Directed Energy Research Centre

# Digital Images Preprocessing for Optical Character Recognition in Video Frames Reconstructed from Compromising Electromagnetic Emanations from Video Cables

**Santiago Morales-Aguilar**

**August, 2020**

Technology Innovation Institute

# Agenda

Directed Energy Research Centre

1. Review of TEMPEST Emanations in the VGA Interface
2. Description of the Strategy
   a) Initial Setup
   b) Image Preprocessing Stage
   c) Text Recognition and Evaluation
   d) Optimization with Evolution Strategy
3. Results
4. Conclusions and Future Work
5. References

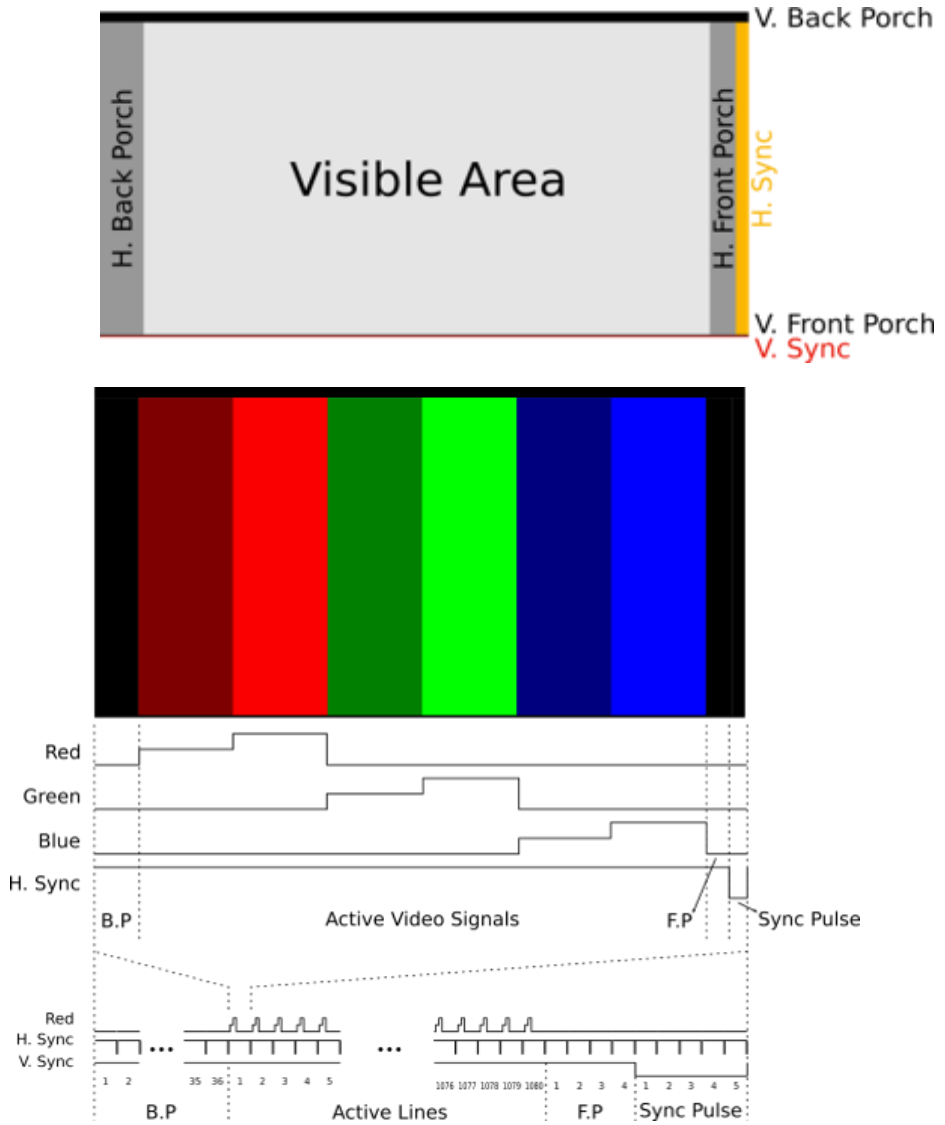
# Review of TEMPEST Emanations in the VGA Interface (1)

Video interfaces such as VGA, HDMI, or DVI transmit video information through cables from a computer to an external display monitor. These signals propagate unintended electromagnetic emanations (a.k.a. TEMPEST emanations) that can be captured and processed to recover video frames.

