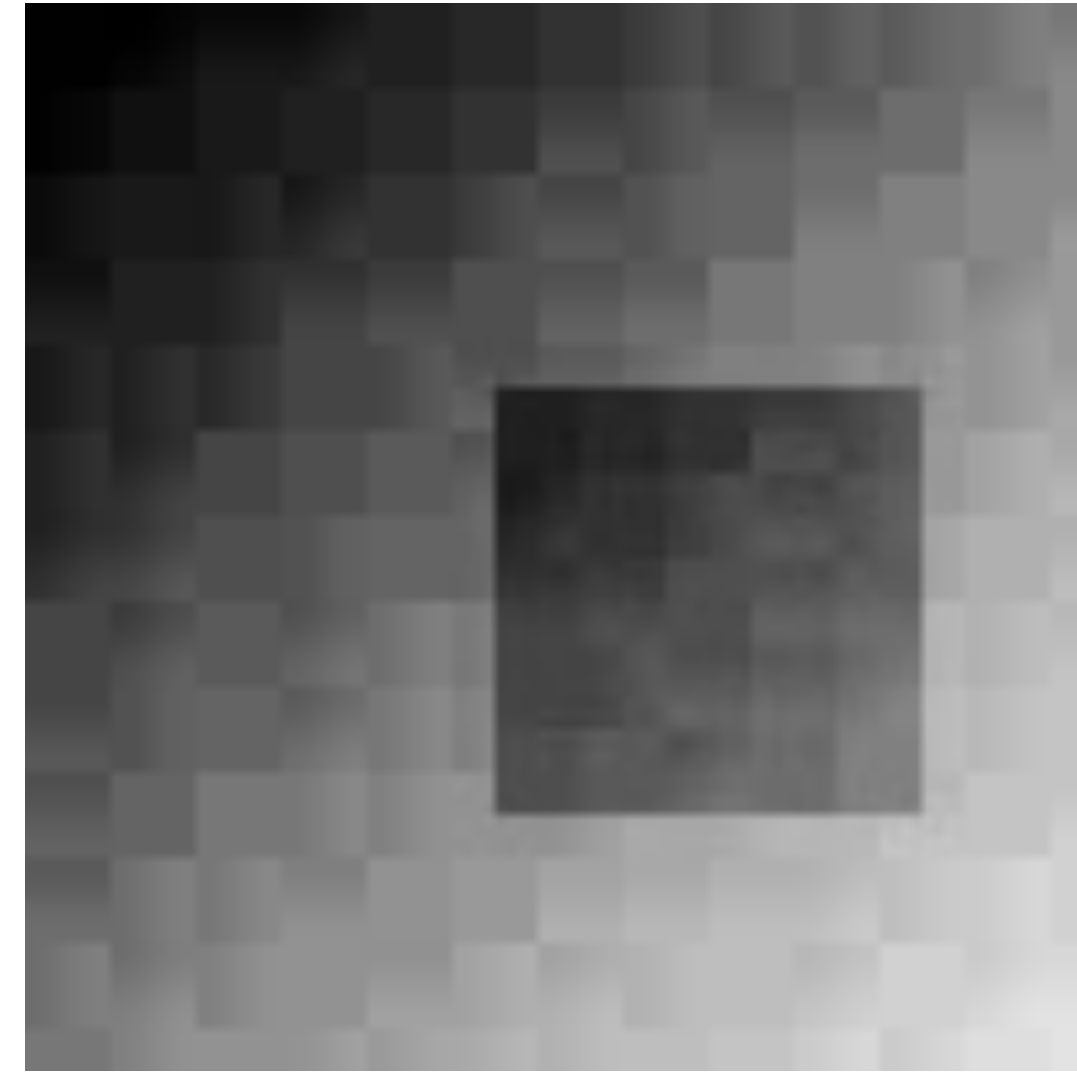
The impact of forgery on the JPEG grid



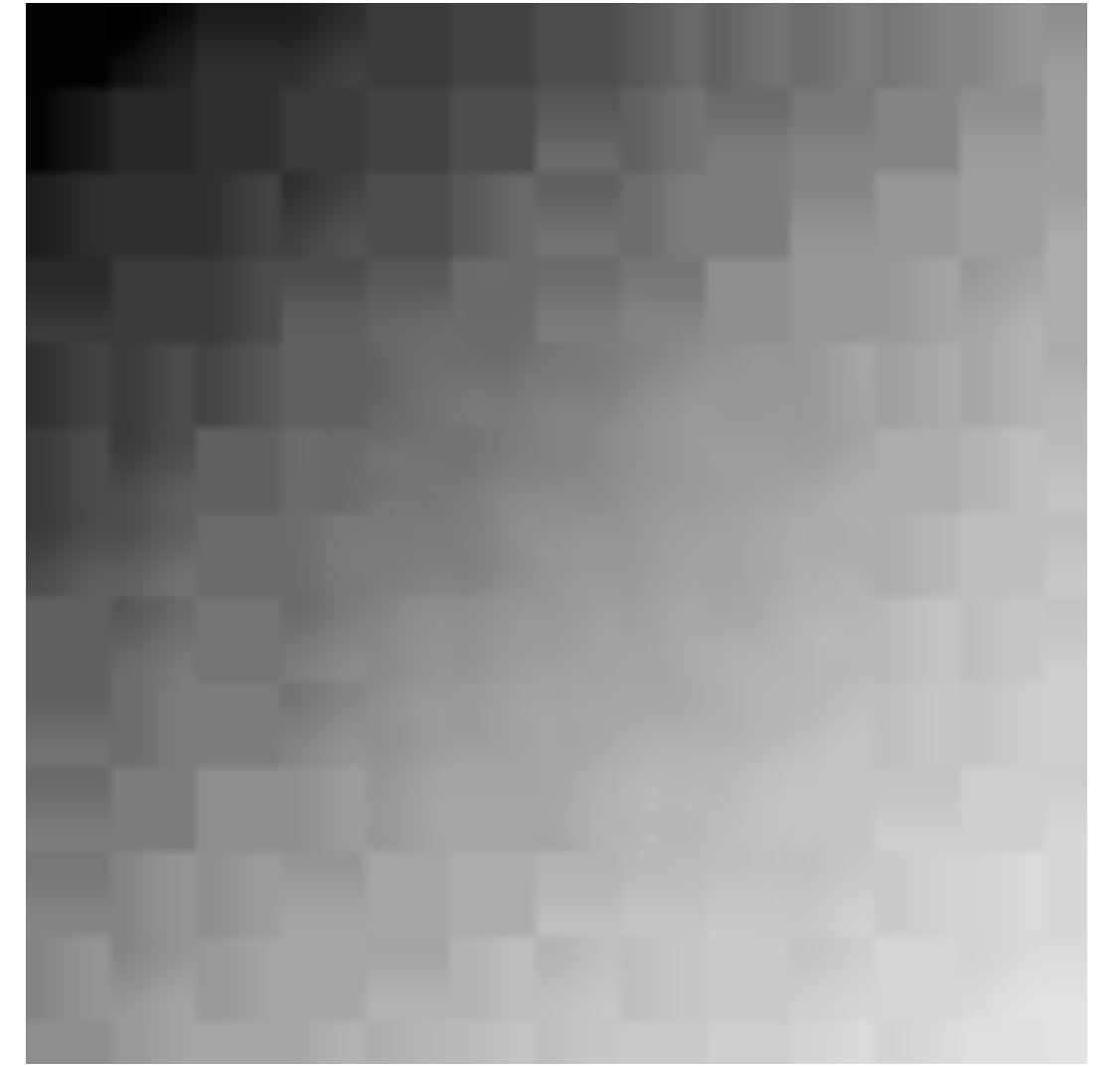
Authentic



Cropped



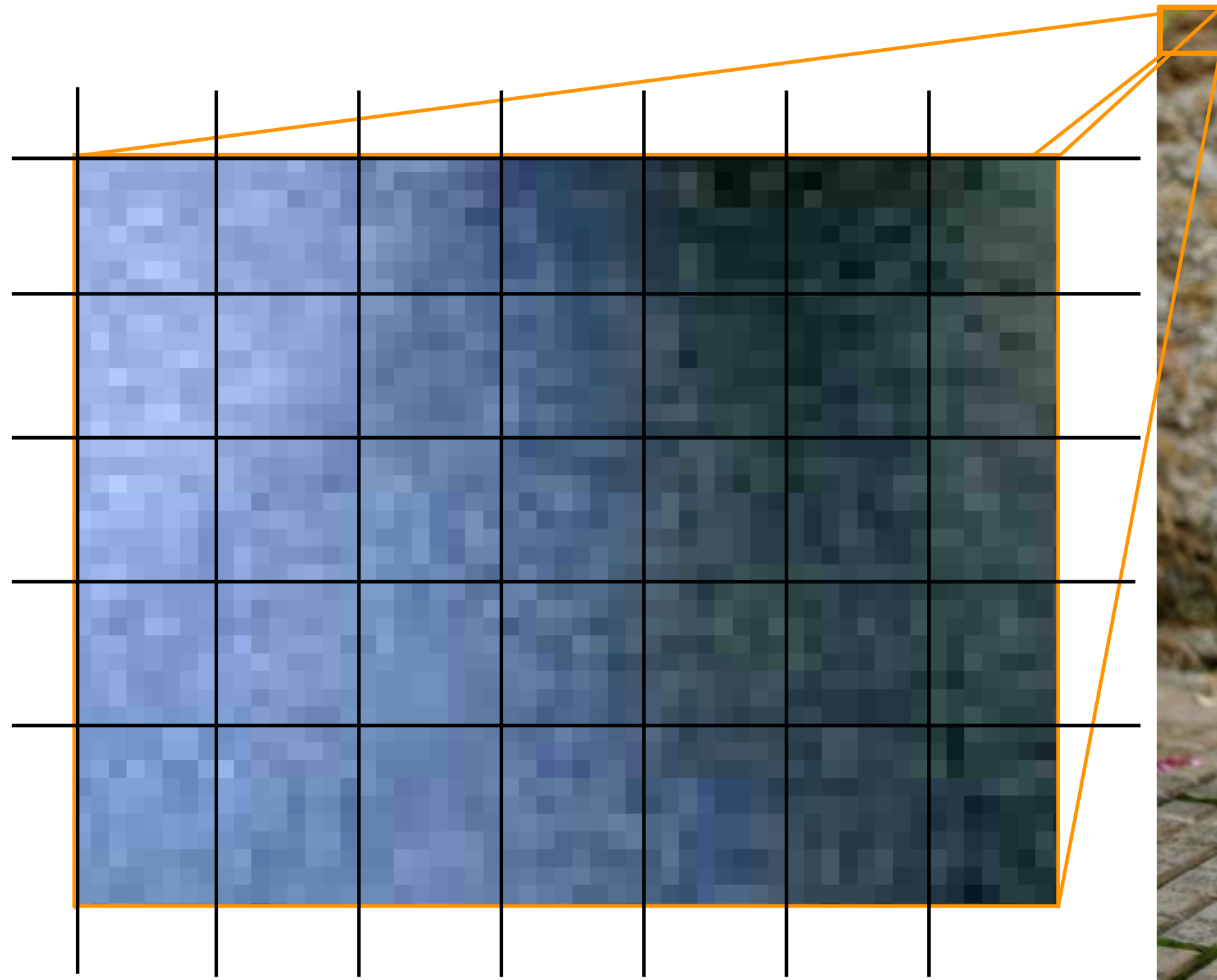
Shifted



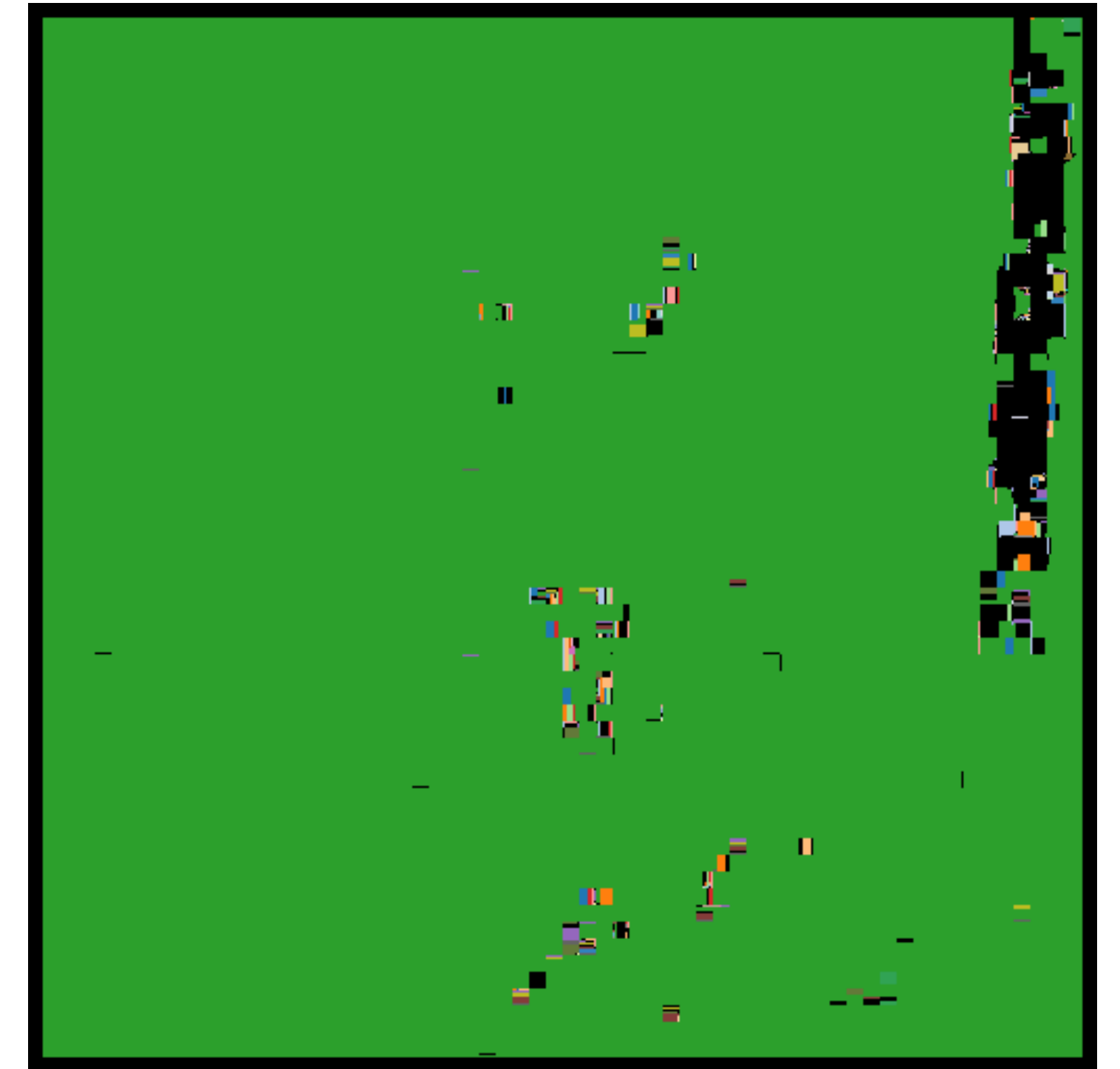
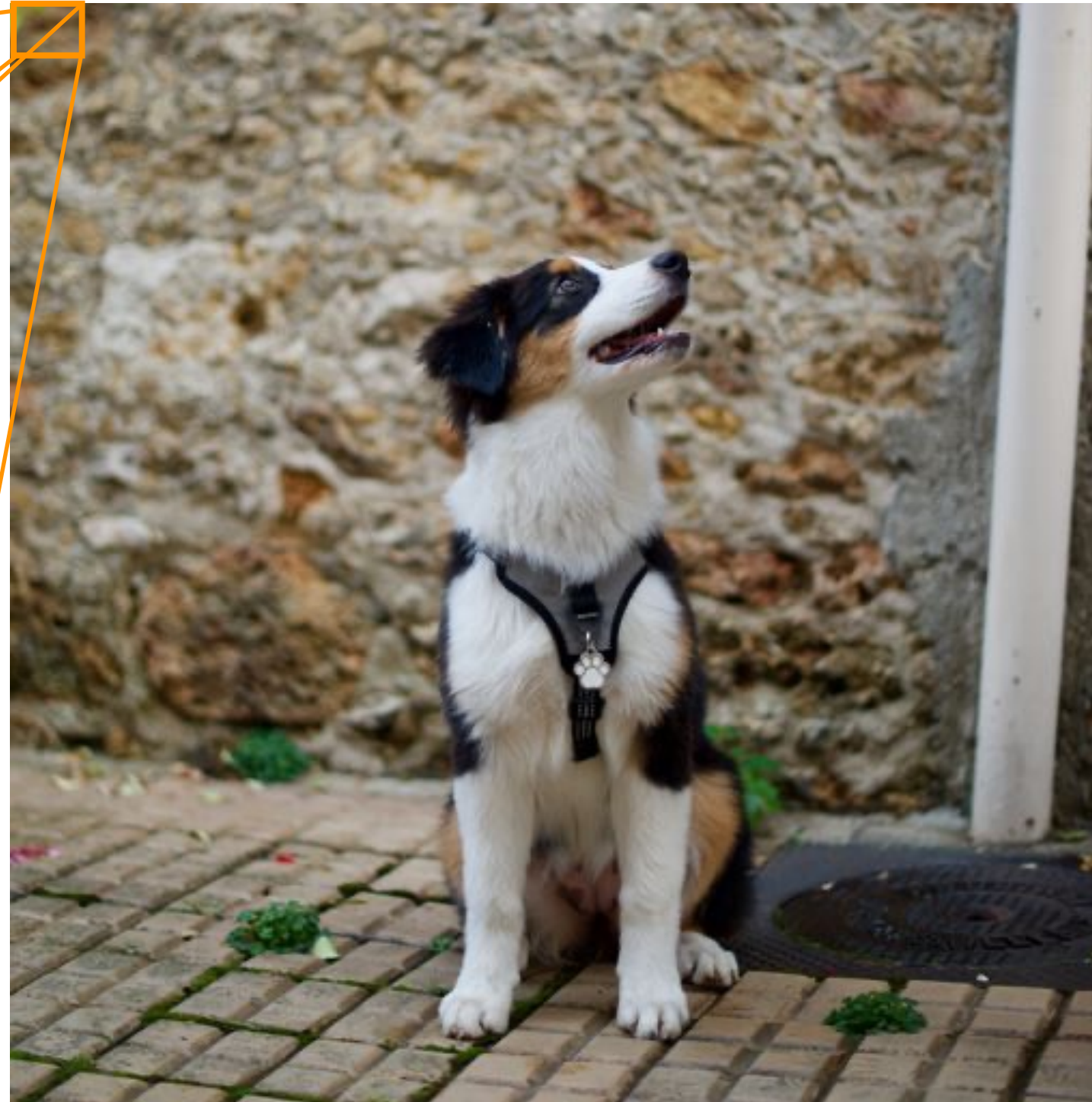
Missing

1. Global grid detection
2. Local foreign grid detection
3. Local missing grid detection

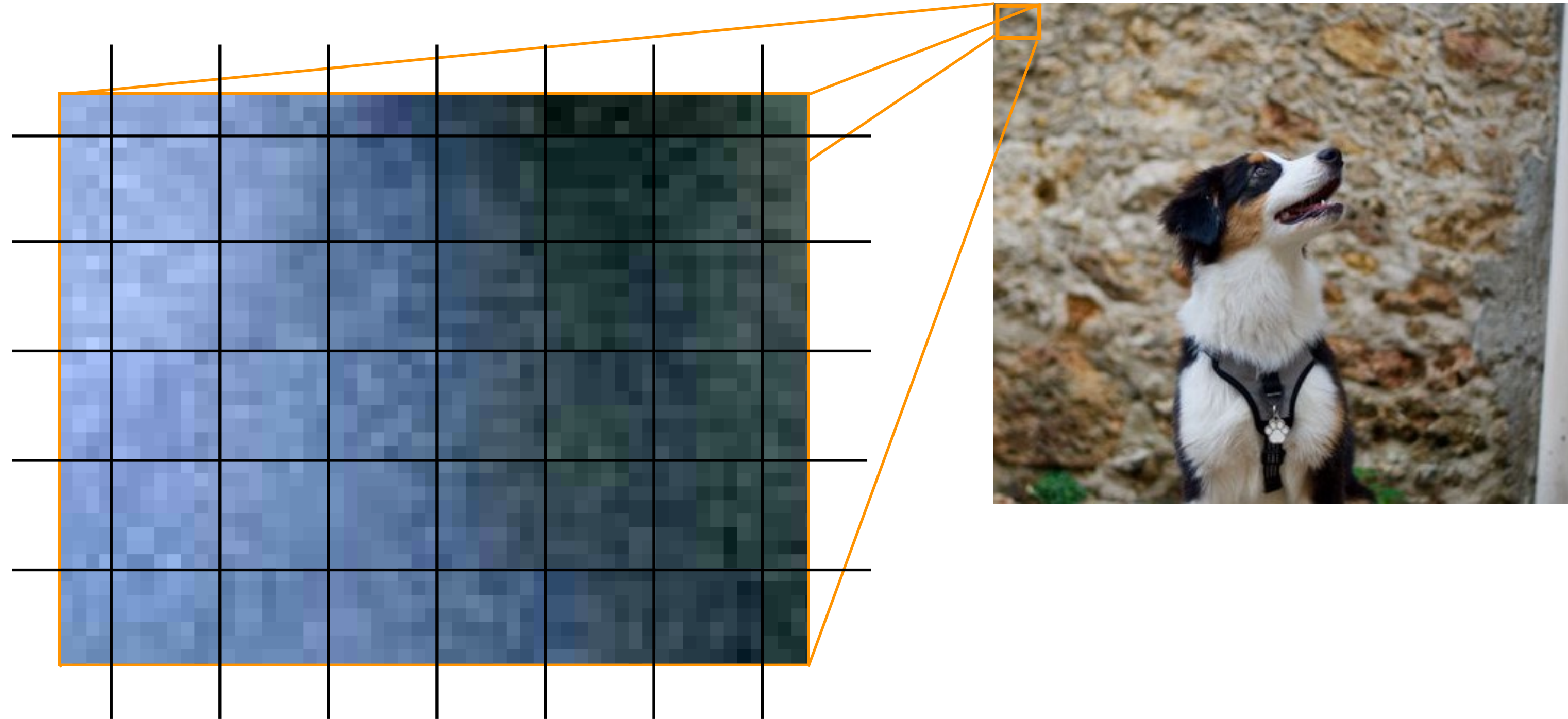
ZERO: a crop detector



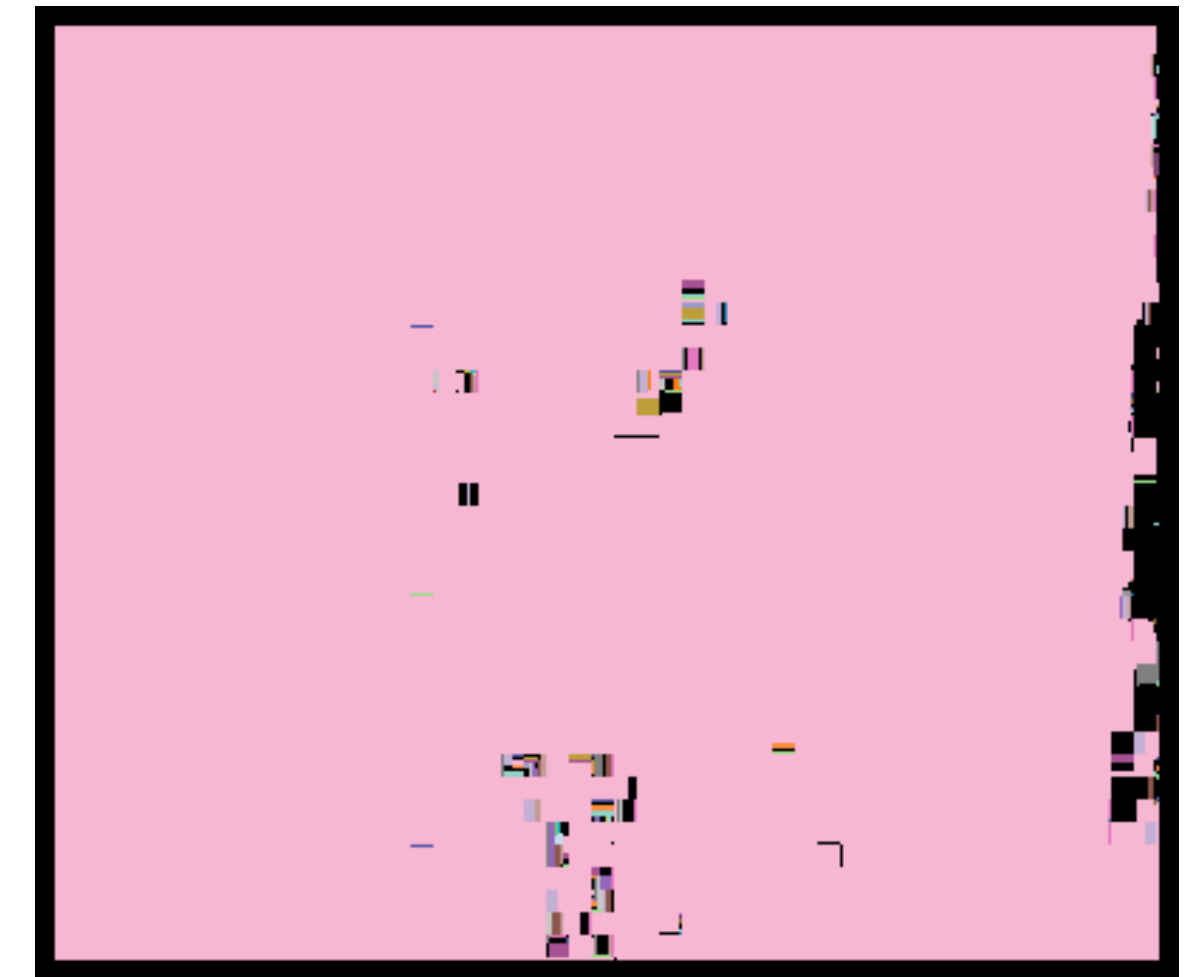
Main grid (0,0)



ZERO: a crop detector



Main grid (6,6)

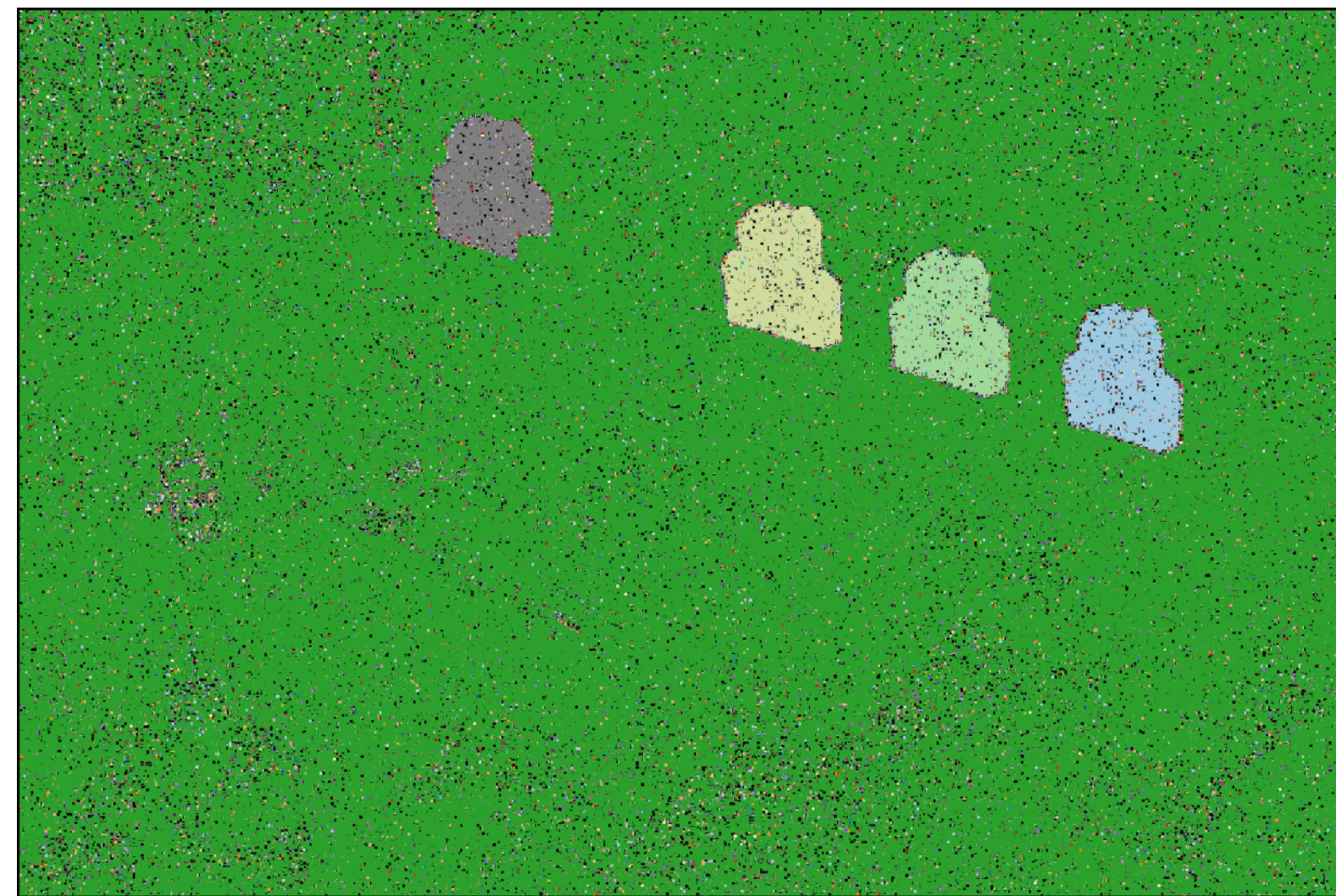
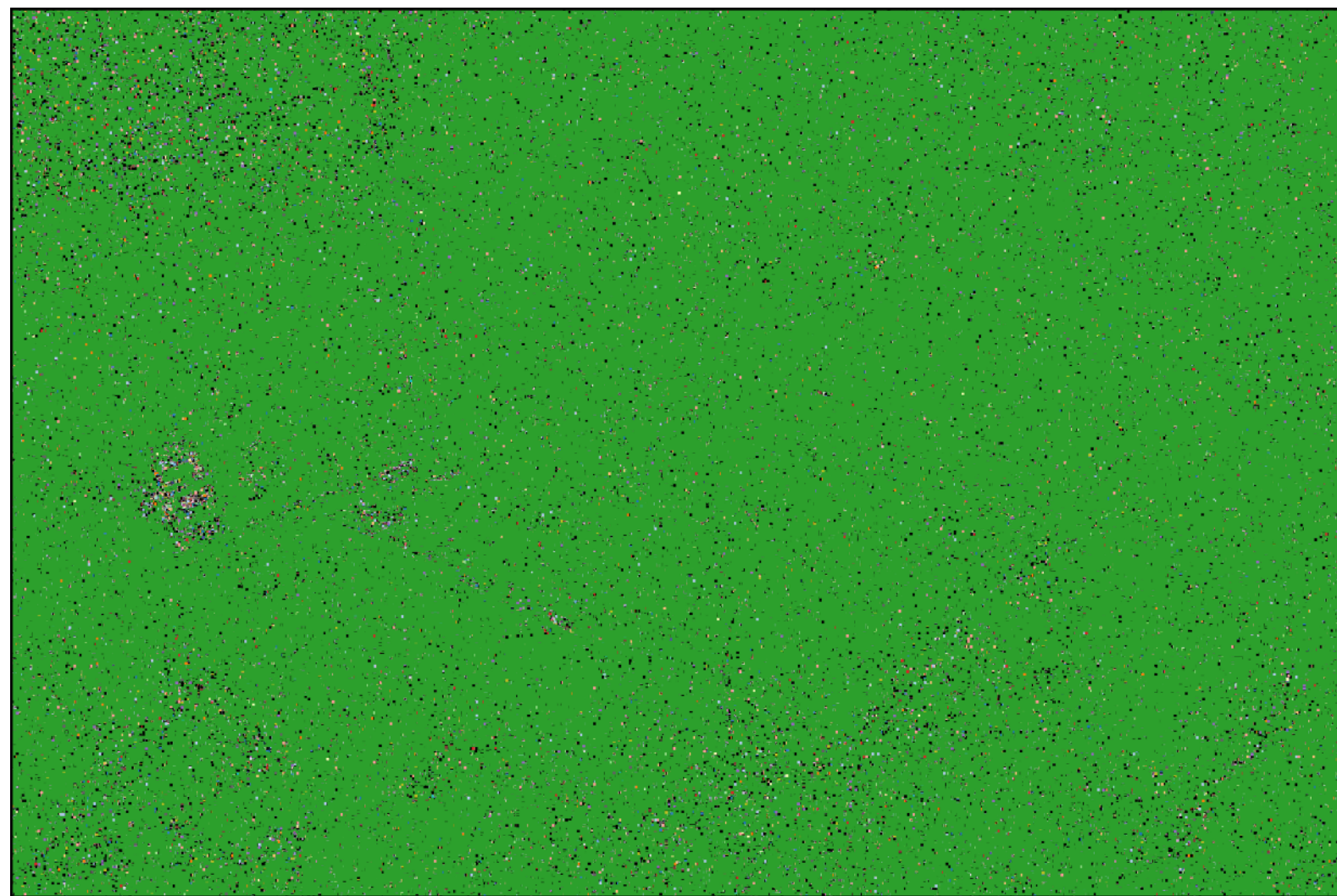


ZERO: A local foreign grid origin detector

Original



Forged



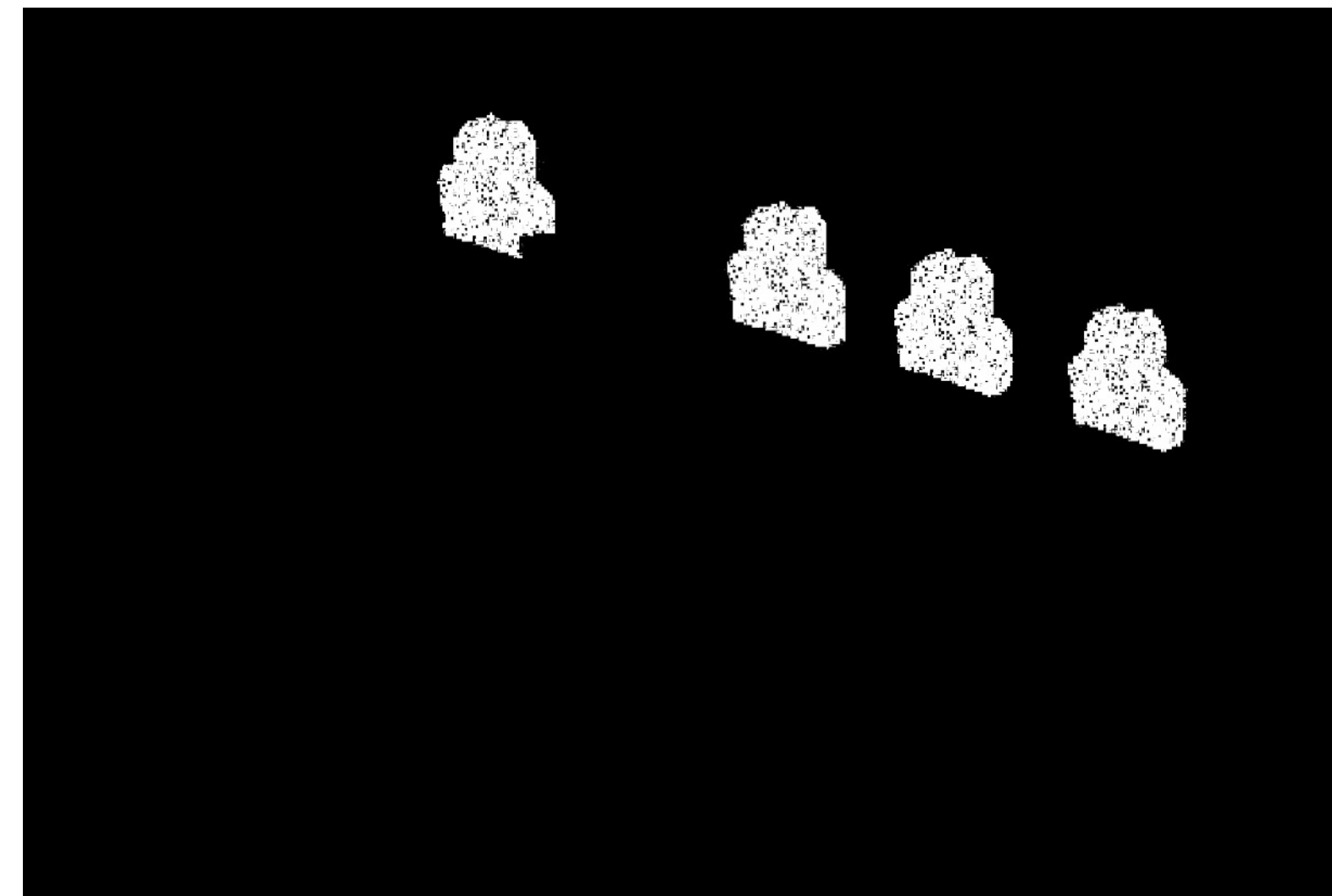
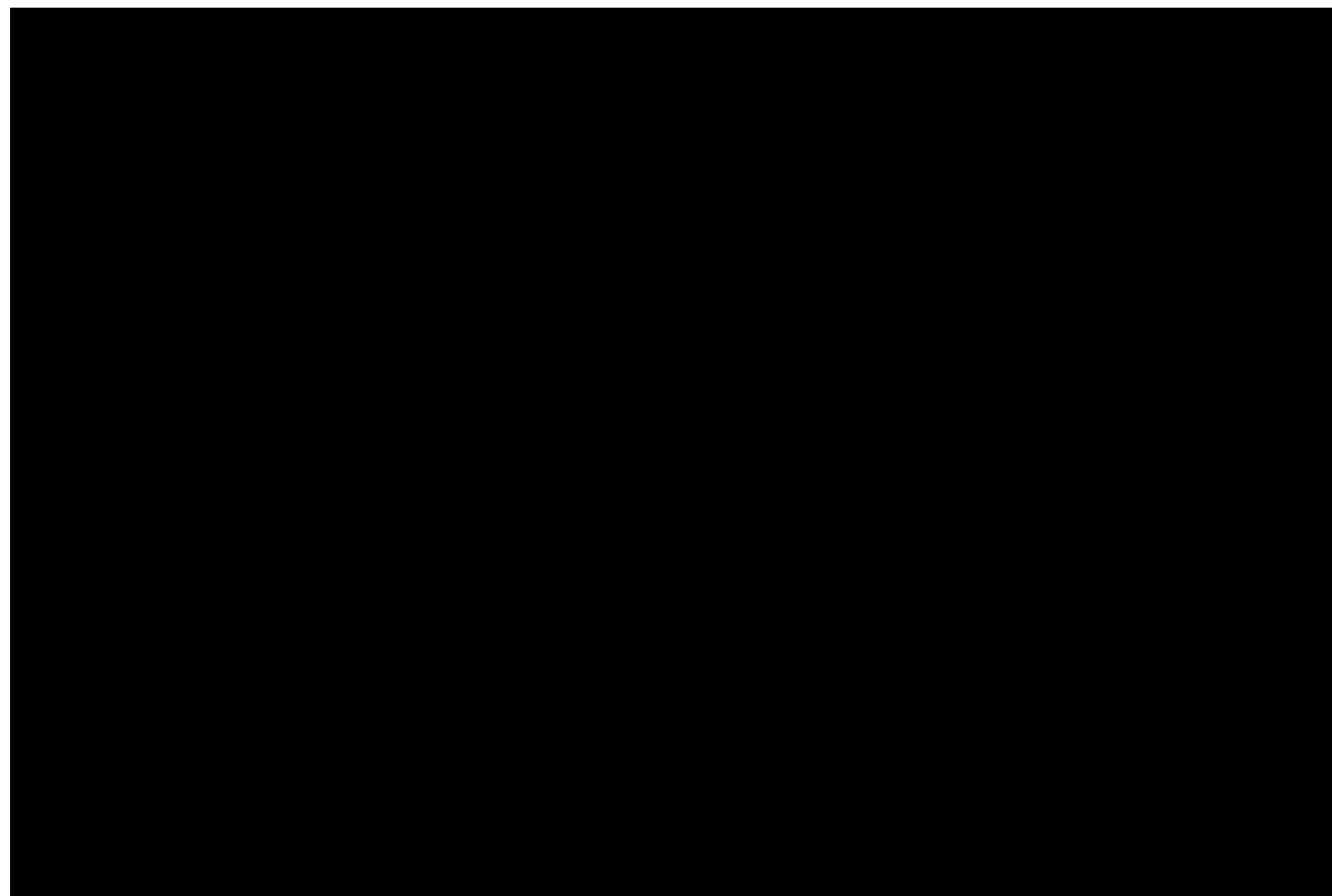
Each color represents a vote. Black corresponds to a non-valid vote, in case of a tie for example.

ZERO: A local foreign grid origin detector

Original



Forged



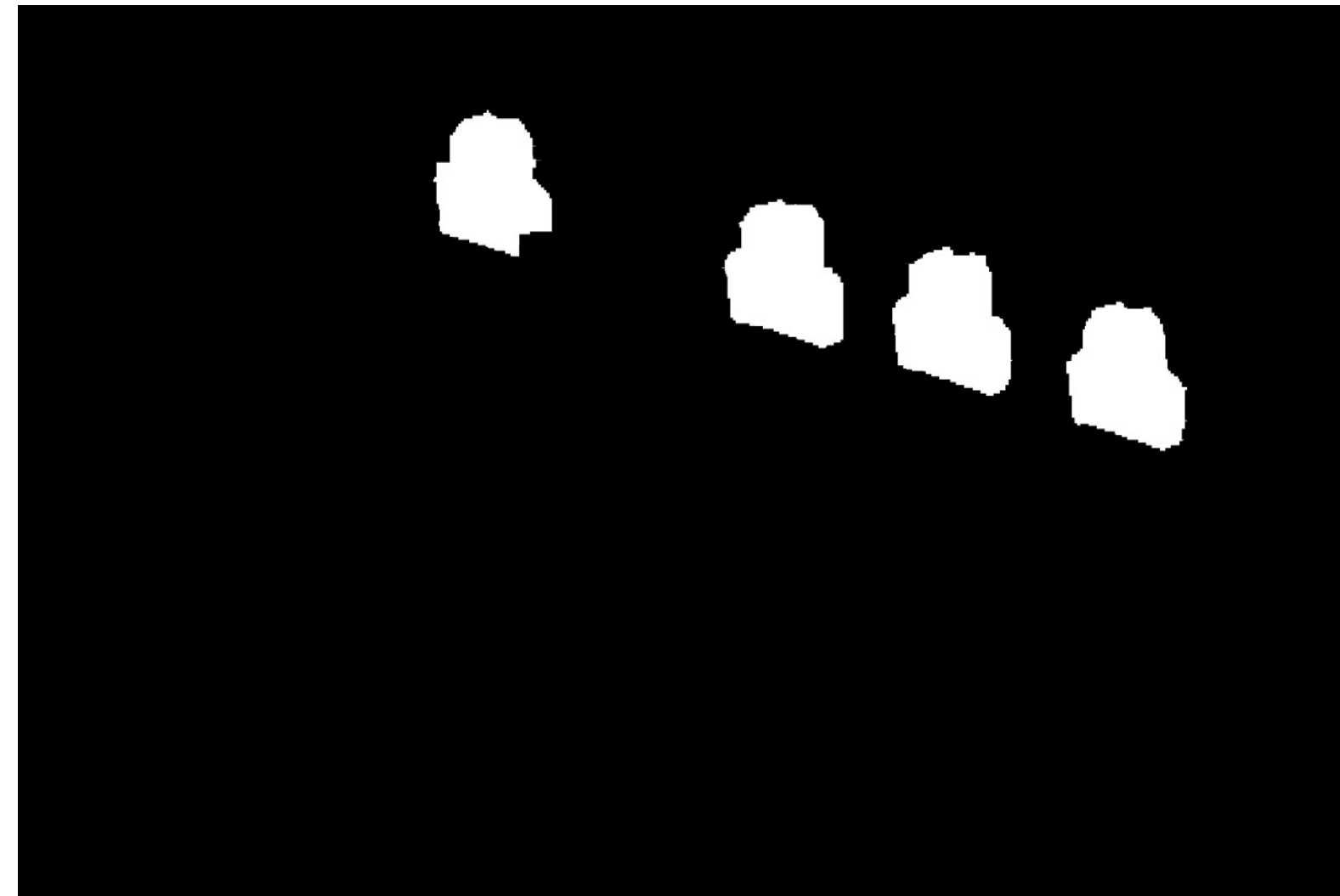
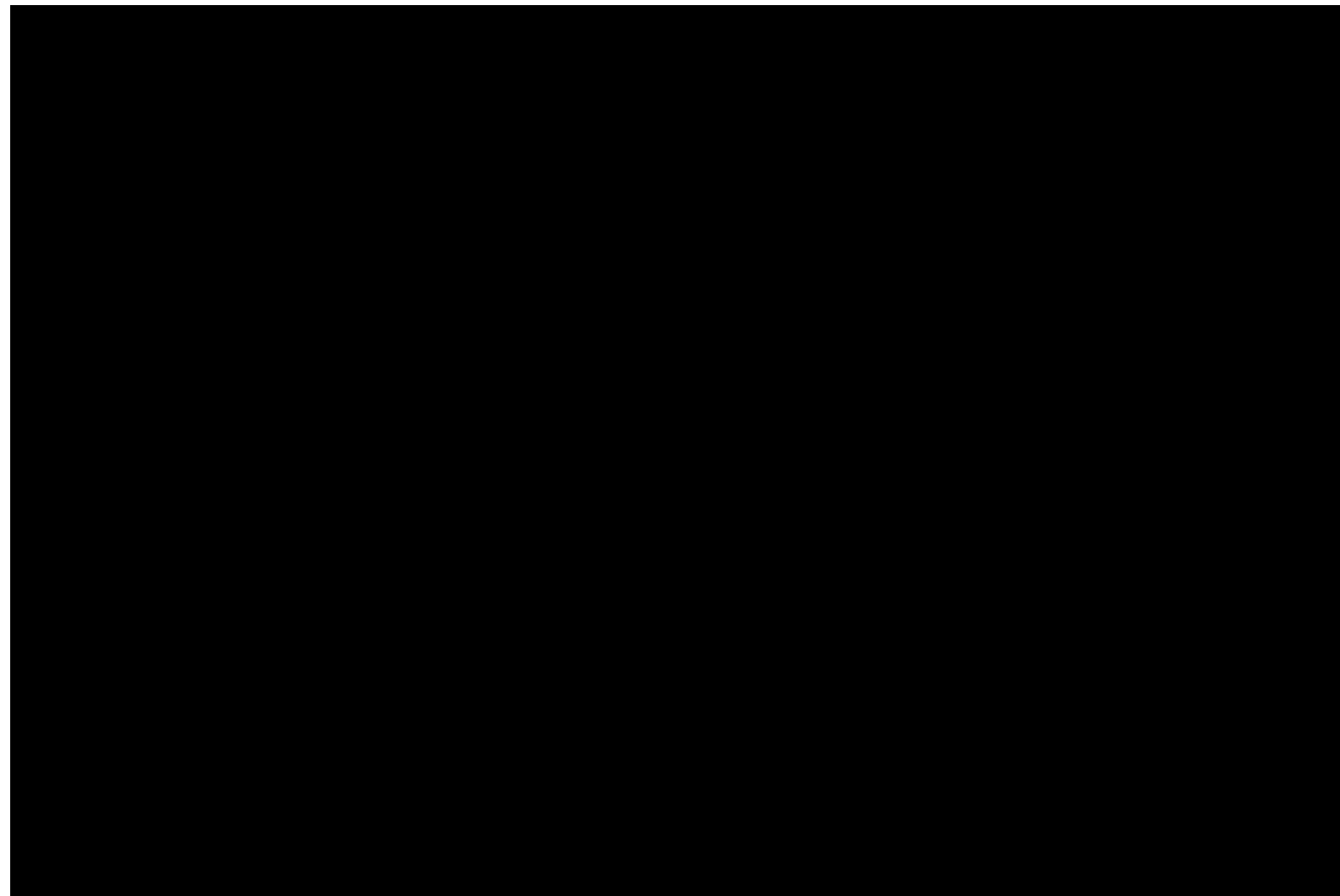
Raw forgery maps

ZERO: A local foreign grid origin detector

Original



Forged



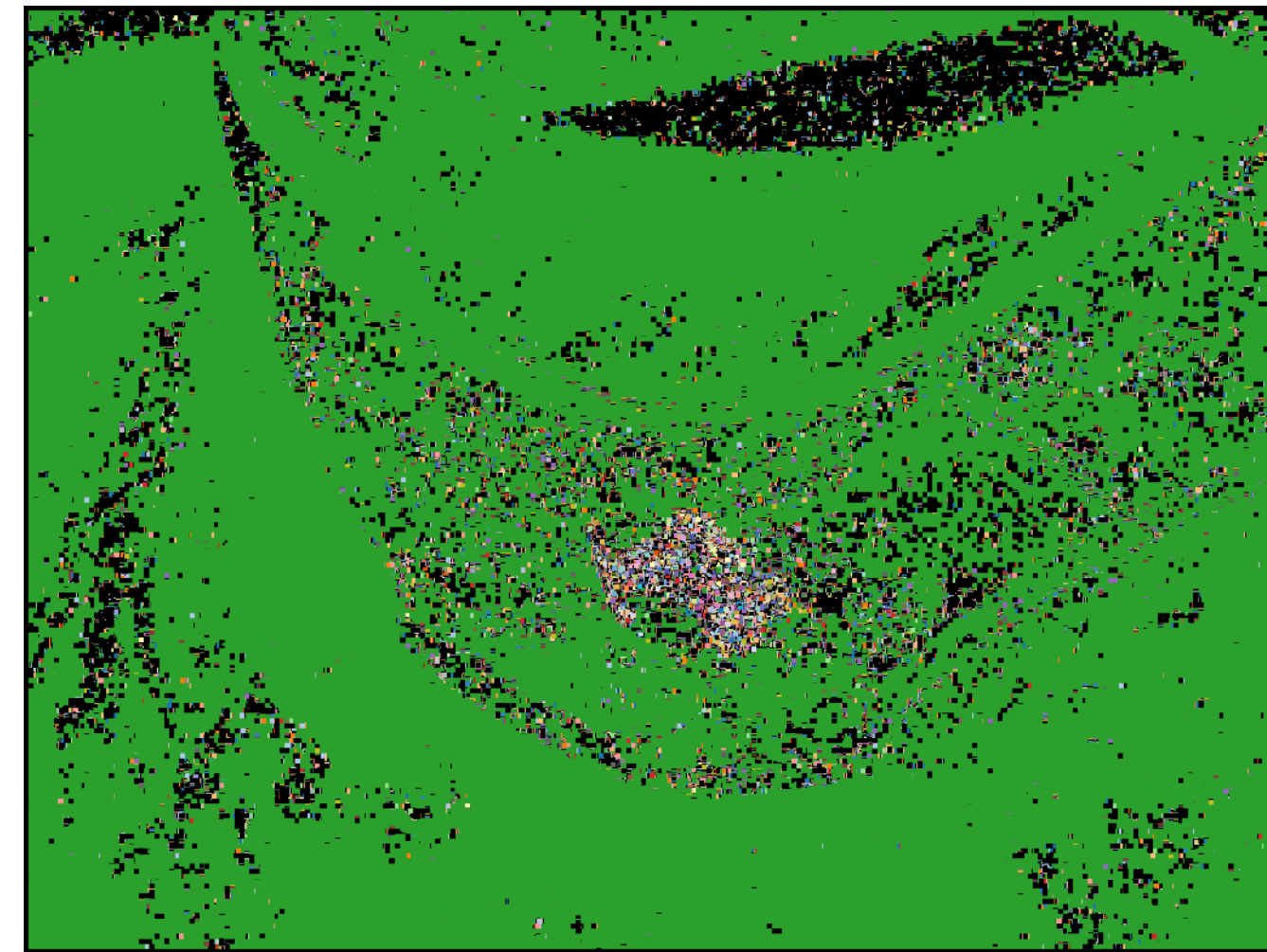
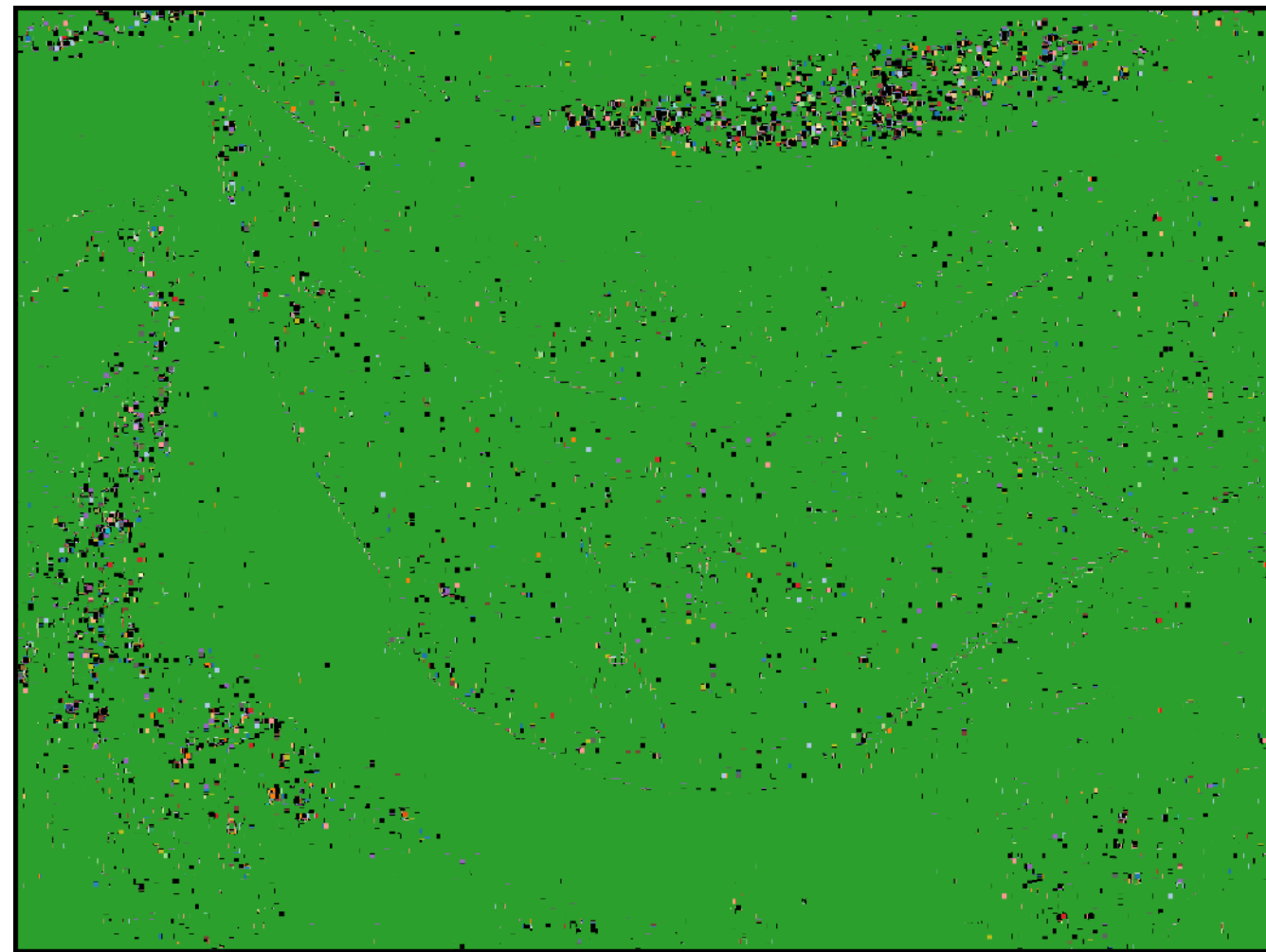
Final forgery mask

ZERO: A local missing grid origin detector

Original



Forged



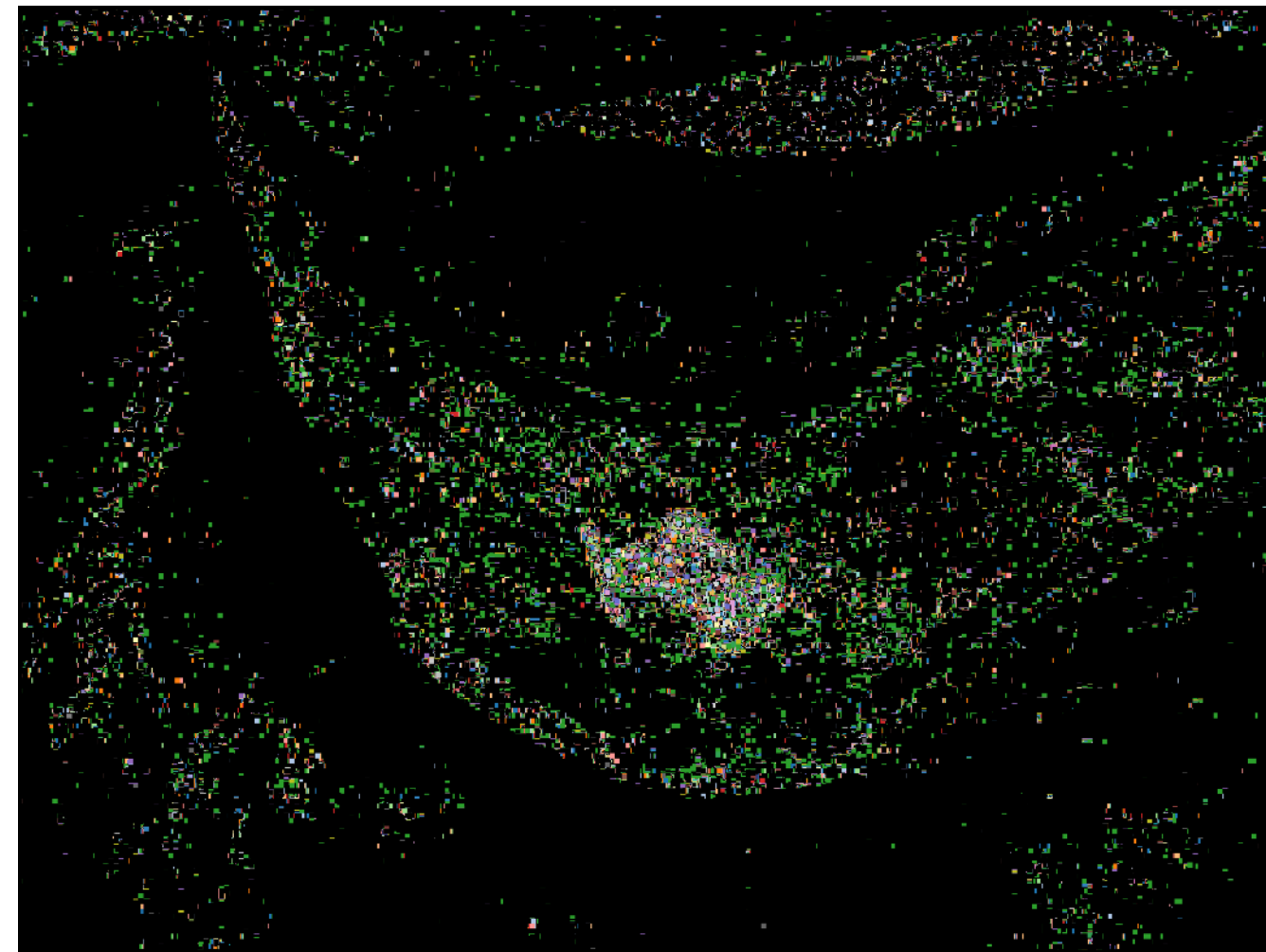
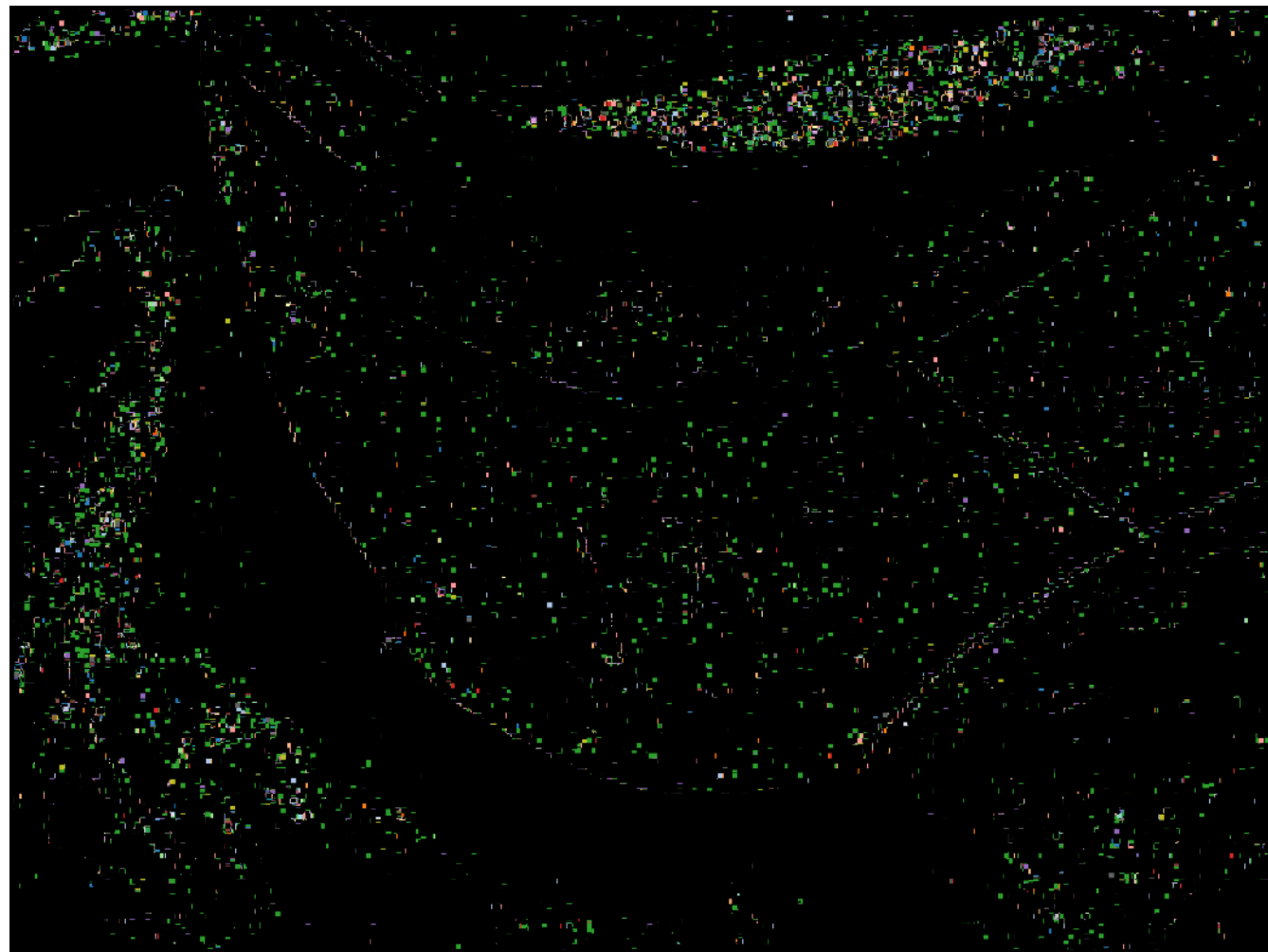
Each color represents a vote. Black corresponds to a non-valid vote, in case of a tie for example.

ZERO: A local missing grid origin detector

Original



Forged



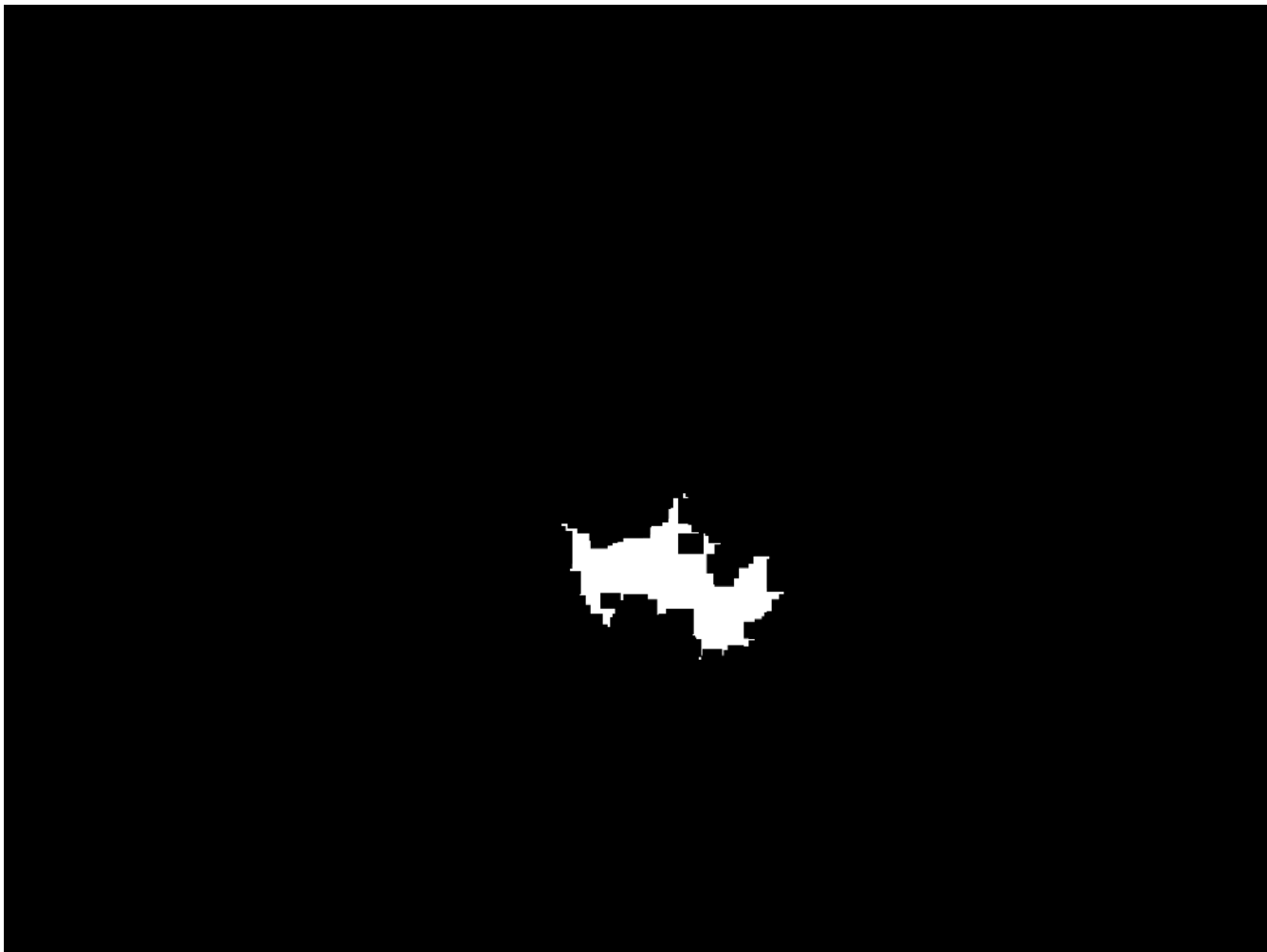
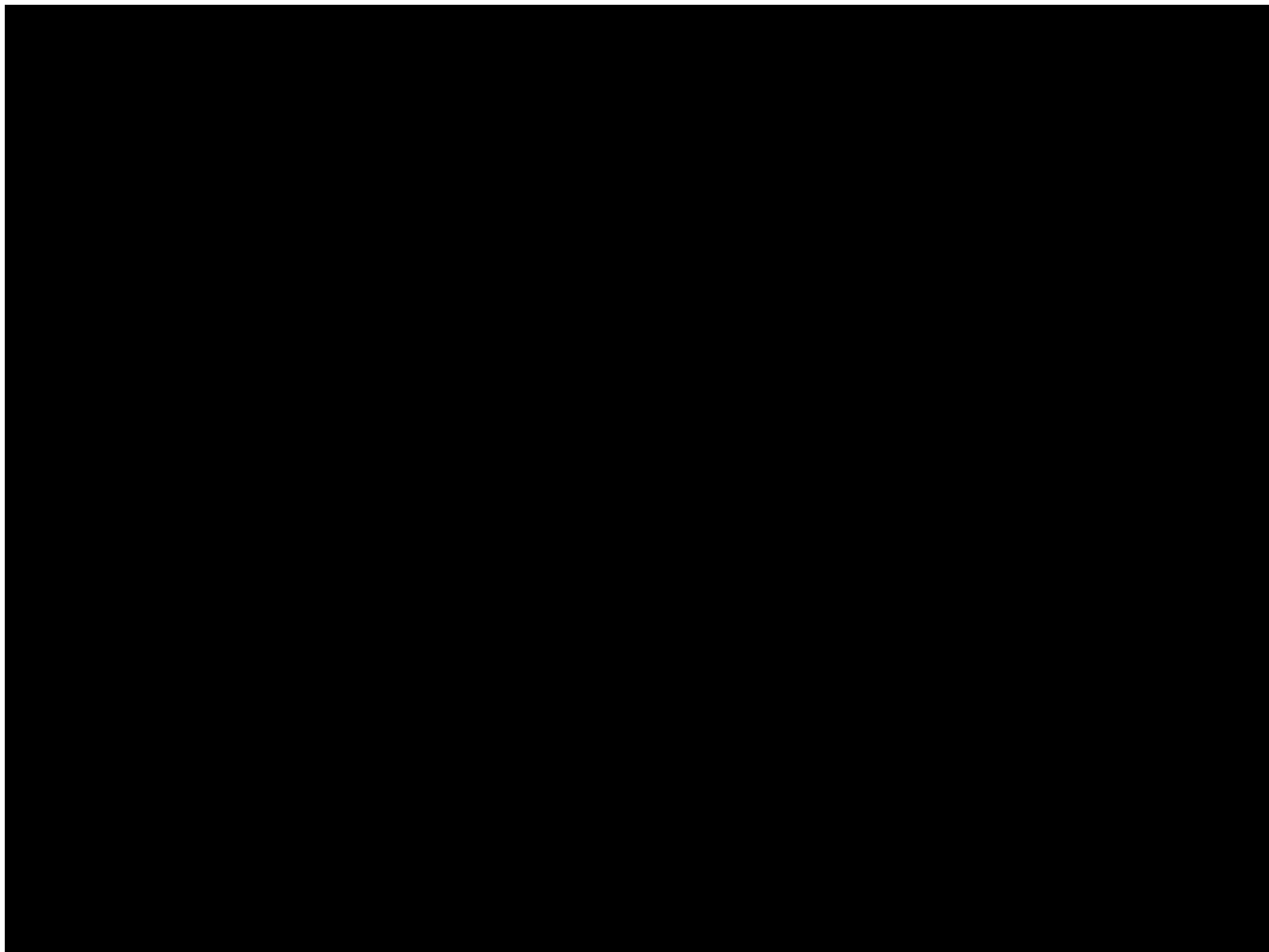
Each color represents a vote. Black corresponds to a non-valid vote, in case of a tie for example or a pixel that already voted.

