https://doi.org/10.2352/ISSN.2470-1173.2021.4.MWSF-346

Proximally Secure Communication in Public Settings Using Specialized Barcodes

Irving R. Barron, Gaurav Sharma; Department of Electrical and Computer Engineering, University of Rochester; Rochester, NY, USA

Abstract

We present a scheme for securely communicating data over close distances in public settings. Exploiting the ubiquity of cameras in modern day devices and the high resolution of displays, our approach provides secure data communication over short distances by using specialized 2-D barcodes along with an adaptive protocol. Specifically, the barcodes carry public data compatible with their conventional design and additionally private data through specialized orientation modulation in the barcode modules. The latter is reliably decoded when the barcodes are captured at close distances but not from farther distances, a property that we call "proximal privacy". The adaptive protocol dynamically modifies the strength of the orientation modulation until it is just recoverable by the capture camera. We validate our approach via simulations and by using physical devices to display and capture the specialized barcodes.

Introduction

Traditionally, individuals have relied on physical proximity to provide a measure of privacy/security, even when communicating information in public settings, for instance, when speaking with someone nearby or when entering a password on one's computer. This proximal notion of security is increasingly threatened by the ubiquitous presence of surveillance systems and mobile devices in public places. In this paper, we present an imaging based approach for securely communicating data at proximal distances that itself relies on the ubiquity of cameras in modern day computational devices.

Although the secure communication over proximal distances could be used for a variety of applications, we showcase our approach using the specific use case of password communication for user-login, which is illustrated in Fig. 1. A surveillance camera can easily record a user logging-in to a laptop and later reveal the password by analyzing the captured video. Even when the keyboard is not in direct sight of the camera, sophisticated techniques can be used to reveal the private password in such settings [1, 2]. For smartphones and tablet devices, increasingly available biometric authentication partly addresses the challenge of password revelation from keyboard entry. Innovative image processing based approaches that rely on the changing perception of imagery with distance have also been proposed for masking the password from the eyes of prying neighbors [3]. Nevertheless, the problem persists for other devices for which a keyboard is the main input method (e.g., laptops, kiosks, etc.).

Specifically, we exploit 2-D specialized barcodes, an augmentation of conventional 2-D barcodes, that carry public and private data. The QR code version of the specialized barcodes was presented in our recent work [4], but, as we note here, the

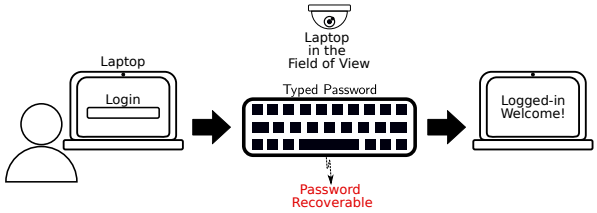


Figure 1: Device log-in in a public setting where video surveillance is present, which can compromise the password.

underlying methodology can be used for any of the common 2-D barcode designs (e.g., QR, Aztec, Data Matrix [5, 6, 7]). Individual modules for these barcode designs carry a binary digit based on whether they are white or black. The public data in our specialized barcodes is embedded in a manner compatible with the underlying 2-D barcode design by using modules that convey a bit value based on whether they are white or contain a black elliptical dot. The private data is embedded within the same barcode spatial footprint by exploiting the high resolution that is available on modern displays. Specifically, the orientation of the elliptical dots in the barcode modules is modulated to carry the private data. Because it becomes harder to identify the orientation of the elliptical dots as the capture distance increases, the private data is decodeable only when the capture camera is close to the displayed barcode, whereby the specialized barcode design offers proximal privacy for the private data. We combine the specialized barcodes with an adaptive protocol that adjusts the strength of the orientation modulation to just allow for decoding by the target camera, thus preserving privacy better than conventional 2-D barcodes. The work presented here incorporates and builds upon our recent work [4]. Here, however, we consider additional barcode designs beyond QR codes and focus on their use in tandem with the adaptive protocol.

