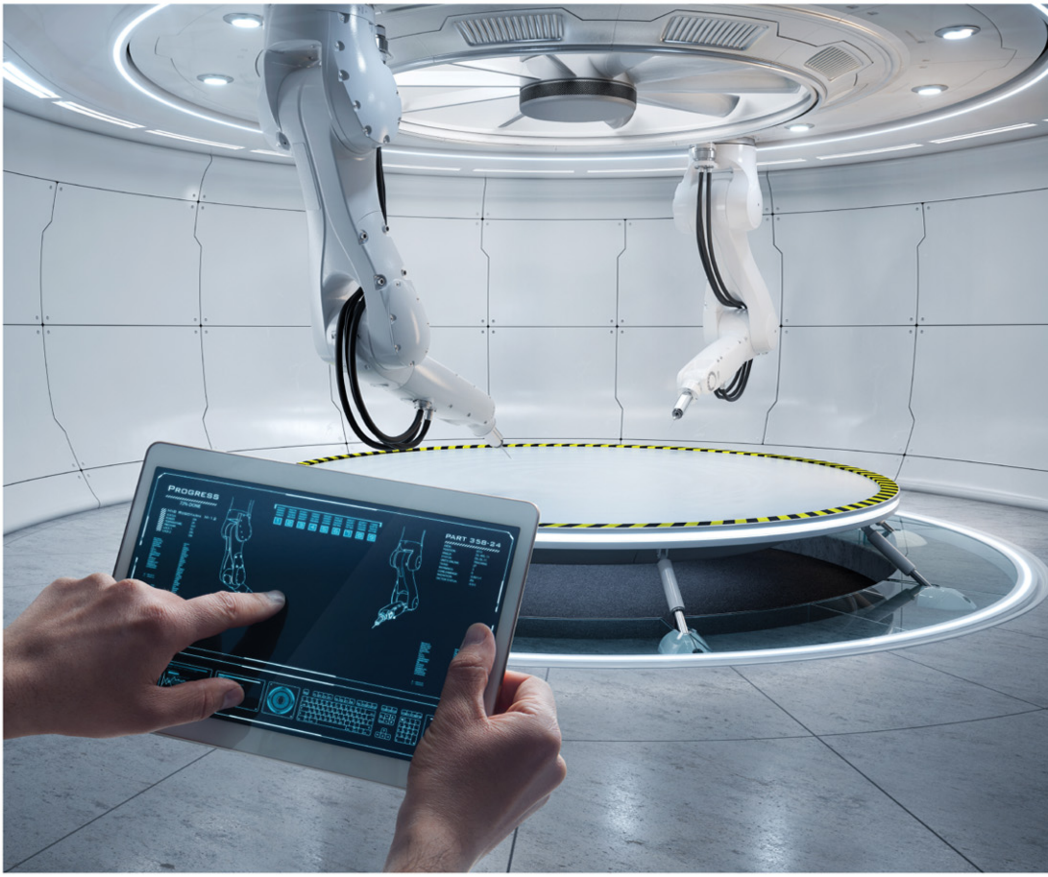
The Institution of
Engineering and Technology

The Nine Pillars of Technologies for Industry 4.0

Edited by
Wai Yie Leong, Joon Huang Chuah and Boon Tuan Tee



IET TELECOMMUNICATIONS SERIES 88

The Nine Pillars of Technologies for Industry 4.0

Other volumes in this series:

Volume 9	**Phase Noise in Signal Sources** W.P. Robins
Volume 12	**Spread Spectrum in Communications** R. Skaug and J.F. Hjelmstad
Volume 13	**Advanced Signal Processing** D.J. Creasey (Editor)
Volume 19	**Telecommunications Traffic, Tariffs and Costs** R.E. Farr
Volume 20	**An Introduction to Satellite Communications** D.I. Dalgleish
Volume 26	**Common-Channel Signalling** R.J. Manterfield
Volume 28	**Very Small Aperture Terminals (VSATs)** J.L. Everett (Editor)
Volume 29	**ATM: The broadband telecommunications solution** L.G. Cuthbert and J.C. Sapanel
Volume 31	**Data Communications and Networks, 3rd Edition** R.L. Brewster (Editor)
Volume 32	**Analogue Optical Fibre Communications** B. Wilson, Z. Ghassemlooy and I.Z. Darwazeh (Editors)
Volume 33	**Modern Personal Radio Systems** R.C.V. Macario (Editor)
Volume 34	**Digital Broadcasting** P. Dambacher
Volume 35	**Principles of Performance Engineering for Telecommunication and Information Systems** M. Ghanbari, C.J. Hughes, M.C. Sinclair and J.P. Eade
Volume 36	**Telecommunication Networks, 2nd Edition** J.E. Flood (Editor)
Volume 37	**Optical Communication Receiver Design** S.B. Alexander
Volume 38	**Satellite Communication Systems, 3rd Edition** B.G. Evans (Editor)
Volume 40	**Spread Spectrum in Mobile Communication** O. Berg, T. Berg, J.F. Hjelmstad, S. Haavik and R. Skaug
Volume 41	**World Telecommunications Economics** J.J. Wheatley
Volume 43	**Telecommunications Signalling** R.J. Manterfield
Volume 44	**Digital Signal Filtering, Analysis and Restoration** J. Jan
Volume 45	**Radio Spectrum Management, 2nd Edition** D.J. Withers
Volume 46	**Intelligent Networks: Principles and applications** J.R. Anderson
Volume 47	**Local Access Network Technologies** P. France
Volume 48	**Telecommunications Quality of Service Management** A.P. Oodan (Editor)
Volume 49	**Standard Codecs: Image compression to advanced video coding** M. Ghanbari
Volume 50	**Telecommunications Regulation** J. Buckley
Volume 51	**Security for Mobility** C. Mitchell (Editor)
Volume 52	**Understanding Telecommunications Networks** A. Valdar
Volume 53	**Video Compression Systems: From first principles to concatenated codecs** A. Bock
Volume 54	**Standard Codecs: Image compression to advanced video coding, 3rd Edition** M. Ghanbari
Volume 59	**Dynamic Ad Hoc Networks** H. Rashvand and H. Chao (Editors)
Volume 60	**Understanding Telecommunications Business** A. Valdar and I. Morfett
Volume 65	**Advances in Body-Centric Wireless Communication: Applications and state-of-the-art** Q.H. Abbasi, M.U. Rehman, K. Qaraqe and A. Alomainy (Editors)
Volume 67	**Managing the Internet of Things: Architectures, theories and applications** J. Huang and K. Hua (Editors)
Volume 68	**Advanced Relay Technologies in Next Generation Wireless Communications** I. Krikidis and G. Zheng
Volume 69	**5G Wireless Technologies** A. Alexiou (Editor)
Volume 70	**Cloud and Fog Computing in 5G Mobile Networks** E. Markakis, G. Mastorakis, C.X. Mavromoustakis and E. Pallis (Editors)
Volume 71	**Understanding Telecommunications Networks, 2nd Edition** A. Valdar
Volume 72	**Introduction to Digital Wireless Communications** Hong-Chuan Yang
Volume 73	**Network as a Service for Next Generation Internet** Q. Duan and S. Wang (Editors)
Volume 74	**Access, Fronthaul and Backhaul Networks for 5G & Beyond** M.A. Imran, S.A.R. Zaidi and M.Z. Shakir (Editors)
Volume 76	**Trusted Communications with Physical Layer Security for 5G and Beyond** T.Q. Duong, X. Zhou and H.V. Poor (Editors)

