ROBUSTNESS OF MORPHING ATTACK DETECTION TO COMPRESSION

Richard Marriott

IFPC 2025

03/04/2025

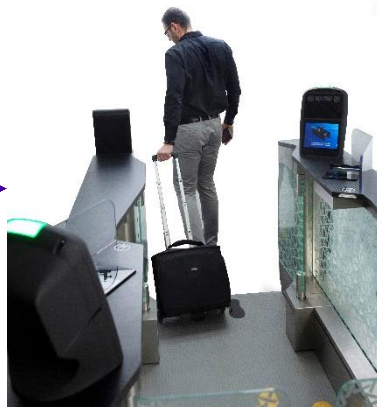
ROBUSTNESS OF S-MAD TO COMPRESSION

Morphing attacks

Accomplice | Morph | Attacker

1) Accomplice succeeds in having the morphed image included in a genuine ID document

2) Attacker uses morphed ID-doc. to gain unauthorised entry



ROBUSTNESS OF S-MAD TO COMPRESSION

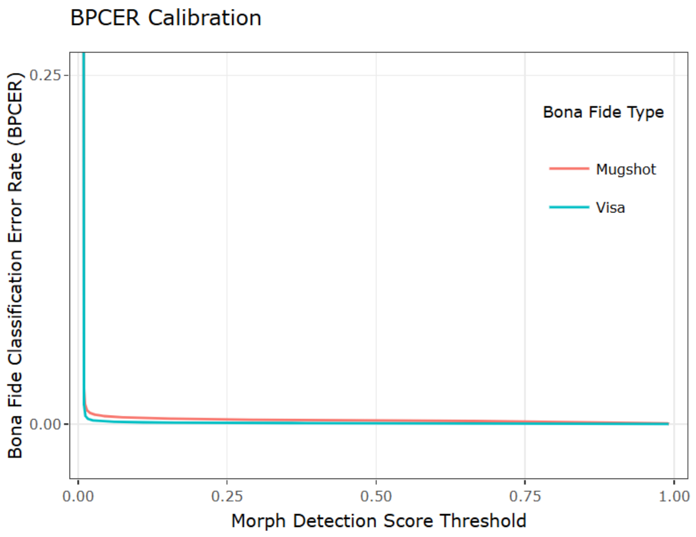
An extreme use case

- At 1100 bytes, we may still be able to recognise faces
- But can we still detect morphs?

ROBUSTNESS OF S-MAD TO COMPRESSION

The study: **algorithm + operational threshold**

Algorithm (+reportcard)	Submission Date	Type	Manual [Tier 3 - High Quality]	Print+Scanned [Tier 3 - High Quality]	Local Morph Colorized Match [Tier 2 - Automated]	Visa-Border [Tier 2 - Automated]	Lincoln [Tier 3 - High Quality]	DST [Tier 3 - High Quality]
idemia_004	2024-12-16	single-image	0.526	0.041	0.000	0.001	0.620	0.626
idemia_002	2024-03-20	differential	0.743	0.455	0.454	0.148	_	_
idemia_003	2024-05-18	differential	0.743	0.179	0.314	0.111	_	_
idemia_001	2024-01-25	differential	0.759	0.440	0.815	0.585	_	_
secunet_003	2025-02-21	differential	0.848	0.433	0.805	0.847	_	_



MACER@BPCER_m=0.003

BPCER_m=0.01 ➔ ~0.015

MACER: Morphing Attack Classification Error Rate (i.e. False Negatives)

(i.e. probability that an attacker will fool the detection algorithm)

BPCER: *Bona fide* Presentation Classification Error Rate (i.e. False Positives)

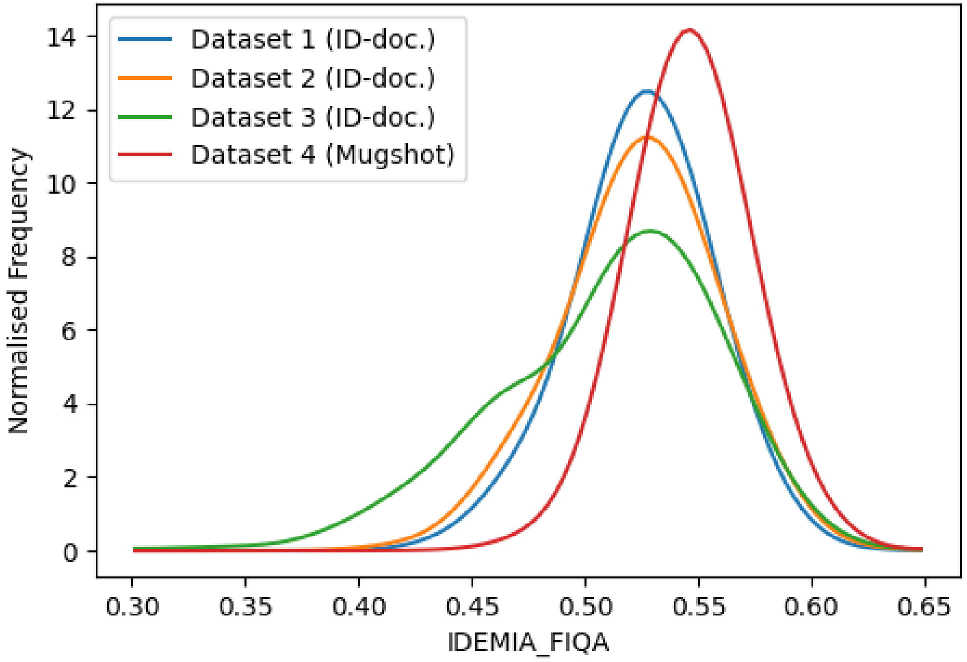
(i.e. probability that a genuine document is rejected due to false morph-detection)