This paper is organized as follows. First, the different elements of the proposed approach are detailed. Next, we describe the experimental set up and performance evaluation criteria for assessing the proposed approach and present results that validate the proposed methodology. Then, we present a discussion that highlights the pros/cons of the proposed approach, contrasting these with other alternatives. Finally, we conclude the paper by summarizing our main findings.

Proposed Approach

The proposed approach has two key components: specialized barcodes and an adaptive protocol. Figure 2 illustrates both components. Fig. 2 (a) shows two specialized barcodes, based on the design of QR and Aztec codes, and highlights how the public and private data are embedded. Fig. 2 (b) illustrates the adaptive

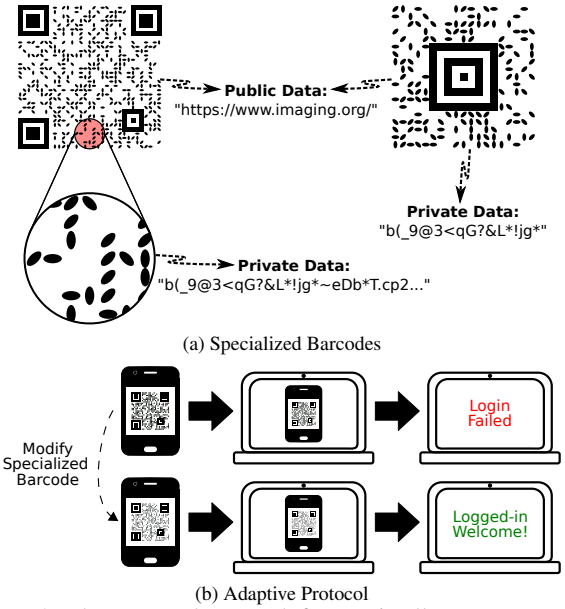


Figure 2: The proposed approach for proximally secure communication in public settings has two key components. (a) specialized barcodes that carry public data (through variations in intensity of the data carrying modules) and private data (via the orientation of elliptical dots), and (b) an adaptive protocol that increases the eccentricity until the decoding threshold is just met for the private data.

protocol where a dynamically updating version of the specialized barcode is used to communicate a website to log-in and the appropriate credentials, using the public and private data, respectively. In the displayed specialized barcode, the strength of the orientation modulation used for embedding the private data is increased just until the point where the target camera successfully decodes the data (and access to the website is granted). Next, we detail the individual components of the proposed approach.

Specialized Barcodes

The specialized barcodes augment the underlying 2-D barcode designs and we describe these modifications in turn for the barcode encoding and decoding processes.

Encoding

Using an Aztec code [6] as an example, Figure 3 illustrates how the traditional 2-D barcode encoding process is modified for the proposed specialized barcodes. In the traditional 2-D barcode, the synchronization patterns establish the overall geometry for the encoding process, defining a grid of square modules. Bits of data are carried in individual square shaped modules (other than those used for synchronization) by rendering the module black or white depending on the value of the data bit. For our specialized barcodes, first a conventional 2-D barcode is generated that encodes the public data. The resulting conventional 2-D barcode is then modified to embed the private data. Specifically, the private data embedding process modifies the black data-carrying modules in the conventional 2-D barcode; the black square in the module is replaced by an elliptical dot centered within the module and with an orientation determined by the private data. In practice, the two steps for embedding the public and private can be combined and there is no need to first generate the conventional 2-D barcode. Angularly equispaced orientation choices are used for the private data embedding, where the number of orientations used for the embedding of the private data is a design choice for the specialized barcodes that we investigate subsequently.

Note that both the public and private data are protected from errors using error correction codes. To ensure that the specialized barcodes remain decodeable with regular decoders for the conventional barcodes (i.e., maintain decoding compatibility), the error correction coding (as well as other pre-processing steps) are maintained identical to those used for the conventional barcodes.