ZERO: A local missing grid origin detector

Original

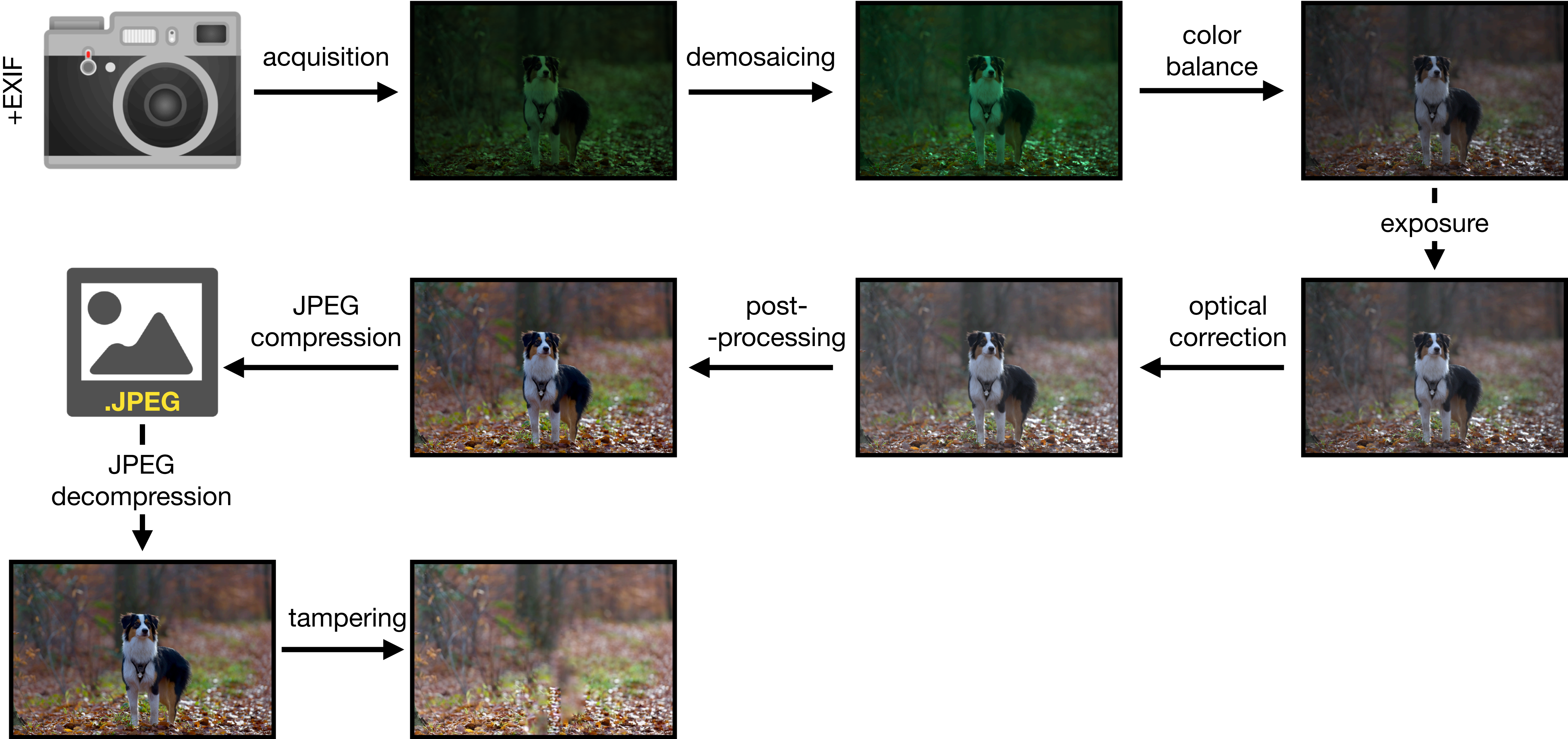


Forged

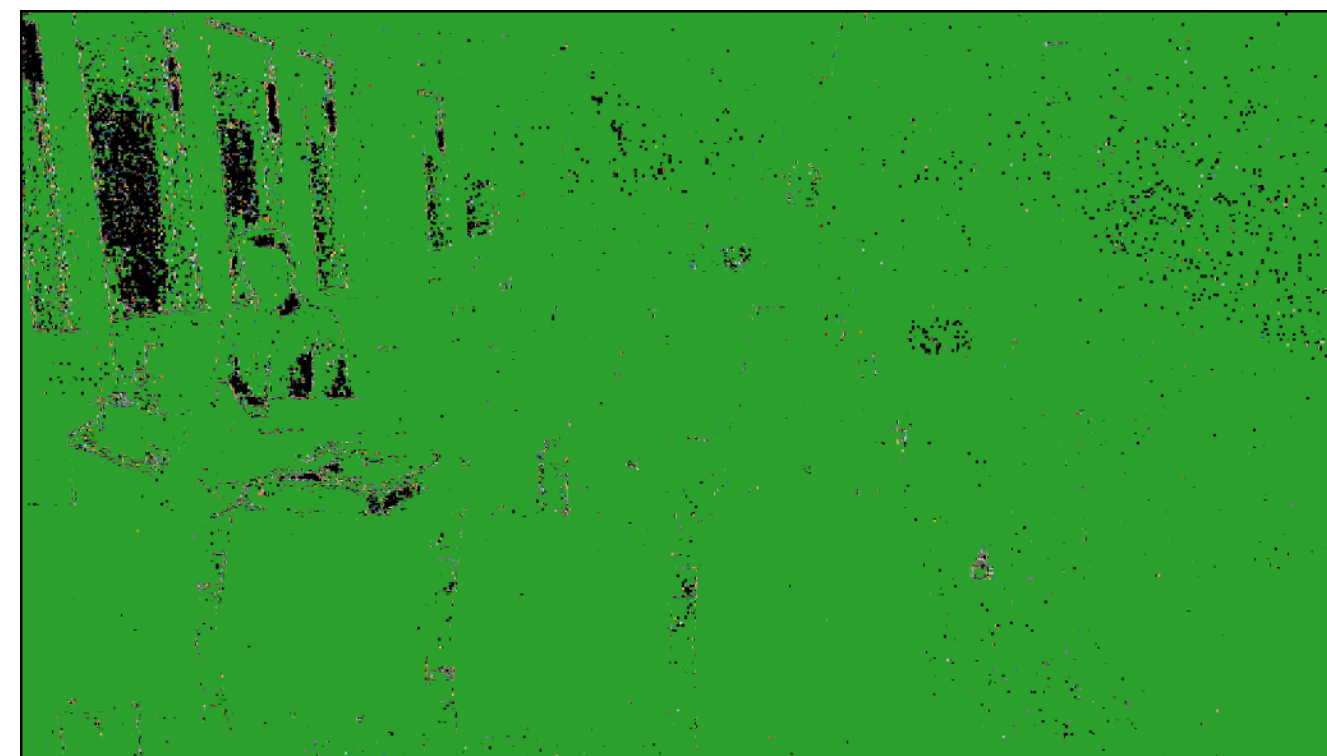


Final forgery mask

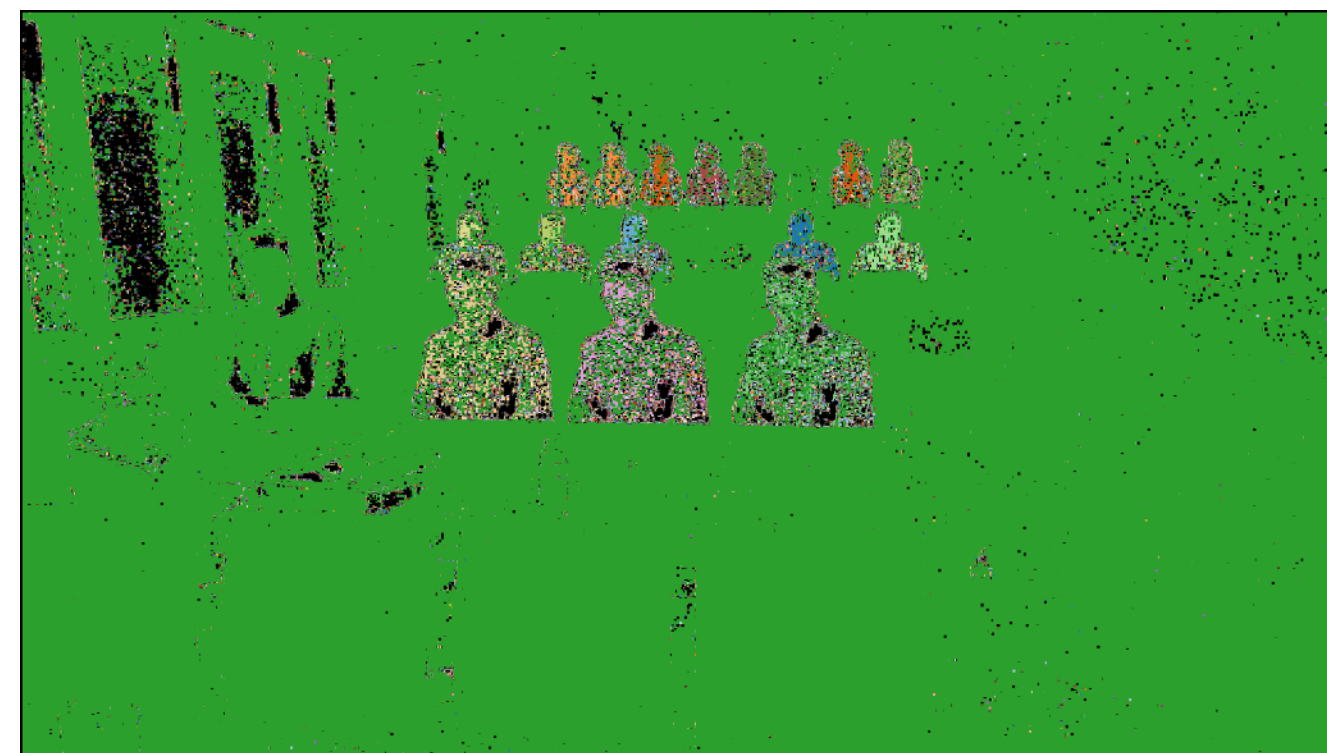
Image processing pipeline



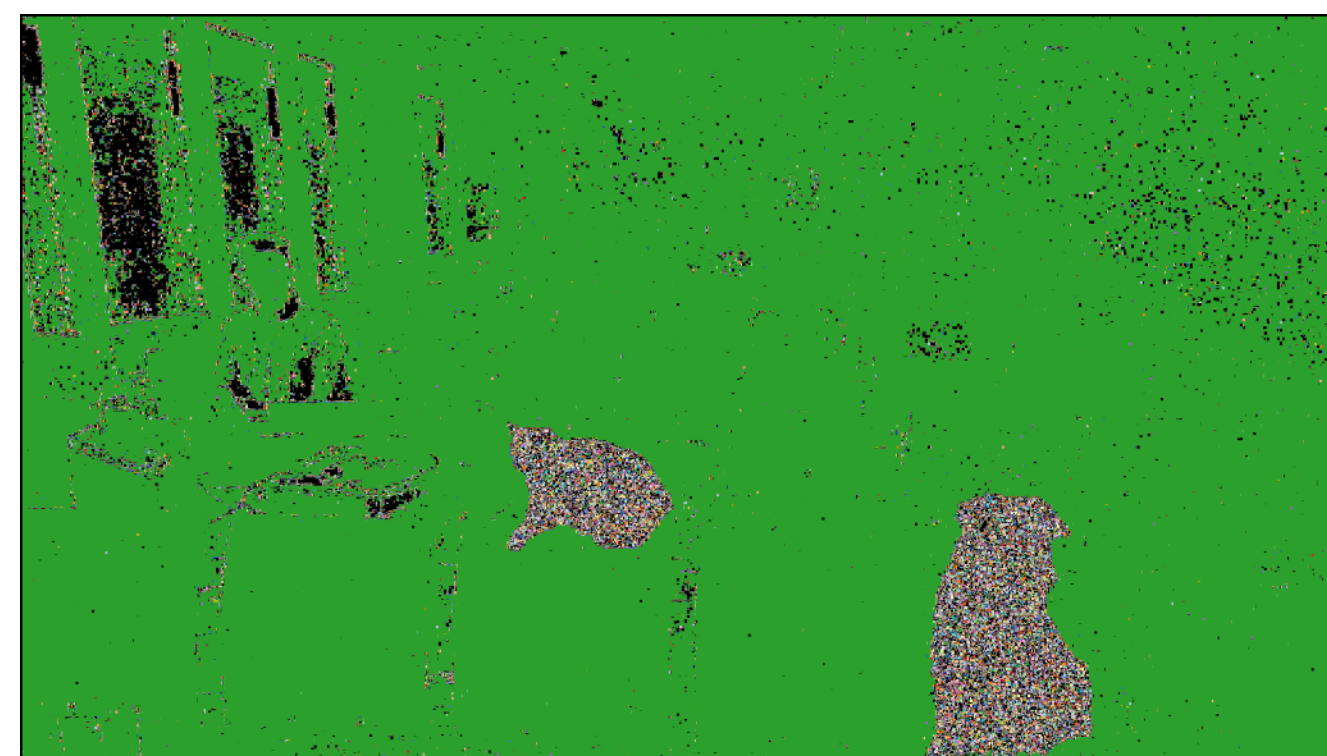
1. Global grid detection and main grid detection



Main grid (0,0)
JPEG image

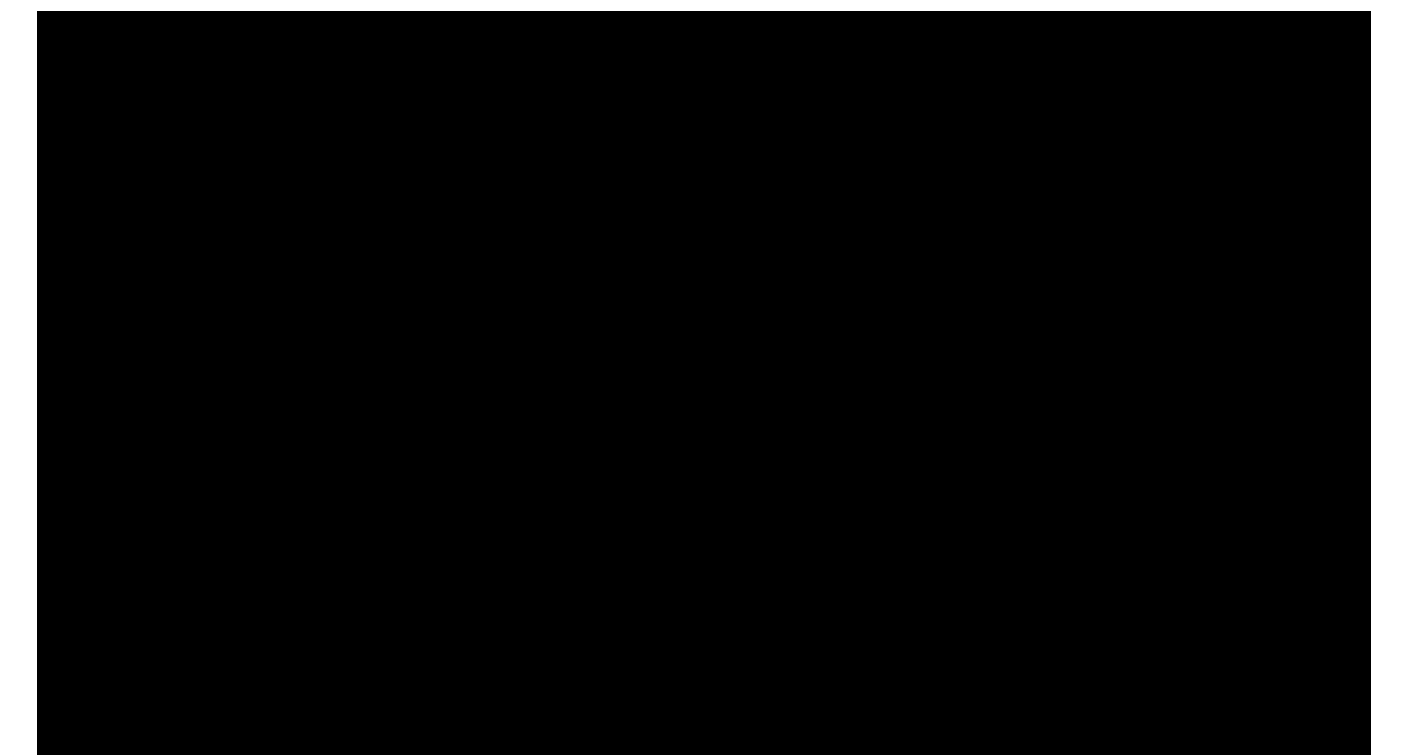
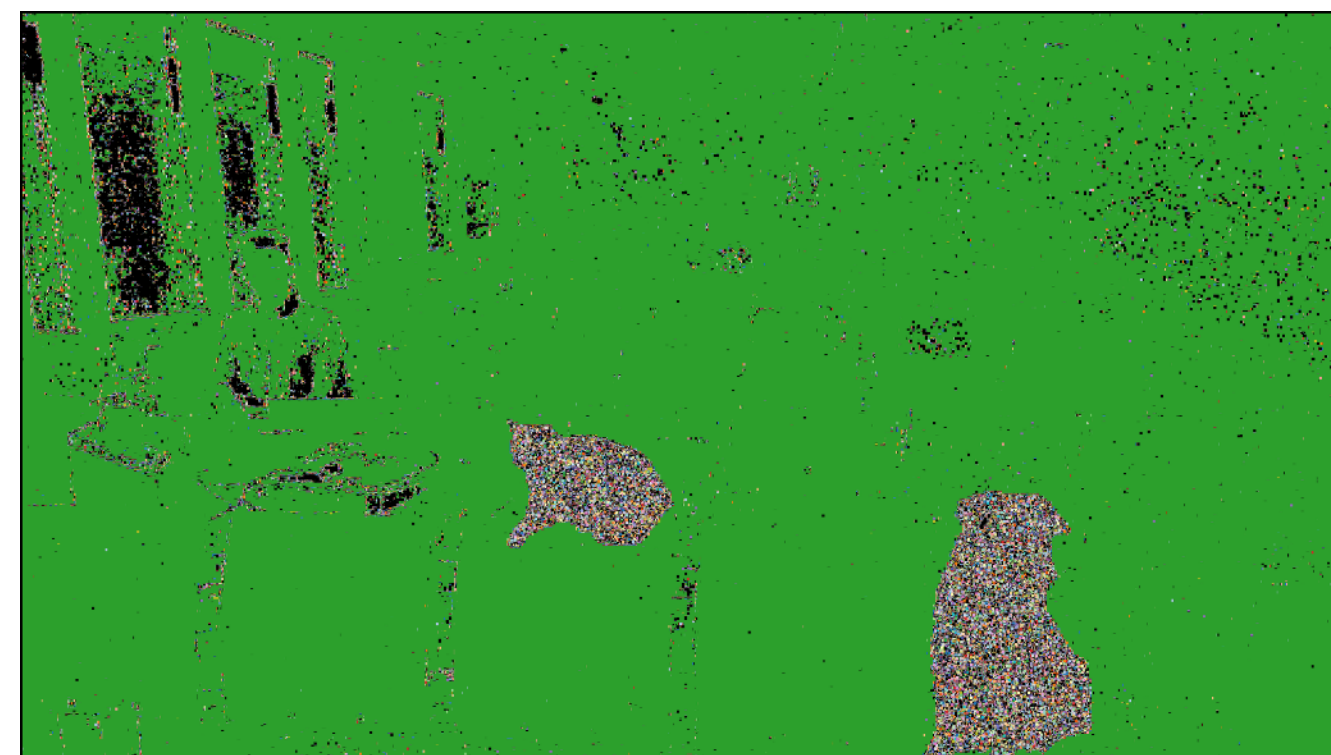
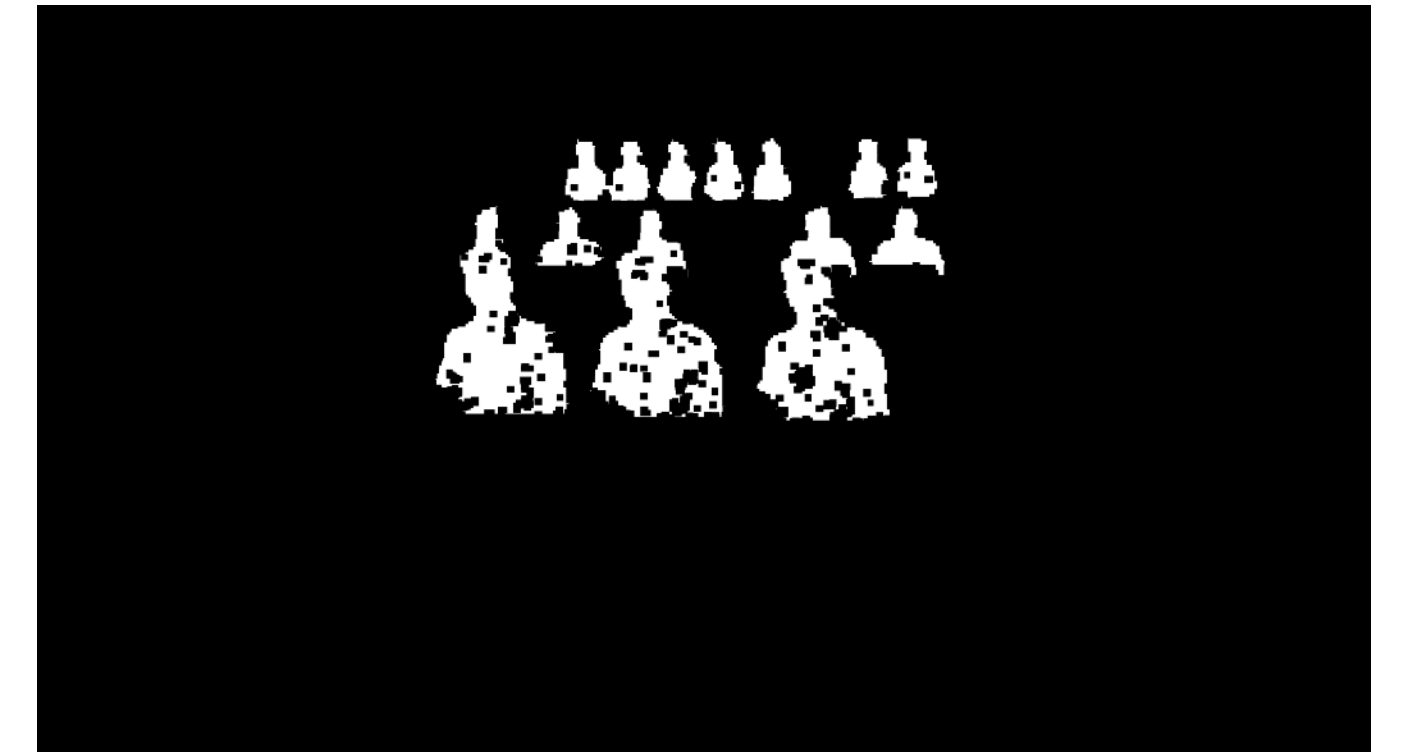
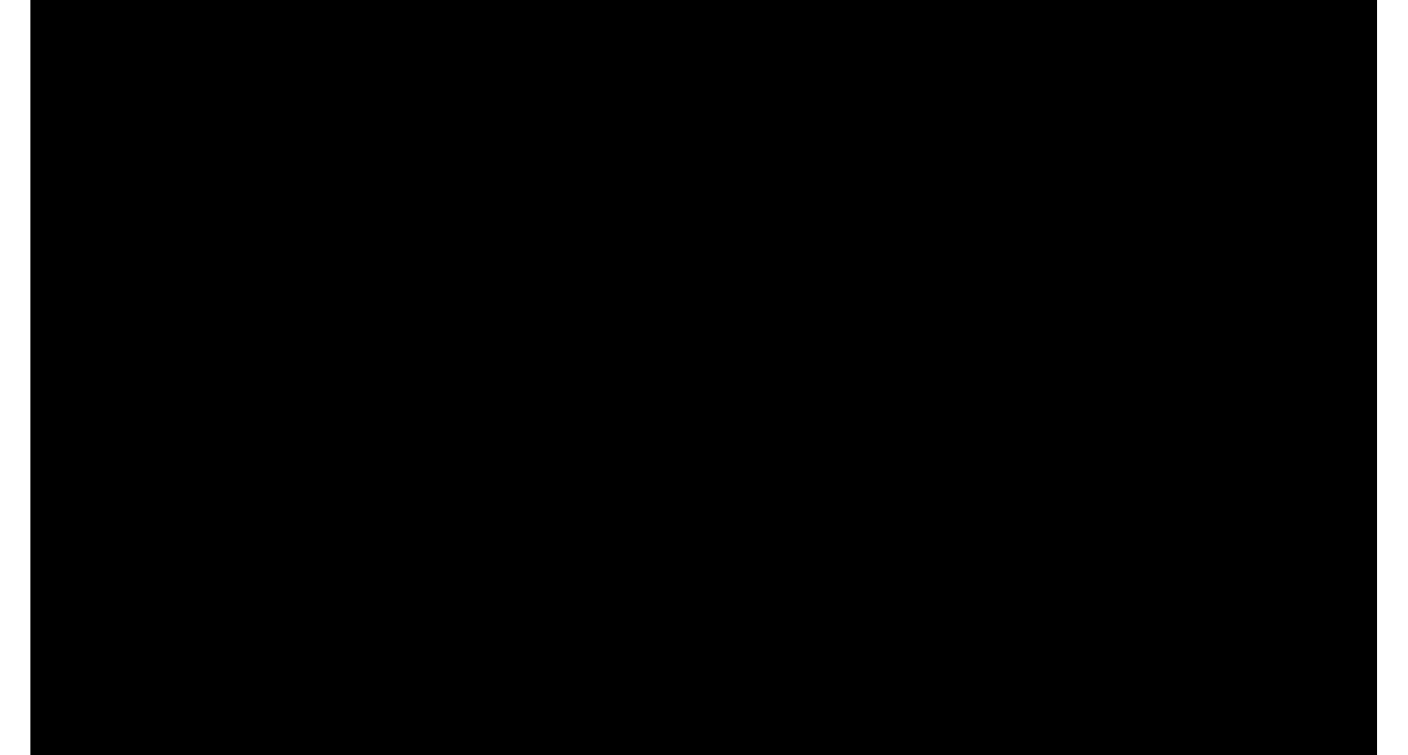
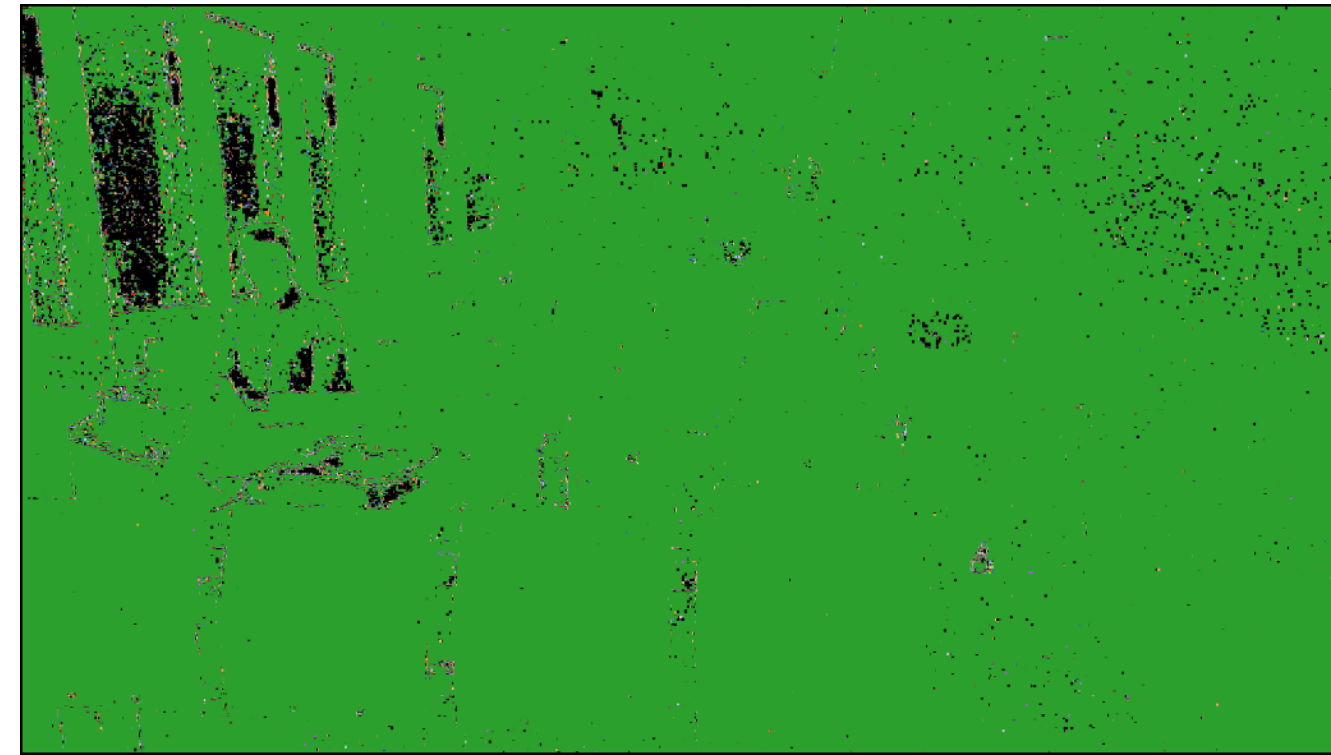


Main grid (0,0)
JPEG image

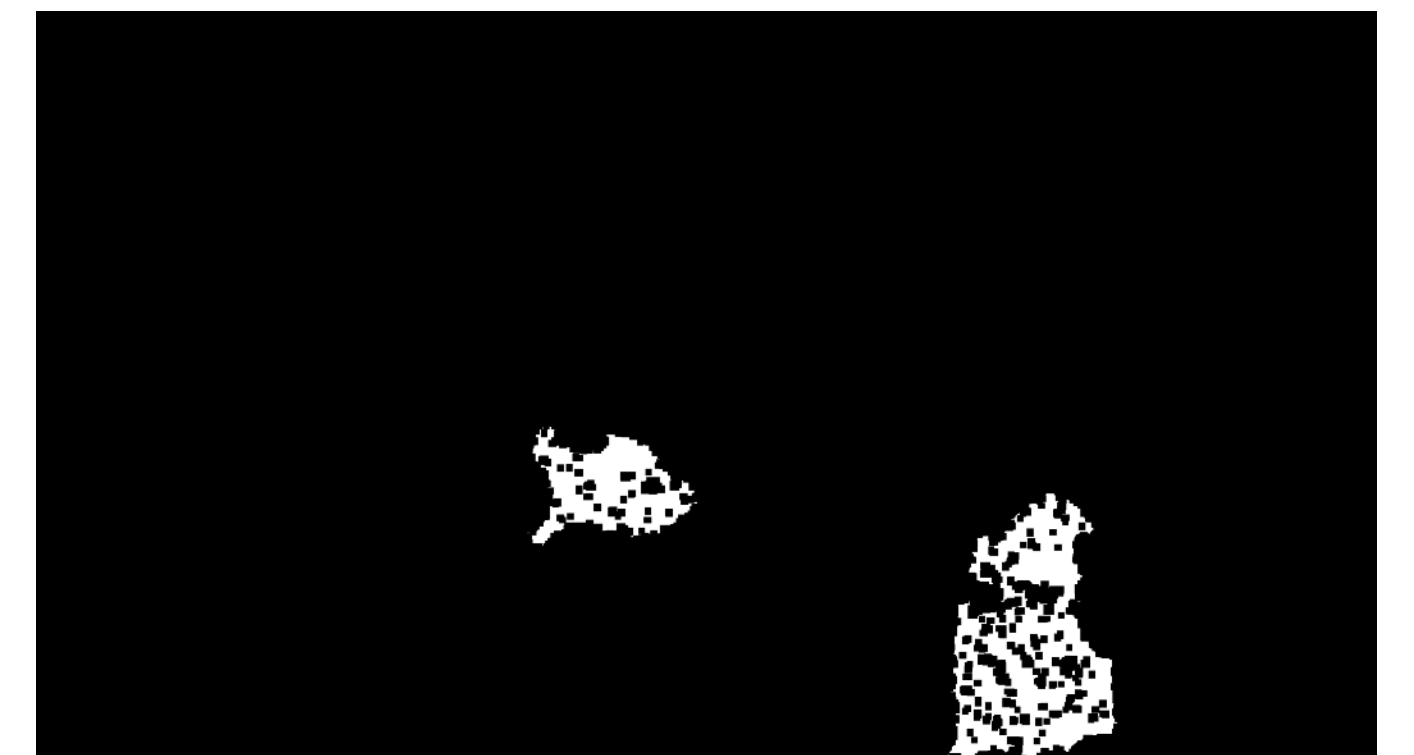
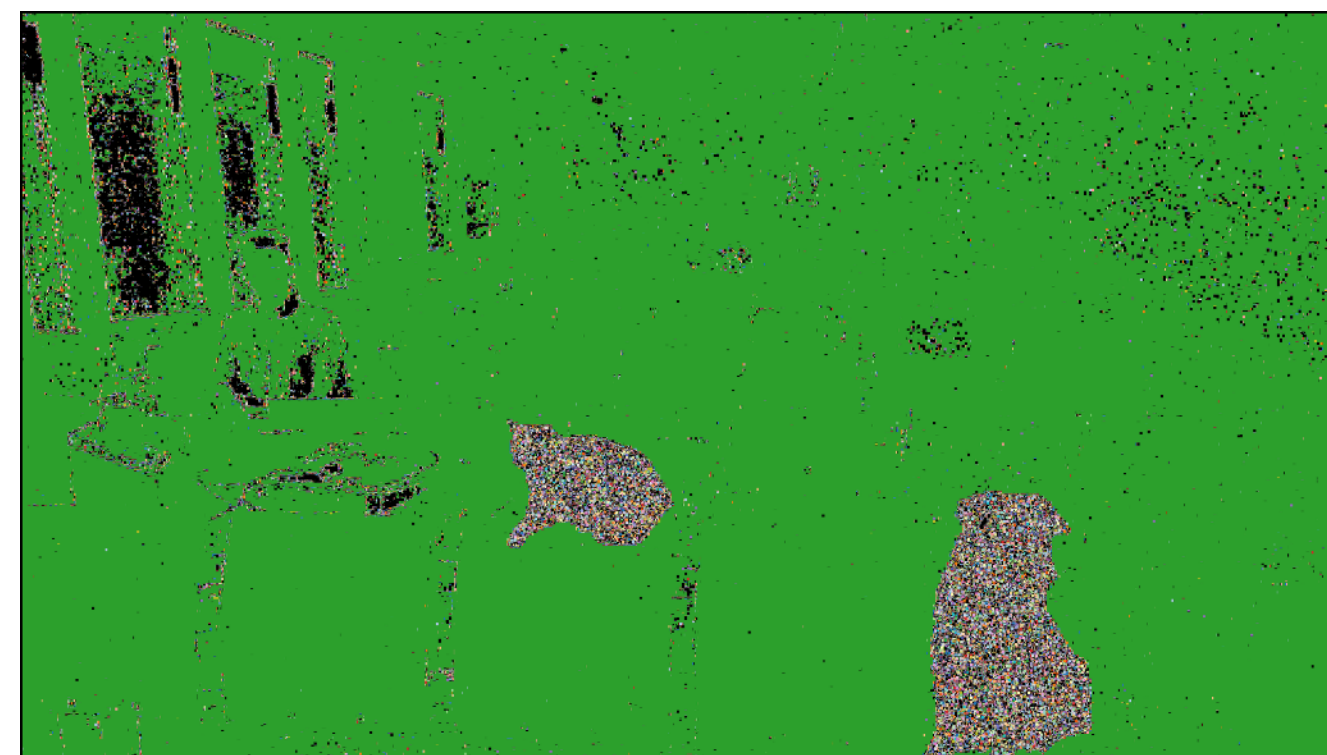
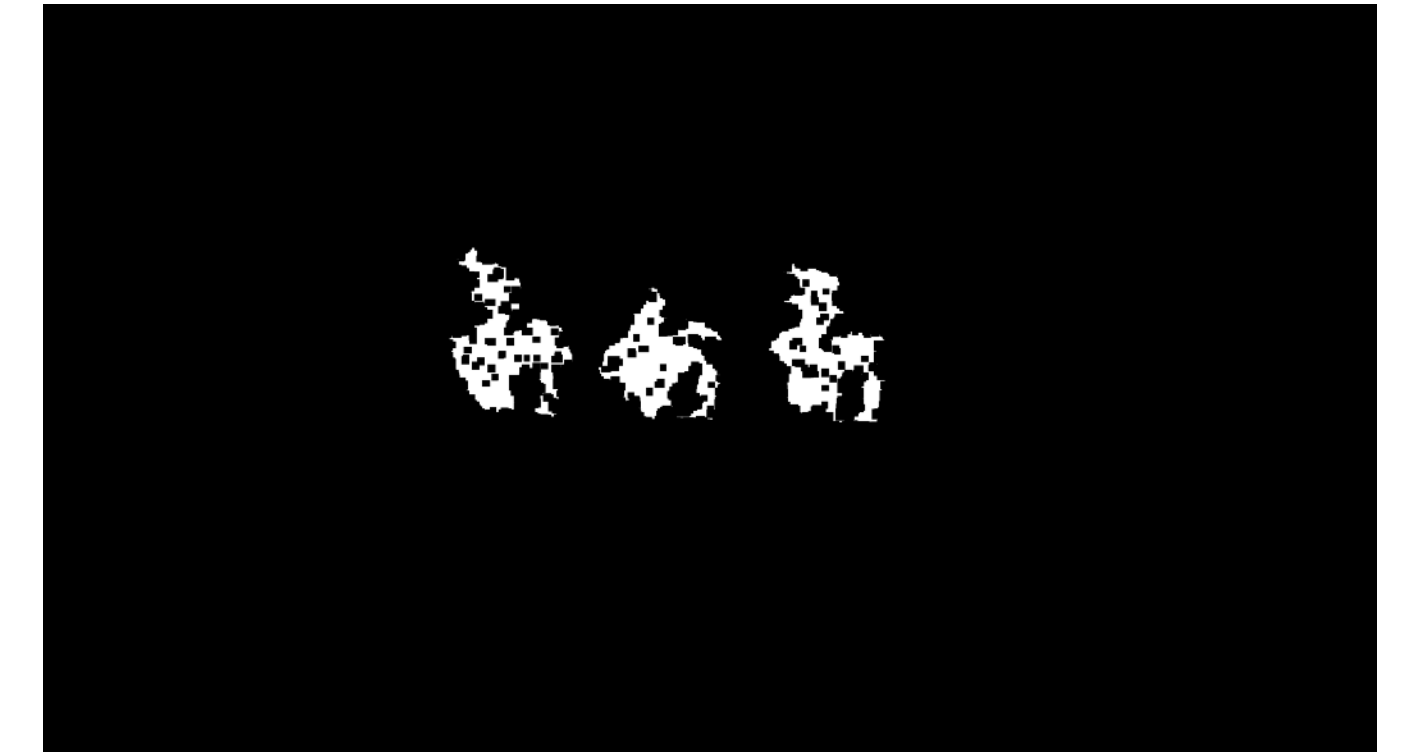
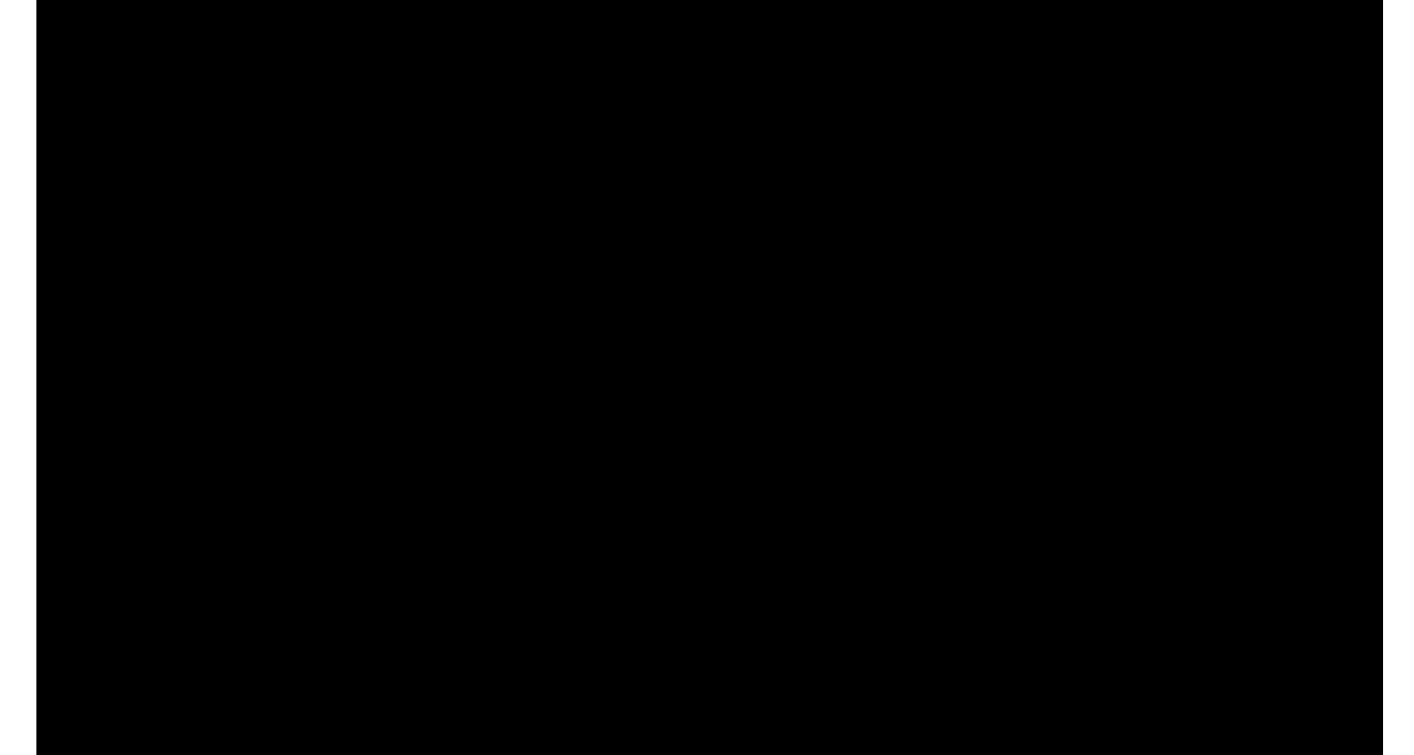
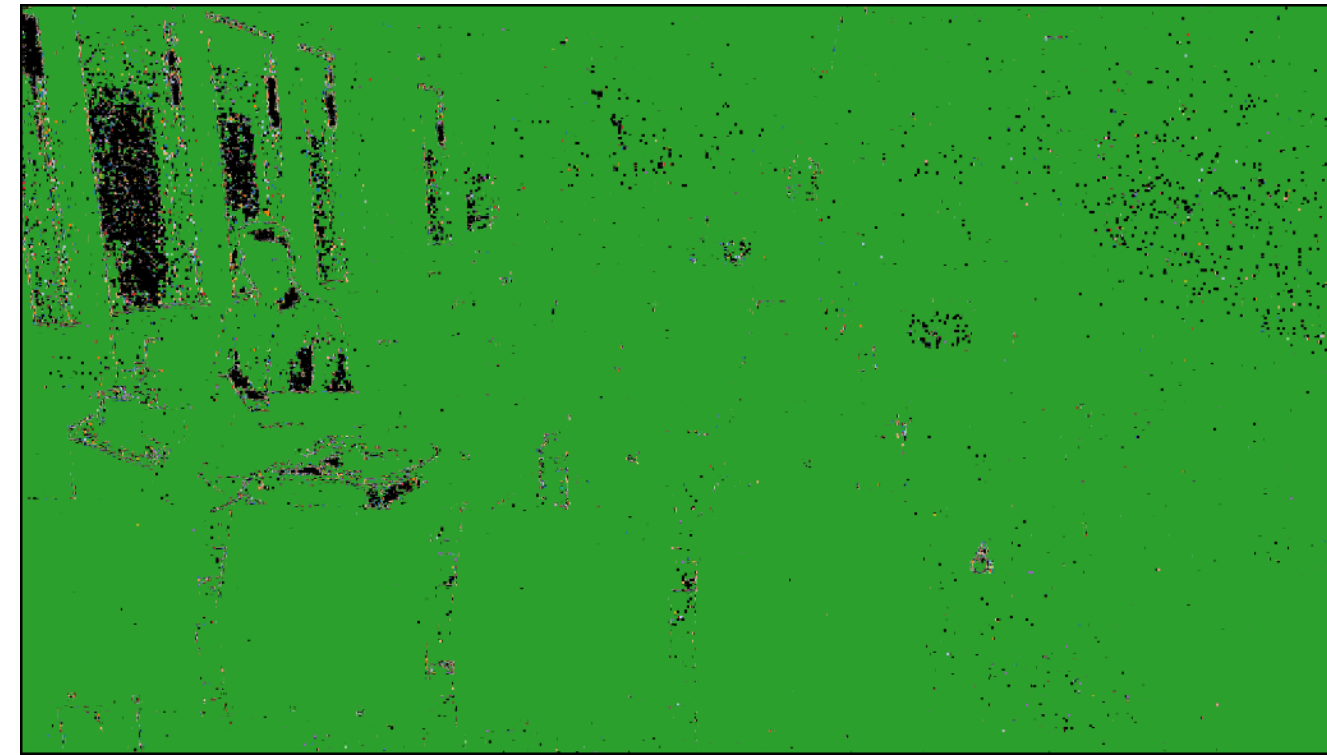


Main grid (0,0)
JPEG image

2. Local foreign grid detection



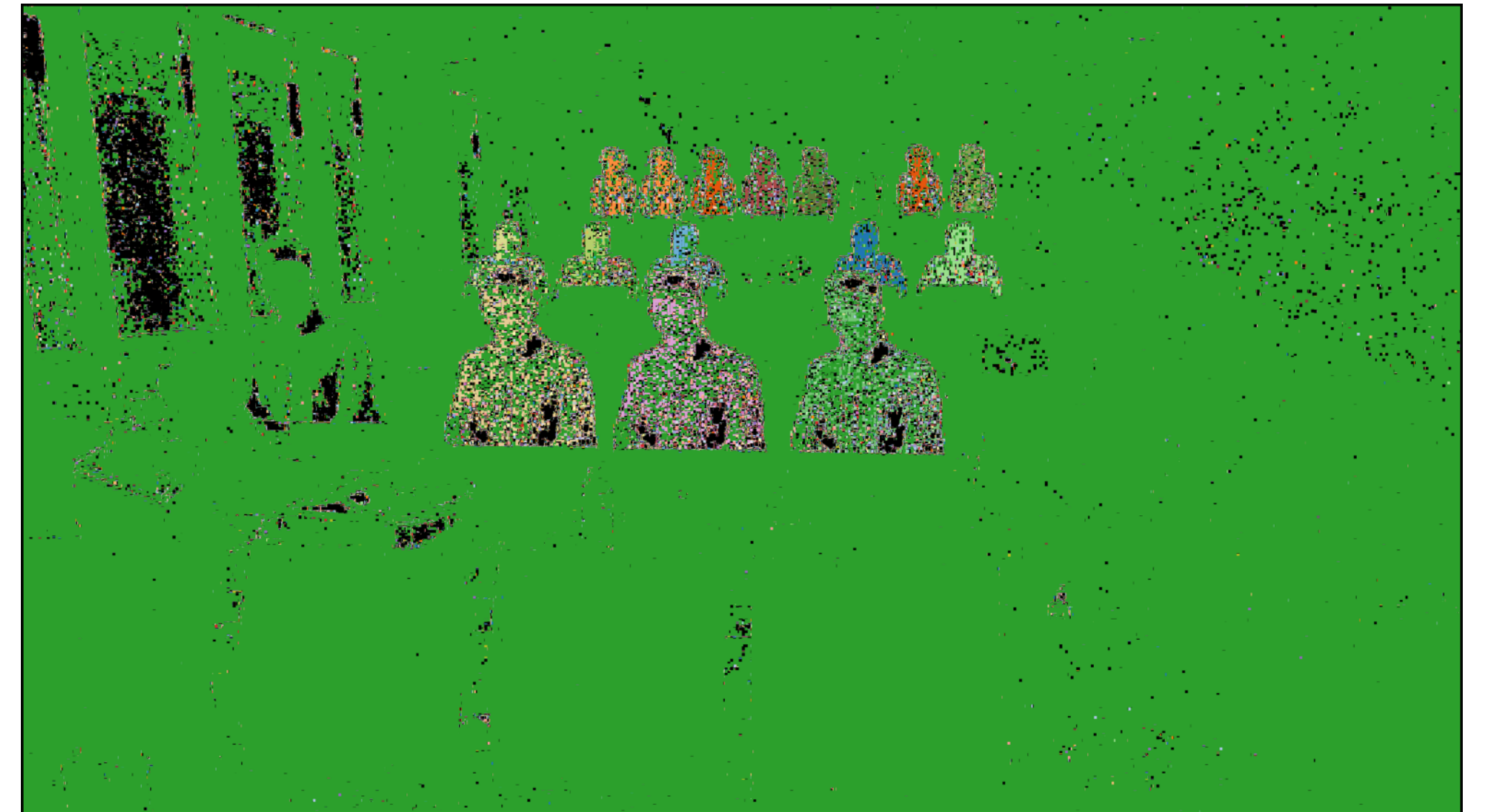
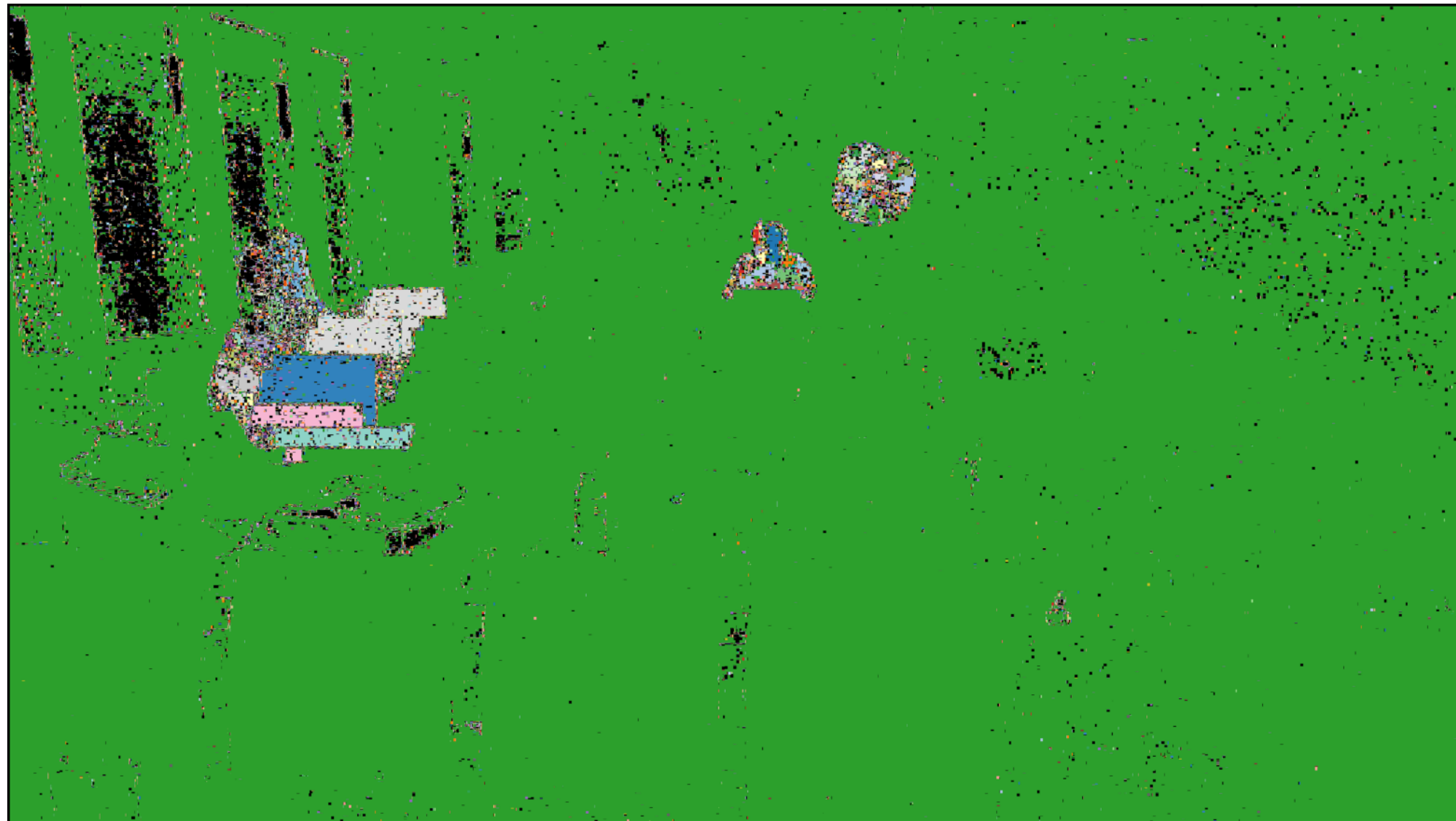
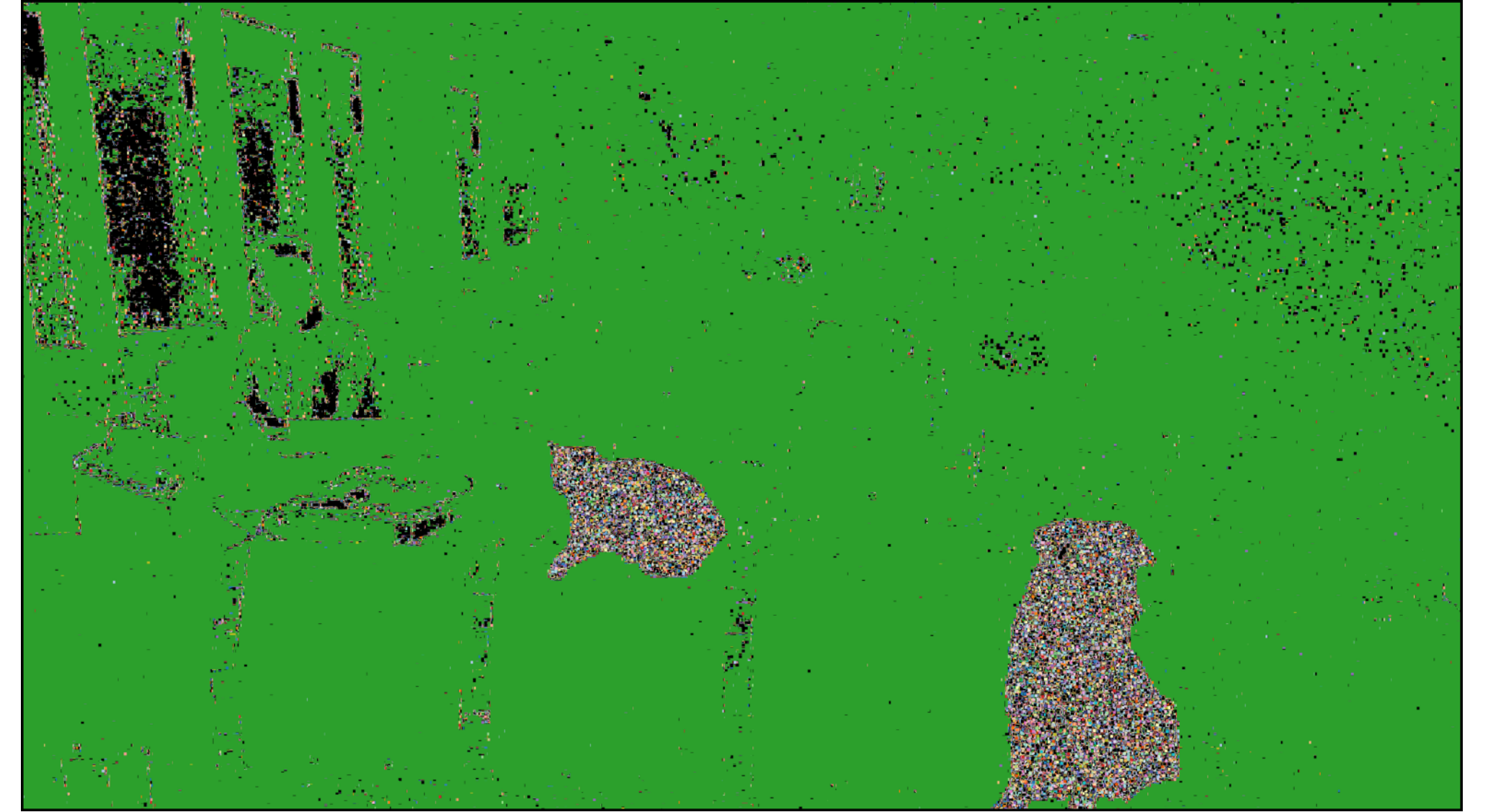
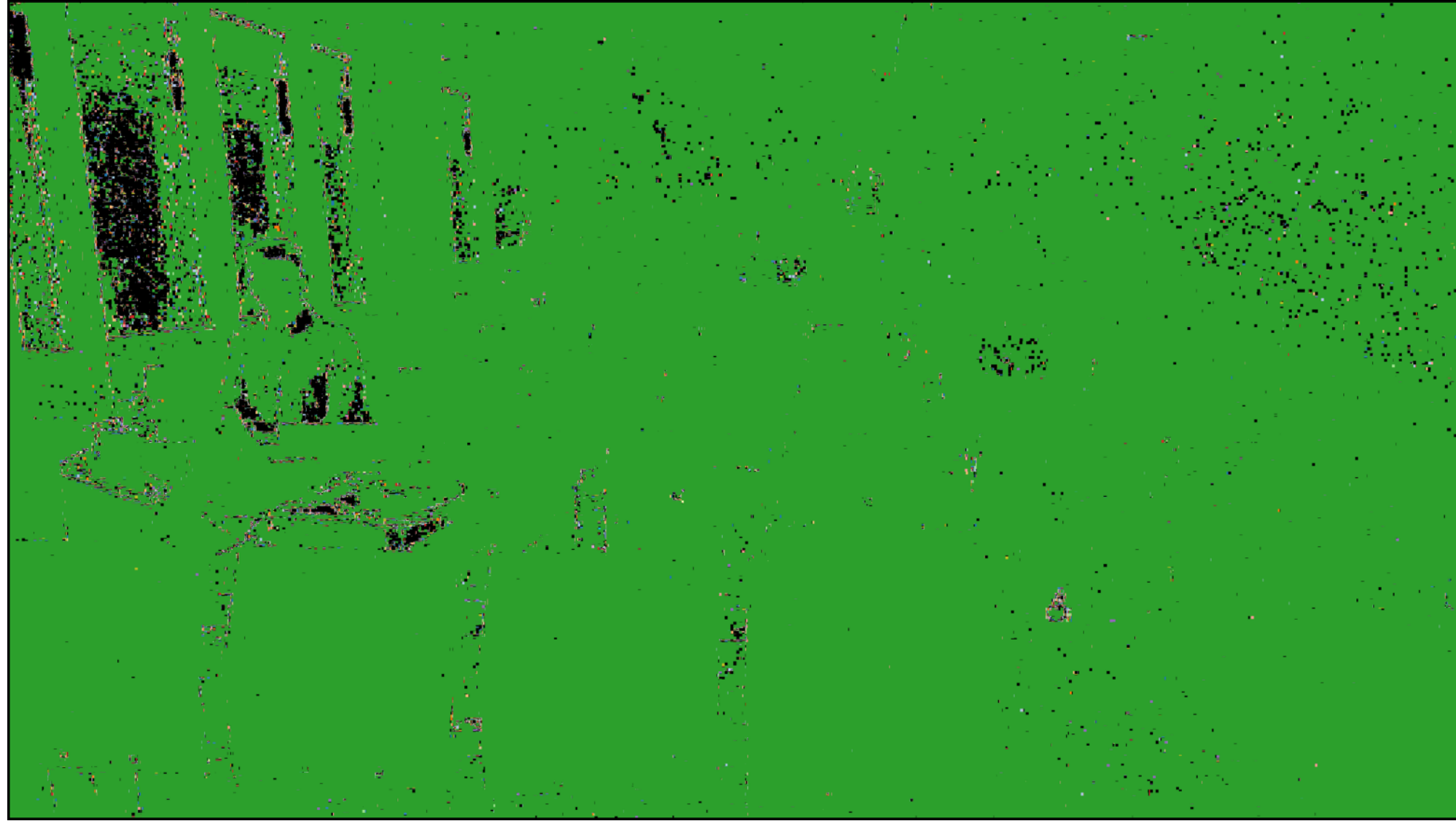
3. Local missing grid detection



ZERO



Global grid detection



Global grid detection

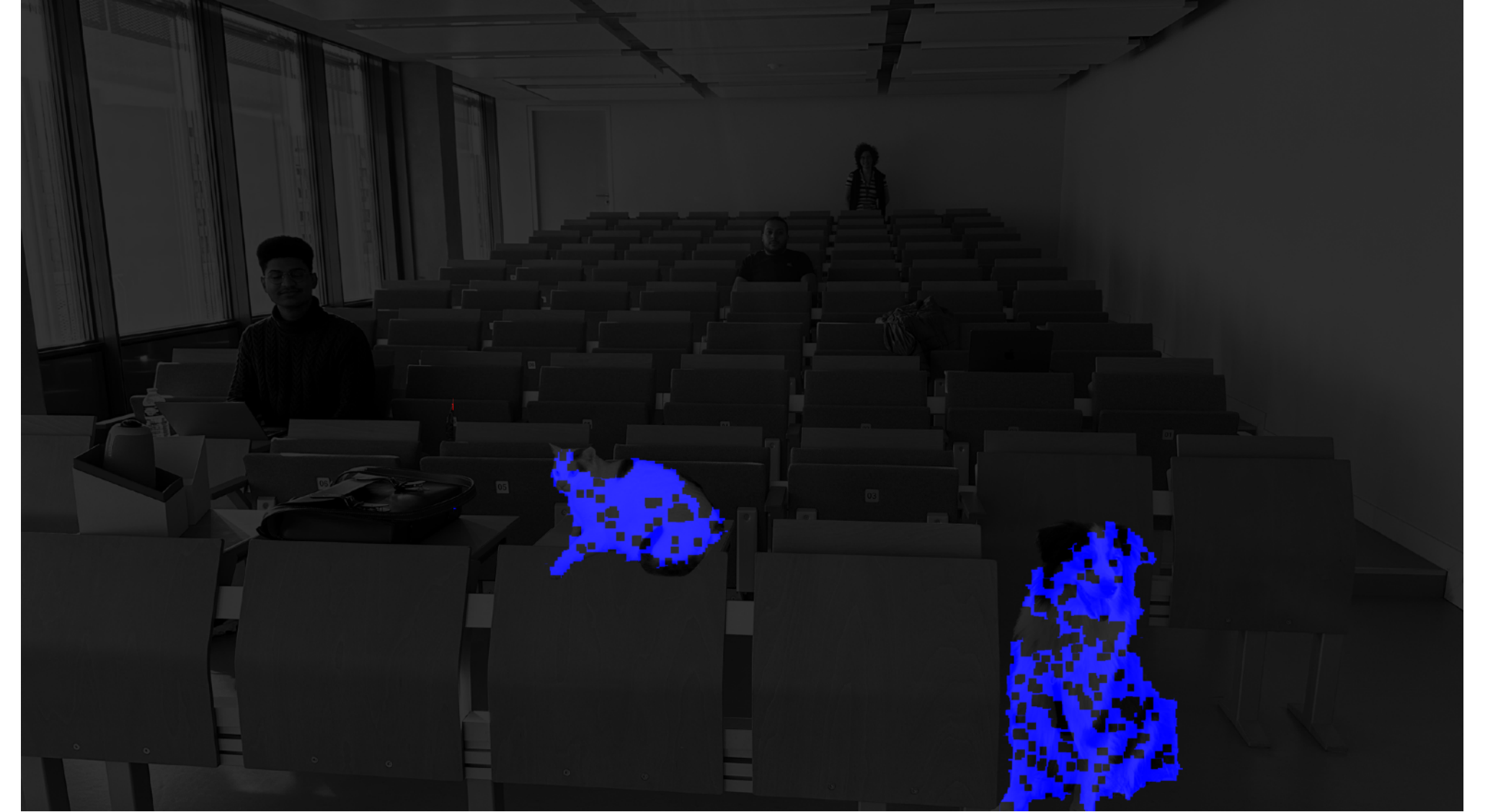
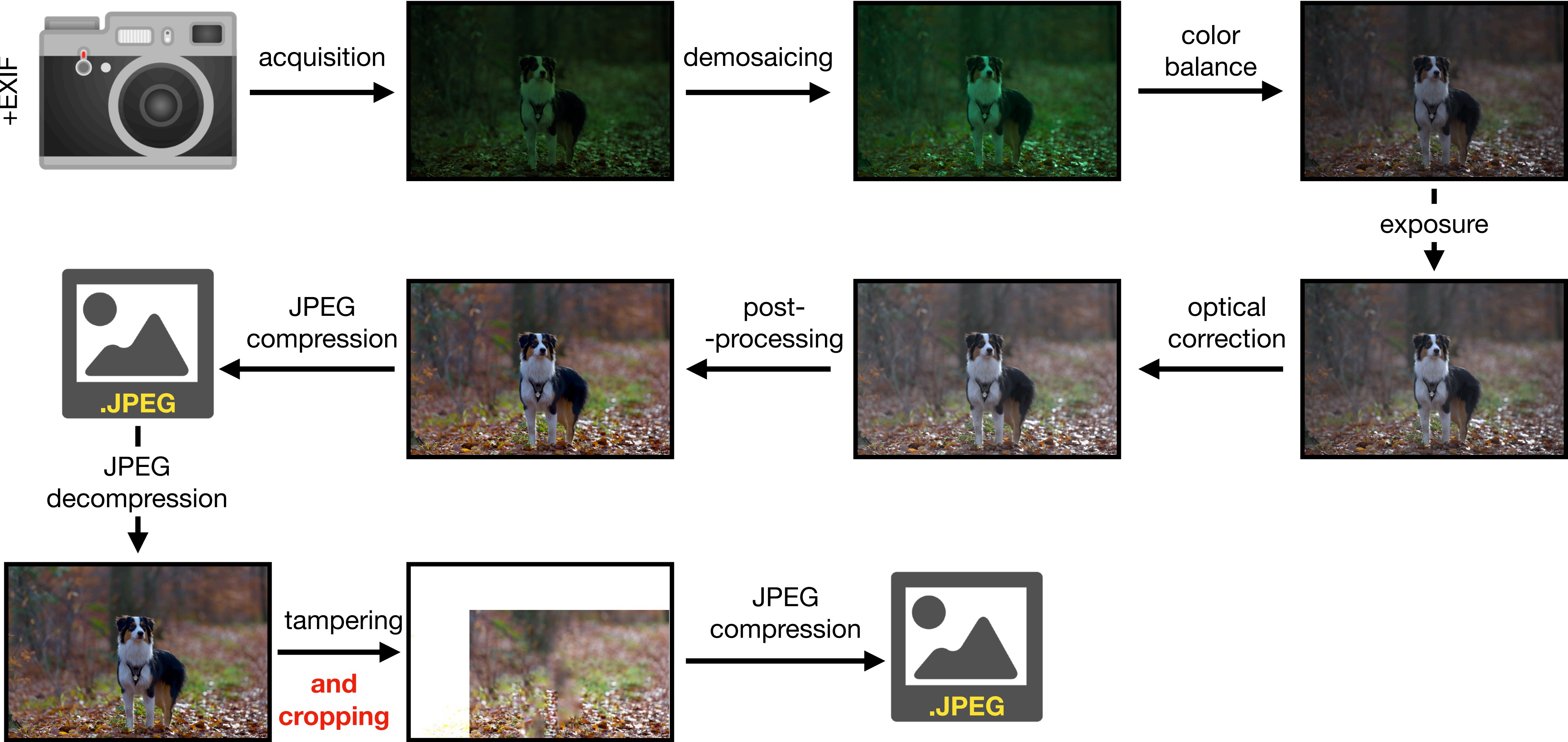
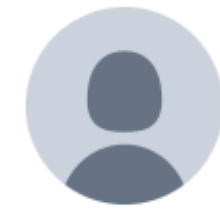


