Do Not Share! Invisible Light Beacons for Signaling Preferences to Privacy-Respecting Cameras

Ashwin Ashok, Viet Nguyen, Marco Gruteser, Narayan Mandayam, Wenjia Yuan, Kristin Dana
{aashok, vietnh, gruteser, narayan}@winlab.rutgers.edu
{wenjia.yuan@,kdana@ece}.rutgers.edu

ABSTRACT

The ubiquity of cameras in today's world has played a key role in the growth of sensing technology and mobile computing. However, on the other hand, it has also raised serious concerns about privacy of people who are photographed, intentionally or unintentionally. The popularity of publishing pictures in social networks adds to the concern that the photographed user has the least control over his/her picture. In this paper, we present the design, implementation and evaluation of "invisible light beacons" where privacy preferences of photographed users are communicated to photographing cameras. Particularly, we explore a design where the beacon transmitters are worn by users on their eye-wear and transmit a privacy code through ON-OFF patterns of light beams from IR LEDs. The beacons are received and decoded by a camera and mapped to different privacy preferences corresponding to that code. Based on the experimental evaluation of thousands of data points using our prototype implementation we show that the detection accuracy of a known privacy code is greater than 98%, and error rate of communicating a random stream of bits over an indoor IR-camera channel is within 7% at packet level and of the order of 10^{-3} at bit level.

Categories and Subject Descriptors

C.2.1 [**Computer-Communication Networks**]: Network Architecture and Design—*Wireless Communication*

Keywords

Cameras; Privacy; VLC; Visual MIMO; Infrared; Wearables

1. INTRODUCTION

The ubiquitous use of cameras and photo/video sharing platforms continues to raise new privacy concerns. The debate over the appropriate use of Google Glass [8, 12] is only the latest incarnation of a century-old effort to negotiate the tension between privacy and recording technology.[1] In many countries photo and video privacy is heavily regulated, often with separate laws applicable to the taking, the publishing, and the copyright of the photos. Whether the snapping of a photo can be considered an invasion of privacy often depends on whether it is taken in public or in a private setting and whether the subject could have reasonably held an expectation of privacy at the time. Even if the photo itself is legal, an invasion of privacy can occur when it is published. This can depend, however, on whether it is published as news or for commercial purposes and whether it is a photo of a larger group of people or whether there is a prominent primary subject. Such sometimes country-specific societal norms have developed over time for traditional photography and publishing. They have not kept up, however, with the recent rapid progress in camera technology and the myriad sharing options. Current services largely focus on negotiating privacy concerns only after a photo is shared. Online photo sharing services may delete or disallow publication of a picture if it is deemed sensitive or may allow un-tagging (i.e., the disassociation of one's identity with the picture) of personal photos.

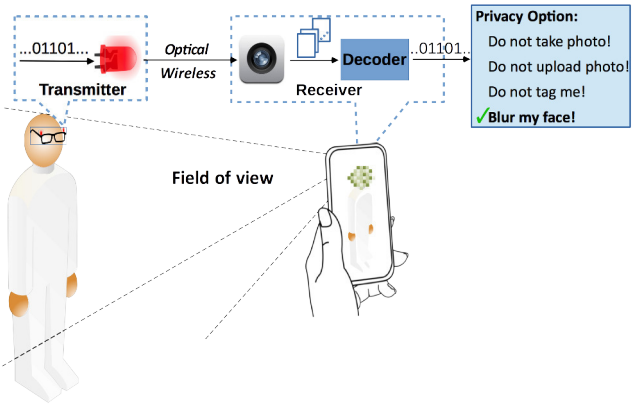


Figure 1: Conceptual diagram of the light beaconing system applied to privacy preservation of photographed users. In this example the transmitter worn on the user's face transmits a privacy code to the camera receiver that takes appropriate actions based on the code.

Challenge. The privacy application example motivates a technology solution for photo subjects to signal meta-data such as privacy preference to the cameras that snap them. This would ensure that an after-the-fact tracking down of the subject is not necessary. The primary technology challenge in signaling preferences to cam-

[1]The invention of photography and newspaper publishing were the subject of the seminal 1890 article "The Right to Privacy" by Warren and later US Supreme Court member Brandeis. It is often considered the first article in the United States which argues for privacy.