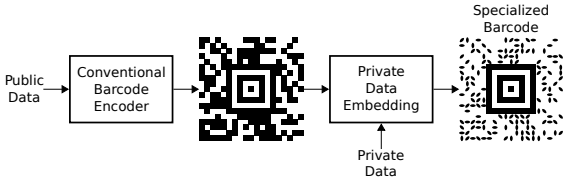


Figure 3: Encoding process for the specialized barcodes.

Decoding

Figure 4 illustrates the decoding process for the proposed specialized barcodes. First, using a decoder for the conventional 2-D barcode, the public data is decoded from the captured image of the barcode. Just like the black modules in the conventional 2-D barcodes the modules with the elliptical dots in our specialized barcodes are darker than the white modules, so conventional barcode decoders are able to decode the public data (for reasonable design choices). The decoding of the public data also synchronizes the captured image to the geometry of the barcode and identifies the elliptical dot carrying modules. By estimating the orientations of the dots within these modules (see [4] for details), the private data can then be decoded in turn. To make the data recovery more resilient, both public and private data decoding processes incorporate error correction decoding matched with the error correction codes used in the encoding process.

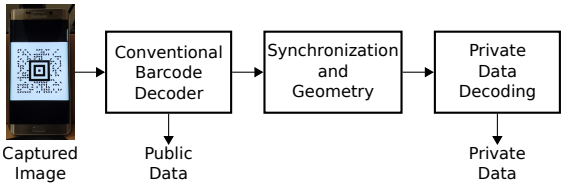


Figure 4: Decoding process for the specialized barcode.

Adaptive Protocol

The decoding of the private data relies on discerning the orientations of the elliptical dots in the captured image. The ability to discern the different orientations is determined by both the eccentricity of the elliptical dots used in the specialized barcodes and the capture distance. As shown in Fig. 5, the adaptive protocol exploits this interplay for enhancing the proximal privacy. When the specialized barcode is first displayed, the dots are circular with no discernible orientation. At this point, the target camera capturing an image of the specialized barcode can localize the barcode and decode the public data but not the private data. Once localization and synchronization of the barcode are established,

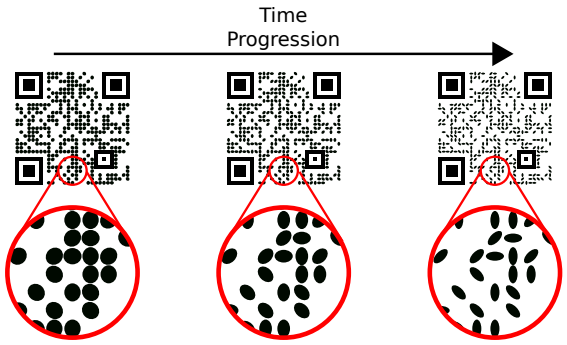


Figure 5: Adaptive protocol that progressively increases eccentricity of the ellipses in the specialized barcodes until the private data is just decodeable for the target camera.

the eccentricity of the dots is progressively increased by shrinking the minor axes of the oriented ellipses until the target camera is just able to decode the private data. Thus, the protocol effectively constrains the capture distances at which the private data is recoverable, making the approach better suited for private communication in public settings.

Experiments and Results

We validate the proposed approach by conducting extensive simulations and a smaller set of experiments with physical display/capture devices. The simulations allow us to effectively determine a comfortable decoding envelope which then help us choose the parameters for the experiments with psychical devices.

For the experiments, we created specialized barcodes that carry a website and a secure password, generated from [8], as the public and private data, respectively. The embedding of the private data considered $2, 4$, and 8 orientation choices[1]. Error correction encoding of the public data is achieved by following the appropriate 2-D barcode framework, while the private data was encoded using a rate $1/2$ convolutional code [9].

For public data decoding, we used the open-source ZXing [10] barcode decoder. The approach described in [4] was utilized for the private data decoding. To quantify the performance of the proposed approach, for public/private data we used the decoding success rate (DSR). The DSR indicates the percentage of specialized barcodes from which the public data and private data are successfully recovered after error correction decoding.

