# GDPR compliance in Video Surveillance and Video Processing Application


2nd Eduard Barnoviciu
*UTI Grup*
Bucharest, Romania
eduard.barnoviciu@uti.ro

1st Veta Ghenescu
*Institute of Space Science*
Bucharest, Romania
ghenescu@spacescience.ro

3rd Serban-Vasile Carata
*Institute of Space Science*
*UTI Grup*
Bucharest, Romania
serban.carata@spacescience.ro

4th Marian Ghenescu
*Institute of Space Science*
*UTI Grup*
Bucharest, Romania
mghenescu@spacescience.ro

5th Roxana Mihaescu
*UTI Grup*
Bucharest, Romania
roxana.mihaescu@uti.ro

6th Mihai Chindea
*UTI Grup*
Bucharest, Romania
mihai.chindea@uti.ro



***Abstract*—In this paper we will present what is the General Data Protection Regulation (GDPR) and its impact on businesses that use and market video surveillance systems. We will detail the regulations and guidelines of both GDPR and the European Data Protection Supervisor (EDPS) regarding the recording and processing of personal and sensitive data and why it is classified as high-risk. We will consider the impact of these laws and regulations on the the field that we are operating in, namely machine learning applied for video analytics. To do that, we will briefly present two of our applications that are affected by those changes: Facial Recognition and Identification and Person Detection and how to adapt them to be GDPR-compliant. Finally we will also present a lightweight piece of software that can be easily applied to existing software with minimal computational overhead.**



***Index Terms*—GDPR, video surveillance, YOLO, blur filter**


## I. Introduction

Video recordings, both for surveillance purposes and entertainment, have become more and more problematic, as the number of cameras and the accessibility to high-quality hardware has increased. In the last ten years, the optical sensors used for monitoring, even in the private sector, have become increasingly performant and cheap. As a consequence, people's privacy can be infringed. With the raise of Big Data, information becomes more and more valuable and attempts at acquiring that information in less than ethical ways have become frequent. Even if we are not considering incidents like hacks and other data leaks, targeted marketing using artificial intelligence is being used extensively. In the face of all these threats to the individual's privacy, the European Union raised the need to regulate the fair use of public data, in the form of collection of laws known as the GDPR, or the General Data Protection Regulation [1] . The GDPR has been applied across all 28 EU member states, as of 25 May 2018. The important thing to note about this is that it makes the companies responsible for the data of their users, especially in the cases of hacking and other similar events. According to [2], the measures that companies and institutions must take can be beneficial to them, as the public is very likely to boycott and disregard a company that does not show initiative towards better handling of their data.

While recent work approached the subject from a legal [3], [4] and from a technological [5] stand-point, the found practical solutions were scarce or absent. In our paper we discuss at length the legal perspective and also offer several practical solutions.

We will focus on the section of the GDPR that regards video data, more exactly, the recording and processing of video data from video surveillance systems. that the GDPR classifies as high-risk operations. [6] Consequently, it is illegal to process personal video data unless at least one of several conditions are met. We will discuss these conditions in the following chapters and what they mean for our applications. Subjectively, there are two ways of looking at these regulations: on one hand, it is a necessary push-back against the invasion of privacy. On the other, it can temporarily hinder the activity of many companies, especially those that not only use video surveillance for their own security, but also commercialize it. We will also address possible means of reducing the consequences of data leaks: our proposed method is adding an extra layer of filtering that makes the identification of individuals impossible, both from live feeds and from recordings. This will come at no significant cost and without having to modify the original software or the legacy hardware. While this can be accomplished in many ways, with varying performance, the most important factor for our applications was to add no extra computational cost to the already existing and optimized software. Therefore, we developed a simple filter that applies a blurring effect to the faces of all the people in our video data.


978-1-7281-0984-8/19/$31.00 2019 IEEE

## II. The General Data Protection Regulation

### A. Legal Grounds

The Article 6 [7] of the GDPR is concerned with regulating data processing, including video data. There are six grounds that legalize data processing. If a company satisfies at least one of them, the conditions are met. These conditions are as follows:

- Obtaining consent for processing
- Performance of a contract
- Compliance with legal requirements
- Vital interests of the individual
- Public interest
- Legitimate Interest

In general, the two most common conditions that allow for data processing are either Legitimate Interest or Consent [8]. Those two conditions will represent the guidelines on which we adapt our systems. What we hope to achieve is to either avoid processing personal data all-together, or to use our surveillance systems with Legitimate Interest or Consent.

