Detection of Insiders' Sabotage using Time-Series Data Analysis of Hand Motion

東京大学	陳　実	Shi CHEN	Student Member
東京大学	出町　和之	Kazuyuki DEMACHI	Member

The importance of nuclear security increased after Fukushima Daiichi nuclear power plant accident. Especially as a threat to nuclear power plants, sabotage by insider is worthy of attention. In response to this situation, hand motion is an important part of human activity and it has high contribution to high-accuracy detection of insiders' sabotage. Moreover, Time series data analysis is a useful method in abnormal behavior detection.
In this research, the real-time hand motion detection system was developed using video camera. In addition, the possibility of insiders' sabotage detection was explored by using Deep Learning.

Keywords: Nuclear Security, Sabotage Detection, Hand Motion Tracking, Time-Series Data Analysis, Deep Learning

1. Introduction

Recently, the threat to nuclear security by sabotage is increased. In addition, when considering the sabotage, due attention should be paid to insider since they could take advantage of their access authority and knowledge, to bypass dedicated physical protection elements or other provisions [1]. The primary Physical Protection System (PPS) functions are prevention, detection, delay and response [2]. It is noticeable that if detection failed, delay and response would become invalid. In this case, detection of insiders' sabotage is necessary and should be enhanced. Considering current countermeasures of PPS to insider sabotage, the most significant challenge is how to distinguish ordinary maintenance behaviors and malicious behaviors since some malicious behaviors may hidden in ordinary maintenance behaviors. Moreover, hand motion has high contribution to human activity and a significant portion of maintenance behaviors and malicious behaviors are realized through hand motion. It is clear from the above that hand motion analysis should be taken into consideration for detection of insiders' sabotage.

Conventional research of abnormal behavior detection commonly use static image analysis and learn features from normal pattern. However, it's difficult to distinguish malicious behaviors from ordinary maintenance behavior by static image analysis since some frames of these two types of motions may share some similarity. In order to solve this problem, time-series data analysis will be used in our research. Compared with static image analysis, time-series data analysis can detect more scenes, more detail information and time variation information. In addition, data compression can be proceeded and amount of computations can be reduced by feature extraction. Machine learning is frequently used to analyze time-series data [3]. Moreover, research has shown the value of using Deep Learning for feature learning [4], and it can be applied in recognition of different patterns of motion.

連絡先:陳　実、〒113-8656　東京都文京区本郷 7－3－1、東京大学大学院工学系研究科　原子力国際専攻
E-mail: shichen@g.ecc.u-tokyo.ac.jp

In this research, the real-time hand motion detection system was developed using video camera. In addition, the possibility of insiders' sabotage detection was explored by using Deep Learning.

2. Methodology

2.1 Hand Motion Detection

Fingertips position can be used to detect hand motion and recognize hand gesture. The fingertips calculation algorithm in this research based on RGB and depth image analysis. The hand motion detection system consists of four main components: RGB and depth data acquisition, hand region classification, fingers segmentation and fingers identification. Stretched fingers pixels and bend fingers pixels of both left and right hands were classified as different parts based RGB and depth image. Fingers were identified by using K-means clustering algorithm [5]. This system is developed by using Visual Studio 2015 with C# as programming language. The roadmap of hand motion detection system development can be demonstrated as Fig.1.

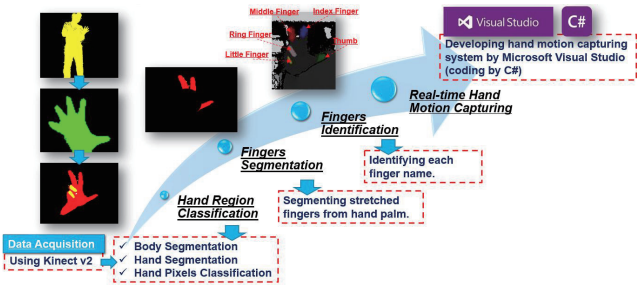

Fig.1 Roadmap of Hand Motion Detection System

2.2 Behavior Recognition

To distinguish malicious behavior and ordinary maintenance behavior, different malicious motion should be classified into different patterns. Deep Learning is considered as a useful method for pattern recognition and was implemented in this research.

