Real-time force doors detection system using distributed sensors and neural networks

Pascual Espada J, García-Díaz V, Núñez-Valdéz ER, González Crespo R. Real-time force doors detection system using distributed sensors and neural networks. *J. Intell. Syst*. 2019; 34: 2243-2252. https://doi.org/10.1002/int.22161

Real-time force doors detection system using distributed sensors and neural networks

Jordán Pascual Espada[1], Vicente García-Díaz[1], Edward Rolando Núñez-Valdéz[1], Rubén González Crespo[2]

[1]Department of Computer Science University of Oviedo, Oviedo, Spain

[2]School of Engineering, International University of La Rioja - UNIR, Logroño, Spain

Abstract

Intelligent security systems have evolved enormously in the last few years. Most of these security systems use a group of physics sensors and algorithms for data analysis and communication systems to notify security alarms. Many security systems that are included in doors can detect intruders when they have already opened the door, but not while intruders are forcing upon the door. However, some security systems include preventive systems, which can detect intruders before they open the door. These preventive systems are usually based on video cameras (image processing) or in-presence sensors, which can generate many false positives, for instance, when a person is next to the door for a few seconds, even if this person is not manipulating the door. This research work proposes a novel force door detection system. The system includes a specific device for monitoring door small vibrations and movements; it analyzes these data using neural networks to detect accurately if someone is forcing upon the door. Artificial intelligence must be able to categorize data records without confusing when someone is forcing upon the door with other actions, like knocking on the door.

Keywords

artificial neural network, classification, force door, security systems, sensor

1 Introduction

Security systems must detect many different criminal actions, like unauthorized access. Forcing locks is a common method used by thieves; they break the lock or fastening to get into a building without using a key. Most security systems are able to detect the presence of the thief when he is already inside the house, using presence sensors. Only complex and expensive security systems include mechanisms to detect thieves before they get inside.

Door monitoring activities are an important part of security systems. Door monitoring analyzes if someone has opened the door; security systems usually include sensors near the door and that information is analyzed to detect intruders. Using a sensor to detect if the door is open or close is relatively simple; many different sensors can detect it accurately.

Detecting thieves before they enter the house is one of the best ways to protect people and their belongings. Early detection warns people living in a house when they are still safe and notifies the crime to the authorities early; it increases the chances of thieves being in the house when the police arrive.

Predictive detection before thieves open doors is not an easy challenge. To complete this task, security systems must include extra sensors or cameras and analyze a lot more information. Some security systems use external presence sensors to monitor activity around the door. These sensors detect when someone is moving next to the door.[1]

Many other security systems use video cameras to monitor the activity around the door. Thus, images can be analyzed using artificial intelligence to determine if there are people next to the door and what kind of activity they are doing (waiting next to the door, knocking the door, using tools to open the door, etc.).[2] There are a lot of challenges trying to detect what people are doing, even using a lot of sensors.[3]

Detecting if the door is actually closed or opened can be done using just a sensor, but detecting if someone, who is next to our door, is doing a criminal action requires getting a lot of data and analyzing them.[4] Because of this, many security systems indicate false door-forced- open alarms. Thus, determining if someone is manipulating the door with bad intentions just by using data from presence sensors or cameras is a complex task since, in many cases, there could be people next to our door without bad intentions.

Artificial neural networks are widely used to analyze sensor data in many industries. Monitoring and classification are possibly two of the most common actions,[5] together with generating predictions[6,7] or estimations.[8,9] These actions could be applied to many areas to achieve great improvements.

In addition, one of the reasons why researchers include artificial intelligence in sensor networks is because some systems have false detections.[10] Artificial intelligence techniques like neural networks, through some research works, have improved the accuracy of the sensors and reduced significantly the percentage of wrong measurements. Sometimes, sensors are not able to avoid interferences without some artificial intelligence.[11,12]

There are many success stories using distributed sensors[13] and neural networks to detect dangerous situations or to classify processes. Many of these successes are related to the chemical industry,[14] wastewater treatment processes[15] or gases.[16,17]

This study aims to propose a novel electronic device, which will be able to detect attempts to force a door, minimizing the false alarm problems. The electronic device that will be created for this aim uses connected sensors and artificial intelligence techniques. The cost of common door alarms oscillates between $8 and $40. The price of this device should be in this range.