We will use this value as the “operational threshold” throughout this study

ROBUSTNESS OF S-MAD TO COMPRESSION

The study: **datasets + metrics**

Dataset	Image-type	Num. images
Dataset 1	ID-doc.	4619
Dataset 2	ID-doc.	5000
Dataset 3	ID-doc.	5000
Dataset 4	Mugshot	8069



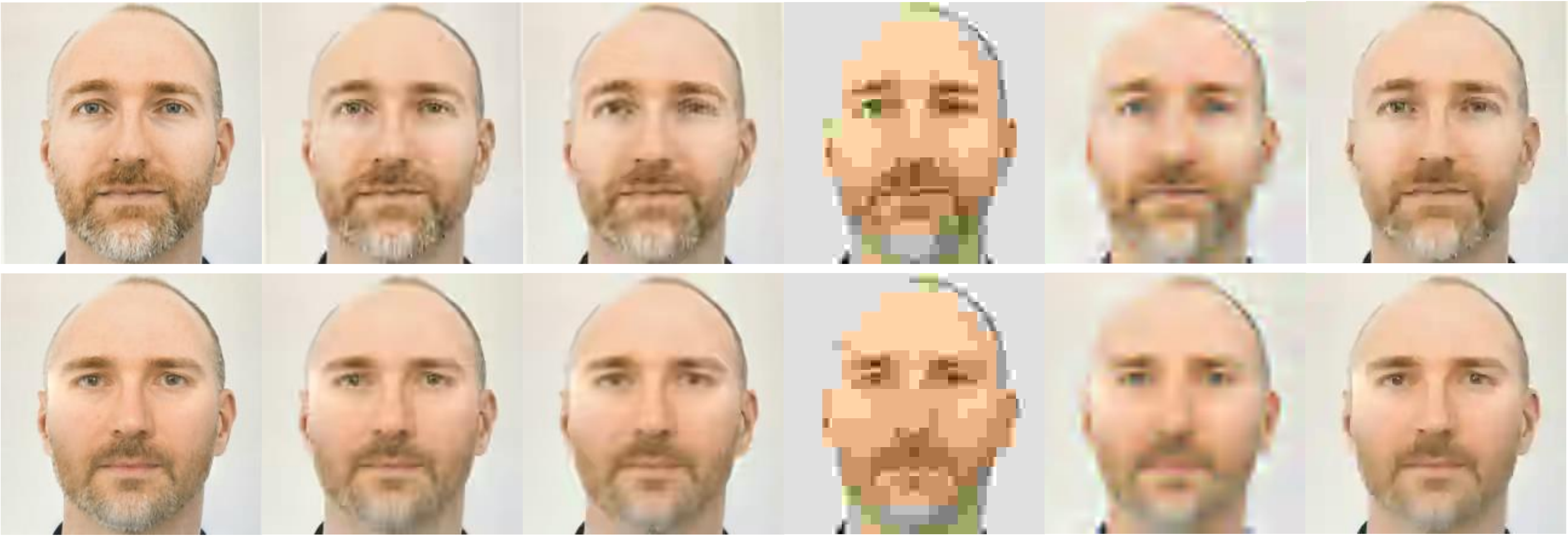
Metrics:

For each of these datasets we will look at the effect of compression on values of...