VLCS'14, September 7, 2014, Maui, Hawaii, USA.

http://dx.doi.org/10.1145/2643164.2643168.

eras is the association problem: given that a person is in a photo, whose privacy preference should be applied? One approach may be to share privacy preferences over a short-range radio link such as Bluetooth or Wifi-Direct [23]. This requires that the camera has the radio receiver and more importantly, if more than one person is nearby, it would not be clear which preferences to apply to the subject on the photo. Face recognition can help but it is very difficult to achieve reliable recognition, even if the pool of possible candidates is very small [9].

Approach. We explore therefore the use of near-visible (infrared) light communication to design beacons that can be detected directly by a camera. Light communication techniques are attractive compared to QR codes, because the time-varying optical signal allows keep the beacon very small in size, yet detectable at typical photo distances. This leverages the trend towards electronic viewfinders in cameras, which means that the camera senses the scene not only during the exposure time of a photo but also during the time when the photographer is composing the scene. This provides a longer window of sensing time, wherein the privacy beacon can announce its presence and potentially communicate information through the time-varying visual code. For the privacy application example, as shown in Figure 1, the beacon itself can be a modulated infrared LED, which is ideally attached to or incorporated into a wearable device close to the face. They could be embedded in Augmented Reality Glasses, or perhaps in jewelry or amulets. With carefully-chosen wavelength, the infrared signal is not visible to the human eye but still passes through the filters of cameras. By emitting a time-varying signal, it can be detected by the camera over a sequence of frames and through it's location inside the photo frame it also indicates which face it applies to. This directly addresses the face association problem.

What should the beacons transmit? The design space ranges from a single-bit (opt-out) to complex individual privacy polices. A study by Ahern et.al. [7] confirms the existence of photo privacy concerns and reports that people are more particular about the content (people, actions) in the photograph when making privacy decisions while some raised concerns about location. Another study [17] also indicates that people wished to have more control of their photos that have been uploaded or *tagged* on social networking sites. While such studies may not necessarily be comprehensive of the exhaustive list of privacy preferences of users, it is intuitive that short codes (3-4 bits) can span a set of key categories of privacy preferences. For example, such categories may include *do not upload*, *always untag me*, *do not reveal location*, *do not save*, *do not reveal face* etc. There may, however, also be some users that are interested in creating highly customized policies that are hundred of bytes in length. To better understand these design options, we therefore consider both basic signal presence detection (single-bit) and communication of arbitrary information.

While we use user privacy scenario as a running example in this paper, we believe that there exists a broader class of applications that benefit from signaling information directly to cameras. When privacy is not desired, such beacons may signal photo subject identities for more reliable tagging. A beacon could also send an emergency signal to a camera surveillance system. These examples show that camera communications do not necessarily have to become a general purposes communication system to be useful. While earlier work involving camera communications has primarily considered screens [27, 14, 20] or lightbulbs [31] as transmitters, this preliminary work focuses on a prototype implementation of a small, single LED light beacon and on characterizing the robustness of such a system.

In summary, the key contributions of this paper are:

1. We identify a novel class of applications for light communications that benefits from signaling meta information directly to a camera at the time of taking the photo or video.
2. As an example, we propose a light beacon design to directly signal privacy preferences to cameras at the time of taking the photo or video.
3. We develop techniques for enhancing the detection of the presence of a beacon in the camera video data and to decode information from this beacon.
4. We implement a prototype beacon and experimentally analyze the robustness of signal detection and communication error rates over thousands of different photo poses.

2. SYSTEM DESIGN AND IMPLEMENTATION

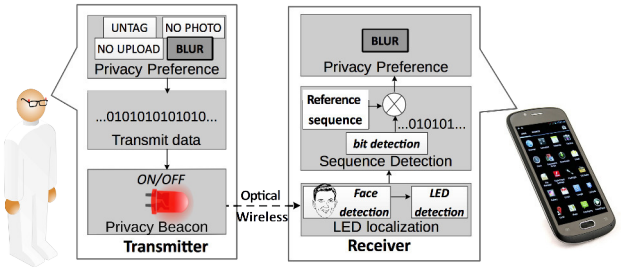


Figure 2: System architecture of the IR beaconing system

In this section, we present the design details of the proposed privacy beaconing system.