The VGA interface defines analog signals (ranging from 0 to 0.7 V) separated into three different channels (red, green, and blue) at a fixed frequency (dependent on the screen resolution) to transmit pixel information.

Blanking intervals (called porches) and synchronization pulses (on additional TTL channels) are needed to keep the video transmitter and receiver coordinated.

For FHD (1920x1080) @60Hz, the pixel frequency is 148.5 MHz, 2200 pixels are transmitted per line, and 1125 lines are transmitted per frame.

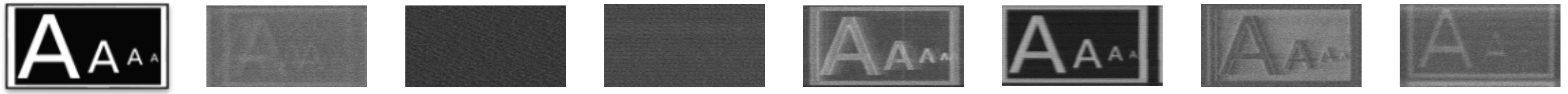


# Review of TEMPEST Emanations in the VGA Interface (2)

Directed Energy Research Centre

Unintended electromagnetic emanations produced by video interfaces can be captured across the spectrum. For example, for the case of a VGA interface transmitting FHD resolution at 60 Hz, TEMPEST emanations can be found at 148, 592, 740, 888, and 1036 MHz (probably at higher frequencies frames can also be reconstructed).

These frequencies are harmonics of the pixel frequency. At 296 and 444 MHz, the frames cannot be recovered, probably due to electromagnetic interference.



Reference | 148 MHz | 296 MHz | 444 MHz | 592 MHz | 740 MHz | 888 MHz | 1036 MHz

# Review of TEMPEST Emanations in the VGA Interface (3)

Directed Energy Research Centre

Software-defined radios (SDRs) are suitable devices to recover video frames, because they are flexible, have the bandwidth to recover enough information (or part of it), and can be tuned to a wide range of frequencies. The process for recovering video frames from TEMPEST emanations is described as follows:

- Tune the SDR to a frequency where information exists to apply the reconstruction.
- Mix, downconvert, and filter the baseband signal for further processing.
- Apply amplitude demodulation to the downconverted samples (the baseband signal).
- Resample to adjust the samples to the required greater quantity of pixels.
- Apply post-processing techniques such as anti-aliasing, auto gain, and frame averaging.
- Find and adjust the beginning of the frame.

# Description of the Strategy

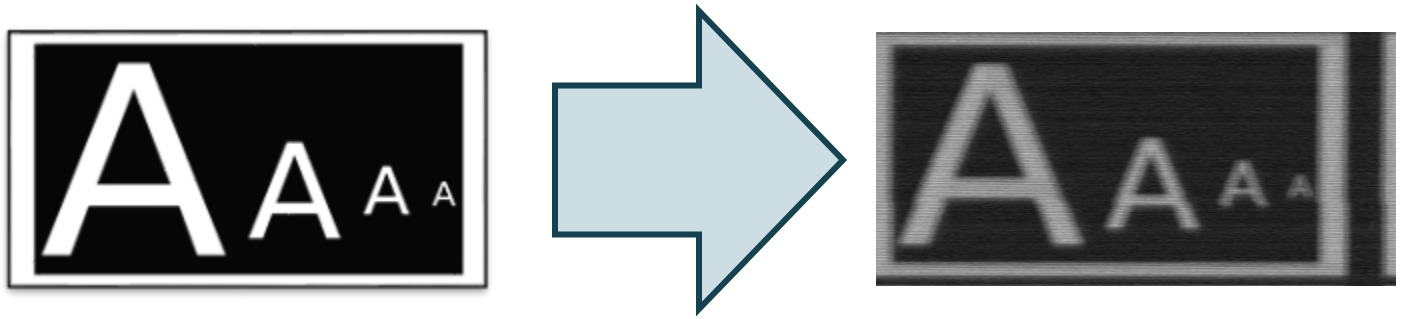
There are limitations in frames reconstruction:

