Demo: A Prototype Vision Sensor for Real-time Focal-plane Obfuscation through Tunable Pixelation

J. Fernández-Berni
Inst. of Microelectr. of Seville
CSIC - Universidad de Sevilla
berni@imse-cnm.csic.es

R. Carmona-Galán
Inst. of Microelectr. of Seville
CSIC - Universidad de Sevilla
rcarmona@imse-cnm.csic.es

Rocío del Río
Inst. of Microelectr. of Seville
CSIC - Universidad de Sevilla
rocio@imse-cnm.csic.es

R. Kleihorst
Ghent University
iMinds/Ugent-IPI
rkleihor@telin.ugent.be

W. Philips
Ghent University
iMinds/UGent-IPI
philips@telin.ugent.be

Á. Rodríguez-Vázquez
Inst. of Microelectr. of Seville
CSIC - Universidad de Sevilla
angel@imse-cnm.csic.es

ABSTRACT

Privacy concerns are hindering the introduction of smart camera networks in prospective application scenarios like retail analytics, factory monitoring or elderly care. The idea of networked cameras pervasively collecting data generates social rejection in the face of sensitive information being tampered by hackers or misused by legitimate users. New strategies must be developed in order to ensure privacy from the very point where sensitive data are generated: the sensors. Protection measures embedded on-chip at the front-end sensor of each network node significantly reduce the number of trusted system components as well as the impact of potential software flaws. In this demonstration, we present a full-custom QVGA vision sensor that can be reconfigured to implement programmable pixelation of image regions at the focal plane. In particular, we show on-the-fly focal-plane face obfuscation supported by the Viola-Jones frontal face detector provided by OpenCV.

Categories and Subject Descriptors

Hardware [**Very large scale integration design**]: Full-custom circuits

General Terms

Algorithms, Security

Keywords

Smart Cameras, Privacy, Security, Vision Sensor, Focal-plane Processing, Obfuscation, Pixelation

ICDSC '14, November 04 - 07 2014, Venezia Mestre, Italy

http://dx.doi.org/10.1145/2659021.2669473

1. INTRODUCTION

Pervasive surveillance by networked image sensors creates legal and societal concerns. Citizens' sensitive information can be put at risk, causing people to reject the technology. Indeed, identifiable personal data—faces, clothes, wearables etc—can usually be discarded when it comes to performing a meaningful visual analysis in prospective application frameworks of smart camera networks like retail analytics, factory monitoring or elderly care. Time spent by customers in front of a showcase, trajectories of workers around a manufacturing site or fall detection in a nursing home are three examples where video analytics could be realized without compromising privacy. However, the concerns are understandably still there. The limitations of current smart imaging systems to ensure privacy come from the significant number of key system components that are part of the implicitly trusted software base: the operating system, the network stack, system libraries etc. It is not possible to provide complete assurance about the potential security and privacy flaws contained in this software [4]. Even widely adopted cryptography libraries are not free of such flaws [3]. A possible hardware-based approach to overcome these limitations is to convey protection as close to the sensor device as possible. The ideal framework would be a front-end vision sensor delivering a data flow stripped off sensitive information. On-chip implementation of privacy awareness would still have to accommodate some degree of reconfigurability in order to balance protection and viability of the video analytics required by particular algorithms. Once protection measures are embedded on-chip at the front-end sensor of each network node, the number of trusted components as well as the impact of potential software flaws are significantly reduced. In this demonstration, we show a 320×240-px prototype vision sensor embedding processing capabilities useful for accomplishing this objective.

2. A QVGA VISION SENSOR WITH MULTI-FUNCTIONAL PIXELS

We have developed a low-power vision sensor aiming at balancing processing flexibility and privacy protection. It is based on the concept of focal-plane sensing-processing [5], arguably the best architectural approach reported in terms of adaptation to the particular characteristics of early vision.