Volume 77 **Network Design, Modelling and Performance Evaluation** Q. Vien
Volume 78 **Principles and Applications of Free Space Optical Communications** A.K. Majumdar, Z. Ghassemlooy, A.A.B. Raj (Editors)
Volume 79 **Satellite Communications in the 5G Era** S.K. Sharma, S. Chatzinotas and D. Arapoglou
Volume 80 **Transceiver and System Design for Digital Communications, 5th Edition** Scott R. Bullock
Volume 81 **Applications of Machine Learning in Wireless Communications** R. He and Z. Ding (Editors)
Volume 83 **Microstrip and Printed Antenna Design, 3rd Edition** R. Bancroft
Volume 84 **Low Electromagnetic Emission Wireless Network Technologies: 5G and beyond** M.A. Imran, F. Héliot and Y.A. Sambo (Editors)
Volume 86 **Advances in Communications Satellite Systems Proceedings of the 36th International Communications Satellite Systems Conference (ICSSC-2018)** I. Otung, T. Butash and P. Garland (Editors)
Volume 89 **Information and Communication Technologies for Humanitarian Services** M.N. Islam (Editor)
Volume 92 **Flexible and Cognitive Radio Access Technologies for 5G and Beyond** H. Arslan and E. Başar (Editors)
Volume 93 **Antennas and Propagation for 5G and Beyond** Q. Abbasi, S.F. Jilani, A. Alomainy and M.A. Imran (Editors)
Volume 95 **ISDN applications in Education and Training** R. Mason and P.D. Bacsich

This page intentionally left blank

The Nine Pillars of Technologies for Industry 4.0

Edited by
Wai Yie Leong, Joon Huang Chuah and Boon Tuan Tee

The Institution of Engineering and Technology

Published by The Institution of Engineering and Technology, London, United Kingdom

The Institution of Engineering and Technology is registered as a Charity in England & Wales (no. 211014) and Scotland (no. SC038698).

First published 2020

The Institution of Engineering and Technology
Michael Faraday House
Six Hills Way, Stevenage
Herts, SG1 2AY, United Kingdom

www.theiet.org

British Library Cataloguing in Publication Data
A catalogue record for this product is available from the British Library

ISBN 978-1-83953-005-0 (hardback)
ISBN 978-1-83953-006-7 (PDF)

Typeset in India by MPS Limited
Printed in the UK by CPI Group (UK) Ltd, Croydon

Contents

This page intentionally left blank

About the editors

Wai Yie Leong is the Chairperson of The Institution of Engineering and Technology (Malaysia Local Network) and Vice President of The Institution of Engineers, Malaysia (IEM). She specializes in sensing and wireless communications and medical signal processing research including wireless sensor networks, wireless communications, and brain signal processing for signal conditioning and classification in various EEG-based mental tasks. She received the Women Engineer of the Year award in 2018, the IEM Presidential of Excellence Award in 2016, and ASEAN Meritorious Award in Science and Technology 2017. She holds a Ph.D. in Electrical Engineering from The University of Queensland, Australia.

Joon Huang Chuah lectures at the Department of Electrical Engineering, University of Malaya, Malaysia and is the Head of VLSI and Image Processing (VIP) Research Group. He specialises in artificial intelligence, image processing and integrated circuit design. He is the Principal Journal Editor of the Institution of Engineers, Malaysia. He received his B.Eng. from the Universiti Teknologi Malaysia, M.Eng. from the National University of Singapore, MPhil in Technology Policy from the Cambridge Judge Business School, and PhD from the University of Cambridge.

Boon Tuan Tee is an Associate Professor at the Faculty of Mechanical Engineering, Universiti Teknikal Malaysia Melaka, Malaysia. His research focuses on energy management system and green technology. He is a Professional Technologist (Green Technology) registered under Malaysia Board of Technologists. His other professional certifications include Certified Energy Manager under ASEAN Energy Management System (AEMAS) and Certified Professional in Measurement & Verification from Malaysia Greentech. He has been a member of the IET since 2015. He holds a Ph.D. degree in Engineering from University of Cambridge, UK.

This page intentionally left blank

Foreword

Industry 4.0 refers to the current trend of automation and data exchange in manufacturing technologies, also called Intelligent or Smart Manufacturing. There is an increasing number of organizations and countries where Industry 4.0 is becoming adopted including the United Kingdom (Industry 4.0 and the work around 4IR), the United States, Japan, China and the European Union. Several research organizations, with a leading role for the Fraunhofer Institute, are pushing a reference architecture model for secure data sharing based on standardized communication interfaces. The nine pillars of technology that are supporting this transition include: the internet of things (IoT), cloud computing, autonomous and robotics systems, big data analytics, augmented reality, cybersecurity, simulation, system integration and additive manufacturing. A key role is played by Industrial IoT with its many components (platforms, gateways, devices) but many more technologies play a role in this process including cloud, fog and edge computing, advanced data analytics, innovative data exchange models, artificial intelligence, machine learning, mobile and data communication and network technologies, as well as robotics, sensors and actuators. Over the IoT, cyber-physical systems communicate and cooperate with each other and with humans in real-time both internally and across organizational services in the value chain. Within smart factories, cyber-physical systems monitor physical processes, create a virtual copy of the physical world and make decentralized decisions. The aim of this edited book is to focus on the nine pillars of technology including innovative research, challenges, strategies and case studies.

Advances in science and technology continuously support the development of industrialization all over the world. The First Industrial Revolution used water and steam power to mechanize production, the Second used electric power to create mass production and the Third used automation for the manufacturing line. Now a Fourth Industrial Revolution, the digital revolution, is characterized by a fusion of technologies that is blurring the lines between the physical, digital and biological spheres. There are three reasons why today's transformations represent not merely a prolongation of the Third Industrial Revolution but rather the arrival of a Fourth and distinct one: velocity, scope and systems impact. The speed of current breakthroughs has no historical precedent. When compared with previous industrial revolutions, the Fourth is evolving at an exponential rather than a linear pace. Moreover, it is disrupting almost every industry in every country. And, the breadth and depth of these changes herald the transformation of entire systems of production, management and governance. The design principles of Industry 4.0 such as virtualization, interoperability, decentralization, service-oriented approaches, real-time capabilities and modularity all play a key role in the radical changes facing industry. In this book series, we describe the advantages of intelligent manufacturing systems and discuss how they will benefit the manufacturing industry by increasing productivity, competitiveness and profitability. (Benefits: enhanced productivity through optimization and automation, real-time, better quality products, sustainability, personalization and customization for consumers, and improved scalability and agility.)

In this book series, the nine pillars of technology that are supporting this transformation have been introduced: the IoT, cloud computing, autonomous and robotics systems, big data analytics, augmented reality, cybersecurity, simulation, system integration and additive manufacturing.

Technologies and Industry 4.0 are about reducing complexity and processes and add value. However, while business processes are changing rapidly, industries and manufacturers are struggling to exploit the full potential of digitization. From both a strategic and technological perspective, the Industry 4.0 roadmap visualizes every further step on the route towards an entirely digital enterprise. Many case studies have been discussed in this book series, which aims to benefit and create impact to industry players, scientists, academicians, researchers and manufacturers.

Chapter 21

Case study: security system for solar panel theft based on system integration of GPS tracking and face recognition using deep learning

Bhakti Yudho Suprapto[1], Meydie Tri Malindo[1], Muhammad Iqbal Agung Tri Putra[1], Suci Dwijayanti[1] and Leong Wai Yie[2]

Security system is important to protect the objects, including solar panel modules. In this study, an integrated system that combines image processing and object tracking is proposed as a security system of solar panel. Face recognition using deep learning is used to detect unknown face. Then, the stolen object can be tracked using Global Positioning System (GPS) that works using General Packet Radio Service and Global System for Mobile communication system. The results show that the integrated security system is able to find the suspect and track the stolen object. Using the combination of FaceNet and deep belief network, unknown face can be recognized with an accuracy of 94.4% and 87.5% for offline and online testing, respectively. Meanwhile, the GPS tracking system is able to track the coordinate data of the stolen object with an error of 2.5 m and the average sending time is 4.64 s. The duration of sending and receiving data is affected by the signal strength. The proposed method works well in real-time manner and they can be monitored through a website for both recorded unknown face and coordinate data location.