- MACER@BPCER_m=0.01
- BPCER@BPCER_m=0.01

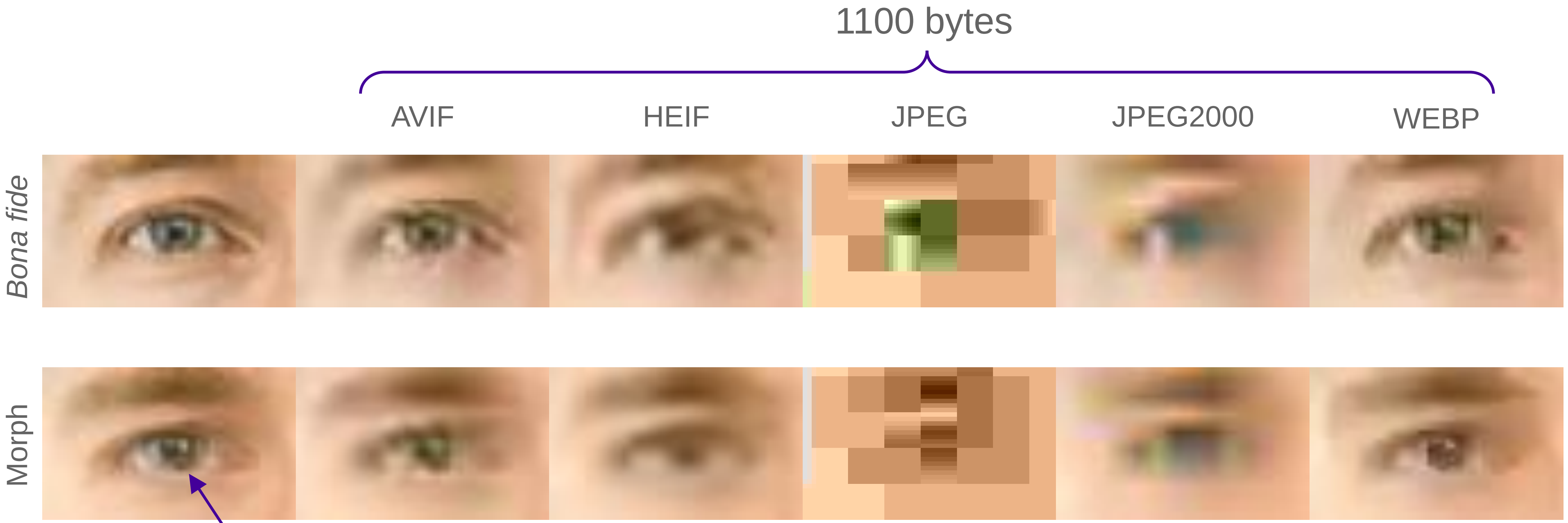
ROBUSTNESS OF S-MAD TO COMPRESSION

The study: **crop + compression types**



ROBUSTNESS OF S-MAD TO COMPRESSION

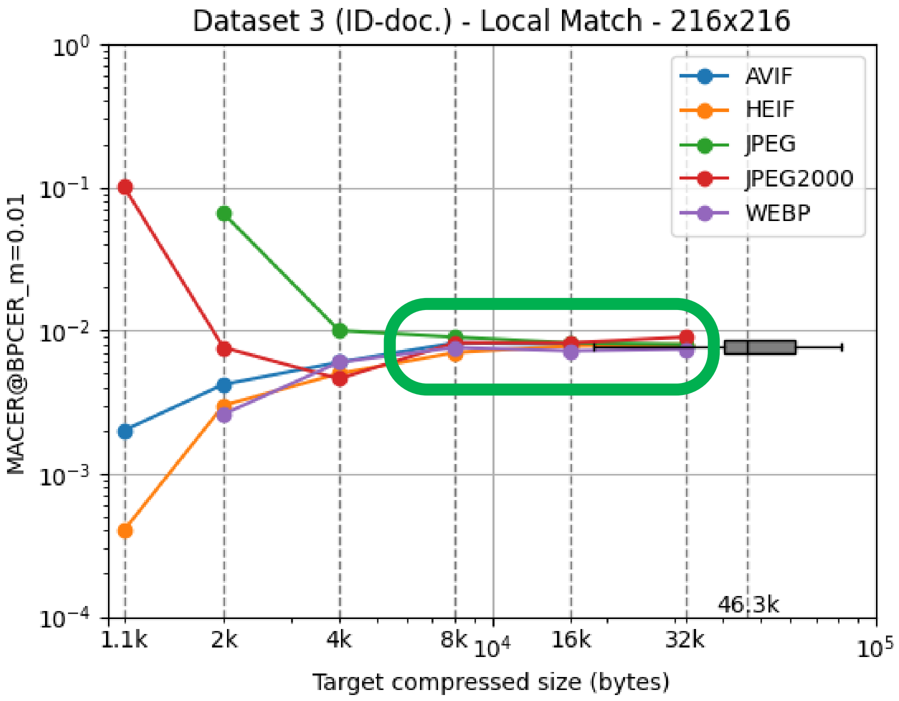
Compression types - zoomed

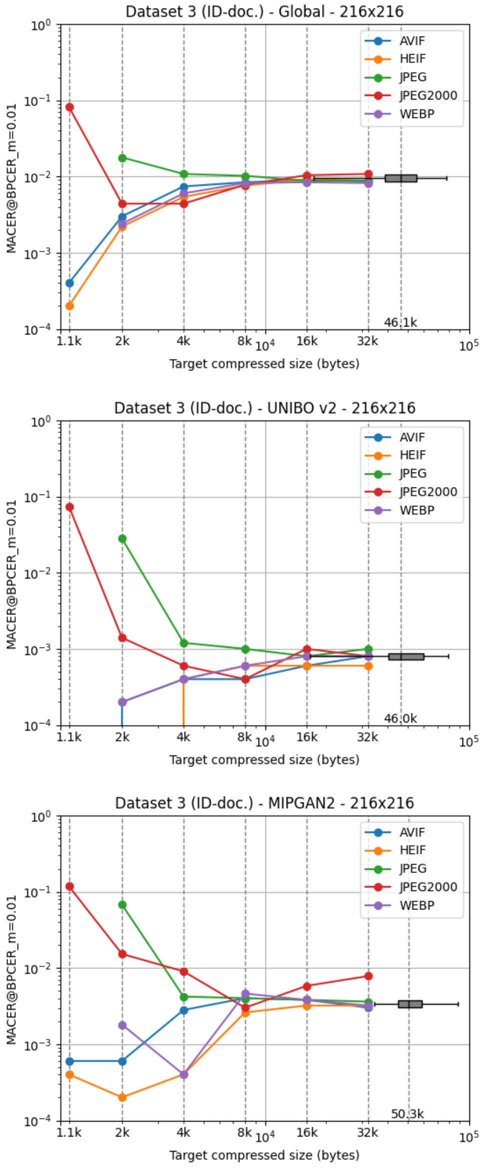


Artifact visible in uncompressed morphed image

