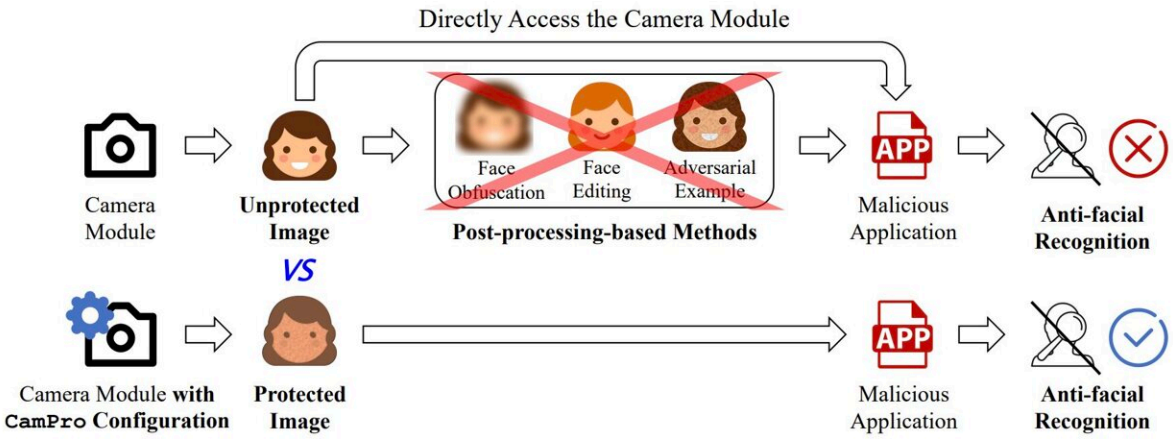
A camera-based anti-facial recognition technique

February 2 2024, by Ingrid Fadelli



CamPro resides inside a camera module to achieve anti-facial recognition (AFR) during the generation of images, i.e., privacy-preserving by birth, while traditional AFR methods desensitize the raw images output by the camera module, i.e., based on post-processing. Credit: Zhu et al.

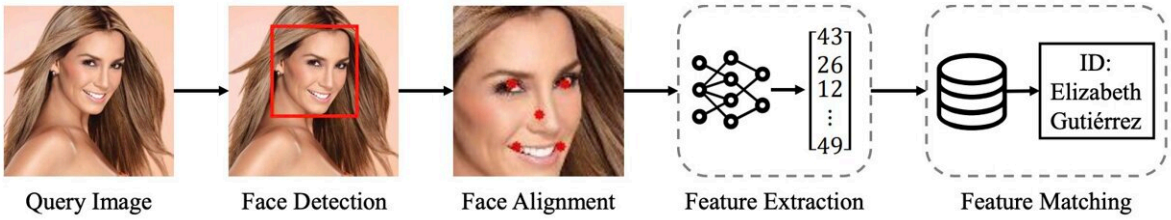
Facial recognition systems, computational tools that can recognize individuals in images or video footage, are now widely employed worldwide. Some users and developers, however, have raised privacy-related concerns, as by definition facial recognition techniques rely on images that capture people's faces. It is possible to use facial recognition techniques to identify the person by his/her face without authorization.

Some recent computer science studies have thus been exploring the possibility of preventing unauthorized facial recognition recognizing users by obfuscating, synthesizing or changing images, to increase the privacy of users. This field of research is now broadly referred to as anti-facial recognition (AFR).

Researchers at USSLAB at Zhejiang University recently developed CamPro, a new technique designed to achieve AFR at the camera sensor level, producing images that can protect users' facial privacy without influencing other applications, such as activity recognition. Their paper, accepted by NDSS 2024 and pre-published on the *arXiv* preprint server, demonstrates their proposed technique using images taken by widely available cameras.

"The rapid development of artificial intelligence (AI) has facilitated various computer vision applications that recognize human activity," Wenjun Zhu, co-author of the paper, told Tech Xplore. "However, the sensitive personally identifiable information (PII), especially the faces in the images, is simultaneously collected and uploaded to untrusted third-party servers. To this end, we propose a camera-sensor-based facial privacy protection technology, CamPro, that can remodel a commodity camera into a privacy-persevering camera that is unable to capture the facial features for identification, i.e., Anti-Facial Recognition (AFR)."

Most previously introduced AFR approaches are based on post-processing, which essentially means that they modify images captured by cameras after they were taken. On the other hand, the CamPro technique developed by USSLAB just starts working when the images are generated by camera sensors, thus malicious users will find it harder to bypass. The researchers called this paradigm "privacy-preserving by birth."



Typical stages of face identification. Credit: Zhu et al.

