AUTHOR GUIDELINES FOR ICIP 2017 PROCEEDINGS MANUSCRIPTS

Author(s) Name(s)

Author Affiliation(s)

ABSTRACT

The abstract should appear at the top of the left-hand column of text, about 0.5 inch (12 mm) below the title area and no more than 3.125 inches (80 mm) in length. Leave a 0.5 inch (12 mm) space between the end of the abstract and the beginning of the main text. The abstract should contain about 100 to 150 words, and should be identical to the abstract text submitted electronically along with the paper cover sheet. All manuscripts must be in English, printed in black ink.

***Index Terms*—** One, two, three, four, five

1. INTRODUCTION

More and more content is being shared everyday on the internet. Most of this content is trivial and does not need to be encrypted. Some of it however needs to be securely transfered, the problem of encryption arises. Full encryption with methods such as AES for exemple are often not needed in addition to not being possible due to computing power constraints. Instead, partial or selective encryption is used, where the goal is sufficient encryption. That is, the image is sufficently distorted and an attacker is not able to access the content. This distortion can be of varying magnitude, a strong distortion for exemple for DRM, or a lighter distortion, where the content is still recognizable to attract the viewers interest. *TODO : encryption state of the art*.

When an image is intented to be consumed by a human, the most accurate measure of its confidentiality is a Mean Opinion Score, where actual people rate the image. It is however not a realistic way to rate the distortion of an image as it is way to expensive and time consuming, security and quality metrics were introduced as a means to automate the process.

According to [**?**], there is not yet a security metric that consistently rates images across all the MOS spectrum. Most quality metrics fail to predict a MOS on low quality images, precisely where it would be most important to do so : decide whether an image is confidential.

We give a quick overview of a few selected metrics. For a more in-depth review, we refer the reader to [**?**].

PSNR : Even though it is known that the PSNR is not well correlated with human judgment, it is still widely used due to its speed and ease of use. The range is [0; $+\infty$], where two identical images would have a PSNR of $+\infty$.

SSIM : [**?**](Structural Similarity Index Measure). A luminance score, au contrast score and a structure score are combined to obtain the actual SSIM score. It has a range of [0;1] where identical images have a score of 1.

ESS : [**?**](Edge Similarity Score). It uses non overlapping 8x8 block directions to compare images. With the range [0;1], a higher score reflects a less distorted image.

LSS : [**?**](Luminance Similarity Score). It uses non overlapping 8x8 block average luminance to compare images. With the range [-8.5; 1] for default parameters of $\alpha = 0.1$ and $\beta = 3$, a higher score reflects a less distorted image.

NPCR : [**?**]It is the number of pixel changes between images. Its range is [0;100], where a fully encrypted image has a NPCR close to 100, where almost all the pixels changed.

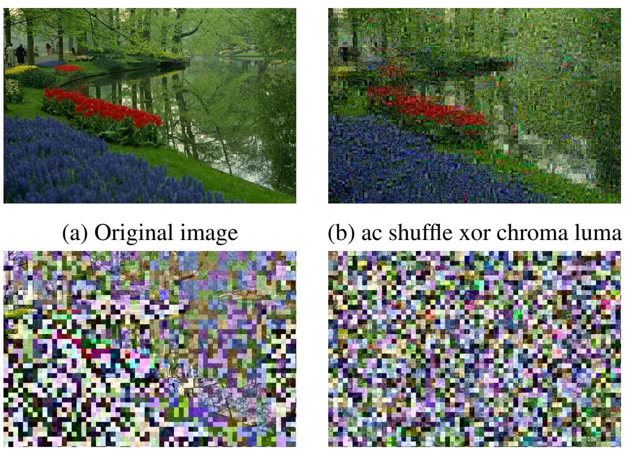
UACI : [**?**]It is the unified averaged changed intensity. It is the average intensity difference between two images. Its range is [0;100], where a fully encrypted image has a value close to 33.

