International Journal of Innovative Research in Computerand Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | Impact Factor: 7.488 |

||Volume 8, Issue 6, June 2020||

Eye Tracking Password Using Blinking Verification System

Sristi V[1], Sushmitha Katherine J[2], Tejasvi M G[3], Tinki Rani[4], Ms. Sandhya Rani[5]

Final year B.E Students (UG),Department of Information Science & Engineering, The Oxford College of Engineering, Bangalore, India[1,2,3,4]

Assistant Professor, Department of Information Science & Engineering, The Oxford College of Engineering, Bangalore, India[5]

ABSTRACT: Personal identification numbers are widely used for user authentication and security. Password authentication using PINs requires users to physically input the PIN, which could be vulnerable to password cracking via shoulder surfing or thermal tracking. PIN authentication with hands-off gaze-based PIN entry techniques, on the other hand, leaves no physical footprints behind and therefore offers a more secure password entry option. Gaze based authentication refers to finding the eye location across sequential image frames, and tracking the center of the eye over time. This paper presents a real-time application for gaze-based PIN entry, and eye detection and tracking for PIN identification using a smart camera.

KEYWORDS: Pins, Smart camera, Real-time systems, Authentication, Gaze tracking, Password

I.INTRODUCTION

The use of Personal Identification numbers (PINs) is a common user authentication method for many applications, such as money management in automatic teller machines (ATMs), approving electronic transactions, unlocking personal devices, and opening doors.

Flawless identity authentication remains a challenge even when PIN authentication is used, such as in financial systems and gate access control. According to the European ATM Security, fraud attacks on ATMs increased by 26% in 2016 compared to that of 2015. The fact that an authorized user must enter the code in open or public places make PIN entry vulnerable to password attacks, such as shoulder surfing and thermal tracking.

The purpose of this work is to enter and identify gaze-based PINs using a smart camera throughreal-timeeyedetectionandtracking.NIVisionBuilderandLabVIEWareusedfor eye tracking and for recording eye center location on board the camera real-time.

The smart camera allows on-board data processing and collection. Non-contact PIN based authentication adds a layer of security to physical PIN entries and are expected to reduce the vulnerability of the authentication process.

II. LITERATUREREVIEW

The current state of functioning systems in offline mode

- With theproject of digitalization of academic and administrative affairs in UP, the phase of complete computerized services has begun.The results obtained from this work are tested and successfully implemented in the Electronic Student Management System (ESMS) also developed from UP. The aim of this paper is to provide new results for data synchronization in different platforms through Web services, which allow software applications to run or to be executed online and offline as well.

Implementation of the proposed solution for ESMS in offline mode

- Files will be transferred as data and not as files, but the central server will return the file format.To provide both modes of operation, ESMS has built a system which enables the data synchronization between faculties that are working offline with the primary system, in the main data base, so that the data could still be synchronous and up to date with the work done in all the different units.For this purpose, it has been provided the data synchronization, for the units working in “Offline” mode, with the primary system andthe network infrastructure that will support the

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | Impact Factor: 7.488 |

||Volume 8, Issue 6, June 2020||

implementation of such technology serving the UP and its data synchronization in both "Offline" and "Online" mode and vice versa.

III. PROBLEMSTATEMENT

The main problem in the existing system is that it is not very secure. Passwords typed on a keypad are easy to hack, which poses a major question on its security. Another problem that exists in the existing system is accuracy. Most of the existing systems are sensor based that makes them inaccurate. Also, not to mention the inconvenience that comes with some head-controlled systems where physical movement is required.

IV. EXISTINGSYSTEM

Systems that have been used for a long time now have some demerits. They have undoubtedly served their purpose but there are instances that make us question the security and accuracy of these systems. As we all know, keypad-based systems are easy to hack, voice-controlled systems are user specific and most systems are sensor dependent which make them mostly inaccurate. It is now a general tendency to make systems more convenient for the users. Hence, the attempt to upgrade from the inconvenience of using head-controlled systems where physical movements are required.