The reconstructed frame is noisy and blurred.

Color cannot be retrieved

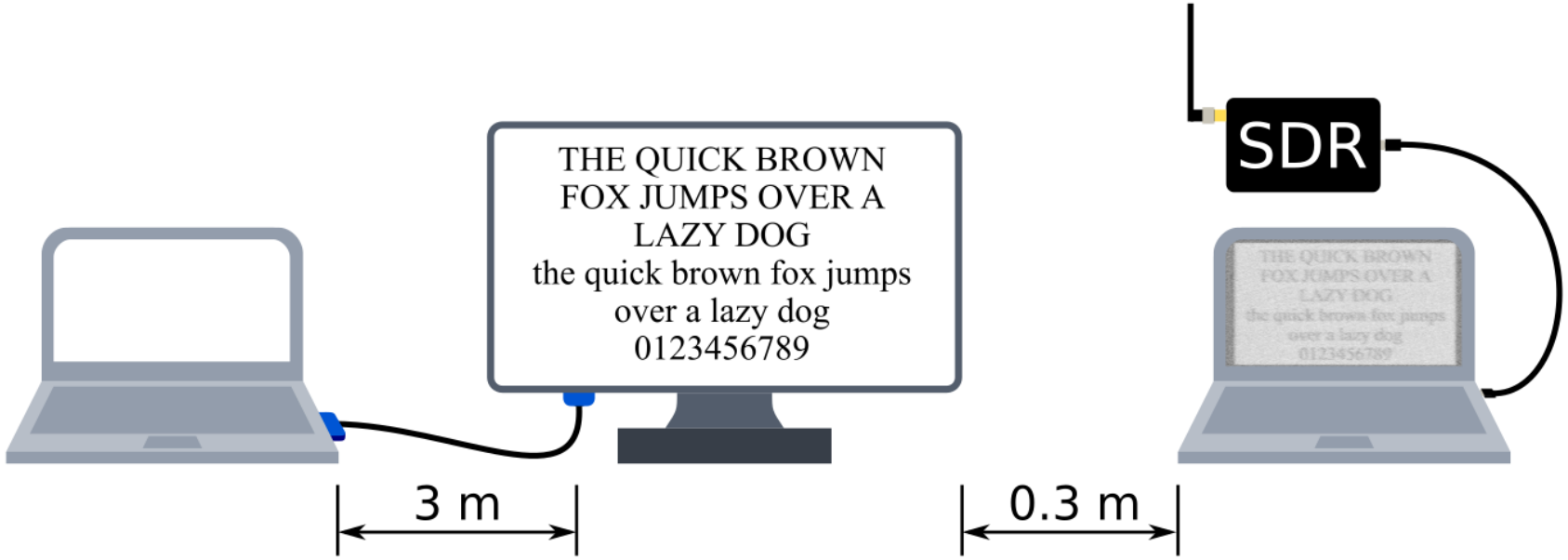
Only the information in high contrast images is feasible.

Nevertheless, the technique favors the reconstruction of text displayed on the external monitor(due to its high contrast nature). To read text automatically (with the help of an OCR), the reconstructed video frames must be further manipulated.