To further analyze this, we need to understand how the GDPR defines personal data and sensitive personal data. Article 4 [9] of the GDPR defines personal data as "any information relating to an identified or identifiable natural person". According to the GDPR, "an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name". It also defines sensitive personal data as data similar with regular personal data but that can also offer details about the person's racial makeup, political inclination, religion, health condition, sexual orientation, criminal records, biometric and genetic data. The last two are considered to be especially important. Furthermore, data is considered personal even if the person is not identified, but it can be identifiable through further analysis or in conjuncture with other similar data. This is important to our method as we must make the anonymization irreversible. The GDPR states that video surveillance is described as high-risk operation. Some of the reasons for that are that video information is very valuable and that it can lead very easily to cases of identity theft and fraud. [6] This is the worst case scenario, but it must be considered, even when companies advocate that video surveillance is necessary to deter vandalism and criminal intent. This is called legitimate interest and is one of the legal conditions that a company must fulfill in order to legitimately use video monitoring.
Another requirement of the GDPR, stated in its Article 35 [10] is a formal documentation of compliance to its provisions. It introduces the concept of Data Protection Impact Assessment (DPIA) as a method of ensuring and controlling compliance. The general, broad rule as to when a DPIA is necessary is when data leak is likely to result in a high risk to the rights and freedoms of natural persons (Article 35(1)). However, it is advised that it should be done, whenever uncertain about its necessity. [11].

### B. Data Processing and Anonymization

There are 7 principles that should be followed when processing public information, as per the GDPR [12].

- Lawfulness, Fairness and Transparency
- Purpose Limitation
- Data Minimization
- Accuracy
- Storage Limitation
- Integrity and Confidentiality
- Accountability

Most of them have been in place in a form or another, but they have now been outlined, equally for all the countries in the EU. This brings an advantage especially for international companies, that can now follow the same procedure for all their regional branches. For some countries, the GDPR is actually a step down from the previous regulations.
We will take a closer look at the second and third principles. The first one urges all bodies that process personal data to limit its use to the original purpose. Also, according to the Data Minimization principle, it is required to limit the acquisition of data to the bare minimum of what is necessary for the original task.
In the case of video surveillance, this translates to positioning your cameras so that they record as little as possible from the public space. It also means that the recordings should not be used for a different purpose other than the declared one. However, the data can be used for scientific, archival and research purposes if pseudonymized.
As stated earlier, anonymization is a big part of protecting the data we process. First of all, the GDPR defines anonymization, in Recital 26, [13] as data rendered anonymous in such a way that the data subject is not or no longer identifiable. While difficult to uphold, true anonymization can place the processing and storage of personal data outside the scope of the GDPR. Separately, the Article 4 [9] also defines pseudoanonymization as the processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information. This relaxes to a degree the restrictions. For instance: pseudoanonymized data can be used beyond the scope that was initially declared. We consider that through our proposed method, our data will be rendered anonymous.

### C. The EDPS and Technology Monitoring

Considering state of the art applications, especially those that use artificial intelligence, the possibilities of what can be extrapolated from existing data are endless. That is why, it is also important to talk about the European Data Protection Supervisor(EDPS) and their technology monitoring program. The EDPS is an institution tasked with supervising how all European institutions handle the personal information they process. As some of the entities that deploy our technology are part of European Institutions, we are obliged to be compliant with their requests. Fortunately, their conditions are mostly aligned with the GDPR. The EDPS are also responsible for

monitoring technology advancement such as deep learning and many of its application. In this category there are included both the ones used for security purposes but also those that can be potentially used for obtaining and abusing private information. Article [14] makes some great points on how machine learning can use data to train models that, against our efforts, still inherit human bias. The GDPR shows concern about respecting three rights of every individual while using such technologies:

- Non-discrimination Right
- Right to Explanation
- Right to be Forgotten

This is very well explained in Cathy O'Neil's book "Weapons of Math Destruction", showing how human bias can be unwillingly embedded in mathematical models. Data as simple as zip codes can result in racial discrimination, as it happened when Amazon's same-day delivery system proved to be less likely to deliver in black areas [15].

## III. The Proposed Method

For this paper, we will discuss the most important ones: Facial Recognition and Person Detection.