Reviewing many research works, which were able to monitor, classify, and predict events based on sensor data, we evidence that the use of neural networks could be an appropriate approach to obtain good results. The proposed devices will include an internal system, which uses neural networks to process the sensor data and classify it. Using artificial intelligence, the system must be able to detect when some person is just touching the door or when the person is doing a criminal activity.

The rest of the paper is organized as follows. Related work is covered in Section 2. Section 3 contains a description of the proposed system and experimental conditions. Section 4 contains the evaluation of the proposals. We conclude this paper in Section 5, presenting the conclusions.

2 Related work

Neural networks are commonly used to analyze sensor data in many industrial systems. There are some approaches, which successfully combine sensor networks and neural networks to monitor polluting emissions. Some research work proposes an electronic nose that can detect dangerous situations for people and classify the substances that are in the environment.[18,19] Smell is not the only sense that researchers are trying to replicate. There are also many works which aim to create an electronic tongue.[20]

Other research works combine sensor data and artificial intelligence to improve the detection of the gas release rate. To that end, So et al[21] collected data using optical sensors. In addition, there are some fire detectors that combine information from different sources and analyze data using artificial intelligence techniques to improve the accuracy of the system.[16]

The use of distributed sensors in buildings or outdoor environments is a very common approach. However, many research works are starting to embed sensors in some moving systems like robots.[22,23] The combination of the data and neural networks is able to create autonomous location systems. Thus, some research works propose to include sensors and neural networks in vehicles to evaluate safety at every moment.[24]

Hua et al[25] propose an intelligent wheelchair able to navigate in indoor environments. Nevertheless, data analysis and artificial intelligence are not only for "big-scale" systems, like entire buildings. These techniques can be included in thousands of devices, even to solve big or small problems for society.[5] In some industries, the artificial intelligence techniques based on sensor information are also used to calibrate devices automatically.[26,27]

There is also a lot of information that can be obtained using sensors, and many of the security systems are based on cameras or laser vision.[28] Machine vision sensors are a common approach to monitor environments.[29] There is also some controversy about protection and privacy when security systems take photos or record videos.[30]

Some very basic security systems use acoustic sensors and neural networks to detect people.[31] These systems are a low-cost alternative to some complex security systems, but they are not able to detect which kind of actions the person is doing. These features could be enough for some security proposals but not for the detection of doors that are being forced, since there could be many people near the door without any malicious plans.

Some buildings include many sensors and intelligent systems, turning these "buildings" into Intelligent buildings.[32] Some of the systems included in the building could be used for security purposes but not for predicting forced doors.

In addition to sensor systems for entire buildings, there are also smaller scale systems that can be used in homes to improve health, comfort, and safety.[33] Even when security is one of the key features of these kind of systems, they cannot prevent dangers, since they usually can only notify about the situation when the damage has already been done (eg, when the door is already open or the window is broken).

Many different kinds of sensors are included in indoor and outdoor security systems. The strengths and weaknesses of every sensor technology are well known.[34] Companies or people could use some different criteria when they want to get a new security system: the cost, high reliability, high detectability, low nuisance alarms, no false alarms, etc. The correct selection of technology is still a very important point.[34]

Passive infrared sensor is also one of the most common type of systems to detect intruders.[1] However, although these systems are very reliable in detecting movements, detecting what kind of action the person is doing is difficult for them. In general, computer vision systems can get more precision in this kind of task.

Future lines of research in security systems suggest that the use of robots for security purposes will be common in the next years.[35] These robots include a lot of different sensors and high processing capacity. In many cases, such robots will be movable, being able to increase the action area and reducing the costs of some fixed security systems.