ROBUSTNESS OF S-MAD TO COMPRESSION

Does compression obscure morphing artifacts?

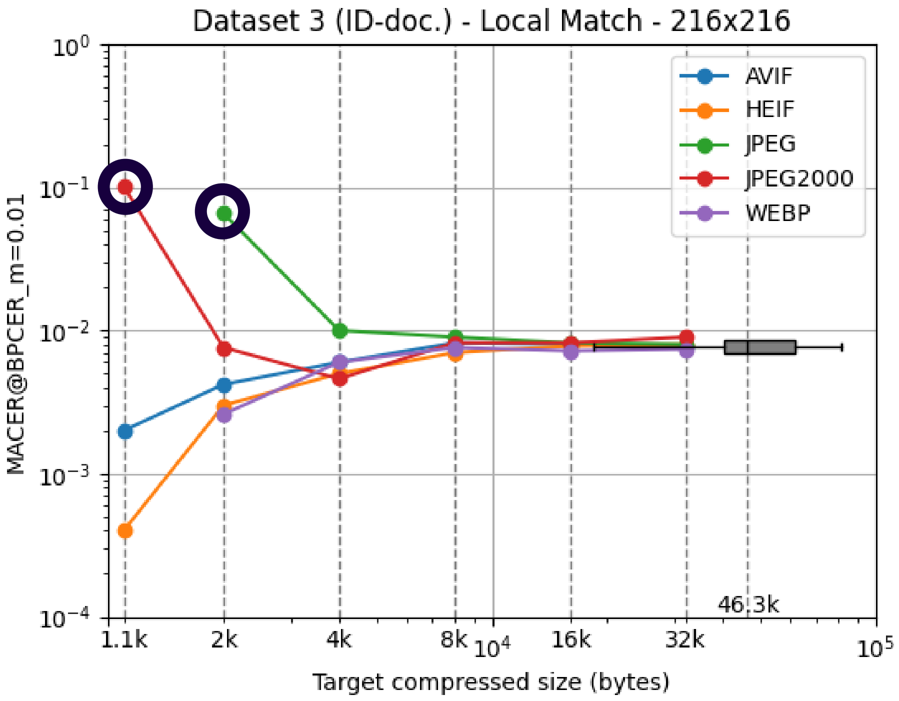


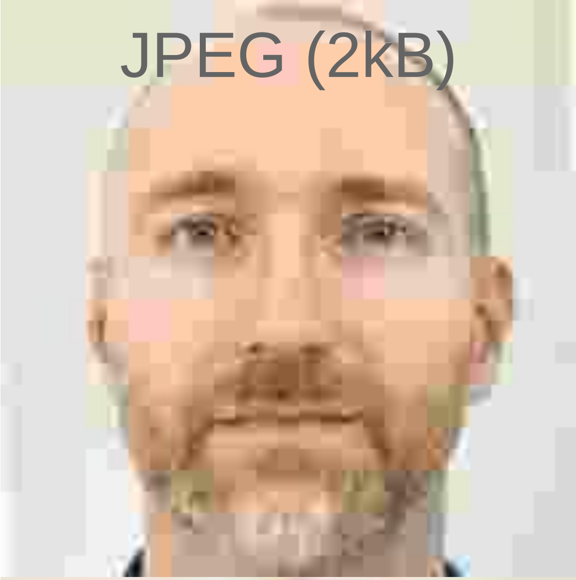


- Light compression does not increase MACER
  - ➢ an attacker can't rely on compression to mask artifacts
- Heavy compression can increase or decrease the rate of detections, depending on the compression type.