V. PROPOSED SYSTEM

The proposed system is an eye recognition-controlled locker. Eye tracking technology, which is based on an eye tracker that measures the movement and positions of the eye. A mounted camera will recognize the eye and lock and unlock the locker. NI Smart Cameras are industrial, high-quality image sensors combined with powerful processors to create rugged, all-in-one solutions for machine vision applications. The first part is the head mounted camera that will track the camera wearer's eye using Arduino. The microprocessor will take a USB output from the camera and convert the signal into signals that will be sent to the locker. The final part of the project is the motor drivers to interface with the locker itself.

A. SYSTEM ARCHITECTURE

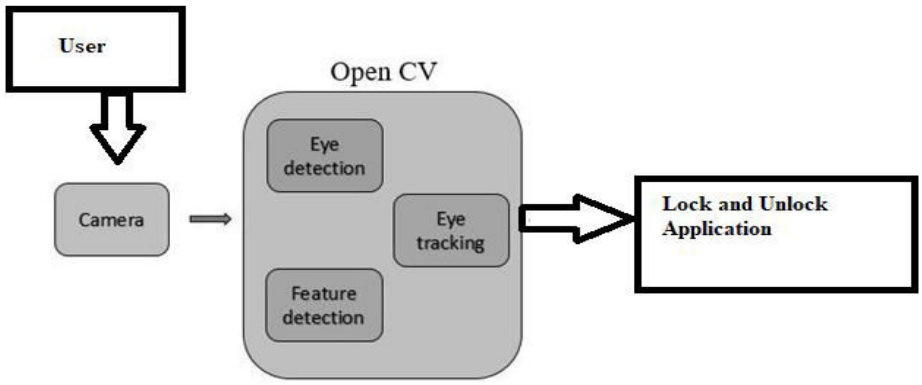

Fig 1: System Architecture

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | Impact Factor: 7.488 |

||Volume 8, Issue 6, June 2020||

The system consists of 4 parts. The user looks into the camera and the user's face is captured by the camera. The image is then processed using the Haar Cascade and the Facial Landmark algorithm to calculate the structure of the face and to detect the eyes on it. Then the pupil is detected.
After which the process of feature extraction takes place. Once that is done, the data is trained and tested based on the prior data stored.