Entropy : It is the amount of information in an image, for an 8-bit image, so an entropy of 8 would be the target for a full encryption method. It ranges from 0 to 8 in this case.

Correlation : The correlation coefficient ranges from 0 to 1, it is the average correlation of adjacent pixels in an image, where a natural image would be highly correlated and a fully encrypted image would have low correlation.

2. CREATING THE DATASET

The cryptocompression method we use is targeted towards JPEG images. We have six parameters that we can enable or not to generate a cryptocompressed image. *Shuffle* and *xor* are the parameters that decide de actual encryption method. *AC* and *DC* control which part of the DCT will be encrypted and two additionnal parameters, *chrominance* and *luminance* decide which of the luminance, chrominance (or both) DCT coefficients will be encrypted. As there must be at least one encryption method, at least one type of coefficient, and chrominance or luminance selected, we have a total of 27 distortions with their different parameters. The distortions range from completely indecipherable images to almost invisible perturbations, as shown in Fig. 1. This way, we hope to have appropriate distortions for different use cases



(a) Original image

(b) ac shuffle xor chroma luma

(c) dc xor chroma luma

(d) All six parameters

Fig. 1: Example of different distortions

Explain shuffle and xor and maybe link Vincent's paper. We use the training images from the BSDS500 [**?**] dataset as our input images for a total of $27 * 200 = 5400$ cryptocompressed images.

The 27 distortions are given in Appendix A, they are named according to the parameters enabled and are sorted by MOS, as explained in Section 3, they are later designated by their number for ease of use.

3. IMAGE EVALUATION

We had a total of *N* different person do the evaluation. They had to give a score from 1 to 5 to the images, where 5 is the best score and 1 is the worst, presented as follows :

1 : The distortion is unbearable, nothing is visible
2 : The distortion is very annoying, I can barely guess the content
3 : The distortion is annoying, but I can see the content
4 : The distortion is slightly annoying, but the content is clear
5 : The distortion is not annoying at all

They had to rate 81 images, three for every distortion, the sessions were 10 to 15 minutes long, depending on the person. Each image was seen at most once by the user, to prevent them from recognising it and give it a higher score. The distortions order was shuffled differently for every evaluation and repeated three times in the same order. We chose to have every distortion rated three times because during our preliminary tests, we saw that for the first few images, the user was not confident on the score to give to an image, confidence that improved as they saw more images and distortion. It allowed us to filter the outliers caused by the learning curve while still having a good amount of rating.

The images were evaluated in a dim room, on a *details of the screen* screen, about n meters away and around eyes level. The user could only see one image at a time, a new image shown once the previous had been rated. The MOS obtained during the evaluation are given Fig. 2. The name of the distortions are given in Appendix A. We can see that after distortions 17, the MOS get marginally better, this is due to the absence of the parameter $luminance$, the $shuffle$ and xor are only performed on the chrominance, hence the better ratings.

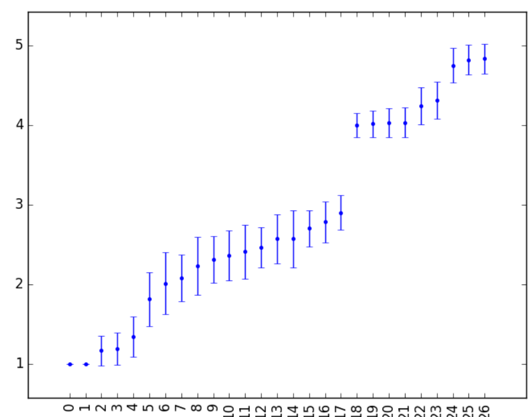


Fig. 2: MOS for the 27 distortions.