ROBUSTNESS OF S-MAD TO COMPRESSION

Does compression obscure morphing artifacts?

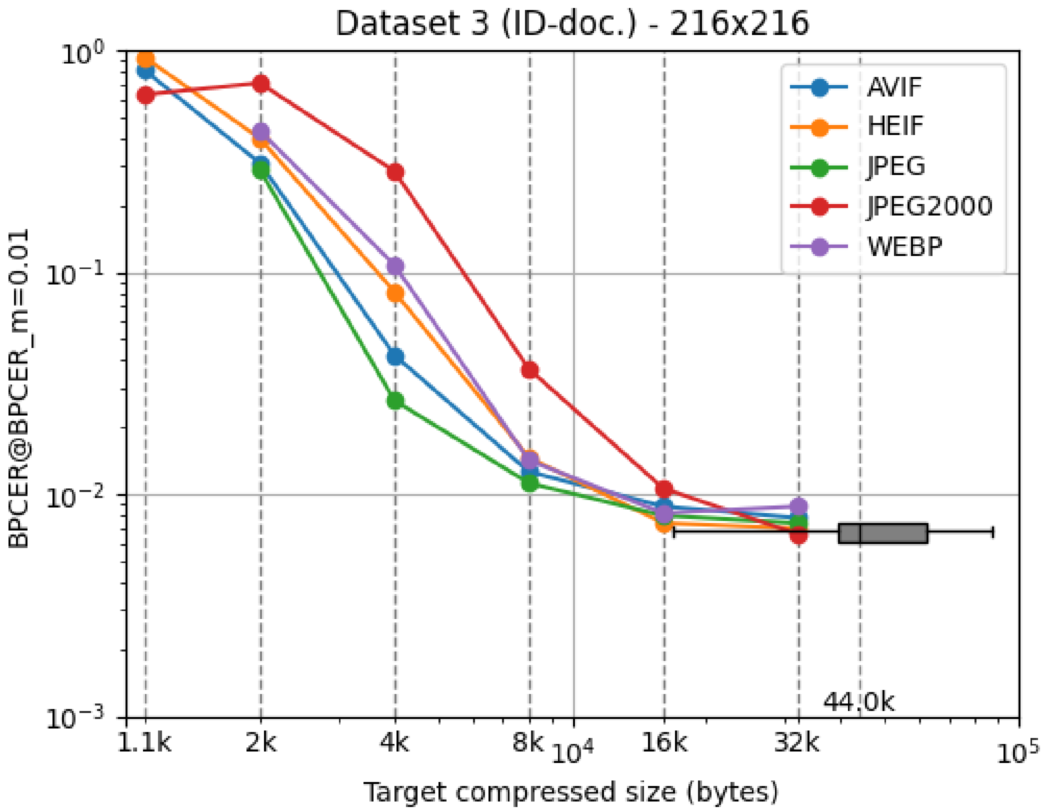


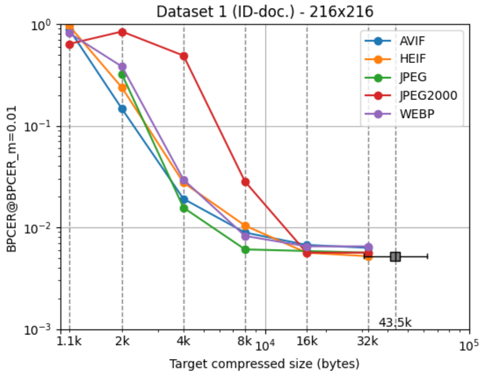


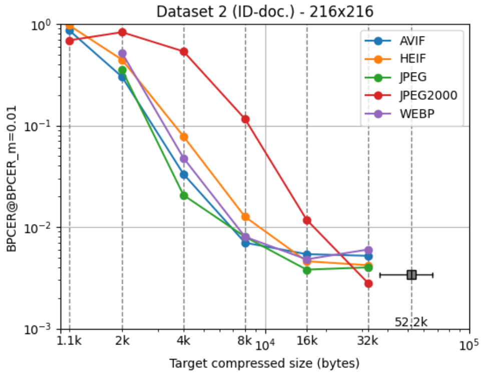
- Light compression does not increase MACER
  - ➢ an attacker can’t rely on compression to mask artifacts
- Heavy compression can increase or decrease the rate of detections, depending on the compression type.