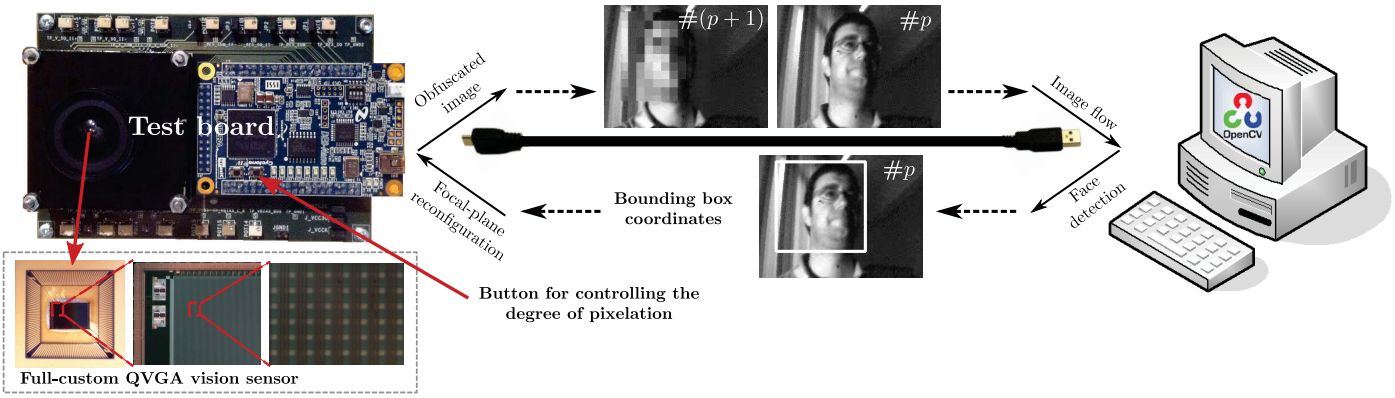

Figure 1: General scheme of the demonstration.

Sensitive image regions can be obfuscated through tunable pixelation just at the focal plane. This permits to preserve the remaining image information if needed. The reconfiguration of the chip to dynamically accommodate vision algorithm requirements takes place on-the-fly. The proposed sensing-processing scheme is also suitable to build a granular space [1] by exploiting focal-plane distributed memory. This granular space constitutes the raw material for subsequent recognition of categorized objects. It can also be adjusted, if afforded by the targeted application, to operate with coarse enough granule scales for the sake of privacy. In such a case, we would be concurrently combining purposeful power-efficient focal-plane processing and privacy protection. Other processing primitives like block-wise High Dynamic Range (HDR), integral image computation and Gaussian filtering can also be implemented by the prototype [2].

For testing and demonstration purposes, the vision sensor has been embedded into a system based on the commercial FPGA-based *DE0-Nano* board from terasIC. The output data flow provided by the sensor is stored in the internal memory of the FPGA for its subsequent serial transmission to a PC through a USB interface. A general scheme of the demonstration is depicted in Fig. 1. The sensor captures images that are sent to a PC from the test board. The Viola-Jones frontal face detector provided by OpenCV is run on these images on the PC. If faces are detected, the coordinates of the corresponding bounding rectangles are sent back to the test board for the vision sensor to reconfigure the image capture in real time. Pixelation of the face regions will take place from that moment on at the focal plane. The degree of pixelation of these regions is adjustable through a button of the test board. Up to three faces can be obfuscated at the focal plane simultaneously. A sequence extracted during the execution of this demo can be download from www.imse-cnm.csic.es/mondego/Sensors/.

3. CONCLUSIONS

The deployment of ubiquitous networked visual sensors seamlessly integrated in our daily lives is still far from being achieved. Privacy and power consumption are two major barriers to be overcome. Once visual information is disconnected from private data and locally processed by low-power trusted computing devices, a wide range of innovative applications and services will be able to be addressed; applications and services now impossible to be implemented because current technology collides with legal constraints and public rejection. This demo shows a full-custom QVGA vision sensor based on focal-plane sensing-processing, a suitable architectural approach to explore privacy protection for smart camera networks. First, sensitive information obfuscated from the very point where it is captured cannot be tapped by design. Second, focal-plane sensing-processing features an architecture adapted for the efficient exploitation of the inherent properties of vision.

4. ACKNOWLEDGMENTS

This work has been funded by the Spanish Government through projects TEC2012-38921-C02 MINECO (European Region Development Fund, ERDF/FEDER), IPT-2011-1625-430000 MINECO and IPC-20111009 CDTI (ERDF/FEDER), by Junta de Andalucía through project TIC 2338-2013 CE-ICE, by the Office of Naval Research (USA) through grant N000141410355 and by the Faculty of Engineering of Ghent University through its program for visiting foreign researchers.

5. REFERENCES

[1] H. Chang, A. Haizhou, L. Yuan, and L. Shihong. Learning sparse features in granular space for multi-view face detection. In *Int. Conf. on Automatic Face and Gesture Recognition (FGR)*, pages 401–406, 2006.

[2] J. Fernández-Berni, R. Carmona-Galán, R. del Río, and A. Rodríguez-Vázquez. A QVGA vision sensor with multi-functional pixels for focal-plane programmable obfuscation. In *Int. Conf. on Distributed Smart Cameras*, 2014.

[3] OpenSSL Project. Heartbeat overflow issue. `https://www.openssl.org/news/secadv_20140407.txt`, 2014. [Online; accessed 15-April-2014].

[4] T. Winkler and B. Rinner. Sensor-level security and privacy protection by embedding video content analysis. In *IEEE Int. Conf. on Digital Signal Processing (DSP)*, 2013.

[5] A. Zarándy, editor. *Focal-plane Sensor-Processor Chips*. Springer, 2011.