Overview. As shown in Figure 2 our proposed system consists of an IR transmitter that communicates to a camera receiver through ON/OFF patterns of light emitted from IR LEDs. The transmitter encodes the user's privacy preferences as a sequence of bits that are transmitted periodically from the IR LEDs. The receiver (camera) acquires the IR signals, localizes the LED and then decodes the bits from the detected ON or OFF states of the LED. The decoded bit-sequence is then mapped to the corresponding privacy preferences, on the camera device locally, or in a remote database.

In this paper, we consider an example application where the IR transmitter is worn by a user near the facial region. Such a placement allows for easier and robust tracking of the LEDs on the image, by detecting the facial features through face-detection techniques [33]. Face detection along with the LED signal helps to associate the privacy preferences to that of a specific user. In general, different applications with non-facial placements of the LEDs may also be possible, and such applications can choose from the plethora of pattern matching techniques that exist today [15, 25], for robust LED tracking, and address the association problem.

We will now discuss the transmitter and receiver design in more detail.

2.1 Transmitter

The IR beacon transmitter transmits a privacy code as bits by modulating the light emissions from the IR LED; ON represents bit 1 and OFF represents 0. The privacy code is generated from a data-source on the transmitter which can be a programmable microprocessor or simple micro-chip that stores the privacy preference data. The codes may also be retrieved from the user's phone

(a) (b) (c)

Figure 3: (a) Sample face detection (face detected region is shown in a green box), (b) LED detected regions within detected face region from (a), and (c) LED detected regions in entire image from (a). (Observe that the LED detection result in (c) is very noisy as compared to searching over only the facial region.)

through a wireless connection. In this paper we assume that the dictionary of privacy preferences are known to both the transmitter and receiver. We consider one use-case scenario as a running example, where the privacy code is a single universally agreed code. Detecting the presence of this code would imply that the camera has been informed that the captured image snapshot should be privacy protected. However, in general, a multitude of such codes may be communicated. Another option would involve transmitting a stream of bits as packets or time-varying codes that map to different levels of privacy options. In the ideal scenario, a random stream of bits like in any communication system would be communicated.

Beacon Prototype. We implemented a prototype IR transmitter that consists of two IR LEDs connected to two input/output (I/O) pins of an Arduino board [1]. The Arduino was programmed to generate a periodical sequence of bits that corresponded to a 13 bit Barker sequence at a data rate of 15bits/sec. Barker codes are widely employed for sequence detection due to their good auto-correlation property [32]. Sequence detection, or more formally preamble detection as called in communication systems, is primarily used for synchronizing the transmitter and receiver. Based on the channel the system may employ different protocols for transmitting the payload. However, in this paper we test the feasibility of detecting such sequences alone, while reserve the protocol design as future work. The LEDs were powered through the 1mA current that was supplied to each LED from the I/O pins of the Arduino board, which was powered by a regulated battery supply voltage of 5V. We placed the two LEDs on two sides of a spectacles, then connected them to the Arduino board that could fit in a shirt pocket. The second LED in our transmitter was used to add redundancy in transmission, by sending the same signal as the other LED.

2.2 Receiver

The receiver for the privacy beacons consists of a camera device, and the supporting software for processing and decoding the information received from the beacons. The receiver decodes the information by processing a series of image frames from the video sequence captured during the time-interval between the instance when the photographer switches ON (shutter open) the camera application and the instance when photographer clicks the snap button. The receiver detects the presence of the LED by correlating the pixels of the image with a reference value (calibrated) of image pixel intensity of the ON and OFF states of the LED. The receiver uses face-detection to localize the LED search region of interest. We observed that the intensity of the LEDs in ON state are usually considerably higher than those that correspond to a face, and hence

(a) (b)

Figure 4: Sample image snapshots from camera video footage. The user (one of the authors) is wearing the beacon transmitter.

the number of false-positives are very low. The sample snapshots of the LED detection results shown in Figure 3 illustrate that using face-detection yields better LED localization on the image.