Image processing pipeline





Photoshop is my life



@Adobe



Can you detect these forgeries? [#TinasPhdDefense](#)

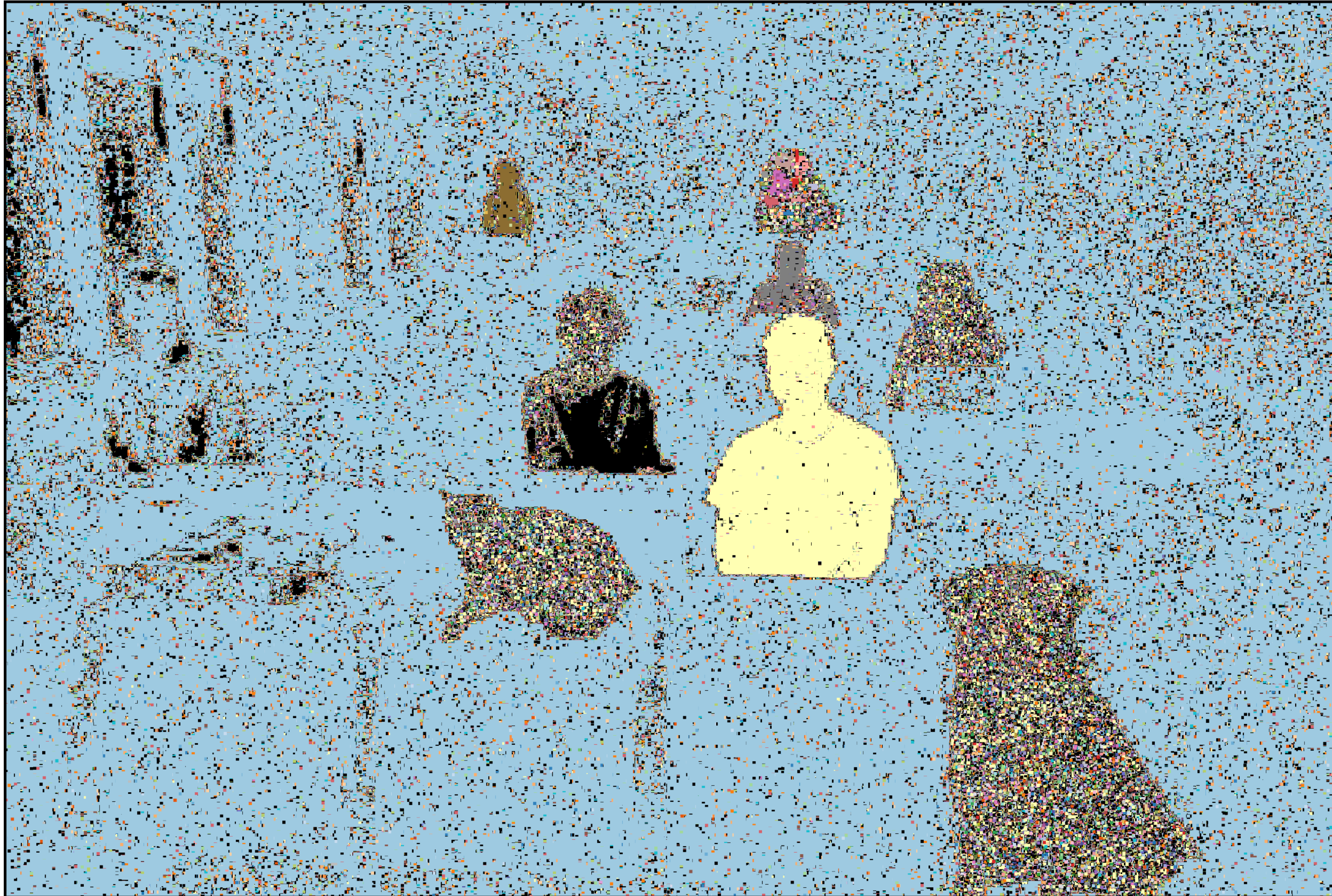


4:10 PM · Nov 8, 2022 · Twitter Web App

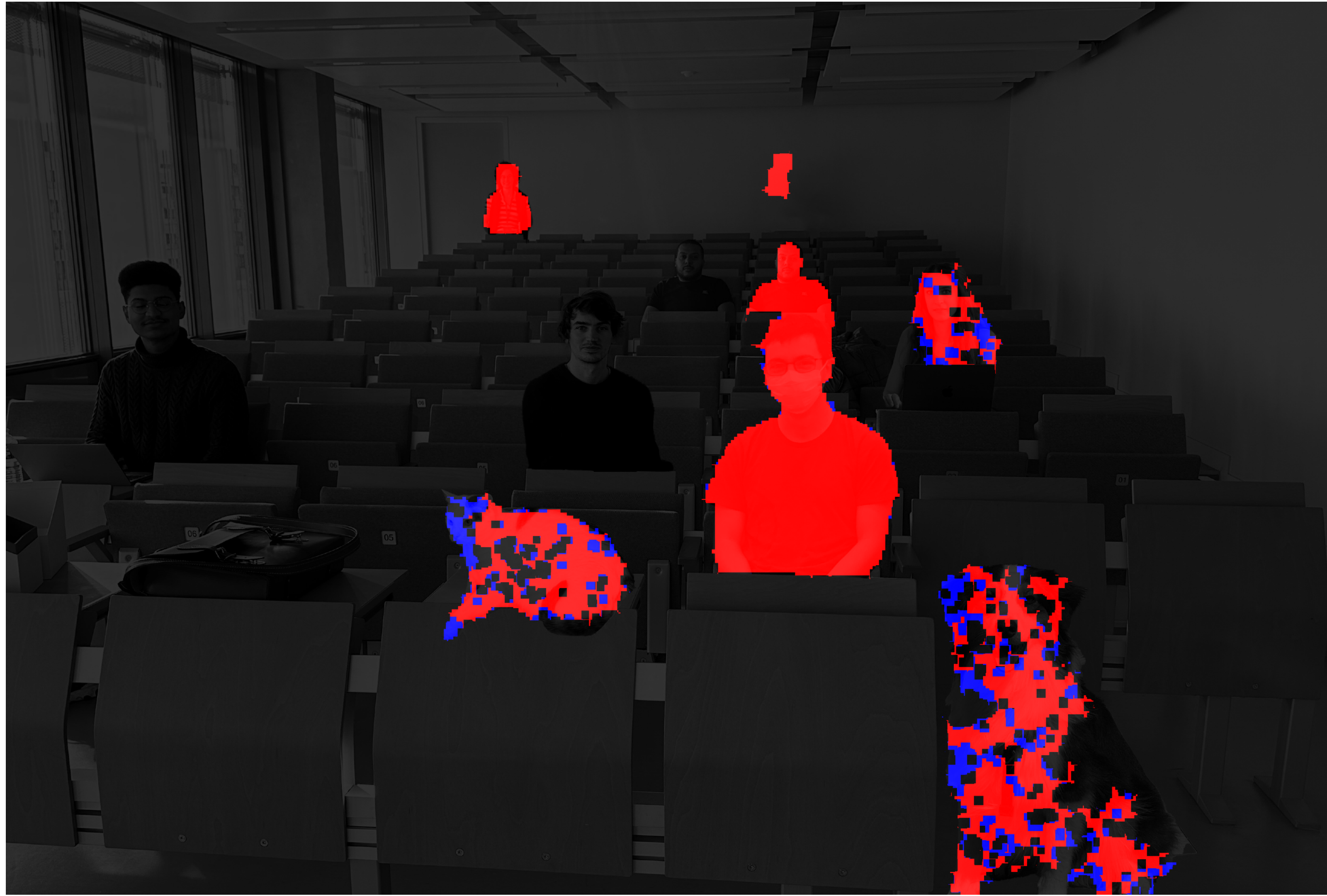
Forged image



Vote map



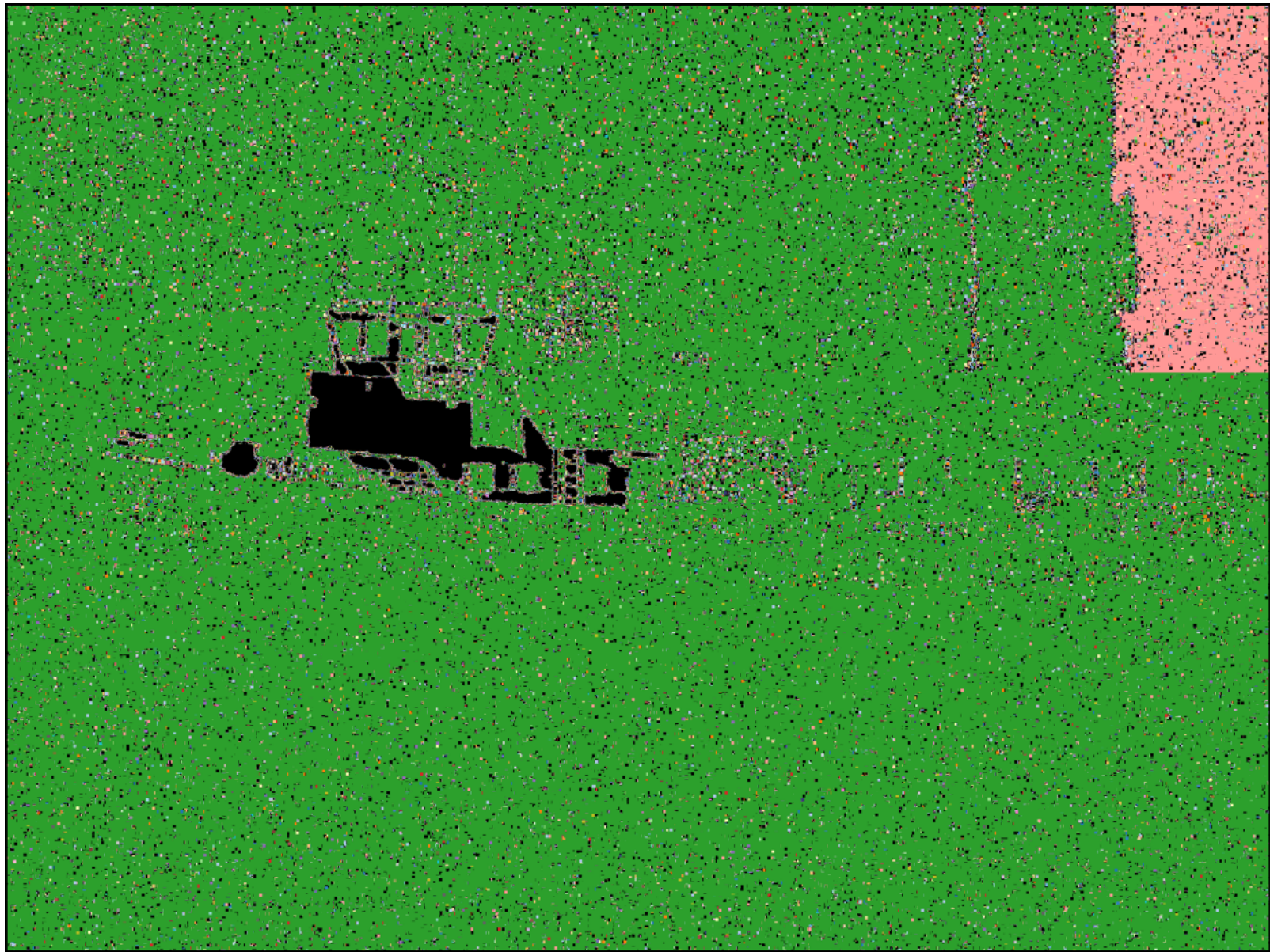
Forgery detection



Limitations: 1/64



Forged image from FAU dataset



Vote map



Detection result

Limitations: uncompressed images



Uncompressed forged image



Mask

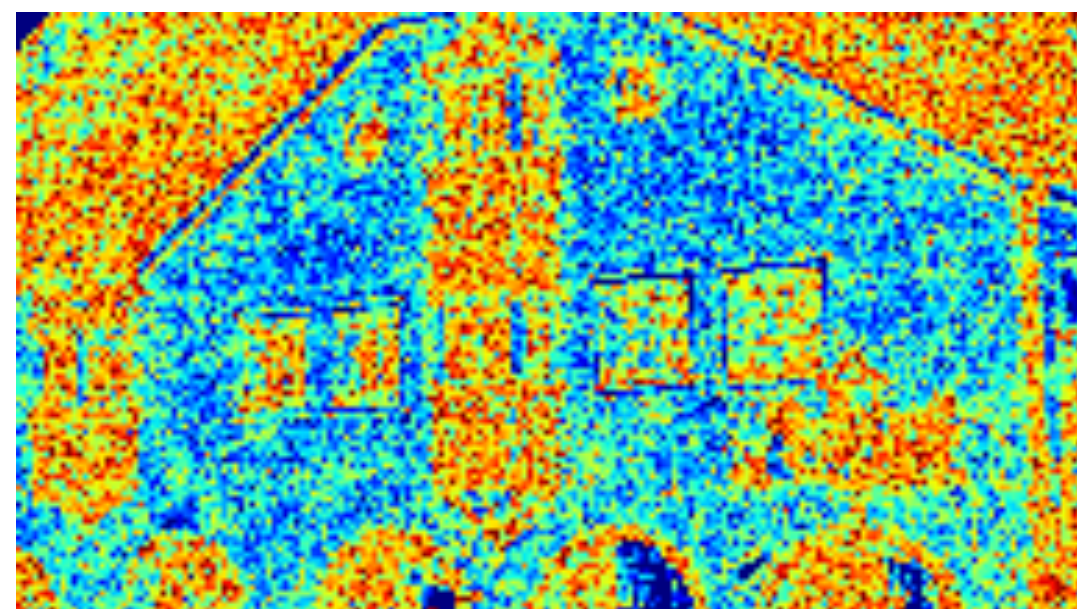
Limitations: uncompressed images



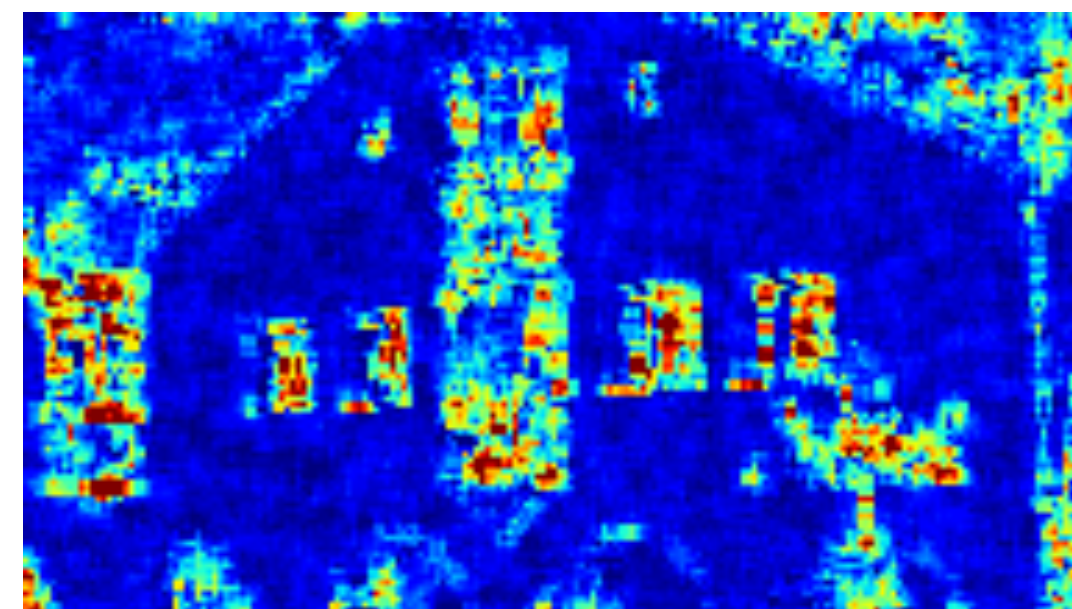
Uncompressed forged image



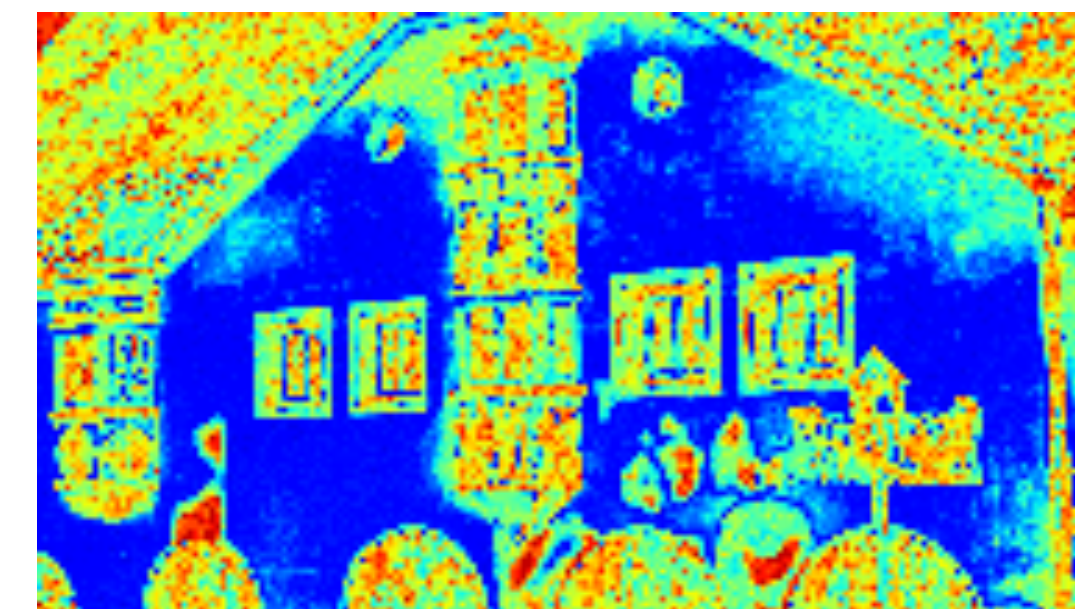
Vote map



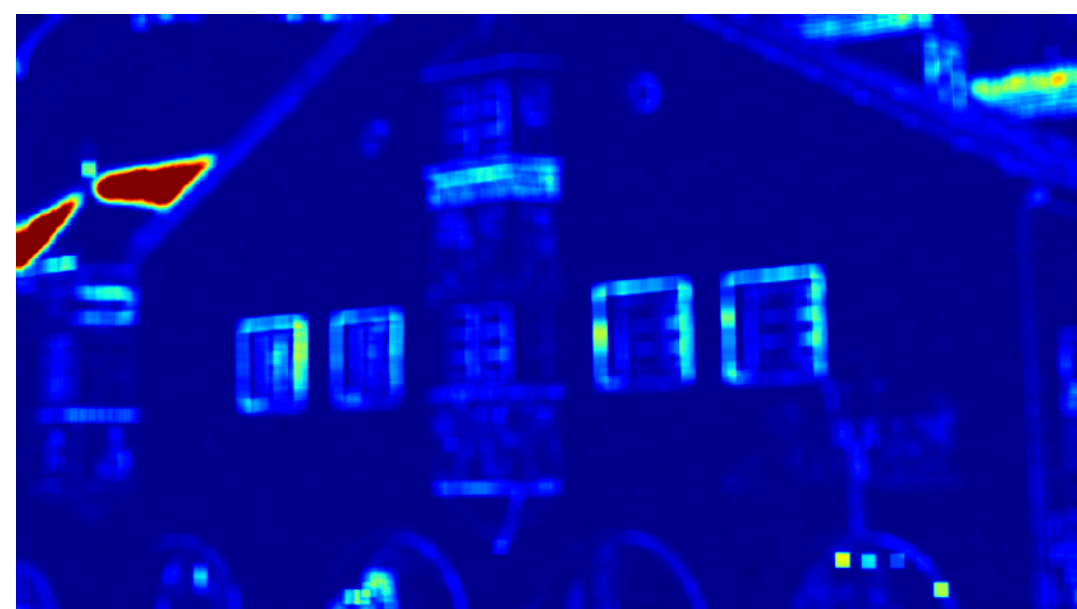
DCT



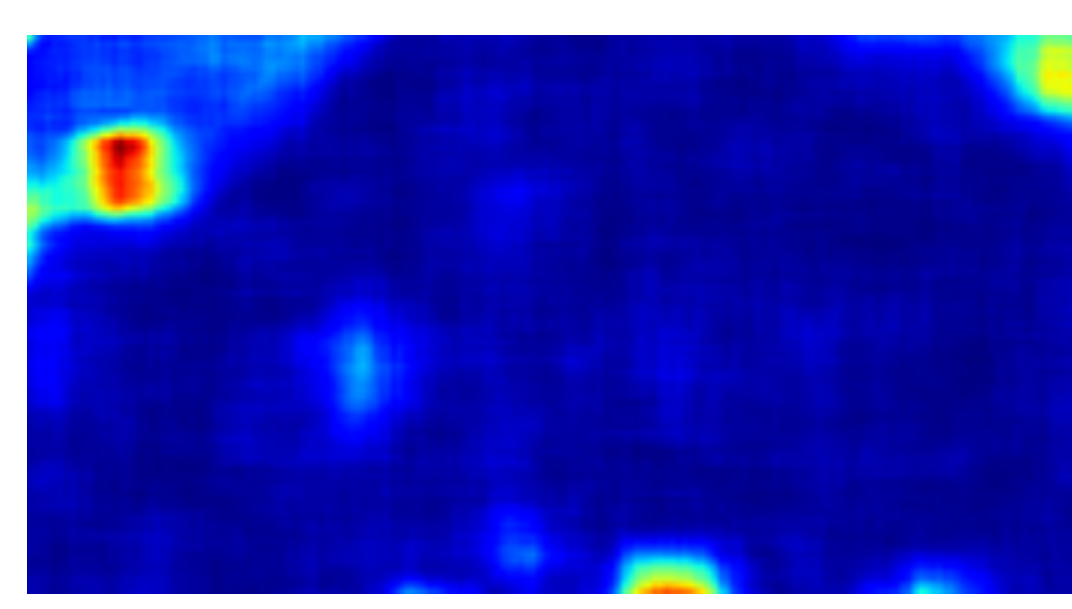
BLK



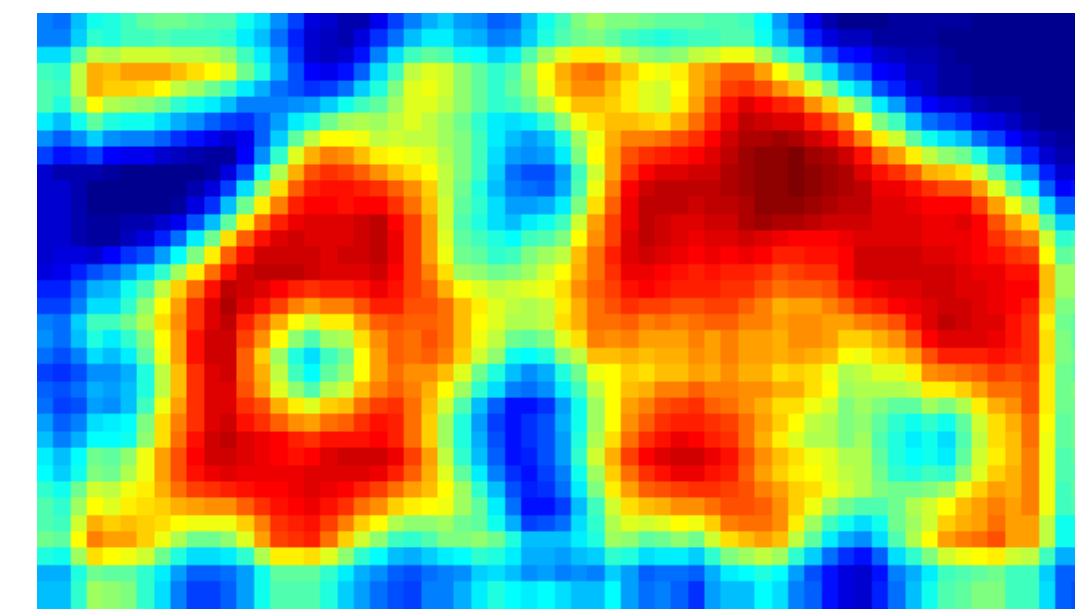
DQ



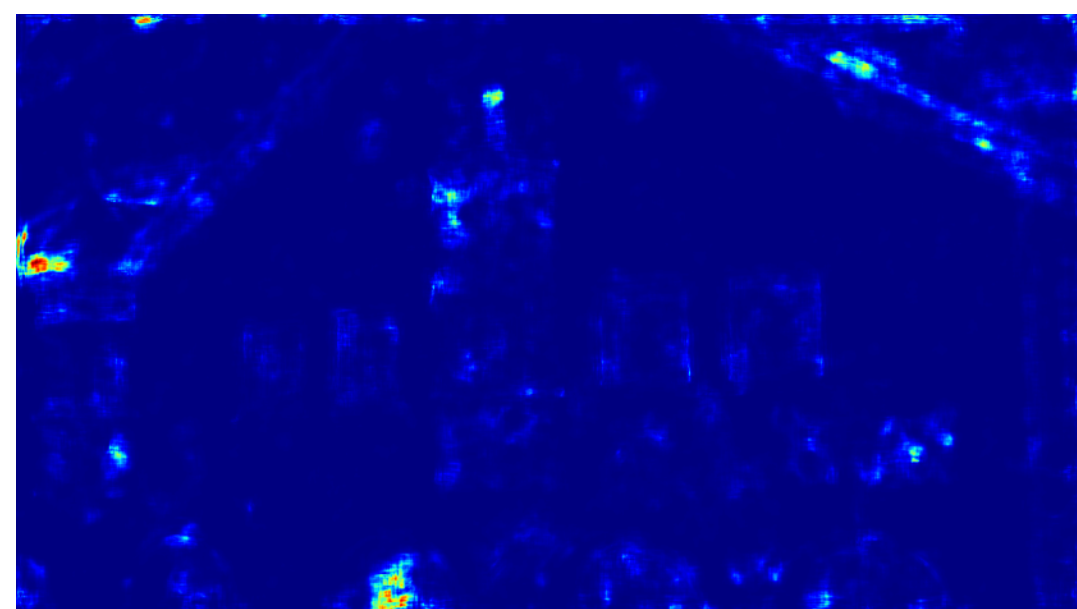
Ghost



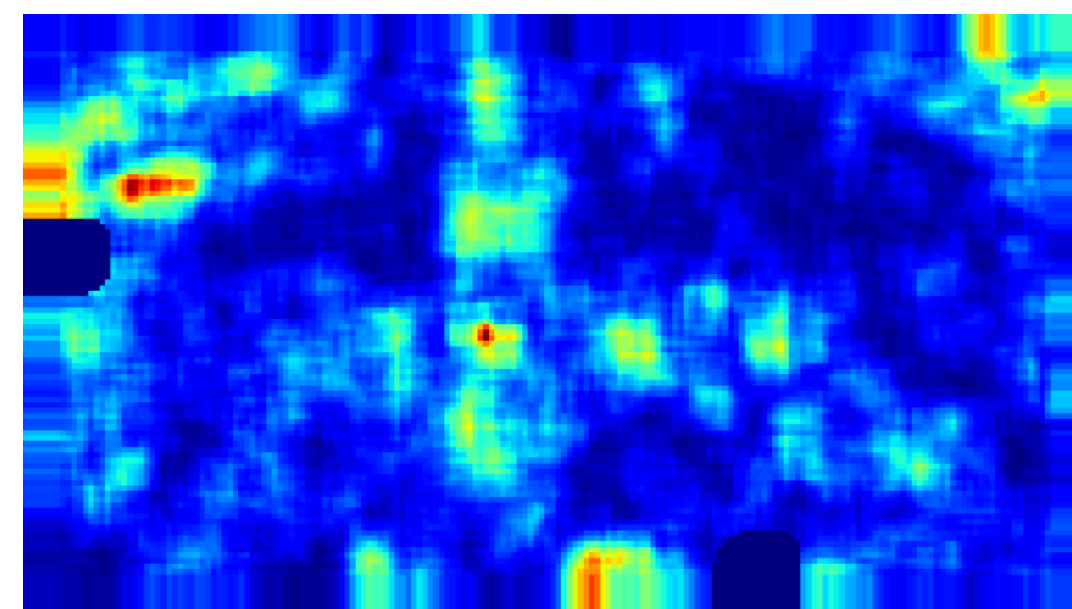
Splicebuster



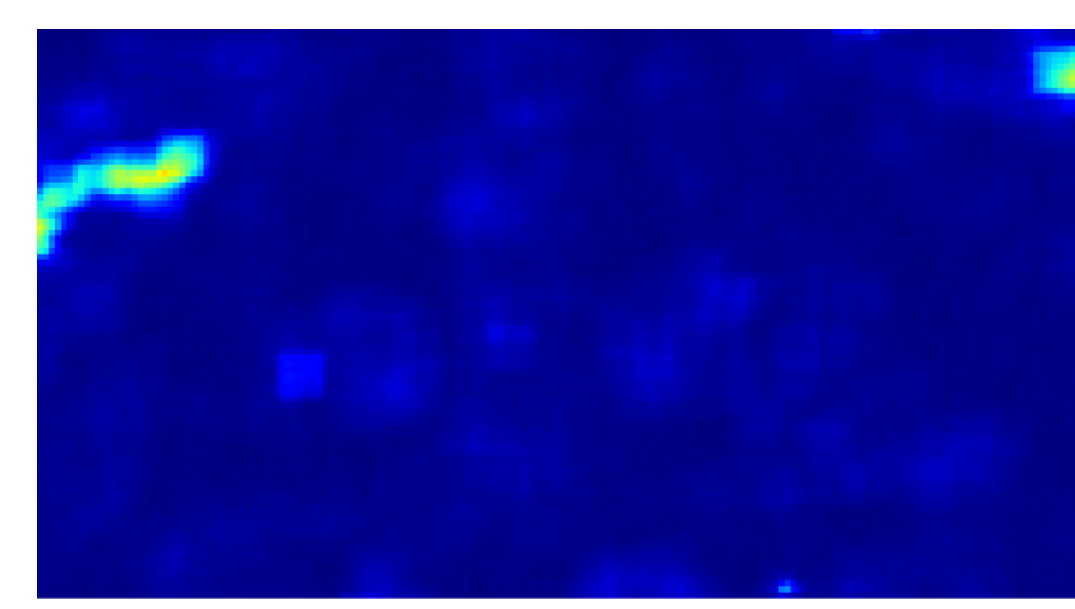
CAGI



ManTraNet



Noiseprint



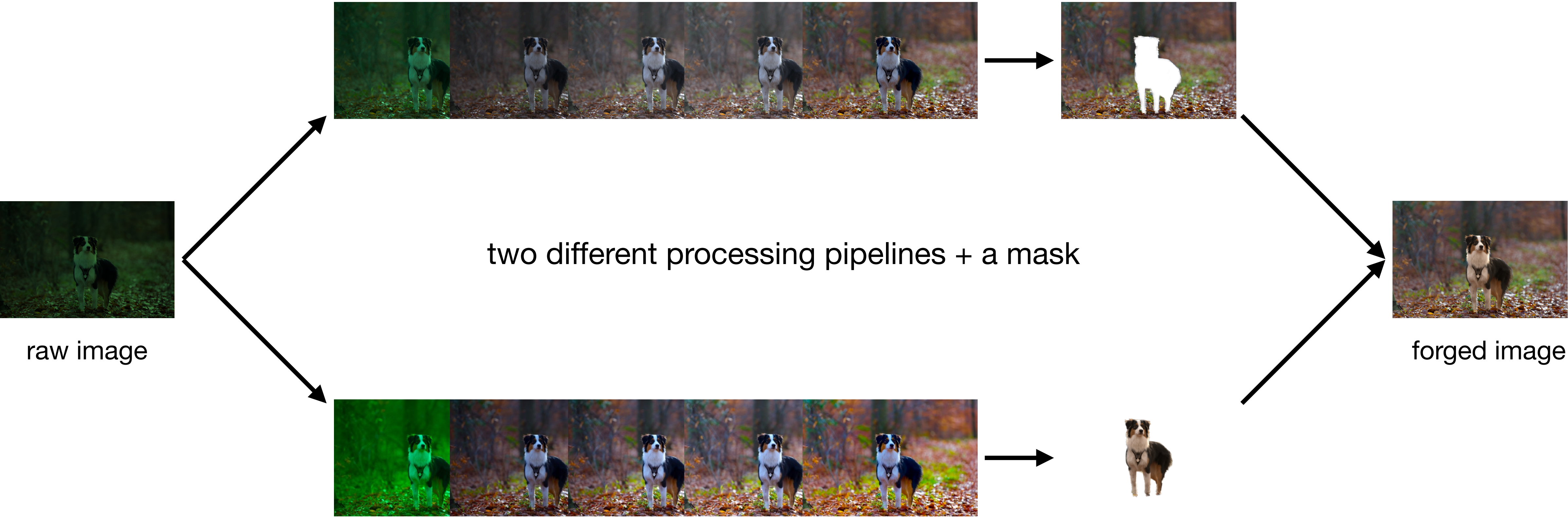
Comprint

NO JPEG TRACES
DETECTED

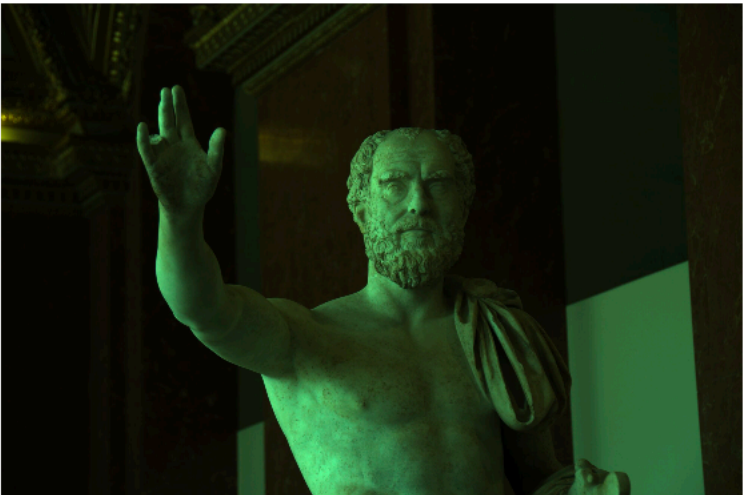
zero

How to know what methods aim at detecting?

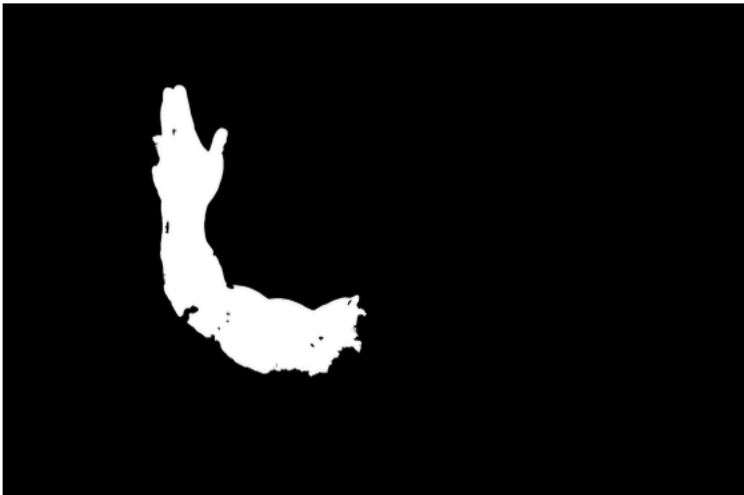
Trace database: A new methodology to evaluate, understand and improve forensic tools



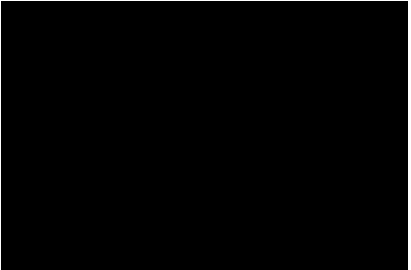
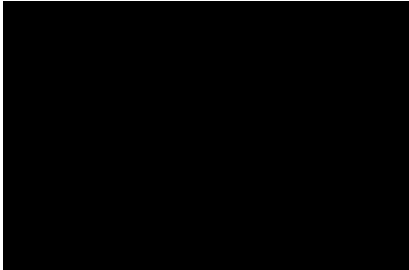
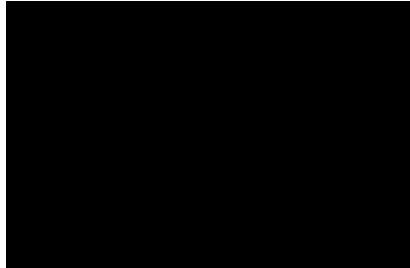
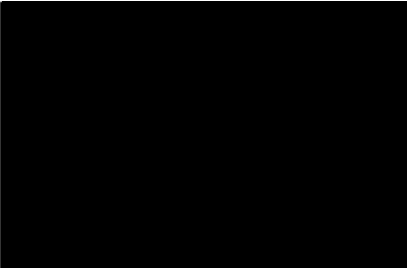
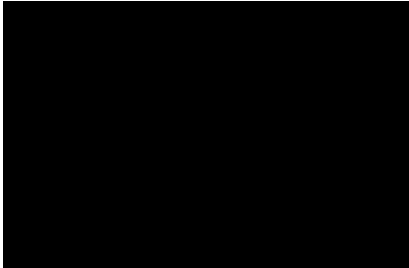
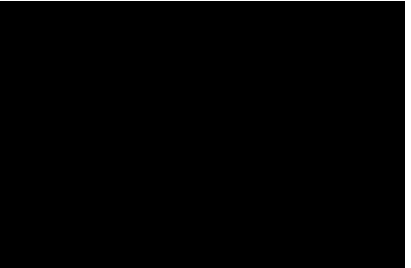
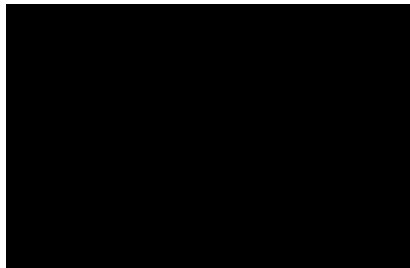
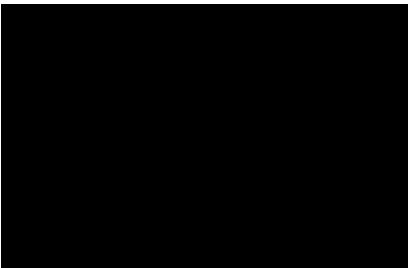
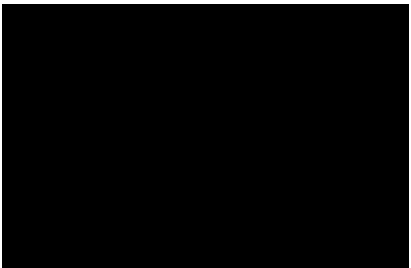
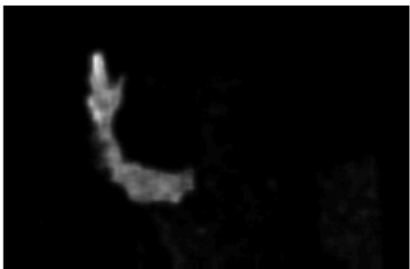
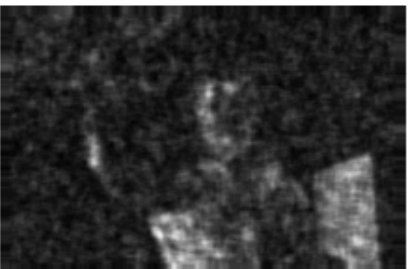
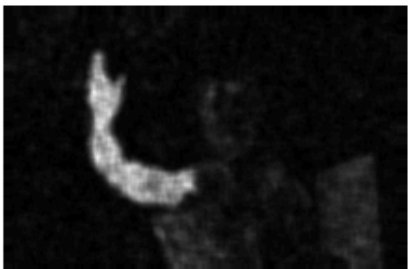
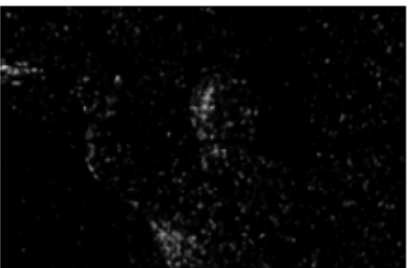
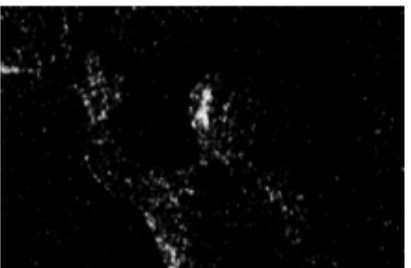
Complementarity of the methods



raw image



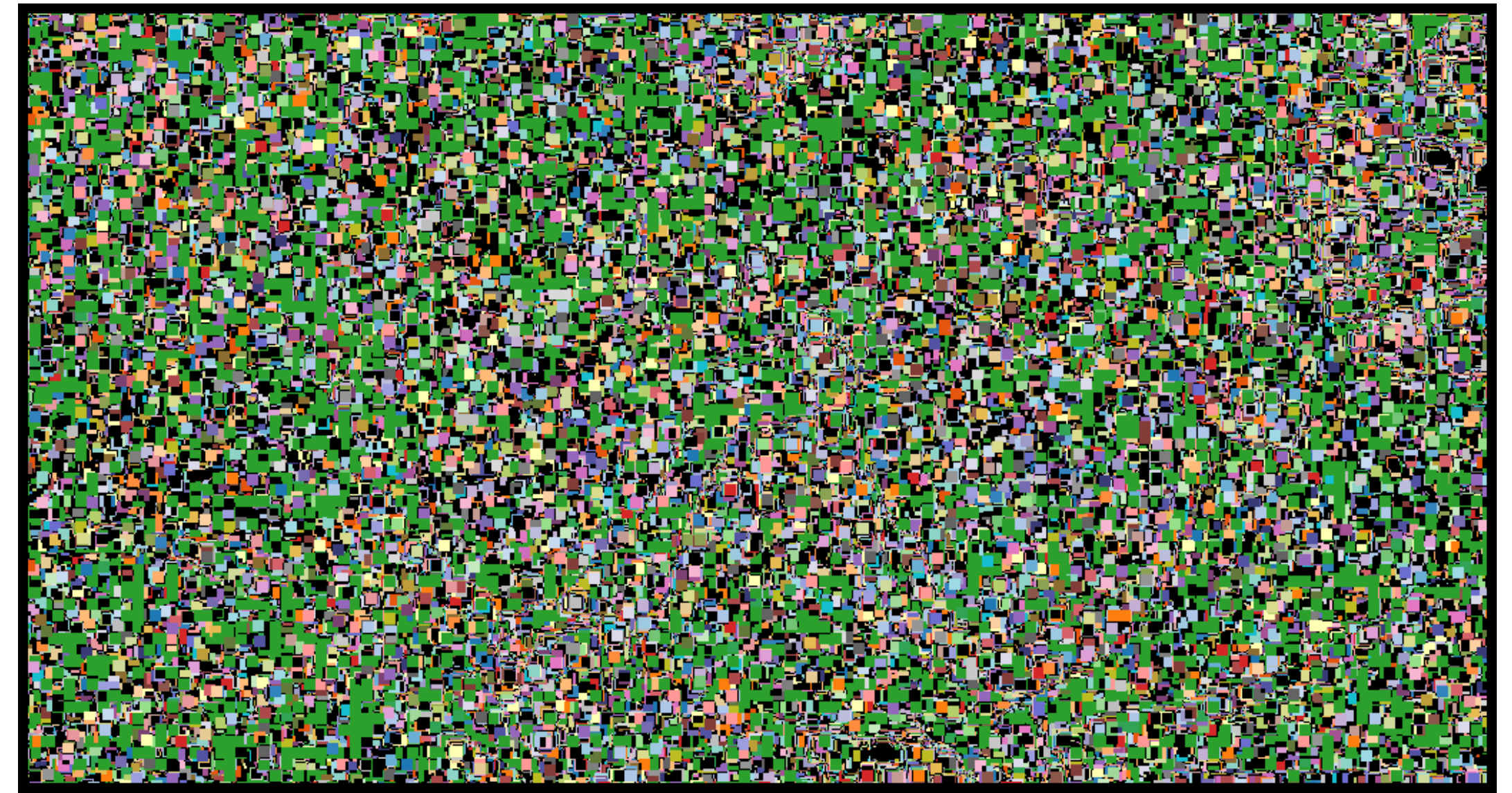
mask

	Noise level	CFA grid	CFA algorithm	JPEG grid	JPEG quality	Hybrid
Splicebuster						
Bammey						
ZERO						
Noiseprint						
ManTraNet						
Self-Consistency						