Our goal is to predict the rating a human would give to an image. In the best case scenario, a metric would be totally correlated with human rating and could be used to completely replace humans in image evaluation, this is however not the case, at least not for the metrics we selected, as shown in figures 3 and 4. Detailed results are available Table 1

As we can se from these figures, most metrics actually follow a rough line, but distortions 5 to 17 are problematic and prevent us from predicting the MOS. These distortions also happen to be between a MOS of 2 and 3, where the threshold for a confidential image would be. Even the SSIM, which is the most accurate metric in our experiment, fails to predict the MOS, as shown in Fig. 5. The SSIM ranges from 0 to 1, and

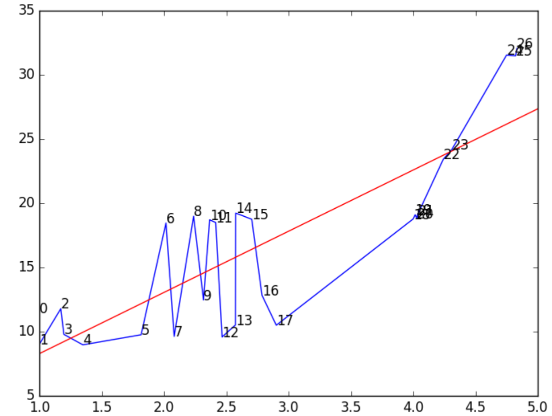


Fig. 3: MOS on the x-axis and PSNR on the y-axis

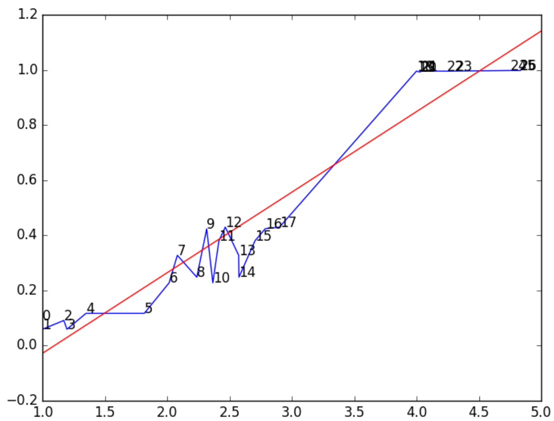


Fig. 4: MOS on the x-axis and SSIM on the y-axis

from Fig. 5, we can see that for the same MOS the SSIM goes across almost all its range. A similar behavior is seen for the other metrics. Table 1 summarizes our results.

A. DISTORTIONS

0. ac_dc_shuffle_chrominance_luminance
1. ac_dc_shuffle_xor_chrominance_luminance
2. ac_dc_shuffle_luminance
3. ac_dc_shuffle_xor_luminance
4. ac_dc_xor_chrominance_luminance
5. ac_dc_xor_luminance
6. ac_shuffle_xor_chrominance_luminance
7. dc_shuffle_xor_chrominance_luminance
8. ac_shuffle_chrominance_luminance
9. dc_shuffle_chrominance_luminance
10. ac_shuffle_xor_luminance
11. ac_xor_chrominance_luminance
12. dc_xor_chrominance_luminance
13. dc_shuffle_xor_luminance
14. ac_shuffle_luminance

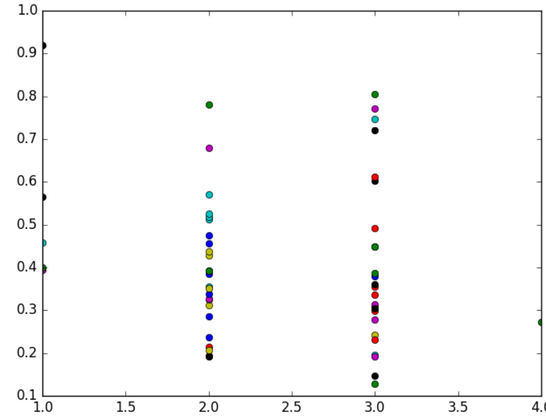


Fig. 5: Details of the MOS on the x-axis and the SSIM on the y-axis for the 11^{th} distortion