21.1 Introduction

Solar power plant is one of the alternative energies which is utilized in many applications in our daily life. Nevertheless, the price of solar panel is relatively high and so it might be stolen. Thus, a security system is needed for the solar panel system.

Most of the security systems considered only one aspect such as the suspect or the position of the stolen object. One of the methods to detect the suspected thief is using image processing approach. Face recognition is often applied for security system because of its high accuracy compared to other biometrics [1]. Thus,

[1]Department of Electrical Engineering, Universitas Sriwijaya, Palembang, Indonesia
[2]Faculty of Engineering and IT, Mahsa University, Kuala Lumpur, Malaysia

surveillance system can be developed using a security system based on face recognition. Nurhopipah and Harjoko [2] developed a monitoring system using closed circuit television (CCTV) that can detect motion and face and then recognize the face. Another research by Wati and Abadianto [3] developed a home security system based on face recognition. However, this system could not work in real time, especially for unknown face that might be the suspected person. In addition, the system did not have any central storage to save the detected face.

Another aspect in a security system is to track the position of the stolen object. Many research have been done to tracking the position using Global Positioning System (GPS). GPS module and Global System for Mobile Communication (GSM) have been used to track the stolen item using the study by Liu *et al.* [4] and Salim and Idrees [5] who proposed security system based on GPS and General Packet Radio Service (GPRS). Singh *et al.* [6] developed an object tracking system using GPS with communication media of GPRS and Short Message Service (SMS), and Shinde and Mane [7] utilized GPRS and GPS to track the location of the object through website or smartphone. However, it did not have backup communication system when there is no GPRS signal [5,7]. On the other hand, no central storage may allow users to save the input data received from GPS manually [4,6].

Based on the problem mentioned earlier, it is important to make one system for securing the object. Hence, this study proposed an integrated system that combines the face recognition for finding the suspect who stole the solar panel module and tracking system to find the current position of the stolen object. This chapter is organized as follows: Section 21.2 describes the proposed method to recognize unknown face and to track the data coordinate of stolen object. Results and discussion are presented in Section 21.3. Finally, this chapter is concluded in Section 21.4.

21.2 Method

In this study, the proposed method is designed as the combination of face recognition and tracking system. CCTV or webcam is attached close to the solar panel. When an unknown person approaches the solar panel, his/her image will be captured by CCTV or webcam and this image will be recognized using deep learning. If the person is unrecognized, then the image will be sent and stored to online database that can be utilized to track the identity of the thief. In the meantime, the position of the stolen solar panel will be tracked using GPS. The detailed process of the proposed method will be described in the following subsections.

21.2.1 Face recognition using deep learning

The face of an unknown person will be a key in the proposed security system in finding a suspected person. The flowchart of the working process of face recognition can be seen in Figure 21.1.

As shown in the flowchart, the first stage is initialization and it is followed by face detection. Here, the system detects the face using Viola Jones algorithm [8]. The next stage is face detection that is utilized whether the face is detected. If the face is

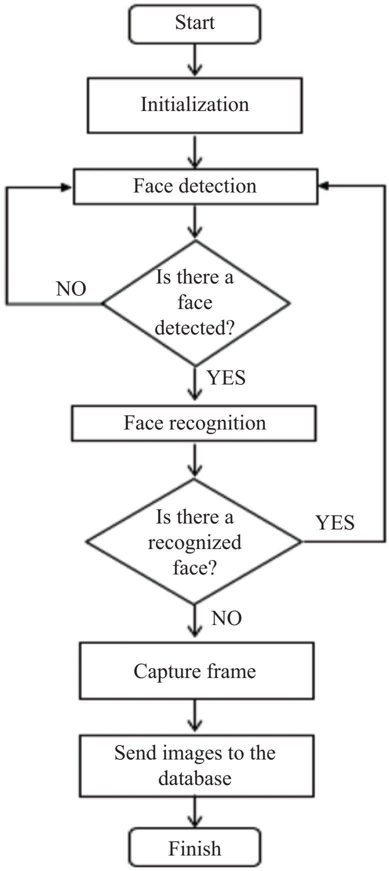


Figure 21.1 Flowchart for face recognition system

detected, the system may continue with the following stage to recognize the face. In this process, the face feature is extracted using embedding Facenet algorithm [9] and the recognition process is performed by deep belief network (DBN). The recognized face will be determined from the confidence value above 80%. The confidence value below 80% is determined as unknown individual who will be captured and sent to the database.

Data used in this research are obtained from different conditions, namely bright and dark. In addition, the object must not cover his or her face. Data used in the training process consist of two people, hereafter called as operator. This training data are obtained from video CCTV. Then, to test the system, eight new faces are utilized.

In obtaining the model, 4,000 images of operators are used where 3,000 images for training and 1,000 images for testing data. FaceNet is used to extract face features to obtain 128 domain points, which is called face embedding. These embedding files are used as the input for DBN. The obtained model is then tested in two conditions, namely offline and online. In the offline test, system is tested for recognized and unrecognized faces coming from images and videos. Nine unrecognized faces are utilized to test the system in both bright and dark. In the online test, the system may recognize the faces in real time and the unknown faces are sent to the database for both bright and dark.

The training process of the proposed method is shown in Figure 21.2. The first stage is to resize the image into 96 × 96 to comply with the input for the purpose of embedding process for FaceNet.

Architecture of FaceNet used in this study is model inception_blocks_v2 in the structure as shown in Table 21.1. Instead of using artificial neural network (ANN) for classification stage, this study utilizes a generative model DBN that consists of restricted Boltzmann machines (RBMs) [10]. DBN does not have any connection in intra layer. Parameters for training network of DBN used in this study can be seen in Table 21.2.

21.2.2 GPS tracking

Face recognition in the previous subsection may be helpful to capture a suspect who stole the solar panel. In the meantime, the stolen object may have been moved to different position. Hence, the security system integrates the face recognition system with GPS tracking to track the position of stolen object.

In this study, the proposed GPS tracking uses the combination of GPRS and GSM as communication system to send the location of the stolen solar panel from Internet network and SMS, respectively. This security system works in parallel with face recognition system. The proposed process of tracking is shown in Figure 21.3.

As shown in Figure 21.3, the system will determine the coordinate location of solar panel using GPS sensor that is aimed as a receiver from GPS satellite to receive and process data to obtain accurate coordinate. When the location is obtained, coordinate data are sent to the database using GPRS or GSM through an SMS. Location and position movement of the stolen solar panel will be tracked in real time and shown in the website. This security system also has website and android application as an interface to track the position and location of the solar panel module. Figures 21.4 and 21.5 represent the website interface and android application, respectively .

While sending the data location, Internet might be interrupted and it will depend on the strength of signal. Hence, this proposed tracking system is also provided to read SMS that is sent to the smartphone.

21.3 Results and discussion

This proposed security system integrates two systems: face recognition to capture the suspect and GPS tracking to track the location of the suspect and the stolen solar panel. In the experiment, both systems will be examined.

21.3.1 Deep learning model for face recognition system

Data used for training consist of two people in two conditions during the day and night as shown in Figure 21.6. Total data for training and testing are 4,000 images.