Depending upon the application scenario, upon detecting the privacy code, the camera may perform actions such as prohibit storing the picture, or blurring the facial region in the picture or simply append a privacy meta tag with the captured photo/video snapshot.

Receiver Implementation. We implemented a prototype receiver where the detection algorithm was implemented in C++ and used the Viola-Jones [33] object-detection implementation from OpenCV library [5] for face-detection. To facilitate evaluation of our receiver algorithm on real traces we developed a camera app on a Samsung S2 smartphone that ran Android, where the camera was operated at 30fps and at 720×1280 resolution. The auto-exposure feature was turned ON during the camera operation.

3. EVALUATION

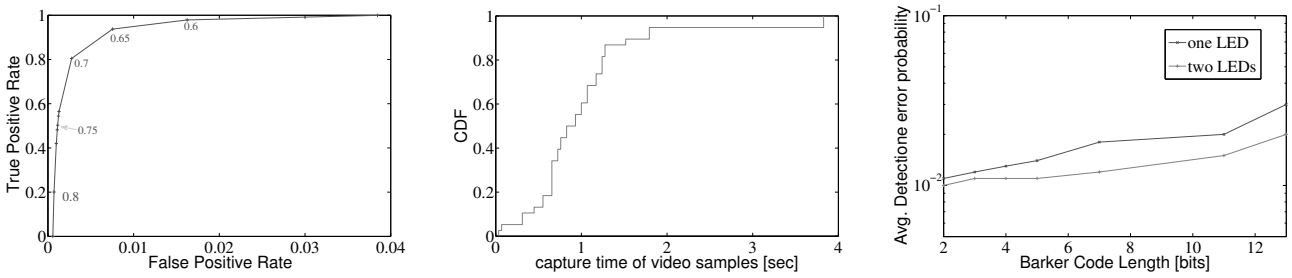
We conducted experiments, to evaluate the performance of our system, using our beacon transmitter and the camera receiver prototype. Our evaluations were aimed at answering two key questions:

- What is the detection accuracy of a known IR signal when decoded by a camera, and what is the effect of the signal design choices on accuracy?
- What are the error rates of decoding a random stream of bits transmitted by our IR transmitter worn by the user and received by a camera?

Our experiments involved a user wearing the transmitter and being videotaped (at 30fps) by another user using a smartphone (Samsung S2). The smartphone camera acquired a video from the instance of the camera app being initialized until the user clicking the snap button. The user was not restricted in their regular head movements but stood stationary during the video shoot. The receiver algorithm ran in parallel with the camera acquisition, to detect the face and decode the information from the LED signal from each image snapshot of the video through a correlation based detection. The correlation value obtained in each iteration corresponds to the product of the reference LED gray-scale pixel-intensity value and the received pixel-intensity, normalized over the product of the maximum intensity ;was 255 in our experiments. This exercise was repeated over multiple trials with multiple users in a well-lit indoor environment.

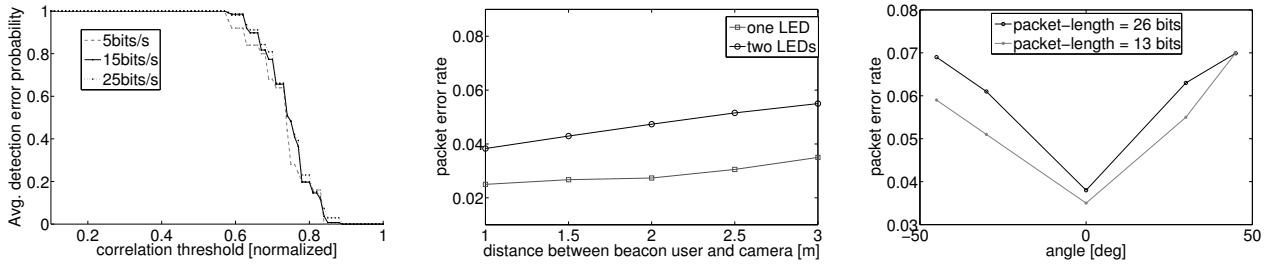
Figures 4 (a) and (b) show sample image snapshots from the video shoot, where one of the authors is wearing the IR transmitter on the glasses.