# Initial Setup (1)

The image and the table summarize the setup used to reconstruct video frames.




| Setup Characteristics | |
|---|---|
| Video Interface | VGA |
| Resolution | 1920 x 1080 |
| VGA cable length | 2 m |
| Distance to target | 0.3 m |

# Initial Setup (2)

A dataset was constructed with a combination of several sizes with two different fonts to test the techniques described in the following slides. In total, 20 combinations where chosen (fonts Arial and Times New Roman in sizes 30, 35, 40, 45, 50, 55, 60, 70, 80, and 90 pts). The figure shows three samples.


A pangram and the ten digits were used to make sure the most common characters are part of the experiment.

# Image Preprocesing Stage

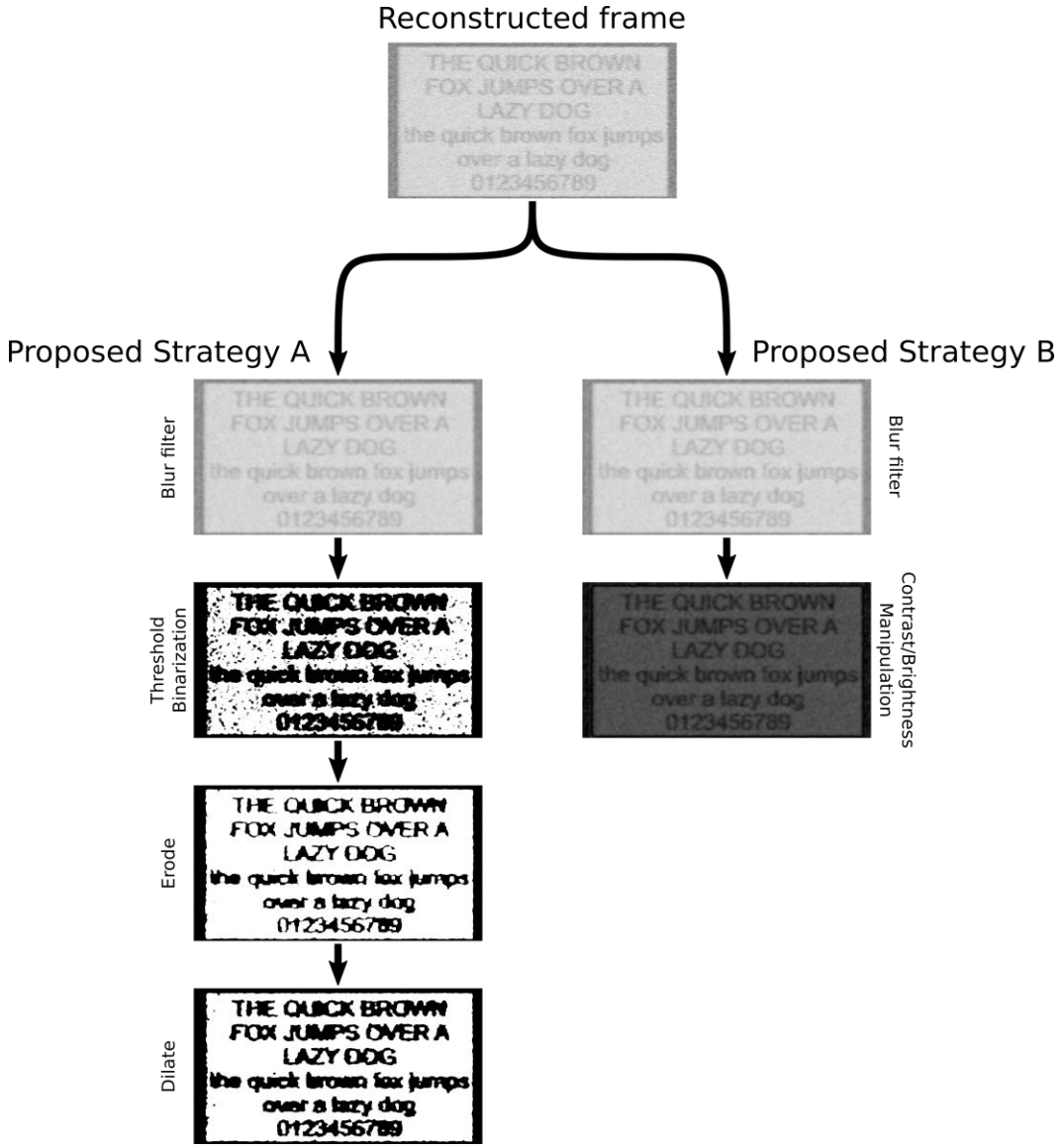
Two different techniques are proposed to improve noisy video frames so that an OCR can recognize the text:

A. Binarization

B. Contrast-Brightness Manipulation

The parameters that can be tuned on each strategy are summarized on the table.

| Technique | Parameter | Min | Max | Type |
|---|---|---|---|---|
| Binarization | Blur filter kernel size | 2 | 30 | Integer |
| | Black/White Threshold | 2 | 253 | Integer |
| | Erosion kernel size | 2 | 30 | Integer |
| | Dilation kernel size | 2 | 30 | Integer |
| Contrast Brightness Manipulation | Blur filter kernel size | 2 | 30 | Integer |
| | Alpha contrast gain | -255.0 | 255.0 | Floating point |
| | Beta Brightness level | -64770.0 | 65025.0 | Floating point |



# Text Recognition and Evaluation

Directed Energy Research Centre

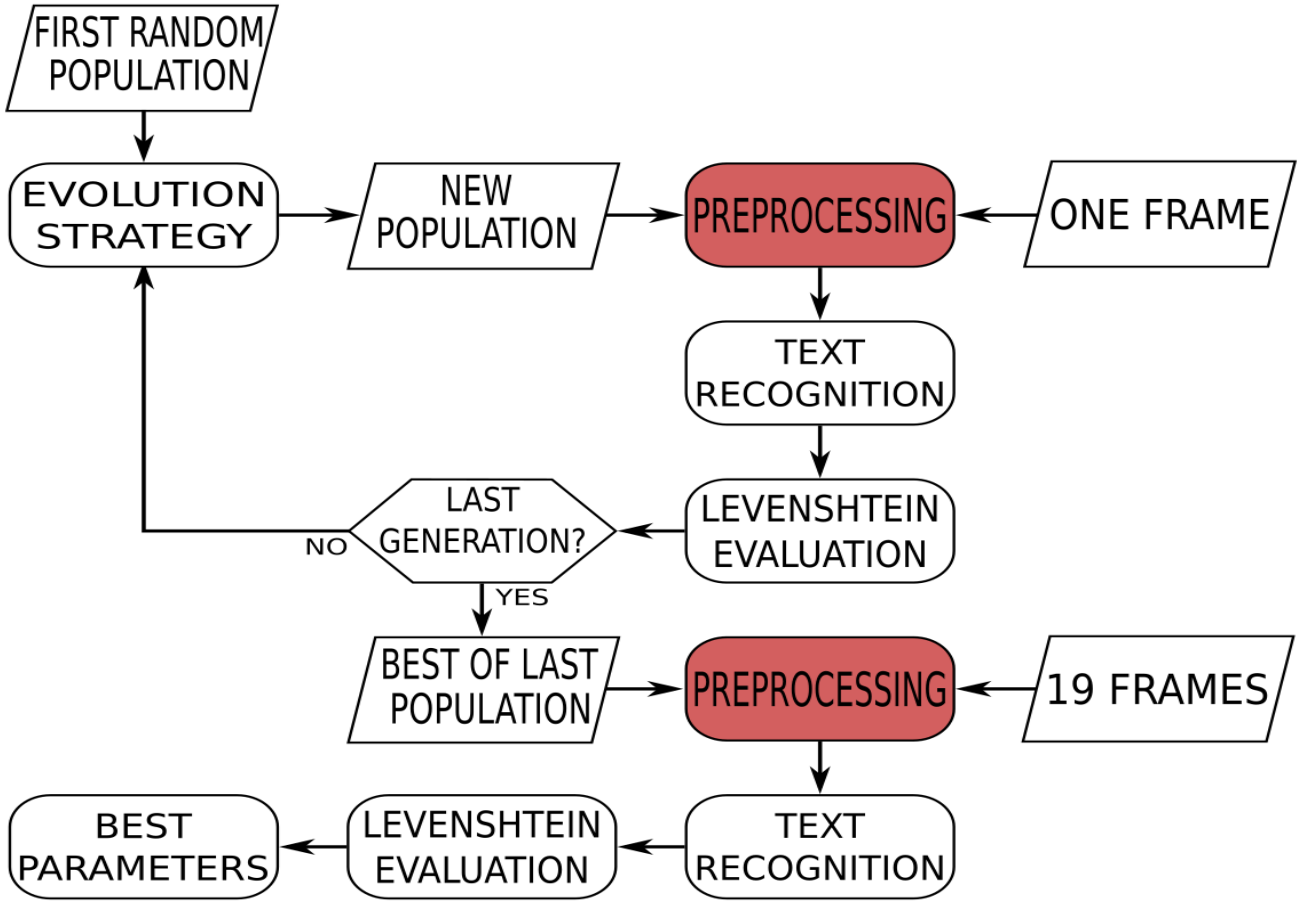
As mentioned before, text can be automatically detected from images and converted to machine-encoded text. Tesseract OCR was chosen for this task because it is powerful, open-source, and tunable.

