Anonymising AI

Processing sensitive camera data through edge computing in compliance with data protection regulations

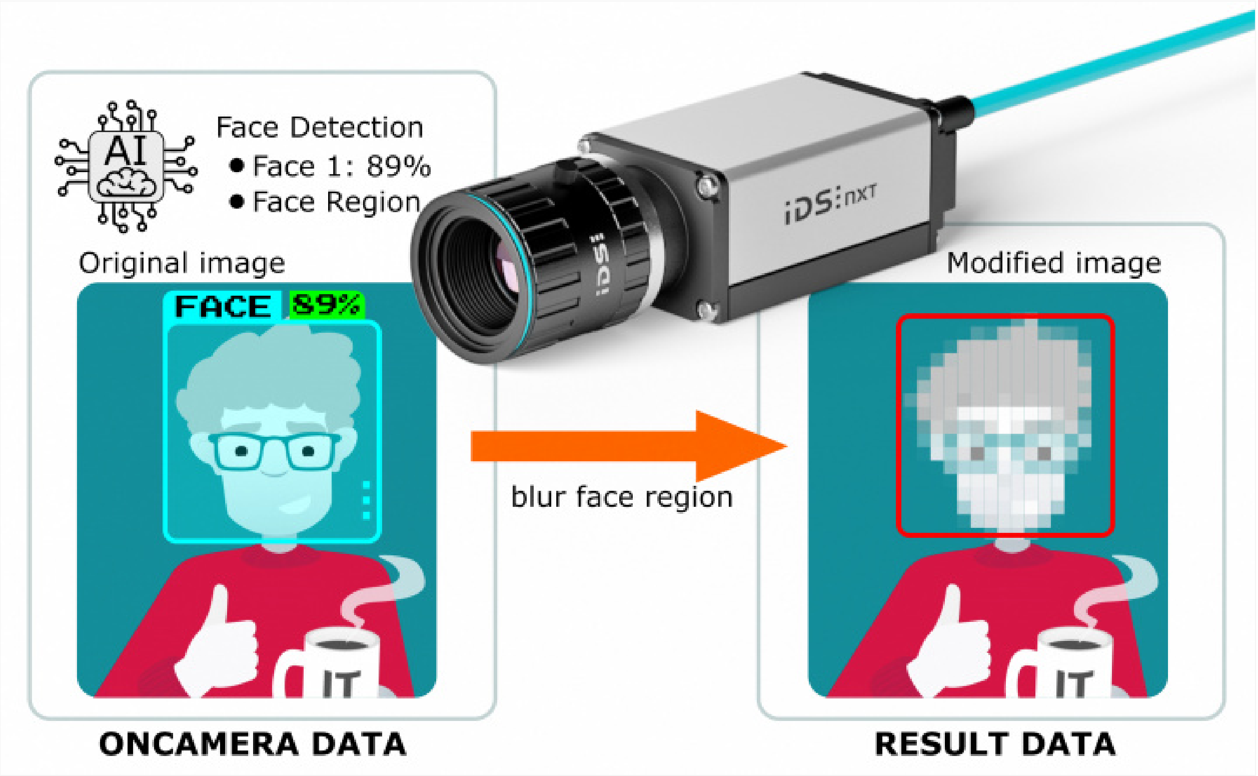
Computer vision and camera-based image processing have become indispensable tools for digital analysis and automation of many processes in different areas. However, especially where personal or other sensitive data are in focus, the issue of data protection plays a major role. Decentralised data processing through edge computing should provide a remedy. Without violating the privacy of individuals, process-relevant information is to be extracted directly in the device or sensitive image areas are to be made unrecognisable before recordings leave the device and are processed further. In addition, experts promise a fully privacy-compliant analysis of image data in conjunction with machine learning algorithms.

Nevertheless, the trendy topic of AI vision, i.e. image processing with the help of artificial intelligence, still makes many people uneasy about data security. Precisely because it is being used more and more frequently in new areas such as public spaces. For example, in cars and buses, where cameras replace the classic rear-view mirror in order to actively alert the driver to dangers, cameras that analyse the traffic volume at intersections in order to improve the flow of traffic by adjusting traffic light times, or cameras that record the occupancy of parking spaces in order to inform drivers about free parking spaces through guidance systems. However, when people think of cameras, they still think of monitoring or the storage of images of themselves. Moreover, even when it comes to knowledge about artificial intelligence, there are still misunderstandings and concerns about its capabilities and intended use.

AI-Vision anonymises data

AI-based embedded vision is the piece of the puzzle that cameras have been missing in order to anonymously process image material directly on site. Contrary to popular belief, AI does not store vast amounts of data in order to analyse it for similarities or differences with known image material. The fear that random faces in the background of an image will remain in a database forever and thus cause a data protection violation is therefore unfounded. On the other hand, AI as we use it today is "weak" and only does exactly what it has been trained to do. No more and no less! When trained with suitable image material, a neural network only learns to associate specific recurring features in the image with given information. These are, for example, distinctive shapes, collections of dots or areas. The ML algorithms do not need an explanatory context for this. The AI is virtually blind in this eye. It is able to identify faces without knowing what a face is. AI does not see the big picture and cannot recognise complex relationships beyond the trained use case.

By way of comparison, a human being who consciously perceives something today will never forget it and will always remember what he or she has "learned" or "stored" - even in completely different contexts. An AI is not trained to do this today, nor is it capable of doing so in terms of performance. The results of the AI vision are therefore only produced based on highly generalised or anonymized data. For this reason, AI-based image processing is an excellent tool for not violating data security in the process.



In a completely autonomous Edge-AI device, image data can be changed or anonymised before the result data is sent on.

Edge computing avoids data storage

If the image data is also evaluated directly in the camera and only the results are passed on, we speak by definition of an "embedded system". In this case, the process-relevant information is extracted directly in the device without having to store or transmit the image material and encrypt it for security. So in the case of a smart camera, sensitive data can be prevented from leaving the device and thus also from falling into the hands of people who could connect with faces. For data protection compliance in connection with personal data, edge computing is thus an effective method to avoid central data storage quite securely.

Edge AI already available

Taken together, AI-based embedded vision solutions form the ideal technology mix to realise and guarantee anonymous processing of sensitive personal data, e.g. in smart city applications! In addition, with intelligent cameras, the appropriate devices are already available on the market. Through vision apps, for example, IDS NXT AI cameras can be easily integrated into such sensitive use cases. With the associated cloud-based AI Vision Studio IDS NXT lighthouse, both suitable vision apps and the necessary neural networks can be created easily and quickly by anyone without prior knowledge of machine learning and application programming. IDS NXT cameras then work completely autonomously and produce direct results, but are also able to modify image material before it is sent on, such as pixelating detected faces. With IDS NXT, AI-based image processing with easy-to-use tools is available to everyone. Thus, everyone can see for himself or herself that edge AI is not a security problem, but can be the solution for completely anonymous data processing.

ⓘ Further information

- Learn more about the IDS NXT embedded vision AI platform on the **product website**.
- Discover the easy entry into Deep Learning technology with the IDS NXT ocean inference camera solution in the technical article "**AI for everyone**".
- In our webinar video "**XCITING NEW EASYNESS**", we show how individual inference tasks can be realised in a few minutes with the new block-based editor and executed in our edge system.