15. ac_xor_luminance
16. dc_shuffle_luminance
17. dc_xor_luminance
18. ac_dc_xor_chrominance
19. dc_shuffle_xor_chrominance
20. ac_dc_shuffle_xor_chrominance
21. dc_xor_chrominance
22. ac_dc_shuffle_chrominance
23. dc_shuffle_chrominance
24. ac_xor_chrominance
25. ac_shuffle_xor_chrominance
26. ac_shuffle_chrominance

index	MOS	psnr	entropy	corr_horiz	corr_vert	uaci	npcr	ssim	lss	ess
0	1.0 (0.0)	11.45 (2.72)	7.31 (0.39)	0.82 (0.05)	0.82 (0.05)	21.99 (6.42)	99.05 (0.73)	0.09 (0.07)	-1.43 (0.52)	0.56 (0.2)
1	1.0 (0.0)	9.02 (1.93)	7.69 (0.16)	0.84 (0.04)	0.84 (0.04)	29.32 (6.34)	99.46 (0.18)	0.06 (0.04)	-1.88 (0.57)	0.56 (0.19)
2	1.17 (0.38)	11.79 (2.82)	7.31 (0.39)	0.82 (0.05)	0.82 (0.05)	21.19 (6.46)	98.84 (1.19)	0.09 (0.07)	-1.43 (0.52)	0.56 (0.2)
3	1.2 (0.4)	9.79 (2.38)	7.62 (0.23)	0.83 (0.04)	0.83 (0.05)	27.03 (6.75)	99.31 (0.38)	0.06 (0.04)	-1.88 (0.57)	0.57 (0.19)
4	1.35 (0.51)	8.97 (1.97)	7.7 (0.19)	0.84 (0.04)	0.84 (0.04)	27.33 (6.32)	99.09 (0.31)	0.12 (0.09)	-1.6 (0.57)	0.62 (0.2)
5	1.82 (0.67)	9.76 (2.42)	7.6 (0.27)	0.83 (0.05)	0.83 (0.04)	24.22 (6.68)	98.46 (0.95)	0.12 (0.09)	-1.6 (0.57)	0.63 (0.19)
6	2.02 (0.78)	18.46 (3.04)	7.3 (0.41)	0.87 (0.07)	0.88 (0.07)	9.12 (3.17)	96.41 (3.52)	0.23 (0.12)	0.16 (0.2)	0.58 (0.18)
7	2.08 (0.58)	9.63 (2.14)	7.69 (0.18)	0.86 (0.03)	0.86 (0.03)	27.3 (6.51)	99.35 (0.23)	0.33 (0.13)	-1.84 (0.55)	0.73 (0.16)
8	2.24 (0.73)	18.99 (3.09)	7.27 (0.42)	0.89 (0.06)	0.89 (0.06)	8.57 (3.02)	96.24 (3.59)	0.25 (0.13)	0.18 (0.2)	0.58 (0.19)
9	2.32 (0.59)	12.47 (3.03)	7.3 (0.4)	0.83 (0.04)	0.84 (0.04)	19.59 (6.28)	98.76 (0.9)	0.42 (0.14)	-1.38 (0.51)	0.74 (0.16)
10	2.37 (0.63)	18.71 (3.13)	7.28 (0.42)	0.87 (0.07)	0.87 (0.07)	8.84 (3.19)	95.83 (4.29)	0.23 (0.12)	0.16 (0.2)	0.58 (0.18)
11	2.42 (0.68)	18.5 (3.03)	7.18 (0.48)	0.87 (0.07)	0.88 (0.07)	7.74 (2.99)	93.26 (5.3)	0.38 (0.16)	0.34 (0.22)	0.65 (0.18)
12	2.47 (0.5)	9.58 (2.17)	7.7 (0.2)	0.86 (0.03)	0.86 (0.03)	24.47 (6.36)	98.47 (0.5)	0.43 (0.14)	-1.54 (0.57)	0.74 (0.15)