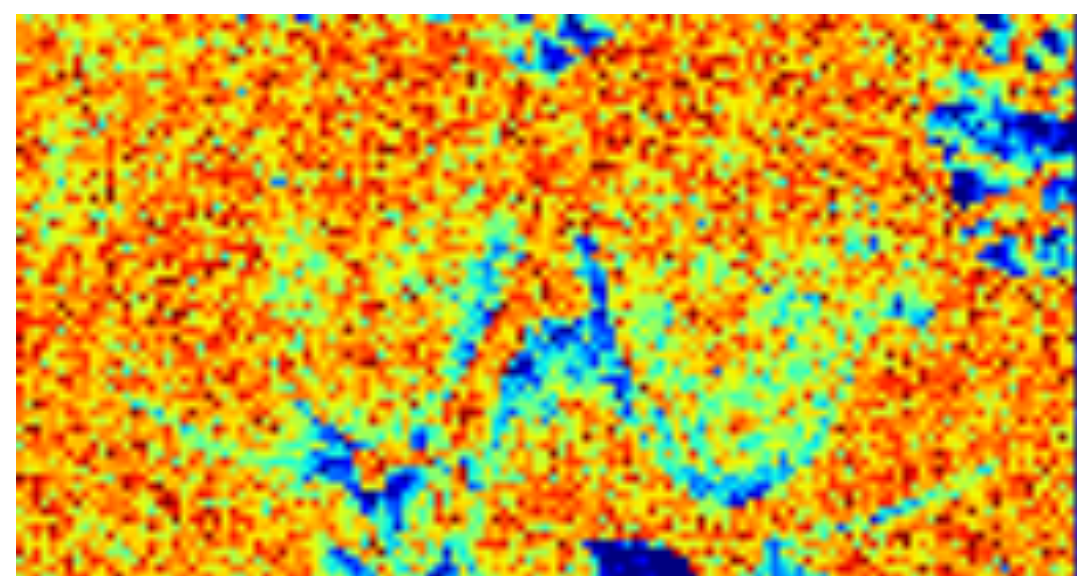
Complementarity of the methods



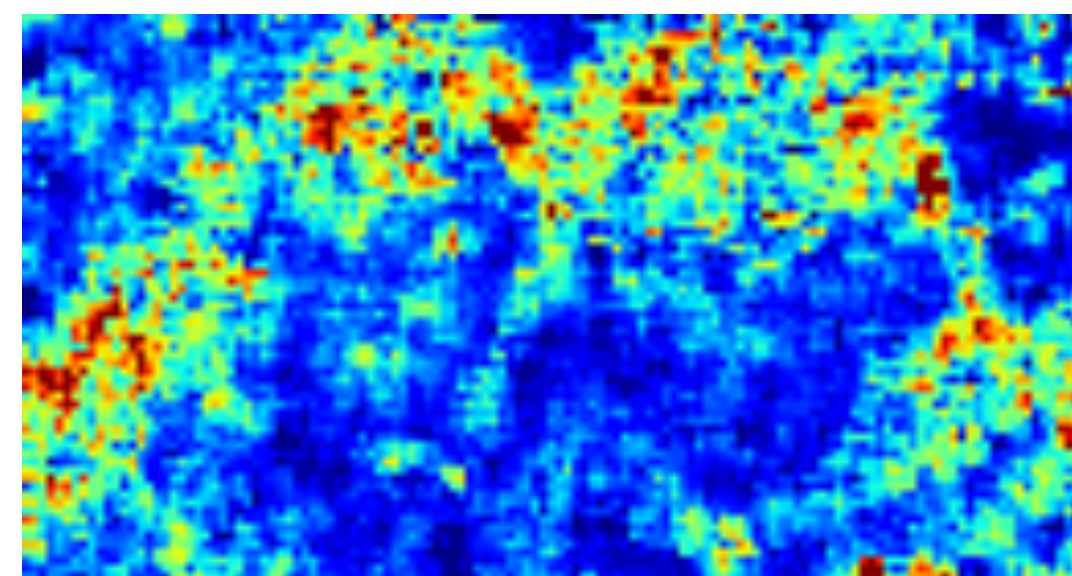
Forged image from @GuillaumeTC



Vote map



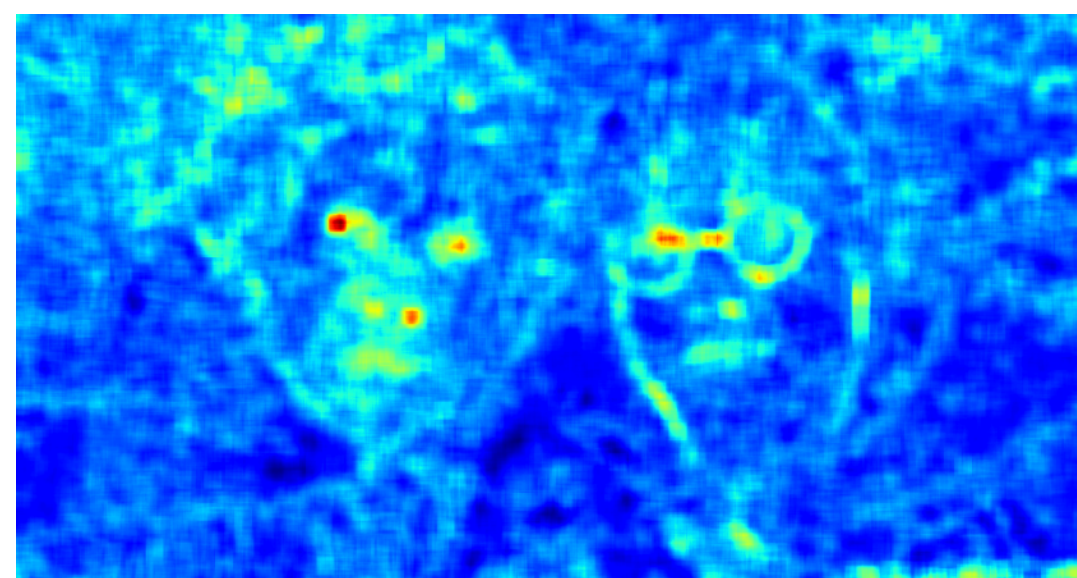
DCT



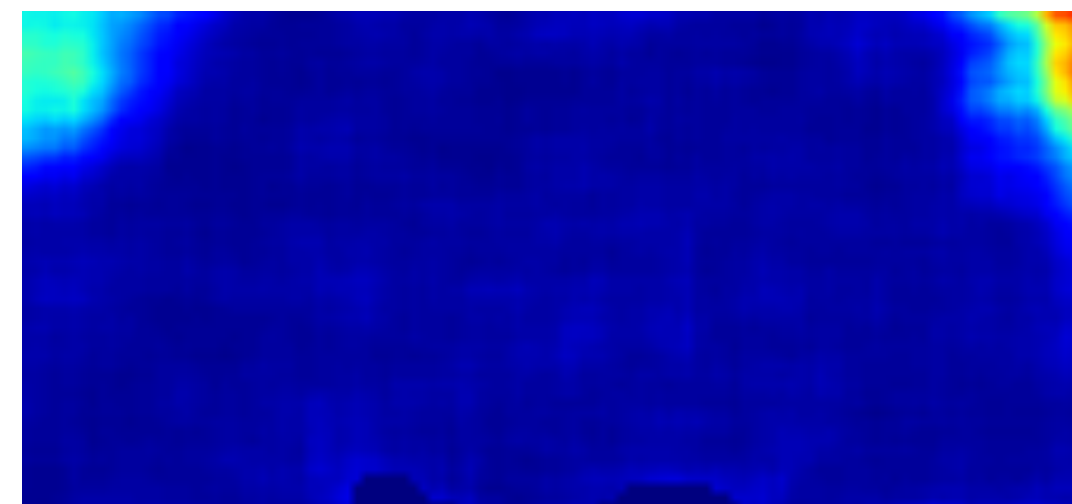
BLK



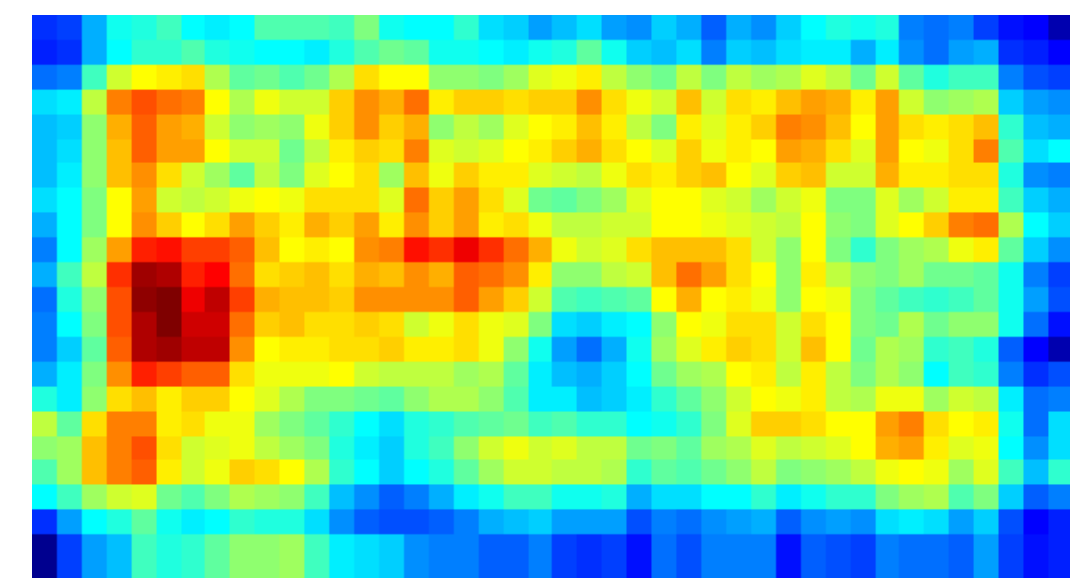
DQ



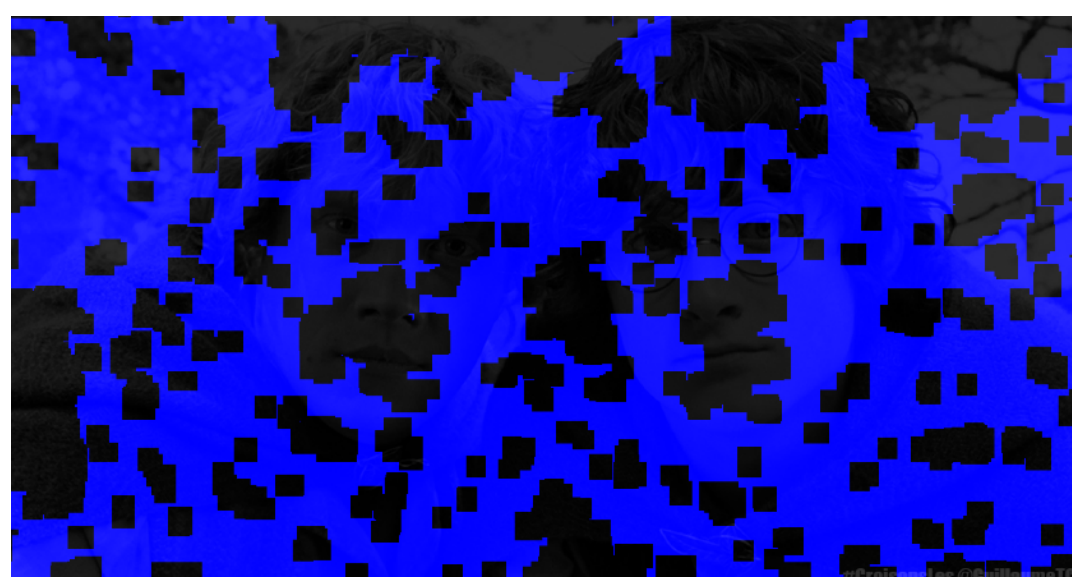
Ghost



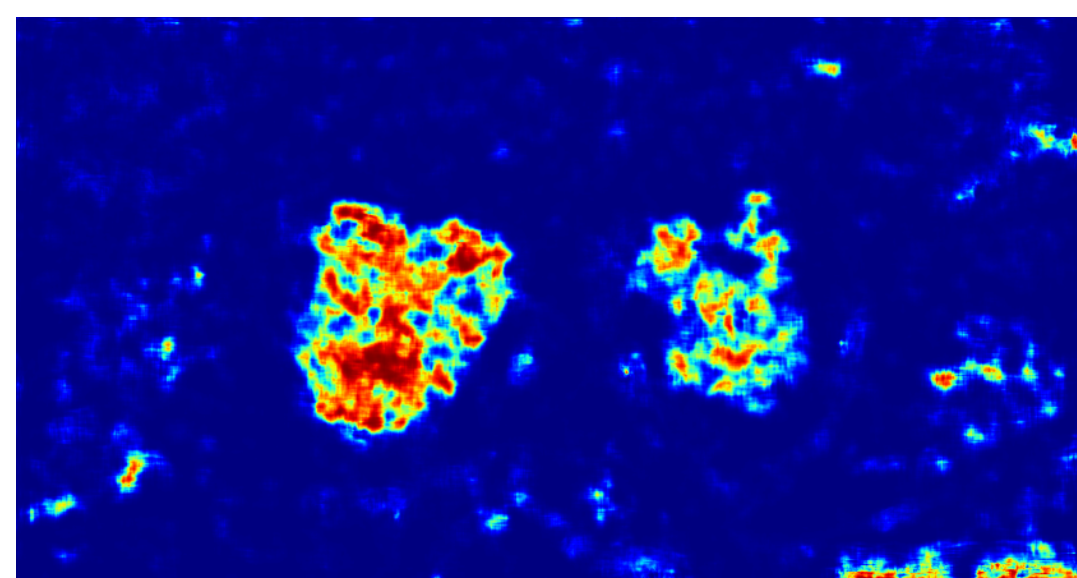
Splicebuster



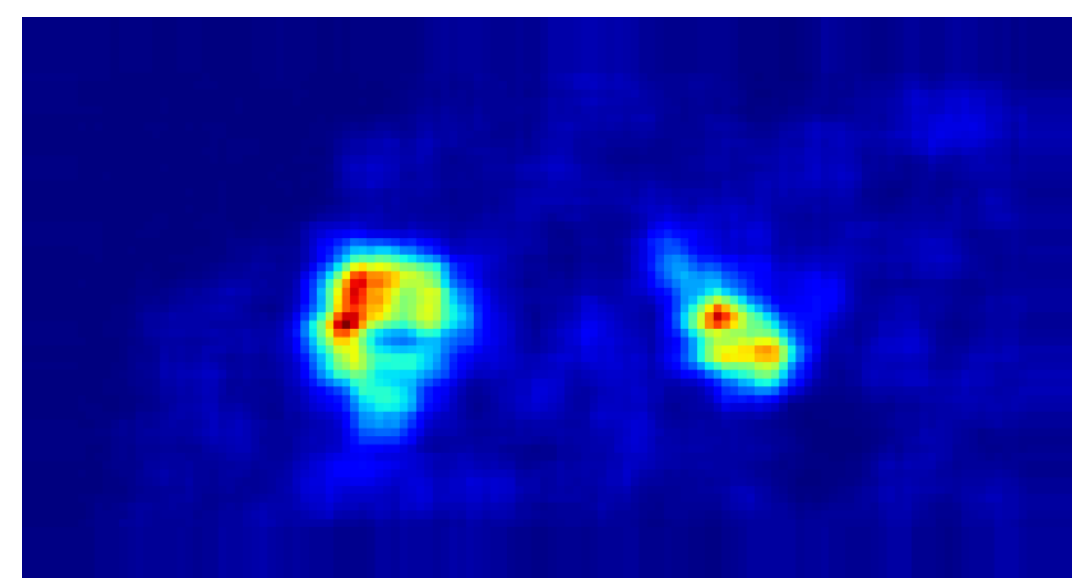
CAGI



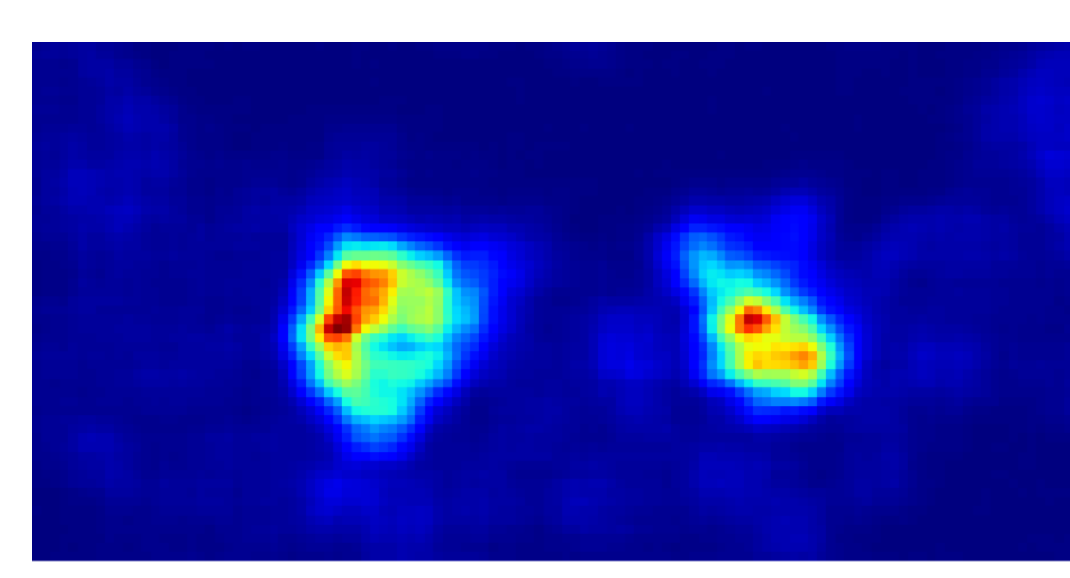
zero



ManTraNet



Noiseprint



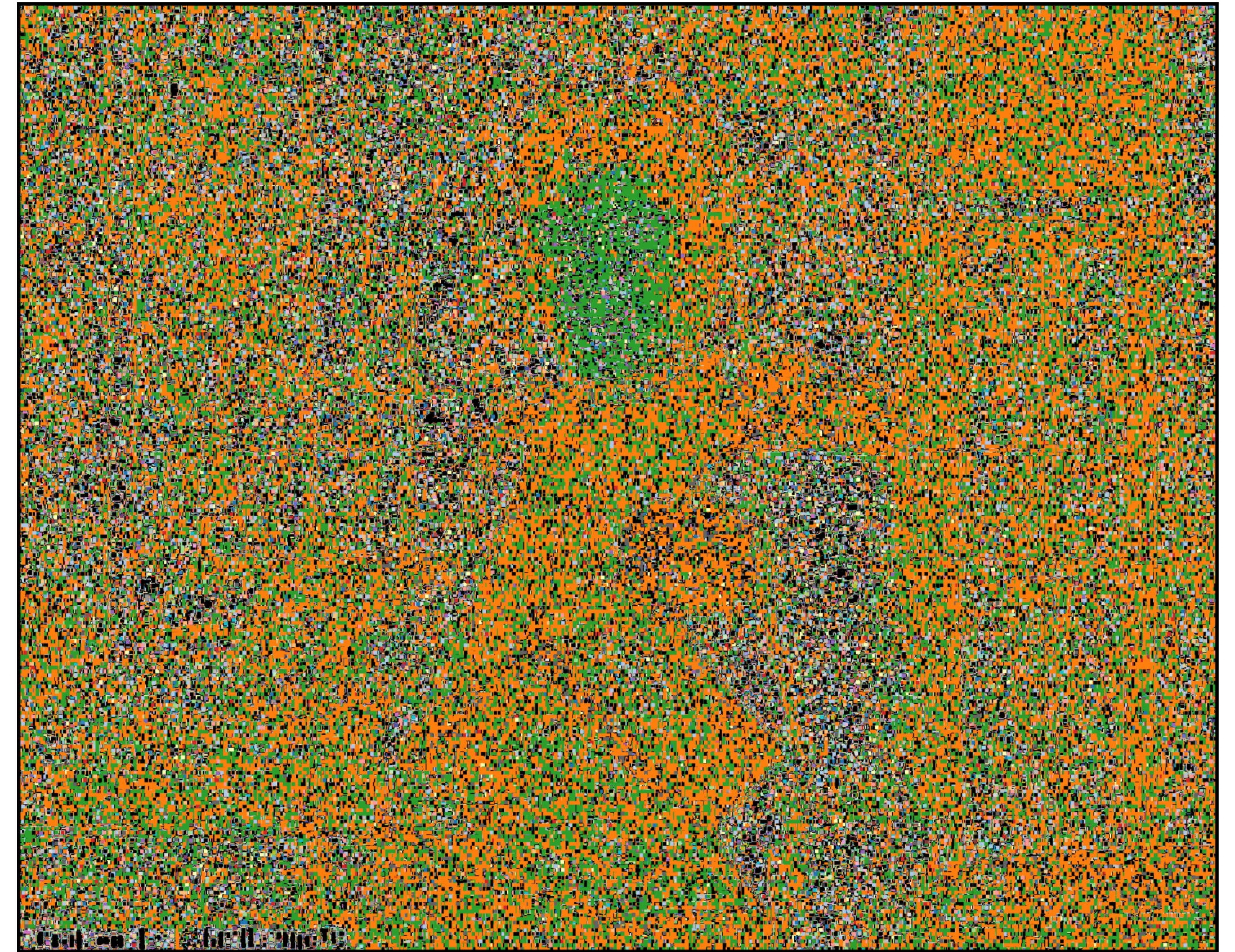
Comprint

Complementarity of the methods



#CroisonsLes @GuillaumeTC

Forged image from @GuillaumeTC



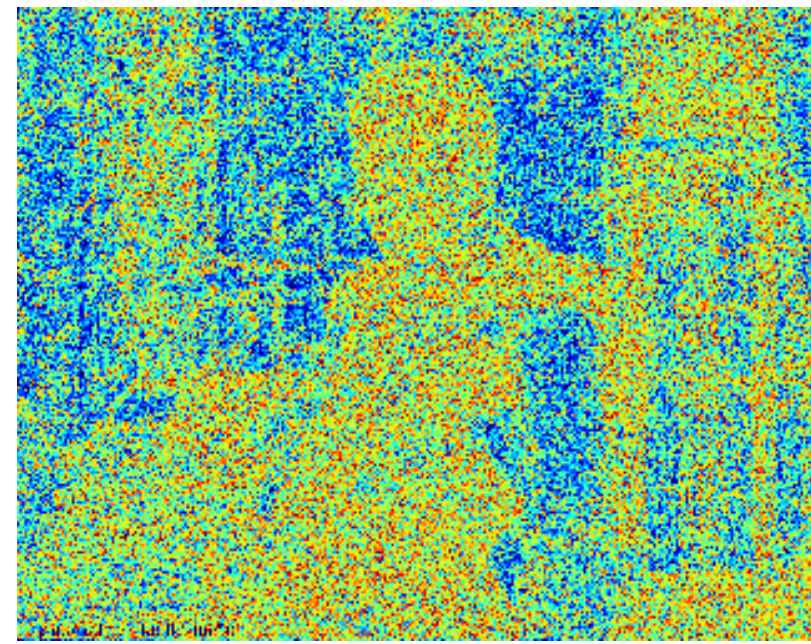
#CroisonsLes @GuillaumeTC

Vote map

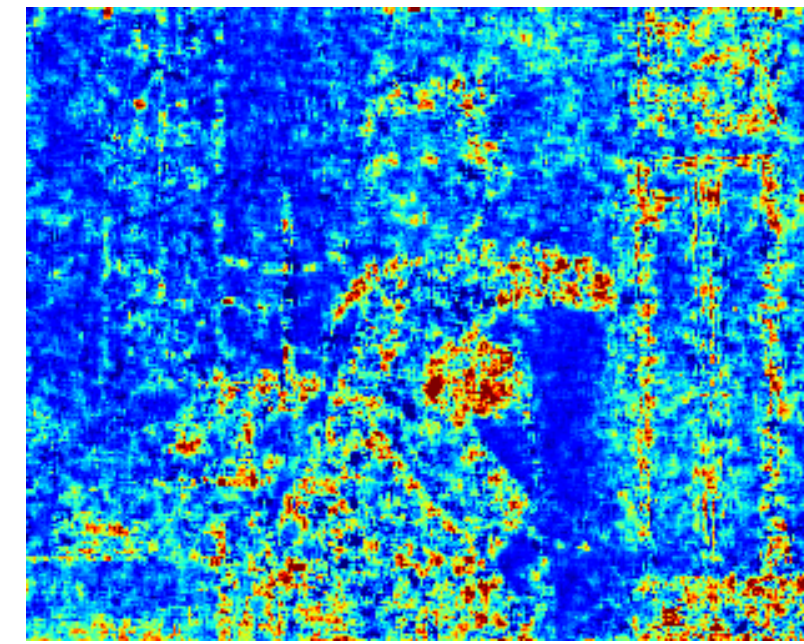


Main grid (2,0)
 Global grid (0,0)
 -> JPEG + crop + JPEG

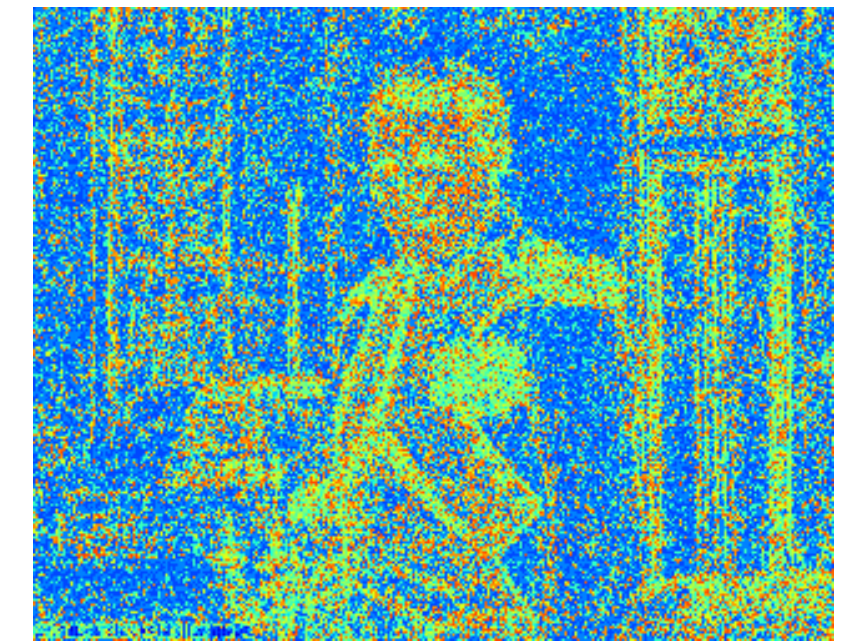
zero



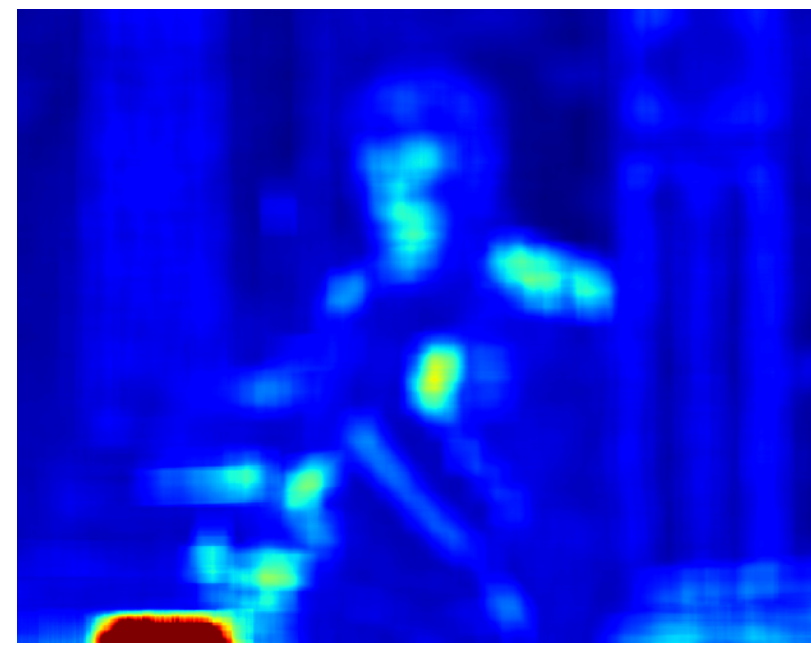
DCT



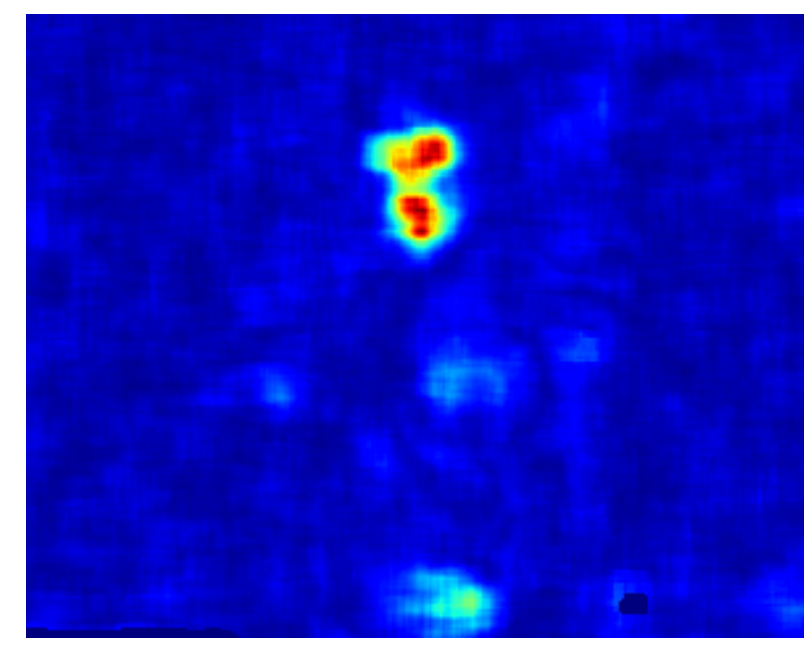
BLK



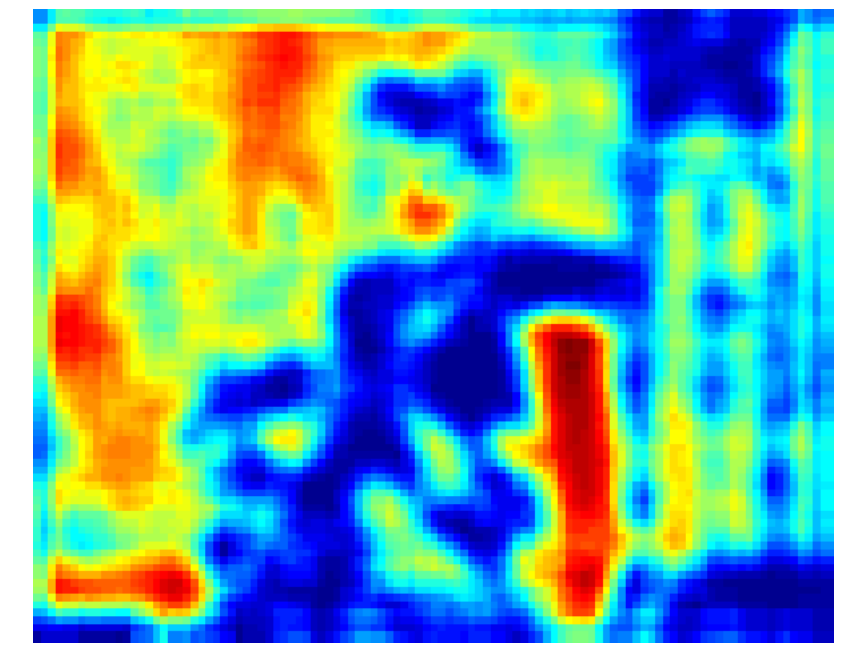
DQ



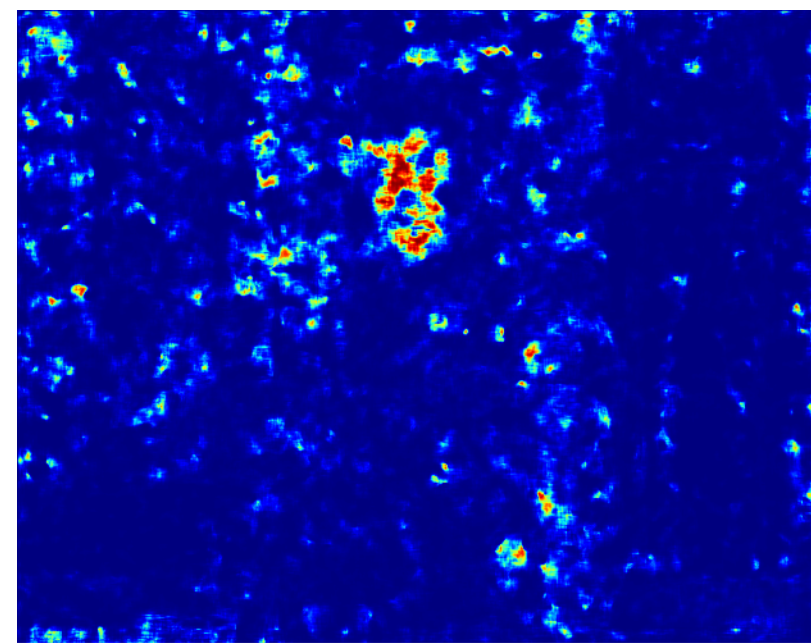
Ghost



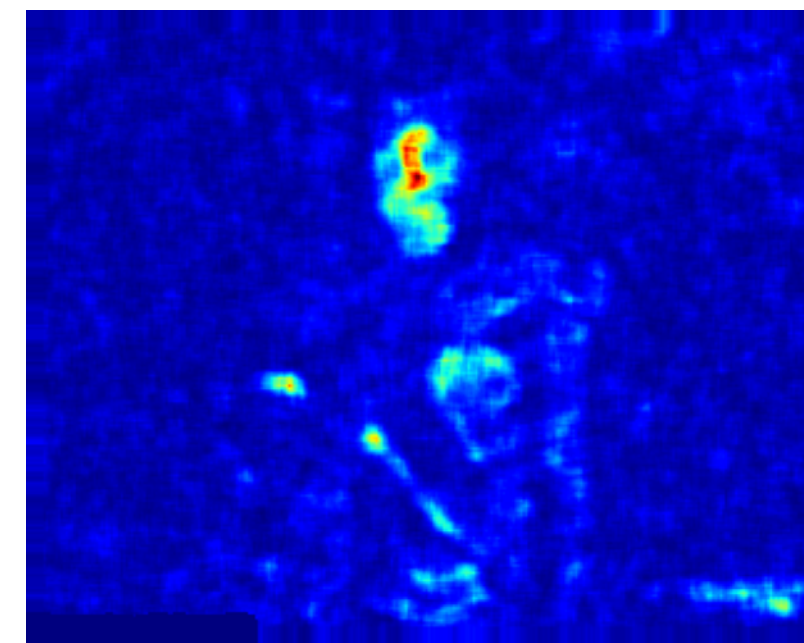
Splicebuster



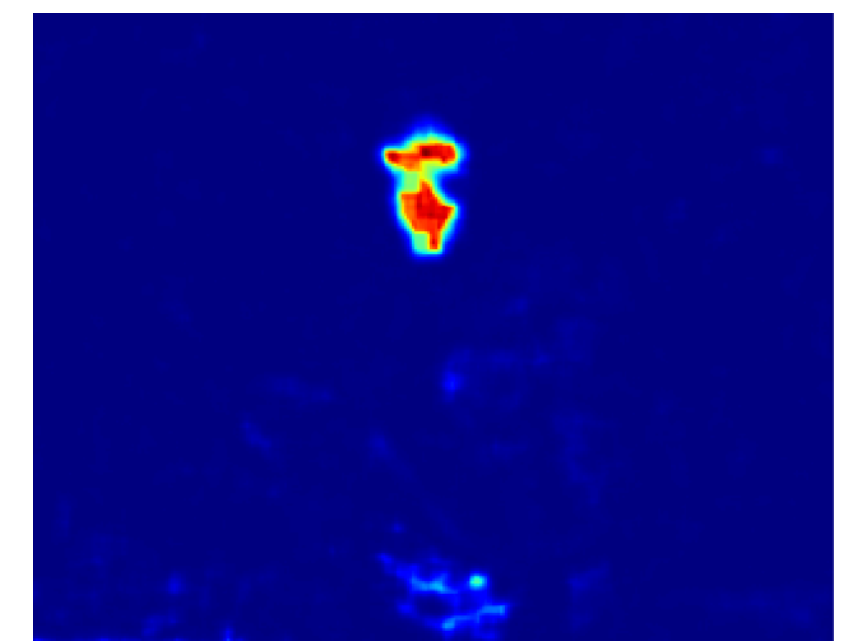
CAGI



ManTraNet



Noiseprint



Comprint

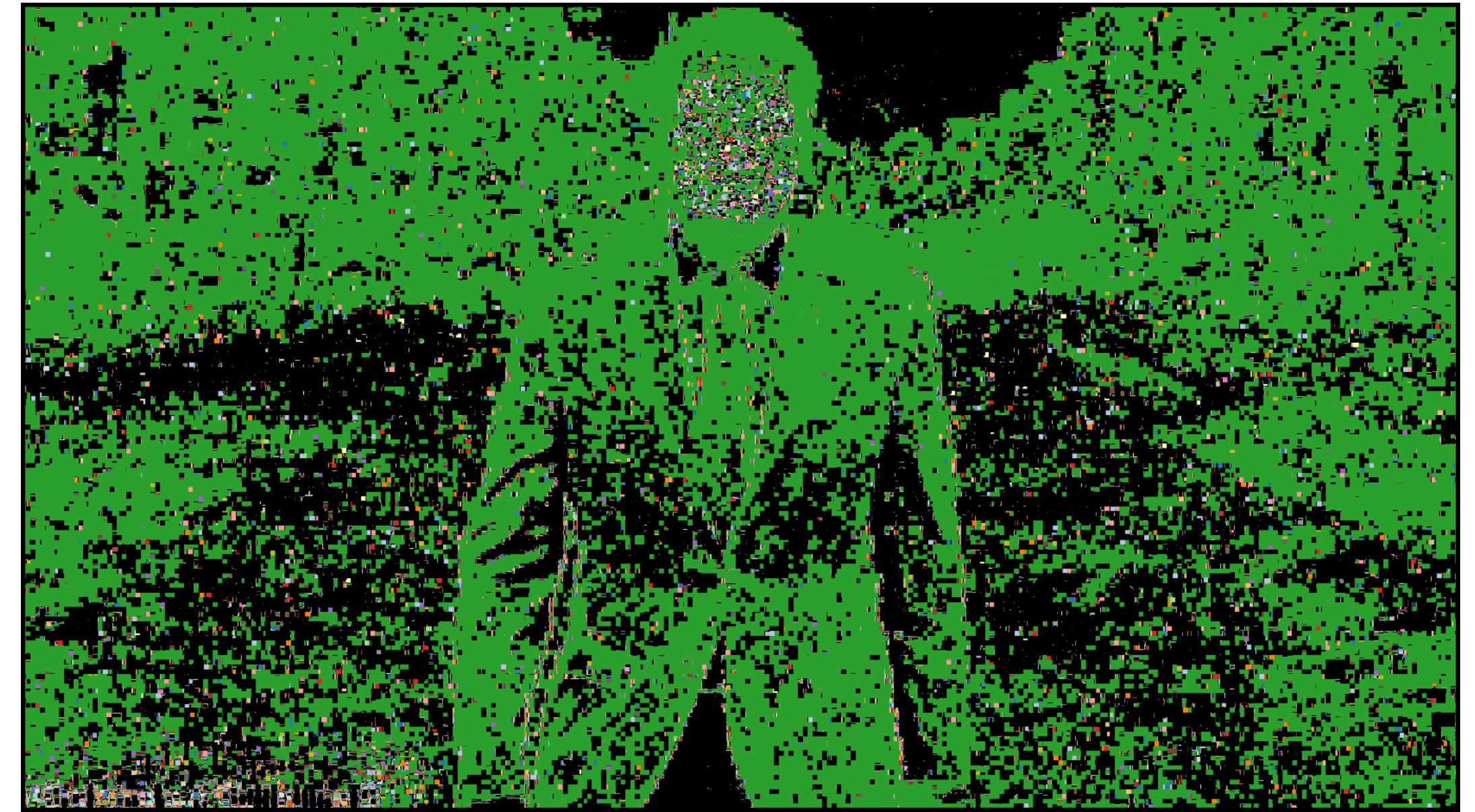
Complementarity of the methods



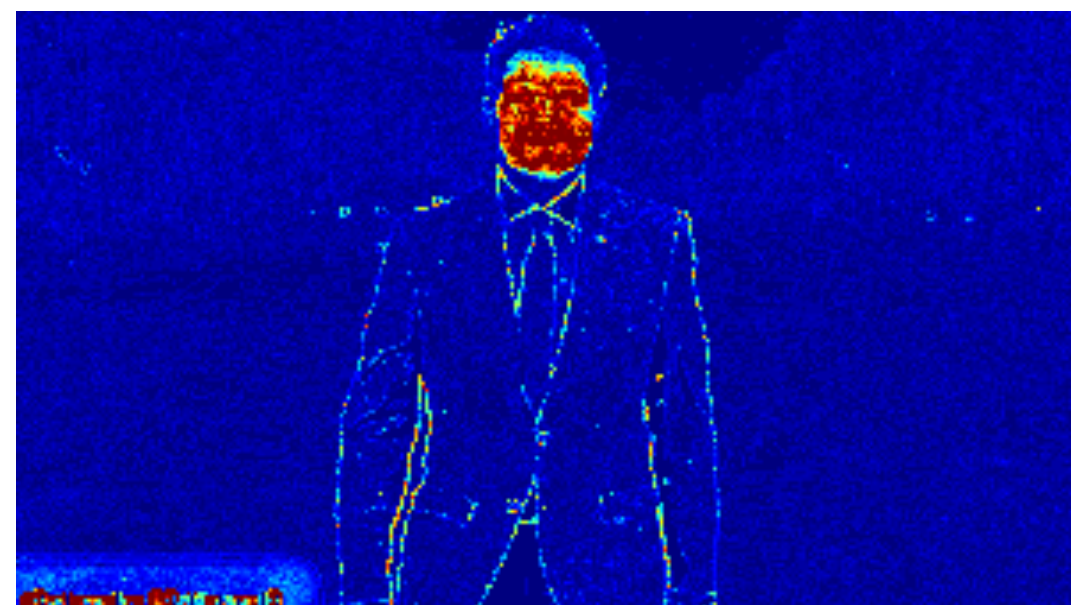
Complementarity of the methods



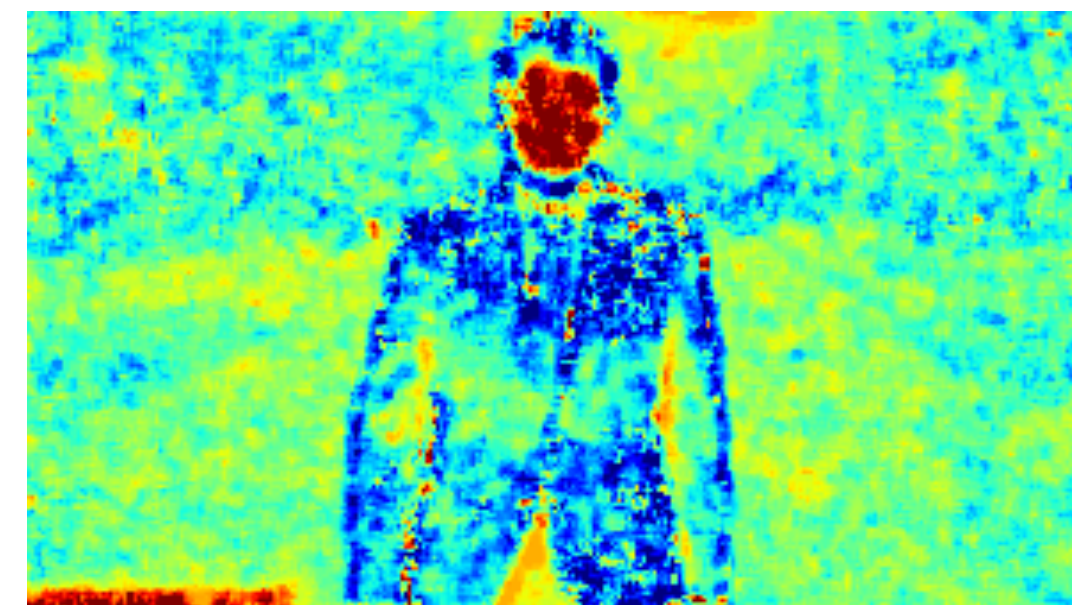
Forged image from @GuillaumeTC



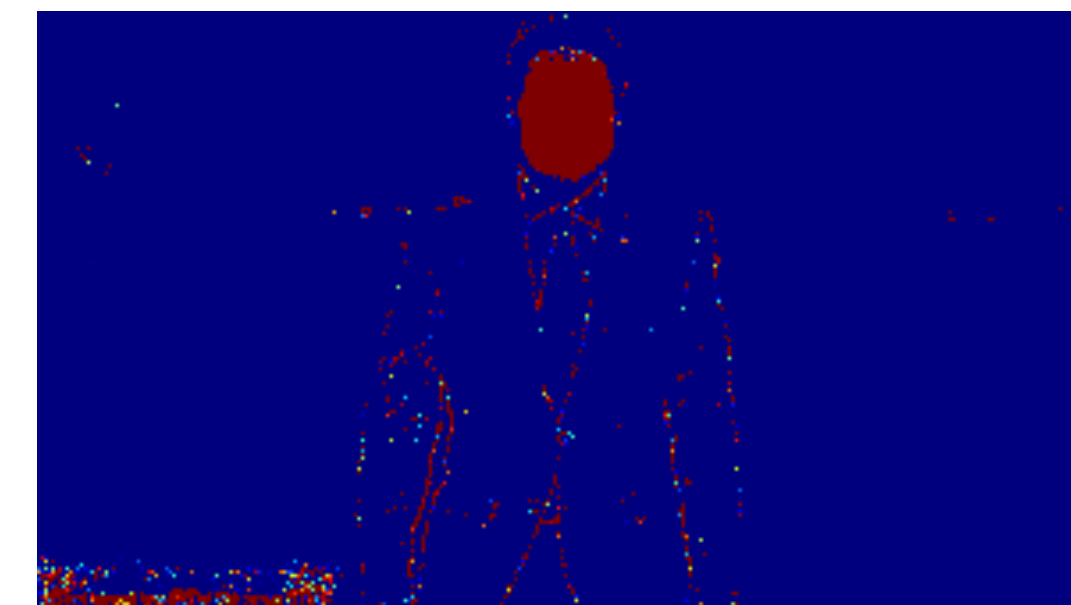
Vote map



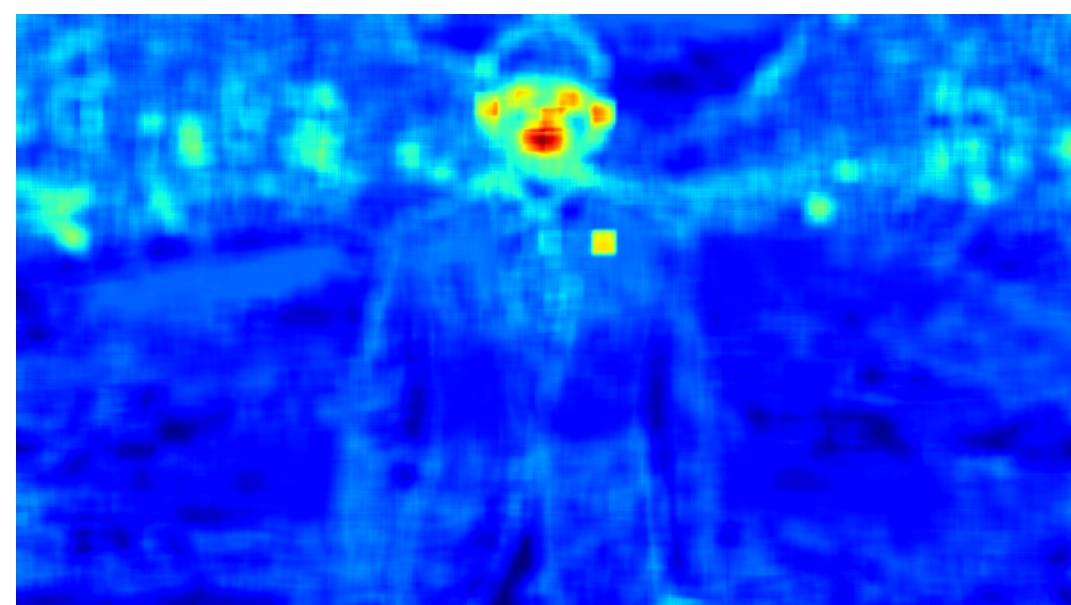
DCT



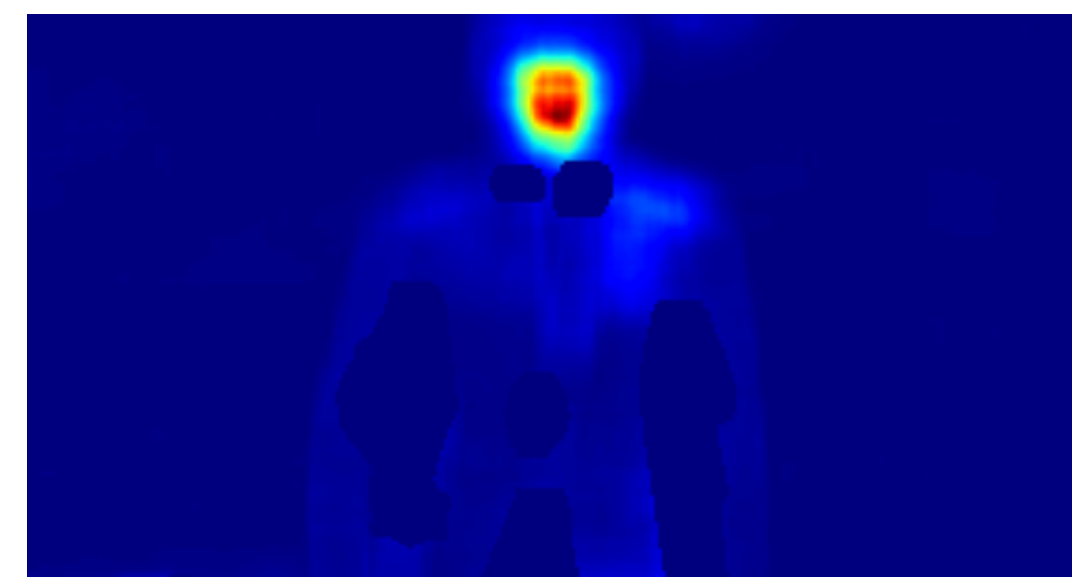
BLK



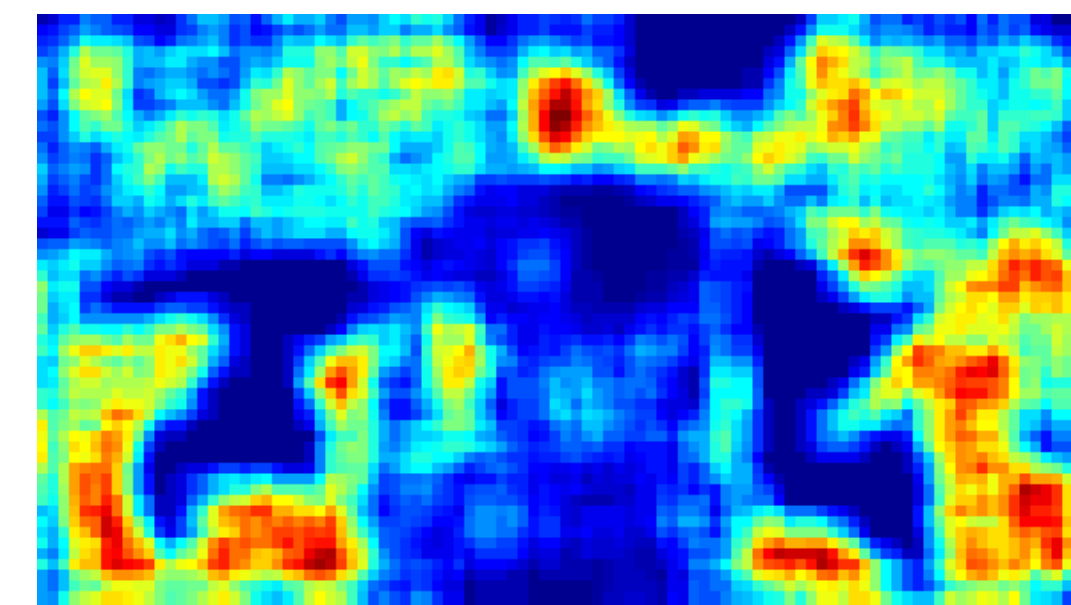
DQ



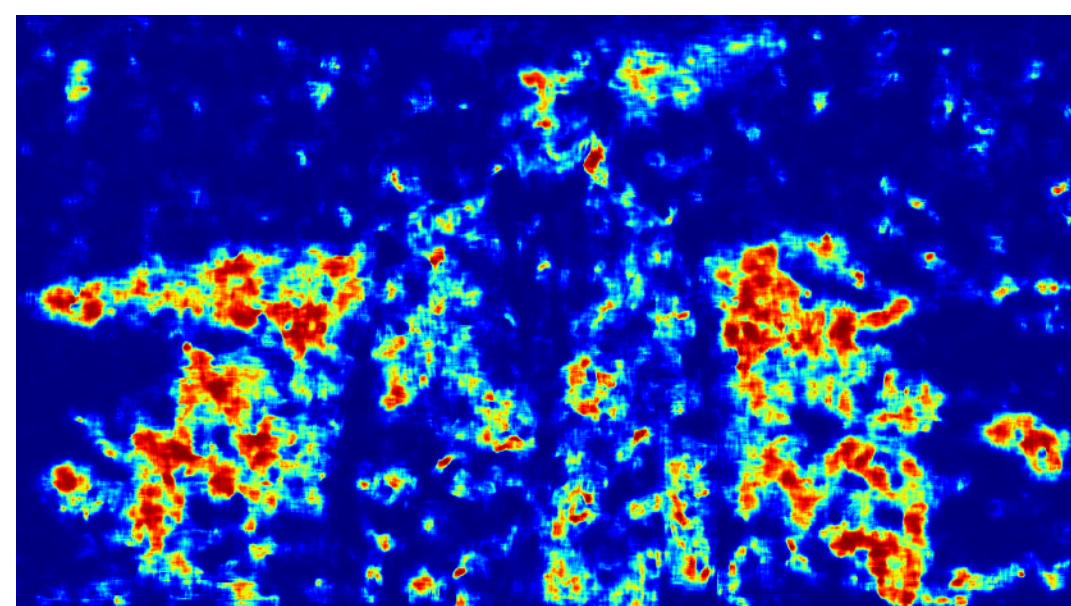
Ghost



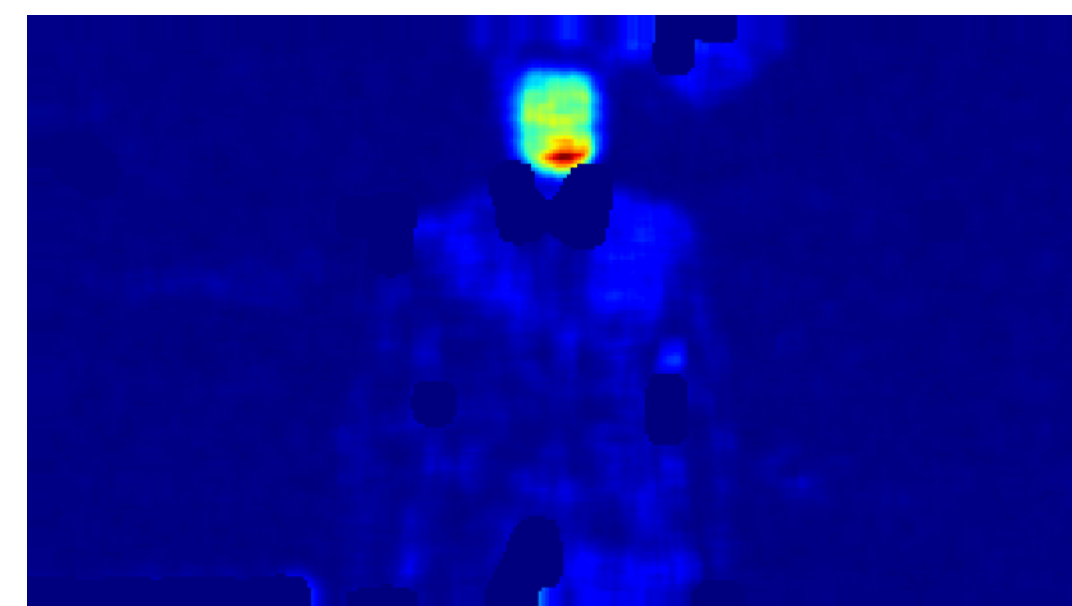
Splicebuster



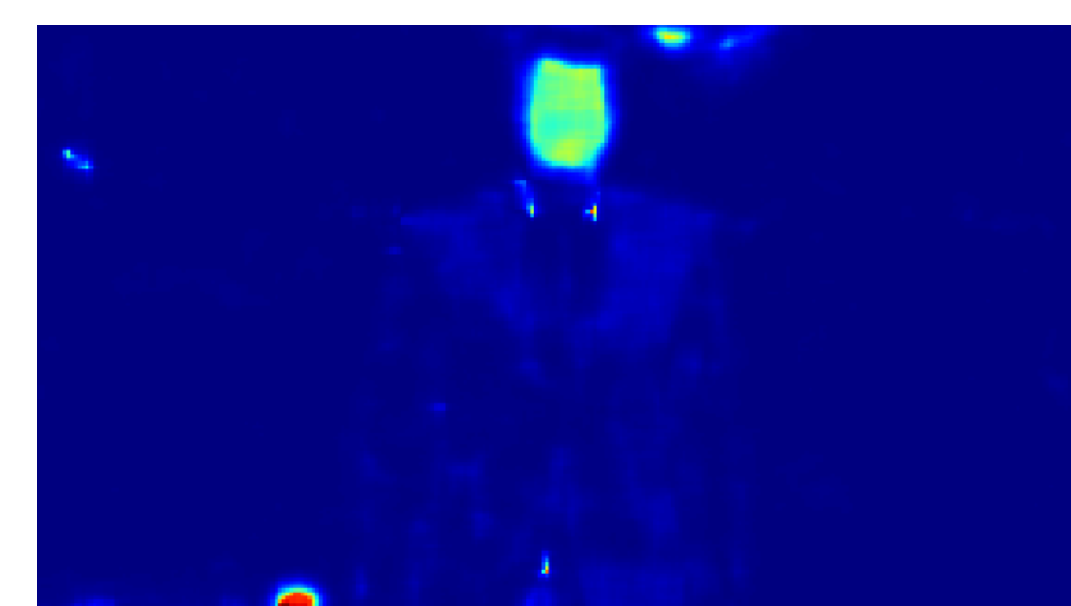
CAGI



ManTraNet



Noiseprint



Comprint

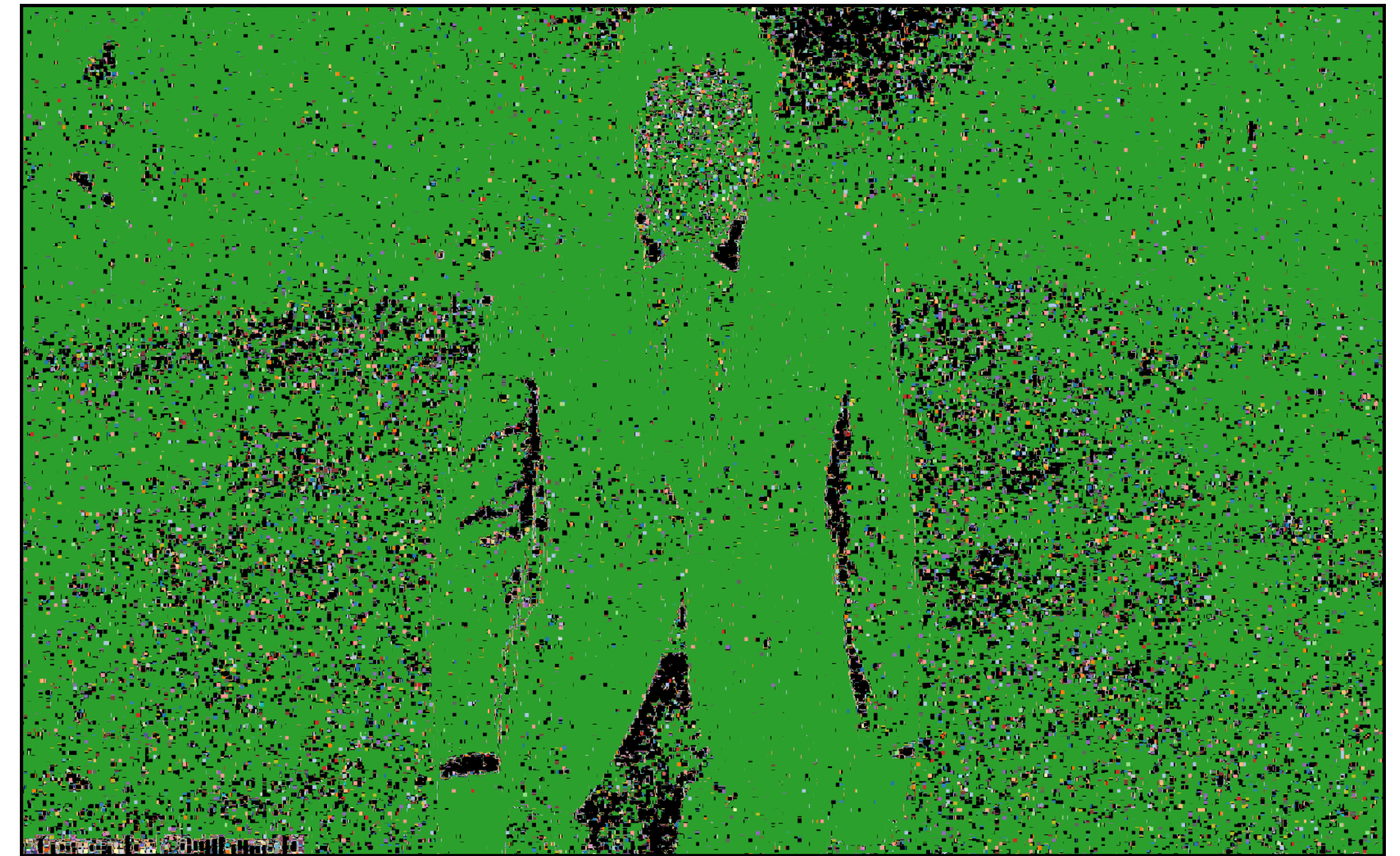
Main grid (0,0)
JPEG image

zero

Complementarity of the methods



Forged image from @GuillaumeTC



Vote map

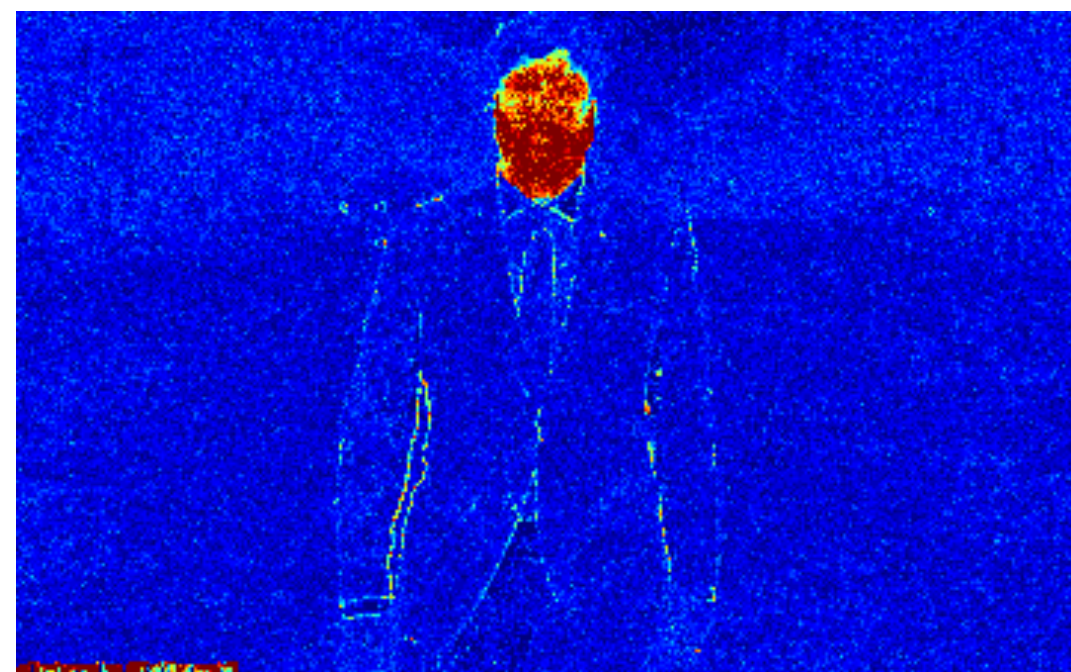
Complementarity of the methods



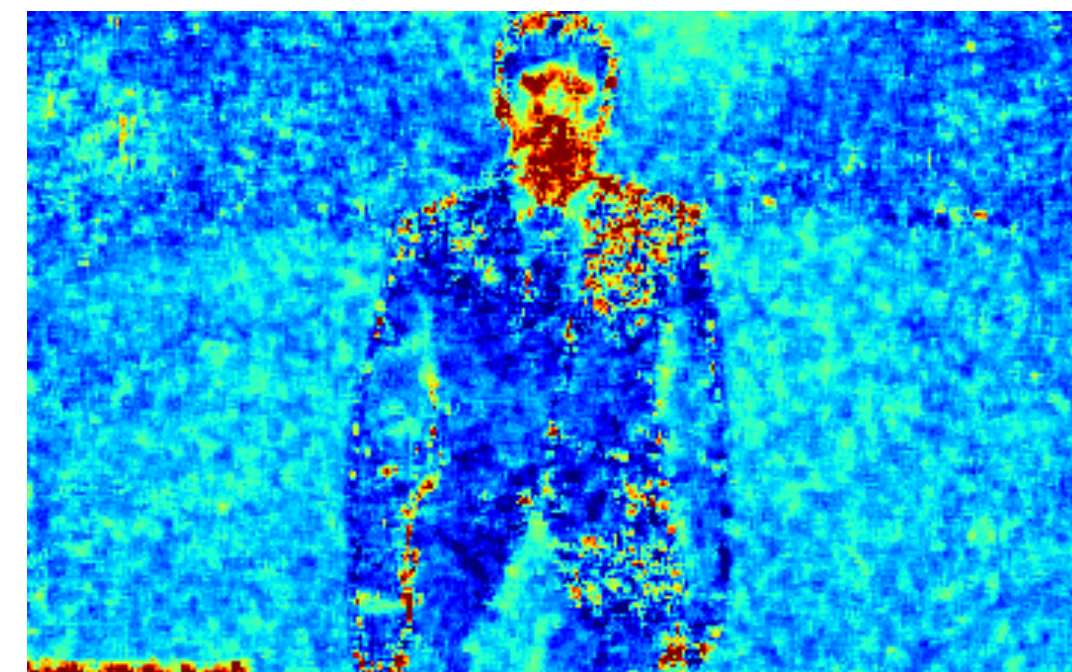
Forged image from @GuillaumeTC



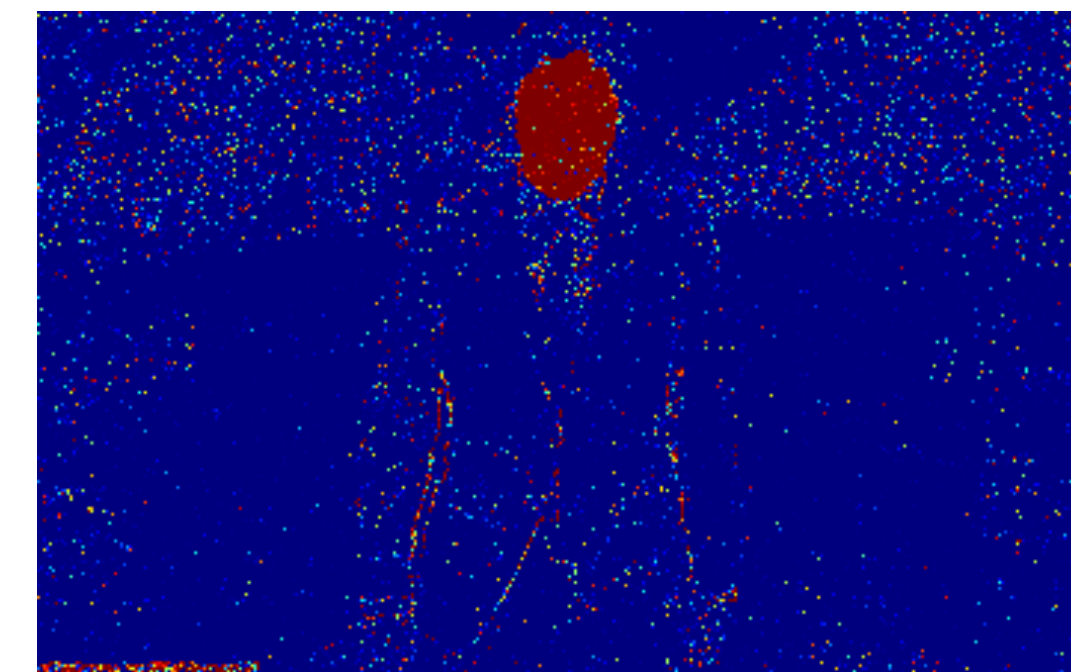
Detection result



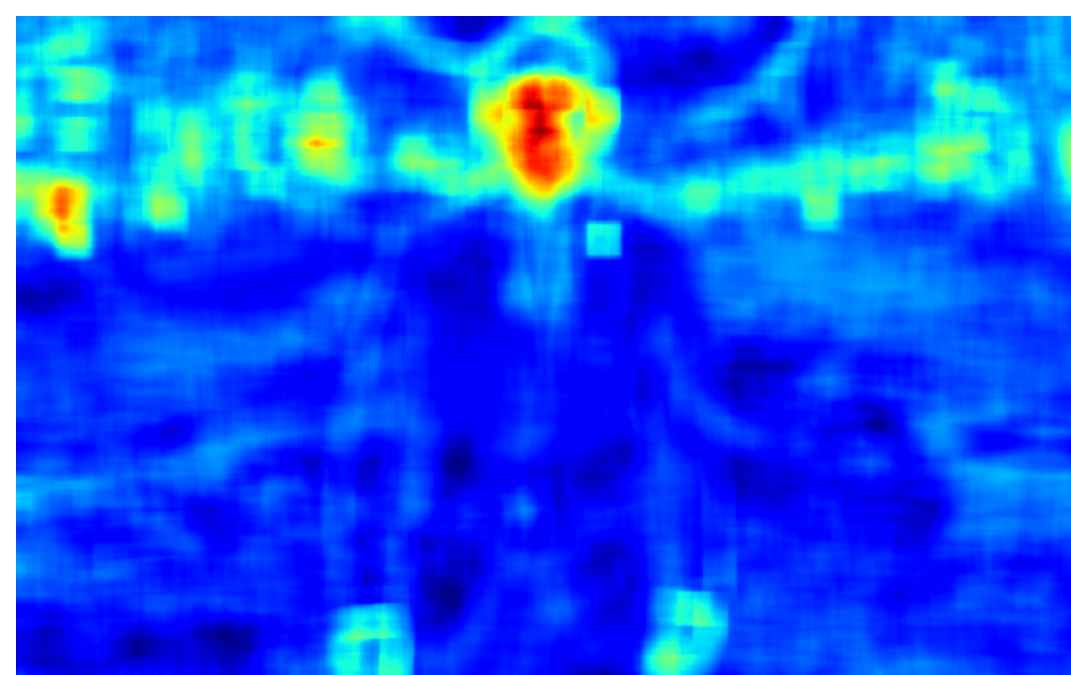
DCT



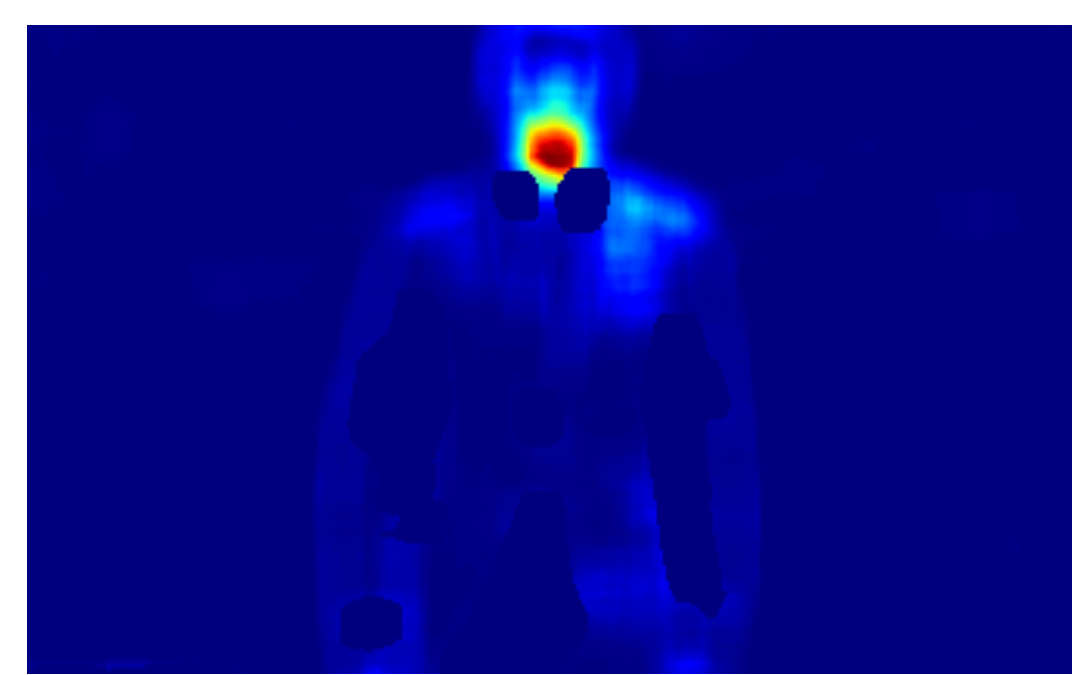
BLK



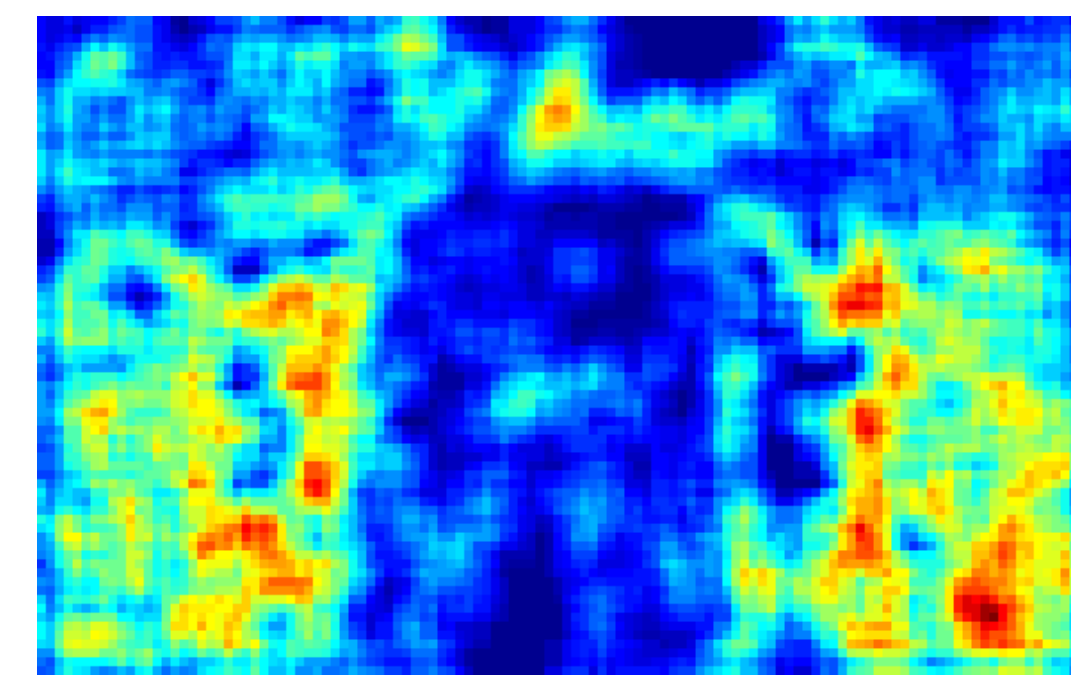
DQ



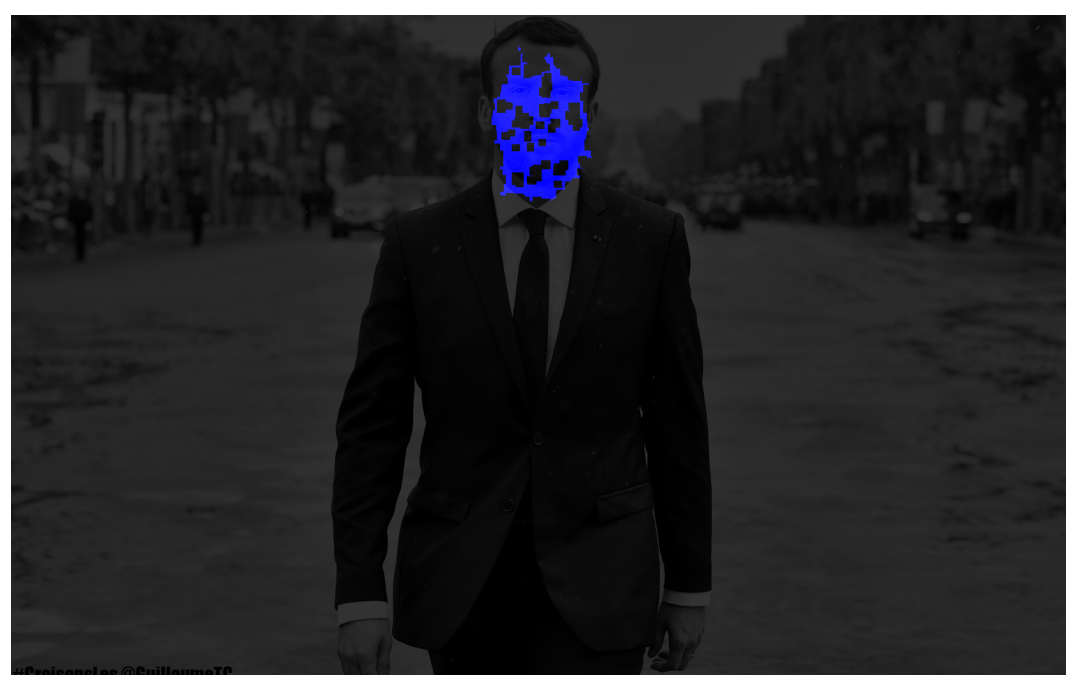
Ghost



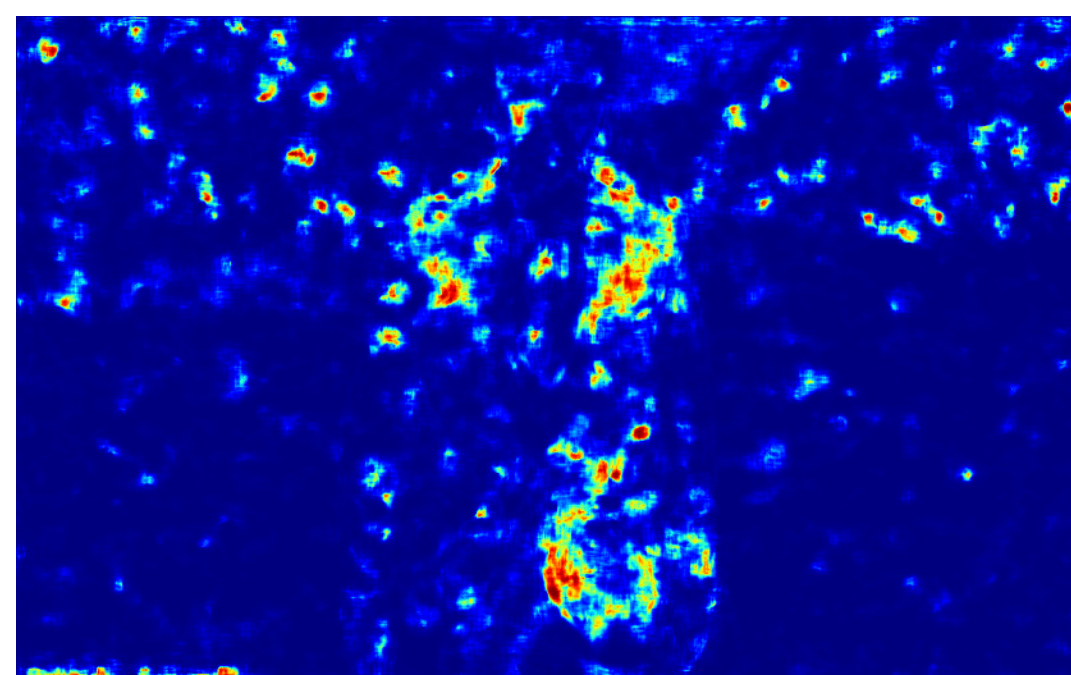
Splicebuster



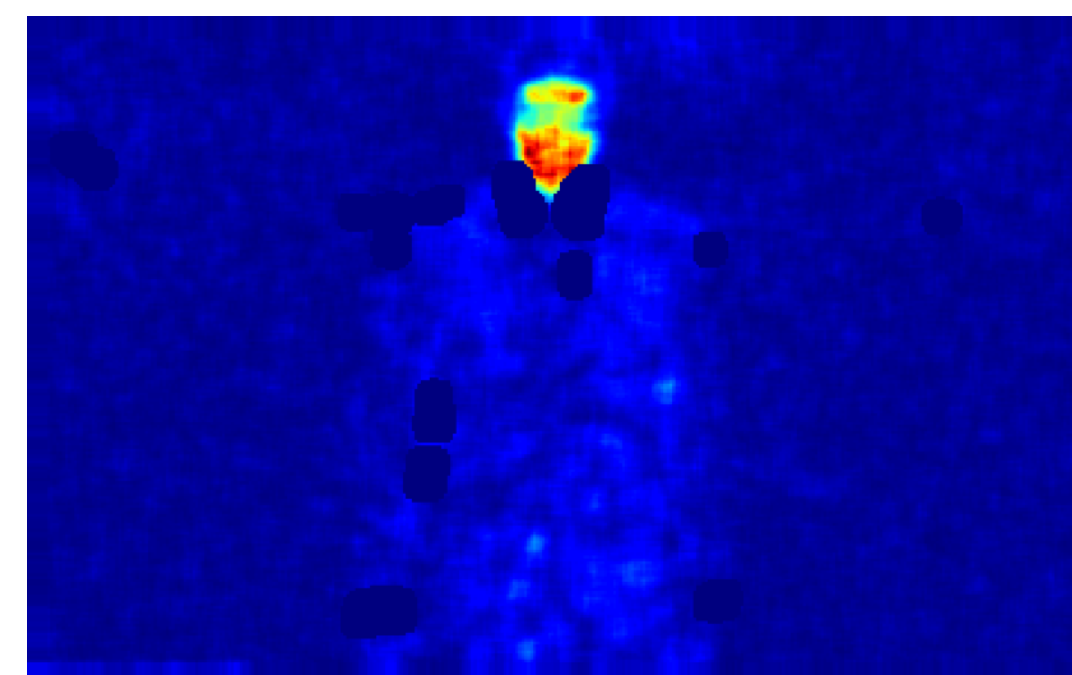
CAGI



zero



ManTraNet



Noiseprint

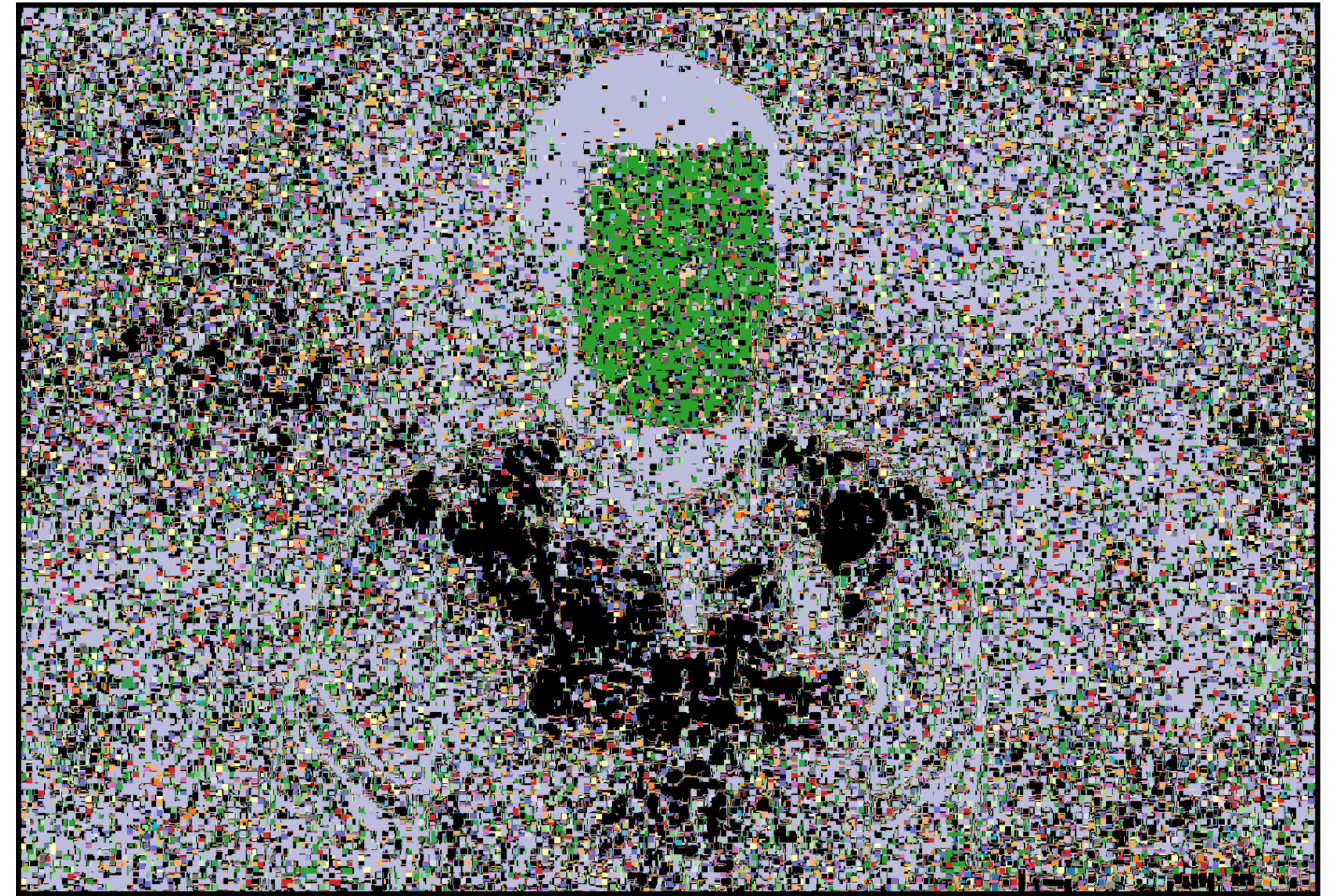


Comprint

Complementarity of the methods



Forged image from @GuillaumeTC



Vote map

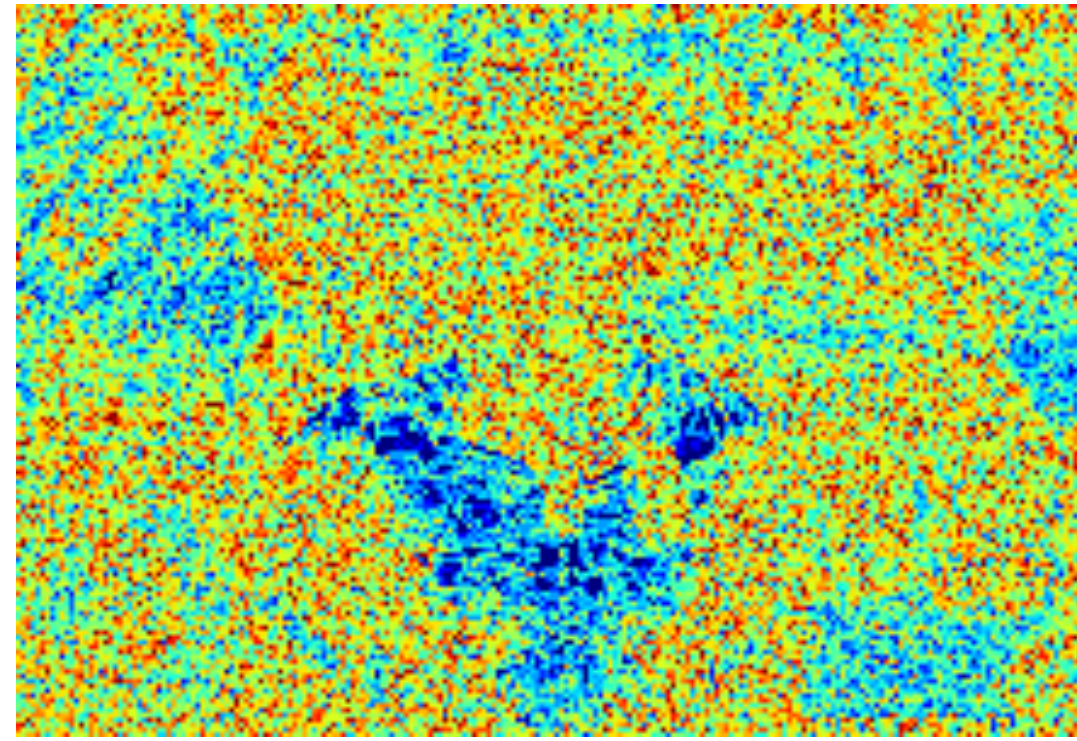
Complementarity of the methods



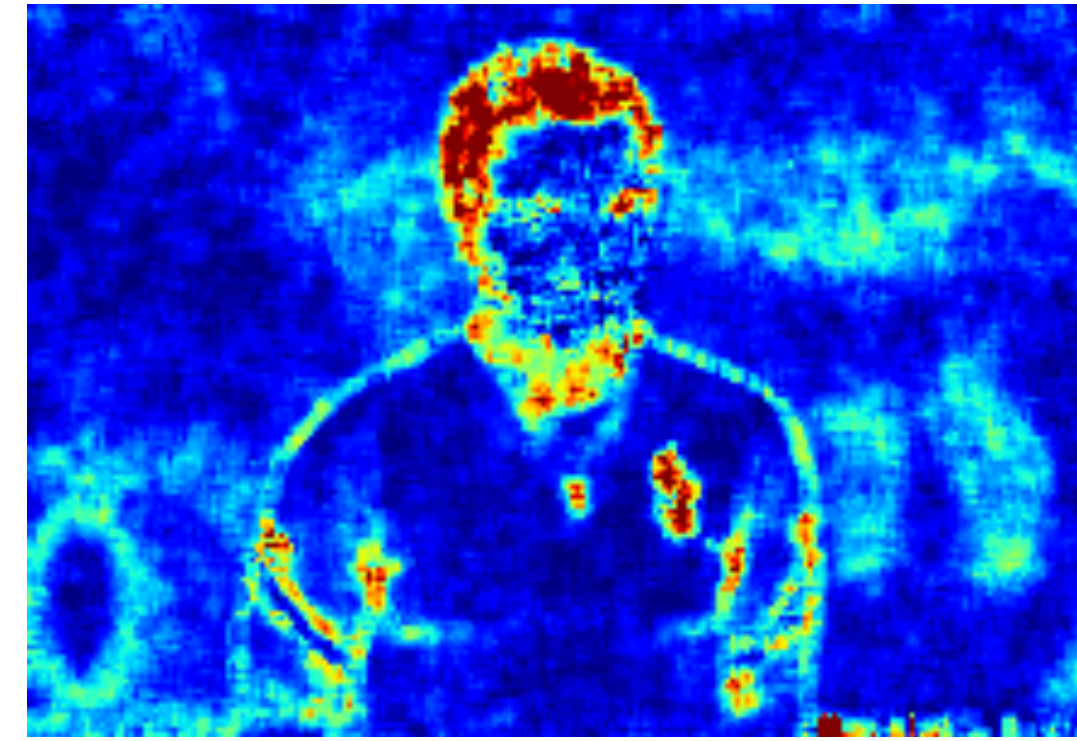
Forged image from @GuillaumeTC



Detection result



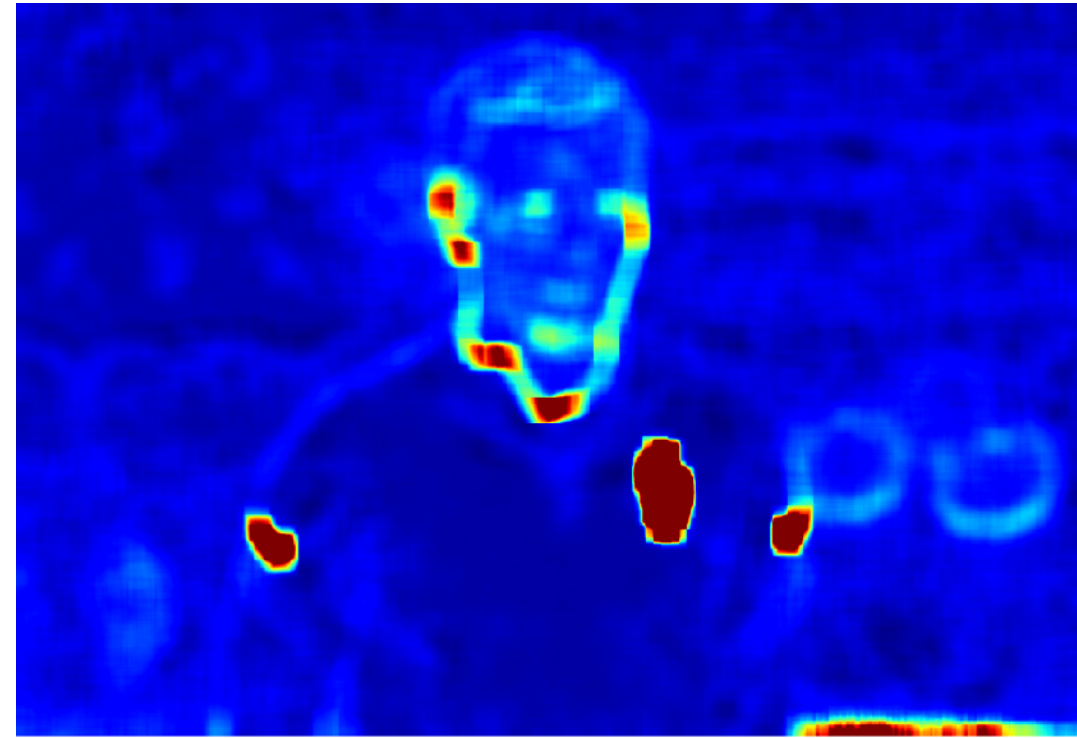
DCT



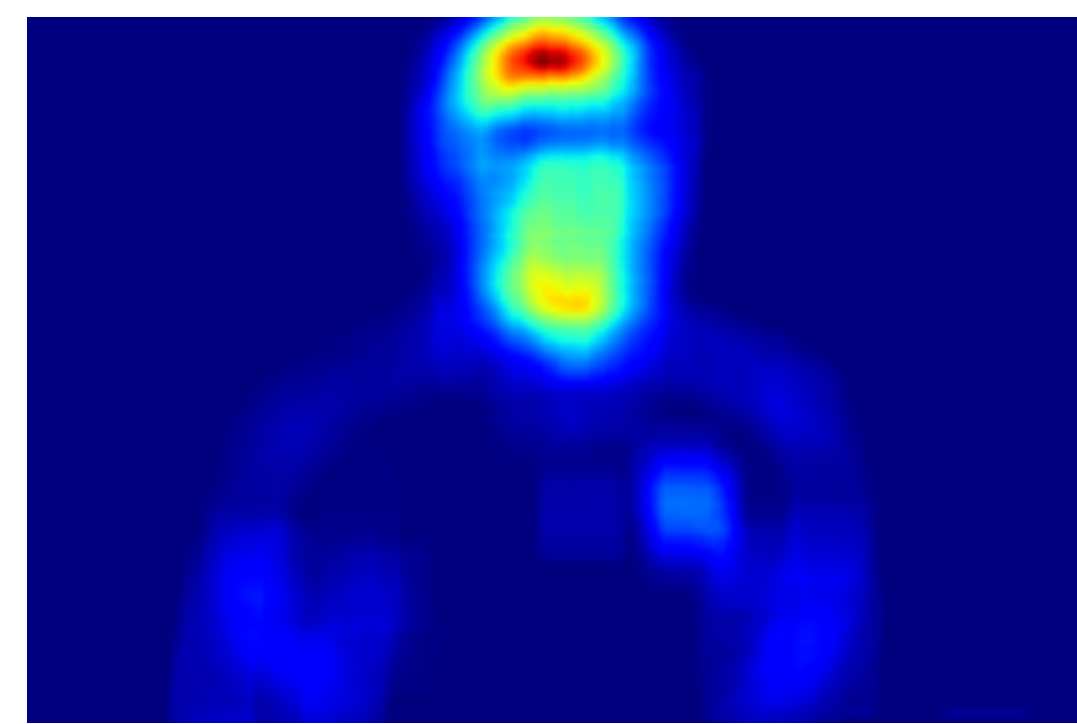
BLK



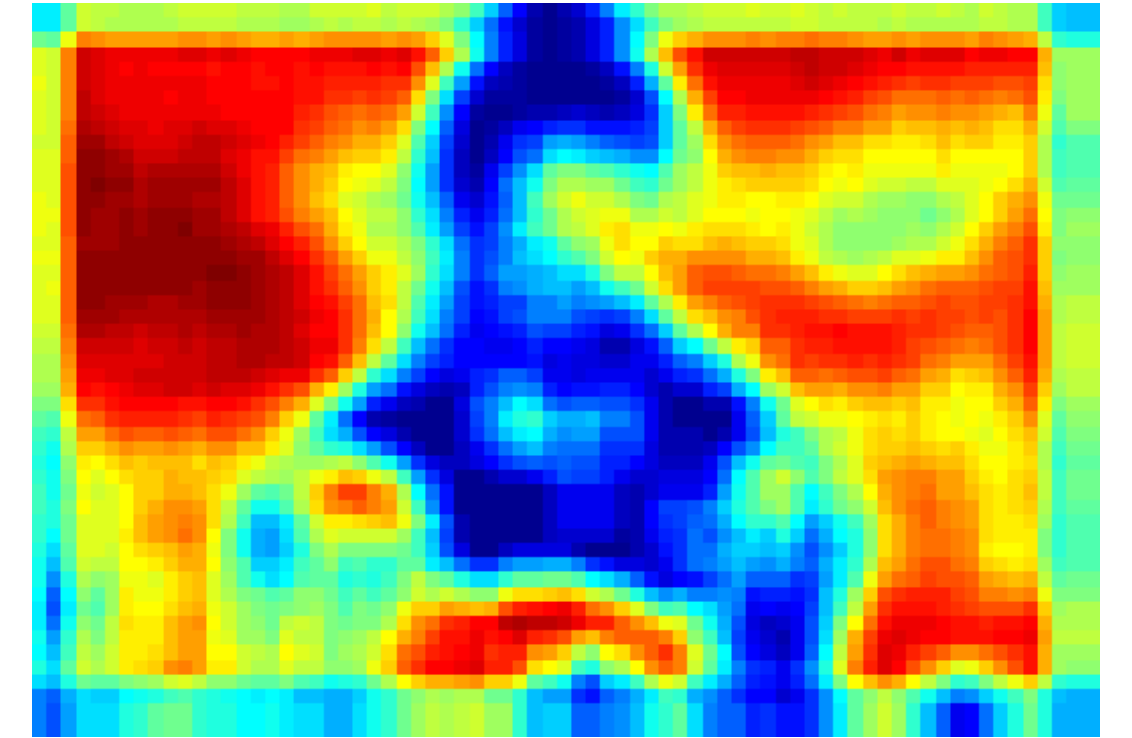
DQ



Ghost



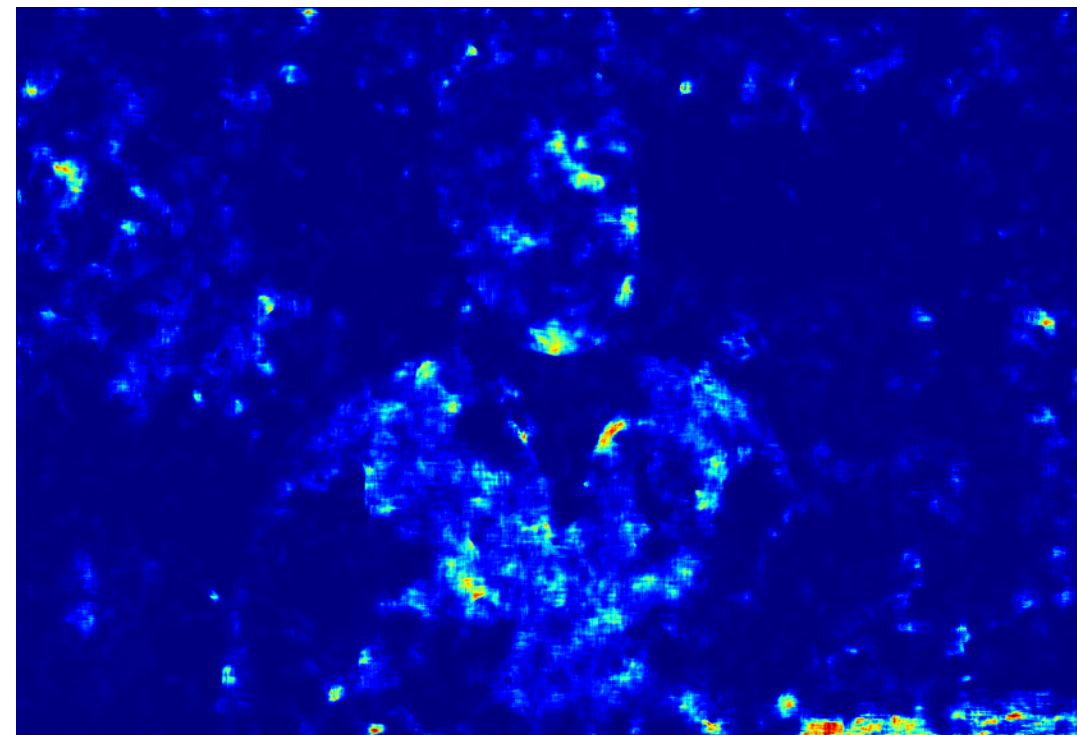
Splicebuster



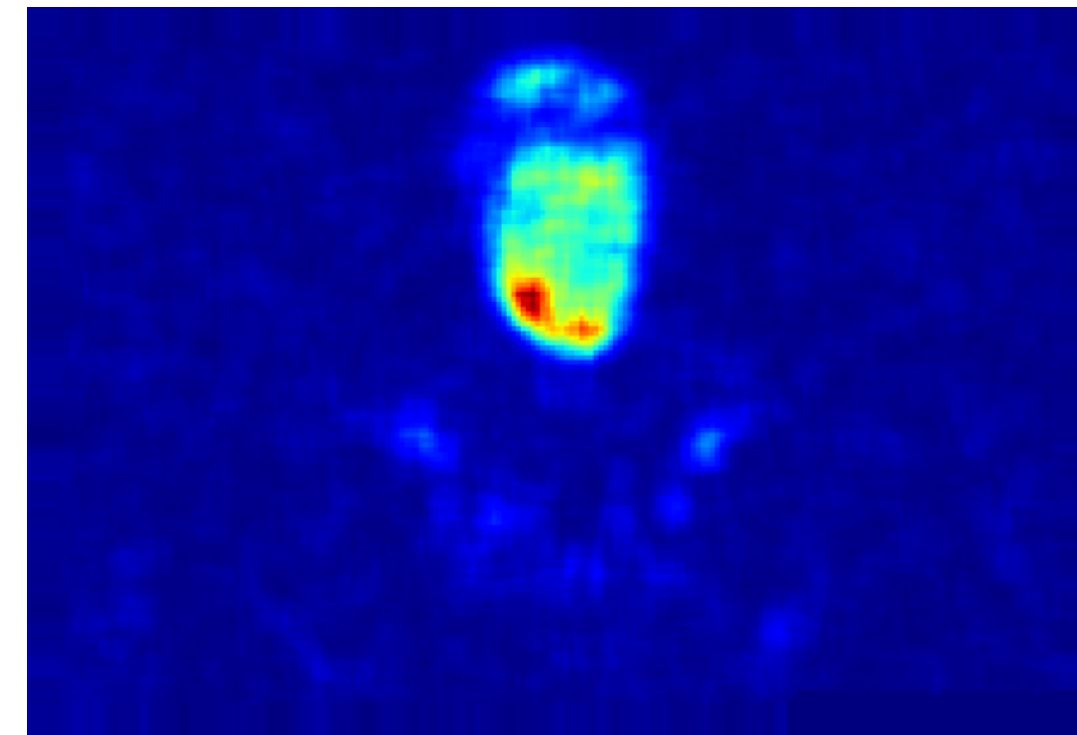
CAGI



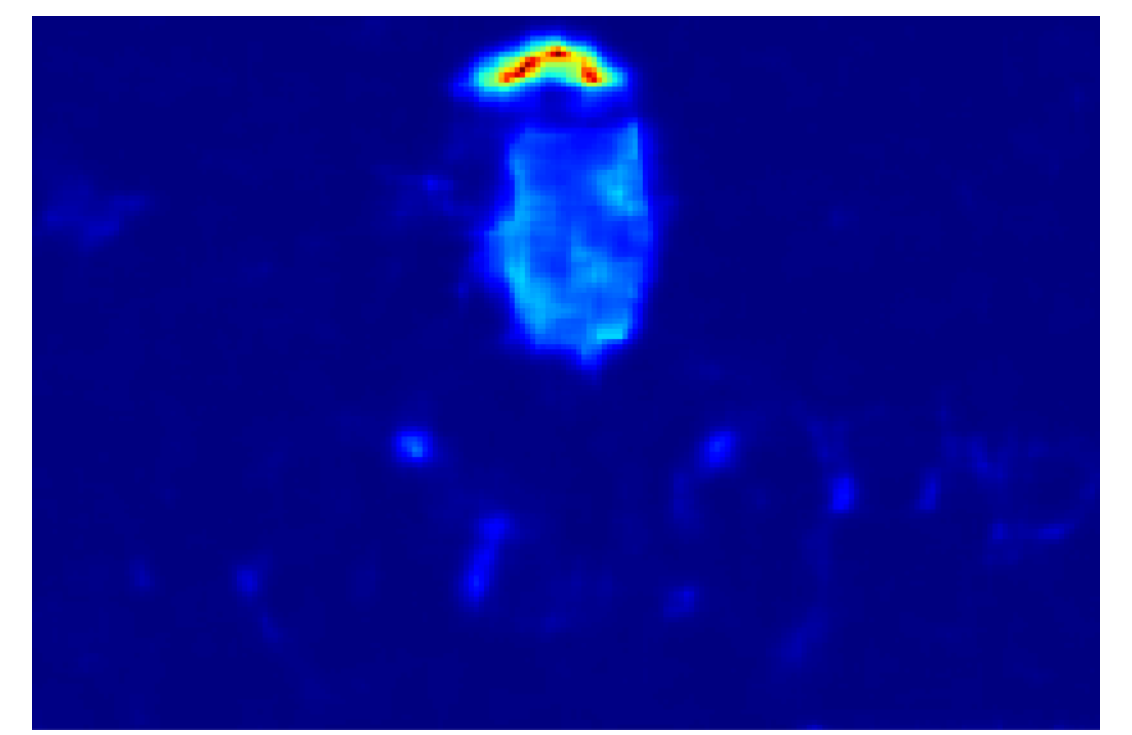
zero



ManTraNet



Noiseprint

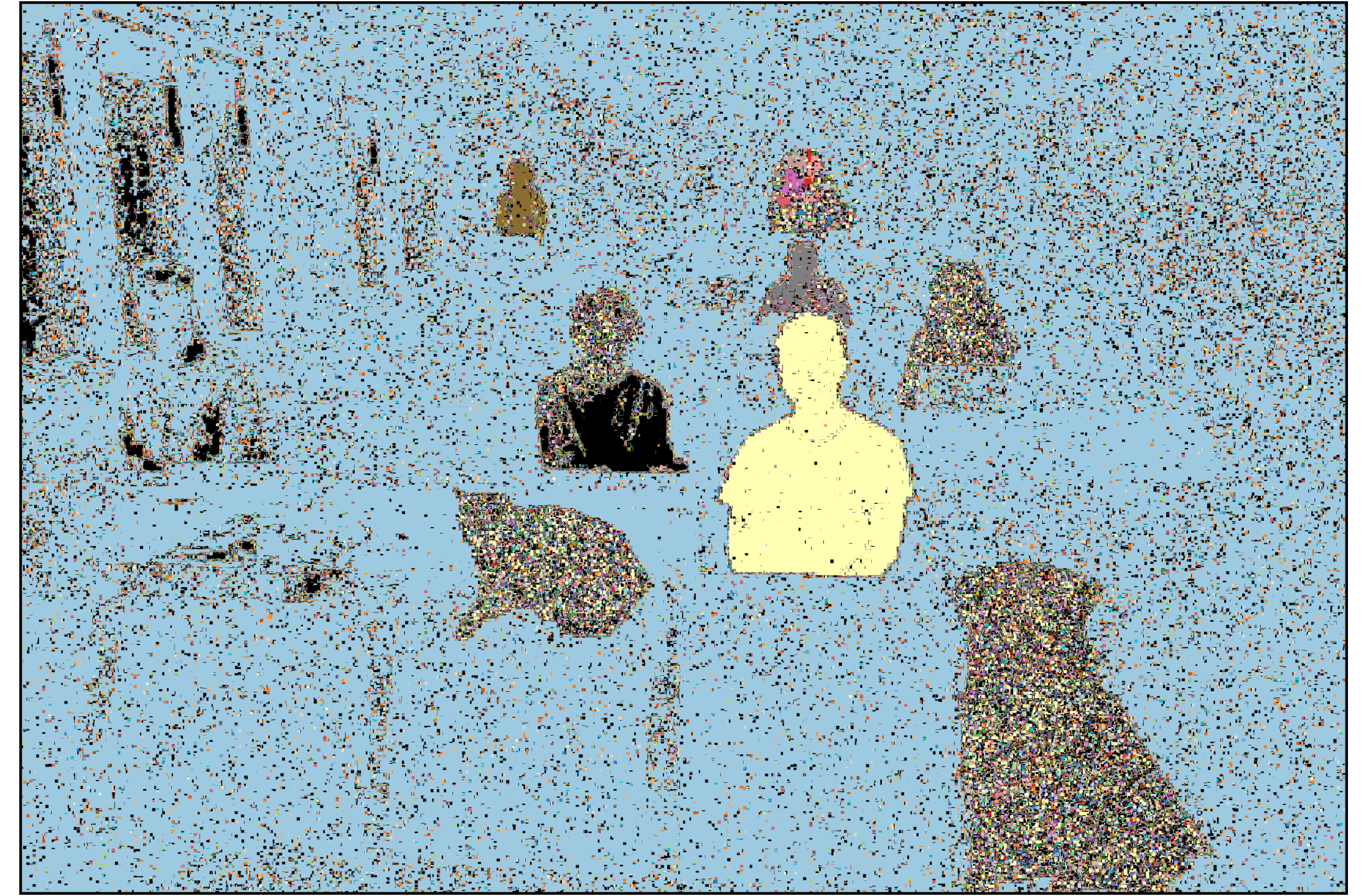


Comprint

Complementarity of the methods



Forged image

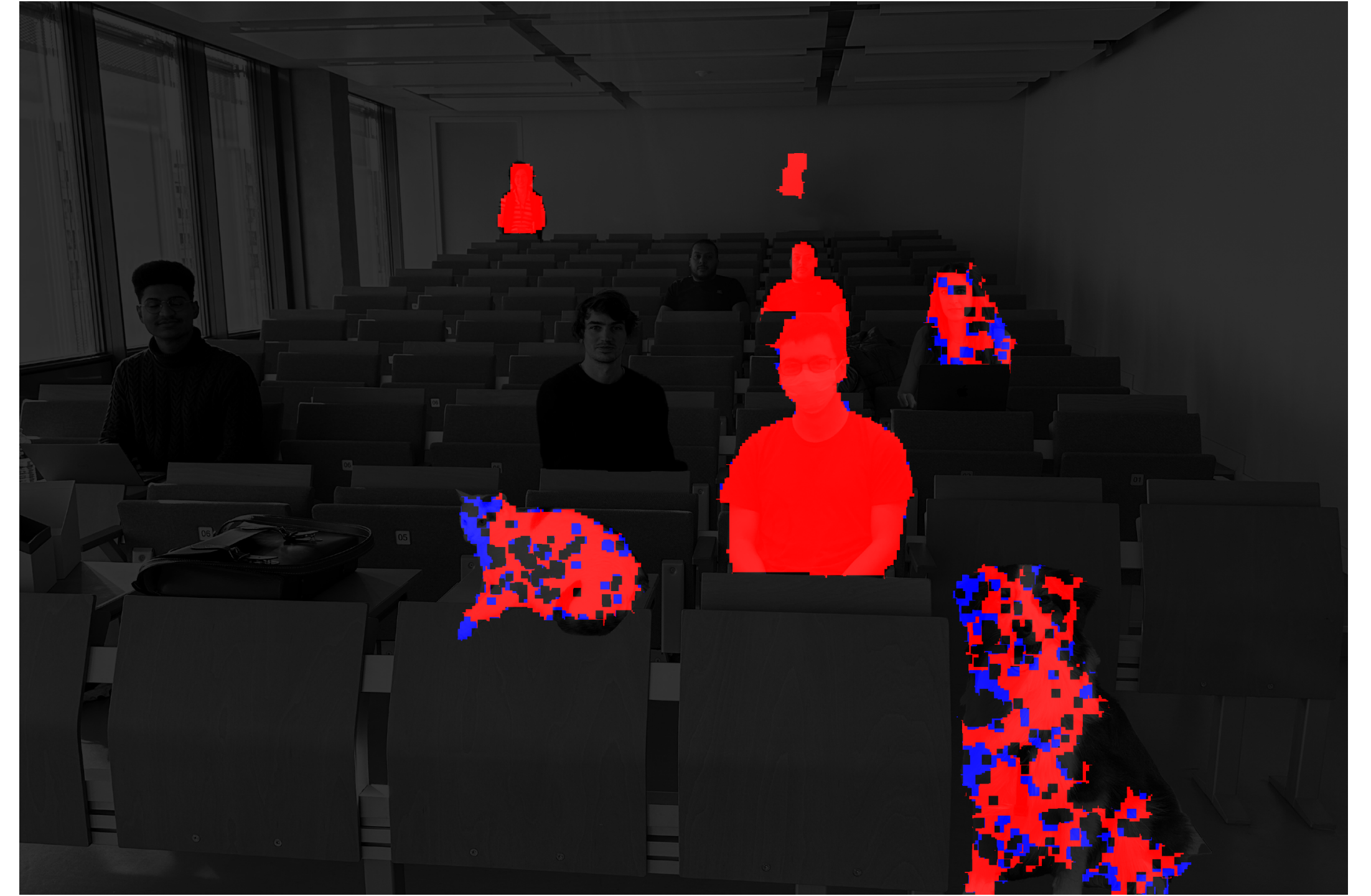


Vote map

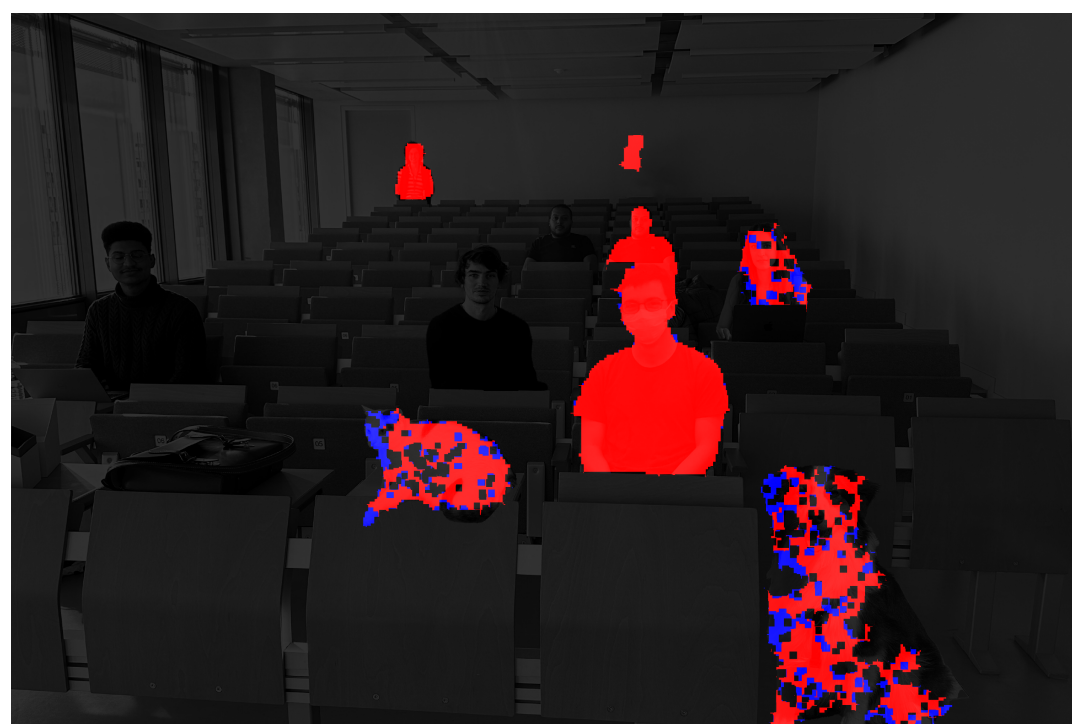
Complementarity of the methods



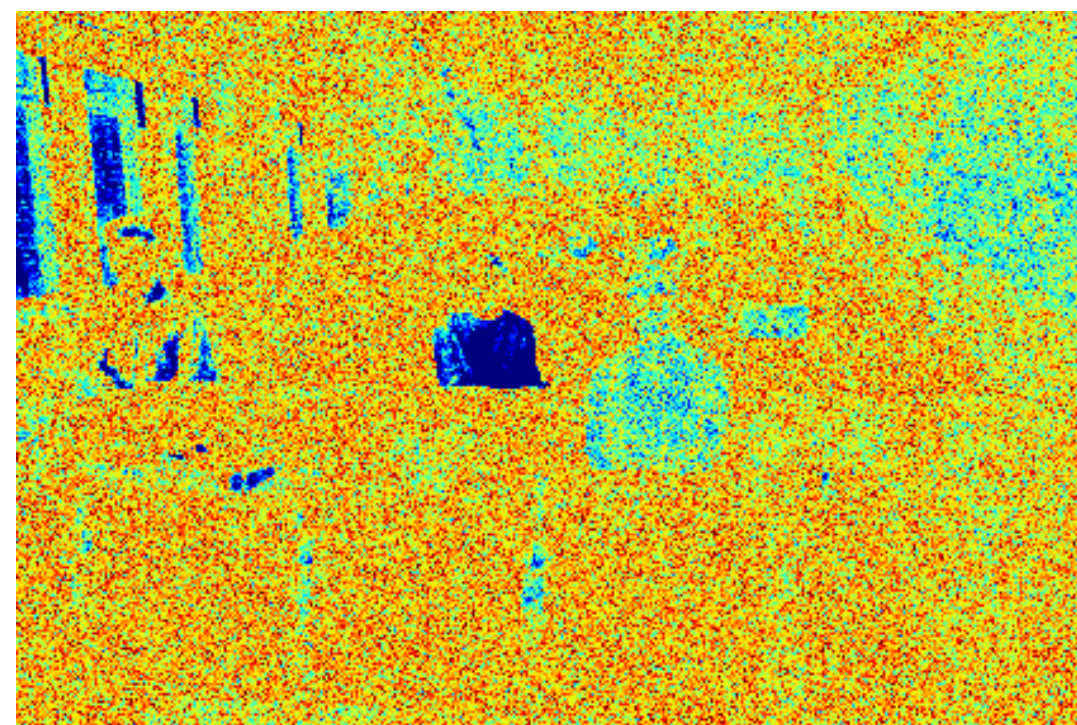
Forged image



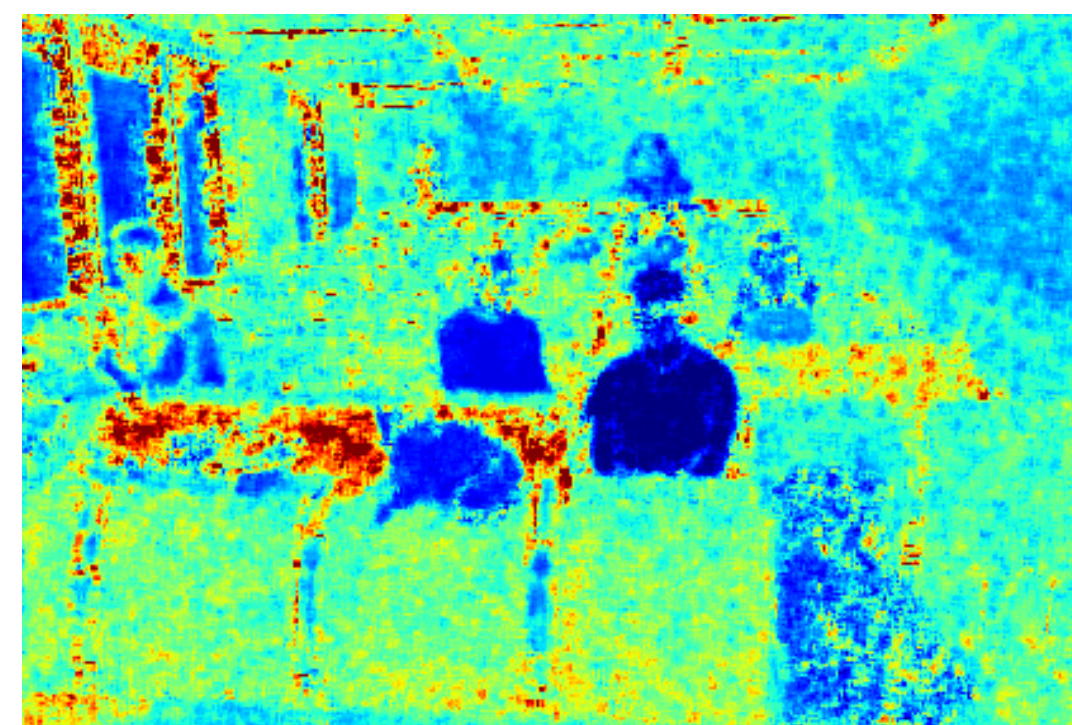
Detection result



zero



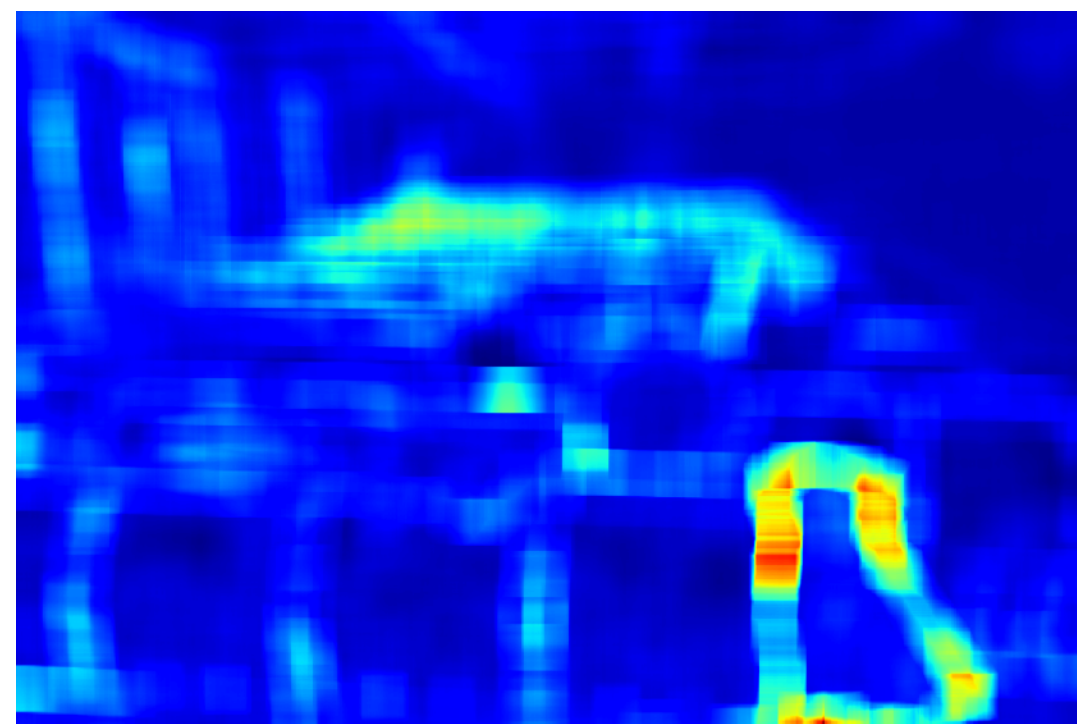
DCT



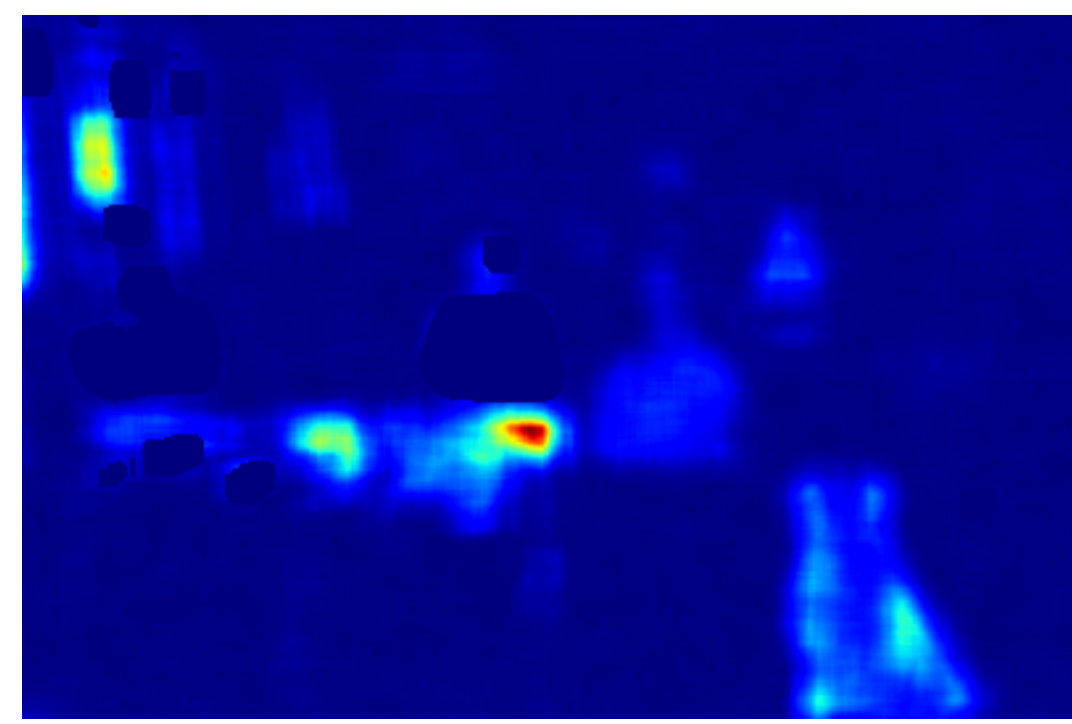
BLK



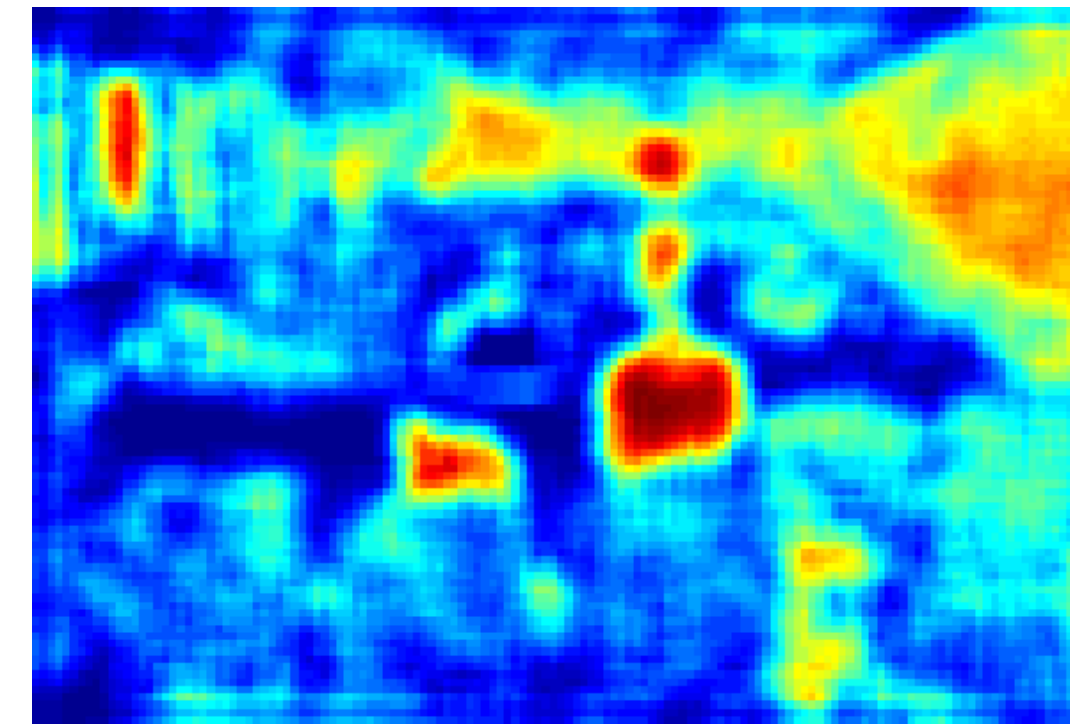
DQ



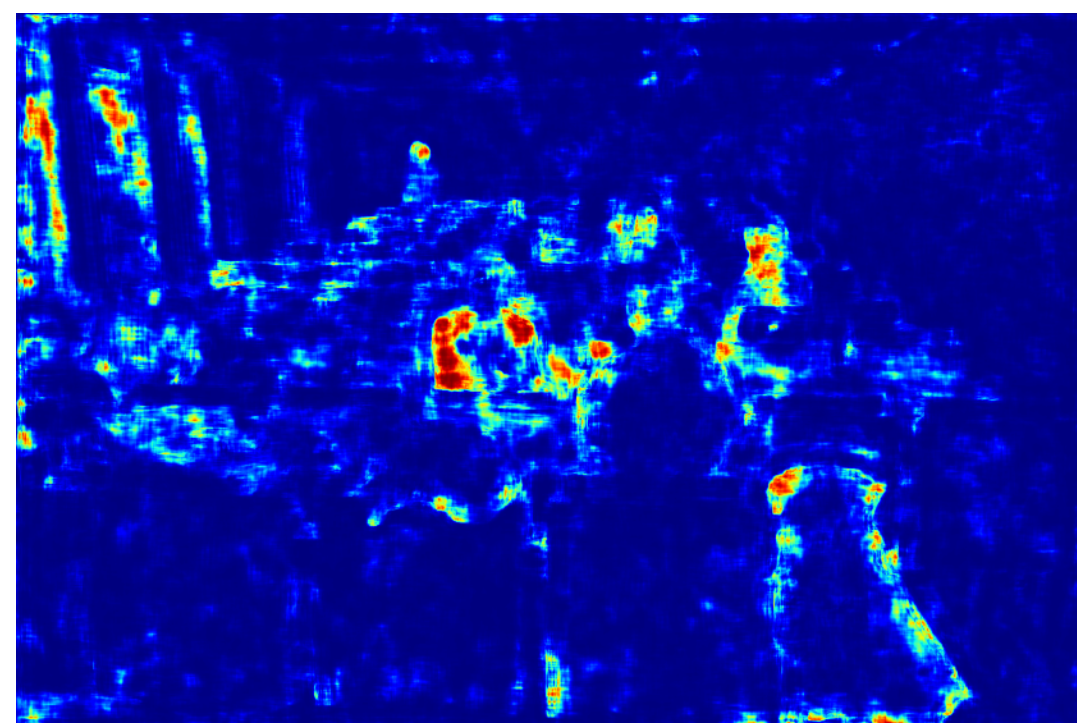
Ghost



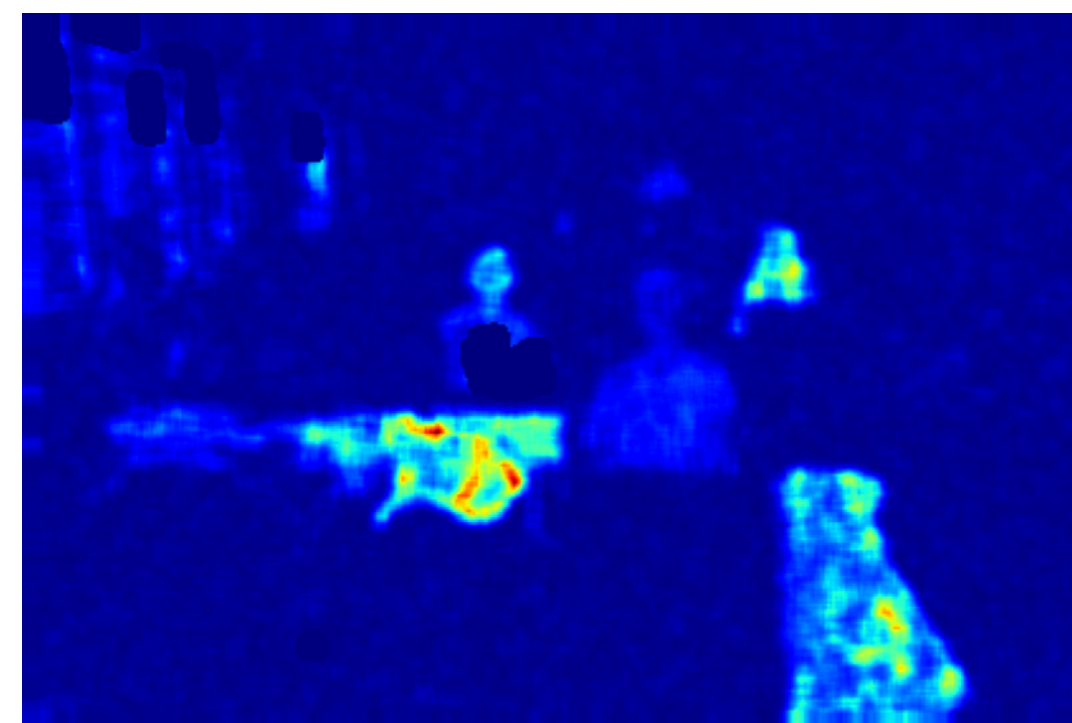
Splicebuster



CAGI



ManTraNet



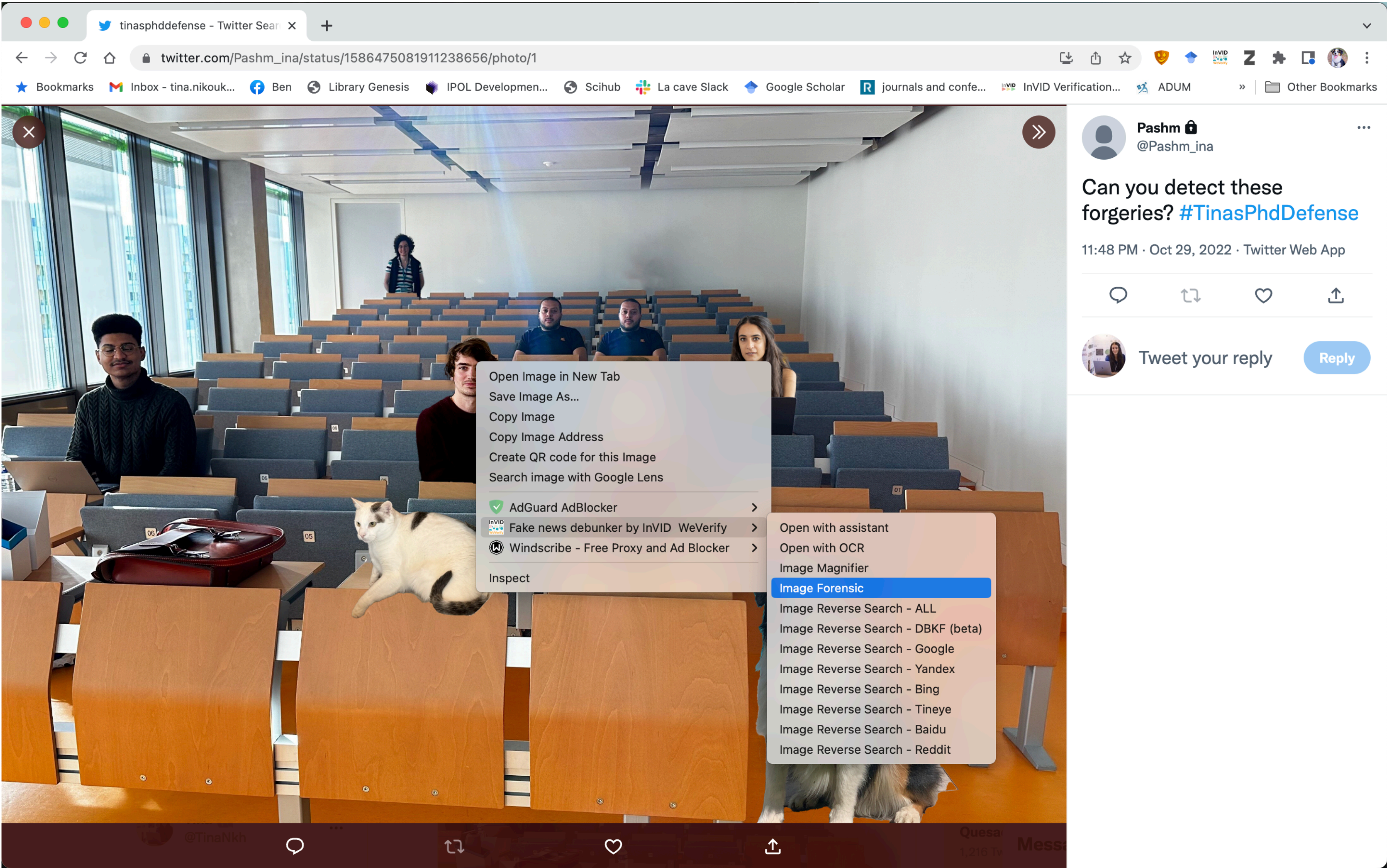
Noiseprint



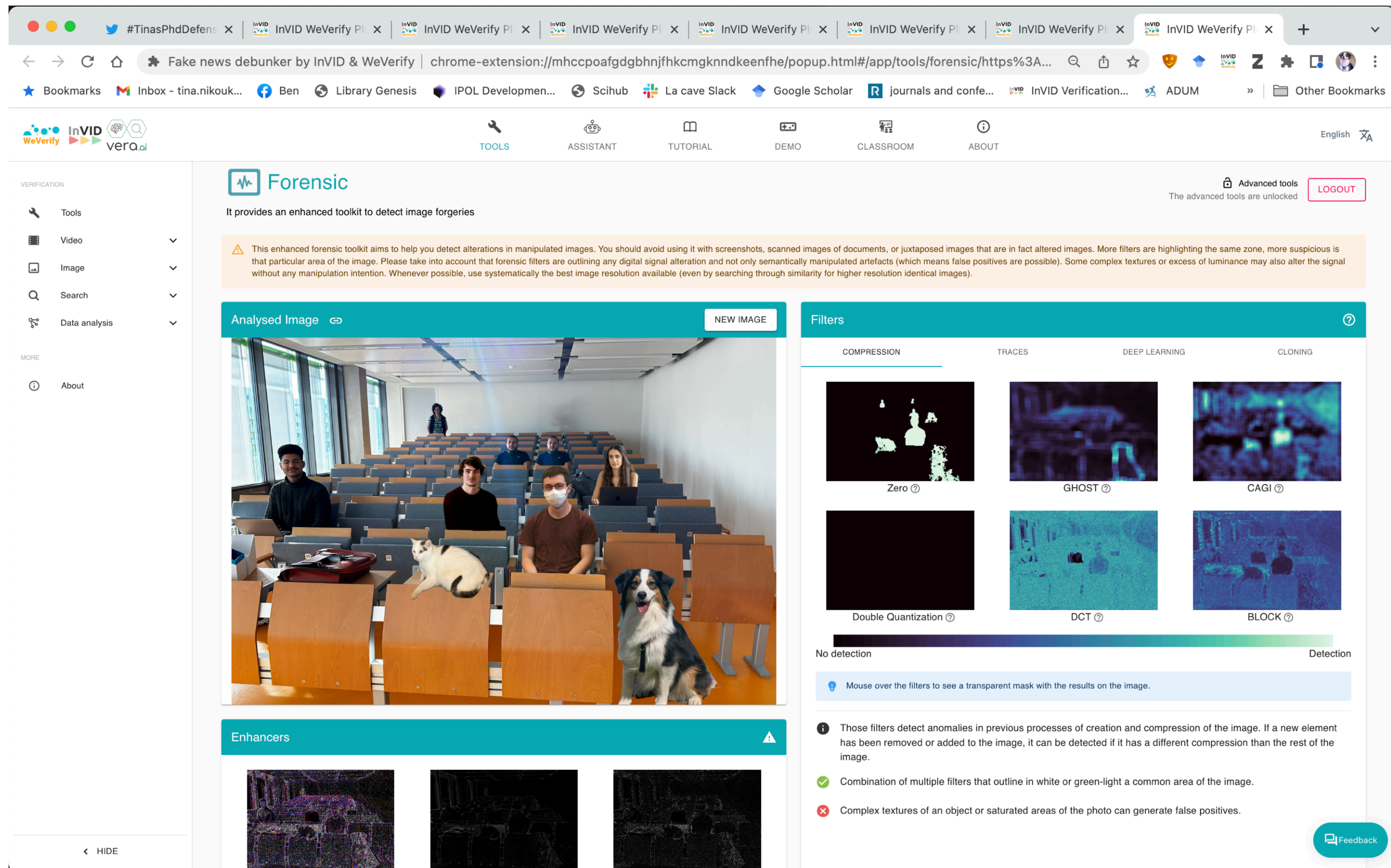
Comprint

How to use these tools?

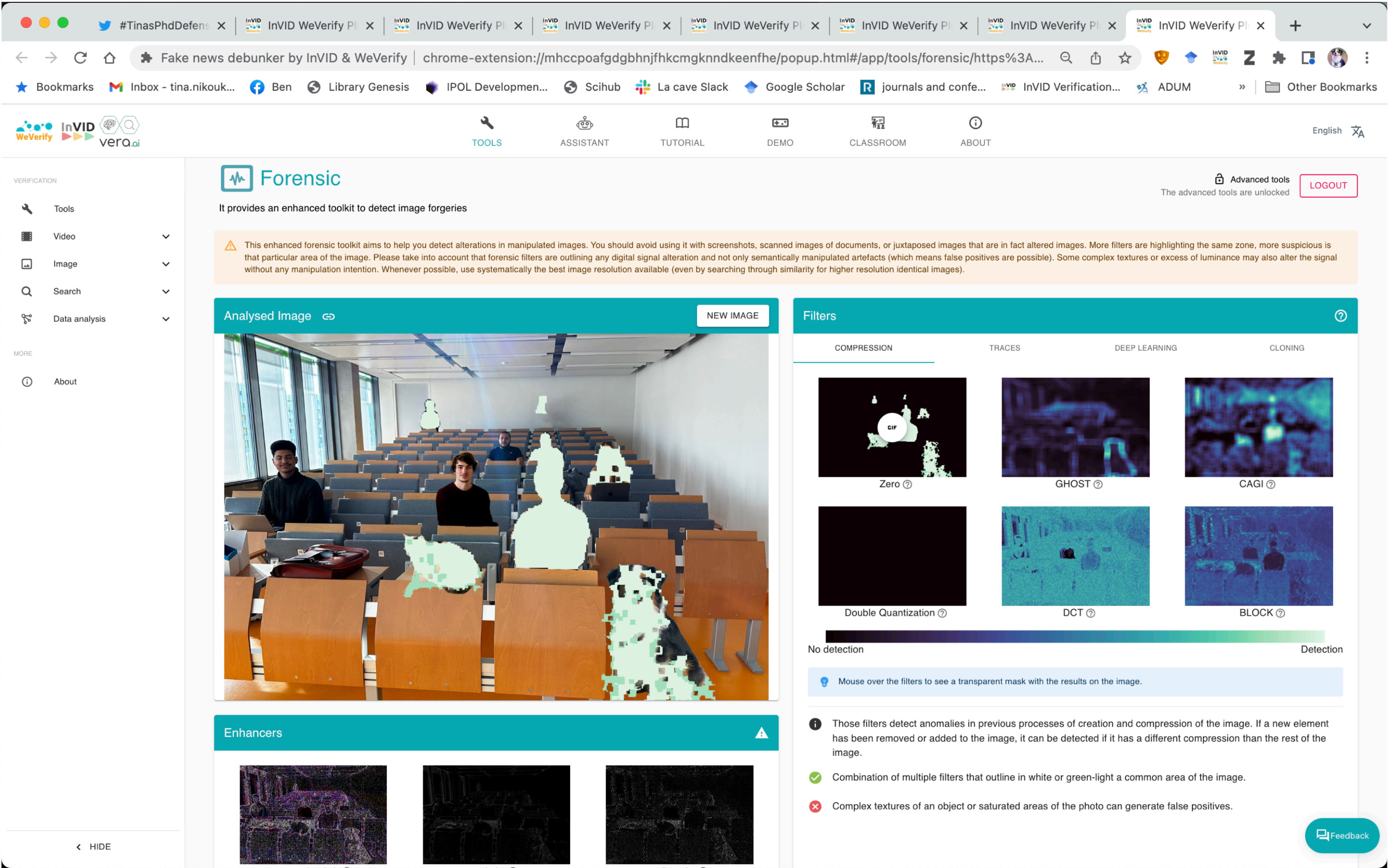
The InVID-WeVerify plug-in



The InVID-WeVerify plug-in



The InVID-WeVerify plug-in



What about the future of image forgery?



Stable Di 
@AI_forall

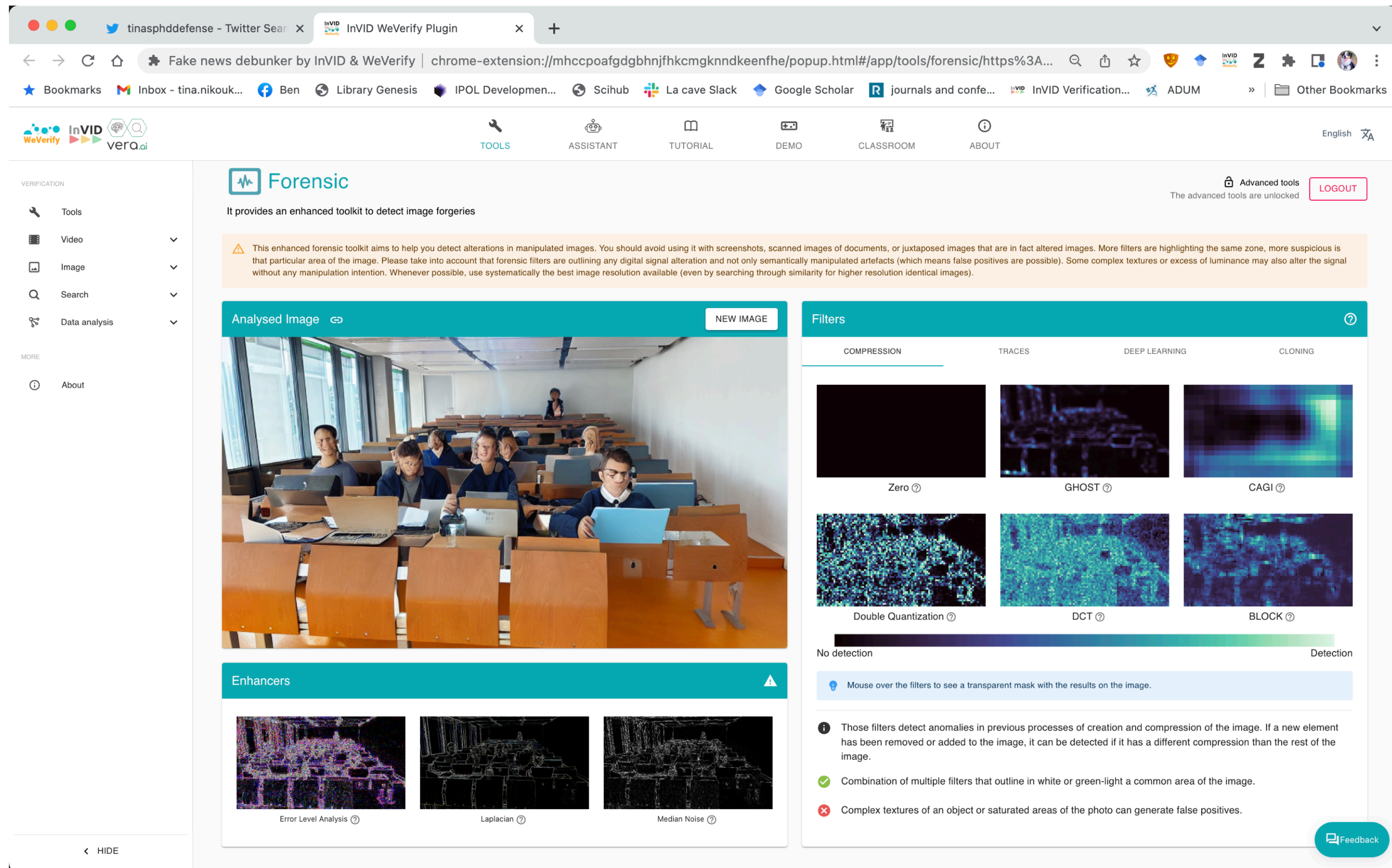


what does stable diffusion say about
[#TinasPhdDefense?](#)



4:07 PM · Nov 8, 2022 · Twitter Web App

What about the future of image forgery?



Contribution of this thesis

- **Local JPEG Grid Detection via Blocking Artifacts (GOD)**
Automatic JPEG grid detection with controlled false alarms, and its image forensic applications. T. Nikoukhah, R. Grompone von Gioi, M. Colom, and J.-M. Morel. IEEE Conference on Multimedia Information Processing and Retrieval (MIPR), 2018.
Local JPEG Grid Detector via Blocking Artifacts, a Forgery Detection Tool. T. Nikoukhah, M. Colom, J.-M. Morel, and R. Grompone von Gioi. Image Processing On Line, 2020.
- **Reliable Quantization Table Estimation (Qtable)**
A Reliable JPEG Quantization Table Estimator. T. Nikoukhah, M. Colom, J.-M. Morel, and R. Grompone von Gioi. Image Processing On Line, 2022.
- **Simple JPEG Grid Origin Detection (SimpleGOD)**
Détection de grille JPEG par compression simulée. T. Nikoukhah, M. Colom, J.-M. Morel, and R. Grompone von Gioi. GRETSI, 2019.
- **Local JPEG Grid Detection via the DCT zeros (ZERO)**
JPEG grid detection based on the number of DCT zeros and its application to automatic and localized forgery detection. T. Nikoukhah, J. Anger, T. Ehret, M. Colom, J.-M. Morel, and R. Grompone von Gioi. IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRw), 2019.
ZERO: a Local JPEG Grid Origin Detector Based on the Number of DCT Zeros and its Applications in Image Forensics. T. Nikoukhah, J. Anger, M. Colom, J.-M. Morel, and R. Grompone von Gioi. Image Processing On Line, 2021.
- **Non-Semantic Evaluation of Image Forensic Tools (Trace database)**
Non-Semantic Evaluation of Image Forensics Tools: Methodology and Database. Q. Bammey, T. Nikoukhah, M. Gardella, R. Grompone von Gioi, M. Colom, and J.-M. Morel. IEEE/CVF Winter Conference on Applications of Computer Vision (WACV), 2022.

Contribution of this thesis

The improvement of JPEG forensics approaches by controlling the false detections.

- Simple JPEG Grid Origin Detection (SimpleGOD)
Détection de grille JPEG par compression simulée. T. Nikoukhah, M. Colom, J.-M. Morel, and R. Grompone von Gioi. GRETSI, 2019.
- Local JPEG Grid Detection via the DCT zeros (ZERO)
JPEG grid detection based on the number of DCT zeros and its application to automatic and localized forgery detection. T. Nikoukhah, J. Anger, T. Ehret, M. Colom, J.-M. Morel, and R. Grompone von Gioi. IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRw), 2019.
ZERO: a Local JPEG Grid Origin Detector Based on the Number of DCT Zeros and its Applications in Image Forensics. T. Nikoukhah, J. Anger, M. Colom, J.-M. Morel, and R. Grompone von Gioi. Image Processing On Line, 2021.
- Non-Semantic Evaluation of Image Forensic Tools (Trace database)
Non-Semantic Evaluation of Image Forensics Tools: Methodology and Database. Q. Bammey, T. Nikoukhah, M. Gardella, R. Grompone von Gioi, M. Colom, and J.-M. Morel. IEEE/CVF Winter Conference on Applications of Computer Vision (WACV), 2022.

Contribution of this thesis

The improvement of JPEG forensics approaches by controlling the false detections.

Reverse engineering the compression of an image.

- **Local JPEG Grid Detection via the DCT zeros (ZERO)**