(1) **Detection Accuracy**



(a) (b) (c)

Figure 5: (a) Accuracy of detecting the presence of a light signal at the camera. Each graph point refers to the TPR and the FPR at the specified correlation threshold (marked numbers on the plot), (b) Available time for light signal reception during photo capture by cameras using electronic view-finders, (c) Effect of Barker code length and number of transmitting LEDs on detection accuracy



(a) (b) (c)

Figure 6: (a) Effect of detection correlation threshold and frequency of light signal on detection accuracy, (b) Effect of distance on camera channel quality (packet-error rate), (c) Effect of angle on camera channel quality (packet-error rate)

We compute the overall detection accuracy of the cumulative dataset of the indoor video samples and plot the receiver operating characteristics (ROC) curve in Figure 5 (a); True-positive rate (TPR) versus False-positive rate (FPR). TPR is the ratio of total number of true positives and sum of true positives and false negatives. FPR is the ratio of total number of false positives and sum of false positives and true negatives.[2]. We can observe from Figure 5 (a) that the TPR is as high as 98.5% while FPR is within 2%. We achieved this performance for a range of 3m between the transmitter and the camera. The high detection accuracy can be attributed to the use of Barker sequence and the use of face-detection to localize the LED search. Face-detection localizes the search to a region where temporal changes in the pixel intensity of the background (face) is less prominent than that of the LED intensity, simplifying receiver processing.

Photo capture duration. We observed from the CDF of the capture duration (time between camera application start to clicking snap button) of the videoshots obtained from our experiments, as shown in Figure 5 (b), that the median duration is 1.2 sec and is within 2 sec in 80 percentile of the cases. This time may perhaps be sufficient for reliably communicating a set of privacy preferences along with short user IDs (10-20 bits). Indeed the data capacity can be improved by transmitting parallel stream of bits over multiple LEDs as in visual MIMO [13].

Code length and data rate. We plot the average detection error, for different Barker-code lengths at a fixed distance of 2.5m between the camera and the transmitter (worn by a single user and posing for the camera), in Figure 5 (c). We can observe that the detection errors reduce when considering the average value of the signal intensity from two LEDs. We also plot average detection error rate at different correlation thresholds and for different repetition frequencies (data rate) of IR signaling in Figure 6 (a). From these results we can observe that the detection errors are less than 1% for data rates 15bits/sec and below as well for typical Barker code-lengths. We can observe (from Figure 6 (a)) that the detection errors rise sharply for a higher data-rate of 25bits/sec, as the number of bit errors in each sequence estimate increase due to interference between bits in successive frames and thus resulting in low correlation with the actual. We can also observe from Figure 6 (a) that a nominal (0.5 to 0.6) correlation threshold suffices for robust detection and that the detection accuracy will fall sharply with stricter correlation thresholds.

(2) **Error rates for decoding random streaming of bits.**
As a test for the link quality when a random stream of bits are communicated in our system, we conducted a simple experiment where a stream of packeted bits were transmitted in parallel from two LEDs on IR transmitter and decoded by the camera. We conducted the experiment for a set of distances (between transmitter and camera) from 1-3m in 0.5m steps, and repeated over 10 trials. In Figures 6 (b), (c), we plot the packet error rate (worst of the two LEDs) over distance and the packet error rate of one LED (whichever was detectable at an angle, at distance at 2.5m) at different angles, respectively. We observe that the packet error rates are below an acceptable 7% at typical use-case distances and angle for the chosen data-rate specification. We also computed the bit error rate to be of the order of 10^{-3}, and was consistent across the set of evaluated distances and angles.

[2]True-positive is the event when a tag is successfully detected when actively transmitting the known sequence. A false-negative is the event when the receiver does not detect a tag, but when tag is actively transmitting. These events also include the case where a face is not detected while tag transmits.

We emphasize that the range of our system can be improved (to about 6m) by operating the LEDs near saturation, however, the battery lifetime will reduce by half. The IR transmissions may also be controlled by the user to be used only when necessary to conserve battery power. We believe that such ranges are sufficient for typical indoor applications where it is only within a few meters where the face of the user can be recognized on a photo and that the privacy will matter.

4. DISCUSSION

We will present some of the discussion points that emanate from our work and also some limitations in our design.