Nevertheless, noisy frames must be first improved for Tesseract to detect any text. The mentioned techniques are mean to be applied to accomplish this goal, but the optimal parameters must be found.

To find these parameters, an objective measure to compare strings must be included. The Levenshtein distance was chosen. It counts the minimum number of changes that should be made in one string to become a second string. An index of zero implies equal strings.

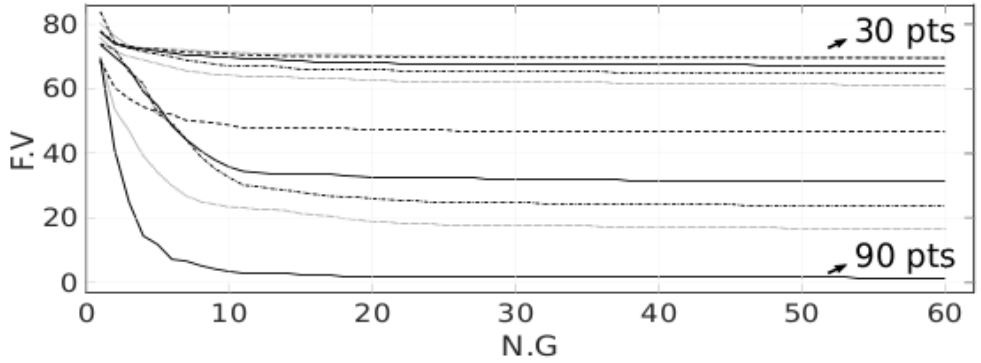
# Optimization with Evolution Strategy

An evolution strategy was developed to find the best parameters (slide 10) for each one of the two proposed techniques. The figure shows the proposed method to achieve this task.