Beside the false alarm problem, cameras and presence sensors that are allocated outside the house can be damaged easily, even several days before an assault attempt. Replacing these sensors and cameras could take days and is expensive.

Sensors inside doors have very good response times, improving the data quality. They allow getting data exactly when the person is manipulating the door. Even though including sensors inside doors for security reasons could be a noncommon approach, there are many useful scenarios where they are used, like doors of elevators,[36] rotatory doors,[37] aircraft cabin doors,[38] etc.

3 Proposed system and experimental conditions

The proposed system consists of two different parts:

- Hardware: we need a new electronic device that can be embedded in a door. It must be able to collect real-time data about small vibrations in different axes. Ideally, the device must be embedded next to the lock for capturing manipulations in the lock.
- Software: it is needed for the device to start collecting data. In each period of time, a value “outside rest state” is triggered. Collected data must be analyzed using artificial intelligence techniques to classify whether these vibrations correspond to a malicious manipulation of the door like someone is trying to force the door.

3.1 The electronic device

As a part of this research work, we designed a specific electronic device that can be attached to the door. This device is undetectable from outside the house, since it can be placed on the inside part of the door.

The electronic parts of such a device consist of a small microcontroller board (48 mm × 18 mm) with a Wi-Fi module based on ESP8266, 16 MHz Clock Speed, 32 kB of flash memory, 7 analog inputs and 12 digital input/output pins, and external power alimentation port. The sum of costs for this device is less than $10.

We used the input pins to connect two Triple-Axis Accelerometer w/ 14-bit ADC (SPI/IIC GY-9250), which is able to read the small accelerations in three axes. Each of the three axes is connected to an analog input. The functionality of the device is implemented using the C programming language that runs on the microcontroller (Figure 1).

The software application implements a trigger. This trigger is used to determine when the door is out of the idle state. After the trigger is launched, the device starts collecting the sensors’ data every 100 milliseconds for 4.1 seconds. After doing many tests with different time intervals, we observe that 4.1 seconds is probably the minimum amount of time to capture in an efficient way the full cycle of a vibration (using this hardware; using another, more accurate hardware, the time interval may probably be smaller). However, an action performed with the door, such as “opening the door,” requires usually many slots of 4.1 seconds.

3.2 Data and neural network design

In the first steps of the research work, we store data while we were performing different actions on the door, leading to different states: (a) idle, (b) opening the door, (c) knocking the door, and (d) forcing the door. After repeating many times all the different actions, we got a massive set of measurements. It is evident that the measures obtained for every action are slightly different. However, data recorded in some of the actions are similar.

Figure 2 shows an example of the acceleration detected by the device in the different X, Y, and Z axes, under four different assumptions. They seem similar but have slightly different trajectories depending on whether the door is in an idle state or if someone is trying to open,