Whose right is it anyway? The use of privacy beacons, on one hand, can provide privacy options for the beacon user, however, on the other hand, can also interfere with the photographer's freedom to take a picture. It can make photographing any event very inconvenient, especially snapping a picture in most interesting scenarios, cause most of these pictures will have one or more human faces in view, voluntarily or involuntarily. What kind of action should be taken once a camera decodes a privacy option remains an open question for decision makers which could also include policy makers.

Power consumption. The peak power consumption of the beacon transmitter during operation is $5mW$, where the peak current drain from the battery is 1mA, which also includes powering the Arduino board. The lifetime of our prototype transmitter is about 225 hours on a 9V alkaline battery supply. The lifetime can be increased by enabling the transmitter beaconing only when necessary.

Wake-up mechanisms. As mentioned earlier, the battery life of the transmitter can be improved by switching it ON only when required. In this regard, we can employ *wake-up* mechanisms, for example using Bluetooth or WiFi, where the camera (phone) can broadcast that it is going to take a photograph, and upon sensing the signal the transmitter enables the optical beacons. Reversely, upon sensing a device, through some radio channel, integrated with a camera, the beacons could also be used to wake-up or enable the camera application seamlessly.

Would people wear a privacy beacon device? This paper uses eye-wear fit with privacy beacon transmitters as a running example for usage. However, in reality, a user may not be inclined to wear a hardware device unless it is embedded into an object he/she is already wearing. We do feel that convincing people to wear a device that enables such a feature would be challenging, and would require some support also from policy makers to bolster this idea. Considering that no convincing solution exists today for the photographed user to communicate his/her privacy option, while or even before the photograph is taken, we feel that our solution takes the right step ahead in this regard.

5. RELATED WORK

The use of light beacons for signaling to cameras/image sensors has been explored earlier [4, 27, 11], however, these approaches use the visible spectrum instead of IR, and thus less unobtrusive. Also, communication at the IR spectrum [22] has so far been using photoreceptor receivers or specialized cameras [2]. Our solution shows the feasibility of using off-the-shelf cameras for IR communication. Yamada et al [34] propose a technique that only prohibits photo capture (but not communicate) using an infrared LED in the form of light-jammers. Tagmenot[10] offers wearable QR codes to specify users' privacy options, but the QR codes may not be detectable or may be hidden in some poses and hence limited in applicability.

Researchers have proposed techniques for encrypting facial areas in photos [30] and for negotiating more complex (e.g., person-specific) sharing policies [17]. Negotiating such privacy protections, however, is only possible if the subject of a photo can be identified and contacted at the time the photo is shared.

However, with the popularity of social networks today image and video content from users' profiles have shown to be (mis) used by employers and law enforcement to investigate the behaviors of individuals [16]. A study by Acquisti et al. [3] shows that a combination of simple face-detection techniques and a large photo collection, such as Facebook public profile pictures, could identify a person in a photo with a high degree of accuracy. Indeed, Google has taken a step to address privacy concerns by blurring faces, house numbers, car license plates in Google Street View [19]. Giving users more control of their privacy was the underlying idea of the Platform for Privacy Preference Project (P3P) [6], however its development was not successful due to its complexity. An effective privacy solution must be simple, light-weight, and almost seamless to users.

Chattopadhyay et al. [18] proposed a privacy preservation method by embedding a secured key inside the photo. Besmer et al. [17] described a solution where people being tagged in the uploaded photos can request the photo owner not to share the content with other users. Both these techniques give the privacy control to the photo owner, complementary to what is proposed in this paper. SnapMe [21] utilizes a cloud server to provide privacy policy while pAws [24] uses a privacy assistant server on the cloud to prevent sensing activity. Both of these solutions require connectivity to the cloud (network). NotiSense [28] provides useful notifications of nearby urban sensing activities to those who choose to subscribe by sending notification to users (directly or indirectly) when their photo is uploaded or shared. In Tricorder [26], which uses QR codes to display sensing activity, the user has to actively get privacy policy from the phone's sensor logger, while in our approach, the user does not do anything as the beacons will contain the privacy preference. TagSense [29] automatically tags, with some known context, of people who are inside a photo. However, it requires a session password before taking photos and can only those pre-registered with the system.