For the simulations, we considered capture distances of $3, 6, 9, 12, 15, 18$ inches. The eccentricity of the elliptical dots was controlled by setting the ratio of the minor axis to the major axis, which started with a value of 1 (corresponding to a circle) and was decremented in steps of 0.1. To conduct the simulations, we use the framework presented in [11], for which a corresponding toolkit is available [12]. The simulated display was chosen from the toolkit to correspond to a 326 pixels per inch (PPI) Apple LCD monitor. The resolution is comparable to that of a (several generations old) iPhone 7 display, representing the low end (and therefore more challenging) resolutions. For the simulated camera (capture device), we chose a fixed focus sensor with resolution of 1280×720 pixels, which also represents the low end of what would be seen in current laptop webcams. For the simulated camera, we assumed an ideal fronto-parallel geometry capture. To account for image compression, the simulated captured images were stored as JPEG files with a quality factor of 90[2]. The simulated captured images were then used as input for the specialized barcode decoder and the DSR statistics were computed for the public/private data over 250 Monte-Carlo simulations.

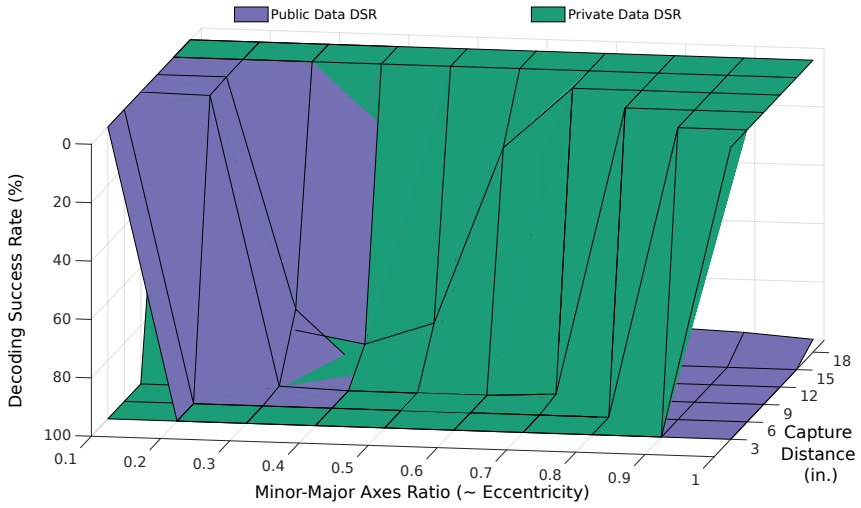
Fig. 6 shows the results from the simulations, where the results for the 2, 4, and 8 orientation choices are shown as sub-figures (a), (b), and (c), respectively. In these sub-figures, the surface plots show the DSR as a function of the capture distance and the eccentricity (of the elliptical dots) for the public and private data as 3-D surfaces that are colored purple and green, respectively. The eccentricity of the elliptical dots is quantified by the ratio of minor to major axes (lengths). To render the region of our particular interest, over which the DSR approaches 100% for both the public and private data, clearly visible, the z-axis scale is inverted, i.e., the maximum DSR is at the bottom. For 2 and 4 orientations Fig. 6 (a) and (b) exhibit similar performance, and in both cases there is a comfortable decoding envelope for the proposed approach. For low eccentricity and proximal distances, the public data is recovered with 100% DSR when starting with the circular dots (minor-major axes ratio of 1) and this remains the case as the eccentricity is increased, until a the minor-major axes ratio is reduced to 0.4. The private data is unrecoverable (0% DSR) when starting with the circular dots (minor-major axes ratio of 1) and, for proximal distances under 9 inches, the DSR increases rapidly as the eccentricity increases (minor-major axes ratio decreases). We can see that the adaptive protocol in the proposed approach would accomplish the desired objective of communicating both the private and public data successfully for capture distances of 3, 6, and 9 inches when the minor-major axes ratio reaches a value of 0.9, 0.8, and 0.7, respectively. Over the corresponding operating range, the private data remains unrecoverable (0% DSR) for distances larger than 15 inches. For 8 orientations Fig. 6 (c) illustrates that the private data is unrecoverable throughout the parameter range as the closer angular spacing of the orientations cannot be reliably determined by the decoder.