B. WORKING

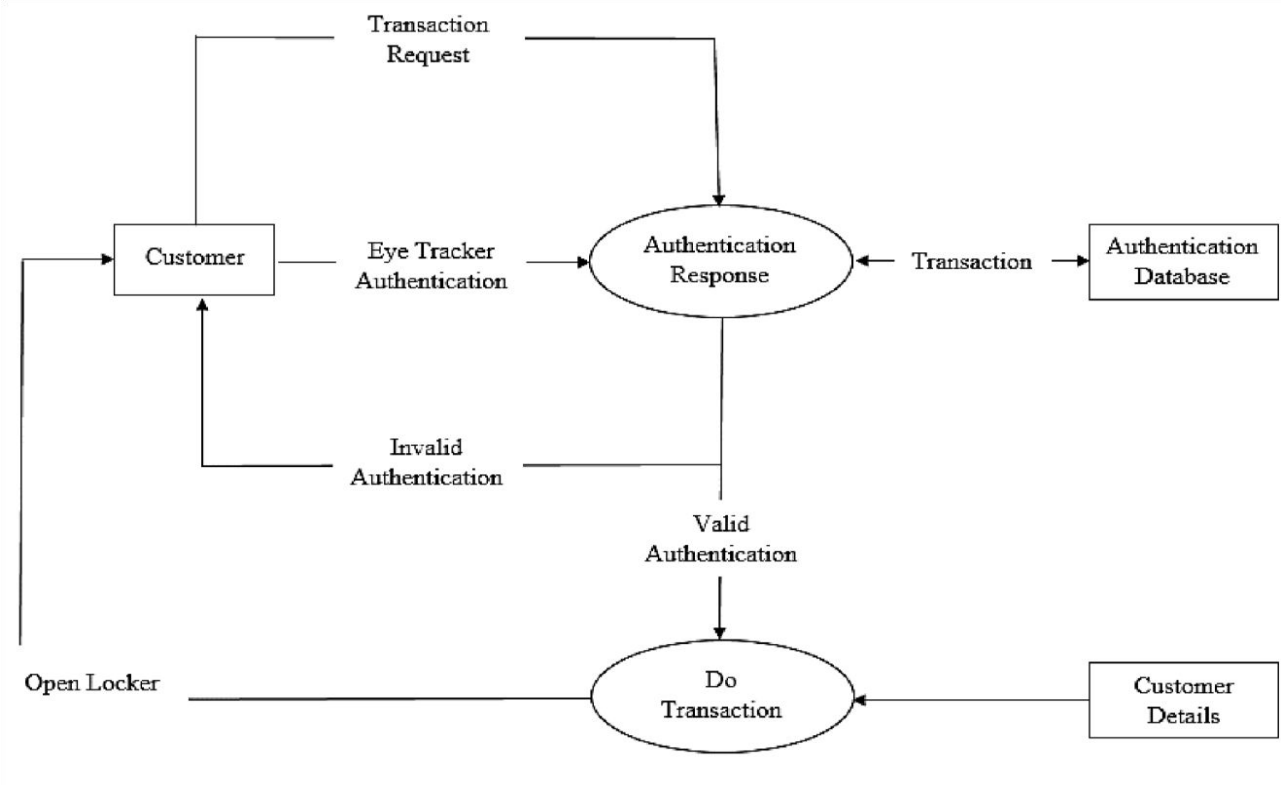

Fig 2: Shows the working of the system

The following shows the working of the system.
The steps start from capturing the image from the camera, then processing the image, detecting the face, detecting the eye, extracting features and testing and training. This is summarized in the following steps:

i. The user/customer requests a transaction by looking into the camera.
ii. The camera captures the face of the user by the process of image acquisition.
iii. The image is then processed by using the Haar Cascade and the Facial Landmark algorithm to calculate the structure of the face and to detect eyes on it.
iv. The complete eye data is captured based on the pupil detected.
v. After which, the features are extracted from the face and eye detection process.
vi. The system then checks if the user is an authorized user or not by checking the authentication database.
vii. If the authentication is valid, then the transaction is done and the locker is opened.
viii. In case of invalid authentication, the control is directed back to the user.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | Impact Factor: 7.488 |

||Volume 8, Issue 6, June 2020||

VI. HARDWAREREQUIREMENTS

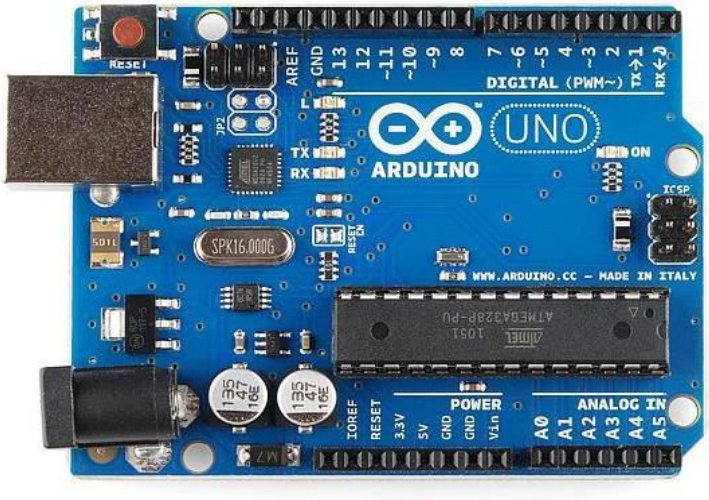

Fig 3: Arduino

The Arduino hardware and software were designed for creating interactive objects or environments. Arduino can interact with buttons, LEDs, motors, speakers, GPS units, cameras, the internet, and even yoursmart- phoneor your TV, thus making it very flexible. Both the Arduino hardware and software are easy to learn.

- **Processor**–x86 compatible processor with 1.7GHz Clock Sleep
- **Microcontroller**-- Arduino
- **RAM**–512MB or greater
- **Monitor**–VGA/SVGA, WEB CAM
- **Keyboard**–104 keys standard
- **Mouse**–2/3 button. Optical/Mechanical