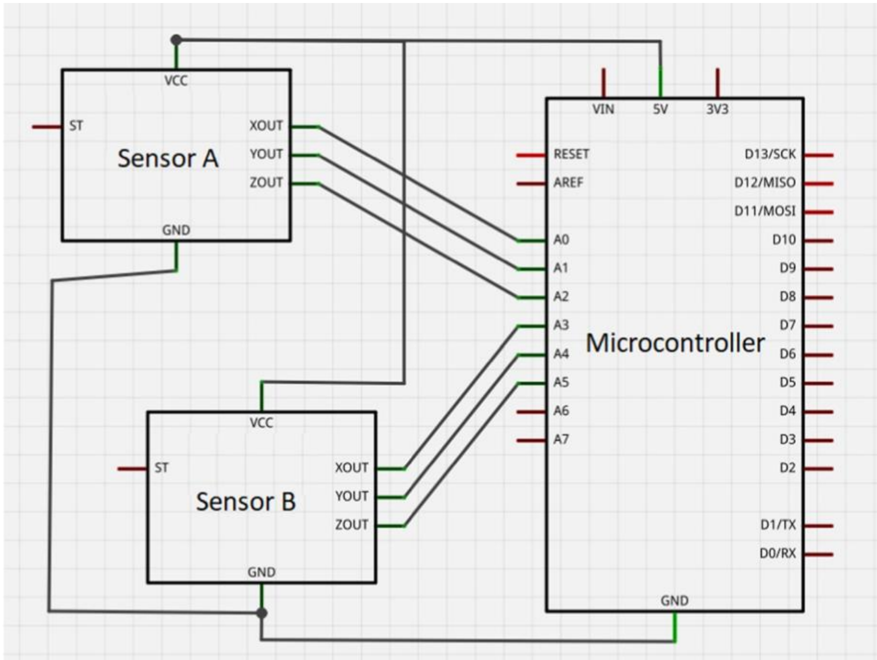

FIGURE 1 Electronic scheme of the designed device

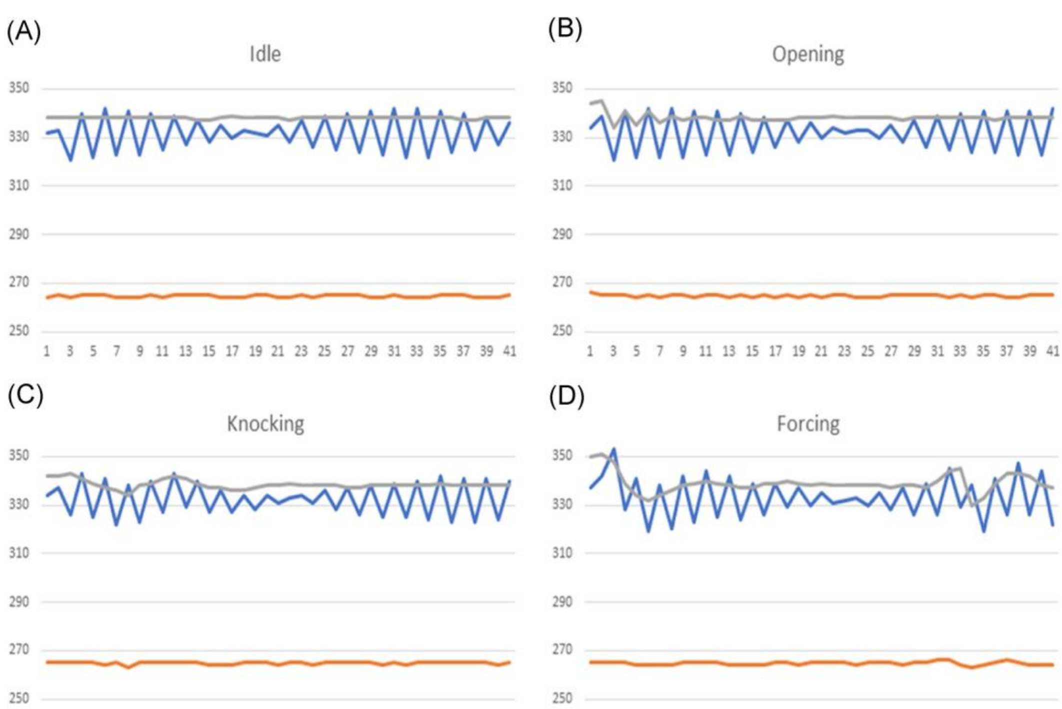

FIGURE 2 Accelerations in 3 axes detected for different actions: idle, opening, knocking the door, and forcing the door [Color figure can be viewed at wileyonlinelibrary.com]

force, or knock on the door. The analog measure of every axis is registered in an analog signal that can take a value between 0 and 1024.

We took a total of 10 240 samples, that is, 2048 of each type, which allows us to have a large enough data set to be able to apply machine learning techniques and extract a data model to detect and model the differences between the four possible actions studied on the door.

