Research on Anomalous Behavior Detection and Dangerousness Assessment among Civil Aviation Passengers at Checkpoints

Haibin Shen

Civil Aviation University of China

yan Zhang (✉ 2017051033@cauc.edu.cn)

beijing bowei airport support ltd. <https://orcid.org/0000-0002-7670-1087>

Research Article

Keywords: security check, civil aviation passengers, anomalous behavior detection, neural network, conjugate gradient method, SMOTE

Posted Date: August 26th, 2021

DOI: <https://doi.org/10.21203/rs.3.rs-266445/v1>

License: © ⓘ This work is licensed under a Creative Commons Attribution 4.0 International License.

[Read Full License](#)

Research on Anomalous Behavior Detection and Dangerousness Assessment among Civil Aviation Passengers at Checkpoints

Haibin Shen ¹ Yan Zhang ^{2,*}

1 Economics & Management College, Civil Aviation University of China;

hbshen@cauc.edu.cn

2 Western Management Department, Beijing Bowei Airport Support Ltd.,

2017051033@cauc.edu.cn

* Correspondence: 2017051033@cauc.edu.cn; +86-15510916092

Abstract: Traditional civil aviation security check measures are focused on baggage rather than passengers. The goal of this study is to enhance the level and effectiveness of security measures. We propose an anomalous behavior detection technique for civil aviation passengers and a passenger risk-assessment method based on a neural network method. A large number of real cases were analyzed and summarized to extract indicators of anomalous behavior of civil aviation passengers, and an index system was developed to detect anomalous behavior of passengers at checkpoints. A neural network method was used to evaluate the passengers and classify the risk level to detect potentially dangerous personnel, monitor people, and create an emergency warning system. The synthetic minority oversampling technique (SMOTE), the conjugate gradient method, and a multilayer perceptron neural network were used to classify the risk level of passengers at checkpoints. The results demonstrated that the proposed index system and evaluation method were well suited to deal with the ambiguity and uncertainty in the recognition process. The anomalous behavior of civil aviation passengers at checkpoints and the associated threat level were accurately identified.

Keywords: security check; civil aviation passengers; anomalous behavior detection; neural network; conjugate gradient method; SMOTE

0. Introduction

Civil aviation security has attracted unprecedented attention, and remarkable achievements have been made in the civil aviation industry in China, which has expanded rapidly. In 2018, there were 11.53 million flight hours with zero liability accidents, representing an annual increase of 8.9% and achieving a record of 200 months of aviation safety with zero liability accidents. However,

problems still exist despite extensive international and domestic efforts to prevent terrorism and explosions due to insufficient development of the industry, ineffective techniques, and an inability to ensure security. Aviation security still faces significant pressure and many challenges ^[1].

Security measures focused on objects are the core of traditional civil aviation safety measures and include the inspection of contraband and hazardous goods; however, this has many disadvantages. In other words, the passenger is deemed harmless and can board a plane provided he/she does not carry any contraband, hazardous goods, or explosives. The terrorists who hijacked the plane on 9/11 did not carry any contraband or explosives but they caused extensive damage. Therefore, security checks focused on objects are not sufficient. Behavior detection can improve the traditional model and increase the effectiveness and level of aviation security by identifying a person that may represent a potential risk.

The report *Security: Safeguarding International Civil Aviation Against Acts of Unlawful Interference*, Annex 17 to the Convention on International Civil Aviation (2017 version) 4.1.3 suggests that each contracting state should consider integrating behavior detection into its aviation security practices and procedures. Anomalous behavior detection in an aviation security environment refers to the application of techniques involving the detection of behavioral characteristics including but not limited to physiological or gestural signs indicative of anomalous behavior to identify persons who may pose a threat to civil aviation ^[2].