VII. IMPLEMENTATION

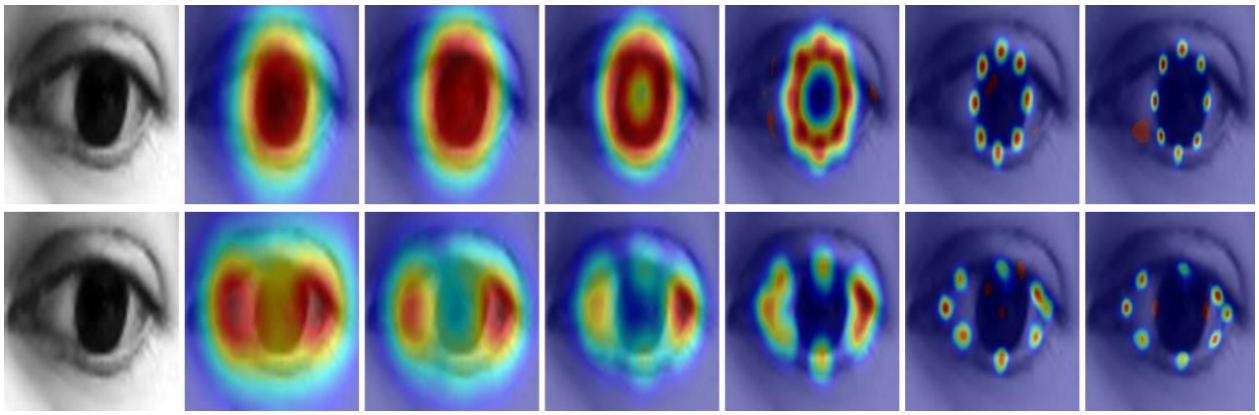

Fig 4: Eye landmarking for recognizing layers

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | Impact Factor: 7.488 |

||Volume 8, Issue 6, June 2020||

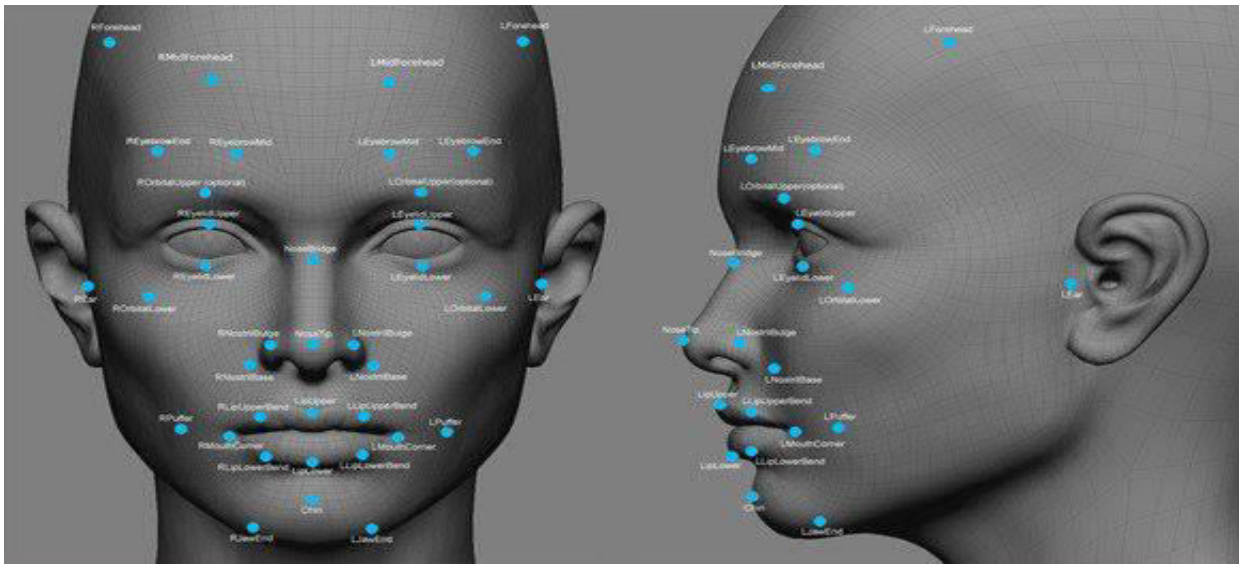

Fig 5: Face and eye detection

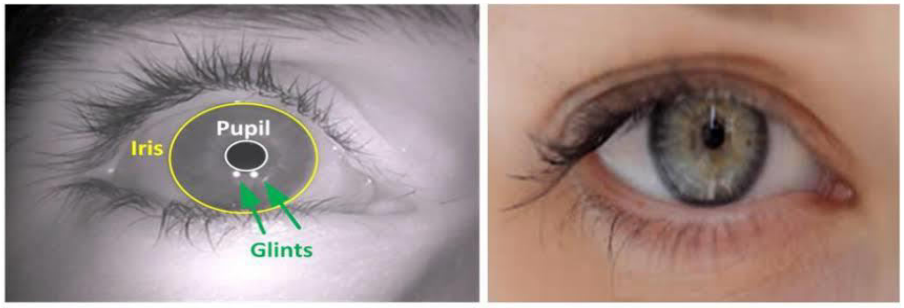

Fig 6:Pupil detection

VIII. RESULT

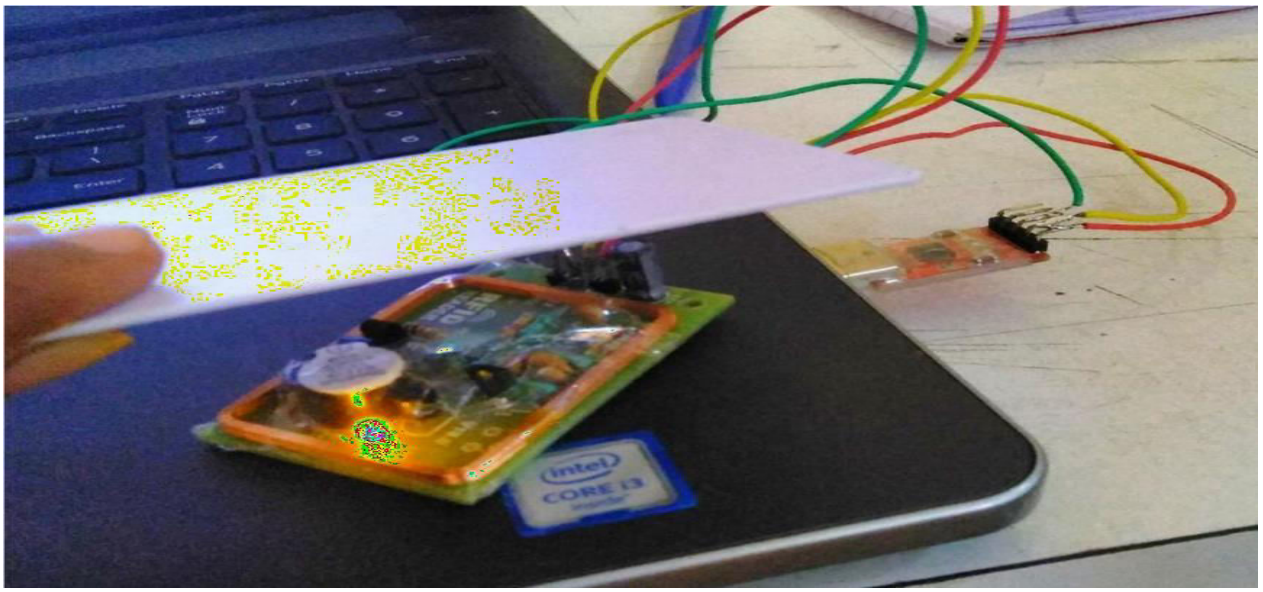

Fig 7: RFID card reading and relay operation

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | Impact Factor: 7.488 |

||Volume 8, Issue 6, June 2020||

Today, we have various security systems such keypad-based systems, voice-controlled systems, head-controlled systems and so on. But the Eye Tracker Password system truly stands out as they are much more secure and accurate compared to the traditional security systems and not to mention the convenience of a completely hands-off gaze-based system.

This system can especially be usefulto the physically challenged as now, they can have access to security systems without having to manually type out a password or make any physical movements.

The Eye Tracker Password system in addition to being secure and accurate also consumes less power. The project is fairly easy to implement and uses commonly available components, which made it quite cost effective. This system can be used schools, banks, or just about anywhere where security is a want or need.