Based on the results from the simulations, for experiments with actual physical devices, we chose the specialized barcodes with 4 orientation choices. Furthermore, we started with an initial minor-major axes ratio of 0.9 reduced it in steps of 0.1 as in the simulations. For displaying the barcodes we used two smartphones (a Xiaomi Mi 8 and an Apple iPhone XR) for the capture we used two laptops (a Lenovo Yoga 730, a Dell Inspiron 13-7368), and a tablet (a 6th generation iPad). The images of the barcodes displayed on the phones were captured from distances of $6, 9$, and 12 inches. As a baseline to compare our proposed approach, we also tested a comparable 2-D barcode carrying the same strong password embedded as the private data in the specialized barcode.

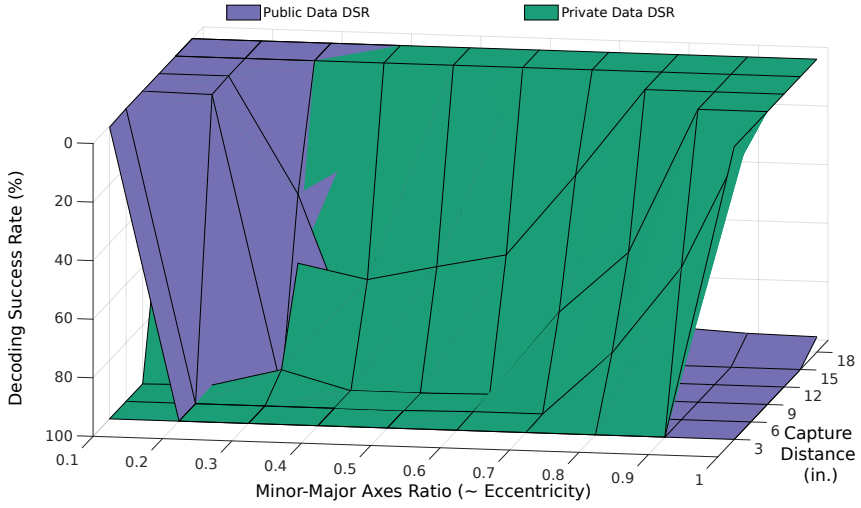
The results from the experiments with actual devices are depicted in Fig. 7 where the plots show the average DSR (across the capture/display device combinations) as a function of the eccentricity of the elliptical dots (minor-major axes ratio) for capture distances of $6, 9$, and 12 inches in sub-figures (a), (b), and (c),

[1]The embedded passwords for 2, 4, and 8 orientation choices for the elliptical dots, the passwords' used were 20, 40 and 60 ASCII characters (bytes) long, respectively.

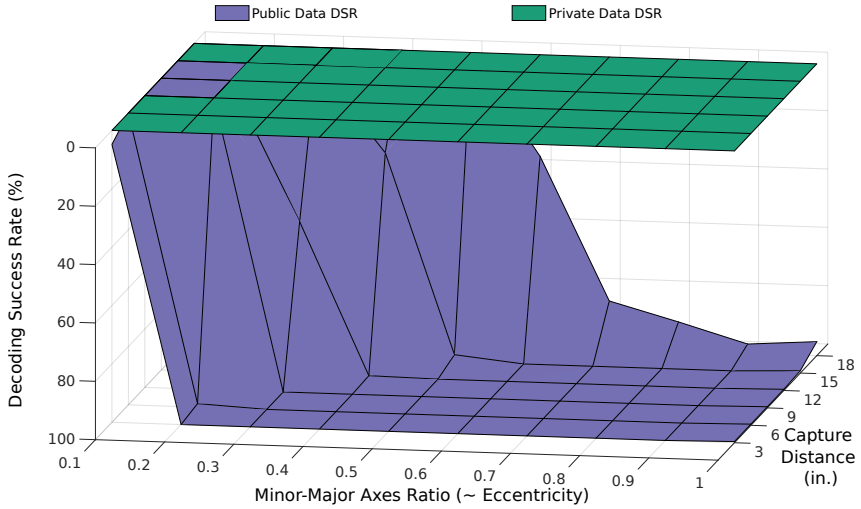
[2]Other simulation parameters, including image capture noise, were kept at the default values in [12].