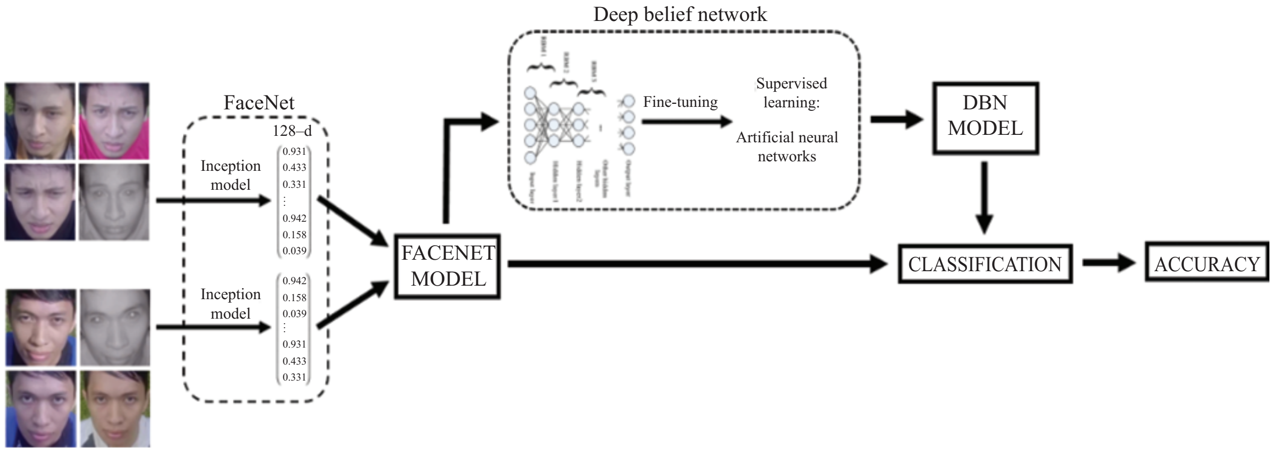


Figure 21.2 Training process

Table 21.1 Inception blocks V2 architecture

ZeroPadding
Conv (7 × 7 × 3.2) + norm
ZeroPadding + max pool
Conv (1 × 1 × 3.1) + norm
ZeroPadding
Conv (3 × 3 × 3.1)+norm
ZeroPadding + max pool
Inception (1a)
Inception (1b)
Inception (1c)
Inception (2a)
Inception (2b)
Inception (3a)
Inception (3b)
Average pool
Flatten
L2

Table 21.2 Parameter training network DBN

Parameter	**Parameter values**
Hidden layer structure	[3,000, 4,500, 3,000]
Jumlah epoch RBM	10
Learning rate RBM	0.001
Jumlah epoch ANN	3,000
Learning rate ANN	0.01
Batch size	32
Dropout	0.2

After obtaining the face feature through FaceNet using the structure as shown in Table 21.1, the features are used as the input to DBN. Parameter structure for DBN is shown in Table 21.2. As DBN is a combination of RBMs, such RBMs reconstruct the input and minimize the reconstruction error. Output of the first hidden layer will be the input for the visible layer in the second RBM and so on. The graph of reconstruction error for RBMs can be seen in Figure 21.7.

As shown in Figure 21.7, the reconstruction error is small for the last RBM. This may indicate that RBM has formed a model that can detect the pattern of the data. This process is performed in an unsupervised manner. The next stage in the training process is performed in a supervised manner which is the same as ANN [11] and its training loss can be seen in Figure 21.8. This training loss decreases significantly in 356th epoch which may indicate that the training process needs relatively high computation time. However, this model is robust to detect the testing data which is not included in training process coming from the operator.

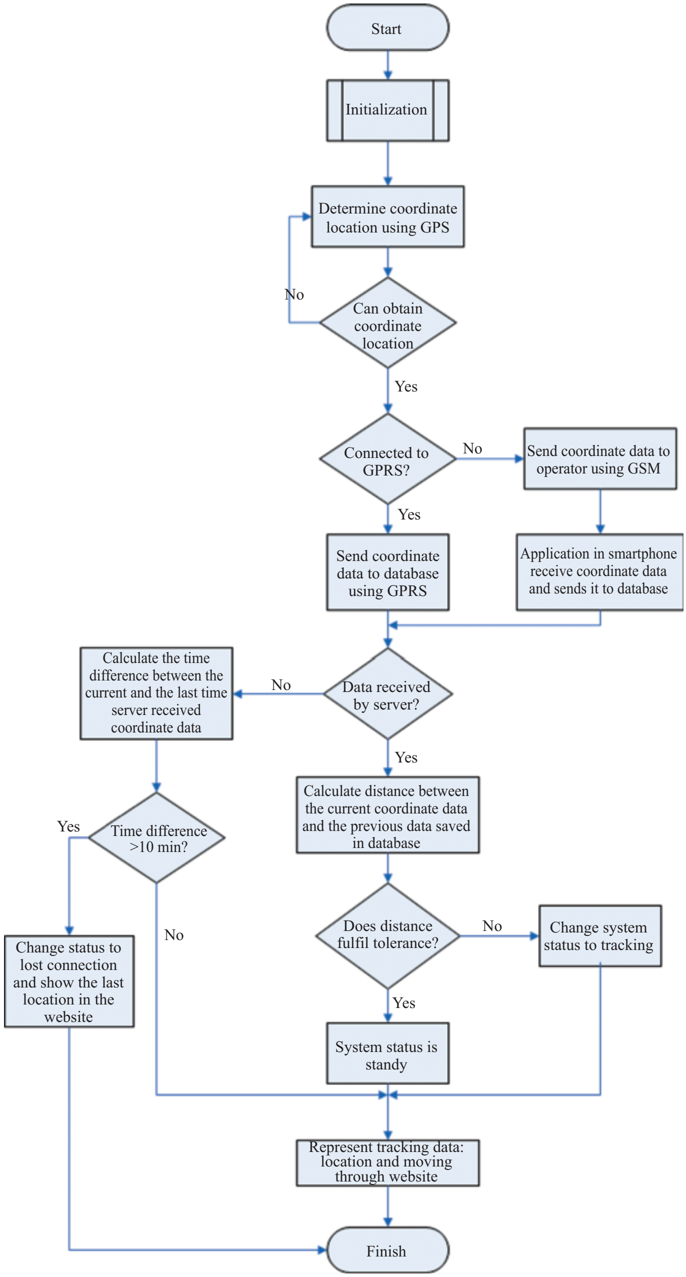


Figure 21.3 Flowchart tracking system using GPS

Figure 21.4 Website interface

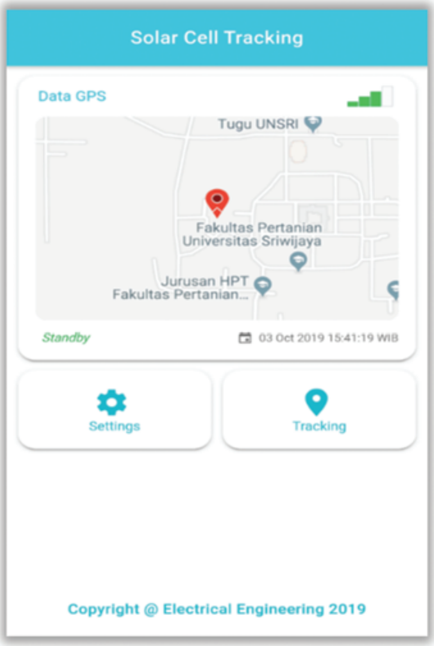


Figure 21.5 Android application interface

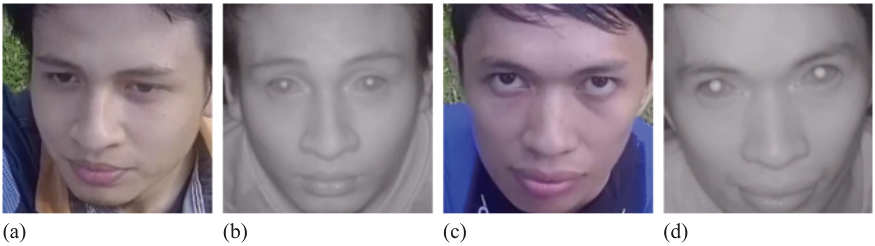


Figure 21.6 Sample of known face (2 operators) used in training, bright 1 (a), dark 1 (b), bright 2 (c), and dark 2 (d)

