Egocentric videos: Finding clues to user identity

December 12 2014, by Nancy Owano

. a) A GoPro video uploaded to YouTube allegedly capturing a crime from the POV of the robber. Can the robber be identified? b) A GoPro video uploaded by US soldiers in combat. Are their identities safe? c) Combating theft of egocentric devices. Credit: *arXiv*:1411.7591 [cs.CV]

Quick assumption: Head-mounted cameras reveal actions without showing the identity of the filmmaker. Message from computer vision experts: Not so fast.

Yedid Hoshen and Shmuel Peleg of the Hebrew University of Jerusalem are authors of the study, "Egocentric Video Biometrics," submitted last month on arXiv. They said that egocentric video is different from hand-held video: The camera is on the user, attached to the user's head, and video can be recorded at any time such as when the user is walking. It is assumed that the anonymity of the wearer can be preserved even when the video is publicly distributed, that the camera does not record images of the user, whose identity is hidden. After reading this paper, one may

not be so sure. The authors said that it is possible for user identity to be recovered. They detailed their method for learning biometrics from head-worn cameras. "We show that motion features in egocentric video provide biometric information, and the identity of the user can be determined quite reliably from a few seconds of video," they wrote. They stated that It has been found that people can be distinctly identified by biometric characteristics such as height, stride length and walking speed.

They extracted biometric information from egocentric video, concentrating on video recorded when the user is walking. Our method relied on biometric information implicit in camera motion, which can identify users accurately. "Egocentric video suffers from bouncy and unsteady motion caused by user head and body motion," they wrote. "Although usually a nuisance, we show that this information can be useful for biometric feature extraction and consequently for identifying the user."

They talked about "Convolutional Neural Network (CNN) architectures on coarse optical flow" as the way in which biometrics may be extracted. They learned biometric features and classifiers using the CNN architecture, which includes layers corresponding to biometric feature extraction and classification. Biometric features were learned automatically using CNNs—these architectures were shown to generalize and improve on physically motivated hand designed features.

MIT Technology Review, in the "Emerging Technology From the arXiv" explained their method further, saying they focused on the optical flow in the videos—the pattern of motion of objects, edges and surfaces in the video from frame to frame. "This can be extracted relatively quickly from sequences just a few seconds long. They used 80 percent of the data extracted in this way to train a neural network to spot the unique pattern of optical flow associated with each user. They then used the

remaining 20 percent of the data to test how accurately the trained network could spot each individual filmmaker, while comparing the technique with other machine learning approaches."

Two lessons from their study are, first, that this sort of biometric identification can be used to prevent unauthorized use of these cameras if the camera is programmed to work only by the one user. The second lesson is that this biometric method could identify a filmmaker. This biometric approach could be used to identify the filmmaker who had otherwise hoped to keep identity unknown. "An important message in this paper," they said, "is that people should be aware that sharing egocentric video will compromise their anonymity."

 More information: Egocentric Video Biometrics, *arXiv*:1411.7591 [cs.CV] arxiv.org/abs/1411.7591

Abstract
Egocentric cameras are being worn by an increasing number of users, among them many security forces worldwide. GoPro cameras already penetrated the mass market, and Google Glass may follow soon. As head-worn cameras do not capture the face and body of the wearer, it may seem that the anonymity of the wearer can be preserved even when the video is publicly distributed.
We show that motion features in egocentric video provide biometric information, and the identity of the user can be determined quite reliably from a few seconds of video. Biometrics are extracted by training Convolutional Neural Network (CNN) architectures on coarse optical flow.
Egocentric video biometrics can prevent theft of wearable cameras by locking the camera when worn by people other than the owner. In video

sharing services, this Biometric measure can help to locate automatically all videos shot by the same user. An important message in this paper is that people should be aware that sharing egocentric video will compromise their anonymity.