Different experiments have been carried out, and the one that worked best is a neural network (Figure 3) with the following features:

- Feedforward type, where connections between nodes do not create cycles. It is one of the simplest types of neural networks moving the information only in one direction. However, they have shown to be more efficient than other more complex methods to solve a large number of problems.
- Three layers, an input, a hidden, and an output layer.
- Linear activation function between the input and the hidden layer, where activation is proportional to input: $f(x) = x$
- Tanh activation function between the hidden and the output layer, which is similar to the sigmoid activation function but scaled from −1 to 1: $f(x) = (e^{2x} - 1)/(e^{2x} + 1)$
- Input layer with nine neurons plus a bias one. After different experiments, the statistical measures with better accuracy are the maximum, the minimum, and the average of the values for each of the axes.
- Hidden layer with 15 neurons plus a bias one.
- Output layer with four neurons, one for each possible type of nominal output.
- Trained with a five-fold cross-validated approach.

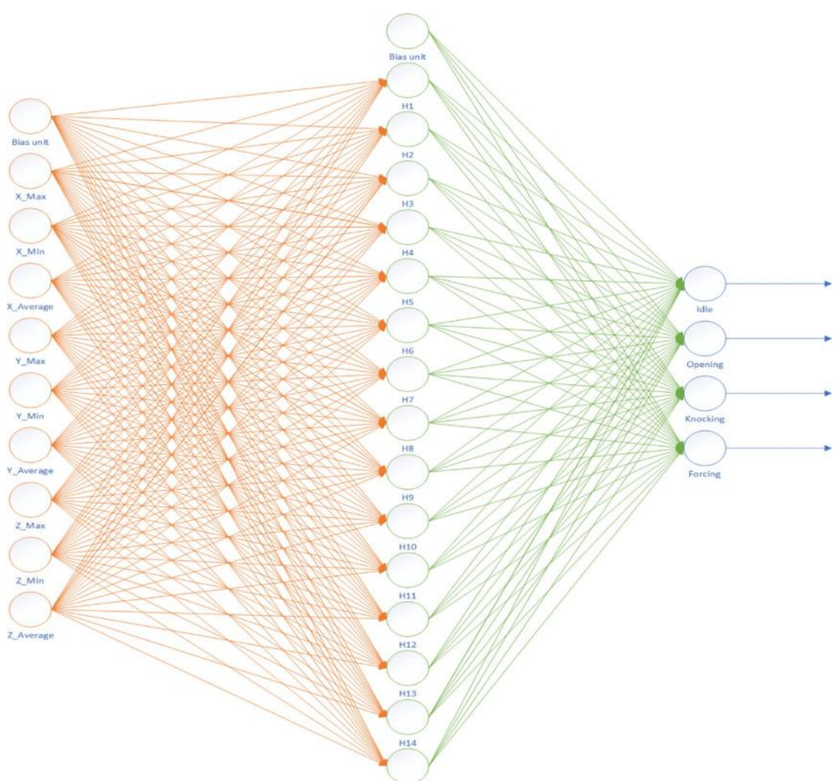

FIGURE 3 Structure of the neural network

4 Evaluation

To evaluate this proposal, we design 10 different tests. Table 1 shows the percentage of success and failures obtained by the different experiments performed with the data set to train the neural network randomly changing the training and the validation data as well as the starting weights of the neurons. The total success rate for the 10 neural networks is 92.75%. That means, that for every 100 cases, in almost 93, the model correctly inferred whether the door is idle, or someone is forcing, opening, or knocking on it (Table 2).

A success of 92.75% means that there is a 7.25% failure, which is a very low failure rate. This failure rate is applied for each slot of 4.1 second. Considering that every criminal action done by a person usually takes a minimum amount of time, it must be divided into four—*N* time slots. Thus, the effectiveness of the proposal system could be very high. For example, in a record composed of four slots, just one of them could statistically have a failure in the classifications, and the other three are likely to have been classified successfully.