The study of anomalous behavior in the field of sociology started around 1960; initial studies were focused on the anomalous behavior of humans in the natural environment. Since then, many international scholars investigated and applied physiological measurement techniques to behavioral studies such as thermal imagery, eye tracking, electric current tests of the skin, and event-related potential (ERP) measures. In recent years, research on surveillance video and image recognition of anomalous behavior has increased. In 2005, Mecocci et al. designed a video surveillance system for detecting anomalous events; the system has shown great value in practical applications ^[3]. Subsequently, Chen et al. proposed a multi-support vector machine (SVM)-based Bayesian network method to detect anomalous behavior ^[4]; Oyama and Shah presented a new method using a social force model to conduct crowd anomalous behavior detection using video data ^[5]. Gao et al. proposed an optimization method for surveillance image recognition in civil aviation airports based on edge detection ^[6]. Choudhary proposed a real-time crowd behavior detection method using the scale-invariant feature transform (SIFT) technique applied to video sequences ^[7].

In China, Zhang investigated video images to identify anomalous behavior in people in 2007. Motion detection, body recognition, and target tracking were used to monitor the target scene in real-time and detect people with anomalous behavior ^[8]. Xu analyzed 55 aerial hijacking cases in China over the past 30 years and created a preparedness, prevention, and contingency (PPC) model of hijackings based on the theory of crime prevention ^[9]. Rao conducted a study from the perspective of criminology and stated that it was necessary to detect anomalous behavior in civil aviation passengers ^[10]. Wang et al. used a mathematical algorithm to identify anomalous behavior in people;

the algorithm allowed for the identification of several persons in one image and detected several anomalous behaviors ^[11]. Wu et al. determined the dominant position of the human face in anti-spoofing technologies and explored how to assess human faces to detect deception ^[12]. Ma studied anomalous behavior detection based on human morphology and classified the anomalies into several levels. The system provided an automatic warning when a high-level anomaly was identified to achieve ease of management ^[13]. Tang et al. ^[14], Shen and Wu. ^[15], and Wei et al. ^[16] studied anomalous behavior detection based on video and image surveillance data. Hua et al. detected anomalous behavior in people based on the speed of walking ^[17].

In summary, research on anomalous behavior detection in international and domestic studies is rather broad and most research has relied on equipment, measurements, and visualization. To date, no theory or application has been developed to help civil aviation staff to assess the level of danger of passengers using anomalous behavior detection techniques, which can screen and classify passengers for security management. In this study, the anomalous behavior of civil aviation passengers at checkpoints is determined and an evaluation index system is developed. The risk level of civil aviation passengers is classified with a neural network, which provides a timely assessment of the risk to ensure the security of civil aviation.

1. Statistical analysis of cases of anomalous behavior detection in civil aviation

As mentioned above, there is a lack of research on the detection of anomalous behavior of civil aviation passengers domestically and internationally; therefore, we collected information on 149 cases that occurred from 2000 to 2019 in China and abroad, as publicized on the Internet to investigate the anomalous behavior. These cases include not only major security incidents such as attempted hijackings and bombings but also routine cases such as the discovery of illegal knives, lighters, and drugs carried or hidden by passengers at security inspection sites. The number and type of cases are sufficient to conduct an analysis and draw reliable conclusions.

As shown in Fig. 1, many kinds of illegal behaviors were observed. Carrying and hiding forbidden objects such as illegal knives, lighters, and drugs comprised the largest proportion (65%), followed by disturbances. All these activities may pose a threat to civil aviation security.

Fig. 1 Statistical result of violations

The statistical analysis of the areas of occurrence of the anomalous behavior indicates that most of this behavior occurred at the security checkpoints (74.5%), followed by the cabin, as shown in Fig. 2.

Fig. 2 Areas of occurrence of anomalous behavior

As shown in Fig. 3, most of the people who identified the anomalous behavior were ground security guards including security staff, police, and customs officers (81.9%), followed by the crew. This result is in line with the statistical results of the area of occurrence of the behavior, i.e., the checkpoints and cabin.

Fig. 3 Persons that identified anomalous behavior

Most of the people who were identified as exhibiting anomalous behavior were passengers (89%), followed by airline staff or airport employees and others, as shown in Fig. 4.