JPEG grid detection based on the number of DCT zeros and its application to automatic and localized forgery detection. T. Nikoukhah, J. Anger, T. Ehret, M. Colom, J.-M. Morel, and R. Grompone von Gioi. IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRw), 2019.
ZERO: a Local JPEG Grid Origin Detector Based on the Number of DCT Zeros and its Applications in Image Forensics. T. Nikoukhah, J. Anger, M. Colom, J.-M. Morel, and R. Grompone von Gioi. Image Processing On Line, 2021.
- **Non-Semantic Evaluation of Image Forensic Tools (Trace database)**
Non-Semantic Evaluation of Image Forensics Tools: Methodology and Database. Q. Bammey, T. Nikoukhah, M. Gardella, R. Grompone von Gioi, M. Colom, and J.-M. Morel. IEEE/CVF Winter Conference on Applications of Computer Vision (WACV), 2022.

Contribution of this thesis

The improvement of JPEG forensics approaches by controlling the false detections.

Reverse engineering the compression of an image.

The introduction of a new automatic JPEG GRID-based forgery detection method, called ZERO.

- Non-Semantic Evaluation of Image Forensic Tools (Trace database)

Non-Semantic Evaluation of Image Forensics Tools: Methodology and Database. Q. Bammey, T. Nikoukhah, M. Gardella, R. Grompone von Gioi, M. Colom, and J.-M. Morel. IEEE/CVF Winter Conference on Applications of Computer Vision (WACV), 2022.

Contribution of this thesis

The improvement of JPEG forensics approaches by controlling the false detections.

Reverse engineering the compression of an image.

The introduction of a new automatic JPEG GRID-based forgery detection method, called ZERO.

The establishment of a new non-semantic methodology to evaluate forensic tools.

Future lines of research

- Adapting the existing methods to the **chroma channels**.
- Making the method Qtable local to create a **JPEG QUALITY-based forgery detection** algorithm.
- Detecting **resampling** operations.
- Adding operations/**datasets to the Trace database**, such as resampling and double compression.
- New/other **compression algorithms** for images and video.
- Fake images generated by **text-to-image** diffusion models!

Image processing team!



From zero to research, projects, teaching, popular science

 This CVPR Workshop paper is the Open Access version, provided by the Computer Vision Foundation. Except for this watermark, it is identical to the accepted version; the final published version of the proceedings is available on IEEE Xplore.

JPEG Grid Detection based on the Number of DCT Zeros and its Application to Automatic and Localized Forgery Detection

T. Nikoukhah J. Anger T. Ehret M. Colom J.M. Morel R. Grompone von Gioi
CMLA, CNRS, ENS Paris-Saclay, Université Paris-Saclay
{nikoukhah, anger, ehret, colom, morel, grompone}@cmla.ens-cachan.fr

Abstract

This work proposes a novel method for detecting JPEG compression, as well as its grid origin, based on counting the number of zeros in the DCT of 8×8 blocks. When applied locally, the same method can be used to detect grid alignment abnormalities. It therefore detects local image forgeries such as copy-move. The algorithm includes a statistical validation step which gives theoretical guarantees on the number of false alarms and provides secure guarantees for tampering detection. The performance of the proposed method is illustrated with both quantitative and visual results from well-known image databases and comparisons with state of the art methods.

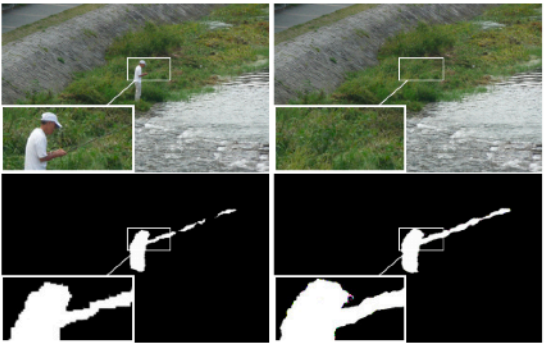


Figure 1: Result of the proposed method, from top left to bottom right: original image, forged image (input of the method), detected forgeries, ground-truth. The fisherman and the fishing rod have been removed. The resulting detected mask does not require visual interpretation.

1. Introduction

Image tampering is currently used massively on the web and continuously feeds fake news [12]. This issue has become important since digital image manipulation tools are available to the general public. Some social networks even allow to edit images and videos directly online. Since these platforms (Facebook, Instagram, Snapchat, etc.) delete all metadata for confidentiality reasons, there is a crucial need for journalists and mass-media producers to have access to tools for detecting forgeries from the image itself. Several such tools are readily available online, *Fotoforensics*, *Forensically*, *Ghiro* and *Reveal*¹ for instance. These tools provide a number of “tampering localization maps” [26] in the form of so-called image *heat maps* revealing suspicious alterations. However, those localization maps work only as trace enhancers and do not provide any solid proof of forgery. The result needs to be analyzed with care and interpreted by experts. We attempt here to fill in this gap by producing an automatic method using the tampering traces left in the image and taking an automatic decision about forgeries and their precise

location. Indeed, even in absence of image metadata, much information about the history of the image is still present in the image itself. Many processes undergone by an image leave invisible but detectable traces all over the image. Following [2, 3, 10, 11, 12, 15, 20, 29], we address one of the most common processes, namely the JPEG compression. This compression leaves traces in the form of 8×8 pixels blocking artifacts that produce a grid over the image.

Here we propose an automatic and statistically founded method for detecting the grid division of the image. The proposed method, hereafter referred to as ZERO, performs a global grid detection and then applies it more locally to detect forgeries. Indeed, image splicing generally breaks locally the original grid alignment. A locally detected grid therefore may contradict the global grid and become a reliable cue that a forgery took place. We evaluate ZERO against several state of the art algorithms on publicly available datasets. The detection does not require a human expert’s decision as shown in Figure 1, and is associated with theoretical guarantees.

¹<https://fotoforensics.com>, <https://29a.ch/photo-forensics>,
<https://www.getghiro.org>, <http://reveal-niklabb.it>, gr



From zero to research, projects, teaching, popular science



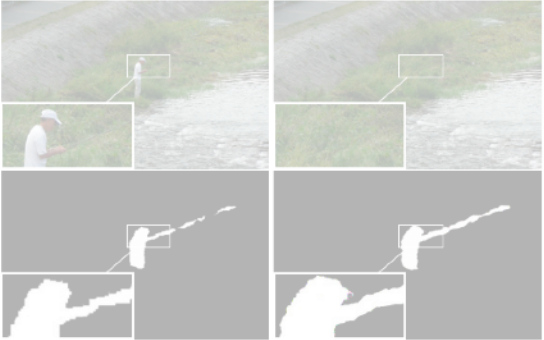
This CVPR Workshop paper is the Open Access version, provided by the Computer Vision Foundation. Except for this watermark, it is identical to the accepted version; the final published version of the proceedings is available on IEEE Xplore.

JPEG Grid Detection based on the Number of DCT Zeros and its Application to Automatic and Localized Forgery Detection

T. Nikoukhah J. Anger T. Ehret M. Colom J.M. Morel R. Grompone von Gioi
CMLA, CNRS, ENS Paris-Saclay, Université Paris-Saclay
{nikoukhah,anger,ehret,colom,morel,grompone}@cmla.ens-cachan.fr

Abstract

This work proposes a novel method for detecting JPEG compression, as well as its grid origin, based on counting the number of zeros in the DCT of 8×8 blocks. When applied locally, the same method can be used to detect grid alignment abnormalities. It therefore detects local image forgeries such as copy-move. The algorithm includes a statistical validation step which gives theoretical guarantees on the number of false alarms and provides secure guarantees for tampering detection. The performance of the proposed method is illustrated with both quantitative and visual results from well-known image databases and comparisons with state of the art methods.