TABLE 1 Test performed to train the network

Model	Success %	Failure %
Test 1	94.140625	5.859375
Test 2	92.96875	7.03125
Test 3	91.015625	8.984375
Test 4	94.921875	5.078125
Test 5	92.1875	7.8125
Test 6	95.703125	4.296875
Test 7	90.234375	9.765625
Test 8	90.625	9.375
Test 9	93.359375	6.640625
Test 10	92.578125	7.421875

TABLE 2 Performance system in use and configuration with different number of slots

Total slots	Slots that have to fail	Failure %
4	2 of 4 ($\geq$ 50%)	0.52
5	3 of 5 ($\geq$ 60%)	0.038
6	3 of 6 ($\geq$ 50%)	0.038
7	4 of 7 ($\geq$ 57%)	0.0000276

If three of four slots point the same action, the program has many guarantees that this is the right action. The probability of obtaining failures in two slots is 7.25/100 * 7.25/100 = 0.52%, which is almost 1 of every 200 times. This percentage will be reduced when the action has more time slots.

5 Conclusions

In this research work, we propose a novel approach to detect when someone is forcing a door even before the intruder opens it. This security system is a predictive system based on small vibrations registered over the door. The system is composed of a specific electronic device and a software application that analyzes the vibrations using neural networks.

By analyzing the current security systems and research work, we did not find any other system based on sensors to detect when someone is forcing a door. Moreover, most of the systems only detect whether someone is next to the door but they cannot determine what kind of action the person is doing, which can generate many false alarms.

The results obtained in the evaluation suggest that the system could contribute to more effective security systems, able to detect when someone is forcing a door with a very small failure rate. On the basis of the evaluation, if someone is trying to force a door during 21 seconds (21 seconds → 4 * 4.1-time slots), the proposal provides a failure rate of only 0.038% approximately, so it could fail 1 out of 3000 times. The system price is also low compared with other door alarms, less than $10.