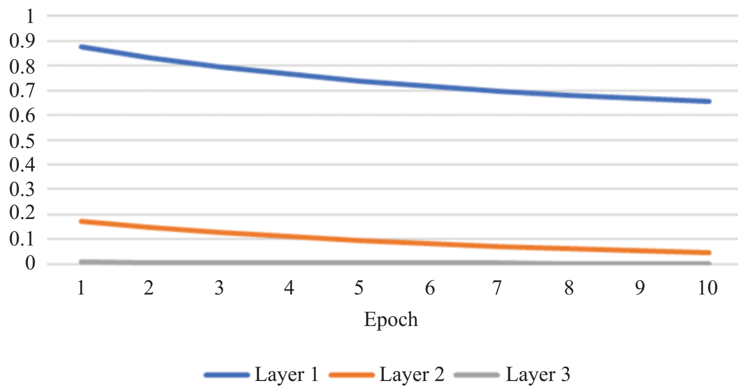


Figure 21.7 RBM reconstruction error

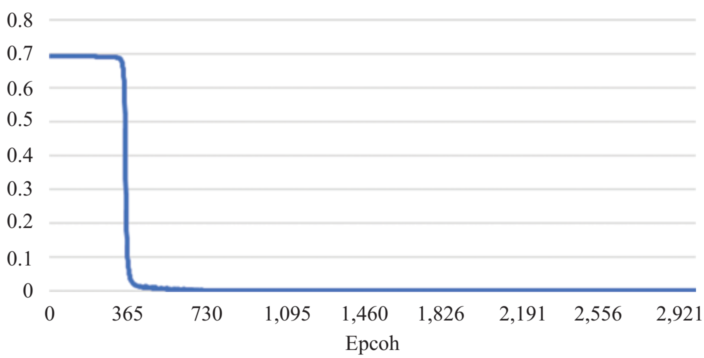


Figure 21.8 Training loss of ANN

21.3.2 Offline test

Offline test is divided into known face (operator) and unknown face (suspect). To detect unknown face, the system must represent the confidence probability based on the model of FaceNet and DBN which have been trained earlier. Here, the confidence probability below 90% may imply unknown face. Higher confidence probability is chosen because the aim of this face recognition is performed as a security system.

For known face, the system has an accuracy of 96.4%. It may recognize 964 images of operators from 1,000 images that are not included in the training process. This result shows that the system is good enough to recognize the known face.

Later, the system is tested using unknown images that are totally new data. These images come from nine different individuals for both image and video. The results of testing using image can been seen in Table 21.3.

As shown in Table 21.3, the proposed system is able to recognize unknown face for each person. The error still occurs in the first unknown image that is recognized as operator. There might be some factors that cause it such as light intensity and the feature of unknown face may have similar characteristics as the operators' faces used in the training.

Next, the test was also performed in the video for unknown faces. Videos for nine unknown faces were recorded using CCTV and webcam to see the performance of the deep learning model in two different cameras. The results can be seen in Table 21.4.

From Table 21.4, the system can work well for moving images (video) using CCTV and webcam. Accuracy of recognizing unknown face is 94.44% for video. However, for the night where lighting is limited, CCTV gives better accuracy than

Table 21.3 Results of offline test for unknown face

No.	Face image	Lighting condition	Recognition	Prediction (confidence)
1	Unknown 1	Bright	False	Operator 1 (100%)
		Dark	False	Operator 1 (99.91%)
2	Unknown 2	Bright	True	Operator 1 (83.16%)
		Dark	True	Operator 2 (56.12%)
3	Unknown 3	Bright	True	Operator 1 (67.55%)
		Dark	True	Operator 1 (84.85%)
4	Unknown 4	Bright	True	Operator 1 (66.23%)
		Dark	True	Operator 2 (75.55%)
5	Unknown 5	Bright	True	Operator 1 (73.38%)
		Dark	True	Operator 2 (52.2%)
6	Unknown 6	Bright	True	Operator 1 (52.94%)
		Dark	True	Operator 1 (61.35%)
7	Unknown 7	Bright	True	Operator 1 (72.43%)
		Dark	True	Operator 2 (78.45%)
8	Unknown 8	Bright	True	Operator 2 (82.94%)
		Dark	True	Operator 2 (79.99%)
9	Unknown 9	Bright	True	Operator 2 (81.95%)
		Dark	True	Operator 1 (50.96%)

Table 21.4 Offline test using video for unknown faces

Face image	Camera	Lighting condition	Capture	Probability (confidence) (%)
Unknown 1	CCTV	Bright	Fail	100
		Dark	Success	77.88
	Webcam	Bright	Fail	100
		Dark	Success	85.27
Unknown 2	CCTV	Bright	Success	70.02
		Dark	Success	64.93
	Webcam	Bright	Success	50.88
		Dark	Success	66.96
Unknown 3	CCTV	Bright	Success	82.77
		Dark	Success	87.84
	Webcam	Bright	Success	81.19
		Dark	Success	74.29
Unknown 4	CCTV	Bright	Success	83.88
		Dark	Success	74.81
	Webcam	Bright	Success	54.65
		Dark	Success	55.39
Unknown 5	CCTV	Bright	Success	73.19
		Dark	Success	79.8
	Webcam	Bright	Success	69.84
		Dark	Success	63.61
Unknown 6	CCTV	Bright	Success	83.74
		Dark	Success	52.9
	Webcam	Bright	Success	73.97
		Dark	Success	73.65
Unknown 7	CCTV	Bright	Success	67.93
		Dark	Success	73.95
	Webcam	Bright	Success	72.79
		Dark	Success	87.74
Unknown 8	CCTV	Bright	Success	50.53
		Dark	Success	63.55
	Webcam	Bright	Success	86.13
		Dark	Success	83.26
Unknown 9	CCTV	Bright	Success	67.65
		Dark	Success	84.11
	Webcam	Bright	Success	55.18
		Dark	Success	85.78

webcam because it has infrared which is helpful in capturing the face compared with webcam as shown in Figure 21.9.

21.3.3 Online test

As the proposed security system will work in real time, the online test should be performed. As shown in Figure 21.9, the face captured using CCTV gives better result than webcam. However, CCTB brand used in the experiment has difficulty in making connection to Python used in face recognition system. Hence, during the online test, webcam is utilized to capture image in video format.

(a) (b)

Figure 21.9 Captured image for unknown face, using CCTV (a) and webcam (b)

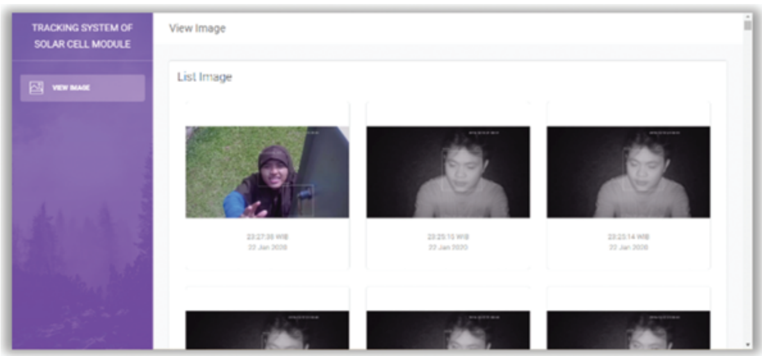


Figure 21.10 Website interface for storing the unknown face captured by the face recognition system

In the online test, using face recognition system that has been trained by deep learning earlier, the unknown detected face will be captured and sent to website as shown in Figure 21.10. Here, website has a role as the database which presents unknown faces captured by the system. Results of online test can be seen in Table 21.5.