6. CONCLUSIONS

In this paper, we showed the feasibility of communicating IR signals to cameras. We showed that IR communication is more feasible indoors, where ranges of the order of few meters can be achieved. As IR signals are invisible to the human eye, such communications can be very useful in applications where high-priority or sensitive information can be directly communicated to cameras. The idea of communicating to cameras, as in our proposed system, is in direct contrast to communicating information through barcodes such as QR codes where camera communication is essentially just another means to send information. In our system the camera image as itself has key relevance, for example, as a privacy context. In this paper, we implemented a prototype transmitter hardware and camera receiver algorithm. We conducted experiments towards understanding *if a known IR signal can be reliably detected* and *if the channel quality is sufficient for IR communication to off-the-shelf cameras*. Our evaluations revealed that it is possible to detect the light signals within the photo capture duration with over 98% accuracy. We learned that the photo-capture duration is usually about 1.5 seconds using an electronic view-finder camera. We also computed the packet-error rate and bit-error rate

of the IR LED–camera channel in the indoor test environment to be within 7% and 10^{-3} respectively.

7. ACKNOWLEDGMENTS

This work is supported by the US National Science Foundation (NSF) under the grants CNS-1065463 and CNS-0845896. The authors would also like to thank the anonymous reviews for their valuable comments and suggestions.

8. REFERENCES

[1] Arduino Duemilanove. **http://arduino.cc/en/Main/arduinoBoardDuemilanove**.

[2] AXIS 213 PTZ Network camera. **http://www.axis.com/files/datasheet/ds_213ptz_33081_en_0909_lo.pdf**.

[3] Faces of Facebook, Privacy in the Age of Augmented Reality. **http://www.blackhat.com/docs/webcast/acquisti-face-BH-Webinar-2012-out.pdf**. Accessed: 2010-09-30.

[4] News - casio unveils prototype of visible light communication system. bit.ly/zpfjY1.

[5] OpenCV. **http://opencv.org/**.

[6] Platform for Privacy Preference (P3P) Project. **http://www.w3.org/P3P/**.

[7] Privacy Decisions for Location-Tagged Media. **http://infolab.stanford.edu/~mor/research/AhernUbi06PrivacyText.pdf**.

[8] Project glass by google. http://www.google.com/glass/start/.

[9] Seamless Customer Identification. **http://research.microsoft.com/en-us/um/people/ssaroiu/publications/tr/msr/msr-tr-2013-31.pdf**.

[10] TagMeNot. **tagmenot.info**.

[11] Visible light beacon system. http://home.jeita.or.jp/tsc/std-pdf/CP1223.pdf.

[12] Will Google Glass be the end of privacy. **http://www.debate.org/opinions/will-google-glass-be-the-end-of-privacy**.

[13] A. Ashok, M. Gruteser, N. Mandayam, J. Silva, M. Varga, and K. Dana. Challenge: mobile optical networks through visual mimo. In *Proceedings of the sixteenth annual international conference on Mobile computing and networking*, MobiCom '10, pages 105–112, New York, NY, USA, 2010. ACM.

[14] A. Ashok, S. Jain, M. Gruteser, N. Mandayam, W. Yuan, and K. Dana. Capacity of pervasive camera based communication under perspective distortions. In *Pervasive Computing and Communications (PerCom), 2014 IEEE International Conference on*, pages 112–120, March 2014.

[15] S. Baker and I. Matthews. Lucas-kanade 20 years on: A unifying framework. *International Journal of Computer Vision*, 56(3):221–255, 2004.

[16] A. Besmer and H. Lipford. Tagged photos: Concerns, perceptions, and protections. In *CHI '09 Extended Abstracts on Human Factors in Computing Systems*, CHI EA '09, pages 4585–4590, New York, NY, USA, 2009. ACM.

[17] A. Besmer and H. Richter Lipford. Moving beyond untagging: Photo privacy in a tagged world. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '10, pages 1563–1572, New York, NY, USA, 2010. ACM.

[18] A. Chattopadhyay and T. Boult. Privacycam: a privacy preserving camera using uclinux on the blackfin dsp. In *Computer Vision and Pattern Recognition, 2007. CVPR '07. IEEE Conference on*, pages 1–8, June 2007.