13	2.57 (0.61)	10.52 (2.67)	7.6 (0.25)	0.85 (0.03)	0.85 (0.03)	24.89 (6.89)	99.04 (0.5)	0.33 (0.13)	-1.84 (0.55)	0.73 (0.15)
14	2.58 (0.72)	19.24 (3.17)	7.26 (0.43)	0.89 (0.06)	0.89 (0.06)	8.31 (3.03)	95.67 (4.37)	0.25 (0.13)	0.18 (0.2)	0.58 (0.18)
15	2.7 (0.46)	18.75 (3.11)	7.16 (0.49)	0.87 (0.07)	0.88 (0.07)	7.4 (2.99)	91.91 (6.31)	0.38 (0.16)	0.34 (0.22)	0.66 (0.18)
16	2.79 (0.52)	12.84 (3.13)	7.28 (0.41)	0.84 (0.04)	0.84 (0.04)	18.76 (6.29)	98.31 (1.48)	0.42 (0.14)	-1.38 (0.51)	0.75 (0.15)
17	2.9 (0.43)	10.5 (2.71)	7.59 (0.29)	0.85 (0.03)	0.85 (0.03)	20.78 (6.65)	96.08 (1.75)	0.43 (0.14)	-1.54 (0.57)	0.74 (0.15)
18	4.0 (0.31)	18.77 (3.9)	7.35 (0.37)	0.94 (0.04)	0.94 (0.04)	7.91 (3.4)	93.51 (3.95)	1.0 (0.01)	0.95 (0.08)	0.86 (0.1)
19	4.02 (0.34)	19.11 (4.1)	7.38 (0.35)	0.94 (0.04)	0.94 (0.04)	8.6 (3.72)	95.79 (3.12)	0.99 (0.01)	0.93 (0.1)	0.86 (0.1)
20	4.03 (0.36)	18.79 (3.93)	7.39 (0.34)	0.94 (0.04)	0.94 (0.04)	8.9 (3.74)	96.2 (2.89)	0.99 (0.01)	0.92 (0.1)	0.86 (0.1)
21	4.03 (0.37)	19.08 (4.08)	7.34 (0.38)	0.94 (0.04)	0.94 (0.04)	7.48 (3.33)	91.2 (4.87)	1.0 (0.01)	0.95 (0.07)	0.86 (0.1)
22	4.24 (0.46)	23.42 (4.04)	7.21 (0.44)	0.93 (0.05)	0.93 (0.05)	5.17 (2.26)	93.73 (3.84)	1.0 (0.01)	0.94 (0.08)	0.86 (0.1)
23	4.31 (0.46)	24.2 (4.26)	7.21 (0.45)	0.93 (0.05)	0.93 (0.05)	4.75 (2.18)	92.69 (4.34)	1.0 (0.01)	0.95 (0.07)	0.86 (0.09)
24	4.75 (0.43)	31.54 (3.66)	7.12 (0.5)	0.93 (0.05)	0.93 (0.05)	1.57 (0.7)	75.75 (10.71)	1.0 (0.0)	0.99 (0.03)	0.87 (0.09)
25	4.82 (0.38)	31.48 (3.71)	7.14 (0.48)	0.93 (0.05)	0.93 (0.05)	1.84 (0.83)	81.63 (9.59)	1.0 (0.0)	0.98 (0.04)	0.86 (0.1)
26	4.83 (0.37)	32.06 (3.75)	7.13 (0.49)	0.93 (0.05)	0.93 (0.05)	1.72 (0.79)	80.68 (10.02)	1.0 (0.0)	0.99 (0.03)	0.86 (0.1)

Table 1: Results for the 27 distortions

B. REFERENCES

[1] A.B. Smith, C.D. Jones, and E.F. Roberts, "Article title," *Journal*, vol. 62, pp. 291–294, January 1920.

[2] C.D. Jones, A.B. Smith, and E.F. Roberts, "Article title," in *Proceedings Title*. IEEE, 2003, vol. II, pp. 803–806.