### A. You Only Look Once - YOLO

In his work, [16] Redmon proposes a new type of neural network architecture that handles object recognition as a unitary regression problem. In general, a deep neural network has to go through two steps, regardless of how each of them works. These two steps are Region Proposal, and Classification. YOLO does both of them at the same time, on the entire image. This process represents a great optimization on classic Deep Neural Networks (DNNs), that need an extra step for proposing regions of interests on which to predict a class. The region proposal (in other DNNs) can be done either through a different detection algorithm, through experimental and heuristic means, or, the most costly way: a comprehensive search.

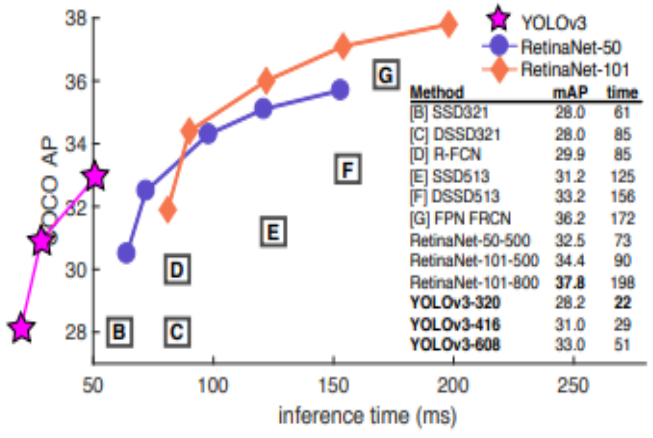


Fig. 1: Yolov3 comparison with RetinaNet [16]

In Figure 1, Yolov3 is compared with one of the state of the art architectures at that time, based on the residual network model, RetinaNet. While the accuracy on the COCO database is not quite as high, the inference time is considerably small, which is very advantageous for our use-cases.

### B. Facial Recognition

In this paper [17] we describe our Facial Detector. This application was designed to identify persons based on their facial characteristics, using the YOLO architecture described in the previous sub-section. We will very briefly describe how it was trained and how it is used.

Originally, this network was designed to classify objects that are entirely different, each being it's own class, but we succeeded in retraining it to classify different subjects of the same class. We modified the original architecture by replacing the last layer with three more convolutional layers and a fully connected one, with enough outputs for all the classes. The number of outputs is determined by the number of classes that we have to classify, according to the following equation:

$$N_{filters} = 5(5 + N_{classes}) \quad (1)$$

We retrained this model on our database, comprised of the faces of employees, taken from different angles ranging from +90 to -90 degrees. We also experimented with different number of feature maps in each convolutional layer and different input resolutions, for a number of generations varying up to 800.000. In the end, we obtained a top accuracy of 89.65%. An example can be seen in Figure 2

Fig. 2: Facial Recognition Example

The way we use this detector is to monitor different access points using fixed and Pan-Tilt-Zoom cameras, detect people's faces and cross-check them with our proprietary database. If a detection has a certainty higher than a set threshold, that person is considered to be identified correctly.

While this application works as intended, it is processing personal data, namely the images of every person that walks

under any of our cameras. As stated in the previous chapter, one of the principles of lawful use of private data is Consent.

While Consent is given for everyone that is already part of the database of employees, partners and so on, there are instances where unconsenting people are filmed. As a consequence, what we propose is an irreversible removal of all the features that could lead to unwilling identification. Practically, any person that does not match our threshold of confidence for identification, will be made unidentifiable.

### C. Person Detection

In this paper [18] we also use YOLO for a person detection system, combined with other algorithms like Trip Wires [19] and Sterile Zones [20] for detecting people attempting to trespass. Our algorithm is applicable both for color and infrared images. The process is described bellow. As in the previous sub-section, we used the YOLO architecture. For the RGB case we used the pre-trained model on the COCO database, while for the infra-red case, we preferred to retrain. We changed the architecture, the number of filters and resolution and we trained for a wide range of generations. In the end, we obtained an accuracy of 68.75%. While it might not appear as much, considering the complexity and difficulty of the database, we consider this value to be more than appropriate. Compared to the original model tested on the same dataset, it showed an increase of 23%(from 45.23%). One example of this application can be seen in Figure 3.

Fig. 3: Person Detection Examples - Thermal

This time, the face of any individual is not used in the detection process so all the faces are filtered out, using the same method as in the previous subsection. The actual method is described and exemplified in the next section.

