Glance Privacy: Obfuscating Personal Identity While Coding Behavioral Video

Mitchell Gordon[1], Walter S. Lasecki[1], Winnie Leung[2], Ellen Lim[2], Steven P. Dow[2], Jeffrey P. Bigham[2]

ROC HCI[1]
Computer Science Department
University of Rochester
{mgord12,wlasecki}@cs.rochester.edu

Human Computer Interaction Institute[2]
Carnegie Mellon University
{winniel,eslim}@andrew.cmu.edu,
spdow@cs.cmu.edu, jbigham@cmu.edu

Abstract

Behavioral researchers code video to extract systematic meaning from subtle human actions and emotions. While this has traditionally been done by analysts within a research group, recent methods have leveraged online crowds to massively parallelize this task and reduce the time required from days to seconds. However, using the crowd to code video increases the risk that private information will be disclosed because workers who have not been vetted will view the video data in order to code it. In this Work-in-Progress, we discuss techniques for maintaining privacy when using Glance to code video and present initial experimental evidence to support them.

Introduction

Behavioral video coding allows researchers in the social sciences to study human interactions (Bakeman and PhD 1997). In HCI, researchers often use video coding to discover how users interact with technology, and to help better explain those interactions. Video coding is important because it provides a systematic measure of behavior. However, it is typically a very time-consuming process, taking up to 5-10x longer than the play time of the video itself (hey 2000). Additionally, video coding requires a significant amount of overhead: researchers must develop a reliable coding scheme, acquire and train coders, and check for inter-rater reliability. All of these factors can make video coding a difficult and time-intensive process.

Our Glance system allows researchers to quickly analyze and code events in large video datasets by parallelizing the video coding process across a large group of crowd workers, which were recruited from Mechanical Turk using the using the LegionTools toolkit (http://rochci.github.io/LegionTools/). (Figure 1) (Lasecki et al. 2014). This approach significantly reduces the time required to code video, allowing researchers to interact with their video data in ways that were impossible before.

While coding video with the crowd introduces new benefits, it also creates a problem: anonymous crowd workers view video that may contain sensitive information, which can create privacy concerns.

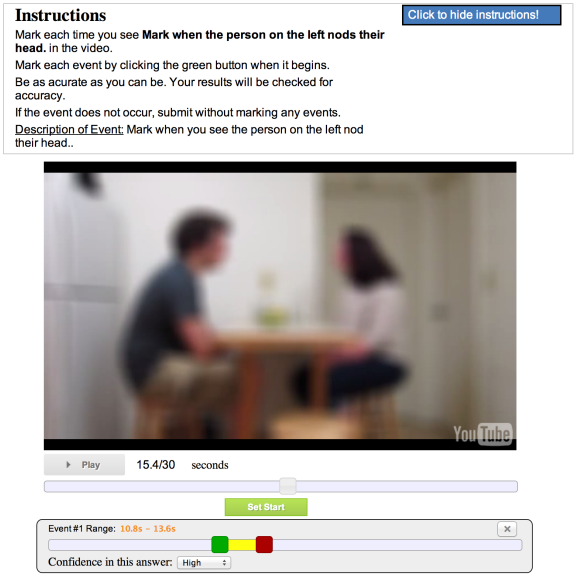

Figure 1: The Glance coding interface containing an obfuscated video of two people on a date.

Privacy

Behavioral Researchers who perform behavioral video coding must work within an Institutional Review Boards (IRB) guidelines. These review boards are concerned with balancing experimental risk/reward. A common risk is releasing personally identifiable information (PII). This risk presents a problem for coding video with the crowd, because the coding process requires many anonymous online crowd workers to access the video. To reduce personally identifiable information and therefore allow for these workers as well as a broader range of video coders, videos must be sufficiently anonymized. At the same time, the video must maintain enough detail for coders to effectively and accurately code for information.

Identity Obfuscation Techniques and Scope

Prior work has examined multiple methods for obfuscating people's identity in video while maintaining aware-

ness of actions, such as applying a blur or pixelation filter. Boyle discusses how blurring proved to be more effective at obscuring identity than pixelation (Boyle, Edwards, and Greenberg 2000). Additionally, Boyle presents 10 different levels of filtering, representing a spectrum of magnitudes for which the effect can be applied. In our initial experiments, we chose to replicate Boyle's blur filter and the exact increments of magnitude for each level.