REFERENCES

1. Surantha N, Wicaksono WR. Design of smart home security system using object recognition and PIR sensor. *Procedia Comput Sci.* 2018;135:465-472. https://doi.org/10.1016/j.procs.2018.08.198
2. Aman F, Anitha C. Motion sensing and image capturing based smart door system on android platform. In: *2017 International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS)*. Chennai, India; 2017:2346-2350. https://doi.org/10.1109/ICECDS.2017.8389871
3. 1Fang B, Sun F, Liu H, Guo D. Development of a wearable device for motion capturing based on magnetic and inertial measurement units. *Sci Program*. 2017;2017:1-11. https://doi.org/10.1155/2017/7594763
4. Efros Berg, Mori Malik. Recognizing action at a distance. In: *Proceedings of the Ninth IEEE International Conference on Computer Vision.* Vol 2. Nice, France; 2003:726-733. https://doi.org/10.1109/ICCV.2003.1238420
5. Nadimi ES, Jørgensen RN, Blanes-Vidal V, Christensen S. Monitoring and classifying animal behavior using ZigBee-based mobile ad hoc wireless sensor networks and artificial neural networks. *Comput Electron Agric*. 2012;82:44-54. https://doi.org/10.1016/j.compag.2011.12.008
6. Yap WK, Karri V. ANN virtual sensors for emissions prediction and control. *Appl Energy*. 2011;88(12): 4505-4516. https://doi.org/10.1016/j.apenergy.2011.05.040
7. Su T-J, Chen Y-F, Cheng J-C, Chiu C-L. An artificial neural network approach for wafer dicing saw quality prediction. *Microelectron Reliab.* 2018;91:257-261. https://doi.org/10.1016/j.microrel.2018.10.013
8. Ghosh N, Ravi YB, Patra A, et al. Estimation of tool wear during CNC milling using neural network-based sensor fusion. *Mech Syst Signal Process*. 2007;21(1):466-479. https://doi.org/10.1016/j.ymssp.2005.10.010
9. Abdel-Nasser M, Mahmoud K, Kashef H. A novel smart grid state estimation method based on neural networks. *Int J Interact Multimed Artif Intell*. 2018;5(1):92-100. https://doi.org/10.9781/ijimai.2018.01.004
10. Morinaga K, Sugars ME, Muteki K, Takada H. Sensor fault detection and validation for chemical process using a neural network model. *IFAC Proc Vol.* 1997;30(11):561-566. https://doi.org/10.1016/S1474-6670(17)42904-1
11. MartıńMA, Santos JP, Vásquez H, Agapito JA. Study of the interferences of NO_2 and CO in solid state commercial sensors. *Sensors Actuators B Chem*. 1999;58(1):469--4473. https://doi.org/10.1016/S0925-4005(99)00128-8
12. Frattini Fileti AM, Pedrosa LS. Pereira JAFR. A self tuning controller for multicomponent batch distillation with soft sensor inference based on a neural network. *Comput Chem Eng*. 1999;23:S261-S264. https://doi.org/ 10.1016/S0098-1354(99)80064-7
13. Kaur R, Arora S. Nature inspired range based wireless sensor node localization algorithms. *Int J Interact Multimed Artif Intell*. 2017;4(6):7-17. https://doi.org/10.9781/ijimai.2017.03.009
14. Sun K, Huang S, Jang S-S, Wong DS-H. Development of soft sensor with neural network and nonlinear variable selection for crude distillation unit process. In: Kravanja Z, Bogataj M, eds. *26th European Symposium on Computer Aided Process Engineering*. 38. Portoroz, Slovenia: Elsevier; 2016:337-342.
15. Cong Q, Yu W. Integrated soft sensor with wavelet neural network and adaptive weighted fusion for water quality estimation in wastewater treatment process. *Measurement*. 2018;124:436-446. https://doi.org/10. 1016/j.measurement.2018.01.001
16. Derbel F. Performance improvement of fire detectors by means of gas sensors and neural networks. *Fire Saf J.* 2004;39(5):383-398. https://doi.org/10.1016/j.firesaf.2004.03.001
17. Lau K-T, Guo W, Kiernan B, Slater C, Diamond D. Non-linear carbon dioxide determination using infrared gas sensors and neural networks with Bayesian regularization. *Sensors Actuators B Chem*. 2009;136(1):242-247. https://doi.org/10.1016/j.snb.2008.11.030
18. Sabilla SI, Sarno R, Siswantoro J. Estimating gas concentration using artificial neural network for electronic nose. *Procedia Comput Sci.* 2017;124:181-188. https://doi.org/10.1016/j.procs.2017.12.145
19. Rahimzadeh H, Sadeghi M, Ghasemi-Varnamkhasti M, Mireei SA, Tohidi M. On the feasibility of metal oxide gas sensor based electronic nose software modification to characterize rice ageing during storage. *J Food Eng.* 2019;245:1-10. https://doi.org/10.1016/j.jfoodeng.2018.10.001
20. Shirmardi A, Shamsipur M, Akhond M, Monjezi J. Electronic tongue for simultaneous determination of cyanide, thiocyanate and iodide. *Measurement*. 2016;88:27-33. https://doi.org/10.1016/j.measurement.2016.03.038
21. So W, Koo J, Shin D, Yoon ES. The estimation of hazardous gas release rate using optical sensor and neural network. In: Pierucci S, Ferraris GB, eds. *20 European Symposium on Computer Aided Process Engineering*. 28. Naples, Italy: Elsevier; 2010:199-204.