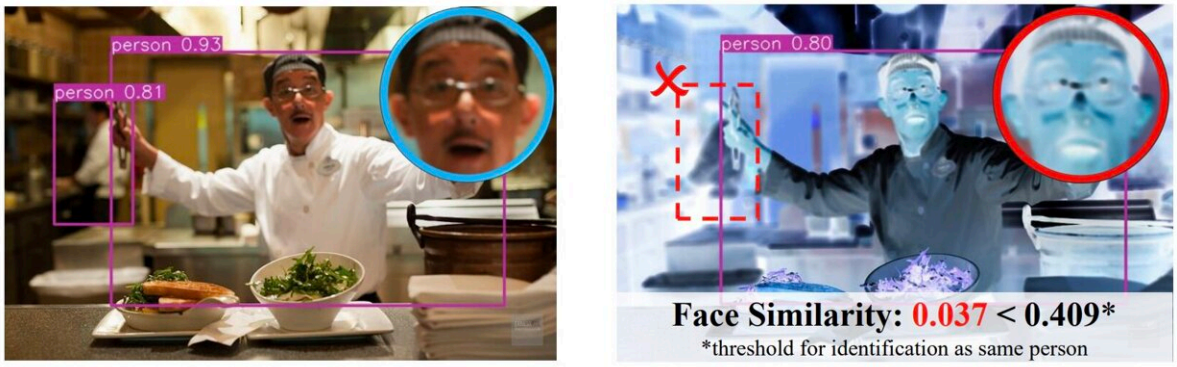
"A camera module usually consists of an image sensor (CMOS or CCD) and an image signal processor (ISP)," Zhu explained. "The image sensor converts the perceived lights to raw readings (RAW), and then, the ISP, a specialized hardware for signal processing, converts the RAW to a standard RGB (sRGB) image that accords with human visual systems."

ISP systems are essential components of modern digital cameras, which have two primary functions. Firstly, they enable the efficient conversion of RAW images into sRGB images. In addition, they offer control over image-capturing sensors, for instance adjusting shutters and ISO sensitivity to realize automatic exposure (AE).

"Due to the decoupled design of the image sensor and ISP, ISPs often provide a set of tunable parameters to cater to different sensors," Zhu said. "CamPro leverages these tunable parameters of the ISP to achieve the functionality of privacy protection. Although the original purpose of these parameters is to produce a plausible image, we found they can also be used to achieve anti-facial recognition while providing enough information for benign visual recognition applications, e.g., person detection, pose estimation, etc."

As part of their recent study, Zhu and his colleagues primarily focused on a camera's process of gamma correction (i.e., Gamma) and the so-called color correction matrix (CCM). To attain optimal parameters that enable the recognition of people without compromising their privacy, they emulated the process through which images are captured, while also introducing a new optimization technique based on adversarial networks.

"We noticed that the quality of the protected images may fail to meet the requirements of human view," Zhu said. "Therefore, we implement a trained image enhancer to restore image quality."



(a) raw image (b) color-inverted image

Color inversion effects on FR and HAR. FR: Faces highlighted in circles are compared by FaceNet, and they are not viewed as the same identity. HAR: The front person is detected yet the back one is missed after color inversion. Color inversion affects the normal operation of HAR less. Credit: Zhu et al.

In contrast to other AFR systems, CamPro works inside a camera by adjusting the existing ISP parameters, without requiring redesigning the

camera. This could greatly simplify its deployment in the real world, as it would not entail the introduction of entirely new sensing devices.

"We believe that this work is groundbreaking. Not only has it achieved sensor-level image privacy protection, but it also proposes a complete function chain from information removal to image restoration, to visual tasks, and is easy to deploy," Zhu said.

In initial tests, CamPro was found to generalize well across various black-box face identification systems, reducing average face identification accuracy to 0.3%. In addition, it was found to be resistant to white-box cyber-attacks, which entrail retraining facial recognition models to circumvent the effects of AFR systems.

"CamPro is more suited to certain specialized cameras, such as those used in smart homes for elderly fall detection, etc.," Zhu said. "These cameras need to accomplish some visual tasks without requiring facial information. CamPro can effectively prevent facial information from being maliciously obtained and utilized in various scenarios."

The new system created by this team of researchers could soon be deployed and tested in real-world settings, to further explore its potential. In addition, CamPro could inspire the development of other AFR approaches that leverage the internal parameters of cameras and sensors.

"We find that a potential attacker can easily collect sensitive personal information from the sensor readings," Zhu added. "We envision that future applications should only obtain the related information from the sensor data. Therefore, we plan to study more kinds of sensors, besides the camera, with the paradigm of privacy-preserving by birth. For CamPro, we plan to enhance its overall performance and attempt to make it a product."

More information: Wenjun Zhu et al, CamPro: Camera-based Anti-Facial Recognition, *arXiv* (2024). DOI: 10.48550/arxiv.2401.00151