(a) 2 Orientations

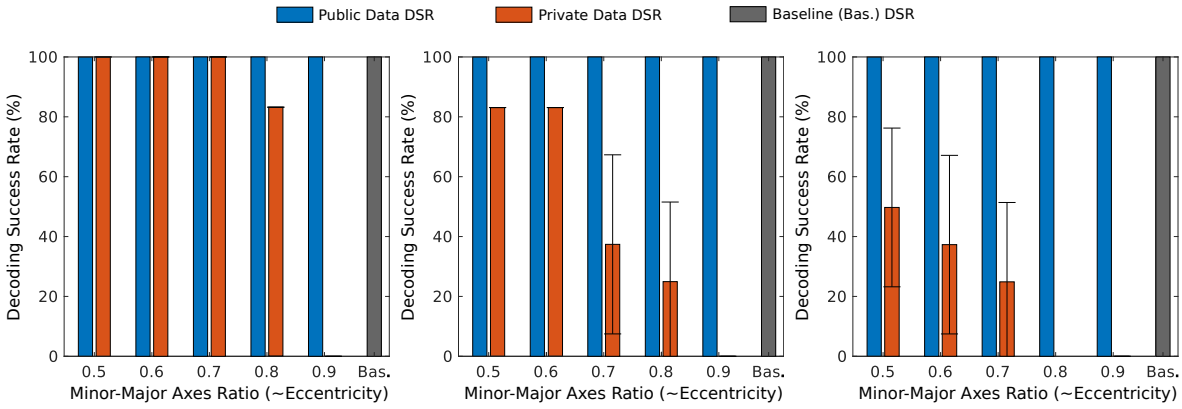


(b) 4 Orientations



(c) 8 Orientations

Figure 6: Simulation results for the proposed approach. Decoding success rate (DSR) as a function of the minor-major axes ratio (which is inversely related to eccentricity of the elliptical dots used for conveying the private data) and capture distance for (a) 2, (b) 4 and (c) 8 orientations. The plots indicate a comfortable operating envelope for the proposed approach for proximal distances under 9 inches for the 2 and 4 orientation choices. Note that the z-axis is inverted and thus, the DSR is 0% at the top and 100% at the bottom.



(a) Capture distance = 6 inches (b) Capture distance = 9 inches (c) Capture distance = 12 inches

Figure 7: Results from experiments on actual devices for the proposed approach with 4 orientation choices for capture distances of (a) 6, (b) 9, and (c) 12 inches. The average DSR across the display/device combinations (see text for specific device models) is shown as a function of the minor-major axes ratio (which is inversely related to eccentricity of the elliptical dots used for conveying the private data). The plots reinforce the simulations and indicate a comfortable operating envelope for the proposed approach at proximal distances.

respectively. The error bars indicate one standard deviation intervals. These results reiterate and reinforce the findings from the simulations. We can see that the adaptive protocol in the proposed approach can accomplish the desired objective of communicating both the private and public data successfully for proximal capture distances and over the corresponding region of operating parameters, the private data remains unrecoverable from larger capture distances. Note that in contrast with the specialized barcodes used in the proposed approach, the baseline conventional 2-D barcode is reliably decoded at all the three capture distances.