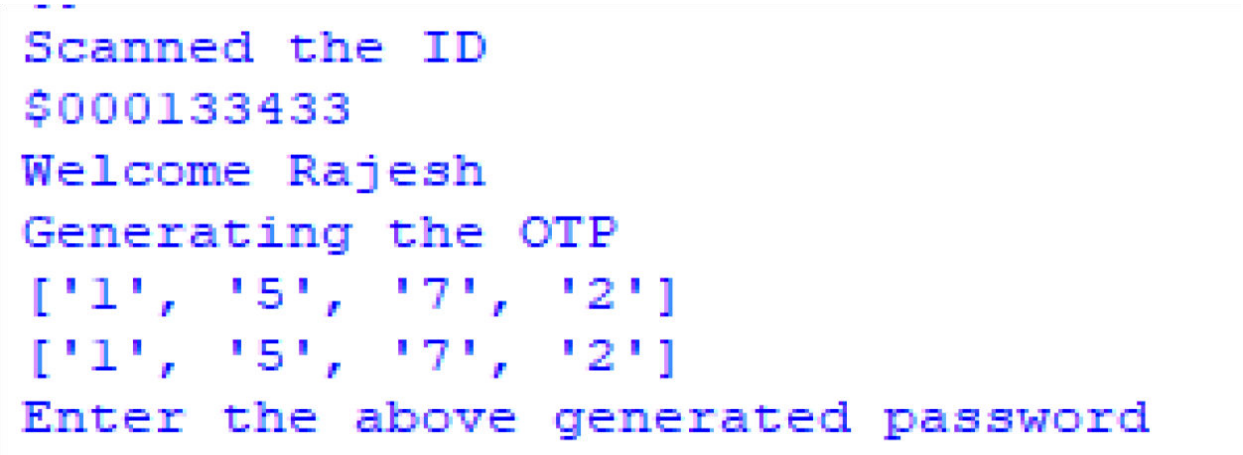

Fig 8: OTP generation after eye scanning

IX.CONCLUSION AND FUTURE WORK

A smart camera-based eye tracking system has been incorporated as a new application for gaze-based PIN identification. The system has been successfully tested with numbers and can be extended to character and digit combination password entry. It mainly protects the user password from various attacks like shoulder surfing and thermal tracking.

Future work includes incorporating the PIN identification algorithm to the real time framework for all in one password identification system. In addition, gaze-based password entry can be extended to mobile devices and other camera-based systems.

REFERENCES

1. R. Revathy and R. Bama, “Advanced Safe PIN-Entry Against Human Shoulder-Surfing,” IOSR Journal of Computer Engineering, vol 17, issue 4, ver. II, pp. 9-15, July-Aug. 2015. (Available: http://www.iosrjournals.org/iosr-jce/papers/Vol17-issue4/Version2/B017420915.pdf)
2. J. Weaver, K. Mock and B. Hoanca, “Gaze-Based Password Authentication through Automatic Clustering of Gaze Points,” Proc. 2011 IEEE Conf. on Systems, Man and Cybernetics, Oct. 2011. (DOI: 10.1109/ICSMC.2011.6084072)
3. “ATM Fraud, ATM Black Box Attacks Spread Across Europe”, European ATM Security Team (E.A.S.T.), online, posted 11 April 2017. (Available: https://www.european-atm-security.eu/tag/atmfraud/)
4. K. Mowery, S. Meiklejohn and S. Savage, “Heat of the Moment: Characterizing the Efficacy of Thermal Camera-Based Attacks,” WOOT ’11, pp. 1-8, August 2011. (Available: https://cseweb.ucsd.edu/~kmowery/papers/thermal.pdf)
5. M. Mehrübeoglu, H. T. Bui and L. McLauchlan, “Real-time iris tracking with a smart camera,” Proc. SPIE 7871, 787104, 2011. (DOI:10.1117/12.872668)
6. M. Mehrubeoglu, L. M. Pham, H. T. Le, M. Ramchander, and D. Ryu, “Real-time eye tracking using a smart camera,” Proc. 2011 IEEE Applied Imagery Pattern Recognition Workshop (AIPR ‘11), pp. 1-7, 2011. (DOI: 10.1109/AIPR.2011.6176373)
7. M. Mehrubeoglu, E. Ortlieb, L. McLauchlan, L. M. Pham, “Capturing reading patterns through a real-time smart camera iris tracking system,” Proc. SPIE, vol. 8437, id. 843705, 2012. (DOI: 10.1117/12.922875)
8. Smart Cameras for Embedded Machine Vision, (product information) National Instruments (Available: http://www.ni.com/pdf/products/us/cat_ni_1742.pdf)