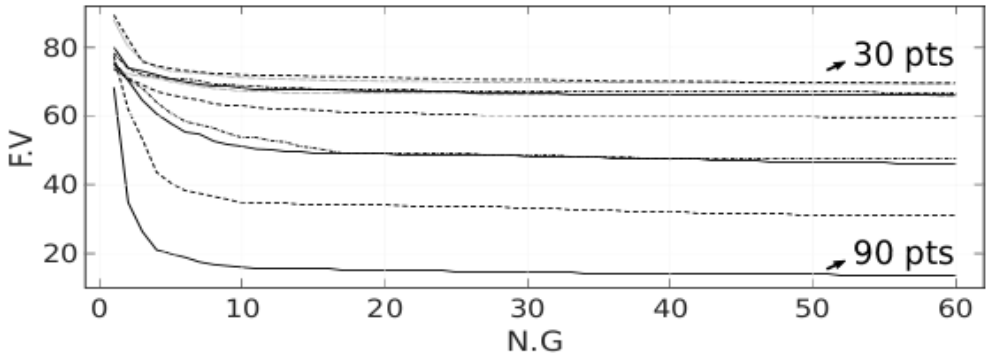


# Results (1)

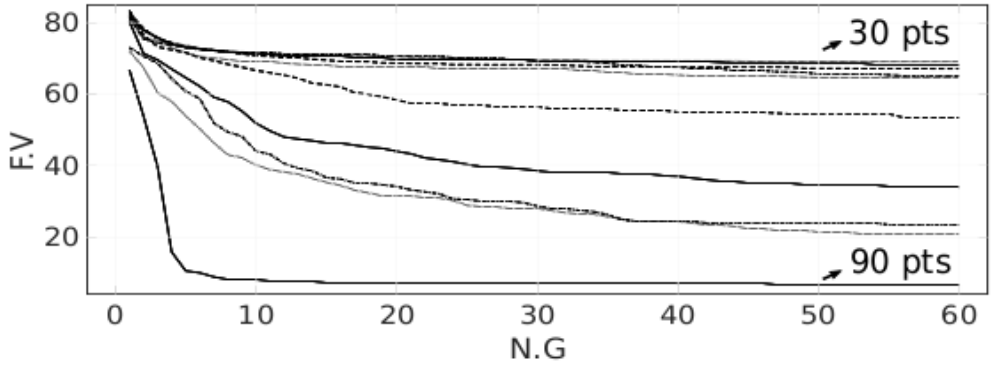
The figures depict the evolution of the fitness value (Levenshtein distance) of the elite of the population (the best parameters) for each case of font type.



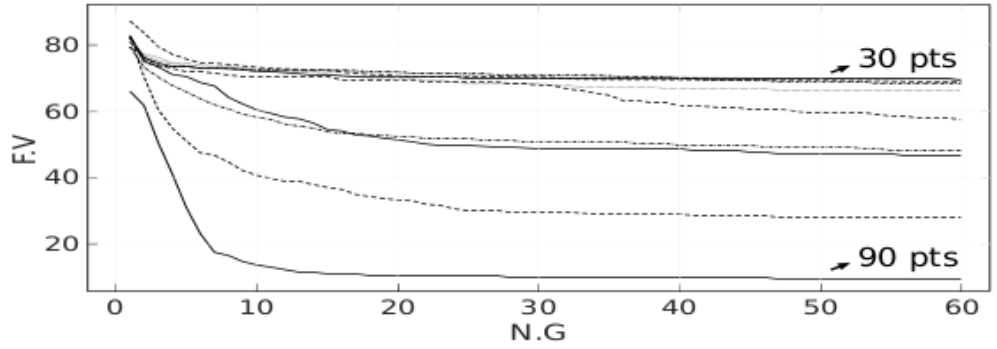

**(a)** Binary image with Arial fonts.




**(b)** Binary image with Times New Roman fonts.




**(c)** Contrast/brightness with Arial fonts.




**(d)** Contrast/brightness with Times New Roman fonts.

# Results (2)

The table summarizes the best parameters found for the cases of Arial (80 and 90 pts), and Times New Rome (80 and 90 pts).