Fig. 4 Persons exhibiting anomalous behavior

The results demonstrate that anomalous behavior in civil aviation is mainly exhibited by passengers and is generally detected by ground security guards such as security staff and checkpoint personnel. Therefore, in this study, we focus on the anomalous behavior of civil aviation passengers at checkpoints.

2. Development of an index system for the detection of anomalous behavior of civil aviation passengers at checkpoints

The statistics indicate that civil aviation passengers with anomalous behavior differ from normal passengers in terms of certain behavioral characteristics; some of these behaviors are similar to those of known criminals or disruptive passengers. This behavior can be identified by security staff during checks. Therefore, it is necessary to conduct research that is applicable to these situations. For instance, security personnel are supposed to observe, analyze, or question passengers regarding their clothing, actions, language expression, facial expression, luggage, etc. when the passengers are in line for security checks or are waiting or boarding to evaluate whether the person is dangerous and may pose a threat to civil aviation security.

The frequency histogram of the indicators of anomalous behavior of passengers is shown in Fig. 5. The most common indicator is the behavior of passengers, followed by facial expressions, language, baggage, clothing, and documents. Passenger documents and physical and baggage inspections have always been the focus of civil aviation safety inspections. The behavioral actions of passengers, their facial expressions, and language are also important aspects of secondary security checks. Therefore, these indications are important for the identification of the anomalous behavior of passengers at checkpoints.

Fig. 5 Frequency histogram of indicators of anomalous behavior

According to the *Guidance for Anomalous Behavior Detection on Passenger Security Checks in Civil Aviation (MD-SB-2013-006)* issued by Civil Aviation Administration of China and the information provided in Section 1, we optimized the indicators to develop a better system for the detection of anomalous behavior of civil aviation passengers at checkpoints; eight indicators are used, as shown in Fig. 6.

Fig. 6 Index system of anomalous behavior detection among civil aviation passengers

(1) Documents

When transporting passengers in civil aviation, standard documents include an ID card or passport. In addition to checking the authenticity of the certificate, the security personnel also determine whether the passenger is a frequent traveler to places of high risk, whether there is defacement, missing pages, or replaced pages in the documents, or whether the passport is newly issued.

(2) Luggage

Many articles carried by civil aviation passengers are common items used during travel. The baggage checks indicate irregularities, for example, whether the luggage is consistent with the

clothing, identity, occupation, and the partner of the traveler, whether the container has an unusual shape or is multi-functional or has several interlayers; it can be determined if the position or manner of the luggage and articles are not in accordance with the general rules. Some passengers may carry far more items than needed for traveling or there is no luggage on a long journey or strange sounds or smells may originate from the passenger or his/her luggage.

(3) Clothing

The clothing of the passenger should be assessed the following anomalies; for instance, whether the appearance or clothing indicates extreme political or religious views; whether the clothing is unusual with regard to the season, climate, or weather; whether the appearance or clothing is unsuitable for his/her luggage, identity, or occupation; whether the clothing or accessories are designed to cover up his/her facial features or expression; whether there are forbidden objects, such as restricted knives or drugs, etc. in artificial limbs, hair or similar prostheses.

(4) Behavioral actions

Behavioral actions include constantly moving towards women or children and following them, as well as body language, such as the gait, gestures, and posture that are anomalous or unnatural. There may be indicators that the physical characteristics of special-identity passengers such as disabled people or pregnant women are not in the normal state. People may use actions such as rubbing the nose, touching the neck or coughing to conceal a lie, dodging, quickly moving away, touching something frequently, looking at a particular object, and other reactions that indicate nervousness.

(5) Facial expressions

Examples in this category include dull eyes; drifting eyes or looking around; avoiding eye contact with staff, frequent eye communication with others, biting lips, swallowing, or licking lips, nose and forehead sweating unusually, reddened or pale face, and unnatural facial expressions.

(6) Language

Examples include remaining silent during questioning by civil aviation security personnel; making frequent mistakes when answering questions; hesitating to answer questions or speaking slowly; providing simple or vague answers; diverting attention by giving an irrelevant answer; speaking loudly, rapidly, or at a high pitch.