[19] A. Frome, G. Cheung, A. Abdulkader, M. Zennaro, B. Wu, A. Bissacco, H. Adam, H. Neven, and L. Vincent. Large-scale privacy protection in google street view. In *Computer Vision, 2009 IEEE 12th International Conference on*, pages 2373–2380, Sept 2009.

[20] T. Hao, R. Zhou, and G. Xing. Cobra: Color barcode streaming for smartphone systems. In *Proceedings of the 10th International Conference on Mobile Systems, Applications, and Services*, MobiSys '12, pages 85–98, New York, NY, USA, 2012. ACM.

[21] B. Henne, C. Szongott, and M. Smith. Snapme if you can: Privacy threats of other peoples' geo-tagged media and what we can do about it. In *Proceedings of the Sixth ACM Conference on Security and Privacy in Wireless and Mobile Networks*, WiSec '13, pages 95–106, New York, NY, USA, 2013. ACM.

[22] J. Kahn and J. Barry. Wireless infrared communications. *Proceedings of the IEEE*, 1997.

[23] M. Langheinrich. A privacy awareness system for ubiquitous computing environments. In *Proceedings of the 4th International Conference on Ubiquitous Computing*, UbiComp '02, pages 237–245, London, UK, UK, 2002. Springer-Verlag.

[24] M. Langheinrich. A privacy awareness system for ubiquitous computing environments. In G. Borriello and L. Holmquist, editors, *UbiComp 2002: Ubiquitous Computing*, volume 2498 of *Lecture Notes in Computer Science*, pages 237–245. Springer Berlin Heidelberg, 2002.

[25] D. G. Lowe. Object recognition from local scale-invariant features. In *Computer vision, 1999. The proceedings of the seventh IEEE international conference on*, volume 2, pages 1150–1157. Ieee, 1999.

[26] G. Maganis, J. Jung, T. Kohno, A. Sheth, and D. Wetherall. Sensor tricorder: What does that sensor know about me? In *Proceedings of the 12th Workshop on Mobile Computing Systems and Applications*, HotMobile '11, pages 98–103, New York, NY, USA, 2011. ACM.

[27] S. D. Perli, N. Ahmed, and D. Katabi. Pixnet: interference-free wireless links using lcd-camera pairs. In *ACM MobiCom*, 2010.

[28] S. Pidcock, R. Smits, U. Hengartner, and I. Goldberg. Notisense: An urban sensing notification system to improve bystander privacy.

[29] C. Qin, X. Bao, R. Roy Choudhury, and S. Nelakuditi. Tagsense: A smartphone-based approach to automatic image tagging. In *Proceedings of the 9th International Conference on Mobile Systems, Applications, and Services*, MobiSys '11, pages 1–14, New York, NY, USA, 2011. ACM.

[30] M.-R. Ra, R. Govindan, and A. Ortega. P3: Toward privacy-preserving photo sharing. In *Proceedings of the 10th USENIX Conference on Networked Systems Design and Implementation*, nsdi'13, pages 515–528, Berkeley, CA, USA, 2013. USENIX Association.

[31] N. Rajagopal, P. Lazik, and A. Rowe. Visual light landmarks for mobile devices. In *Proceedings of the 13th International Symposium on Information Processing in Sensor Networks*, IPSN '14, pages 249–260, Piscataway, NJ, USA, 2014. IEEE Press.

[32] T. Rappaport. *Wireless Communications: Principles and Practice*. Prentice Hall, 2nd edition, 2001.

[33] P. Viola and M. Jones. Rapid object detection using a boosted cascade of simple features. In *Computer Vision and Pattern Recognition, 2001. CVPR 2001. Proceedings of the 2001 IEEE Computer Society Conference on*, volume 1, pages I–511–I–518 vol.1, 2001.

[34] T. Yamada, S. Gohshi, and I. Echizen. Use of invisible noise signals to prevent privacy invasion through face recognition from camera images. In *Proceedings of the 20th ACM International Conference on Multimedia*, MM '12, pages 1315–1316, New York, NY, USA, 2012. ACM.