Discussion

Psychologists consider the boundary of a person's intimate space to be defined by a distance of about 18 inches from the person [13, pp. 117]). The results in the previous section demonstrated that the proposed approach can accomplish its desired objective of communicating data within this intimate space while keeping the data private from most adversaries that are likely to be encountered in public spaces. Specifically, if the adversary is using equipment comparable to the primary user, to recover the private data, they would have to overcome significant challenges due to larger capture distances and sub-optimal capture geometry. While a well-resourced adversary, could potentially use a camera with a high optical zoom and a tripod, they would also have a limited time window and exposure duration over which they would need to capture a high resolution image of the displayed specialized barcodes that are dynamically changing under the adaptive protocol. Additionally, the bulk of such equipment is itself likely to attract attention, get recorded in surveillance video, and noticed by users of the proposed approach.

As an alternative to the proposed approach, one may also consider simply adapting the size of a conventional barcode to limit the distance over which it is decodeable. While such an approach is indeed feasible, it conflates the three tasks of synchronization, public, and private data communication, which are advantageously separable in the proposed approach with the specialized barcodes. Additionally, having both public and private data in a single barcode can also enable more applications.

Conclusion

The proposed approach presented in this paper enables proximally secure communication in public settings. The security is provided by a combination of specialized barcodes and an adaptive protocol. Specifically, the specialized barcodes carry public/private data with the later being only decodeable from an image of the specialized barcode captured at proximal distances while the adaptive protocol augments the proximal privacy of the specialized barcodes by adjusting the strength of the embedding used for the secondary data such that it is just decodeable by the target camera. Simulations and experiments with actual devices demonstrate that the proposed approach achieves its desired objective of communicating both the private and public data successfully for proximal capture distances while keeping the private data secure from distant capture distances.

Acknowledgments

We thank the Center for Integrated Research Computing, University of Rochester, for providing access to computational resources for this work. Irving R. Barron thanks Dr. Gaurav Sharma, the University of Rochester and CONACYT for supporting his PhD.

References

[1] Yi Xu, Jared Heinly, Andrew M. White, Fabian Monrose, and Jan-Michael Frahm. Seeing double: Reconstructing obscured typed input from repeated compromising reflections. In *Proc. ACM SIGSAC Conf. Comput. & Commun. Secur.*, pages 1063–1074, 2013. doi:10.1145/2508859.2516709.

[2] D. Shukla and V. V. Phoha. Stealing passwords by observing hands movement. *IEEE Trans. Inf. Forensics Security*, 14(12):3086–3101, Dec. 2019. doi:10.1109/TIFS.2019.2911171.

[3] A. Papadopoulos, T. Nguyen, E. Durmus, and N. Memon. Illusion-PIN: Shoulder-surfing resistant authentication using hybrid images. *IEEE Trans. Inf. Forensics Security*, 12(12):2875–2889, December 2017. doi:10.1109/TIFS.2017.2725199.

[4] I. R. Barron, H. S. Yeh, K. Dinesh, and G. Sharma. Dual modulated QR codes for proximal privacy and security. *IEEE Trans. Image Proc.*, 30:657–669, 2021. doi:10.1109/TIP.2020.3037524.

[5] ISO/IEC. ISO/IEC 18004:2015: information technology — automatic identification and data capture techniques — QR code bar code symbology specification, Feb. 2015. accessed May 18, 2020. URL: https://www.iso.org/standard/62021.html.

[6] A. Longacre and R. Hussey. Two dimensional data encoding structure and symbology for use with optical readers. United States Patent 5,591,956, 7 January 1997.

[7] The 2D data matrix barcode. *Computing Control Engineering Journal*, 16(6):39, January 2005. doi:10.1049/ccej:20050609.

[8] Secure password generator. accessed Oct. 17, 2019. URL: https://passwordsgenerator.net/.

[9] S. G. Wilson. *Digital Modulation and Coding*. Prentice-Hall, Upper Saddle River, NJ, 1996.

[10] ZXing C++ port. accessed Oct. 15, 2019. URL: https://github.com/glassechidna/zxing-cpp.