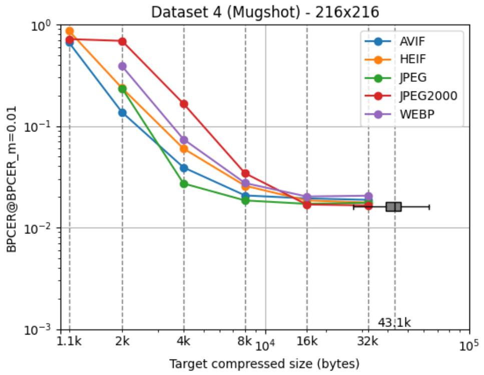
ROBUSTNESS OF S-MAD TO COMPRESSION

How does compression affect false detections?





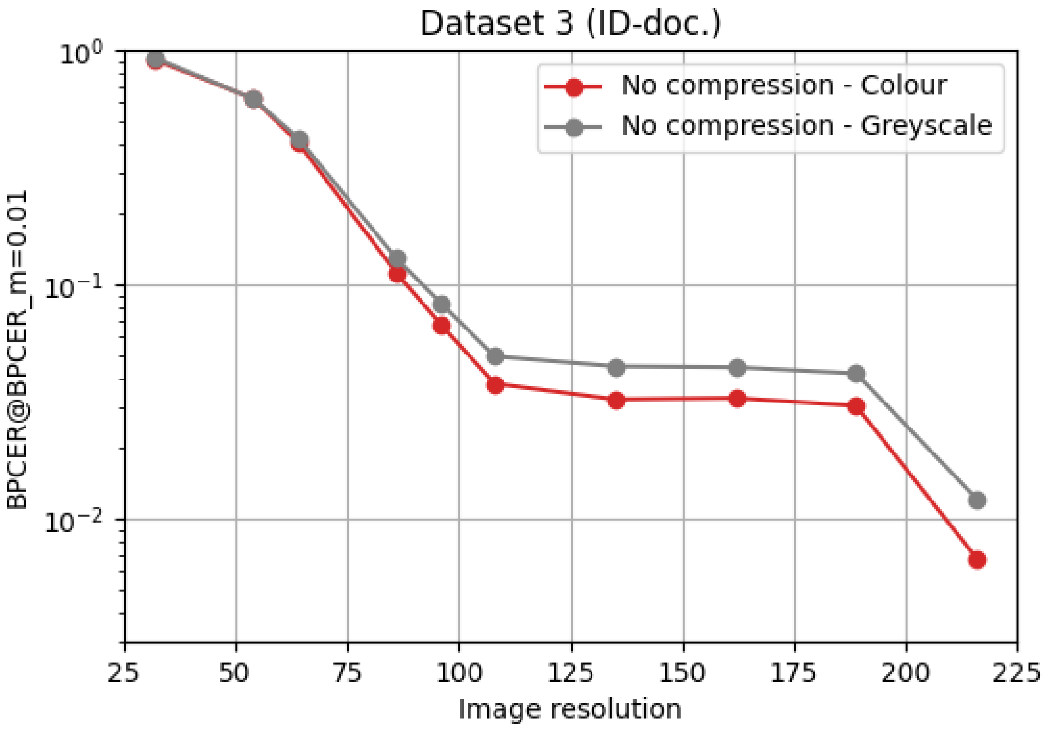




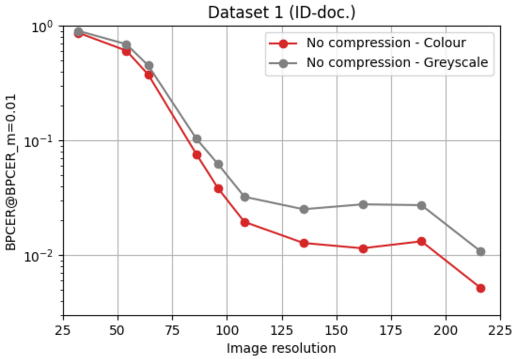
- Lower quality, compressed images cause more false positives
- We can safely compress to around 20kB