Crowd workers might be able to determine identity in video based off a number of factors, including facial recognition, clothing, voice, and environment. Additionally, video can be shot and recorded in a variety of conditions that present challenges to a "one solution fits all" approach, such as resolution, angle (front-on, side, etc.), zoom, contrast, and number of people present in the video. For a feasible initial experiment, we chose to focus on just facial recognition in ideal lighting conditions and high video resolution.

Preliminary Experiments

To evaluate how effective blurring is at hiding identity in video while maintaining awareness of actions, we ran a feasibility study. We used Glance to code a video at different levels of blurriness. The video contained a constant, sideways shot of two people on a date, and workers coded for instances of when the person on the left nodded their head (Figure 1). Head nodding was chosen for this preliminary experiment because it is a subtle enough action that blurring a video too much could make it impossible to code for, while it is not so subtle that a mild blurring would prevent its identification. When blurring the video, we chose a blur magnitude level of 6 on Boyle's scale. We believe that this level is just before the "threshold" for the maximum amount of blur that can be applied to the video before coding for head-nodding and other similar actions in our date video becomes inaccurate.

Lineup Tool

To determine whether workers can identify a person after watching a video containing that person, we built a police-lineup style identification tool that displayed images horizontally (Figure 2). We required workers to answer whether the recognized the person in each image from the video they just watched. We first asked workers to code the date video for head-nodding, and then immediately directed them to this lineup tool, which contained one image of a person from the video they just watched (not a screenshot from the video, but a separate picture entirely), mixed in with 5 other images of different people with similar appearances. These six images were displayed in a random order to each worker. We did not give workers any warning or indication that they would be completing the lineup tool after coding a video.

Results

We ran our experiment on Amazon Mechanical Turk and received 120 worker responses. The crowd coded 10 minutes of our date video, split into twenty 30-second segments, at blur levels of 6 and 10 (unblurred) as a baseline. Each segment was coded redundantly by three unique workers.

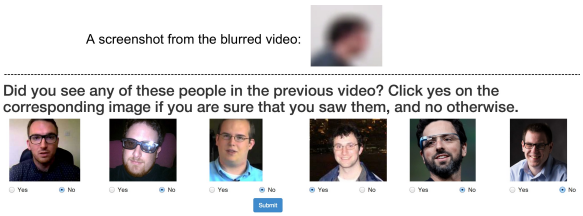

Figure 2: Workers are shown a police-lineup style tool, allowing us to determine whether they can identify a person they just saw in the previous video. The image above the lineup was from the blurred video (note that workers are not shown this image when they perform the task).

We first coded the original, unblurred video (level 10 on Boyle's scale). The crowd coded this accurately, with a precision of .942 and recall of .016. We then coded the same video, but blurred with a level 6 filter and the crowd was very nearly as accurate, with a precision of .939 and recall of .017.

While the coding was similar, the lineup identification results showed that ability to identify participants was not. For the unblurred video, 29 of 43 workers were able to correctly identity the participant, whereas for the blurred video at level 6, just 6 of 35 workers identified the participant. This shows that, by using a blur filter at an optimal level, the crowd is able to code the video accurately without significantly compromising the identity of participants.

Future Work

Our preliminary experiments have just begun to explore how we can effectively obfuscate identity in video while maintaining awareness of actions. Future work will significantly expand our evaluation to a full study that includes:

- Video from psychology researchers.
- Video that spans multiple variables, such as differing levels of zoom, resolution, contrast, and number of people in the video, as discussed in the Identity Obfuscation Techniques and Scope section.
- Evaluating how well the crowd can identify people when it is warned in advance that it will need to do so.
- Using the fact that we have multiple workers to identify parts of actions that are hidden with just one type of filter.

References

Bakeman, R., and PhD, J. M. G. 1997. *Observing Interaction: An Introduction to Sequential Analysis*. Cambridge University Press.

Boyle, M.; Edwards, C.; and Greenberg, S. 2000. The effects of filtered video on awareness and privacy. In *CSCW*, CSCW '00, 1–10. New York, NY, USA: ACM.

2000. *Handbook of Research Methods in Social and Personality Psychology*. Cambridge University Press.

Lasecki, W. S.; Gordon, M.; Koutra, D.; Jung, M.; Dow, S. P.; and Bigham, J. P. 2014. Glance: Rapidly coding behavioral