As shown in Table 21.5, the system can detect unknown face and send it to the database. This can be helpful for the operators to monitor solar panel, especially when the solar panel is stolen. This security system based on face recognition works well in the day when the light is bright. Nevertheless, in the night, the system experiences difficulty in detecting and recognizing the face because the face image is not clear. Overall, the proposed system is able to recognize unknown face with an accuracy of 87.5% for real-time condition.

21.3.4 GPS tracking test

As an integrated security system, the GPS tracking system may work when the stolen solar panel has moved from its original position. The face recognition may be helpful

Table 21.5 Results of online test

Thief	**Upload image**	
	Bright (day light)	**Dark (night)**
Unknown 1	Success	Success
Unknown 2	Success	Success
Unknown 3	Success	Success
Unknown 4	Success	Success
Unknown 5	Fail	Success
Unknown 6	Success	Success
Unknown 7	Success	Success
Unknown 8	Success	Success

Table 21.6 Initial coordinate data of solar panel

Smartphone data		**Sensor GPS data**	
Latitude	Longitude	Latitude	Longitude
−3.21525°	104.64857°	−3.21521°	104.64859°

for the operator to find the suspect who stole the solar panel. However, the solar panel that has been stolen needs to be tracked so that its position can be found.

In the first experiment for testing the accuracy of GPS system, the solar panel is placed in the initial position and the coordinate for this initial position can be seen in Table 21.6.

As shown in Table 21.6, the coordinate GPS sensor has good accuracy as the difference between the coordinate from smartphone which is obtained from Google Maps is 0.00004 and 0.00003 for latitude and longitude, respectively. Then, the solar panel module box is moved to different locations of 1, 10, 50, 100, 150, 200 m away from the initial location. The results of coordinate changes can be seen in Table 21.7. As shown in the table, the first data have coordinates of −3.21523° and 104.64860° for latitude and longitude, respectively, when the GPS sensor is moved for 1 m. Hence, we can find the distance from two coordinates (see Table 21.6 for initial coordinate and the data in Table 21.7) using Haversine equation [12] as follows.

$$\Delta \text{lat} = \text{lat2} - \text{lat1}$$

$$\Delta \text{lng} = \text{lng2} - \text{lng1}$$

$$a = \sin^2\left(\frac{\Delta \text{lat}}{2}\right) + \cos(\text{lat1}) \times \cos(\text{lat2}) \times \sin^2\left(\frac{\Delta \text{lng}}{2}\right)$$

$$d = 2 \times R \times \text{arc}\sin\left(\sqrt{a}\right)$$

Table 21.7 Coordinate data after moving the position of GPS sensor

Smartphone data		Sensor GPS data		Distance (m)		
Latitude	Longitude	Latitude	Longitude	Smartphone	Sensor	Actual
−3.21523°	104.64860°	−3.21523°	104.64860°	4.01	2.49	1
−3.21509°	104.64858°	−3.21515°	104.64862°	17.85	7.47	10
−3.21477°	104.64860°	−3.21477°	104.64860°	53.54	48.99	50
−3.21433°	104.64860°	−3.21432°	104.64860°	102.47	99.08	100
−3.21391°	104.64860°	−3.21387°	104.64860°	149.21	149.17	150
−3.21345°	104.64870°	−3.21342°	104.64860°	200.90	199.26	200

where d is the distance in meter, R is the radius of earth at the equator which is 6,378,137 m, and Δlat, Δlng, lat1, lat2, lng1, and lng2 are in radian.

From Table 21.7, the difference between actual data and GPS sensor as well as smartphone is large enough for the first three data. This difference becomes smaller for the fourth to sixth data. The difference is about 2.53 m which is suitable with the specification of the sensor in this research with the error of about ±2.5 m [13].

21.3.5 GPS tracking: communication system

The proposed tracking system must have good communication system. Thus, the success of sending data and time while sending data is important. In this study, GPRS will be utilized as communication data system for Internet network and GSM is a backup system for SMS.

The initial position is shown by red bullet in Figure 21.11. This figure represents the moving lane of solar panel box. The aim is to get the coordinate data and time for sending the data from initial to the current position.

Results for communicating system using GPRS after moving object 16 times can be seen in Table 21.8. As shown in the table, the time need for sending and receiving the coordinate data is around 2–4 s with the average of 2.38 s. And the time to send the moving object from one location to other is about 17–22 s. Meanwhile, server may receive the data in about 18–21 s. The average time is 19.53 and 19.40 s for sending and receiving, respectively. Table 21.8 also shows the signal strength with the unit of received signal strength indicator (RSSI) [14] where the higher is the better signal strength.

In addition, this study also performed experiment for different speeds while the object is moving from one to another position. The speed varies from 20 to 60 km/h as shown in Tables 21.9 and 21.10.

We can see from Table 21.10 that the duration for sending the data is the same as Table 21.9 which is 2 s. Time delay for sending and receiving the data is 19 and 18.75 s, respectively. This means that the speed of moving object may not influence GPRS in sending and receiving the data. Using GPRS, the tracking system needs 2.38 s for receiving coordinate data and 19.4 s for receiving them. This process of sending and receiving data may depend on the signal strength.

Figure 21.11 Moving lane of solar panel box to test communication system

Table 21.8 Results of communication system using GPRS

Sending time (WIB)	Receiving time (WIB)	Sending time duration (s)	Time differences		Signal strength
			Sent (s)	Received (s)	
13:38:57	13:38:59	2	0	0	17
13:39:16	13:39:18	2	19	19	17
13:39:35	13:39:37	2	19	19	18
13:39:54	13:39:56	2	19	19	21
13:40:13	13:40:15	2	19	19	19
13:40:32	13:40:34	2	19	19	19
13:40:51	13:40:53	2	19	19	14
13:41:10	13:41:12	2	19	19	16
13:41:28	13:41:31	3	18	19	15
13:41:48	13:41:51	3	20	20	14
13:42:08	13:42:12	4	20	21	14
13:42:30	13:42:33	3	22	21	18
13:42:51	13:42:53	2	21	20	19
13:43:10	13:43:13	3	21	20	23
13:43:30	13:43:32	2	20	19	29
13:43:48	13:43:50	2	18	18	31
Average		2.38	19.53	19.40	19

As communication data also utilizes GSM, the testing of sending and receiving coordinate data is also performed in this study. The results can be seen in Table 21.11.

Table 21.11 shows that the duration of sending data using GSM is longer than using GPRS. The average time is 4.87 s which is twice that of GPRS. It might happen because GSM has two stages in sending data. First, the system sends the coordinate data through SMS to smartphone and later, application in smartphone reads SMS and sends the coordinate data to database using Internet connection. Figure 21.12 shows the SMS sent to the smartphone.

Table 21.9 Results of communication system using GPRS (20 km/h)

Sending time (WIB)	Receiving time (WIB)	Sending time duration (s)	Time differences		Signal strength
			Sent (s)	Received (s)	
11:14:02	11:14:04	2	0	0	18
11:14:21	11:14:23	2	19	19	16
11:14:40	11:14:42	2	19	19	15
11:14:59	11:15:01	2	19	19	16
11:15:18	11:15:20	2	19	19	15
Average		2	19	19	16

Table 21.10 Results of communication system using GPRS (60 km/h)

Sending time (WIB)	Receiving time (WIB)	Sending time duration (s)	Time differences		Signal strength
			Sent (s)	Received (s)	
11:35:05	11:35:07	2	0	0	25
11:35:24	11:35:26	2	19	19	18
11:35:42	11:35:44	2	18	18	21
11:36:01	11:36:03	2	19	19	17
11:36:20	11:36:22	2	19	19	16
Average		2	18.75	18.75	19.4

As shown in Figure 21.12, there are some information sent in this SMS. The sequences information is as follows: the sending time, signal strength, status, type of communication, latitude and longitude. As seen in Table 21.11, GSM needs 18.71 and 18.57 s time delay for sending and receiving the coordinate data, respectively. This may imply that the time delay for sending and receiving may not be influenced by the type of communication data and the speed of moving object. It may be affected by the feedback response given by SIM808. From Tables 21.8 to 21.11, the time delay for sending each data is almost equal to about 19 s. Hence, communication using GSM can be utilized as a backup system when signal strength is low or Internet is unavailable.