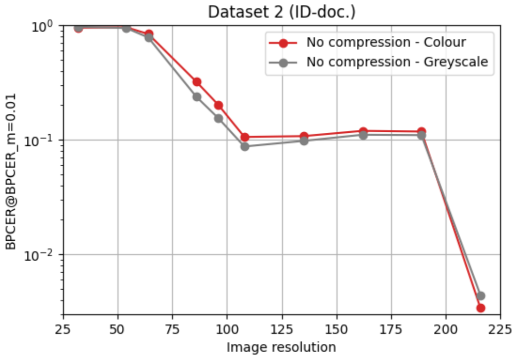
ROBUSTNESS OF S-MAD TO COMPRESSION

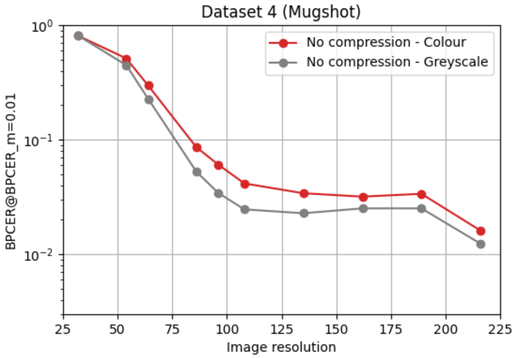
Can we do better by pre-processing images before compression?



Here we see that, even with no compression, pre-processing images increases the BPCER.