### D. Anonymization

The base of the algorithm we propose is designed to have an insignificant computational cost, in order to maintain the previously determined minimum requirements for our systems. For that reason, we use the detections that the neural network already produces.

- In the case of person detection we select the top-most quarter of the image, corresponding to the face. Just for triggering person detection alarms, the facial characteristics of any individual are not necessary.
- In the case of face recognition, we select as a region of interest any proposed detected face that cannot be correctly identified in our database. We take into account the possibility that any person who is not identifiable did not give consent for their image to be processed.

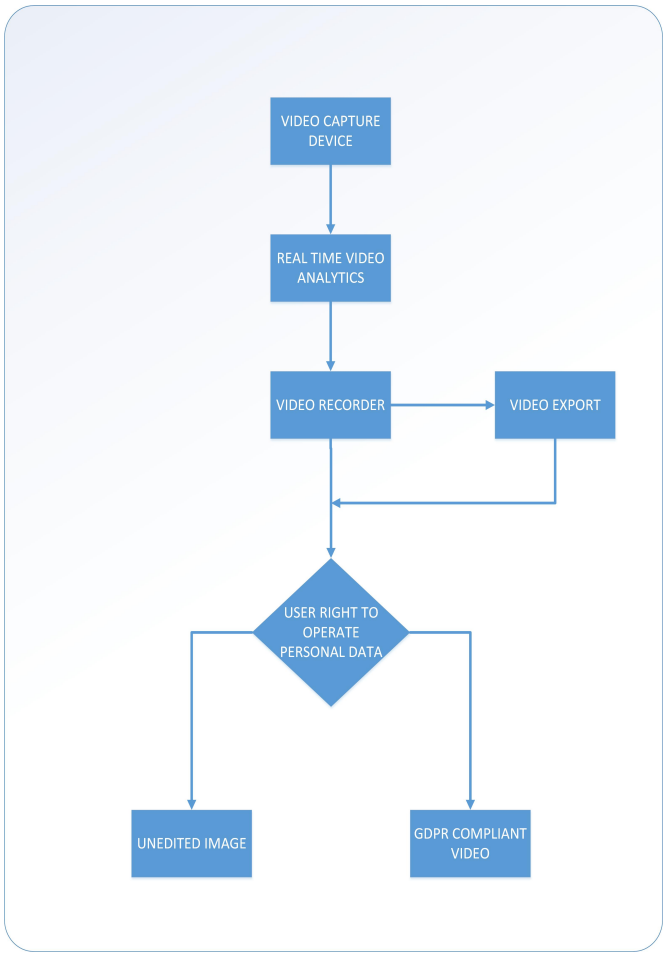


Fig. 4: Pipeline Diagram

Finally, we apply a simple blur filter by re-sizing to a very small resolution, in the orders of 10ˆ-1 the original resolution. We then re-size to the original resolution. According to the authorizations of the operator, either the raw or the filtered videos are shown or stored. We consider this to be a on optimal solution that, for our detection systems, make the data GDPR-compliant. In the diagram from Figure 4, we show the new pipeline we use.

### E. Reversibility

With the anonymization of data, the problem of its unwanted recovery is raised: impressive efforts, such as [21] have been made to reverse the blurring process. While this brings concerns for some cases, with our proposed method, the scale of the resizing can be easily modified, up to the point where the face is covered with a solid rectangle. Furthermore, it is designed in such a way that the original image is completely and irreversibly lost, unless the administrator of the

surveillance system chooses to save a clean copy (following a lawful procedure). In conclusion, neither the recovery of original data, nor the reversal of blurred data is a concern.

### F. Other cases

Fortunately, for our more advanced detection system we can rely on already predicted detections. In the cases where we only deploy basic video surveillance, without the help of a neural network, we propose two solutions, for two different cases:

- The case where computational overhead is allowed, optimal face detectors can be used to apply the Face Blurring. These algorithms may range from Viola-Jones Facial Detection algorithm [22] to more complex ones, like OpenFace [23]
- The case where the extra cost on the system resources should be kept minimal, the blurring can be applied on different sections of the installed cameras.