1. Introduction

Image tampering is currently used massively on the web and continuously feeds fake news [12]. This issue has become important since digital image manipulation tools are available to the general public. Some social networks even allow to edit images and videos directly online. Since these platforms (Facebook, Instagram, Snapchat, etc.) delete all metadata for confidentiality reasons, there is a crucial need for journalists and mass-media producers to have access to tools for detecting forgeries from the image itself. Several such tools are readily available online, *Fotoforensics*, *Forensically*, *Ghiro* and *Reveal*¹ for instance. These tools provide a number of “tampering localization maps” [26] in the form of so-called image *heat maps* revealing suspicious alterations. However, those localization maps work only as trace enhancers and do not provide any solid proof of forgery. The result needs to be analyzed with care and interpreted by experts. We attempt here to fill in this gap by producing an automatic method using the tampering traces left in the image and taking an automatic decision about forgeries and their precise

location. Indeed, even in absence of image metadata, much information about the history of the image is still present in the image itself. Many processes undergone by an image leave invisible but detectable traces all over the image. Following [2, 3, 10, 11, 12, 15, 20, 29], we address one of the most common processes, namely the JPEG compression. This compression leaves traces in the form of 8×8 pixels blocking artifacts that produce a grid over the image.

Here we propose an automatic and statistically founded method for detecting the grid division of the image. The proposed method, hereafter referred to as ZERO, performs a global grid detection and then applies it more locally to detect forgeries. Indeed, image splicing generally breaks locally the original grid alignment. A locally detected grid therefore may contradict the global grid and become a reliable cue that a forgery took place. We evaluate ZERO against several state of the art algorithms on publicly available datasets. The detection does not require a human expert’s decision as shown in Figure 1, and is associated with theoretical guarantees.

¹<https://fotoforensics.com>, <https://29a.ch/photo-forensics>,
<https://www.getghiro.org>, <http://reveal-niklabb.it>,gr



From zero to research, projects, teaching, popular science



This CVPR Workshop paper is the Open Access version, provided by the Computer Vision Foundation. Except for this watermark, it is identical to the accepted version; the final published version of the proceedings is available on IEEE Xplore.

JPEG Grid Detection based on the Number of DCT Zeros and its Application to Automatic and Localized Forgery Detection

T. Nikoukhah J. Anger T. Ehret M. Colom J.M. Morel R. Grompone von Gioi

CMLA, CNRS, ENS Paris-Saclay, Université Paris-Saclay

{nikoukhah,anger,ehret,colom,morel,grompone}@cmla.ens-cachan.fr

Abstract

This work proposes a novel method for detecting JPEG compression, as well as its grid origin, based on counting the number of zeros in the DCT of 8×8 blocks. When applied locally, the same method can be used to detect grid alignment abnormalities. It therefore detects local image forgeries such as copy-move. The algorithm includes a statistical validation step which gives theoretical guarantees on the number of false alarms and provides secure guarantees for tampering detection. The performance of the proposed method is illustrated with both quantitative and visual results from well-known image databases and comparisons with state of the art methods.

1. Introduction

Image tampering is currently used massively on the web and continuously feeds fake news [12]. This issue has become important since digital image manipulation tools are available to the general public. Some social networks even allow to edit images and videos directly online. Since these platforms (Facebook, Instagram, Snapchat, etc.) delete all metadata for confidentiality reasons, there is a crucial need for journalists and mass-media producers to have access to tools for detecting forgeries from the image itself. Several such tools are readily available online, *Fotoforensics*, *Forensically*, *Ghiro* and *Reveal*¹ for instance. These tools provide a number of “tampering localization maps” [26] in the form of so-called image *heat maps* revealing suspicious alterations. However, those localization maps work only as trace enhancers and do not provide any solid proof of forgery. The result needs to be analyzed with care and interpreted by experts. We attempt here to fill in this gap by producing an automatic method using the tampering traces left in the image and taking an automatic decision about forgeries and their precise

¹<https://fotoforensics.com>, <https://29a.ch/photo-forensics>, <https://www.getghiro.org>, <http://reveal-niklabb.it>, gr



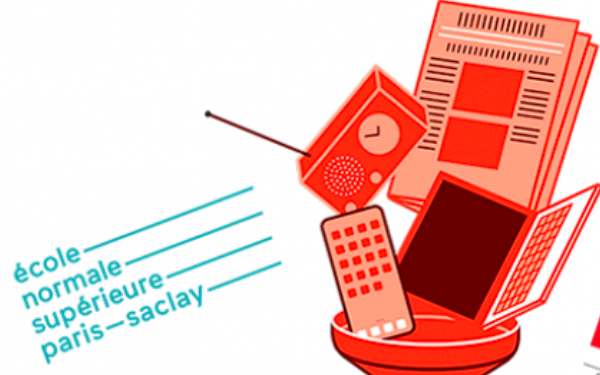












Diplôme éducation aux Médias et à l'Information























From zero to research, projects, teaching, popular science



This CVPR Workshop paper is the Open Access version, provided by the Computer Vision Foundation.
Except for this watermark, it is identical to the accepted version;
the final published version of the proceedings is available on IEEE Xplore.

JPEG Grid Detection based on the Number of DCT Zeros and its Application to Automatic and Localized Forgery Detection

T. Nikoukhah J. Anger T. Ehret M. Colom J.M. Morel R. Grompone von Gioi

CMLA, CNRS, ENS Paris-Saclay, Université Paris-Saclay

{nikoukhah,anger,ehret,colom,morel,grompone}@cmla.ens-cachan.fr

Abstract

This work proposes a novel method for detecting JPEG compression, as well as its grid origin, based on counting the number of zeros in the DCT of 8×8 blocks. When applied locally, the same method can be used to detect grid alignment abnormalities. It therefore detects local image forgeries such as copy-move. The algorithm includes a statistical validation step which gives theoretical guarantees on the number of false alarms and provides secure guarantees for tampering detection. The performance of the proposed method is illustrated with both quantitative and visual results from well-known image databases and comparisons with state of the art methods.

1. Introduction

Image tampering is currently used massively on the web and continuously feeds fake news [12]. This issue has become important since digital image manipulation tools are available to the general public. Some social networks even allow to edit images and videos directly online. Since these platforms (Facebook, Instagram, Snapchat, etc.) delete all metadata for confidentiality reasons, there is a crucial need for journalists and mass-media producers to have access to tools for detecting forgeries from the image itself. Several such tools are readily available online, *Fotoforensics*, *Forensically*, *Ghiro* and *Reveal*¹ for instance. These tools provide a number of “tampering localization maps” [26] in the form of so-called image *heat maps* revealing suspicious alterations. However, those localization maps work only as trace enhancers and do not provide any solid proof of forgery. The result needs to be analyzed with care and interpreted by experts. We attempt here to fill in this gap by producing an automatic method using the tampering traces left in the image and taking an automatic decision about forgeries and their precise

location. Indeed, even in absence of image metadata, much information about the history of the image is still present in the image itself. Many processes undergone by an image leave invisible but detectable traces all over the image. Following [2, 3, 10, 11, 12, 15, 20, 29], we address one of the most common processes, namely the JPEG compression. This compression leaves traces in the form of 8×8 pixels blocking artifacts that produce a grid over the image.

Here we propose an automatic and statistically founded method for detecting the grid division of the image. The proposed method, hereafter referred to as ZERO, performs a global grid detection and then applies it more locally to detect forgeries. Indeed, image splicing generally breaks locally the original grid alignment. A locally detected grid therefore may contradict the global grid and become a reliable cue that a forgery took place. We evaluate ZERO against several state of the art algorithms on publicly available datasets. The detection does not require a human expert’s decision as shown in Figure 1, and is associated with theoretical guarantees.

¹<https://fotoforensics.com>, <https://29a.ch/photo-forensics>,
<https://www.getghiro.org>, <http://reveal-niklabb.it>,gr

Figure 1: Result of the proposed method, from top left to bottom right: original image, forged image (input of the method), detected forgeries, ground-truth. The fisherman and the fishing rod have been removed. The resulting detected mask does not require visual interpretation.

126

From zero to research, projects, teaching, popular science



This CVPR Workshop paper is the Open Access version, provided by the Computer Vision Foundation.
Except for this watermark, it is identical to the accepted version;
the final published version of the proceedings is available on IEEE Xplore.

JPEG Grid Detection based on the Number of DCT Zeros and its Application to Automatic and Localized Forgery Detection

T. Nikoukhah J. Anger T. Ehret M. Colom J.M. Morel R. Grompone von Gioi
CMLA, CNRS, ENS Paris-Saclay, Université Paris-Saclay
{nikoukhah, anger, ehret, colom, morel, grompone}@cmla.ens-cachan.fr

Abstract

This work proposes a novel method for detecting JPEG compression, as well as its grid origin, based on counting the number of zeros in the DCT of 8×8 blocks. When applied locally, the same method can be used to detect grid alignment abnormalities. It therefore detects local image forgeries such as copy-move. The algorithm includes a statistical validation step which gives theoretical guarantees on the number of false alarms and provides secure guarantees for tampering detection. The performance of the proposed method is illustrated with both quantitative and visual results from well-known image databases and comparisons with state of the art methods.

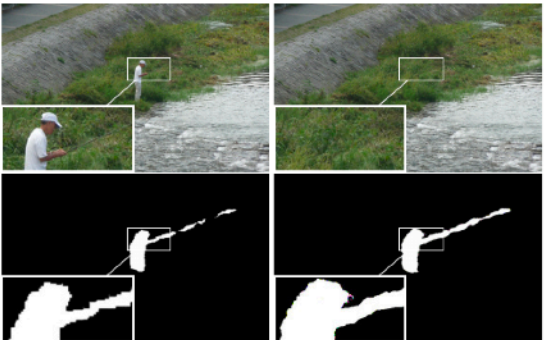


Figure 1: Result of the proposed method, from top left to bottom right: original image, forged image (input of the method), detected forgeries, ground-truth. The fisherman and the fishing rod have been removed. The resulting detected mask does not require visual interpretation.

1. Introduction

Image tampering is currently used massively on the web and continuously feeds fake news [12]. This issue has become important since digital image manipulation tools are available to the general public. Some social networks even allow to edit images and videos directly online. Since these platforms (Facebook, Instagram, Snapchat, etc.) delete all metadata for confidentiality reasons, there is a crucial need for journalists and mass-media producers to have access to tools for detecting forgeries from the image itself. Several such tools are readily available online, *Fotoforensics*, *Forensically*, *Ghiro* and *Reveal*¹ for instance. These tools provide a number of “tampering localization maps” [26] in the form of so-called image *heat maps* revealing suspicious alterations. However, those localization maps work only as trace enhancers and do not provide any solid proof of forgery. The result needs to be analyzed with care and interpreted by experts. We attempt here to fill in this gap by producing an automatic method using the tampering traces left in the image and taking an automatic decision about forgeries and their precise

location. Indeed, even in absence of image metadata, much information about the history of the image is still present in the image itself. Many processes undergone by an image leave invisible but detectable traces all over the image. Following [2, 3, 10, 11, 12, 15, 20, 29], we address one of the most common processes, namely the JPEG compression. This compression leaves traces in the form of 8×8 pixels blocking artifacts that produce a grid over the image.

Here we propose an automatic and statistically founded method for detecting the grid division of the image. The proposed method, hereafter referred to as ZERO, performs a global grid detection and then applies it more locally to detect forgeries. Indeed, image splicing generally breaks locally the original grid alignment. A locally detected grid therefore may contradict the global grid and become a reliable cue that a forgery took place. We evaluate ZERO against several state of the art algorithms on publicly available datasets. The detection does not require a human expert’s decision as shown in Figure 1, and is associated with theoretical guarantees.

¹<https://fotoforensics.com>, <https://29a.ch/photo-forensics>,
<https://www.getghiro.org>, <http://reveal-niklabb.it/gr>

110



The secret life of JPEG images

Forgery detection using compression traces

Tina Nikoukhah

Thesis defense, November 8th 2022

<https://nikoukhah.com/tina/>

Appendix

Local JPEG Grid Detection via Blocking Artifacts (GOD)

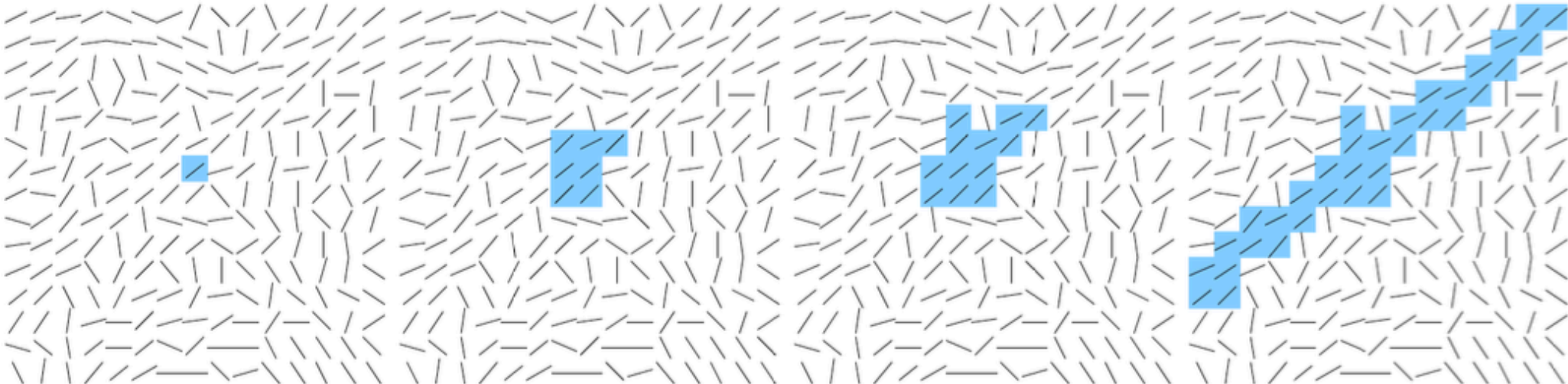
Reliable Quantization Table Estimation (Qtable)

Simple JPEG Grid Origin Detection (SimpleGOD)

Local JPEG Grid Detection via the DCT zeros (ZERO)

Local JPEG Grid Detection via the DCT zeros (ZERO)

Region growing



Non-Semantic Evaluation of Image Forensic Tools (Trace database)

Team work!



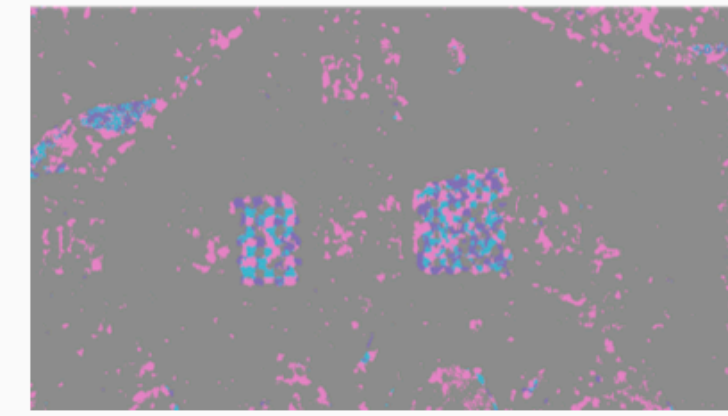
Ground Truth



ZERO ↓



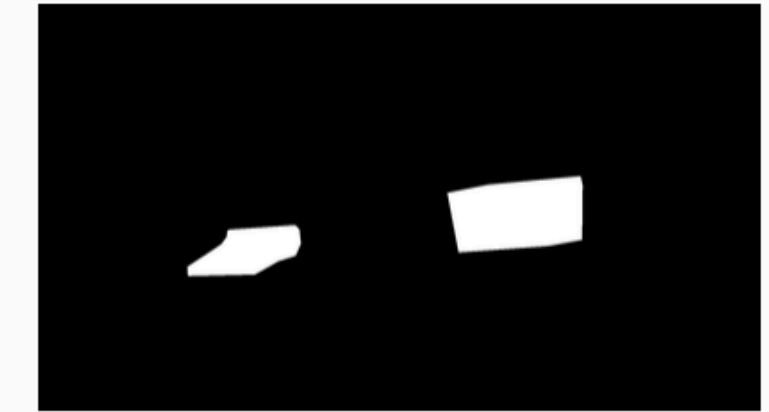
Noise ↓ sniffer



CFA ↓

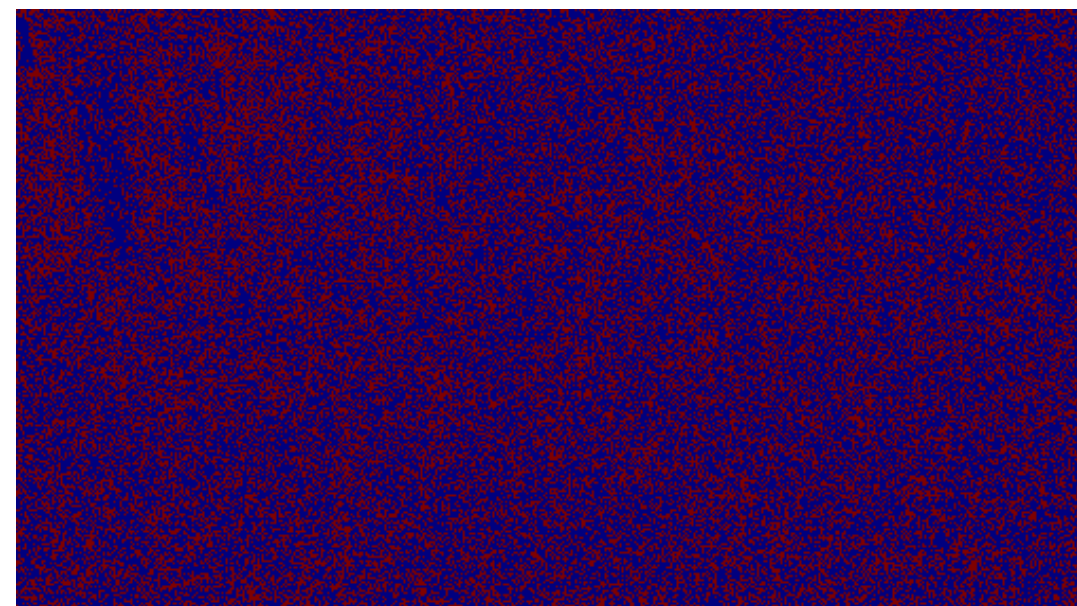


RCMFD ↓

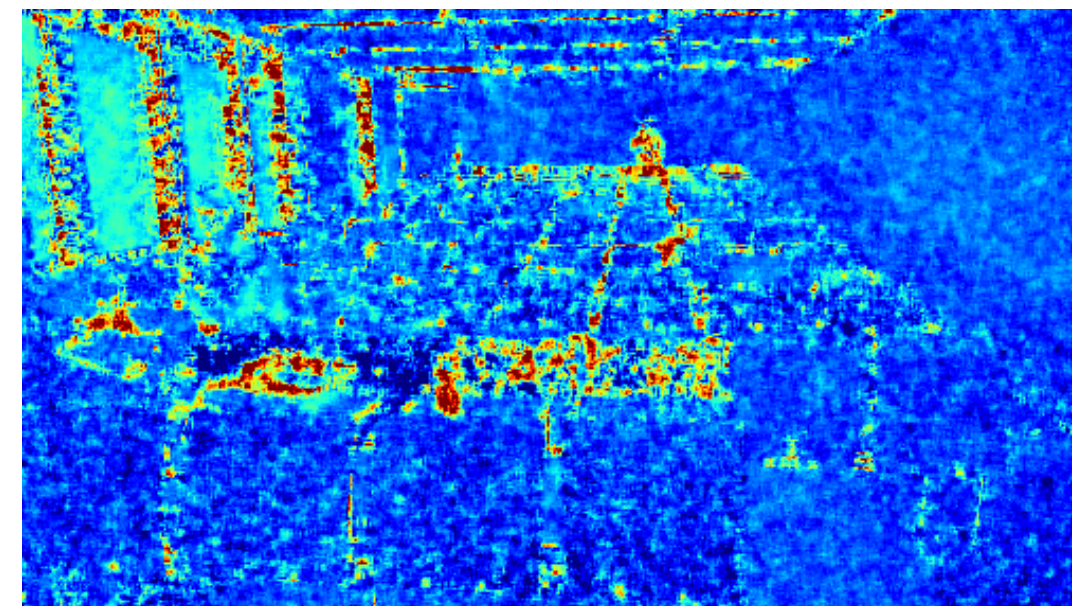


A contrario detection:

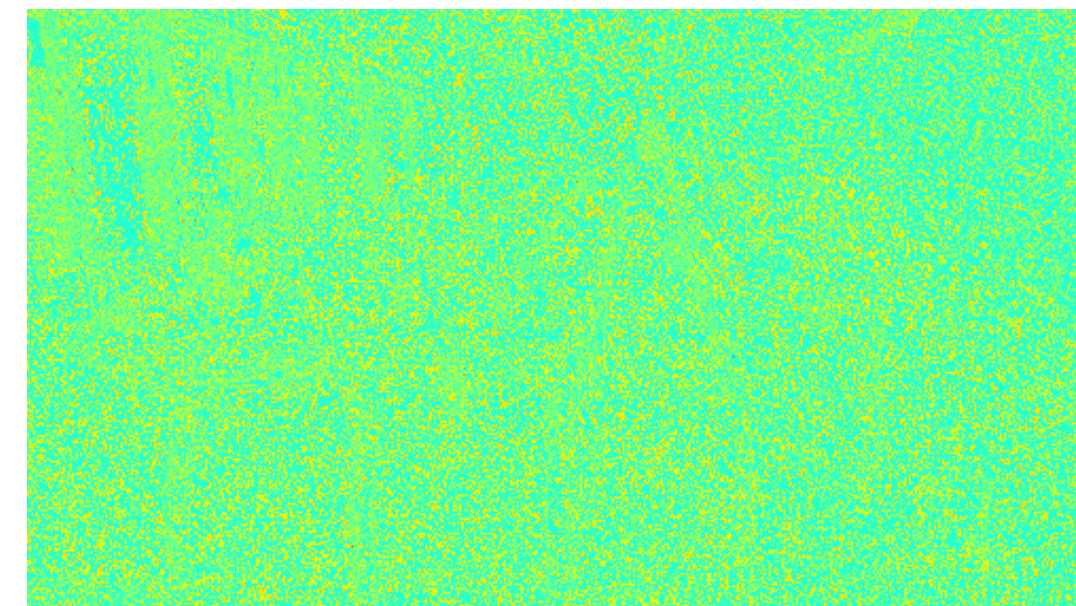
- Automatic detection (no need for expert interpretation)
- Control the rate of false positives
- Provide explainable detections: we know *why* we make a detection (vs. black-box models)