(7) Partners

Examples include unusual partners; the passenger is identified as anomalous and he/she has a partner; a person who is obviously the partner of the passenger but they pretend not to know each other and make eye contact.

(8) Other indicators

Other suspicious behaviors include purchasing a passenger ticket in cash; purchasing a one-way ticket; purchasing connecting air tickets but the itinerary is inconsistent with that of regular passengers; passengers with a history of crime, drug abuse, or bad credit; having bought excess

insurance; coming in and out the airport many times; constantly observing something at the security check site; accompanied by an insider ^[18].

3. Multilayer Perceptron Based on Conjugate Gradient

3.1 Multilayer Perceptron

An artificial neural network (ANN) is a nonlinear adaptive network similar to the neural network of a human brain; an ANN is used to process complex tasks, is capable of processing large amounts of data, has strong self-learning capacity, and provides an optimal solution rapidly. ANNs are widely used for face recognition, speech recognition, and signal processing and classification problems. A multilayer perceptron (MLP) is a feed-forward neural network with at least one hidden layer. The standard model (Fig. 7) includes an input layer, hidden layer, and output layer. As long as there are a sufficient number of hidden layer neurons, a three-layer network can be used to fit any nonlinear function with good precision. The detection of abnormal behavior of passengers involves the use of many evaluation indices and complex evaluation data; therefore, the MLP is suitable for dealing with nonlinear problems and a large amount of data that has to be classified ^[20].

Fig. 7 MLP model

The layers of the MLP are fully connected, i.e., each neuron in the previous layer is linked to all neurons in the next layer. Model training is achieved by comparing the error between the expected output and the actual output, and the training process ends when the error of the training sample reaches the allowable range; otherwise, the connection weights of the network are modified by the back-propagation (BP) algorithm until the error threshold is reached.

3.2 Conjugate gradient algorithm

The ANN algorithm used in this study is a BP algorithm. The original BP algorithm uses a gradient descent method to find the optimal solution. During training, the information propagates from front to back layer by layer, while the weights in the network are adjusted by the BP of the error. The optimization direction of the algorithm is the steepest descent direction. The negative

gradient direction, which reflects the local property of the error function at a certain point, is the steepest descent direction, but not necessarily the global steepest descent direction. Therefore, the algorithm can easily fall into local minima and cannot provide a globally optimal solution; the generalization ability is also poor. The directions of the two adjacent iterations are mutually orthogonal. When the iteration point is close to the minimum point, the smaller the search step size, the slower the convergence speed is.

The conjugate gradient method uses the same first derivative information as the steepest descent method, but it has greater global convergence, faster convergence speed, smaller storage requirements, and does not need any external parameters; therefore, it is widely used to solve unconstrained optimization problems. The search direction of the conjugate gradient method at each step is not the negative direction of the gradient but a group of conjugate directions constructed by the gradient at known points. The known point's next iteration point x_{t+1} has the following form:

$$x_{t+1} = x_t + \alpha_t d_t \quad (1)$$

$$d_t = \begin{cases} -g_t, & t = 1 \\ -g_t + \beta_t d_{t-1}, & t \geq 2 \end{cases} \quad (2)$$

where $g_t = \nabla f(x_t)$, d_t is the search direction, $\alpha_t > 0$ is the search step; the selection of β_k meets the condition of conjugacy.

This weight optimization method improves the effectiveness and reliability of the algorithm. Therefore, we use the conjugate gradient method to train the MLP network to obtain good convergence performance and convergence speed of the neural network.