21.3.6 GPS tracking: real-time system test

The purpose of GPS tracking in the security system of solar panel is to track the position of the stolen solar panel box in a real-time manner. The initial coordinates for this real-time test is shown in Table 21.12.

When the initial position has been saved in the database, the system will have "standby" status automatically as shown in Figure 21.13. The object will not be moved for 10 min to distinguish whether the position is moving or not. Table 21.12

Table 21.11 Results of communication system using GSM

Sending time (WIB)	**Receiving time (WIB)**	**Sending time duration (s)**	**Time differences**		**Signal strength**
			Sent (s)	**Received (s)**	
14:11:29	14:11:35	6	0	0	18
14:11:51	14:11:56	5	22	21	16
14:12:09	14:12:14	5	18	18	21
14:12:27	14:12:32	5	18	18	18
14:12:45	14:12:50	5	18	18	28
14:13:06	14:13:11	5	21	21	21
14:13:24	14:13:29	5	18	18	18
14:13:42	14:13:46	4	18	17	16
14:13:59	14:14:04	5	17	18	16
14:14:17	14:14:22	5	18	18	19
14:14:35	14:14:40	5	18	18	14
14:14:53	14:14:57	4	18	17	14
14:15:10	14:15:15	5	17	18	20
14:15:30	14:15:35	5	20	20	26
14:15:51	14:15:55	4	21	20	29
Average		4.87	18.71	18.57s	19.6

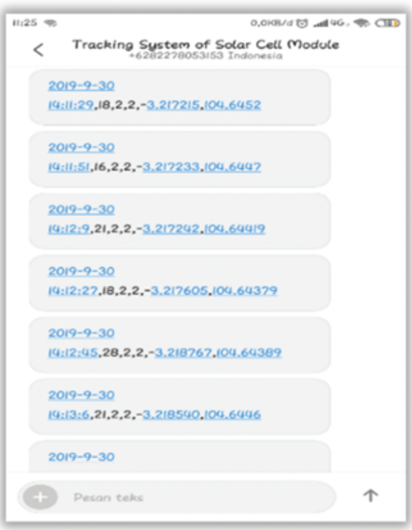


Figure 21.12 Coordinate data from GSM communication system through SMS

Table 21.12 Coordinate data for initial position to test the real-time GPS system

	Coordinate		Signal strength	Status
	Latitude	Longitude		
Initial position	−3.21737°	104.64520°	15	Standby
After 10 min without moving the object	−3.21737°	104.64520°	20	Standby

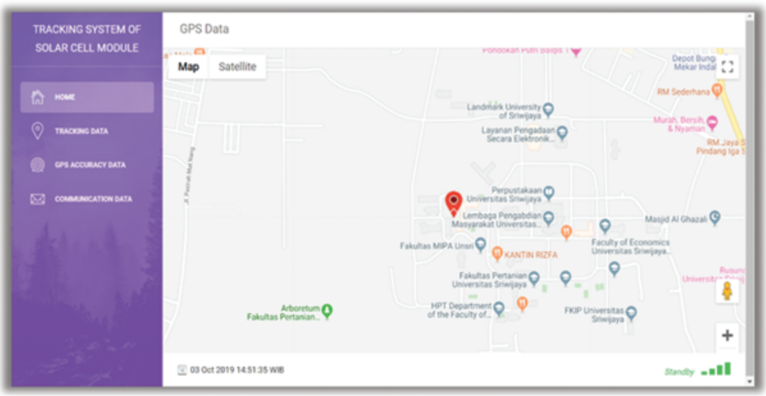


Figure 21.13 System interface in standby mode

Figure 21.14 System interface in tracking mode

shows that the coordinate data do not change for 10 min when the object is not moving. Thus, the system is able to distinguish the standby mode.

Later, the object is moved to new position as shown in Figure 21.14 and the coordinate data can be seen in Table 21.13. As shown in Figure 21.14, pin location colored blue represents the initial position of solar panel module and the red represents the final location of it. From this figure, we can see that the proposed system

Table 21.13 Coordinate data for real-time GPS tracking system

No.	Sending time (WIB)	Coordinate		Signal strength	Communication type
		Latitude	Longitude		
1	14:54:56	−3.21726°	104.6446°	15	GPRS
2	14:55:12	−3.2173°	104.644°	20	GPRS
3	14:55:28	−3.21784°	104.64388°	18	GPRS
4	14:55:44	−3.21913°	104.64376°	24	GPRS
5	14:56:00	−3.2201°	104.64378°	17	GPRS
6	14:56:15	−3.22041°	104.6442°	15	GPRS
7	14:56:31	−3.22039°	104.6454°	15	GPRS
8	14:56:47	−3.22044°	104.6465°	17	GPRS
9	14:57:03	−3.22001°	104.64682°	13	GPRS
10	14:57:19	−3.21947°	104.6468°	13	GPRS
11	14:57:36	−3.21956°	104.6475°	11	GPRS
12	14:57:53	−3.21952°	104.6483°	10	GPRS
13	14:58:09	−3.21950°	104.64900°	9	GSM
14	14:58:25	−3.21954°	104.64970°	9	GSM
15	14:58:41	−3.21921°	104.6504°	12	GPRS
16	14:58:57	−3.21823°	104.65059°	12	GPRS
17	14:59:35	−3.21729°	104.6508°	21	GPRS
18	14:59:51	−3.21735°	104.6514°	19	GPRS
19	15:00:08	−3.21733°	104.6526°	18	GPRS
20	15:00:24	−3.21729°	104.6534°	23	GPRS
21	15:00:42	−3.21734°	104.6548°	22	GPRS
22	15:00:59	−3.21731°	104.656°	18	GPRS
23	15:01:16	−3.21731°	104.657°	19	GPRS
24	15:01:34	−3.21729°	104.6585°	19	GPRS
25	15:01:52	−3.21808°	104.65902°	19	GPRS
26	15:02:10	−3.21853°	104.65939°	19	GSM
27	15:02:26	−3.21897°	104.6593°	24	GPRS
28	15:02:42	−3.21898°	104.6593°	23	GPRS

may recognize the position of the solar panel from standby to moving. Figure 21.14 also shows that the tracking system is able to draw the lane that is passed by the solar panel box. In Table 21.13, data of 28 coordinates represent different communication systems. It is in GSM mode for three times (13th, 14th, and 26th data). The system will automatically move to GSM when the system cannot send the data using Internet or there is an error as well as disturbance while sending the data which may cause failure. In the 13th and 14th data, the signal strength is 9 which is considered low and hence the system uses GSM directly. Meanwhile, in the 26th data, the signal strength is 19 which is good enough but there might be failure or error while sending the data.

Figure 21.15 shows the visualization of coordinate data as shown in Table 21.13. The red and gray colors represent the data sending by GPRS and GSM, respectively. The details of sending time can be seen in Table 21.14.

Figure 21.15 Visualization of coordinate data and the signal strength in real-time test of tracking system

From Table 21.14, the average sending time is 4.64 s. This time duration may be affected by the strength of the signal. In this experiment, the signal strength is 16.93 so the system needs lesser time in sending the coordinate data.

Lastly, the experiment is also performed for a condition when the system cannot connect to the satellite or when there is no GPRS or GSM connection. Figure 21.16 shows the interface when the system cannot be connected to the server.