[11] Joyce E. Farrell, Peter B. Catrysse, and Brian A. Wandell. Digital camera simulation. *Appl. Opt.*, 51(4):A80–A90, Feb. 2012. doi:10.1364/AO.51.000A80.

[12] ISETCam. accessed Oct. 19, 2019. URL: https://github.com/ISET/isetcam.

[13] E.T. Hall. *The Hidden Dimension*. Doubleday, New York, NY, 1966.

Author Biography

Irving R. Barron obtained the Engineer's degree in electronic engineering and Master's degree in electronic engineering specialized in digital signal processing from the Universidad Autónoma de San Luis Potosí, San Luis Potosí, México. He is currently a PhD student working towards his degree at the University of Rochester under the supervision of Dr. Gaurav Sharma.

Gaurav Sharma is a professor at the University of Rochester in the Department of Electrical and Computer Engineering, in the Department of Computer Science, and in the Department of Biostatistics and Computational Biology. He is the editor of the Color Imaging Handbook, published by CRC Press in 2003. He is a fellow of the Society of Imaging Science and Technology (IS&T), of SPIE, and of the IEEE, and a member of Sigma Xi.

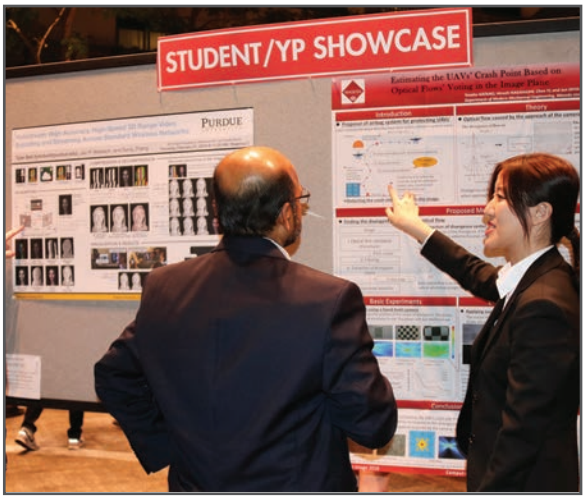
JOIN US AT THE NEXT EI!

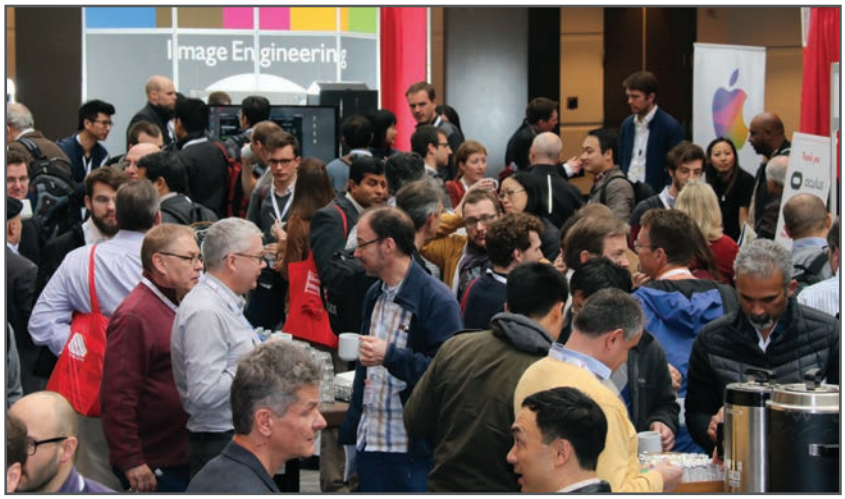
IS&T International Symposium on

Electronic Imaging

SCIENCE AND TECHNOLOGY

Imaging across applications . . . Where industry and academia meet!





• SHORT COURSES • EXHIBITS • DEMONSTRATION SESSION • PLENARY TALKS •
• INTERACTIVE PAPER SESSION • SPECIAL EVENTS • TECHNICAL SESSIONS •

www.electronicimaging.org

IS&T
imaging.org