3.3 SMOTE algorithm

When machine learning classification methods are used with unbalanced data for training, the results tend to be biased towards majority samples because the number of minority samples is low and feature learning is not comprehensive, which will affect the classification accuracy; often, the focus of classification is whether minority samples can be identified. We use the synthetic minority oversampling technique (SMOTE), which is a very effective and widely used algorithm, to solve the problem of data imbalance. Dataset balance is achieved by adding a few synthetic samples to the data, which not only reduces overfitting but also improves the feature usage of the minority samples and improves the generalization performance of the classifier on the test set. SMOTE uses a linear interpolation method to synthesize new samples between two minority samples. The basic principle is as follows: if the sampling rate is m , for each minority sample point

X_i , we find its K minority neighbor points and choose m neighbor points $y_{ij}(j=1, 2, \dots, m)$; we then synthesize new minority samples p_j according to Eq. (2):

$$p_j = x_i + rand(0,1) \times (y_{ij} - x_i) \quad (2)$$

where Rand (0,1) represents a random number in the range of (0,1). The newly synthesized minority samples are merged into the original dataset and the training set is re-sampled, thereby improving the data imbalance.

4. Network Construction and Training

4.1 Data preprocessing

We deleted the samples that did not contain sufficient information and obtained a total of 310 valid samples. The passengers are divided into four categories according to the risk level; the safety score is 1, slight danger is 2, danger is 3, and high danger is 4. The higher the score, the higher the risk level is. We asked experts to score the characteristics of the samples and determine the final risk levels; the safety category (category 1) has 160 samples the slight danger category (category 2) has 109 samples, the danger category (category 3) has 33 samples, and the high danger category (category 4) has 8 samples. The input variables for the MLP neural network input layer are the eight features (passenger documents, baggage, etc.) in the index system and the output layers are the four risk levels.

Prior to training, the SMOTE sampling method is used to construct a new minority class sample to balance the data set. Then the data are normalized by scaling the features (e.g., x_i) in the training set from 0 to 1 using the equation $x'_i = \frac{x_i - \min(x_i)}{\max(x_i) - \min(x_i)}$. Normalization improves the convergence speed and convergence accuracy.

4.2 Network construction and training

The literature indicates that three-layer neural networks are most suitable for this study; a large number of layers will often decrease the accuracy of the model; therefore, we use a three-layer network structure with a hidden layer.

The selection of the number of nodes in the hidden layer is generally based on experience; the empirical equation is $\frac{m+n}{2} \leq l \leq \sqrt{m+n} + \alpha$, where l , m , and n are the number of nodes in the hidden layer, input layer, and output layer, respectively, and α is an integer between 1 and 10. The model accuracy with different numbers of neurons is shown in Figure 8. The accuracy is highest for 13 neurons, which is the number of neurons used in this study.

Fig. 8 The accuracy of models with different numbers of neurons

The activation function of the hidden layer is the ReLU function, which is defined in Eq. (3). When $x > 0$, the gradient is not attenuated and the convergence speed is fast.

$$f(x) = \max(0, x) \quad (3)$$

The output layer contains four neurons and the activation function is a softmax function. The expression is shown in Eq. (4), where V_i is the output of the previous layer of the classifier, i represents the index of the class, the total number of classes is C , and S_i represents the ratio of the exponent of the current element to the exponent sum of all the elements. The softmax function transforms the output values of multiple classes into the relative probability of the different classes to obtain more intuitive results.

$$S_i = \frac{e^{V_i}}{\sum_{i=1}^C e^{V_i}} \quad (4)$$

The loss function is a cross-entropy function. Cross-entropy is a concept in information theory; it describes the distance between two probability distributions, as shown in Eq. (5). It describes the difficulty of expressing the probability distribution p through the probability distribution q . p represents the original label and q represents the predicted value. The smaller the cross-entropy, the closer the two probability distributions are. The softmax function changes the output of the neural network to a probability distribution, and the distance between the predicted probability distribution and the real probability distribution is calculated using the cross-entropy function.

$$H(p, q) = -\sum_x p(x) \log q(x) \quad (5)$$

The data are divided into a training set and test at a ratio of 2: 1. The MLP is established; the input layers are the 8 features of the index system, the output layers are the 4 risk levels, including a hidden layer with 13 neurons. Batch processing is used to update the weights and to calculate the

gradient and loss value to speed up the training speed, avoid falling into a local minimum, and minimize the total error.