22. Sabto NA, Mutib KAl. Autonomous mobile robot localization based on RSSI measurements using an RFID sensor and neural network BPANN. *J King Saud Univ - Comput Inf Sci*. 2013;25(2):137-143. https://doi.org/ 10.1016/j.jksuci.2012.10.001
23. Raj M, Bhaskar Semwal V, Nandi GC. Hybrid model for passive locomotion control of a biped humanoid: the artificial neural network approach. *Int J Interact Multimed Artif Intell*. 2018;5(1):40-46. https://doi.org/10. 9781/ijimai.2017.10.001
24. Rovetta A, Zocchi C, Giusti A, Adami A, Scaramellini F. Methodology of evaluating safety in automobiles using intelligent sensor architecture and neural networks. *Sensors Actuators A Phys*. 2007;134(2):622-630. https://doi.org/10.1016/j.sna.2006.05.042
25. Hua B, Hossain D, Capi G, Jindai M, Yoshida I. Human-like artificial intelligent wheelchair robot navigated by multi-sensor models in indoor environments and error analysis. *Procedia Comput Sci*. 2017;105:14-19. https://doi.org/10.1016/j.procs.2017.01.181
26. Taib MN, Narayanaswamy R. Multichannel calibration technique for optical-fibre chemical sensor using artificial neural network. *Sensors Actuators B Chem*. 1997;39(1):365-370. https://doi.org/10.1016/S0925- 4005(97)80235-3
27. Chen T, Sun L, Zhang Q, Wu X, Wu D. Field geometric calibration method for line structured light sensor using single circular target. *Sci Program*. 2017;2017:1-8. https://doi.org/10.1155/2017/1526706
28. Yoo W-S, Na S-J. Determination of 3-D weld seams in ship blocks using a laser vision sensor and a neural network. *J Manuf Syst*. 2003;22(4):340-347. https://doi.org/10.1016/S0278-6125(03)80049-3
29. Zhang Q, Bruce Litchfield J, Reid JF, Ren J, Chang S-W. Coupling a machine vision sensor and a neural net supervised controller: controlling microbial cultivations. *J Biotechnol*. 1995;38(3):219-228. https://doi.org/10. 1016/0168-1656(94)00123-T
30. Naarttijärvi M. Balancing data protection and privacy – The case of information security sensor systems. *Comput Law Secur Rev*. 2018;34(5):1019-1038. https://doi.org/10.1016/j.clsr.2018.04.006
31. Wang Y, Chen Y, Bhuiyan MZA, Han Y, Zhao S, Li J. Gait-based human identification using acoustic sensor and deep neural network. *Futur Gener Comput Syst*. 2018;86:1228-1237. https://doi.org/10.1016/j.future.2017.07.012
32. Moreno-Cano MV, Zamora-Izquierdo MA, Santa J, Skarmeta AF. An indoor localization system based on artificial neural networks and particle filters applied to intelligent buildings. *Neurocomputing*. 2013;122:116-125. https://doi.org/10.1016/j.neucom.2013.01.045
33. Schütze A. Integrated sensor systems for indoor applications: ubiquitous monitoring for improved health, comfort and safety. *Procedia Eng*. 2015;120:492-495. https://doi.org/10.1016/j.proeng.2015.08.681
34. Pearson RL. 6 - Exterior and interior security sensors. In: Pearson RL, ed. *Electronic Security Systems: A Manager's Guide to Evaluating and Selecting System Solutions*. Burlington, MA: Butterworth-Heinemann; 2007:95-110.
35. Marek G, Peter Š. Design the robot as security system in the home. *Procedia Eng*. 2014;96:126-130. https:// doi.org/10.1016/j.proeng.2014.12.130
36. Yu-hui J, Hong-xing W, Bao-quan K, Li-yi L. Research on position sensor magnetic encoder based on the elevator door machine servo system. In: *2008 3rd International Conference on Sensing Technology*. Tainan, Taiwan; 2008:431-434. https://doi.org/10.1109/ICSENST.2008.4757142
37. Lehrasab N, Fararooy S, Allan J. Fault detection in intelligent early failure warning sensors system for train rotary door operator. In: *IEE Colloquium on Intelligent Sensors (Digest No: 1996/261)*. Leicester, UK; 1996:5/1. https://doi.org/10.1049/ic:19961386
38. Shi X, Zhang G, Chao D, Zhao H, Chen X. Design of an in-situ test equipment for the proximity sensor of the aircraft cabin door. In: *CSAA/IET International Conference on Aircraft Utility Systems (AUS 2018)*. Guiyang, China; 2018:171-175. https://doi.org/10.1049/cp.2018.0302