DOI:10.1145/3375569

To view the accompanying paper, visit doi.acm.org/10.1145/3375571 rh

# Technical Perspective
# Lighting the Way to Visual Privacy

By Marco Gruteser

AS CAMERAS PERVADE our lives, a defining question is how to design technologies that can protect proprietary information and respect the privacy preferences of individuals. Mobile devices have already significantly reduced the effort to capture and share images. Moreover, technology trends are moving toward continuous visual sensing where even mobile cameras remain always active to monitor the environment and user context. What technical approaches help balance the convenience and usefulness of such applications against the preferences of subjects whose likeness or property is captured in such recordings?

Such questions are frequently addressed through fair information principles such as disclosure and consent that should be incorporated into the system design. Such consent solutions have been difficult to apply to camera images since a subject may be unaware of the images being captured. Short of hiding from sight or using masks, few systems offer provisions for opting out of having images of one's likeness or property recorded. Some ad hoc opt-out solutions allow subjects to have photographs showing their likeness or property removed from sharing services. This places responsibility on the subject to identify where recordings of them or their property are shared, a process that is becoming increasingly onerous as the number of services using and sharing imagery multiply.

Short of hiding from sight or using masks, few systems offer provisions for opting out of having images of one's likeness or property recorded.

The following paper presents a new technique to address this issue at the point of image capture—it stops most digital cameras from recording a useful image while the scene remains visible to human eyes. How is this possible? The authors introduce a smart high-intensity LED light that flickers at a high rate so that it creates a striping effect that severely degrades the image. It exploits the rolling shutter image sensors used in a vast majority of digital cameras, where each row in the pixel array is exposed at a slightly different time while the camera exposure control remains adjusted to the average brightness over the frame period. When the illuminating light flickers at a rate higher than the frame capture rate, this results in sets of rows alternatingly over- and underexposed and hence the striping effect. The human eye, however, will not perceive it, provided the flicker frequency of the LED light is high enough, since it essentially acts as a low-pass filter. The degradation therefore only materializes in captured images with rolling shutter cameras.

The paper also introduces two variants of this technology. First, it shows how specific cameras can be allowed to take uncompromised images while the degradation remains in effect for other unauthorized cameras. In a corporate setting, for example, this could allow taking photos with company devices while making it more difficult to capture proprietary information with personal or visitor devices. Second, it shows how this technology can be used to encode a watermark in the captured image. This can offer a weaker form of protection, particularly in areas where lighting conditions do not support degradation of the image. Such a watermark could make it easier to identify unauthorized images that are shared or published.

How might this technology evolve? Further research and development could aim to support a wider range of lighting conditions and camera to subject/light source distances than those studied to date. Research could also tackle power consumption to enable deployment in the form of battery-powered tokens or even in wearable applications. Additionally, one might study how a level of protection can also be realized for global shutter cameras, which the current technology cannot address, and further understand the level of protection offered against a broader range of image processing and computational photography techniques. More generally, one may ask whether related ideas apply to other types of sensors that can capture sensitive information such as microphones.

Overall, this work represents a significant step toward privacy-enhancing technologies that can protect against the capture of information and suggests that there is a richer design space waiting to be explored. C

**Marco Gruteser** is a research scientist at Google AI, chair of ACM SIGMOBILE, and the Peter D. Cherasia Faculty Scholar and professor (on leave) in the Department of Electrical and Computing Engineering at Rutgers University, New Brunswick, NJ, USA.