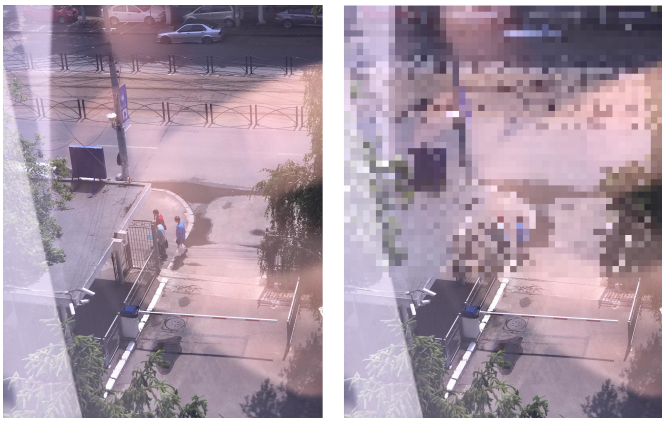

Fig. 5: Blur Zone Example

This second solution can be very advantageous because, according to the GDPR, cameras must be places such that they intrude the public space, as little as possible . For many cases, this would mean re-installing and re-positioning many cameras, which can be difficult and unnecessary. The advantages of simply marking the public areas as "to be anonymous" has two advantages: it makes already installed cameras GDPR-compliant but also can still use information from those areas for more basic means of detection, such as motion detection, etc. One side-by-side example can be seen in Figure 5. It can be applied as a customized area wherever the field of view of one camera includes public areas, needlessly. This way you can avoid all complications in a very simple and cheap way, without having to actually move the camera.

## IV. Results

In the Figures 6, 7 and 8 we show some of our results. In Figure 6 one we only use the person detection algorithm that automatically blurs the face of any detected subject. Figure 7 and Figure 8 shows the facial recognition system. As it can be seen, the person who was part of the database was recognized while the other one was blurred.


Fig. 6: Person Detection Blur Example


Fig. 7: Facial Recognition Blur Example: (a) left-profile:1m, (b) frontal:1m, (c)right-profile:1m,(d) left-profile:3m, (e) frontal:3m, (f)right-profile:3m

## V. Conclusion

In this paper, we presented an overview of the GDPR regulations in general, while also highlighting the topics that impact our activity.

Firstly, we went over the purpose of the GDPR in protecting data in general and how it defines personal data and sensitive personal data. We also detailed how this applies to video surveillance and what are the regulations and principles we should abide. Another important topic we approached was how is anonymization defined by the GDPR, why this is necessary and how it could be done. We also briefly touched on how high level machine learning can learn human bias, and how this can result in discrimination.

Secondly, we focused on how all of this influences our work. To illustrate this, we described two of our application that are affected by these regulations and we proposed a method of how we can easily adapt them. We had two different approaches, based on two legal requirements for any video surveillance platform: Consent, applied in our Facial Recognition application and Legitimate Interest, applied for our Person Detection.

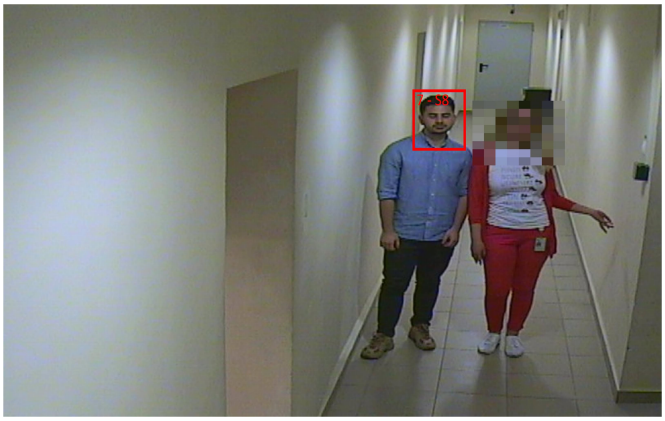

Fig. 8: Facial Recognition Blur Example

This method protects the privacy of any person filmed with our detection systems, during the normal use of our software and in case of a data leak, with minimal computational cost. We also propose some other solutions that can be easily applied on a system different than ours, in order to help others get in line with the new regulations.

Lastly, we consider that our paper fulfills its two roles: It acts as a starting point for staying informed with the new regulations and it presents our method of staying GDPR-compliant.

## ACKNOWLEDGMENT

This work was partially supported by the Romanian UEFISCDI Agency under Contracts 18PCCDI/2018, Solutii PN3-P2-520/2017 and 483/2017 and MCI by the Nucleu programme, grant no. 16N/2019.