As shown in Figure 21.16, the interface is quite different with Figure 21.14. Status system has changed to a lost connection and there is a circle around the red pin. The radius represented by this condition is set to be 100 m. This may indicate the last location of the solar panel box. This condition may occur after 10 mins that the system cannot send data to the server.

From the results and discussions earlier, we can see that the face recognition system and tracking system work together as integrated security system. The security system is able to capture the unknown face who is suspected to be harmful to the solar panel module. The face recognition developed using deep learning can distinguish the known and unknown faces. On the other hand, the tracking system that is aimed to track the position of the stolen solar panel box works well using GPS technology based on GPRS and GSM. The tracking system can recognize the solar panel module position whether it stays still or move to a new location. Those both face recognition and tracking system can be monitored through an interface based on website. Thus, this security system can be applied in real-time condition. In addition, the tracking system is able to manage the lost connection status by giving the information of the last location in radius of 100 m after 10 min when the system cannot send new coordinate data.

Table 21.14 Data for communication system in real-time test of tracking system

Sending time (WIB)	**Receiving time (WIB)**	**Sending time duration (s)**	**Time differences**		**Signal strength**
			Sent (s)	**Received (s)**	
14:54:56	14:55:02	6	0	0	15
14:55:12	14:55:18	6	16	16	20
14:55:28	14:55:34	6	16	16	18
14:55:44	14:55:50	6	16	16	24
14:56:00	14:56:06	6	16	16	17
14:56:15	14:56:21	6	15	15	15
14:56:31	14:56:37	6	16	16	15
14:56:47	14:56:53	6	16	16	17
14:57:03	14:57:06	3	16	13	13
14:57:19	14:57:22	3	16	16	13
14:57:36	14:57:40	4	17	18	11
14:57:53	14:57:56	3	17	16	10
14:58:09	14:58:14	5	16	18	9
14:58:25	14:58:30	5	16	16	9
14:58:41	14:58:44	3	16	14	12
14:58:57	14:59:05	8	16	21	12
14:59:35	14:59:38	3	38	33	21
14:59:51	14:59:55	4	16	17	19
15:00:08	15:00:11	3	17	16	18
15:00:24	15:00:28	4	16	17	23
15:00:42	15:00:45	3	18	17	22
15:00:59	15:01:03	4	17	18	18
15:01:16	15:01:20	4	17	17	19
15:01:34	15:01:39	5	18	19	19
15:01:52	15:01:55	3	18	16	19
15:02:10	15:02:17	7	18	22	19
15:02:26	15:02:31	5	16	14	24
15:02:42	15:02:45	3	16	14	23
Average		4.64	17.26	17.15	16.93

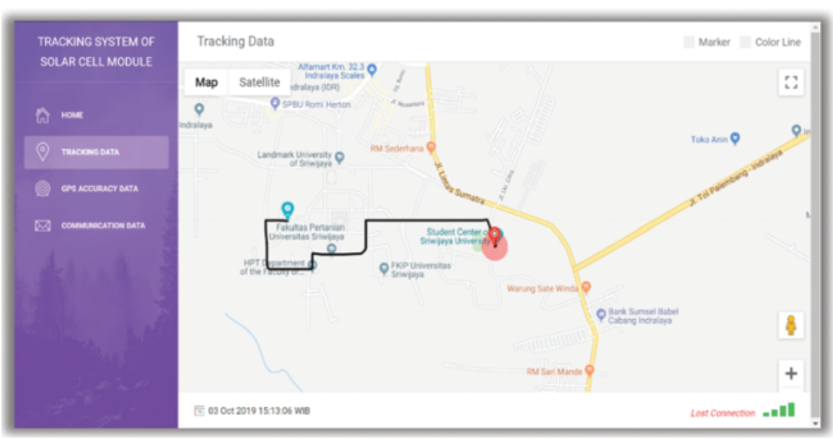


Figure 21.16 Interface for system response when the solar panel box has lost connection to the server

21.4 Conclusion

This study proposed an integrated system for a security system to find and track the stolen good. The first level of security system is face recognition system that may recognize unknown face using FaceNet as the feature extraction and DBN for the classifier. This system is integrated to the database. From the experiment performed in offline and online manner, the system is able to recognize unknown face with an accuracy of 94.4% for offline and 87.5% for online or in real-time condition. The unknown face recognized by the system is captured and sent to the database may be helpful to find the suspect who stole the object. Meanwhile, the stolen object position needs to be tracked. This tracking is performed in the second level of security system once the object has been stolen. The tracking system utilizes GPS integrated to the database using GPRS and GSM as communication system. The error of GPS sensor is about 2.5 m with the sending time duration of 4.64 s. The system can also track the coordinate location well using both GPRS and GSM and this is affected by the strength of the signal.

The proposed security system could be useful for the security system as it combines the technology of face recognition and GPS tracking.

References

[1] P. Kumar, M. Agarwal, and S. Nagar, "A Survey on Face Recognition System—A Challenge," *Int. J. Adv. Res. Comput. Commun. Eng.*, vol. 2, no. 5, pp. 2167–2171, 2013.

[2] A. Nurhopipah and A. Harjoko, "Motion Detection and Face Recognition for CCTV Surveillance System," *IJCCS (Indonesian J. Comput. Cybern. Syst. Yogyakarta, Indones.)*, vol. 12, no. 2, pp. 107–118, 2018.

[3] D. A. R. Wati and D. Abadianto, "Design of Face Detection and Recognition System for Smart Home Security Application," *2017 2nd Int. Conf. Inf. Technol. Inf. Syst. Electr. Eng.*, pp. 342–347, 2017.

[4] Z. Liu, A. Zhang, and S. Li, "Vehicle Anti-Theft Tracking System Based on Internet of Things," in *Proceedings of 2013 IEEE International Conference on Vehicular Electronics and Safety, ICVES 2013*, 2013.

[5] K. A. Salim and I. M. Idrees, "Design and Implementation of Web-Based GPS–GPRS Vehicle Tracking System," *IJCSET Dec*, vol. 3, no. 3, pp. 5343–5345, 2013.

[6] P. Singh, T. Sethi, B. B. Biswal, and S. K. Pattanayak, "A Smart Anti-Theft System for Vehicle Security," *Int. J. Mater. Mech. Manuf.*, vol. 3, no. 4, pp. 249–254, 2015.

[7] P. A. Shinde and Y. B. Mane, "Advanced Vehicle Monitoring and Tracking System Based on Raspberry Pi," *Proc. 2015 IEEE 9th Int. Conf. Intell. Syst. Control. ISCO 2015*, 2015.

[8] P. Viola and M. J. Jones, "Robust Real-time Object Detection," *2nd Int. Work. Stat. Comput. Theor. Vis.—Model. Learn. Comput. Sampling. Vancouver, Canada*, vol. 57, pp. 1–30, 2001.

[9] F. Schroff, D. Kalenichenko, and J. Philbin, "FaceNet: A Unified Embedding for Face Recognition and Clustering," *2015 IEEE Conf. Comput. Vis. Pattern Recognit.*, pp. 815–823, 2015

[10] I. Goodfellow, Y. Bengio, and A. Courville, *Deep Learning*, vol. 1. London, England: Nature Publishing Group, 2016.

[11] G. E. Hinton, "Deep Belief Networks," *Scholarpedia*, vol. 4, no. 5, p. 5947, 2009.

[12] I. Setyorini and D. Ramayanti, "Finding Nearest Mosque Using Haversine Formula on Android Platform," *J. Online Inform.*, vol. 4, no. 1, p. 57, 2019.

[13] S. W. Sun, X. Wang, X. Xiao, L. Teng, X. Zhang, and H. Yang, *SIM808 Hardware Design*. Shanghai: Shanghai SIMCom Wireless Solutions Ltd., 2015.

[14] SIMCom, *SIM800 Series AT Command Manual*, vol. 1. Shanghai: Shanghai SIMCom Wireless Solutions Ltd., 2015.