4.3 Results

For the ordinary gradient descent algorithm, after 1124 iterations, the final loss value is 0.43, the overall classification accuracy is 82.7%, and the classification accuracies of categories 3 and 4 are very low. For the SMOTE method, after 1053 iterations, the loss function converges, the final loss value is 0.04, and the overall classification accuracy is 91.1%; the results are shown in Table 1. It is observed that the loss value of the optimized neural network is lower and the classification accuracy is higher for the SMOTE method.

Table 1 Classification results before and after data oversampling

Label	Classification accuracy of the original data set (%)	Classification accuracy of the oversampled data set (%)
1	98	98
2	76	92
3	25	81
4	33	94
Total	82	91

The classification results of the statistical classifier are shown in the confusion matrix in Fig. 9. The horizontal and vertical directions represent the predicted classes and the real classes, respectively, and the values in the matrix represent the recall rate of the class, i.e., the proportion of correct predictions in the class. The darker the color, the higher the proportion is. The results indicate high classification accuracy.

Figure 9 Confusion matrix of the classifier

The evaluation indices of the classifier include the precision rate and recall rate. The final classification results are shown in Table 2, where the F1 value is the harmonic average of the precision rate and recall rate. If the precision rate and recall rate are high, the F1 value is high. The closer the value is to 1, the better the performance of the classifier is.

Table 2 Performance of the MLP classifier

Label	Precision	Recall	F1	Number
1	0.98	1.00	0.99	47
2	0.92	0.73	0.81	45
3	0.81	0.92	0.86	48
4	0.94	0.98	0.96	52
Weighted/total	0.91	0.91	0.91	192

5. Conclusion

In this study, an MLP based on SMOTE sampling and the conjugate gradient method is used as a classifier to evaluate the anomalous behavior of passengers at security inspection sites. The following conclusions are drawn:

(1) A comprehensive assessment index system was developed for the detection of anomalous behavior of civil aviation passengers at checkpoints. Eight indicators were used, including documents, luggage, clothing, actions, facial expression, language, partners, and other indicators. The system provides guidance to detect anomalous behavior of passengers at checkpoints and is focused on improving civil aviation security.

(2) The conjugate gradient-based MLP neural network is used to evaluate the behavior of passengers and determine the risk level to reduce uncertainty and subjectivity in the evaluation process.

(3) The classification accuracy of the risk levels of civil aviation passengers was 91.1%, indicating that this method has high application value for the identification of anomalous behavior of passengers at security checkpoints. Additional research and modifications should be performed and the applicability of the method should be evaluated in the future to improve the identification index system and risk assessment method for the detection of anomalous behavior of passengers at checkpoints.

Funding

This study is supported by The Civil Aviation University of China's 2018 Central University Fund ,Project title Research on Civil Aviation Passenger Abnormal Behavior Identification System (Project Number: 3122018F004).

Conflict of interest

The authors declare that there is no conflict of interests regarding the publication of this paper.

Ethical approval

This article does not contain any studies with human participants or animals performed by any of the authors.

Authorship contributions

Haibin Shen: contributed to the conception of the study; contributed significantly to analysis and manuscript preparation; helped perform the analysis with constructive discussions.

Yan Zhang: performed the experiment; performed the data analyses and wrote the manuscript; contributed to perform the analysis with constructive discussions.

References

- [1] Civil Aviation Administration of China. Promote the High-Quality Development of Civil Aviation Security Under and Led by the New development Concept. 2018 Aviation Security Regulatory Conference. [EB/OL]. BEIJING, 2018.
http://www.caac.gov.cn/XWZX/MHYW/201812/t20181207_193368.html
- [2] International Civil Aviation Organization, V10, Annex 17, Convention on International Civil Aviation (1-1) [Z].2017-4.
- [3] Mecocci A , Pannozzo M , Fumarola A . Automatic detection of anomalous behavioural events for advanced real-time video surveillance[C]// IEEE International Symposium on Computational Intelligence for Measurement Systems & Applications. IEEE, 2005.
- [4] Chen Y , Liang G , Ka K L , et al. Abnormal behavior detection by multi-SVM-based Bayesian network[C]. International Conference on Information Acquisition. IEEE, 2007.
- [5] Oyama A , Shah M . Abnormal crowd behavior detection using social force model[C].IEEE Conference on Computer Vision & Pattern Recognition. IEEE, 2009.
- [6] Gao Yanfei, Chen Junjie, Zhang Ning. Optimization of Surveillance Image Recognition of Civil Aviation Airport [J].Recent Patents on Computer Science,2017,4(10):270-274.