## REFERENCES

[1] E. Parliament and C. of the European Union. (2016) General data protection regulation. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

[2] E. T. Leon Hempel, "Cctv in europe." Urban Eye, 2004.

[3] C. Cliza, S. Olanescu, and A. Olanescu, "Video surveillance: Standpoint of the eu and national legislation on data protection," *Challenges of the Knowledge Society*, pp. 465–471, 2018.

[4] A. Šidlauskas, "Video surveillance and the gdpr," 2019.

[5] M. N. Asghar, N. Kanwal, B. Lee, M. Fleury, M. Herbst, and Y. Qiao, "Visual surveillance within the eu general data protection regulation: A technology perspective," *IEEE Access*, vol. 7, pp. 111 709–111 726, 2019.

[6] G. Informer. (2017) The gdpr and video surveillance. [Online]. Available: https://gdprinformer.com/gdpr-articles/gdpr-allows-video-surveillance

[7] E. Parliament and C. of the European Union. (2016) Article 6. [Online]. Available: https://gdpr-info.eu/art-6-gdpr/

[8] G. Informer. (2017) Legal grounds for processing gdpr. [Online]. Available: https://gdprinformer.com/gdpr-articles/legal-grounds-processing-gdpr

[9] E. Parliament and C. of the European Union. (2016) Article 4. [Online]. Available: https://gdpr-info.eu/art-4-gdpr/

[10] ——. (2016) Article 35. [Online]. Available: https://gdpr-info.eu/art-35-gdpr/

[11] G. Informer. (2017) Impact assessments the how-to guide. [Online]. Available: https://gdprinformer.com/gdpr-articles/impact-assessments-guide

[12] ——. (2017) 7 essential gdpr data processing principles. [Online]. Available: https://gdprinformer.com/gdpr-articles/7-essential-gdpr-data-processing-principles

[13] E. Parliament and C. of the European Union. (2016) Recital 26. [Online]. Available: https://gdpr-info.eu/recitals/no-26/

[14] A. Tabakovic. (2018) Gdpr compliance and its impact on machine learning systems. [Online]. Available: https://dzone.com/articles/gdpr-compliance-and-its-impact-on-machine-learning

[15] E. Weise. (2016) Amazon same-day delivery less likely in black areas, report says. [Online]. Available: https://eu.usatoday.com/story/tech/news/2016/04/22/amazon-same-day-delivery-less-likely-black-areas-report-says/83345684/

[16] J. Redmon and A. Farhadi, "Yolov3: An incremental improvement," *arXiv preprint arXiv:1804.02767*, 2018.

[17] V. Ghenescu, R. E. Mihaescu, S.-V. Carata, M. T. Ghenescu, E. Barnoviciu, and M. Chindea, "Face detection and recognition based on general purpose dnn object detector," in *2018 International Symposium on Electronics and Telecommunications (ISETC)*. IEEE, 2018, pp. 1–4.

[18] V. Ghenescu, E. Barnoviciu, S.-V. Carata, M. Ghenescu, R. Mihaescu, and M. Chindea, "Object recognition on long range thermal image using state of the art dnn," in *2018 Conference Grid, Cloud & High Performance Computing in Science (ROLCG)*. IEEE, 2018, pp. 1–4.

[19] P. L. Venetianer, M. C. Allmen, P. C. Brewer, A. J. Chosak, J. I. Clark, M. F. Frazier, N. Haering, T. Hirata, C. Horne, A. J. Lipton *et al.*, "Video tripwire," Feb. 24 2004, uS Patent 6,696,945.

[20] A. Shahbaz and K.-H. Jo, "Probabilistic foreground detector for sterile zone monitoring," in *2015 12th International Conference on Ubiquitous Robots and Ambient Intelligence (URAI)*. IEEE, 2015, pp. 199–201.

[21] X. Yu, B. Fernando, R. Hartley, and F. Porikli, "Super-resolving very low-resolution face images with supplementary attributes," in *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, 2018, pp. 908–917.

[22] P. Viola and M. J. Jones, "Robust real-time face detection," *International journal of computer vision*, vol. 57, no. 2, pp. 137–154, 2004.

[23] T. Baltrušaitis, P. Robinson, and L.-P. Morency, "Openface: an open source facial behavior analysis toolkit," in *2016 IEEE Winter Conference on Applications of Computer Vision (WACV)*. IEEE, 2016, pp. 1–10.