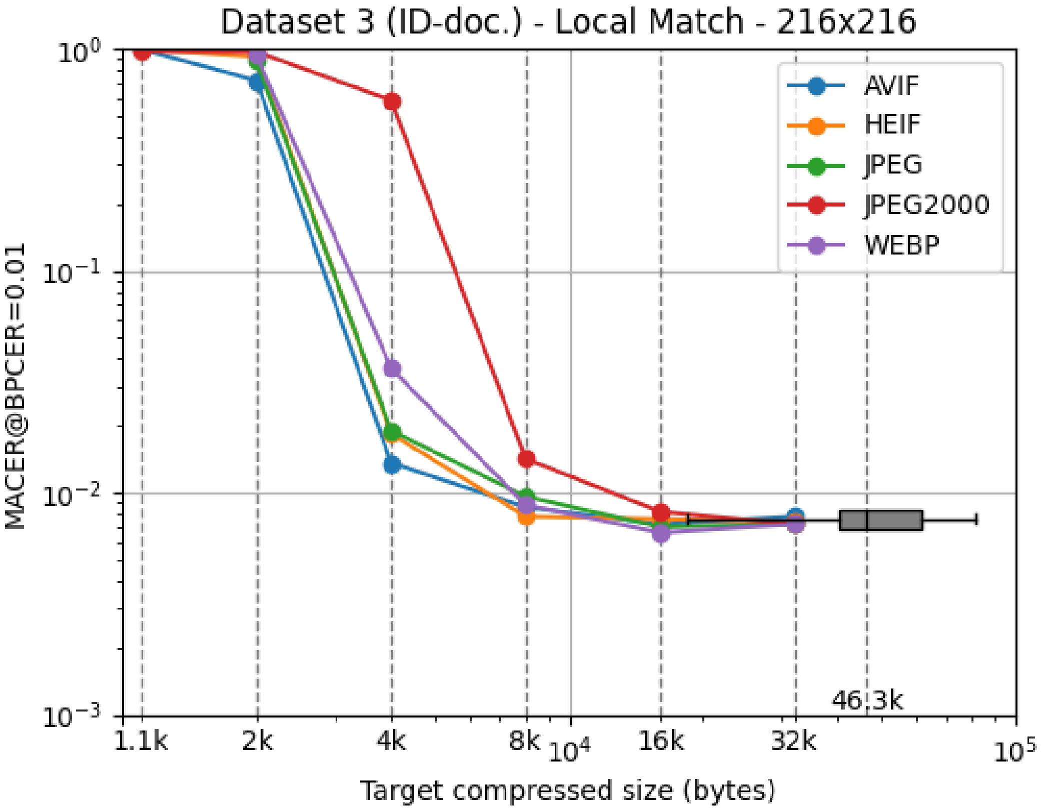


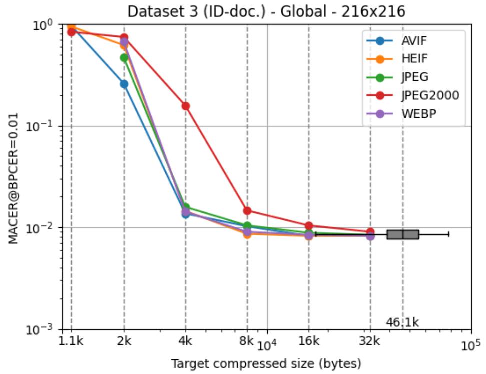


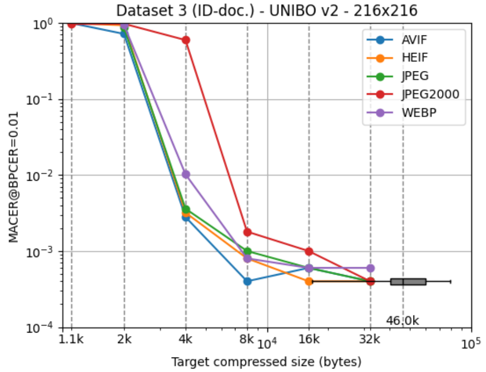


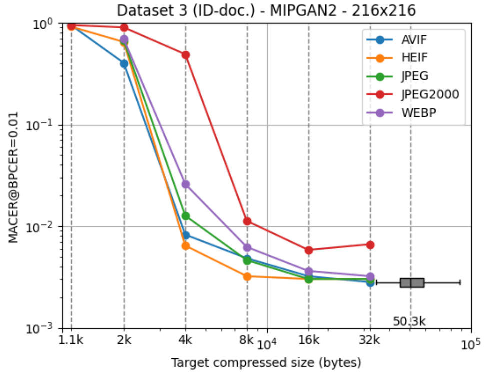
ROBUSTNESS OF S-MAD TO COMPRESSION

Can we maintain performance by adapting the threshold as a function of observed file-size?







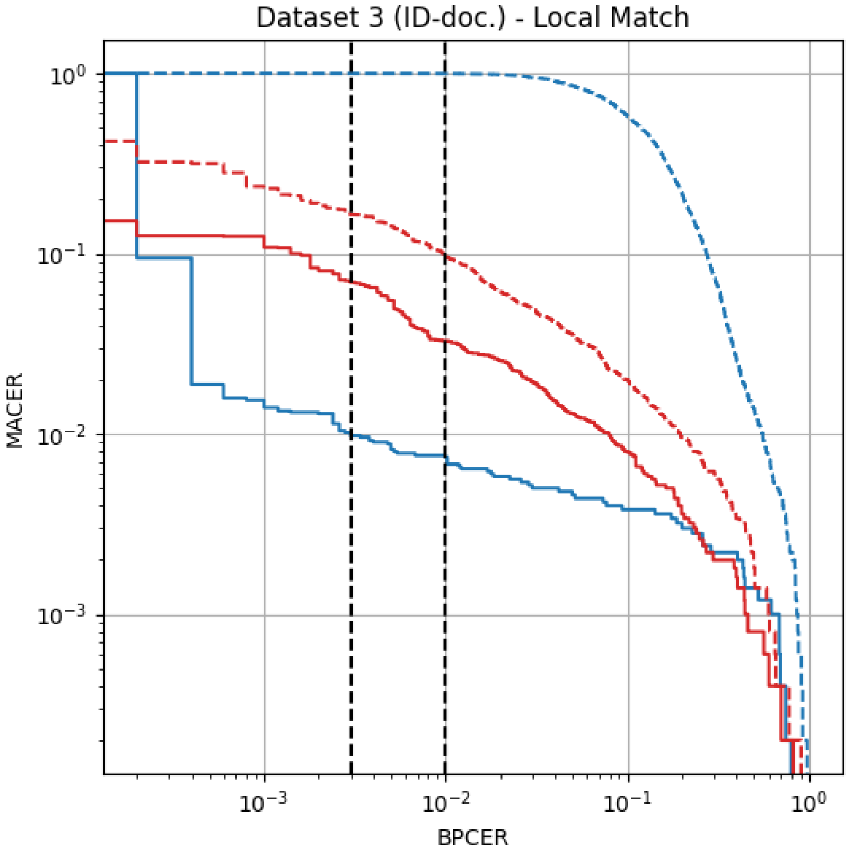


Adapting the threshold based on file-size does not help much to stabilise performance.

ROBUSTNESS OF S-MAD TO COMPRESSION

Preliminary work on improving robustness to compression

We re-trained idemia_004 on images compressed to 1.1kB using AVIF.



_____ idemia_004 (Uncompressed)

_ _ _ idemia_004 (AVIF 1.1kB)

_____ idemia_004_AVIF (Uncompressed)

_ _ _ idemia_004_AVIF (AVIF 1.1kB)

We see that performance can be improved by re-training but that it is still far from base levels.

ROBUSTNESS OF S-MAD TO COMPRESSION

Conclusions and recommendations

Conclusions:

- Compression to 1.1kB is too extreme for morph detection
  - ➢ QR codes should only be used for securely captured images
- Compression can hide morphing artifacts but also triggers increased numbers of detections (whether images are morphs or *bona fide*)
  - ➢ An attacker therefore cannot use compression to evade detection
- Performance for heavily compressed images can be improved by specialised training but is still far from base levels

- **Recommendations:**
  - Compression should not be < ~20kB (for crop 216x216, IED=70px)
  - AVIF, HEIF and WEBP formats are preferable to JPEG and JPEG2000