The structure of Deep Neural Network in this research can be demonstrated in Fig.2. First-order features can be learned by train the raw inputs (time series data of all malicious motions, 900 neurons in each sample). Next, these features will be feed into the second layer to obtain the second-order features. Finally, these second-order features will be treated as raw input to a SoftMax classifier, and the probability of each pattern can be output.

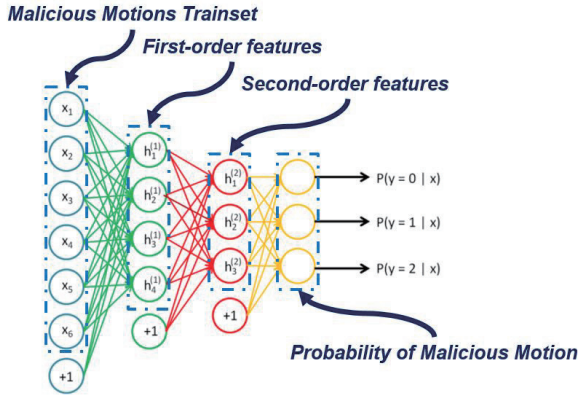

Fig.2 Structure of Deep Neural Network

3. Results

For hand motion detection, positions of each fingertip can be captured by the real-time detection system we developed with the frame rate of 22fps. The result of hand motion detection can be seen in Fig.3.

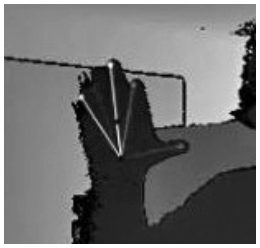

Fig.3 Results of Hand Motion Detection.

Recently, we assumed five malicious motions for the experiment behavior detection:

(1) Cutting motion (by using scissor, etc.);
(2) Patting motion (control panel, etc.);
(3) Turning motion (switch, etc.);
(4) Grasping motion (tools);
(5) Pushing motion (buttons).

In current experiment, we captured five malicious motions with different persons in different distance and angle to camera. By training Deep Neural Network using this trainset, these five malicious motions can be classified into different pattern. Then this trained Deep Neural Network can be used to detect malicious motions. All of these five motions can be distinguished from ordinary normal motions by using trained Deep Neural Network. Detection accuracy is shown in Table 1:

Table 1 Accuracy of Malicious Motion Detection

Motion	Accuracy (%)
Cutting	100
Putting	100
Turning	92.47
Grasping	96.23
Pushing	84.25
Normal	77.23

4. Conclusion and Future Work

In this research, a fingertips calculation algorithm was proposed and a real-time hand motion detection system was developed. In addition, assumed insider malicious motions can be classified into different patterns and detected using Deep Neural Network.

For future work, how to achieve practicality of new method and exploring the possibility of practical implementation will be considered. Moreover, the possibility of AI-based automatically insiders' sabotage detection system development will be explored.

Reference

[1] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5), Nuclear Security Series No. 13, IAEA, Vienna (2011).

[2] Garcia, Mary Lynn, "Design and evaluation of physical protection systems," Butterworth-Heinemann (2007).

[3] Dorffner, Georg. "Neural networks for time series processing." Neural Network World, 6 (4) (1996), 447–468.

[4] Vincent, Pascal, et al. "Stacked denoising autoencoders: Learning useful representations in a deep network with a local denoising criterion." Journal of Machine Learning Research 11. Dec (2010): 3371-3408.

[5] Ray, Siddheswar, and Rose H. Turi. "Determination of number of clusters in k-means clustering and application in colour image segmentation." Proceedings of the 4th international conference on advances in pattern recognition and digital techniques. 1999.