| Technique | A80 | | A90 | | T80 | | T90 | |
|---|---|---|---|---|---|---|---|---|
| Binarization [Erotion size, Dilation size, Black-White Threshold, Blur filter size] | 7, 11, 201, 20 | 49 | 5, 13, 198, 16 | 36 | 0, 6, 202, 13 | 43 | 5, 6, 205, 23 | 36 |
| | 9, 10, 202, 18 | 55 | 10, 17, 200, 19 | 39 | 4, 13, 201, 15 | 45 | 2, 7, 204, 24 | 38 |
| | 10, 16, 202, 18 | 56 | 8, 17, 199, 18 | 39 | 3, 10, 202, 13 | 46 | 4, 5, 204, 24 | 39 |
| | 12, 14, 203, 20 | 56 | 8, 16, 199, 18 | 39 | 0, 10, 202, 13 | 46 | 8, 5, 206, 21 | 41 |
| Contrast Brightness Manipulation [Alpha, Beta, Blur filter size] | -0.68, 108.40, 24 | 62 | -1.68, 264.36, 21 | 37 | 0.89, -142.42, 18 | 44 | 1.55, -254.25, 22 | 35 |
| | -1.08, 172.40, 24 | 63 | -1.68, 262.32, 21 | 42 | -0.69, 110.15, 18 | 45 | 1.59, -261.45, 22 | 35 |
| | -1.33, 212.48, 24 | 63 | -2.20, 347.00, 30 | 42 | -0.59, 94.55, 18 | 45 | 1.56, -255.80, 21 | 37 |
| | -1.59, 253.04, 24 | 64 | -1.15, 180.50, 20 | 44 | -0.60, 96.00, 18 | 45 | 0.76, -125.28, 19 | 38 |

# Conclusions and Future Work

Directed Energy Research Centre

The main conclusions are the following:

- Text recognition from reconstructed frames is possible without human intervention; with preprocessing techniques, Tesseract can capture text.
- From the two preprocessing techniques, the binarization strategy seems to be slightly more effective than contrast-brightness manipulation.
- Detection on Times New Roman font (a serifed font) seems to lead to better results than Arial (sans-serifed font). Probably serifed fonts can retain more information with erode-dilate techniques.

The following future work is proposed:

- Improve the RF receiver stage in frames reconstruction to be able to reach smaller fonts.
- Fine-tune Tesseract with distorted fonts to reduce the error in text recognition.
- A natural language engine could be added to correct recognition errors that prevail at the end of the process.

# References


[1] W. Van Eck, “Electromagnetic radiation from video display units: An eavesdropping risk?” Computers & Security, vol. 4, no. 4, pp. 269–286, 1985.

[2] M. G. Kuhn and R. J. Anderson, “Soft tempest: Hidden data transmission using electromagnetic emanations,” in International Workshop on Information Hiding. Springer, 1998, pp. 124–142.

[3] M. Marinov, “Remote video eavesdropping using a software-defined radio platform,” M.S. thesis, University of Cambridge, jun 2014. [Online]. Available: https://github.com/martinmarinov/TempestSDR

[4] P. Winston, Artificial Intelligence, ser. A-W Series in Computerscience. Addison-Wesley Publishing Company, 1992. [Online]. Available: https://books.google.ae/books?id=b4owngEACAAJ

[5] R. Smith, “An overview of the tesseract ocr engine,” in Ninth International Conference on Document Analysis and Recognition (ICDAR 2007), vol. 2. IEEE, 2007, pp. 629–633.

[6] F. Lemarchand, C. Marlin, F. Montreuil, E. Nogues, and M. Pelcat, “Toxicia: Apprentissage profond appliqué à l’analyse des signaux parasites compromettants,” 2019.

[7] J. Liang, J. Piper, and J.-Y. Tang, “Erosion and dilation of binary images by arbitrary structuring elements using interval coding,” Pattern Recognition Letters, vol. 9, no. 3, pp. 201–209, 1989.

[8] V. I. Levenshtein, “Binary codes capable of correcting deletions, insertions, and reversals,” in Soviet physics doklady, vol. 10, no. 8, 1966, pp. 707–710.

[9] A. Auger, “Convergence results for the (1, λ )-saes using the theory of φ -irreducible markov chains,” Theoretical Computer Science, vol. 334, no. 1-3, pp. 35–69, 2005.

[10] S. Baluja and R. Caruana, “Removing the genetics from the standard genetic algorithm,” in Machine Learning Proceedings 1995. Elsevier, 1995, pp. 38–46.


TII
Technology
Innovation
Institute


Directed
Energy
Research
Centre