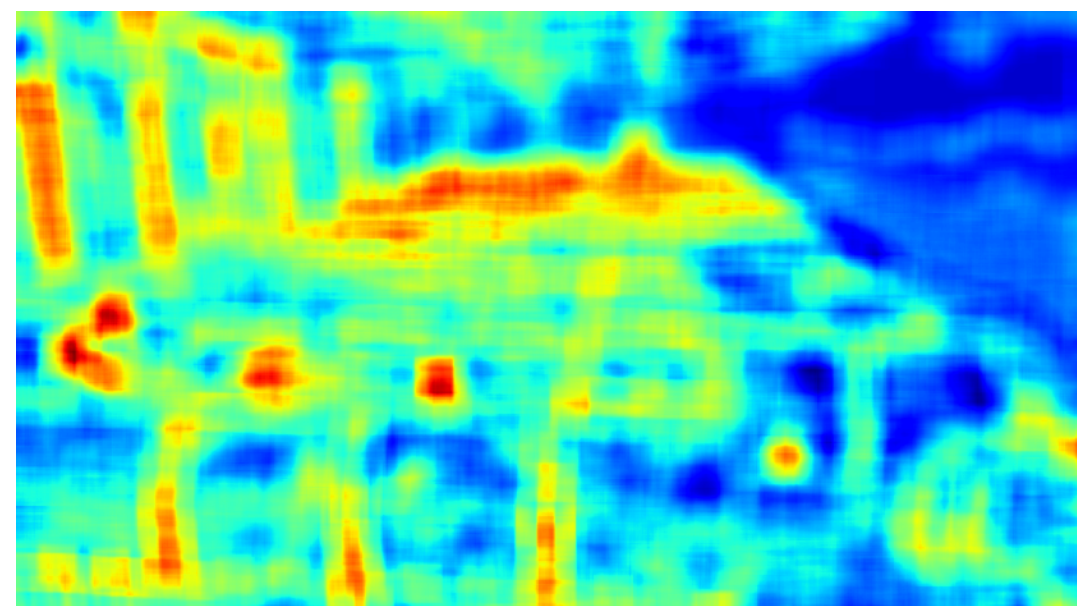
DCT



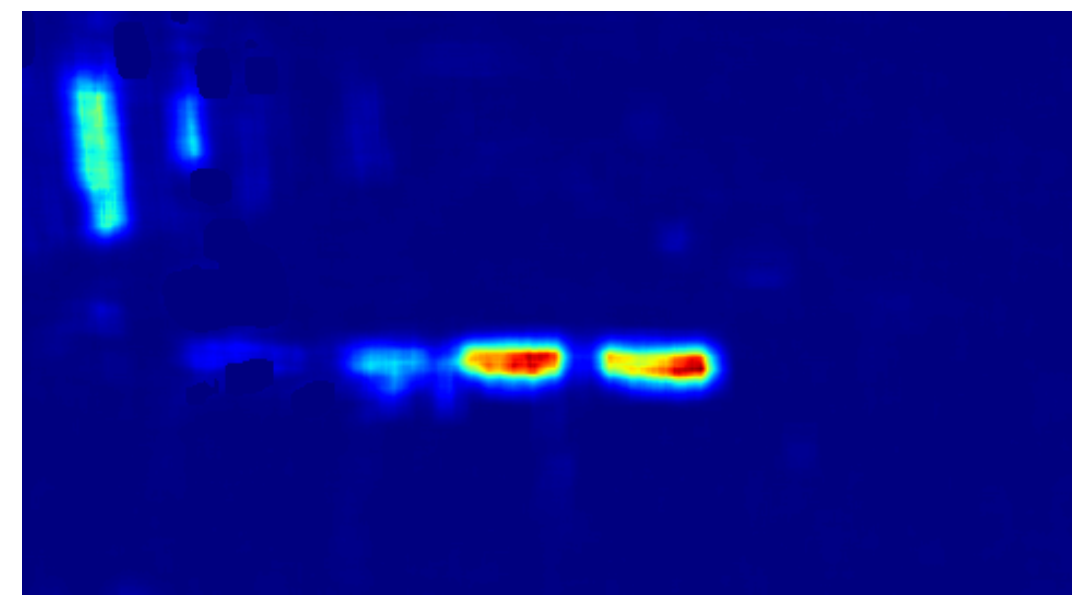
BLK



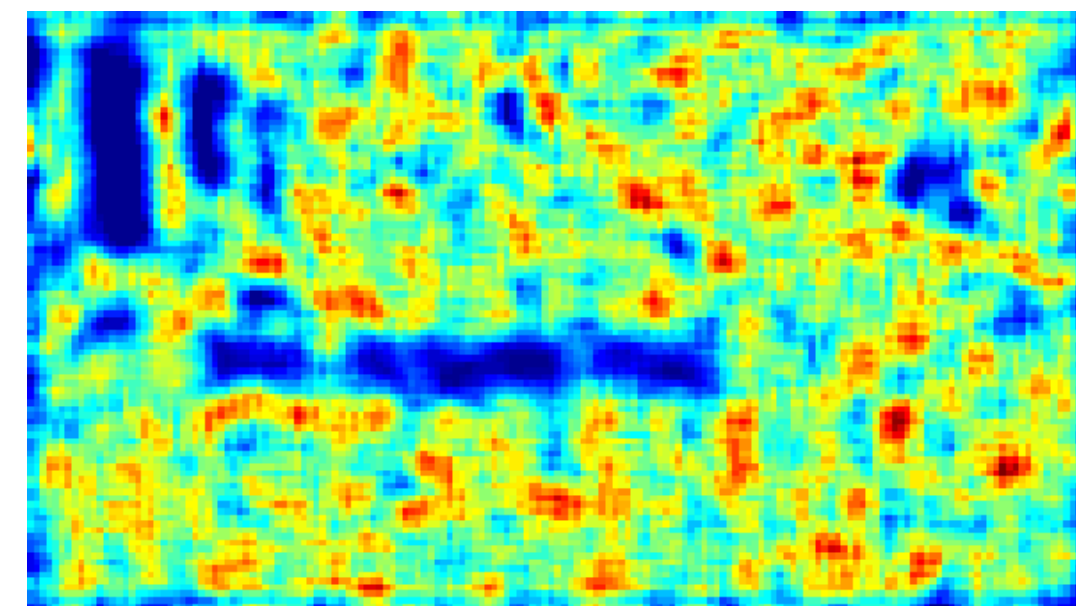
DQ



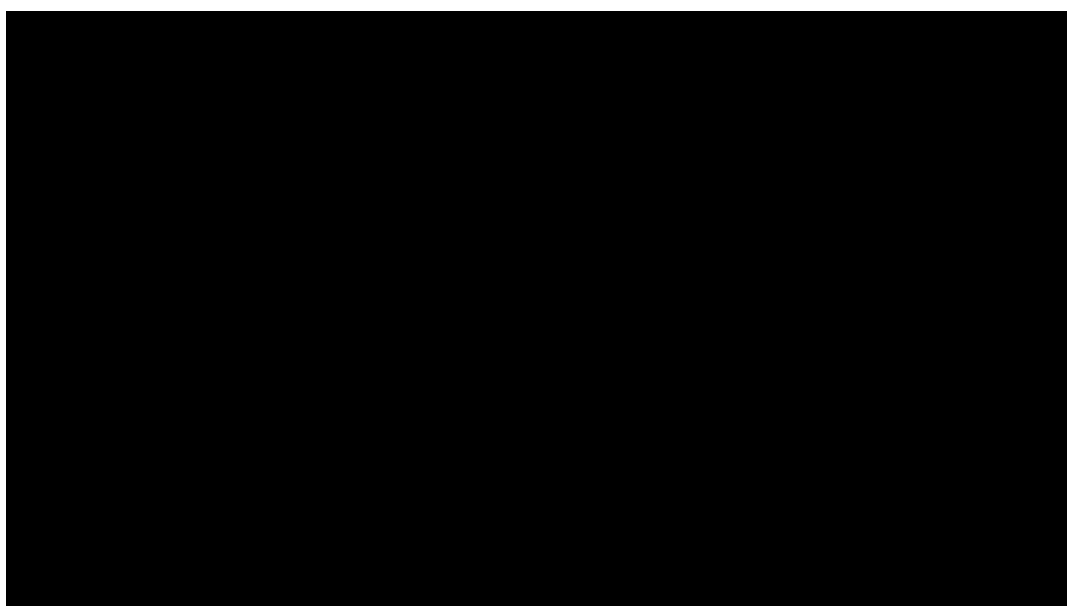
Ghost



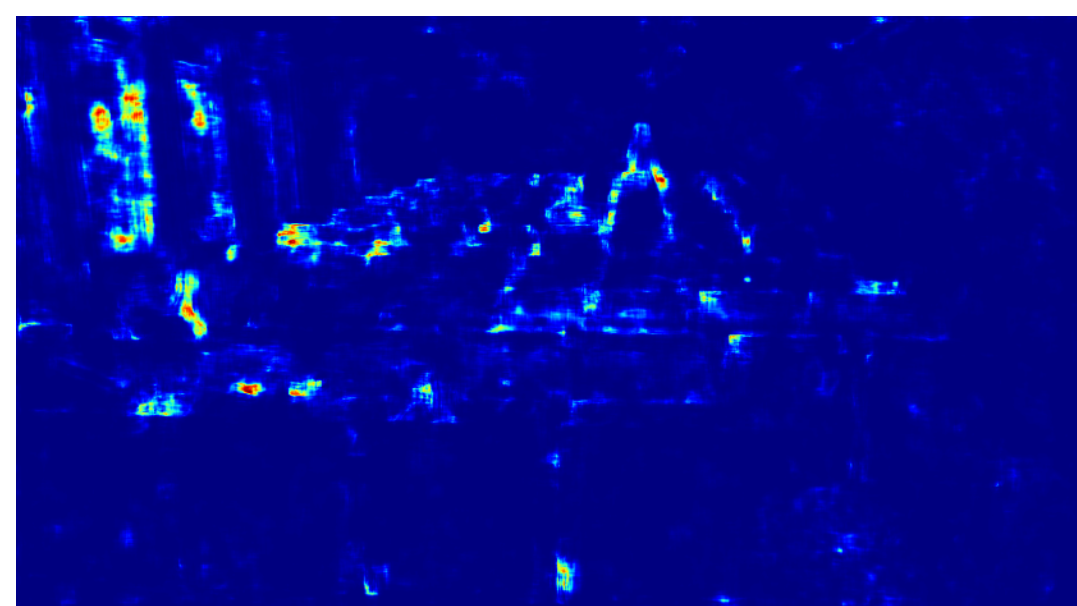
Splicebuster



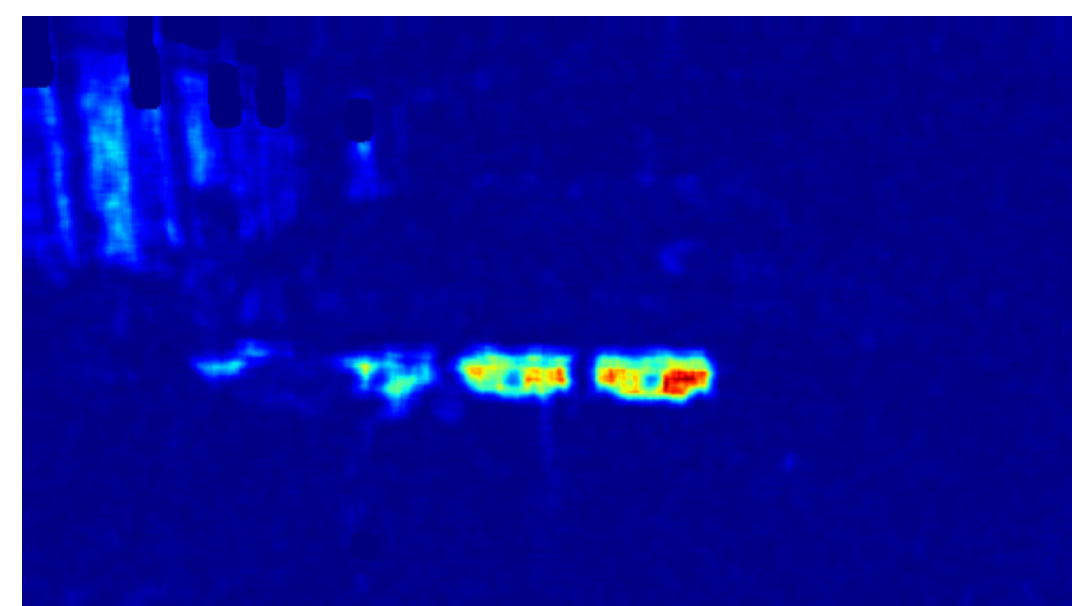
CAGI



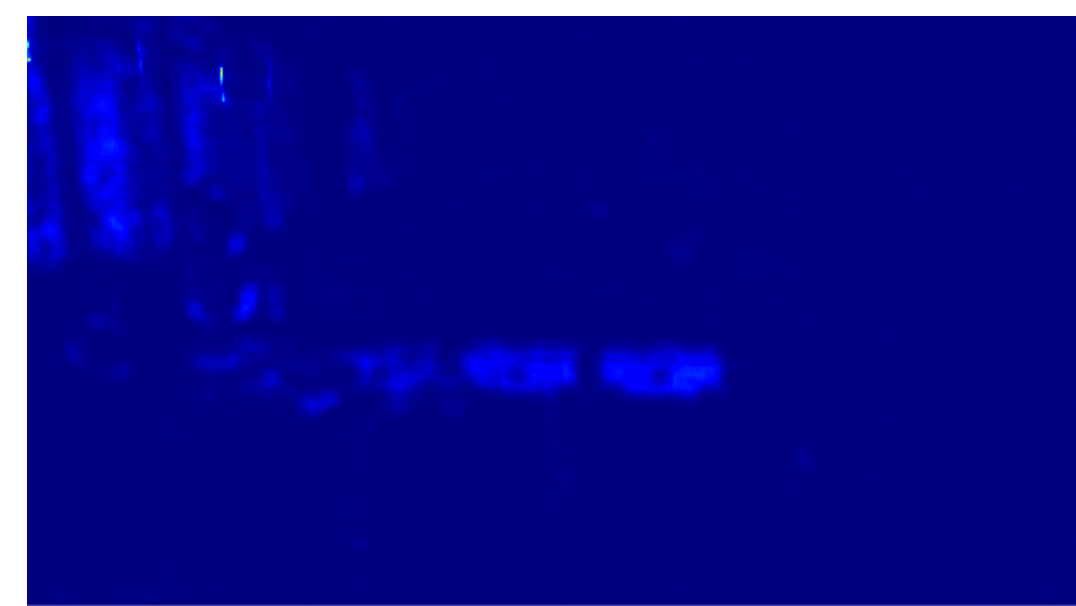
zero



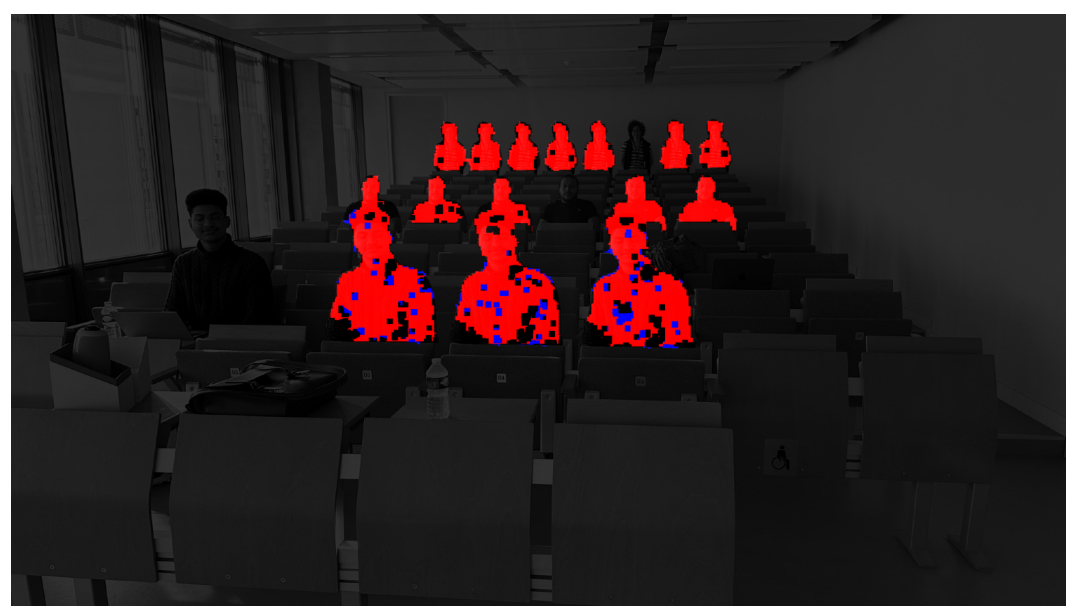
ManTraNet



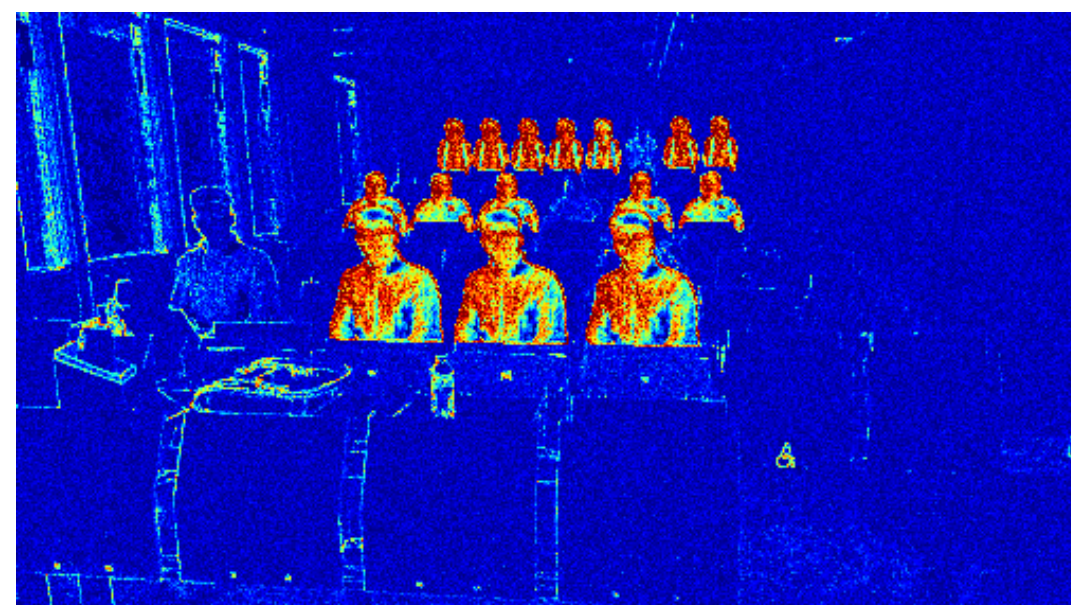
Noiseprint



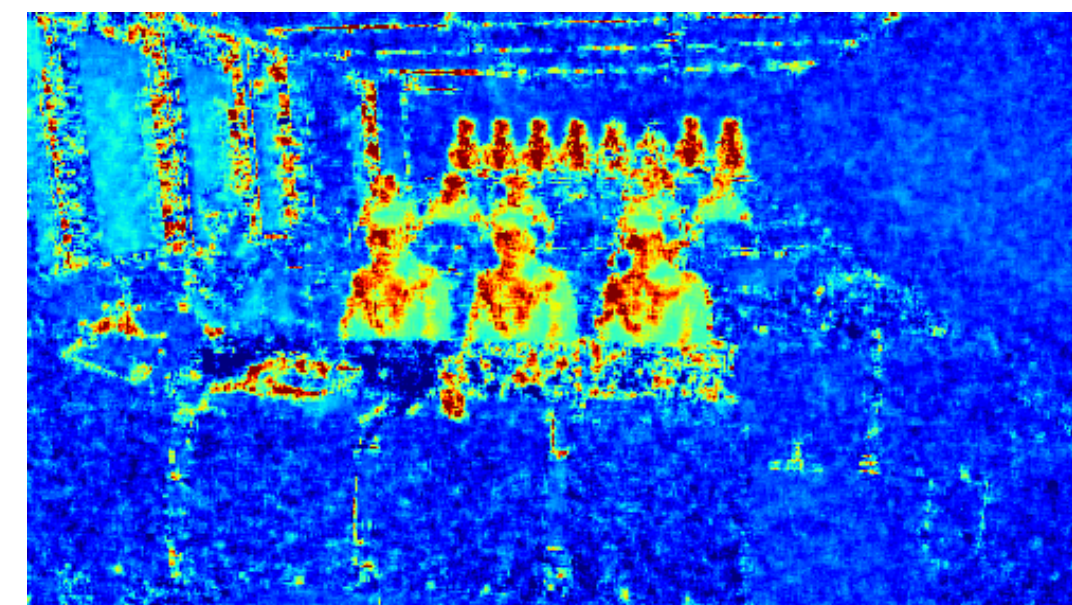
Comprint



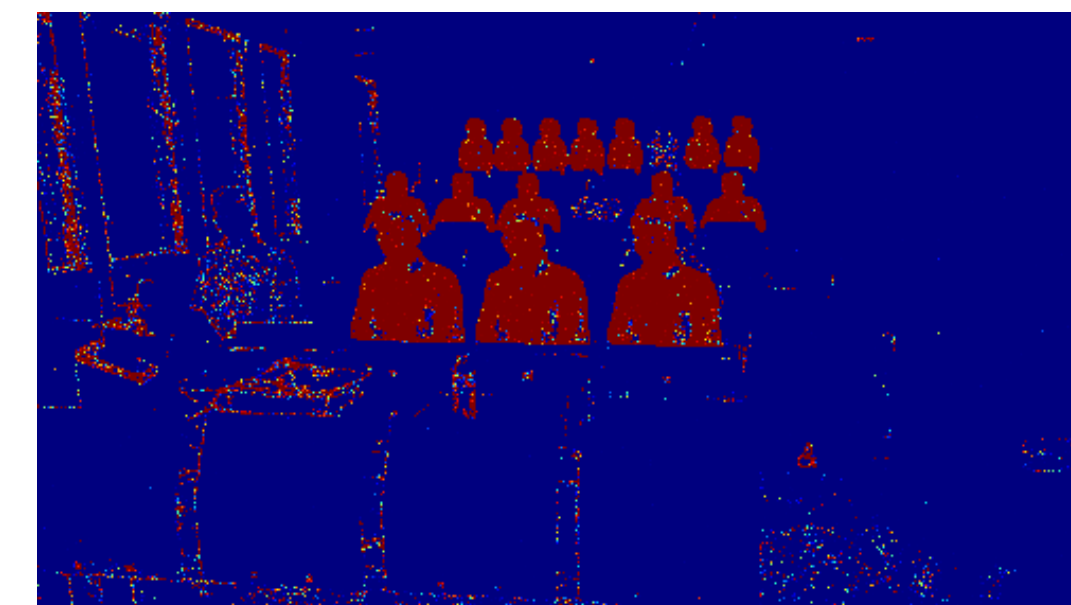
zero



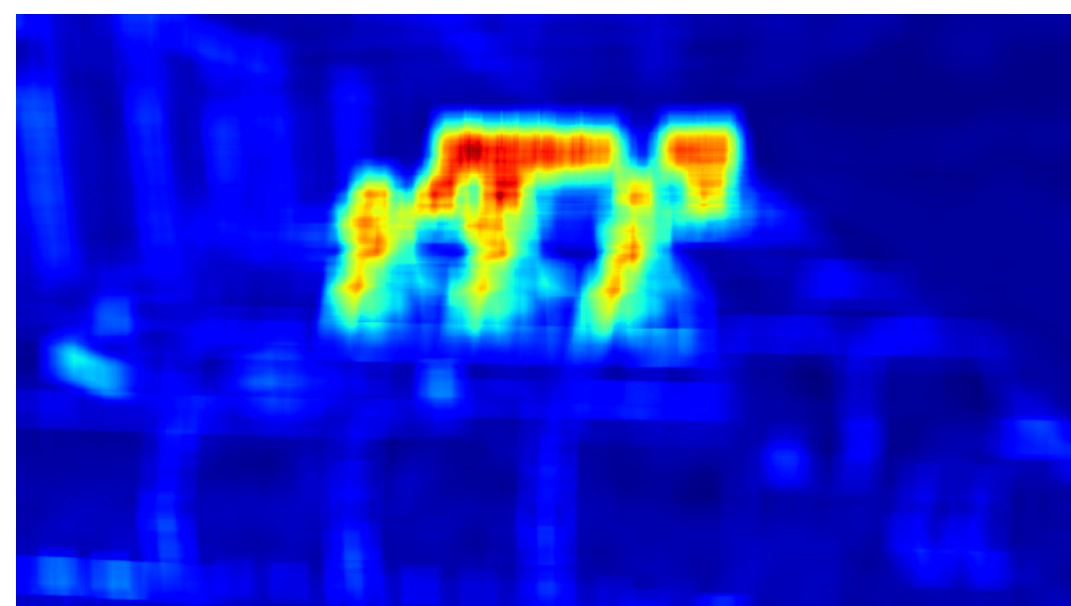
DCT



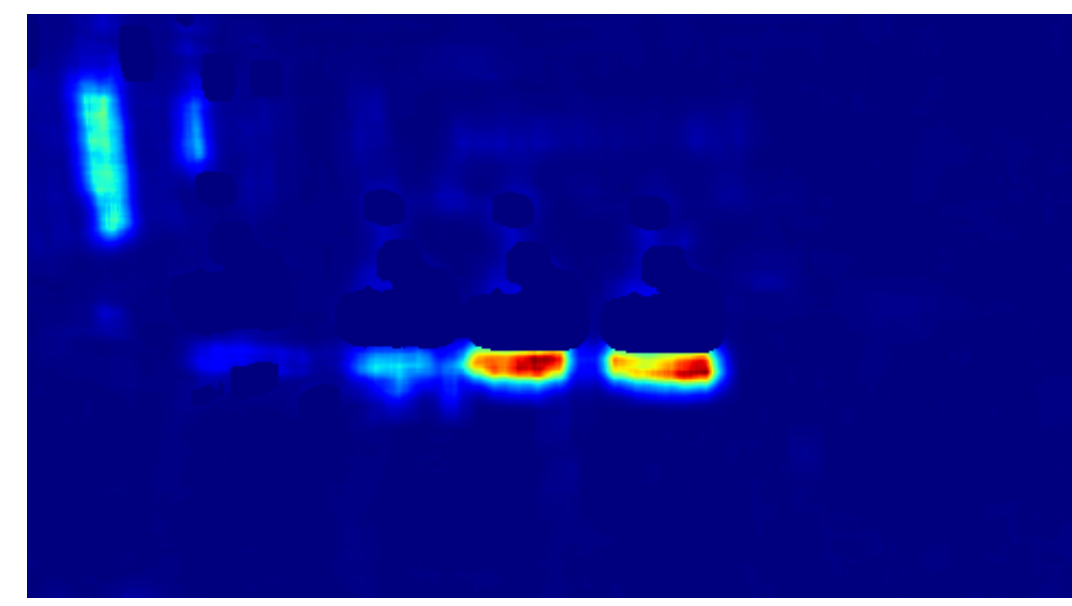
BLK



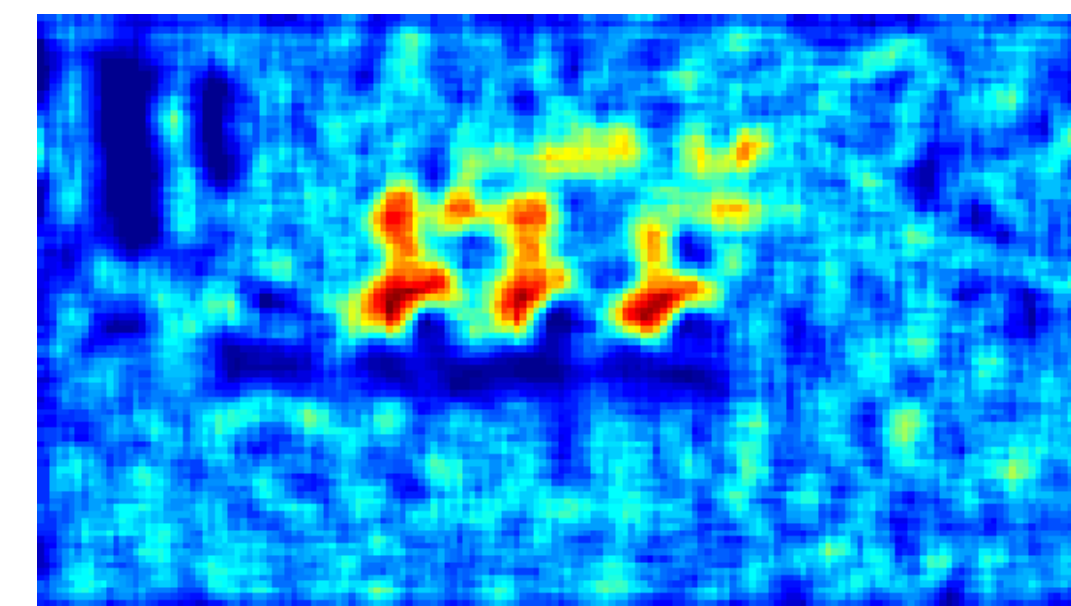
DQ



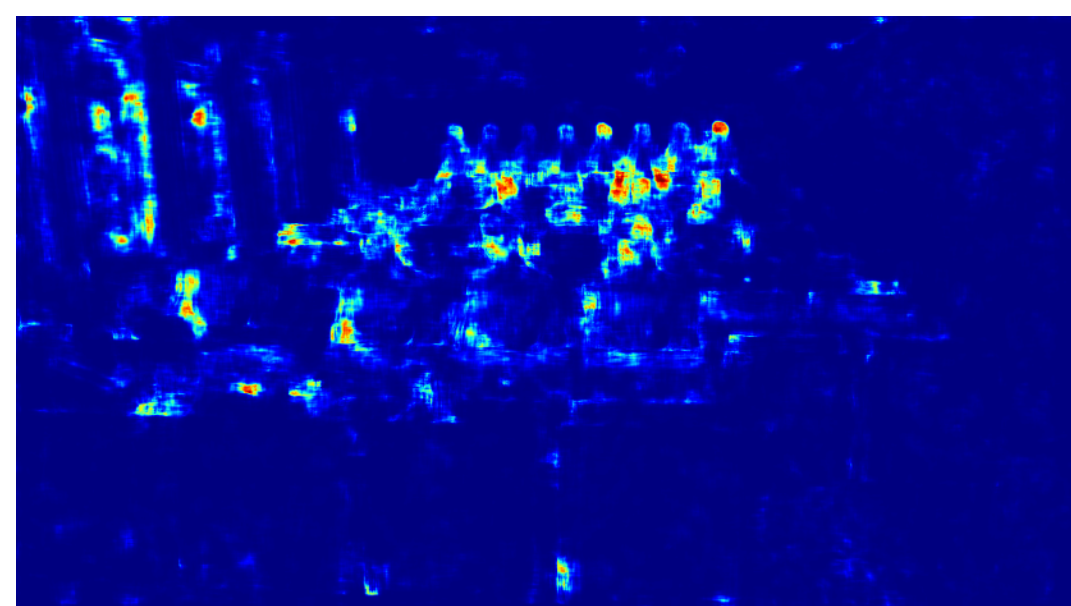
Ghost



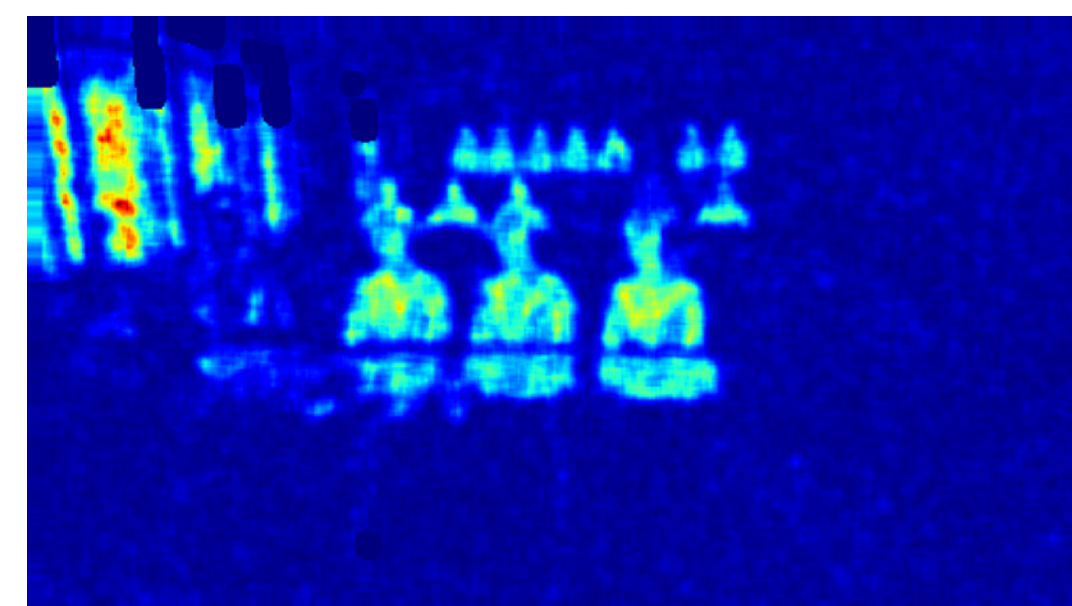
Splicebuster



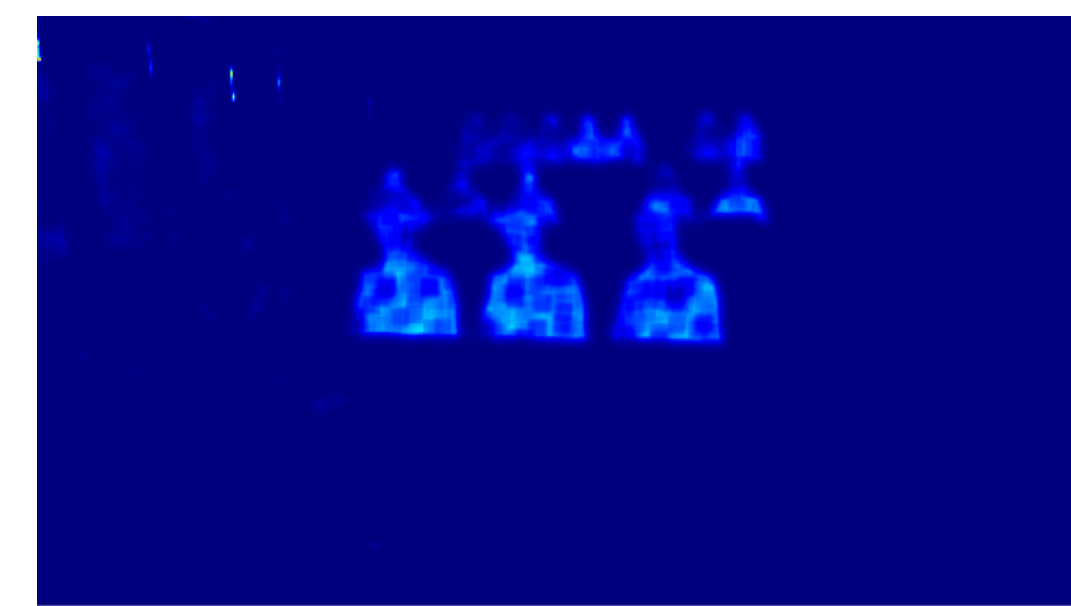
CAGI



ManTraNet



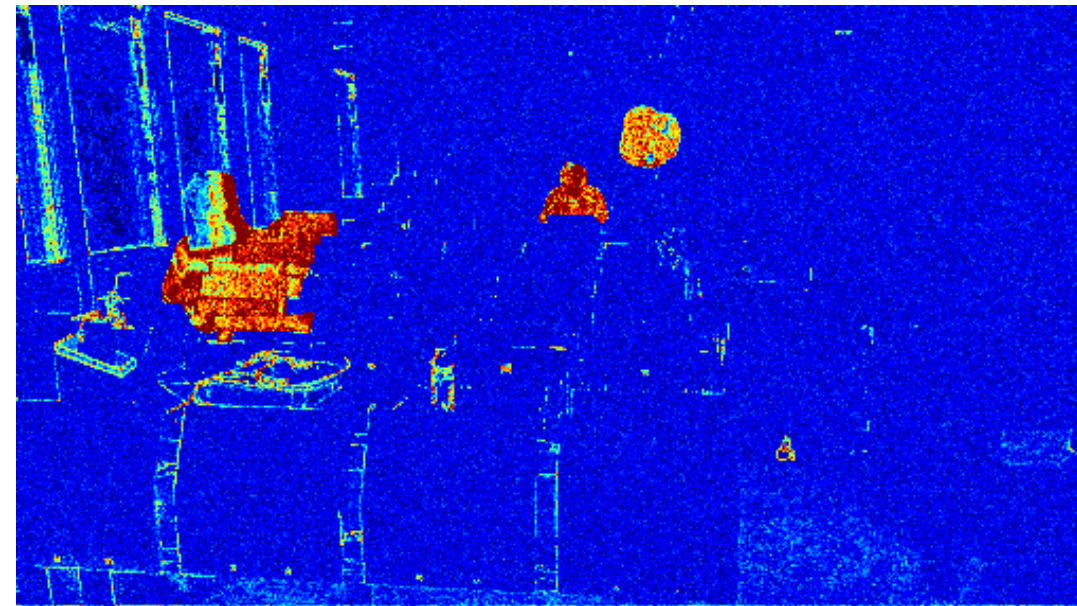
Noiseprint



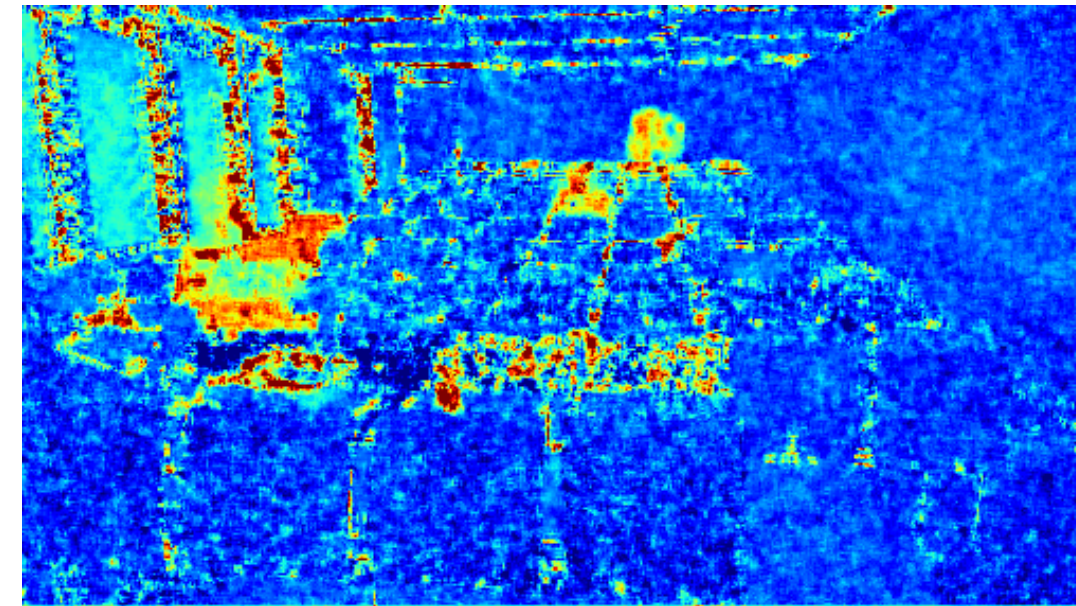
Comprint



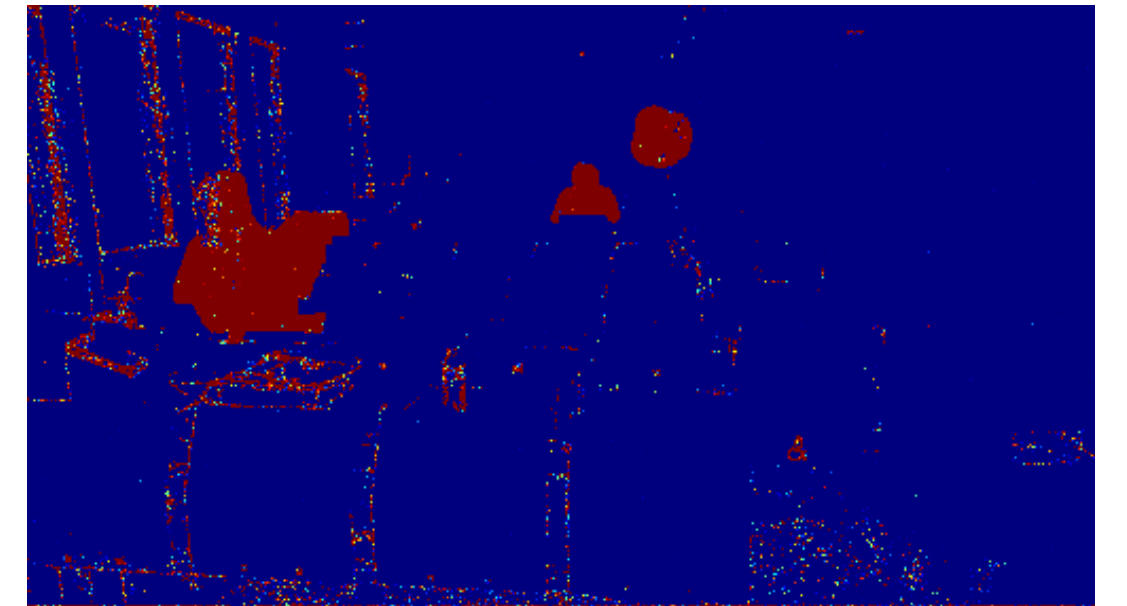
zero



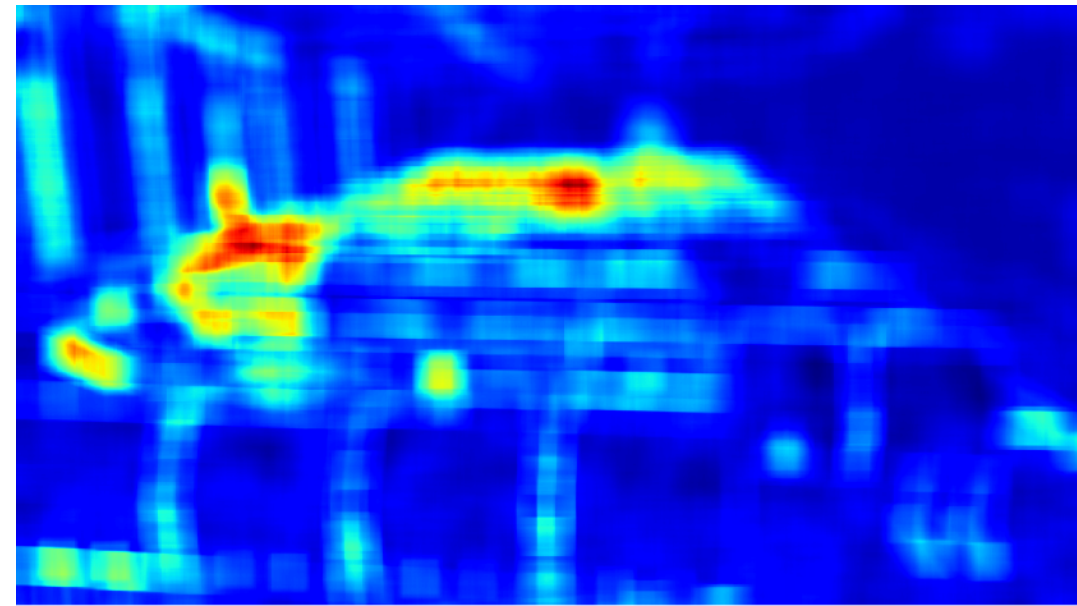
DCT



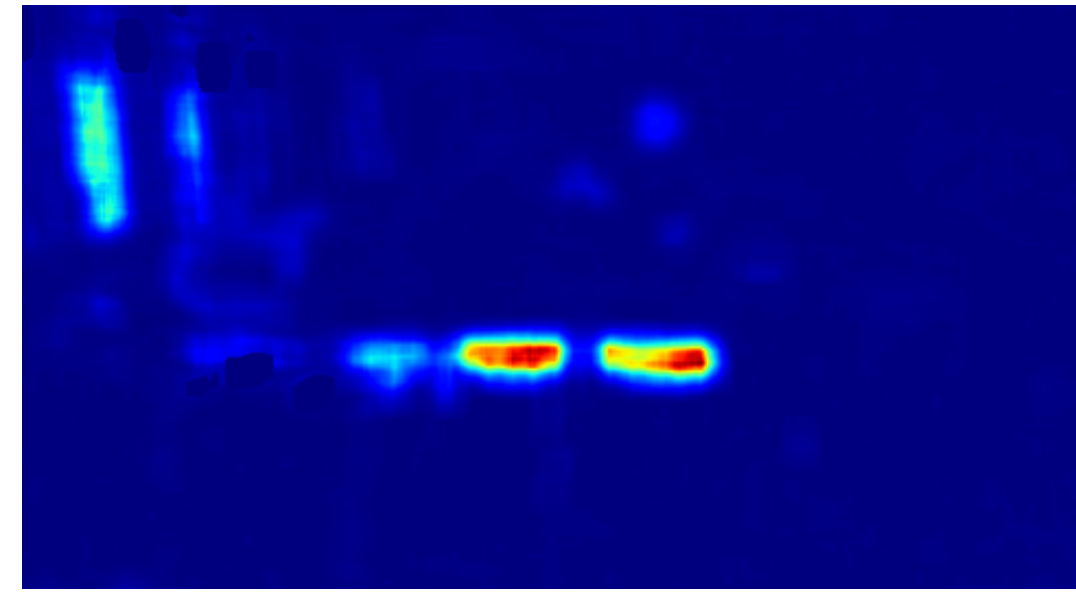
BLK



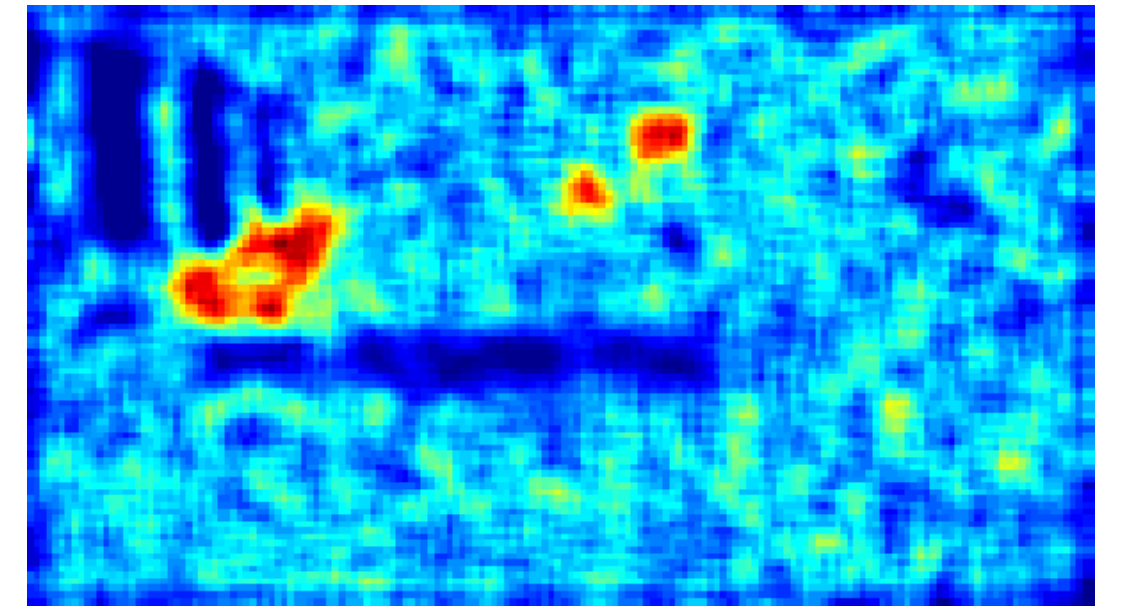
DQ



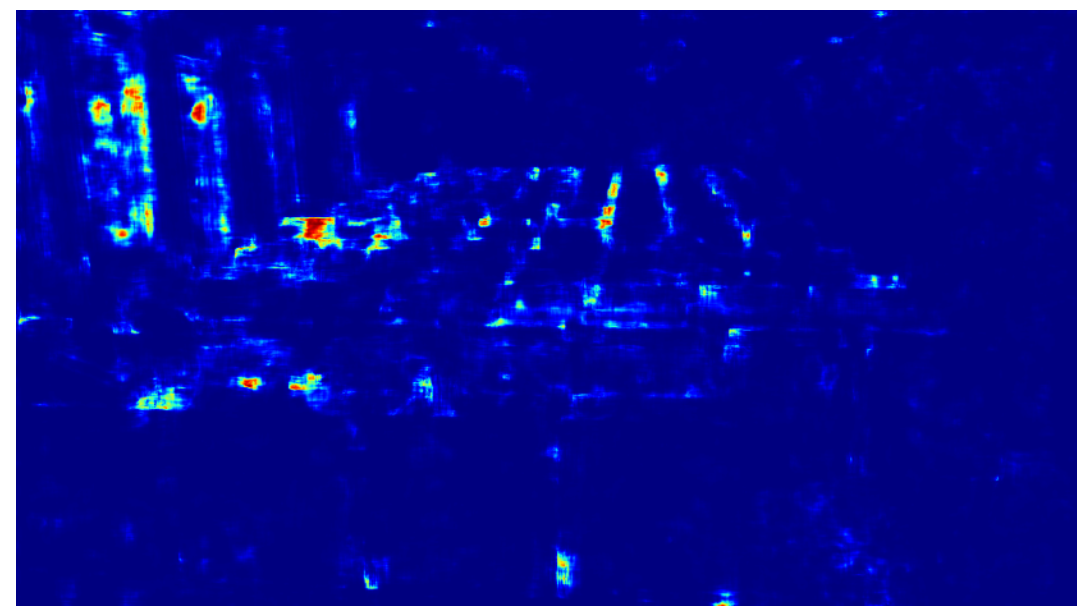
Ghost



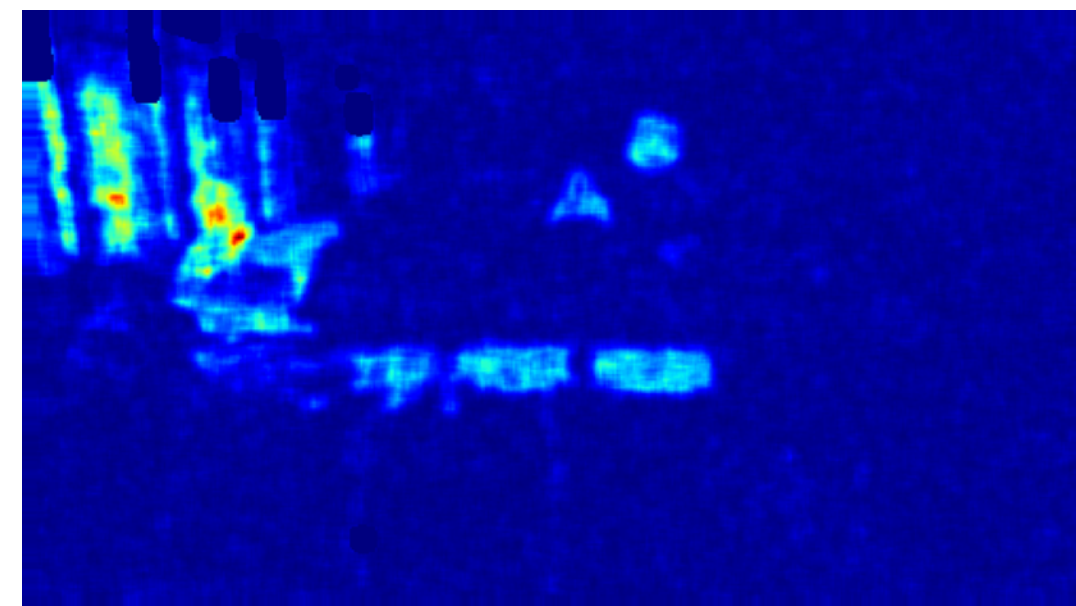
Splicebuster



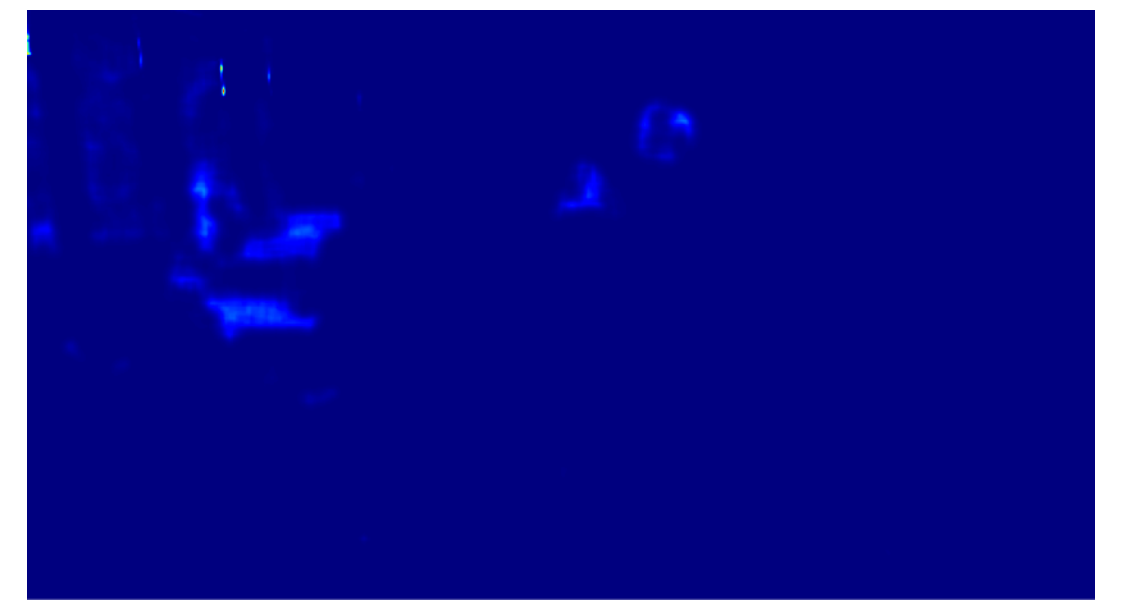
CAGI



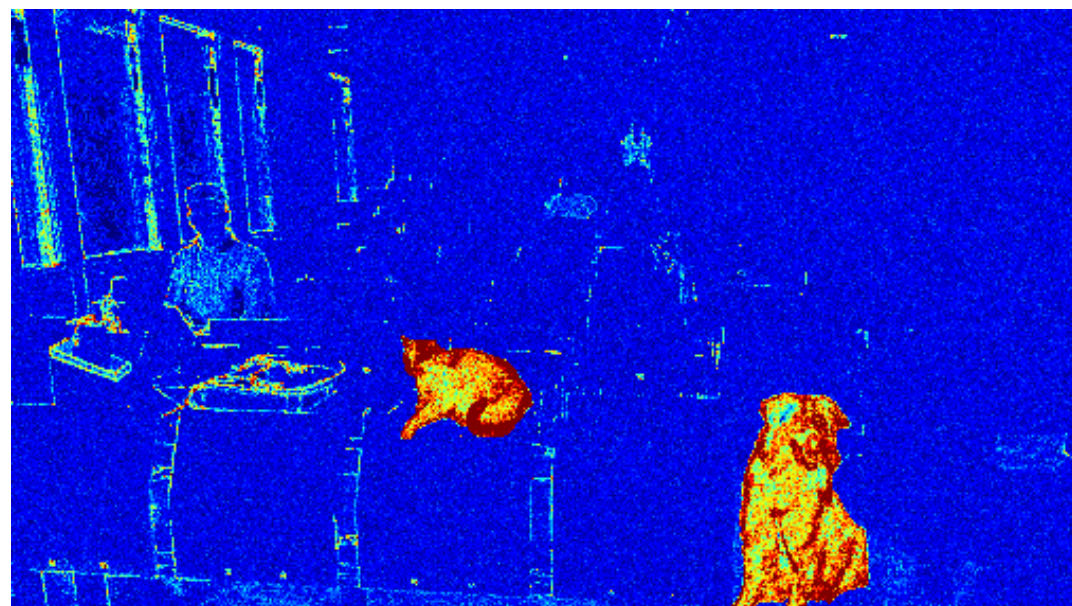
ManTraNet



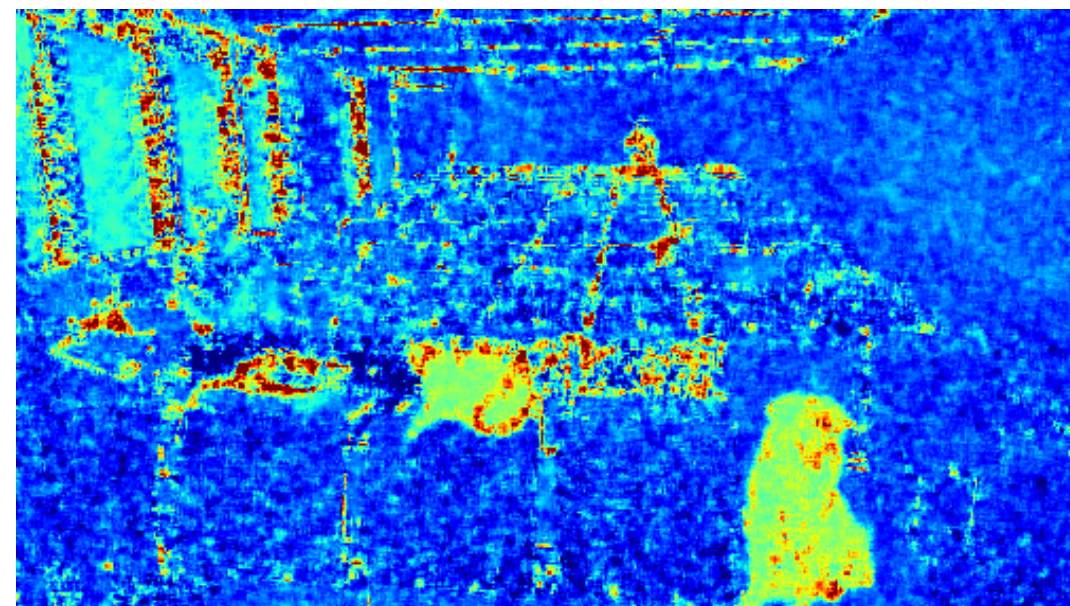
Noiseprint



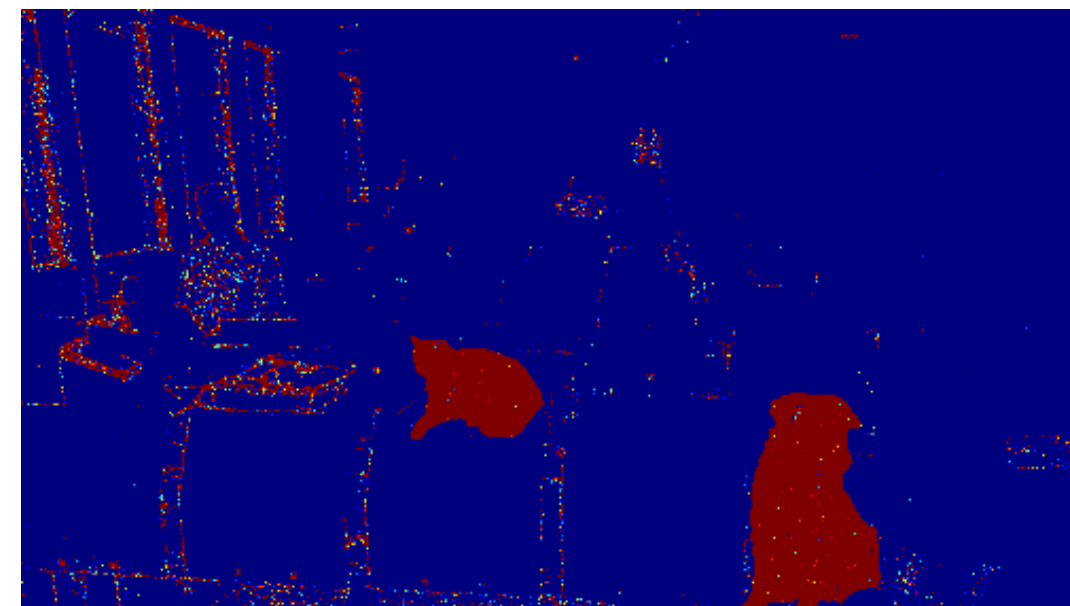
Comprint



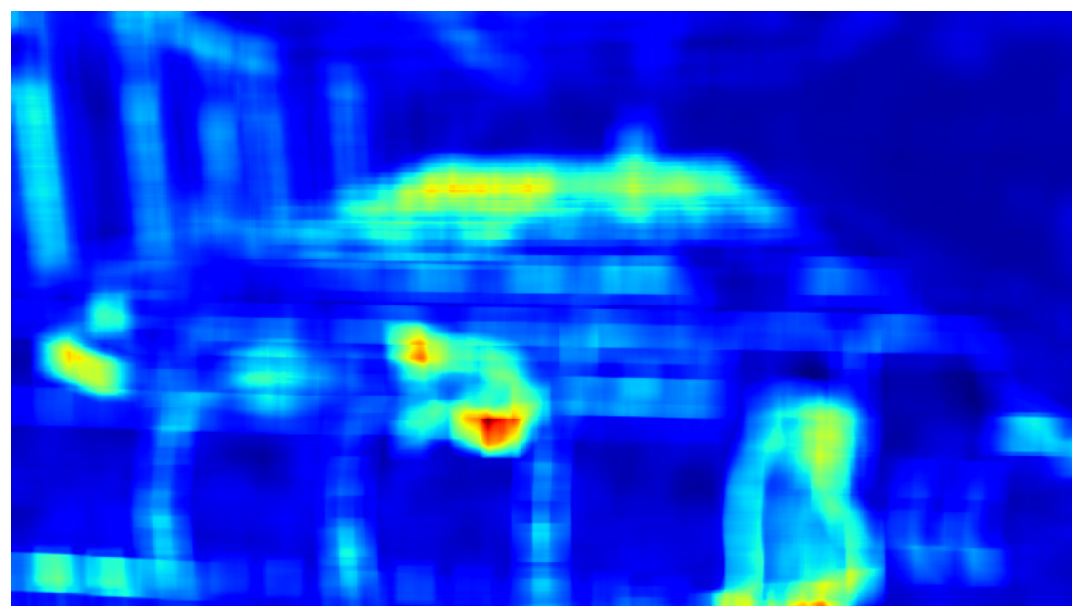
DCT



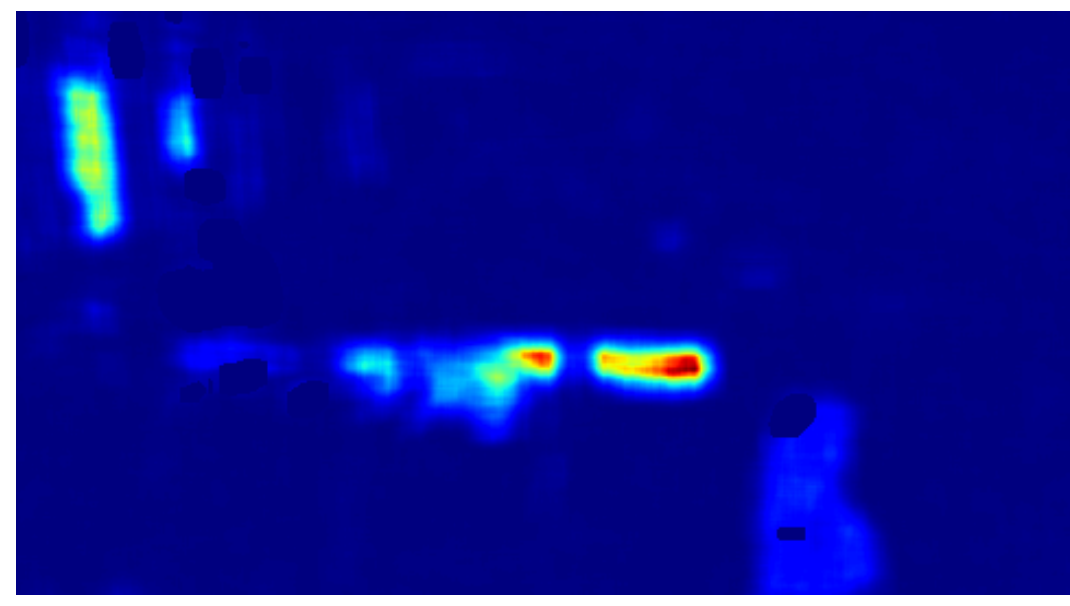
BLK



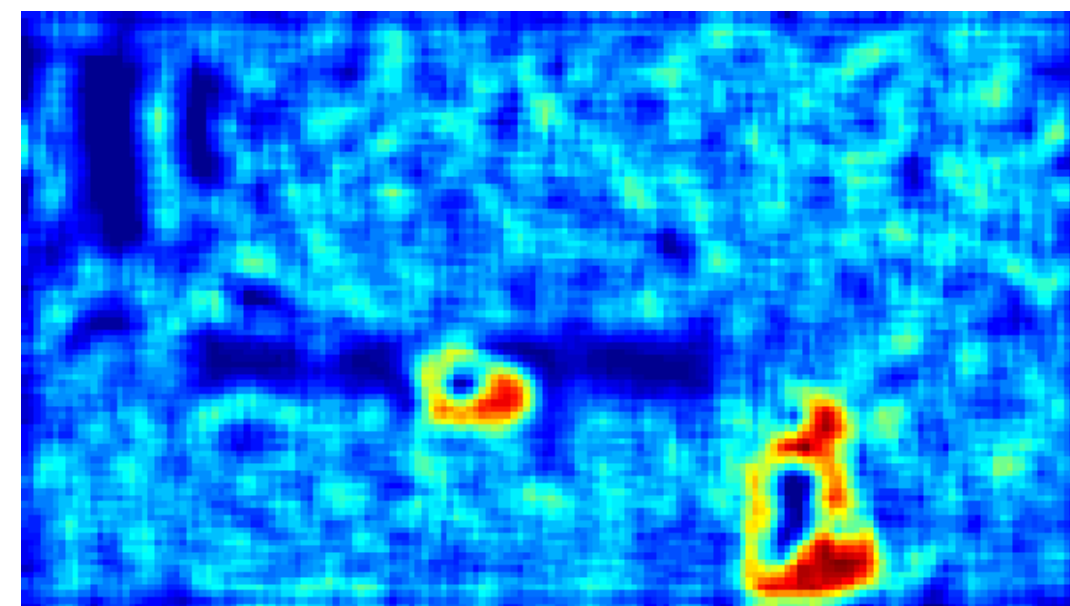
DQ



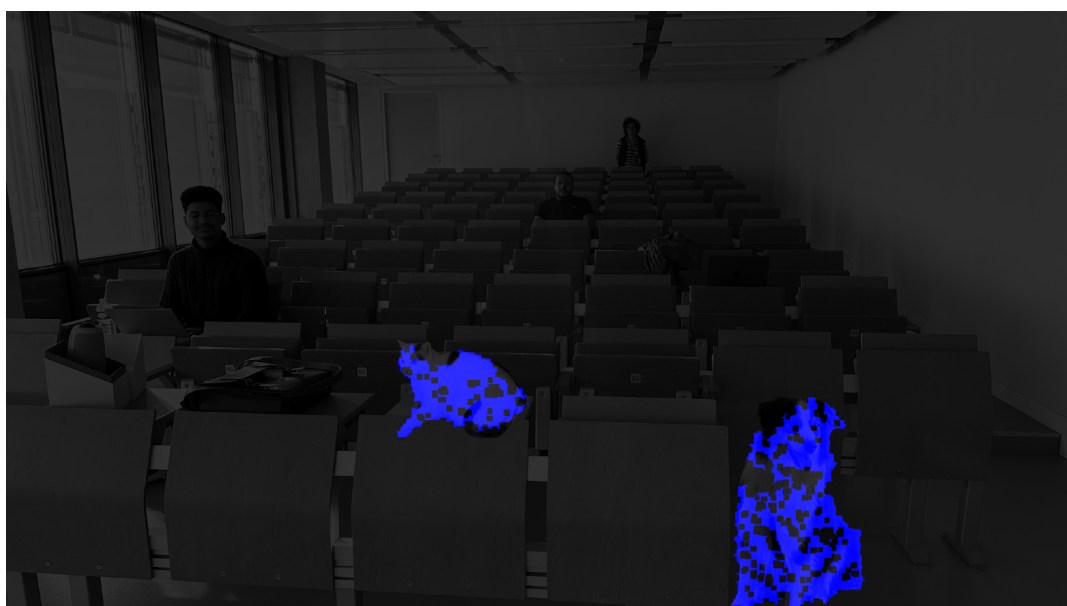
Ghost



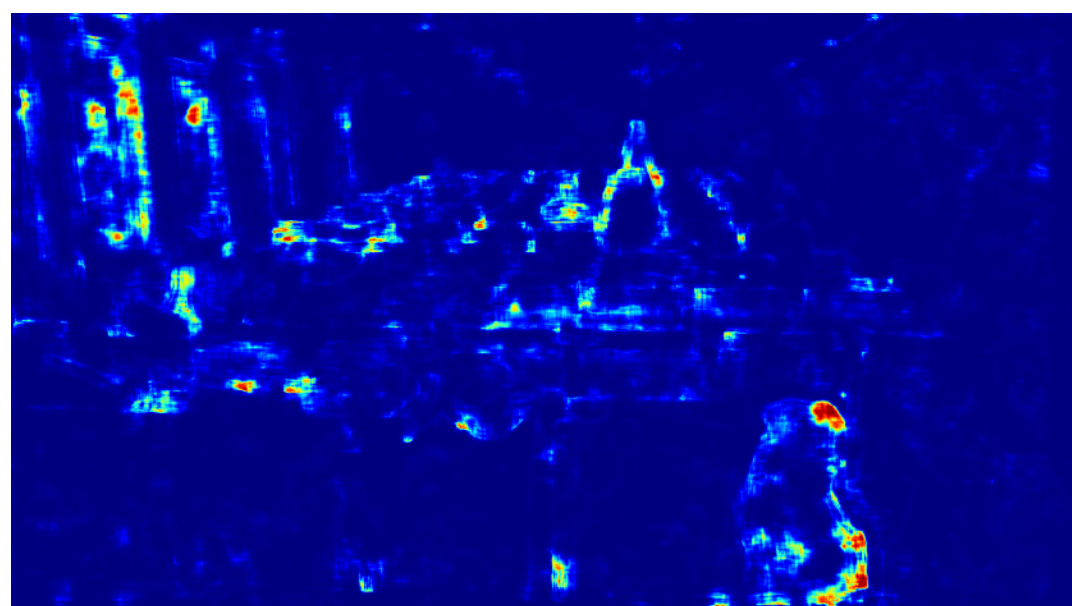
Splicebuster



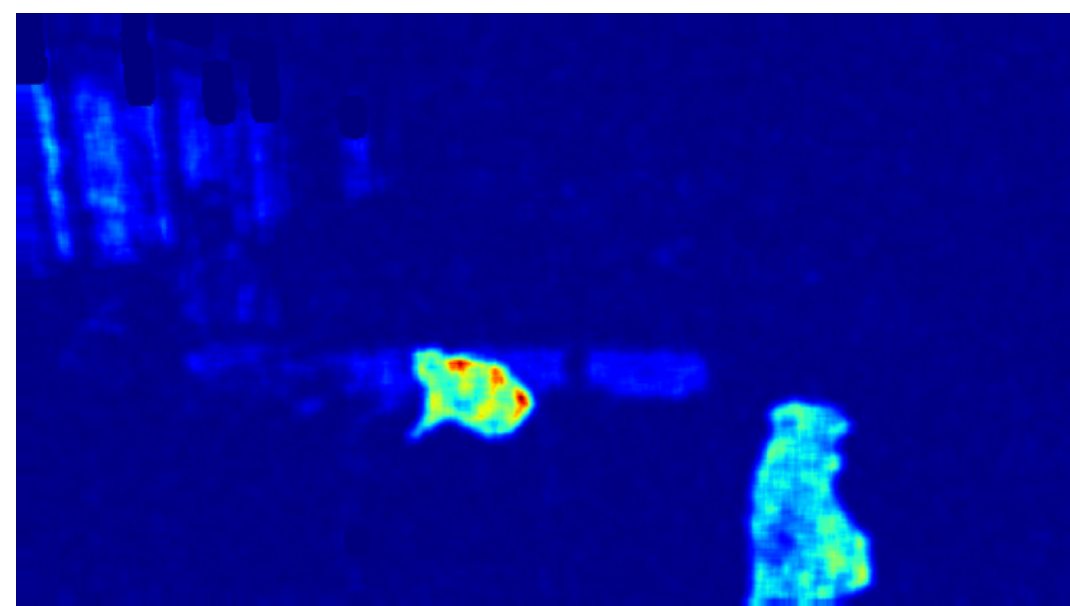
CAGI



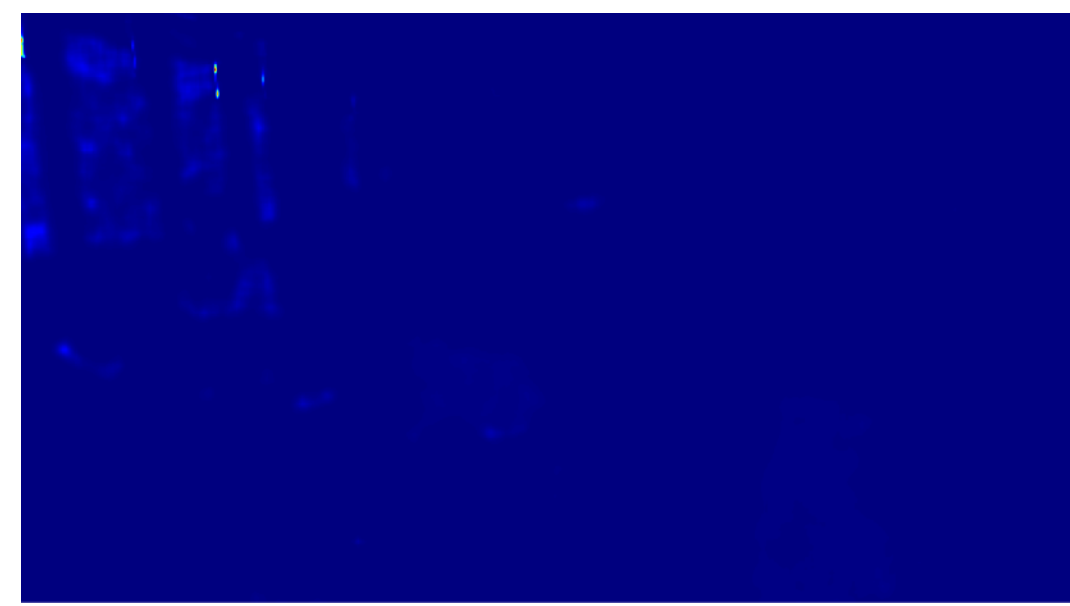
zero



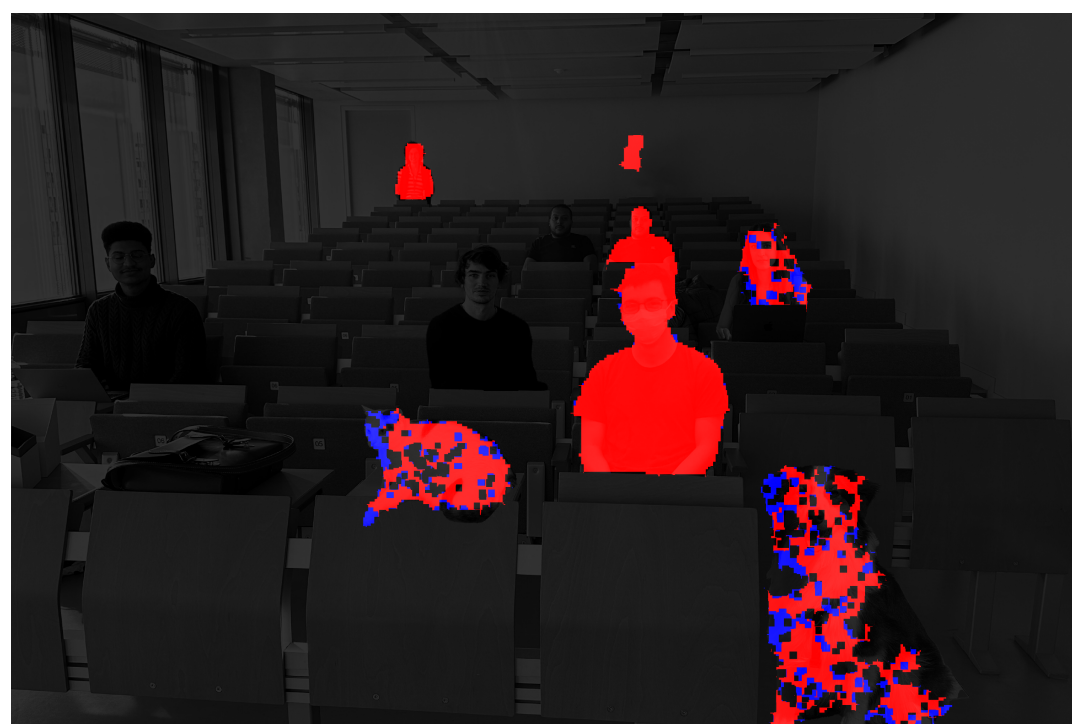
ManTraNet



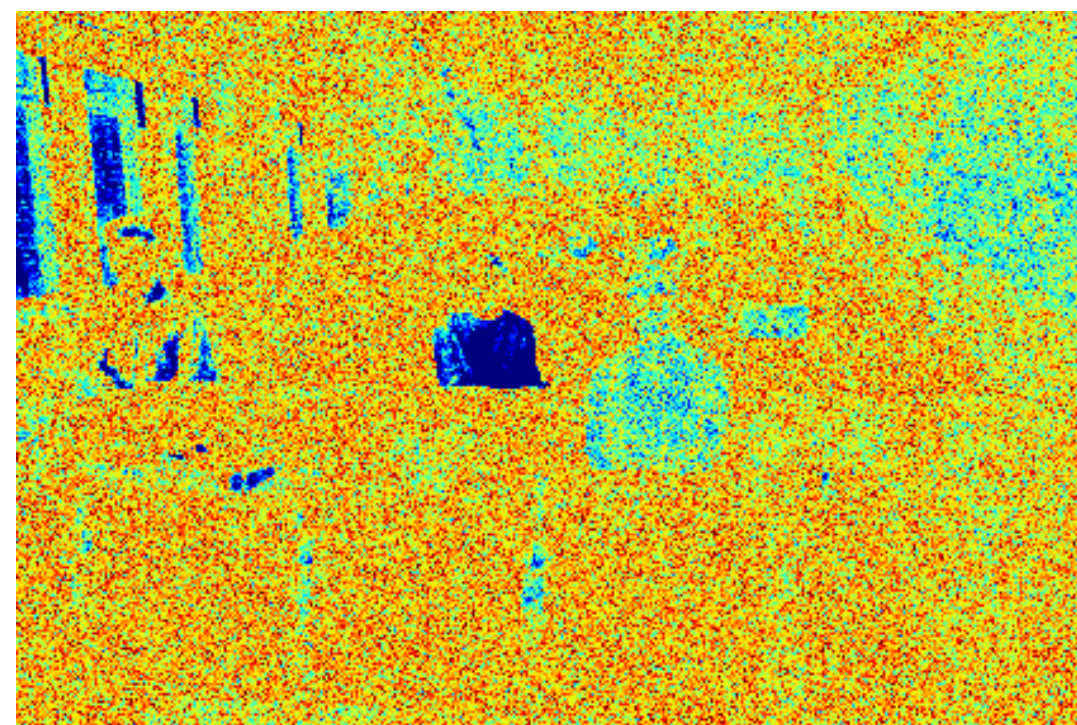
Noiseprint



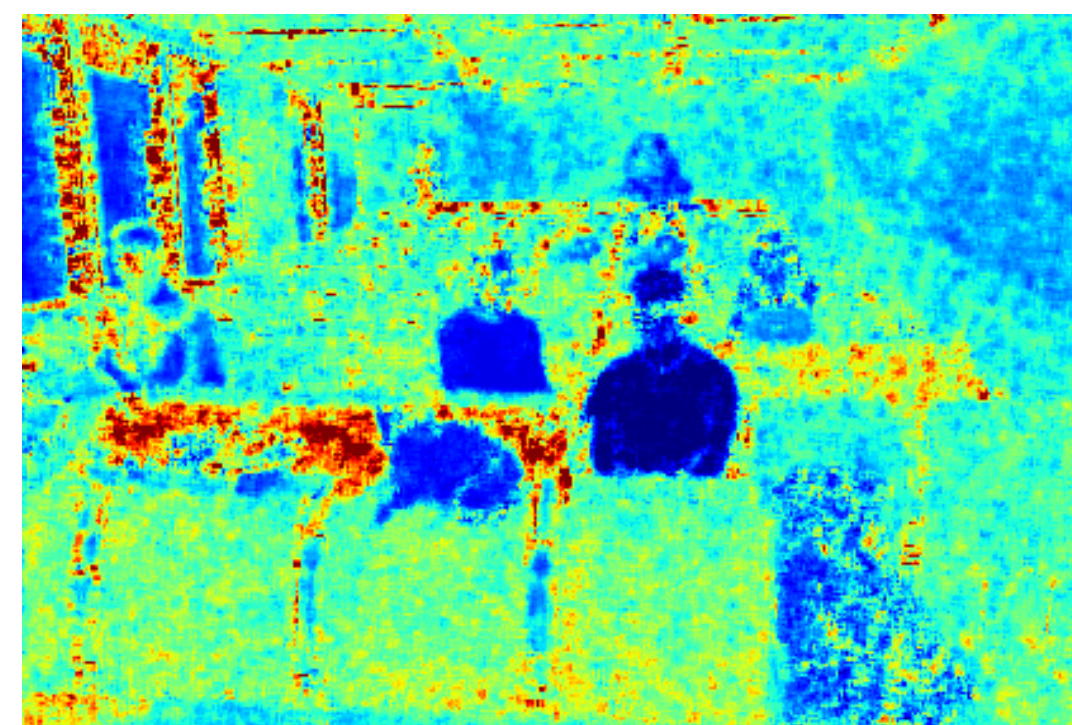
Comprint



zero



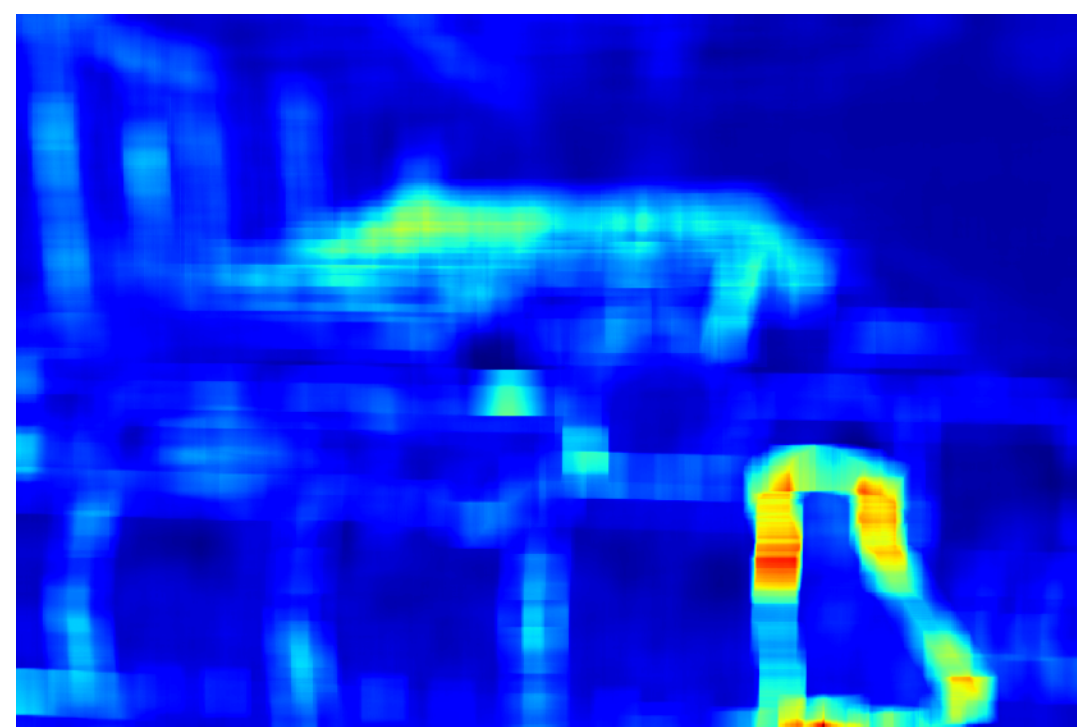
DCT



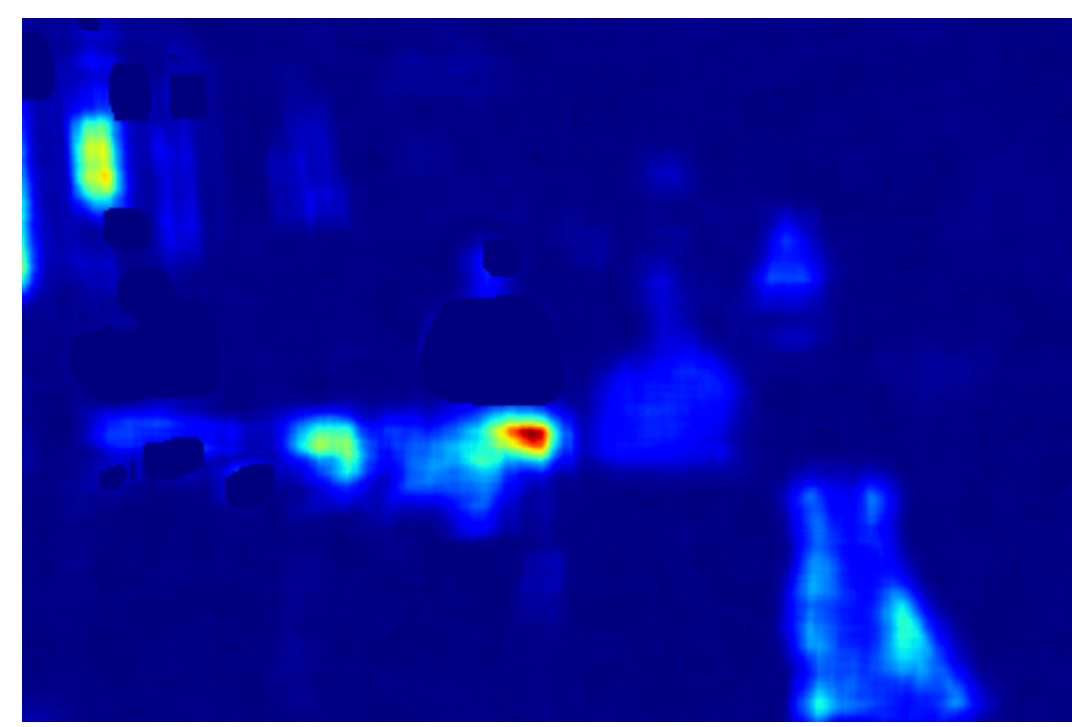
BLK



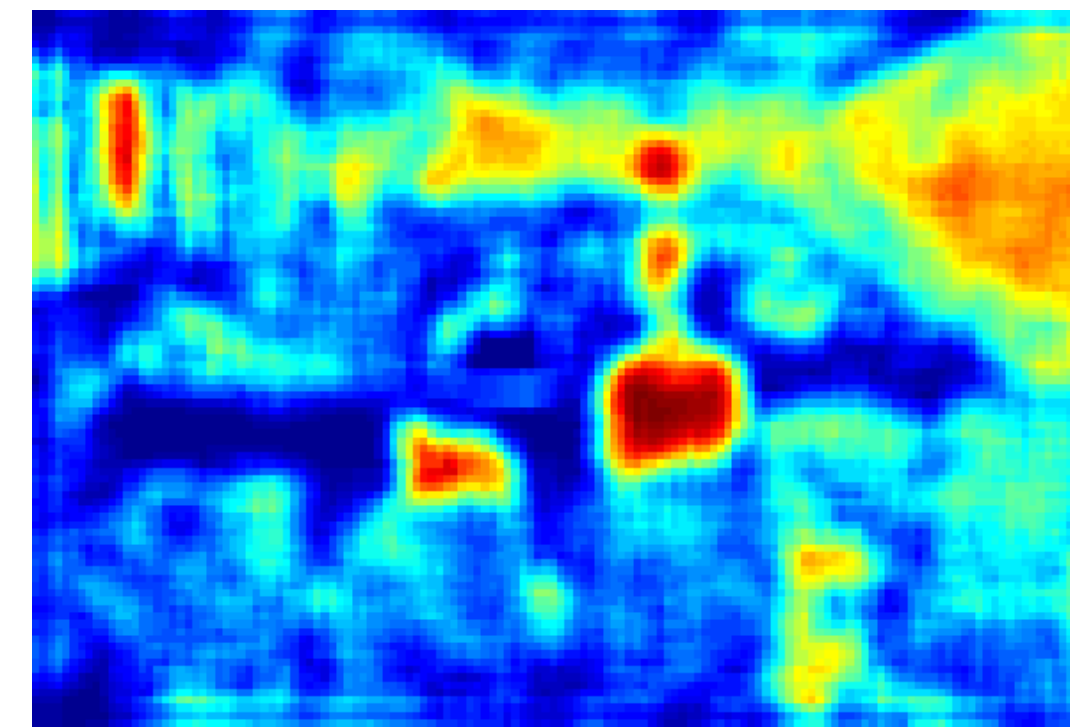
DQ



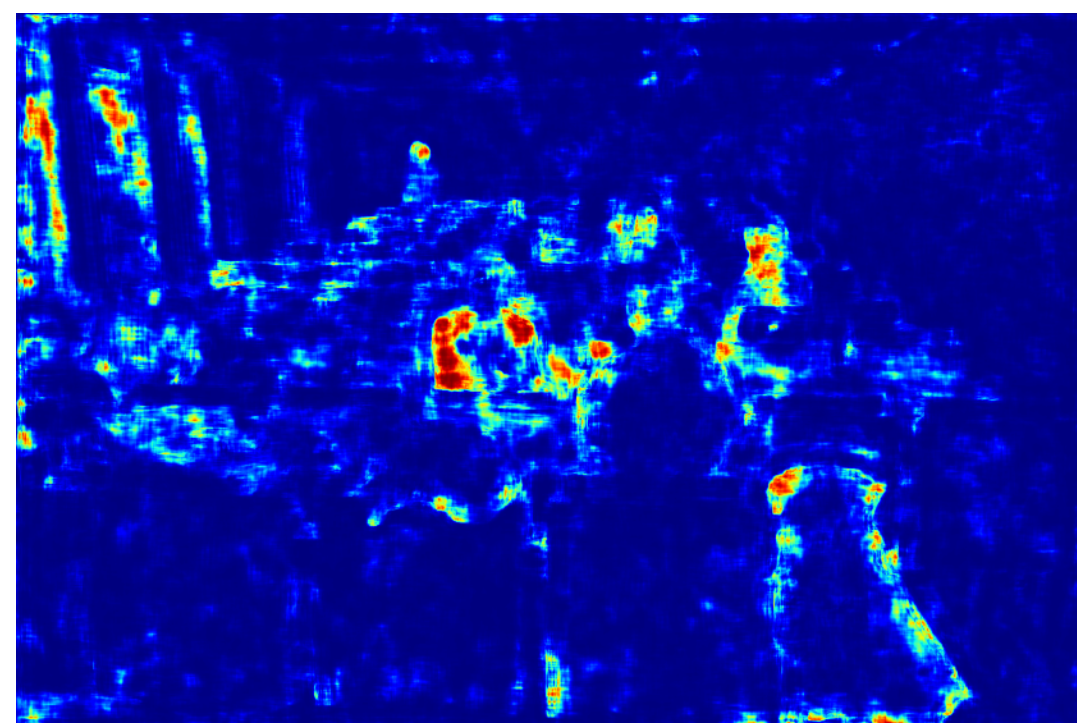
Ghost



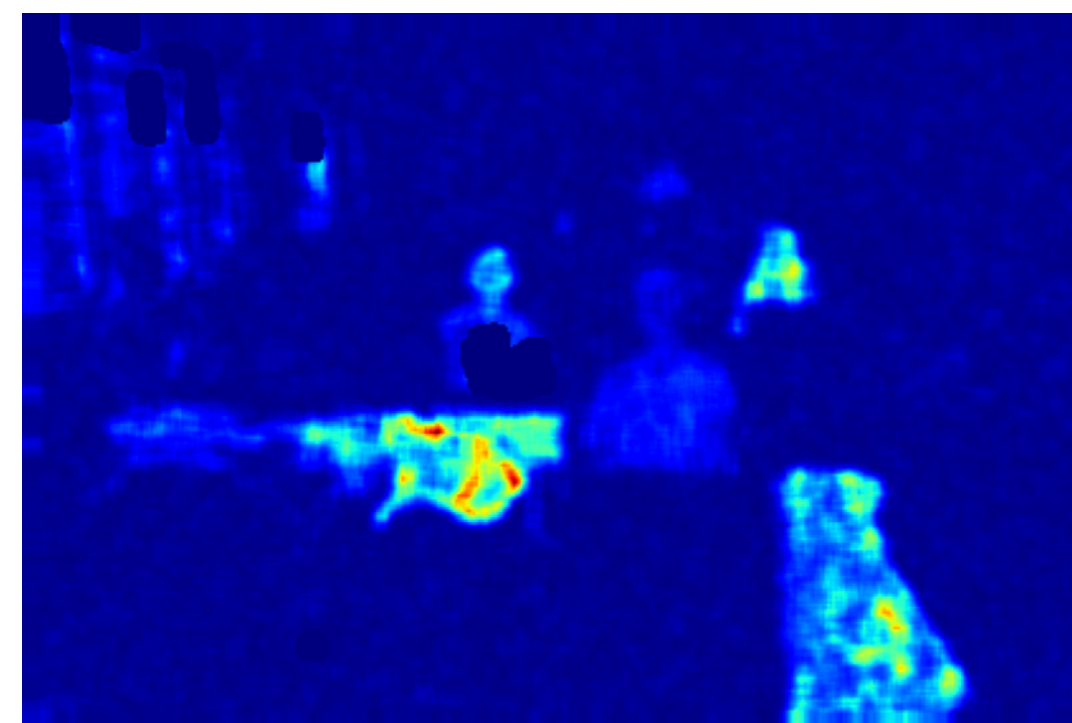
Splicebuster



CAGI



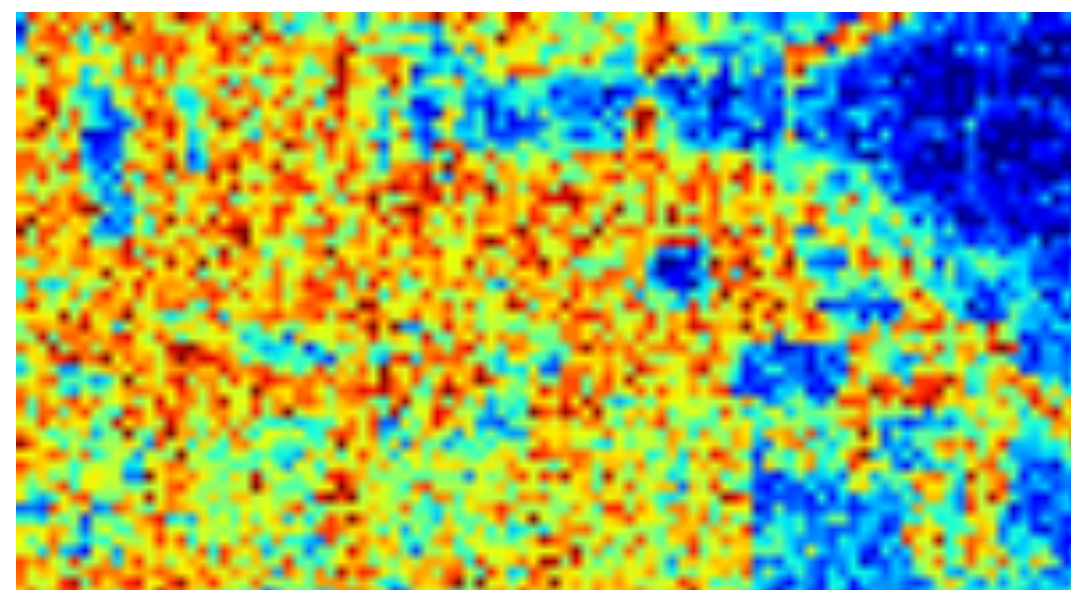
ManTraNet



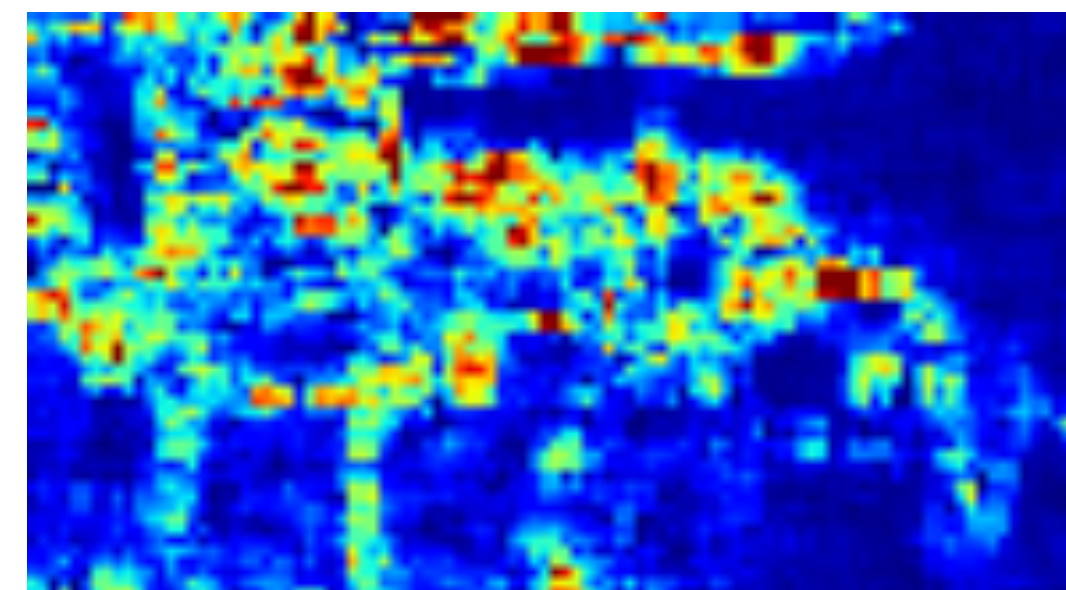
Noiseprint



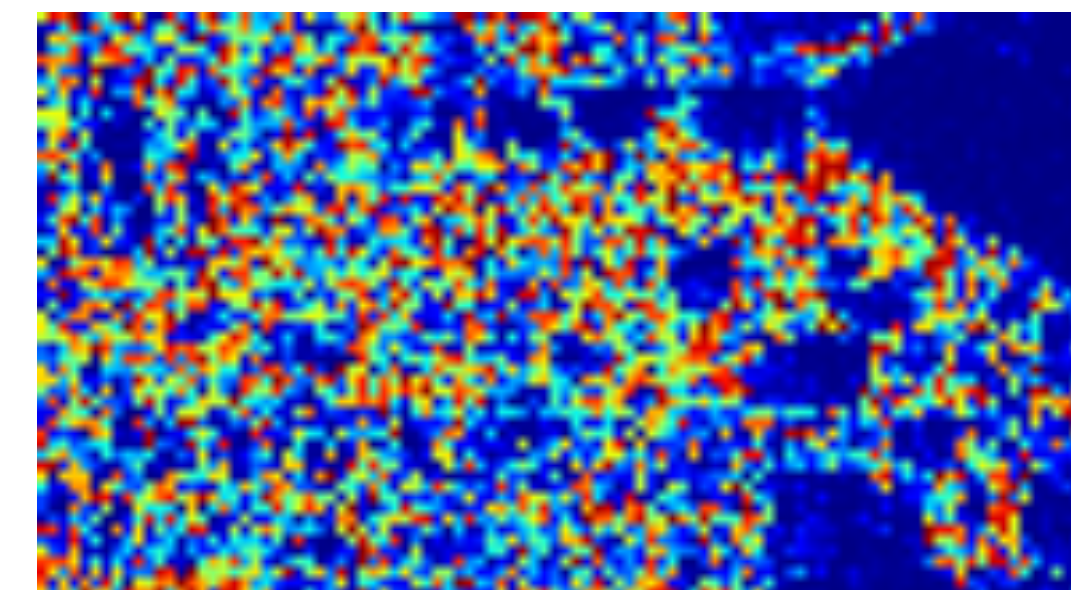
Comprint



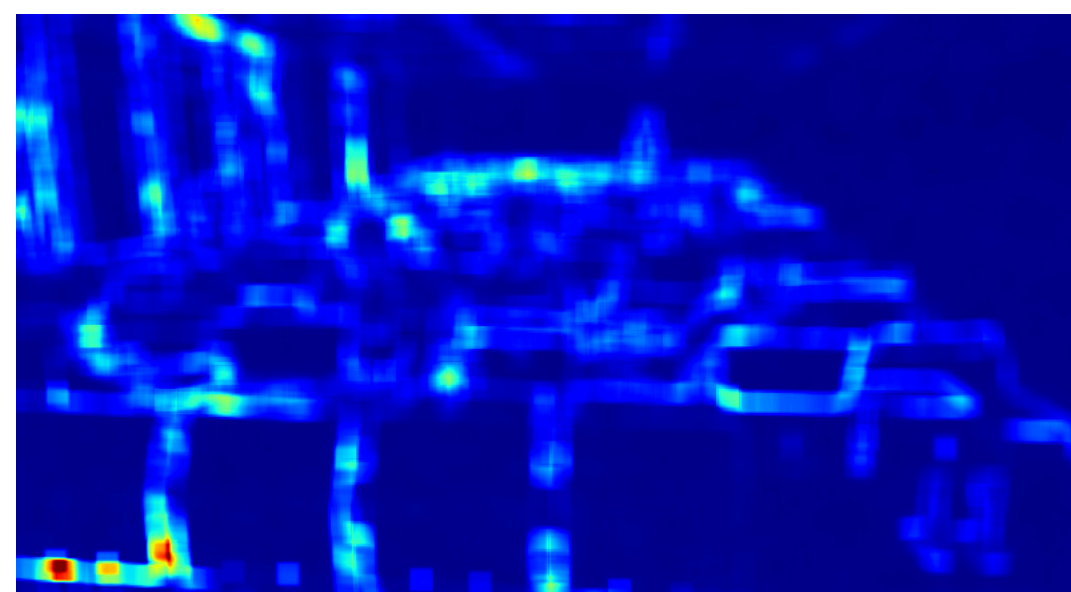
DCT



BLK



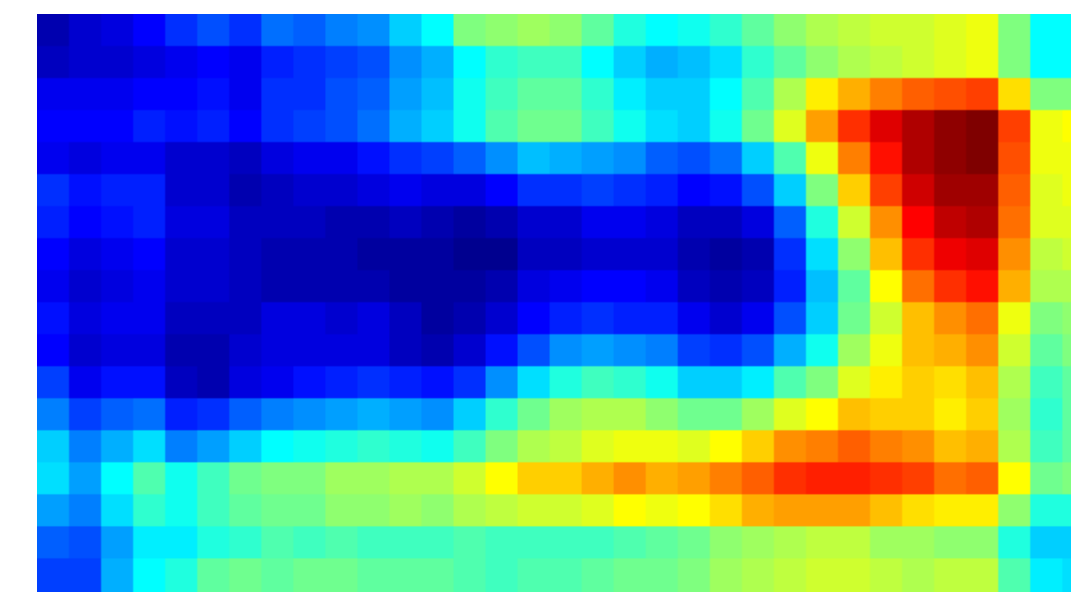
DQ



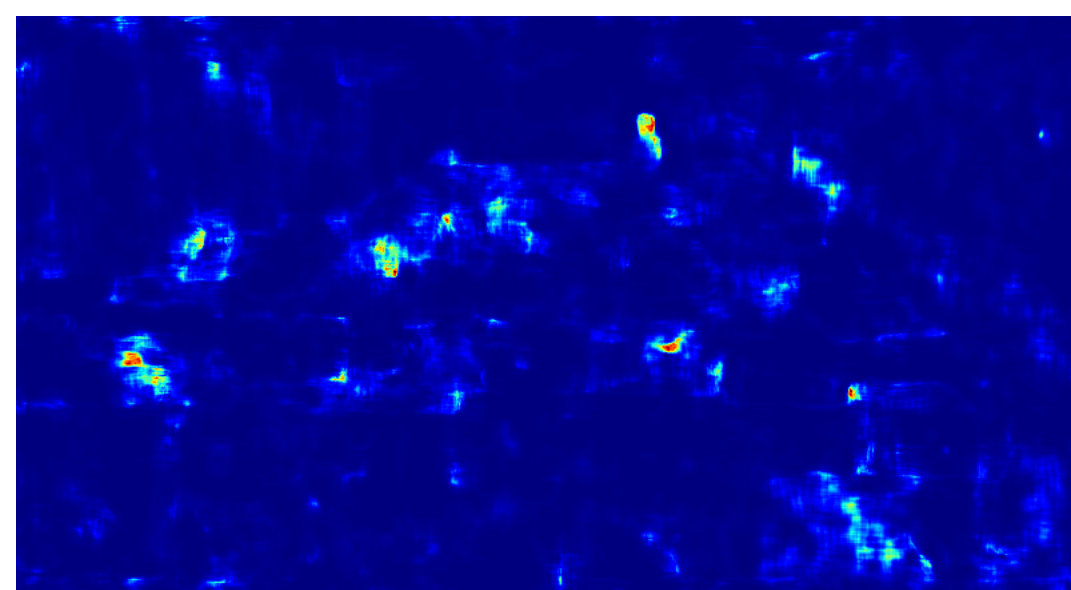
Ghost



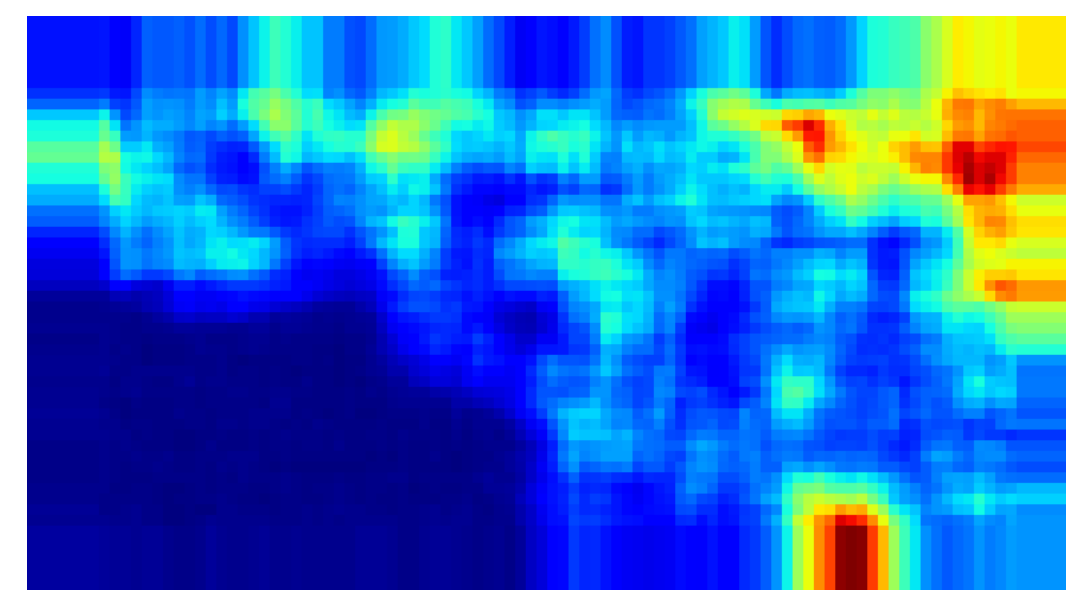
Splicebuster



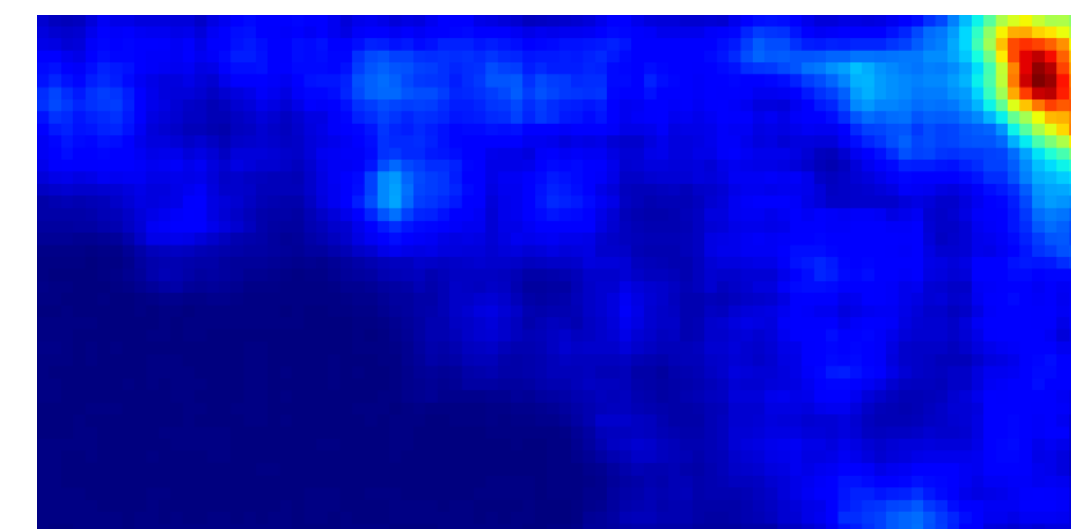
CAGI



ManTraNet



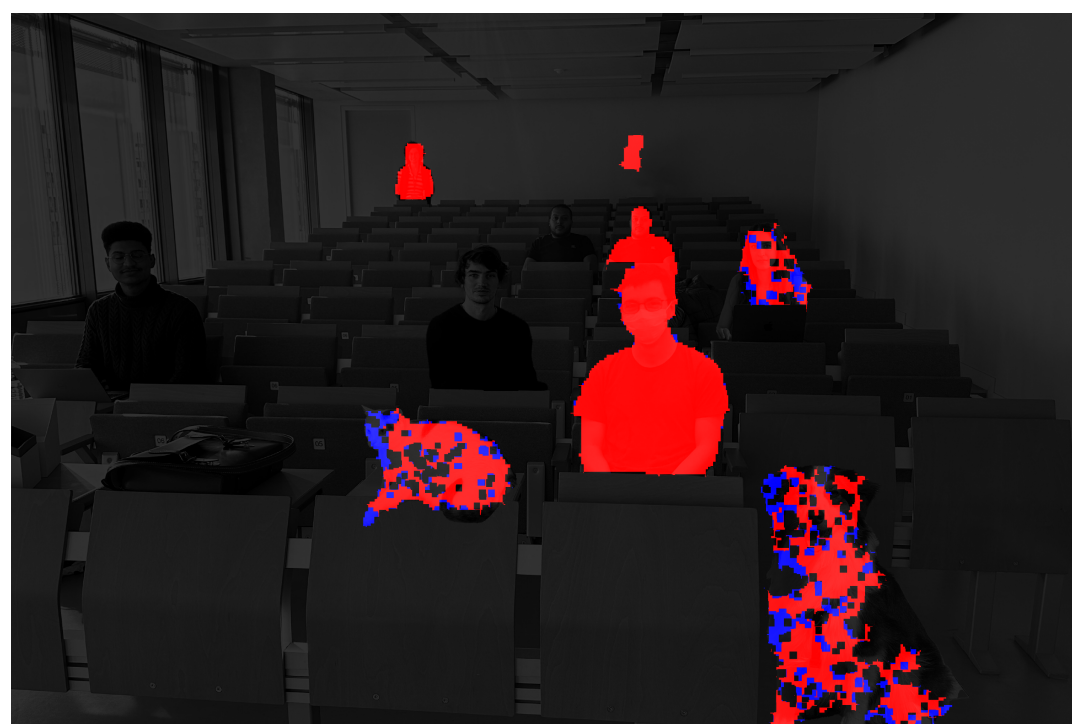
Noiseprint



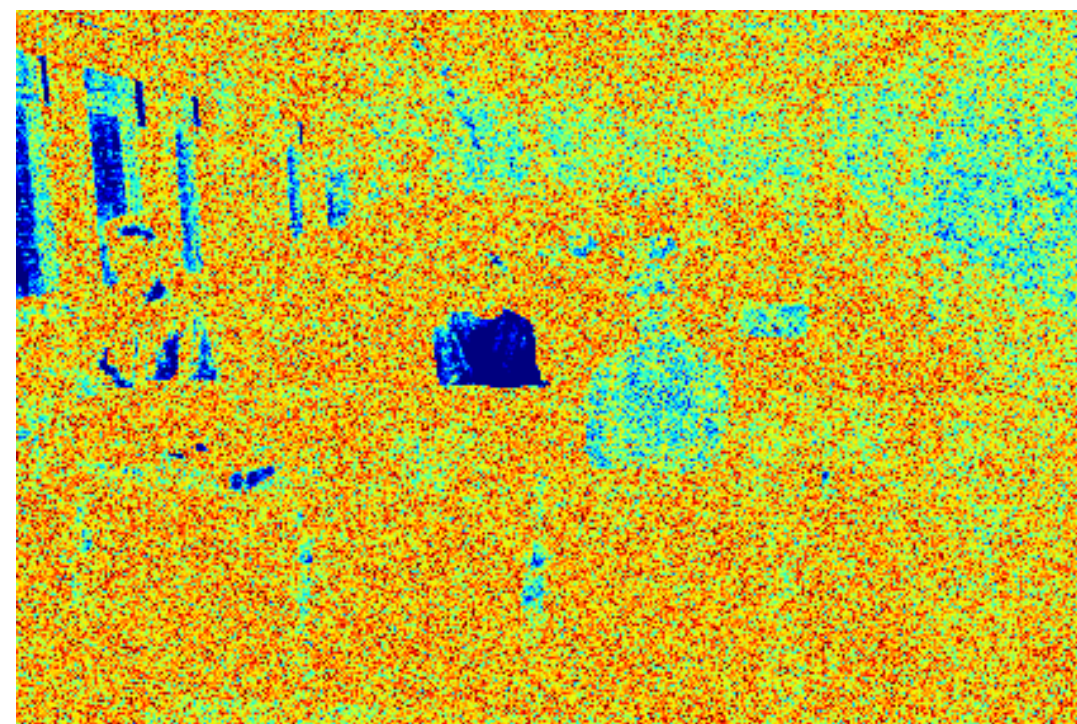
Comprint

NO JPEG TRACES
DETECTED

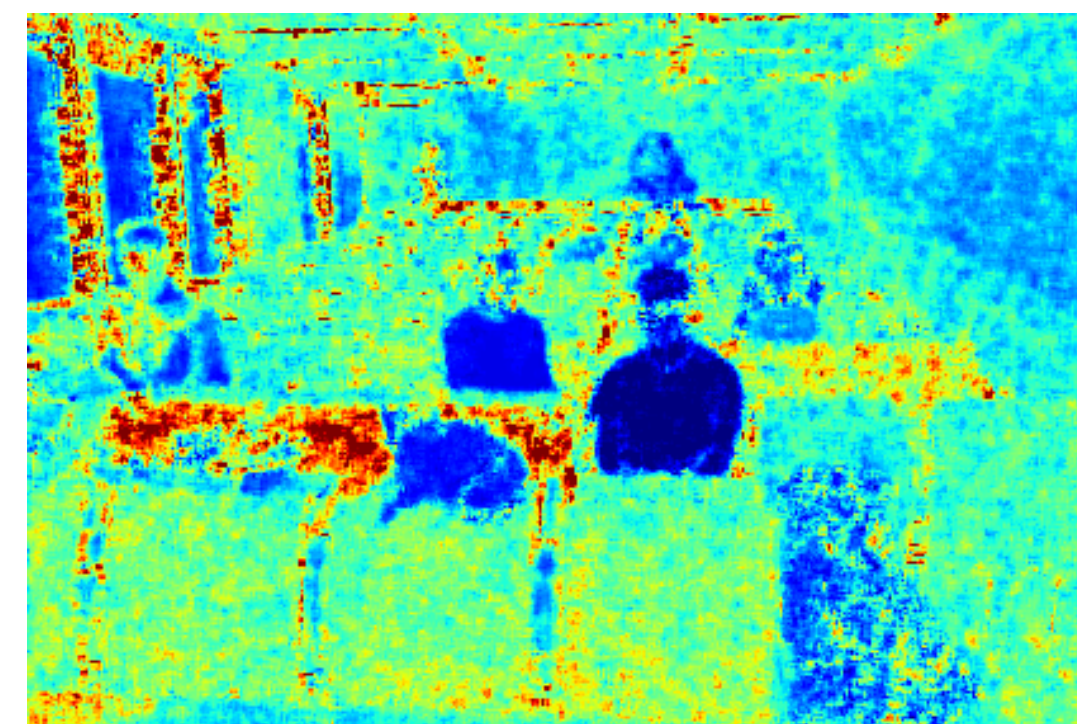
zero



zero



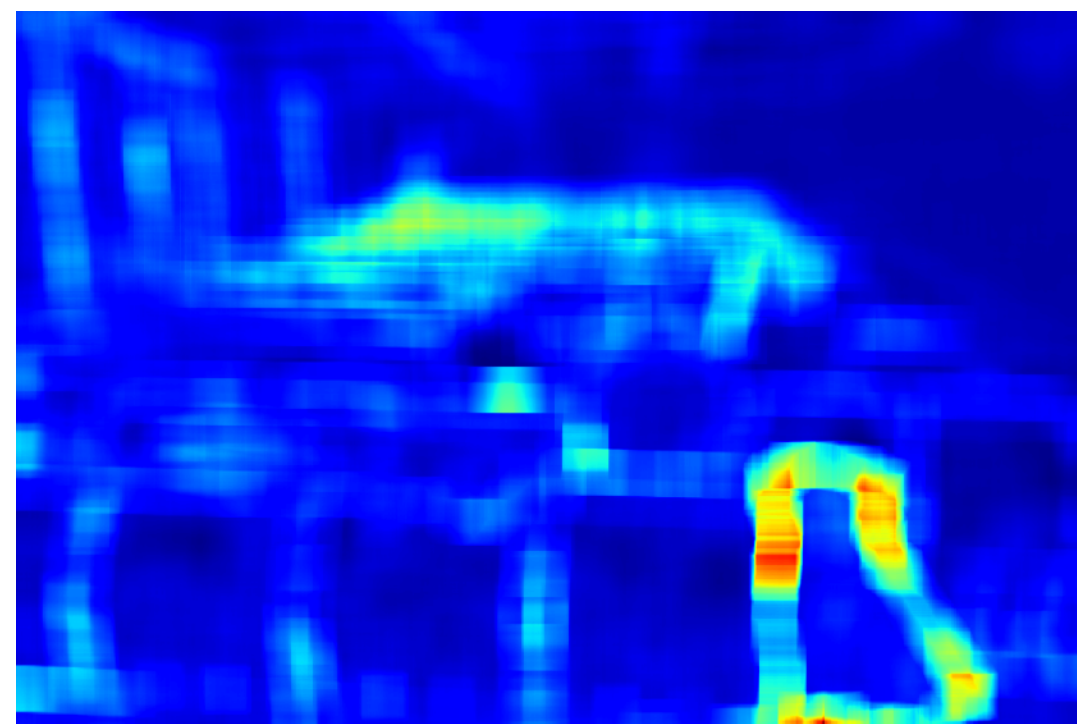
DCT



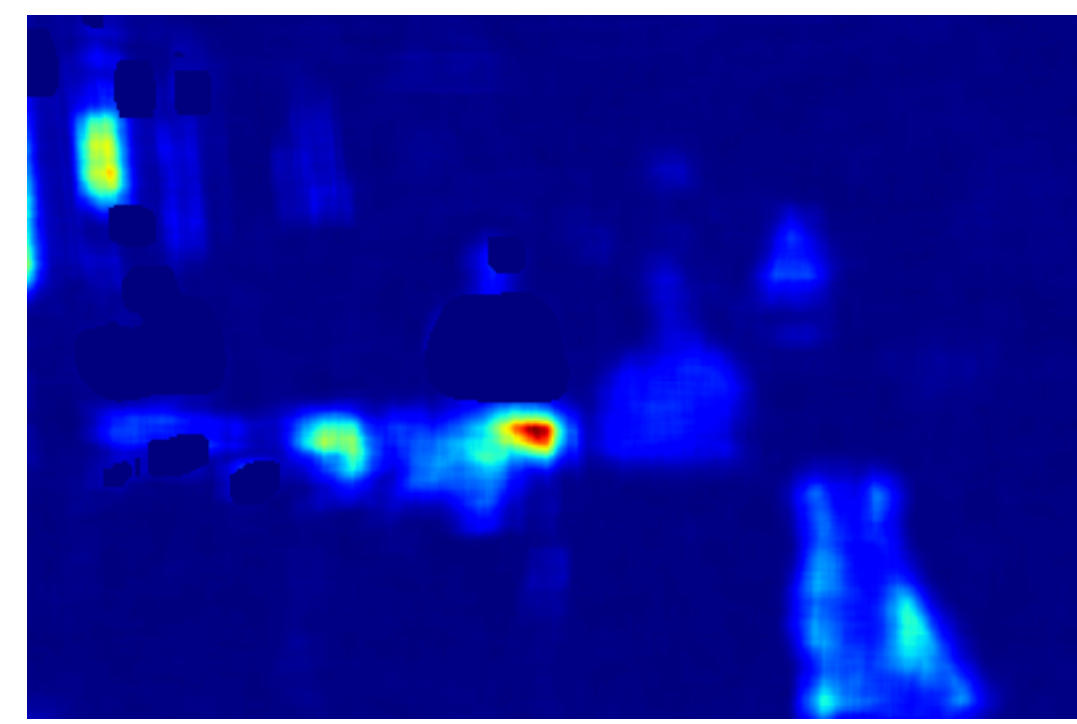
BLK



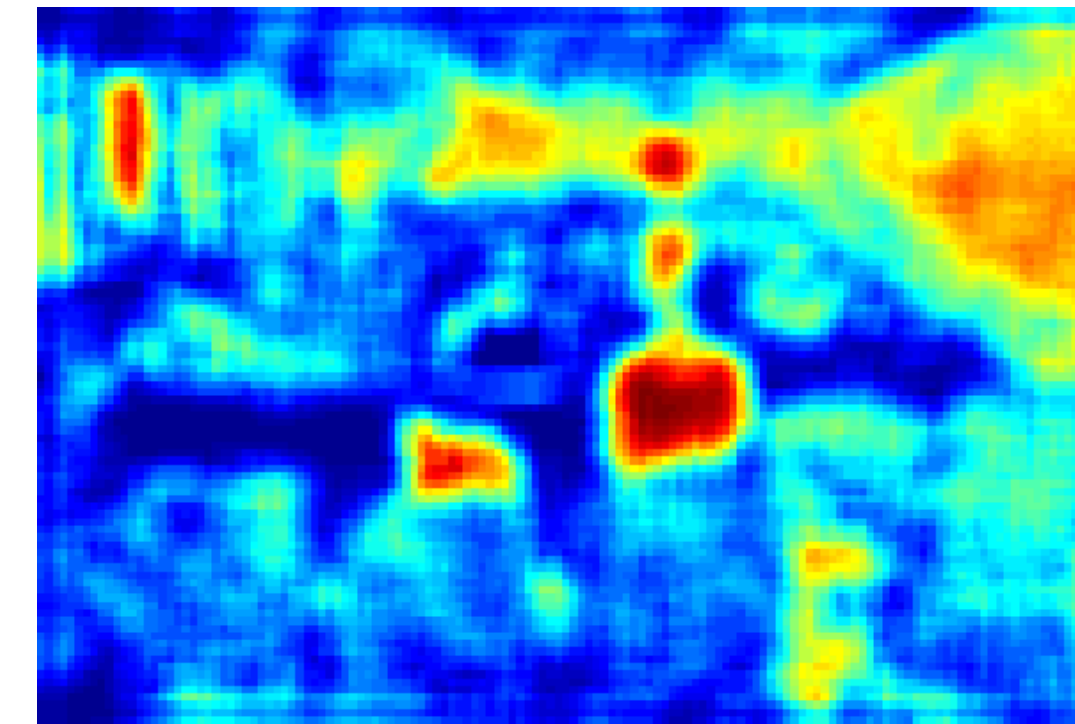
DQ



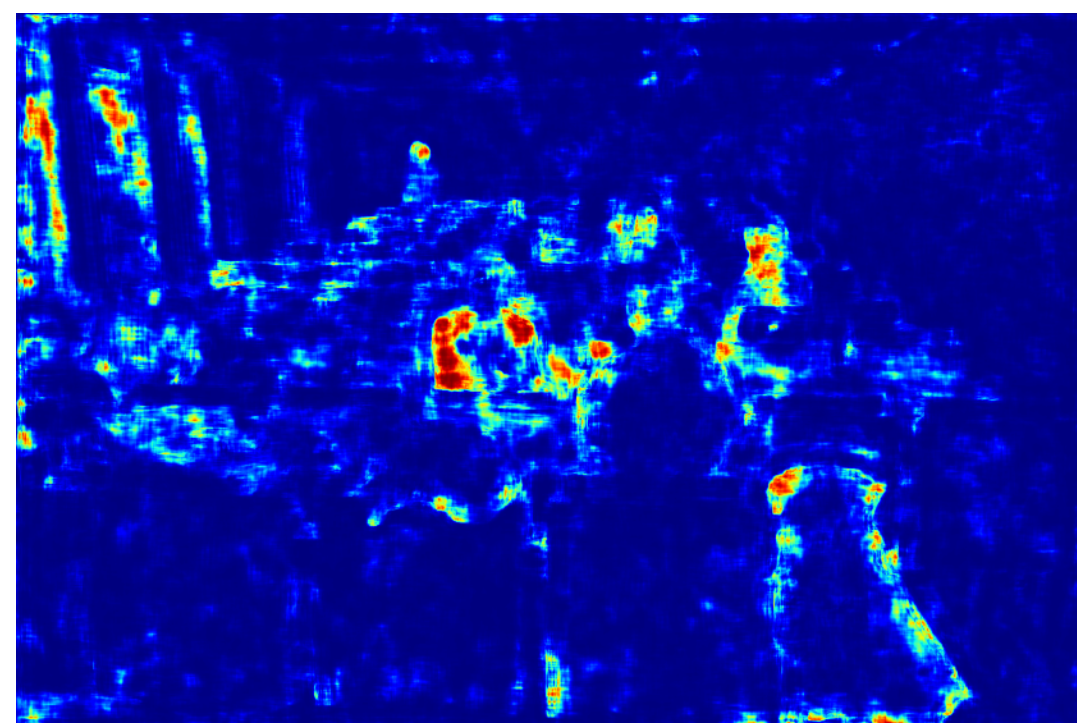
Ghost



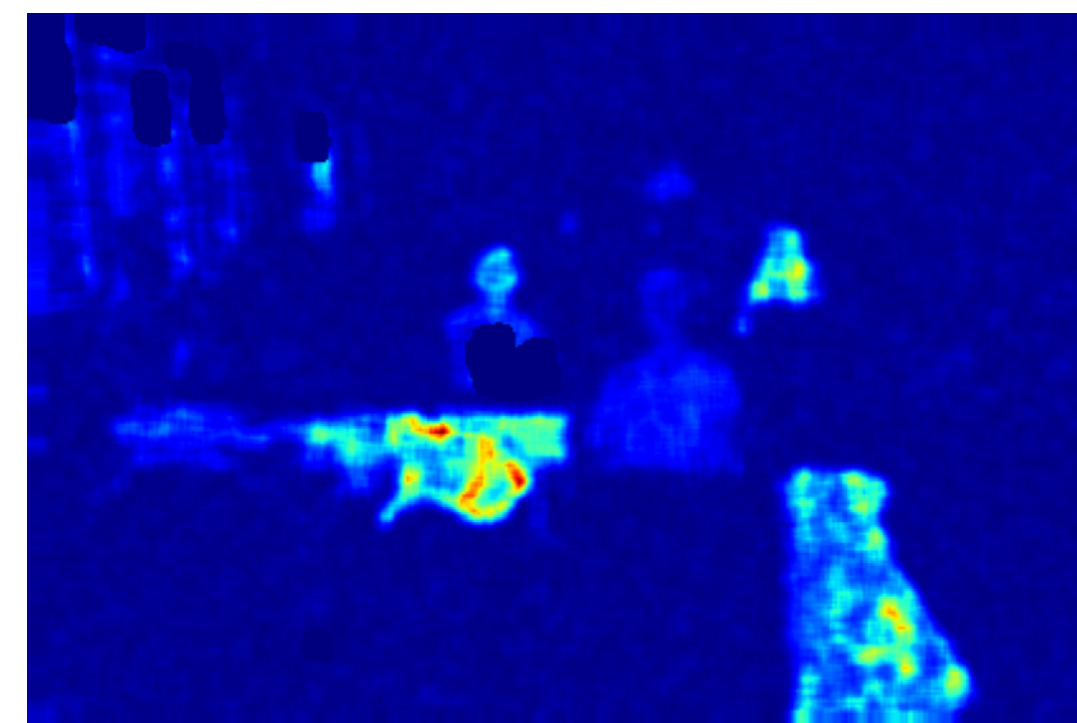
Splicebuster



CAGI



ManTraNet



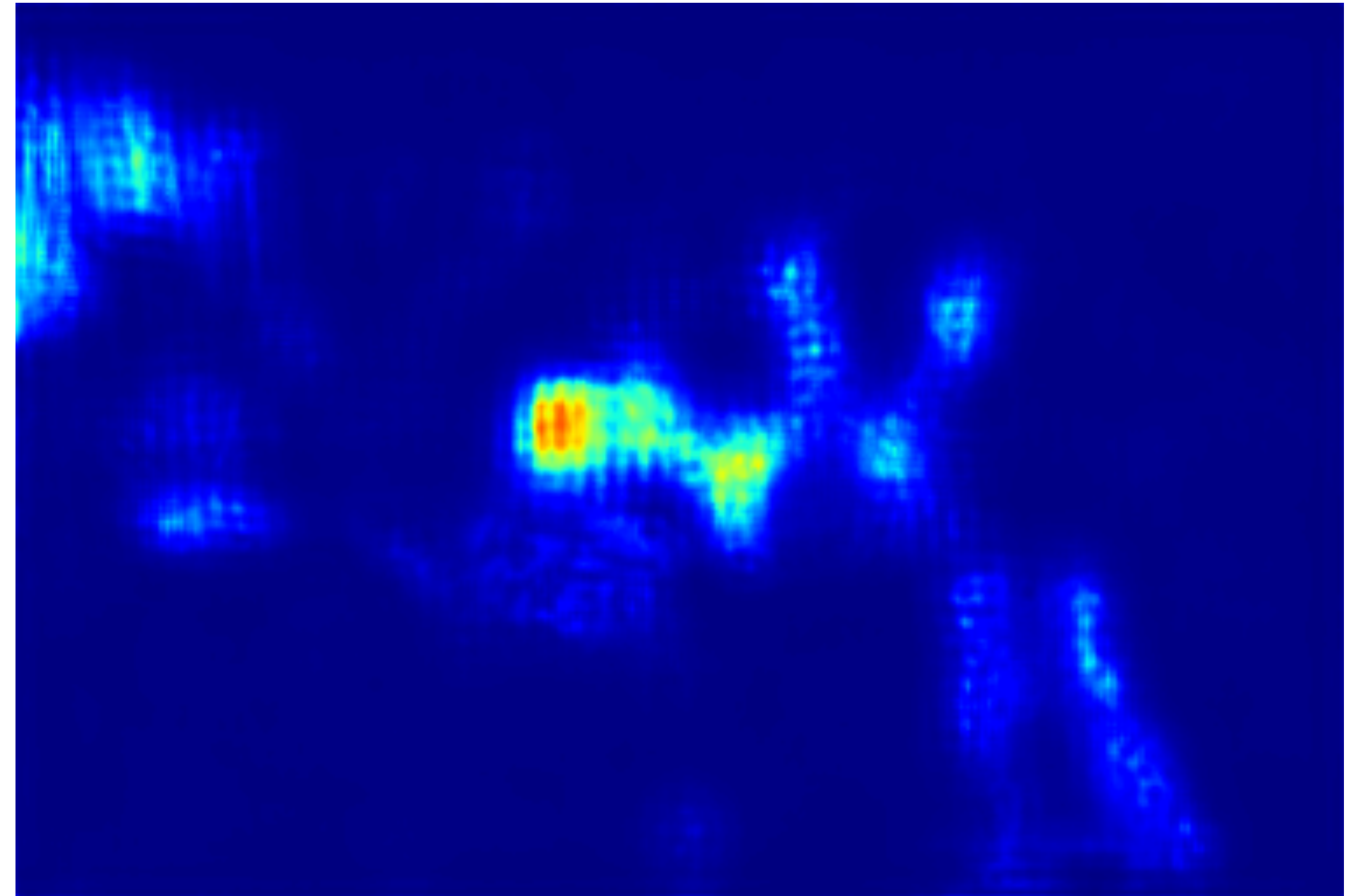
Noiseprint



Comprint

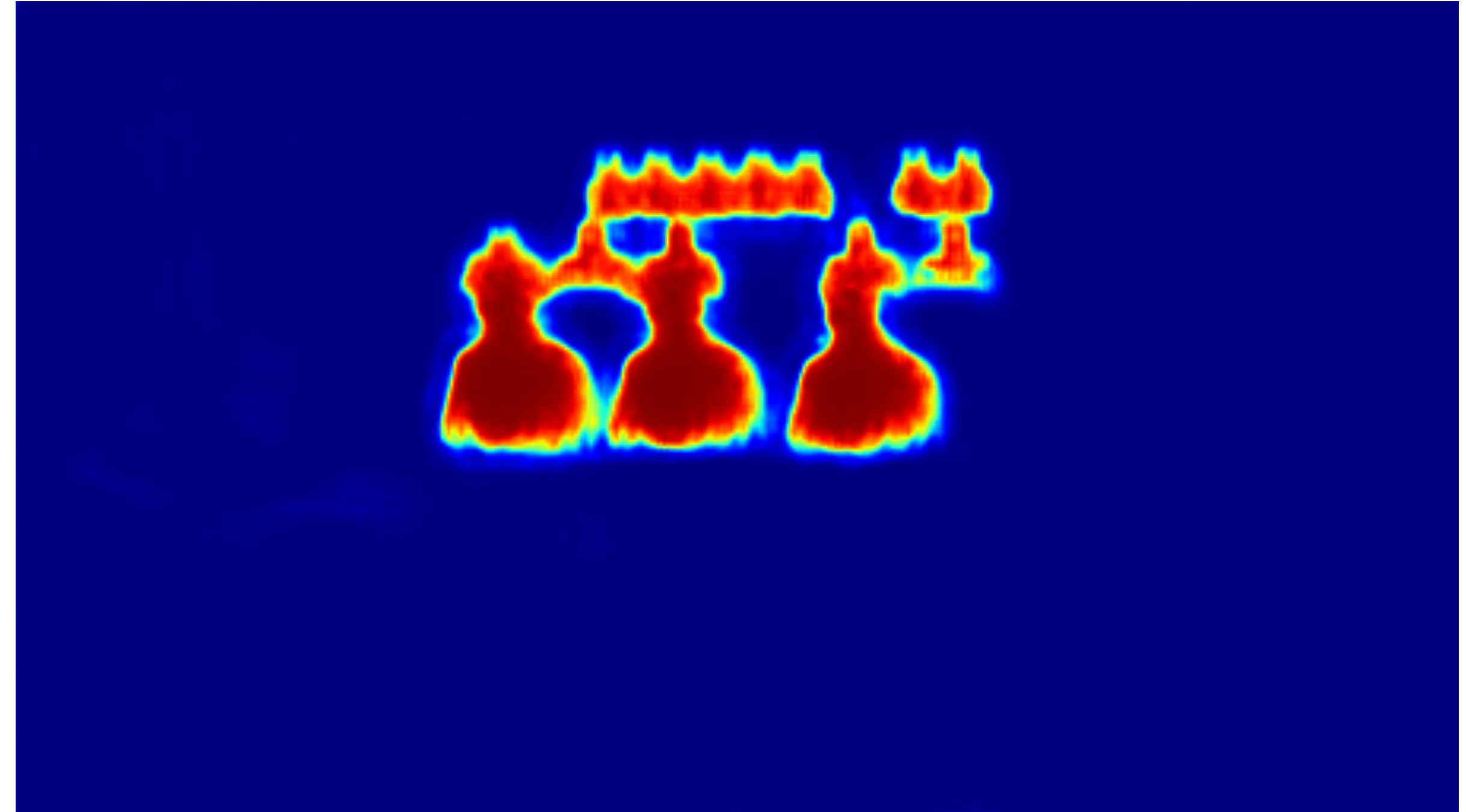
Fusion

P. Charitidis, G. Kordopatis-Zilos, S. Papadopoulos and I. Kompatsiaris, "Operation-wise Attention Network for Tampering Localization Fusion," *2021 International Conference on Content-Based Multimedia Indexing (CBMI)*, 2021, pp. 1-6, doi: 10.1109/CBMI50038.2021.9461920.



Fusion

P. Charitidis, G. Kordopatis-Zilos, S. Papadopoulos and I. Kompatsiaris, "Operation-wise Attention Network for Tampering Localization Fusion," *2021 International Conference on Content-Based Multimedia Indexing (CBMI)*, 2021, pp. 1-6, doi: 10.1109/CBMI50038.2021.9461920.