- [7] Shivali Choudhary ; Nitish Ojha ; Vrijendra Singh. Real-time crowd behavior detection using SIFT feature extraction technique in video sequences[C]. 2017 International Conference on Intelligent Computing and Control Systems (ICICCS), Madurai, India: IEEE,2017.
- [8] Zhang Bolun. Research and Design of Intelligent Monitoring System Based on Recognition of Unusual Behavior[D].Xidian University, 2007.
- [9] Xu Lingjie. Characteristics of Civil Aviation Hijacks in China and the PCC ' prevention model [J]. Social Science Research, 2009 (1): 72-79.
- [10] Rao Jing. A Brief Technical Analysis on Behavior Types of High-risk Passengers in Foreign Civil Aviation [J]. Legality Vision, 2015 (6): 52.
- [11] Wang Tian, Li Qingwu, Liu Yan, etc. Anomalous Human Body Behavior Recognition Using Pose Estimation [J]. Chinese Journal of Scientific Instrument, 2016 (10): 2366-2372.
- [12] Wu Xiaoyong, Feng Sihai, Sun Huacheng. Study on Facial Features in Deceptive Recognition [J]. Journal of Jiangsu Police Institute, 2014 (2): 104-109.
- [13] Ma Yifei. The Safety Protection Modeling in the Public Area Based on the Recognition of Anomalous BehaviourBehaviour [D]. Changchun: Jilin University, 2016.
- [14] Tang Chunming, Lu Yongwei. Pedestrian Anomalous Behavior Analysis Based on Optimized Sparse ReconstructionAlgorithm [J]. Computer Engineering and Applications, 2017, 53 (08): 165-169+185.
- [15] Shen Zheng, Wu Wei. Anomalous Crowd Behavior Detection on Bus Based on Image Processing Algorithm [J]. Computer Engineering and Design, 2018, 39 (01): 165-171.
- [16] Wei Zhaojing, Qing Linbo, Wang Zhengyong, He Xiaohai, Li Kai. An Anomalous Behavior Classification Detection Algorithm Based on Crowd Density [J]. Video Engineering, 2018, 42 (03): 97-102.
- [17] Hua Bin, Liang Xi, Liu Shang, Sheng Jiachun Renovated abnormal passenger crowd behavior detection system based on the speeding-up and squeezing in the public places[J]. Journal of Safety and Environment,2017,17(03):1043-1048.
- [18] Civil Aviation Administration of China, Guidance for Anomalous Behavior Detection on Passenger Security Checks in Civil Aviation (MD-SB-2013-006) [Z].2013.

- [19] Hornik K . Multilayer feedforward networks are universal approximators[J]. Neural Networks, 1989, 2(5):359-366.
- [20] Bishop C M . Neural Networks for Pattern Recognition[J]. 1995.
- [21] Wu Shirong, Gao Dongxu, Deng Junjun. Application of conjugate gradient BP neural network in pattern classification [J]. Telecom World, 2017(3):29-30.
- [22] Jiang Zongli, Shi Qian Yue. Classification Algorithm for Imbalanced Data Set[J]. Computer Systems & Applications, 2019(08):120-128.
- [23] Min Zeng. Effective prediction of three common diseases by combining SMOTE with Tomek links technique for imbalanced medical data[A]. IEEE Computer Society.Proceedings of 2016 IEEE International Conference of Online Analysis and Computing Science(ICOACS 2016)[C].IEEE Computer Society:IEEE BEIJING SECTION, 2016:4.