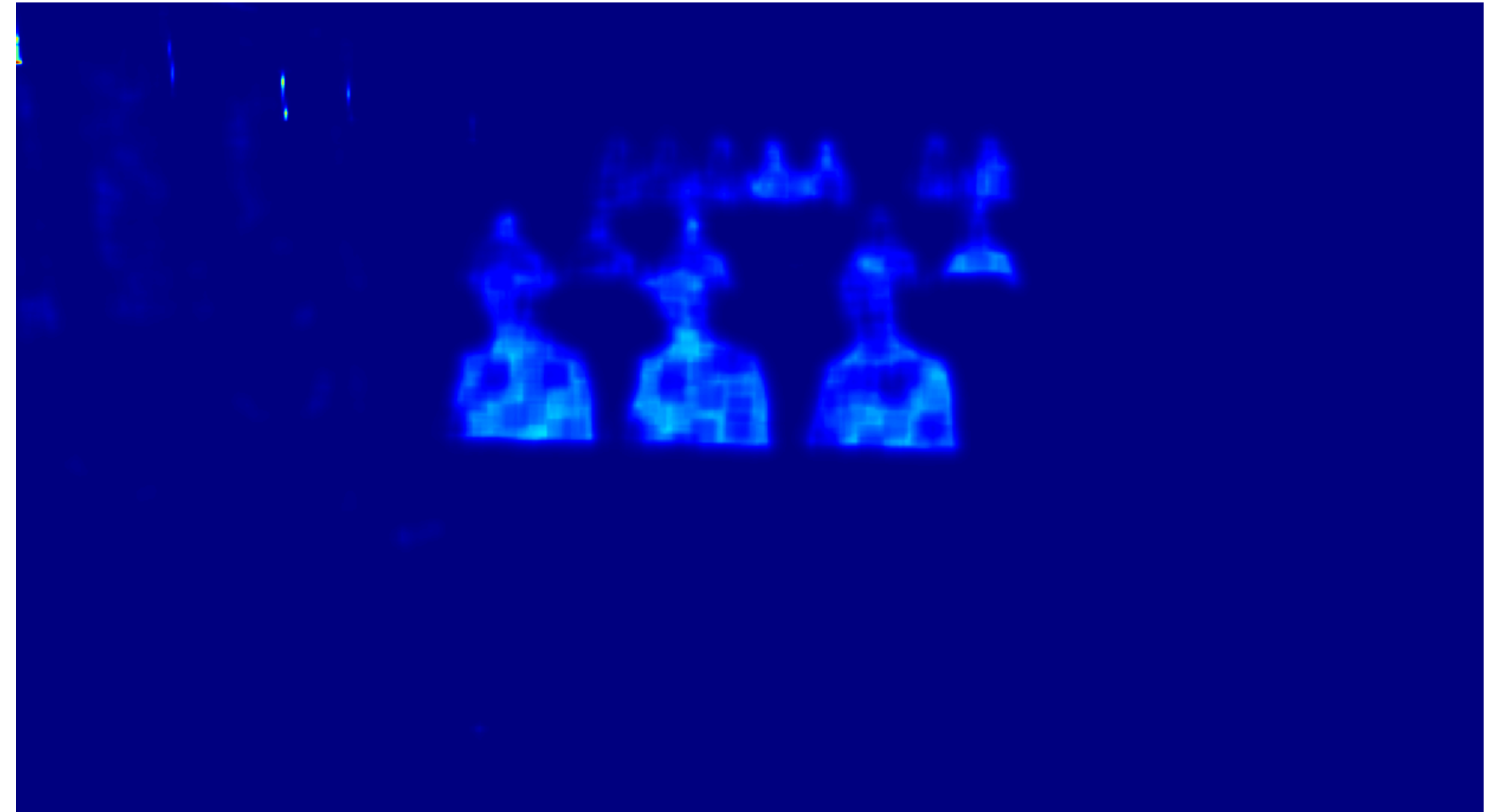
Copy-move detection

T. Ehret, "Robust copy-move forgery detection by false alarms control," 2019, arXiv [1906.00649](https://arxiv.org/abs/1906.00649).



Comprint

Mareen, Hannes, Dante Vanden Bussche, Fabrizio Guillaro, Davide Cozzolino, Glenn Van Wallendael, Peter Lambert, and Luisa Verdoliva. "Comprint: Image Forgery Detection and Localization using Compression Fingerprints." *arXiv preprint arXiv:2210.02227* (2022)



Comprint

Mareen, Hannes, Dante Vanden Bussche, Fabrizio Guillaro, Davide Cozzolino, Glenn Van Wallendael, Peter Lambert, and Luisa Verdoliva. "Comprint: Image Forgery Detection and Localization using Compression Fingerprints." *arXiv preprint arXiv:2210.02227* (2022)

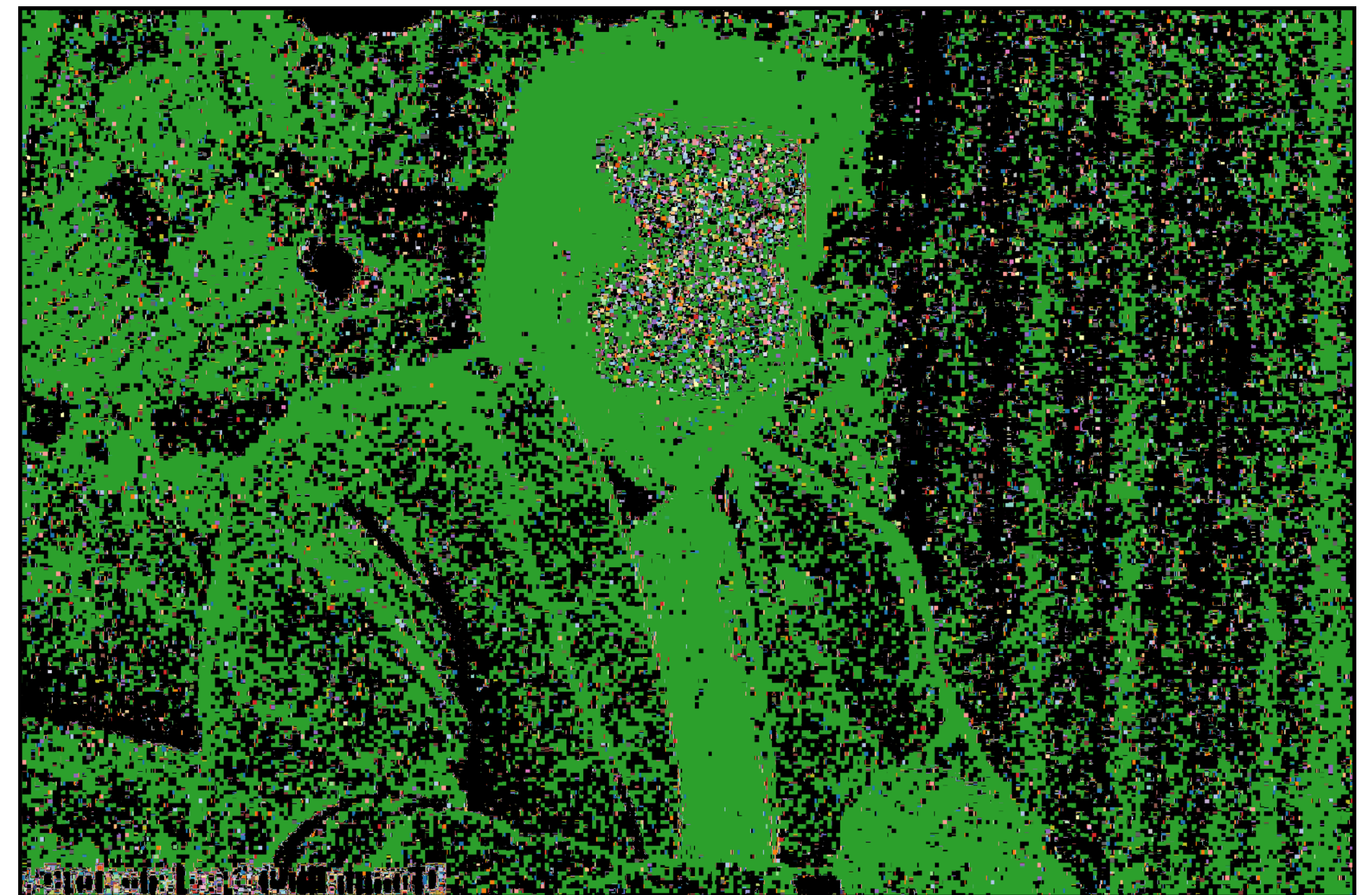
Failures



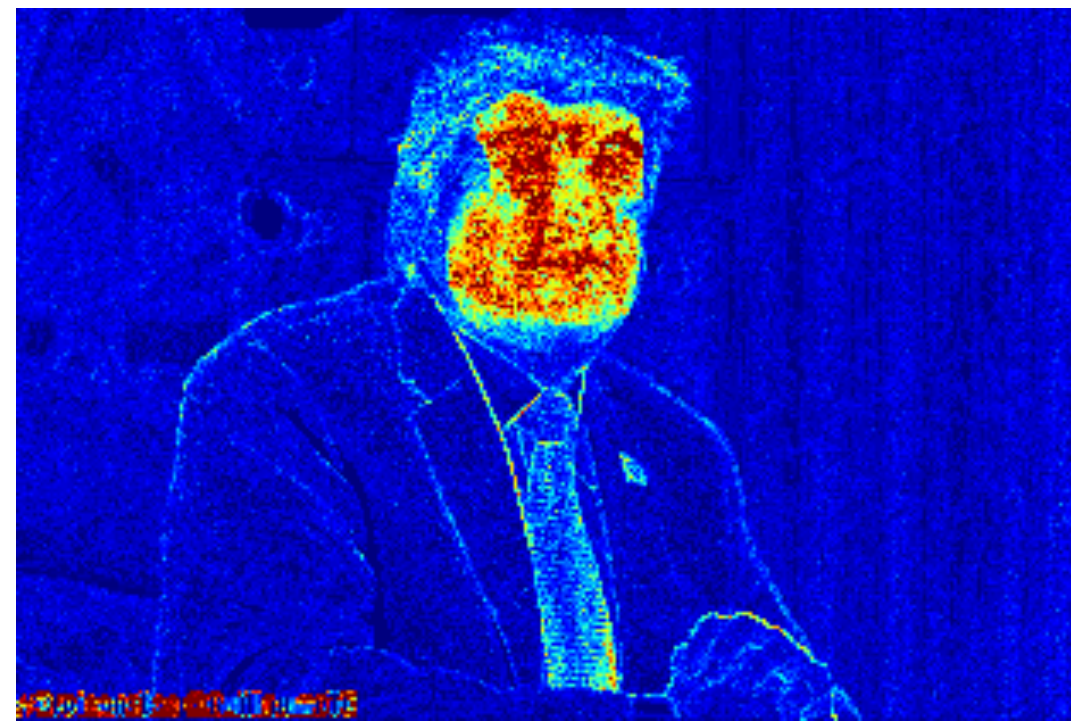
Failures



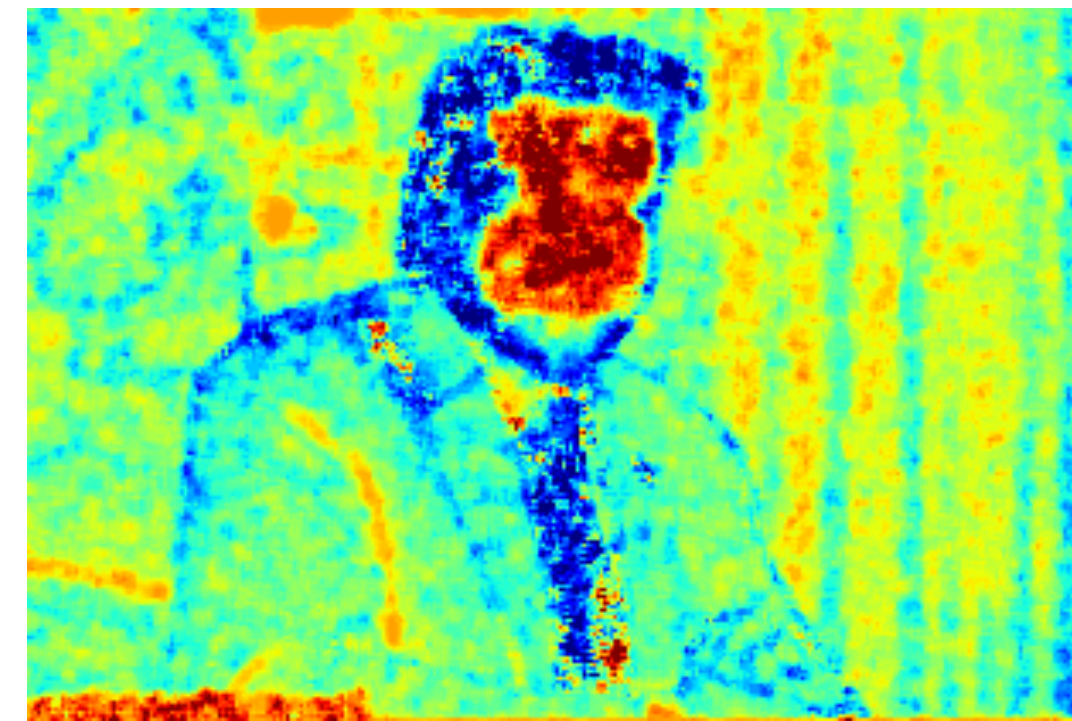
Forged image from @GuillaumeTC



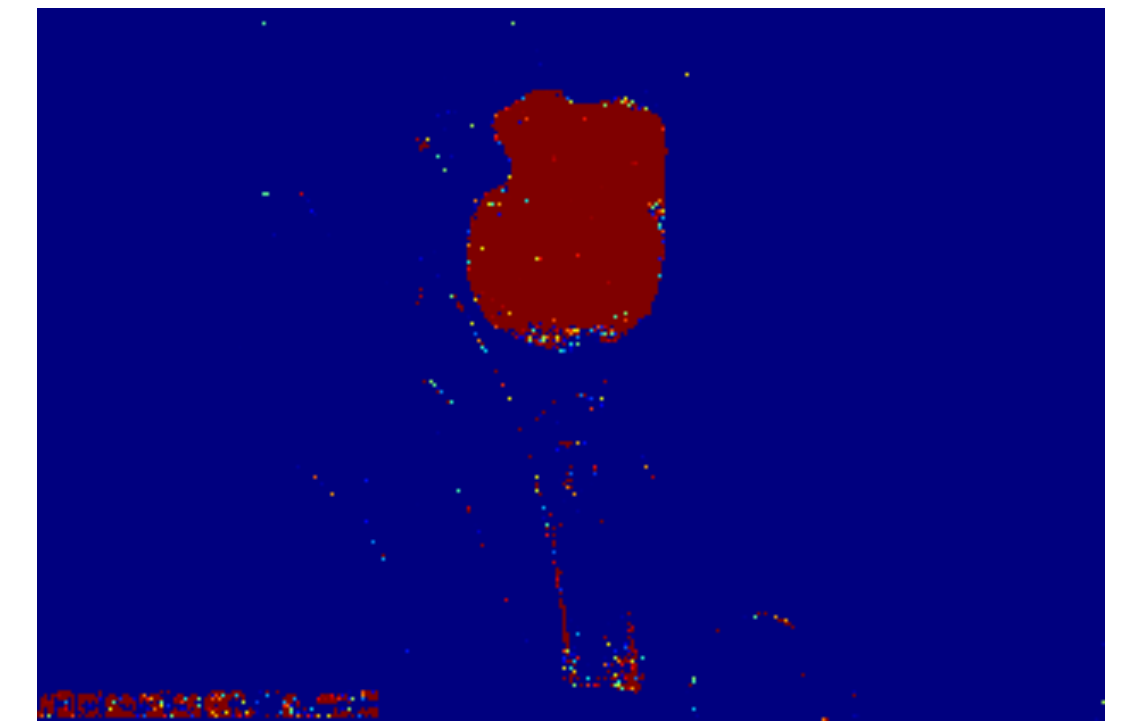
Vote map



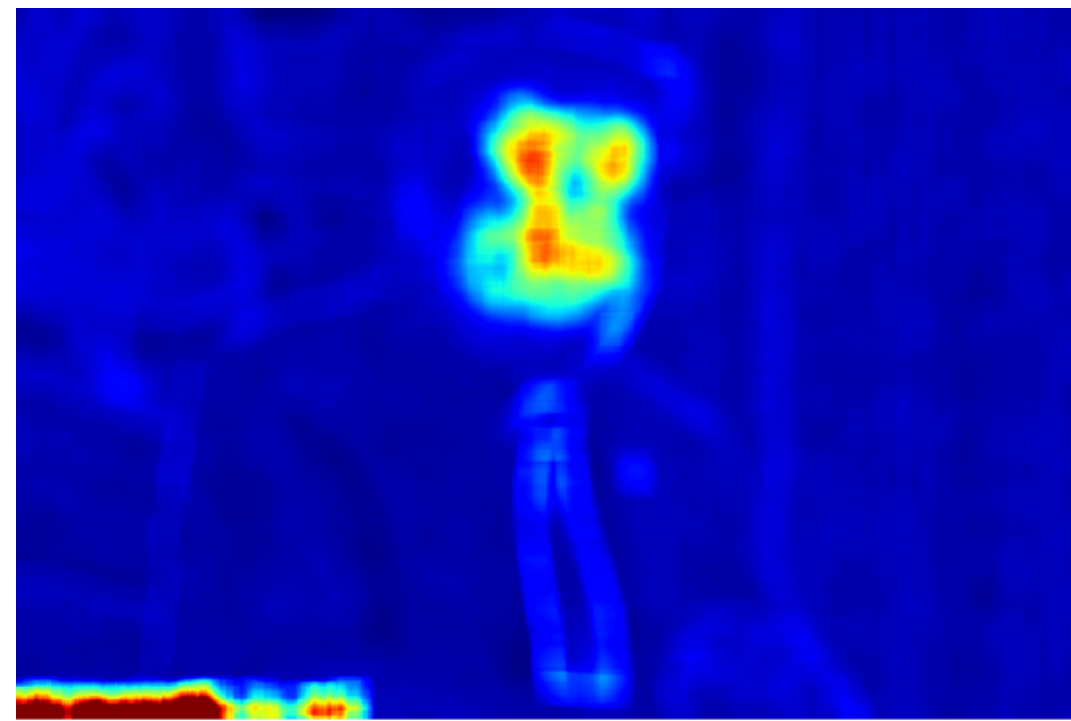
DCT



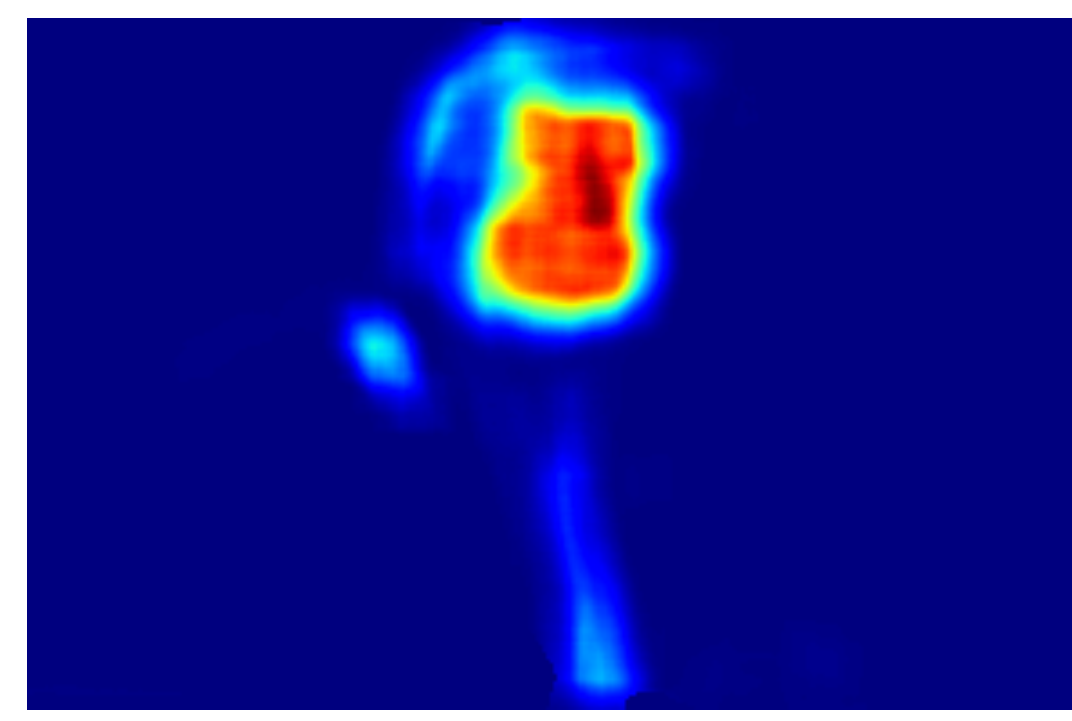
BLK



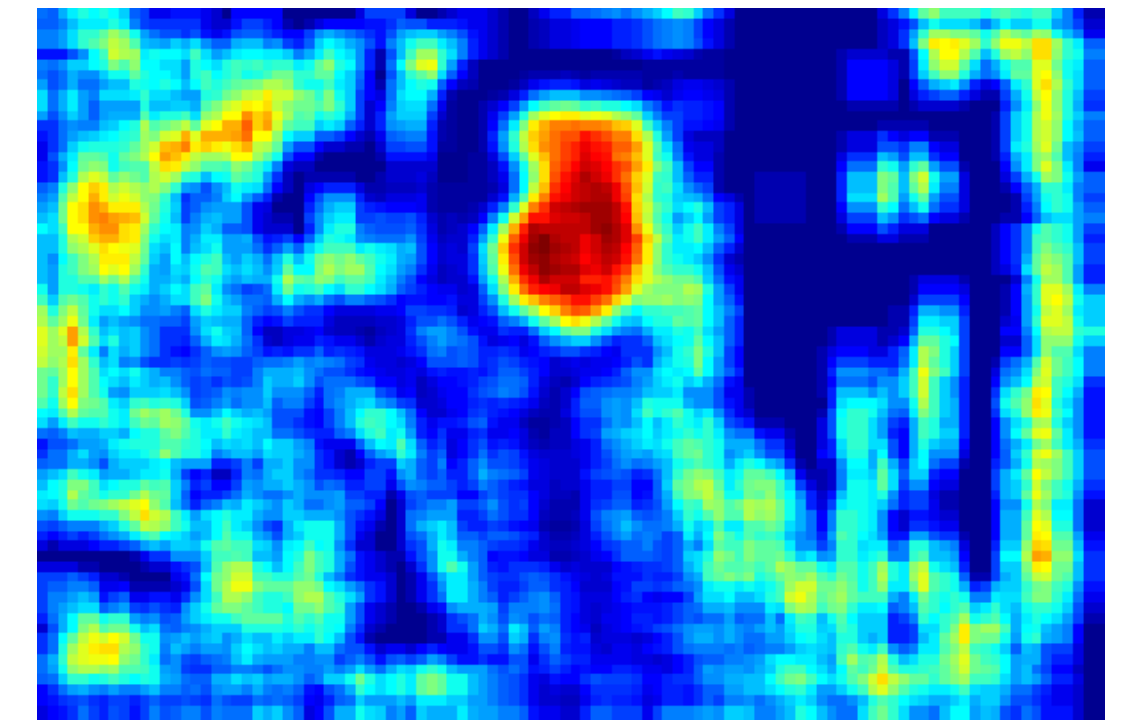
DQ



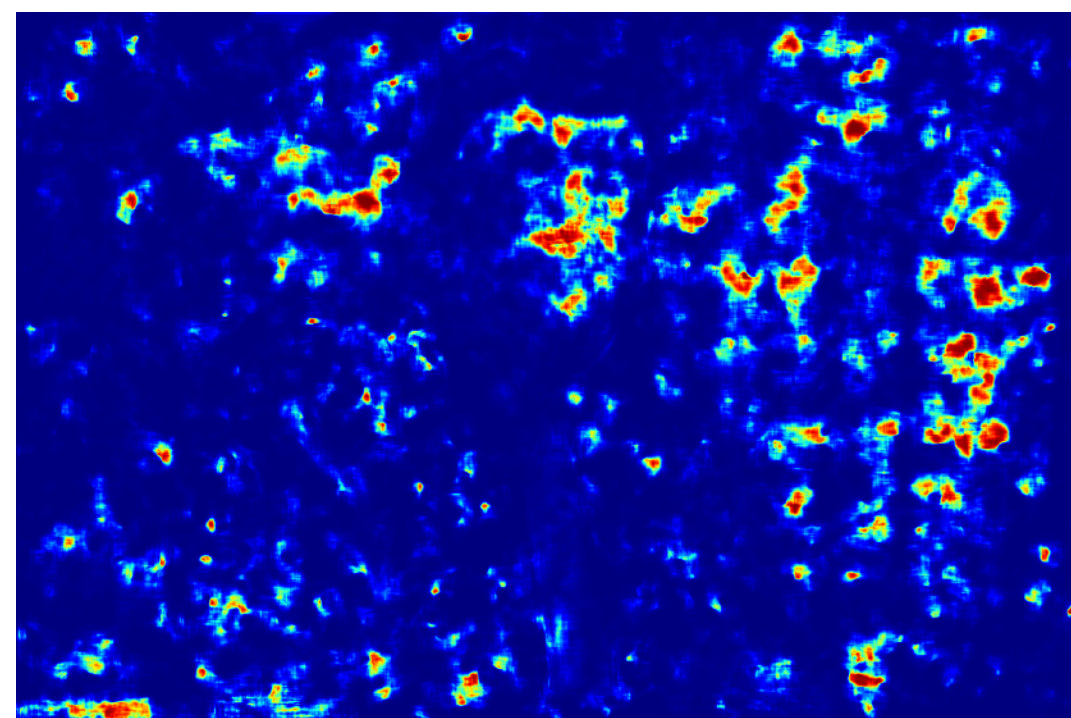
Ghost



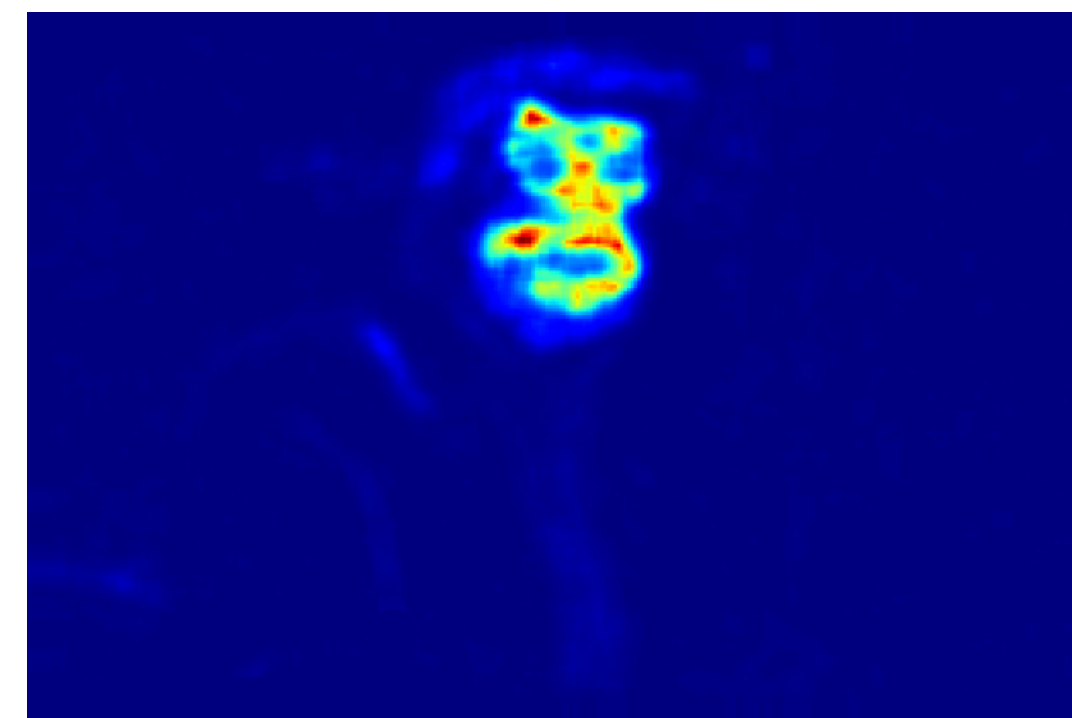
Splicebuster



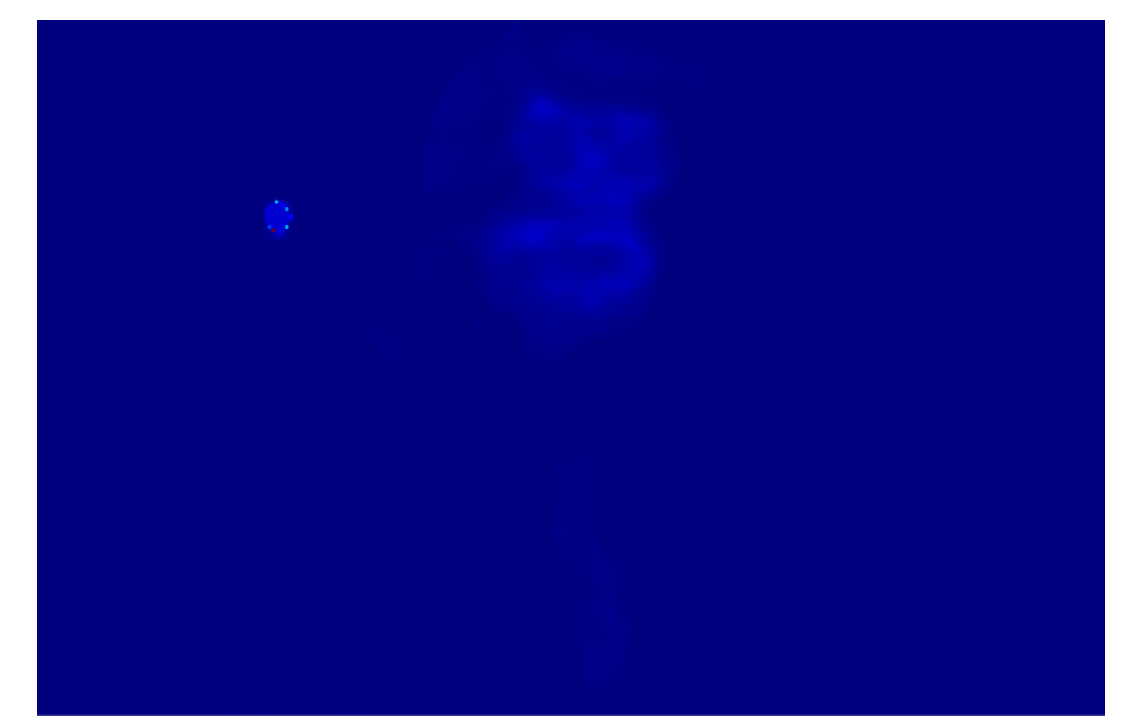
CAGI



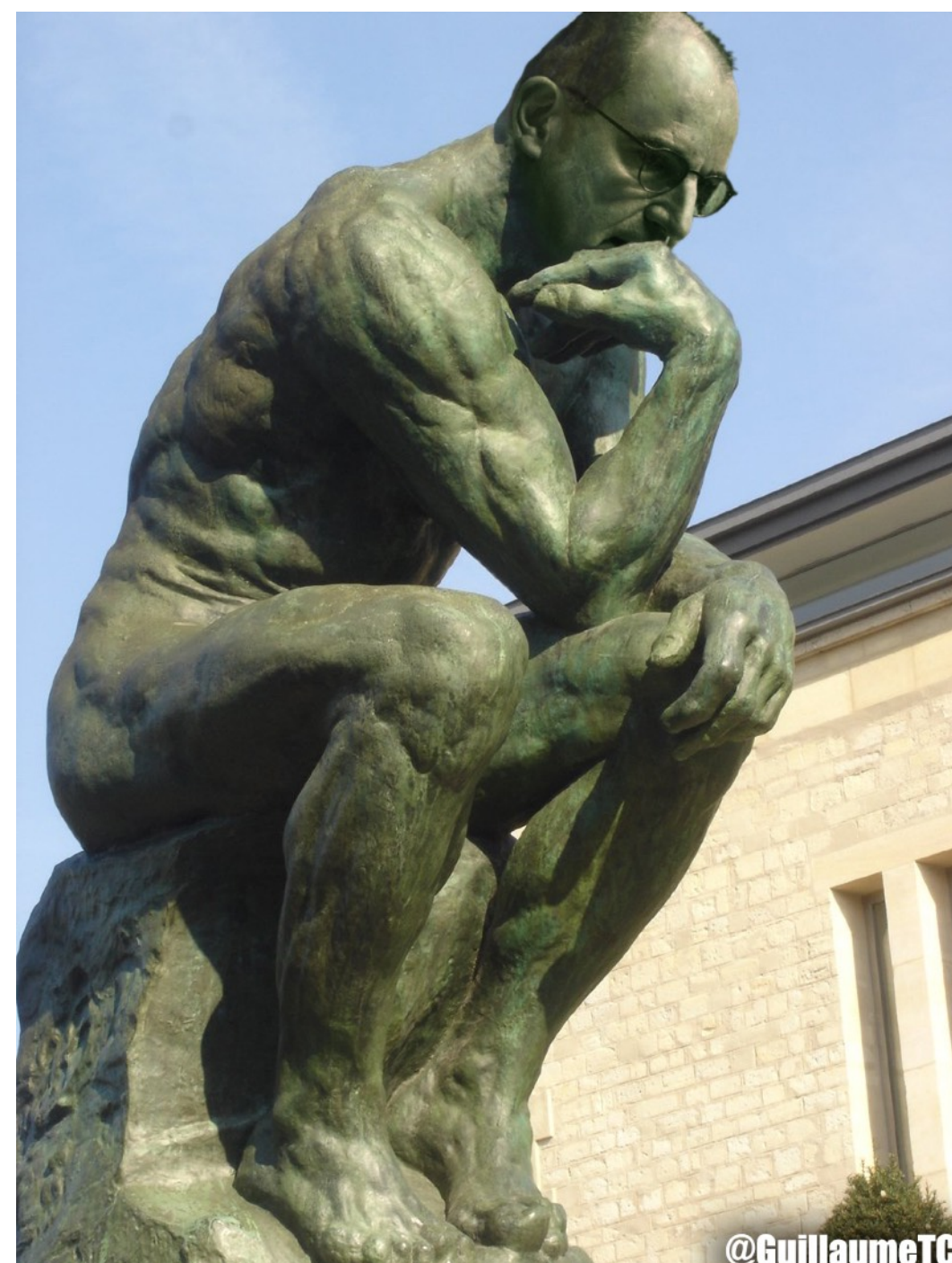
ManTraNet



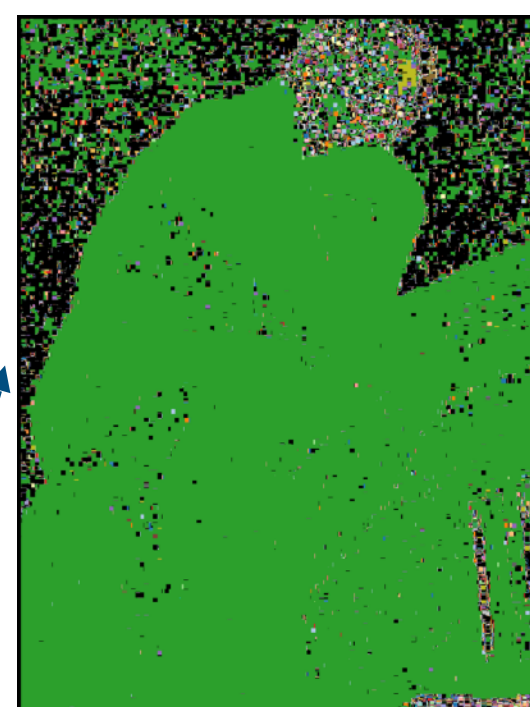
Noiseprint



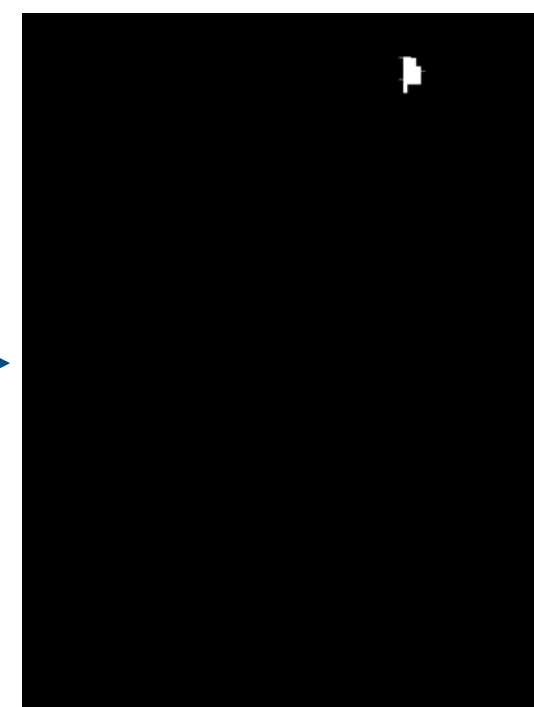
Comprint



Forged image

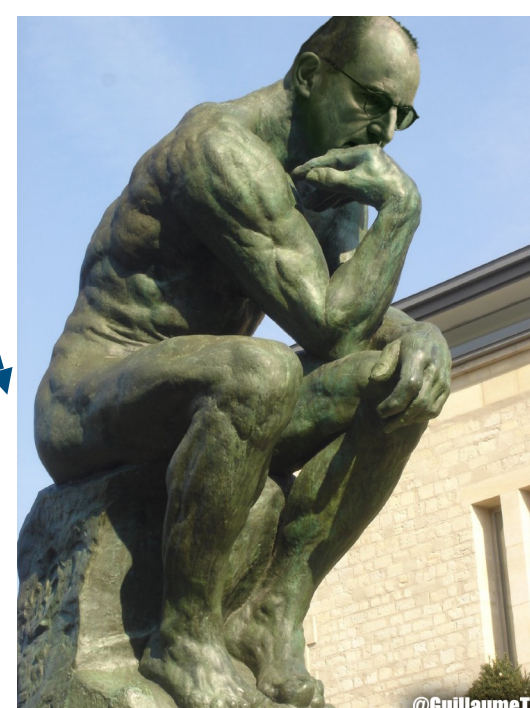


Vote map

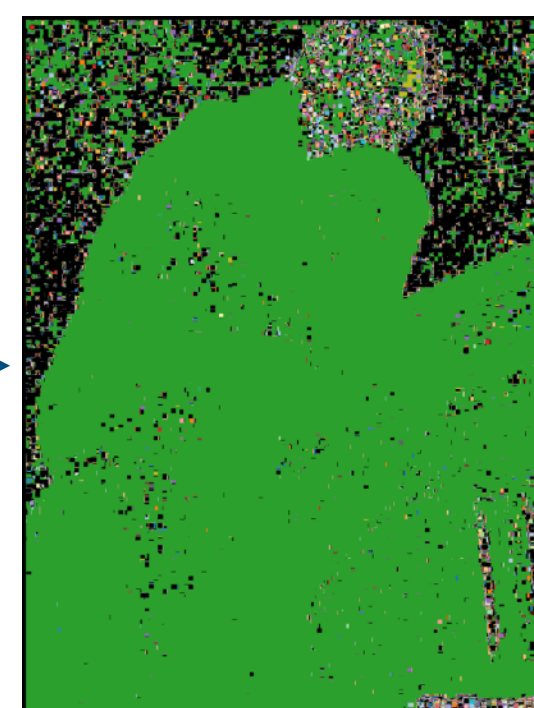


Foreign grid
detection

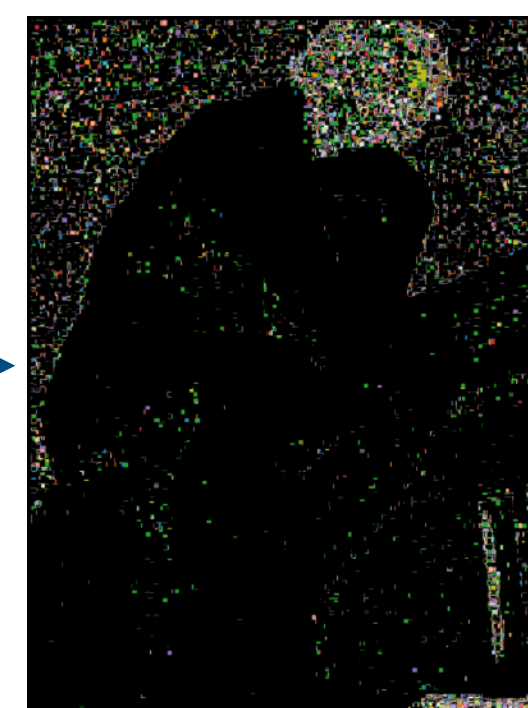
Global grid is (0,0)
and foreign grid
detection



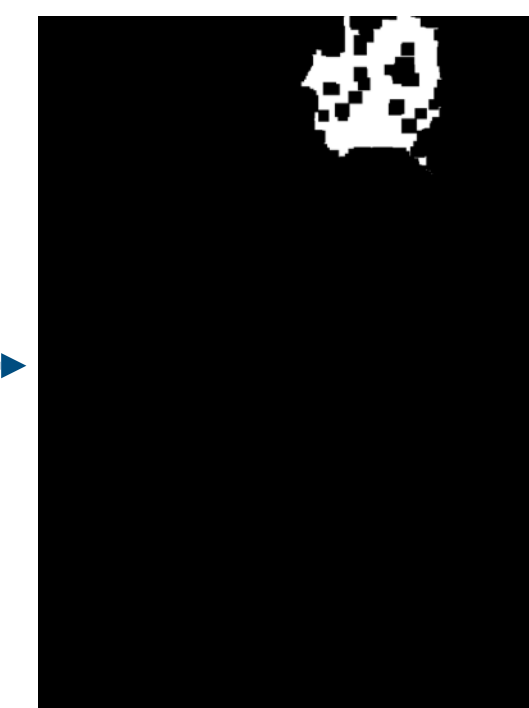
Compressed version
Q=99



Vote map



New vote map



Missing grid
detection



Une boîte à outils améliorée pour détecter les falsifications d'images

 Outils Avancés

Les outils avancés sont déverrouillés

DECONNEXION

 Cette boîte à outils forensic améliorée vise à vous aider à détecter des manipulations dans les images. Vous devriez éviter de l'utiliser avec des captures d'écran, des images scannées de documents ou des images juxtaposées qui, de facto, sont déjà des images manipulées. Plus de filtres mettent en évidence une même zone commune, plus suspecte est cette région particulière de l'image. Veuillez prendre en compte que les filtres forensic mettent en évidence tout type de modifications du signal numérique de l'image et pas seulement des manipulations altérant le sens de l'image (ce qui veut dire qu'il peut y avoir des faux positifs). Certaines textures complexes ou excès de luminance peuvent également modifier le signal sans intention de manipulation. Si possible, utilisez systématiquement la meilleure résolution d'image disponible, au besoin en faisant une recherche inversée d'image.

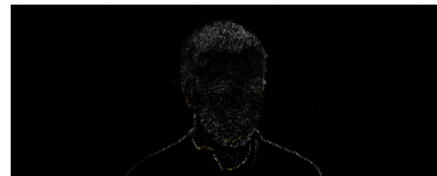
Image analysée ➞

NOUVELLE IMAGE



#CroisonsLes @GuillaumeTC

Amplificateurs



Filtres

COMPRESSION

TRACES

DEEP LEARNING

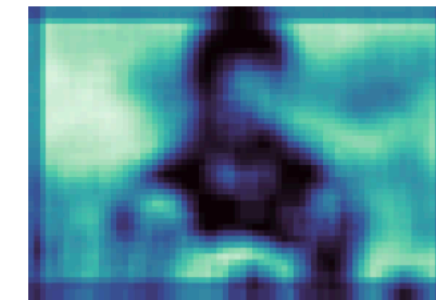
CLONAGE



Zero ②



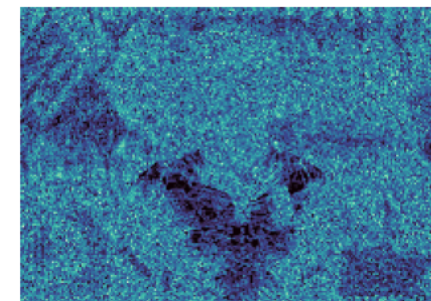
GHOST ?



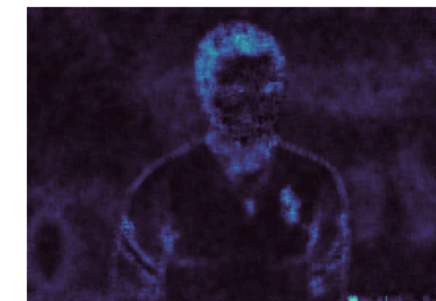
CAGI (?)



DQ ②



DCT (?)



BLOCK ⑦

Pas de détection

Détection

 Passez la souris sur les filtres pour voir un masque transparent avec les résultats sur l'image.

i Ces filtres détectent les anomalies dans les processus antérieurs de création et de compression de l'image. Si un nouvel élément a été supprimé ou ajouté à l'image, il peut être détecté si la zone correspondante a une compression différente du reste de l'image.

- ✓ Combinaison de plusieurs filtres qui mettent en évidence en blanc ou vert pâle une zone commune de l'im



