# International Journal of Civil Engineering and Machinery Manufacture

**Volume 5, Issue 2, June, 2020**


Publisher: HongKong New Century Cultural Publishing House
Address: Unit A1, 7/F, Cheuk Nang Plaza, 250 Hennessy Road, Wanchai, Hong Kong
Tel: 00852-28150191
Fax: 00852-25445670

# Contents

# The Application of Artificial Intelligence Method in 5G Network Automatic Identification

Jing Xia
The Research Institute of Informatization and Industrialization Integration, China Academy of Information and Communications Technology, Beijing, 200001, China

**Abstract:** Due to the inaccuracy of local identification results of traditional 5g network identification method, the recognition accuracy is low. Therefore, an automatic identification method based on artificial intelligence for 5g network identification is proposed. Combined with the principle of convolution layer, we collect the identity characteristics of 5g network users, extract the identity behavior characteristics of network users through the activation curve, use windowing method to process the user behavior characteristics, and verify the identity according to the processing results, and use artificial intelligence method to complete the automatic identification of 5g network identity. Experimental results show that the proposed method can accurately identify local identity features and improve the recognition accuracy.

**Keywords:** Artificial intelligence; 5G network; Identity recognition

## 1. Introduction

With the development of society and the progress of science and technology, there is an urgent need for fast and effective automatic authentication system. Biometrics is the internal attribute of human beings, which has strong self stability and individual difference. Therefore, biometrics is the ideal basis of authentication system. Compared with the above system's biometrics, network identity recognition has the characteristics of direct, friendly, convenient and easy to be accepted by users [1]. One of the important reasons for the importance of network identity automatic identification is that it has great potential application value in the fields of economy, security, social security, crime, military and so on, especially in the occasions where user identity needs to be verified or identified. Because the automatic identification of network identity is a non rigid body with great changes, it is a complex, widely involved and widely applied research topic [2]. In recent years, there has been a research upsurge of automatic identification at home and abroad, and a breakthrough has been made. This paper first studies the history and status quo of automatic identification technology and the main methods of identification, and then proposes an identification technology based on wavelet transform, principal component analysis and artificial neural network, which has the advantages of no damage to the user and easy to hide because of its non contact data collection method without too much user participation Look good [3]. The research and solution of network identity recognition is helpful to the research and analysis of other object recognition problems. Therefore, network identity recognition has become one of the important topics in these basic research fields, which has important theoretical research value. Based on the basic theories and key technologies of identity detection and recognition, this paper focuses on the issues of network user identity enhancement, feature extraction, feature recognition method based on multi classifier combination, feature recognition fusion method, multi-agent structure model of 3D feature recognition, etc [4]. Aiming at the main difficulties of network identity detection algorithm, a new method to enhance the accuracy of network identity recognition is proposed.

## 2. Automatic Identification Method based on Artificial Intelligence

### 2.1. 5g network identity feature collection

Network identity feature collection technology is a kind of technology that extracts the identity features of users through computers and verifies them according to these features. The uniqueness of network identity features and the good characteristics that are not easy to be copied provide the necessary premise for identity authentication [5]. Compared with other mature user biometric identification methods, network identity features are easier to obtain, especially in the non-contact environment and the situation of not disturbing the detected users, the advantages of network identity recognition are far more than other identification technologies. Com-

pared with other feature recognition technologies, feature recognition technology has the advantages of simple operation, intuitive results and good concealment [6]. Therefore, feature recognition has a wide range of application prospects in information security, criminal detection, access control and other fields. Therefore, combining artificial intelligence technology to analyze the user's network login status attributes, and randomly build a feature function detection model, which can quickly collect and identify the identity features under the condition of signal interference, fully combining the fuzzy neural theory and network structure [7]. For the feature data with discrete type, the fuzzy rule reasoning ability is used to provide technical support for the dynamic identification of network identity. Three feature analysis models are used to represent the features of each pixel in the digital network user identity [8]. When the new frame number network user identity features are obtained, the pixel points and the feature analysis model are matched to judge the background points and the former scenic spots of the dynamic user login digital network user identity. In the feature analysis model, observe the likelihood of the dynamic information of a network user's feature:

$$P = \sum_{n=1}^{m} \mathrm{a}_i \, f_i(n) / 2m \tag{1}$$

In the formula, M is the number of dynamic collected information; AI is the weight of user information component I; fi (n) is a one-dimensional feature analysis model function. The dynamic behavior of different users can be analyzed accurately by using the formula. Design a N-group subgraph module, and obtain n estimated values by combining with the filtering. Generally, these values are not coincident. In a certain sense, a single subgraph module has more or less relationship with the filtering [9]. The steps of combining the three-dimensional information similar to the drawing field and ground module are as follows: the first step is to carry out the linear change of the information group The second step is to get the reduced noise through the shrinkage conversion, and the third step is to get the estimated data of each sub graph module through the reversible linear conversion, so as to achieve the low-frequency range of noise reduction [10]. Use the above to establish low frequency values, which are recorded as qj and other corresponding viewpoints qj1, qj2 The radius and the number of rings of the high-dimensional curvature network user identity are determined by the density of the samples [11]. In addition, the high-dimensional curvature network user identity of qj and qj1, qj2 , the distance between user identities of qjk's high dimensional curvature network is compared according to the following formula. The specific algorithm can be recorded as:

$$x = \prod P^{*} g / \mathrm{q}_{\mathrm{j}} \prod \sqrt{\left(\frac{1}{n+z}\right) \sum_{j=1}^{n} \mathrm{u}\left[L-K\right]^{2}} \tag{2}$$

In the above formula, l is the dimension of 3D drawing site attributes, K is the number of high-dimensional curvature network user identity groups of Z point, and u is the high-dimensional curvature network user identity groups of G point [12]. Based on the above algorithm, different network identity features are further searched and collected, and the corresponding continuous network graph structure of user feature mining item group is established, as follows:

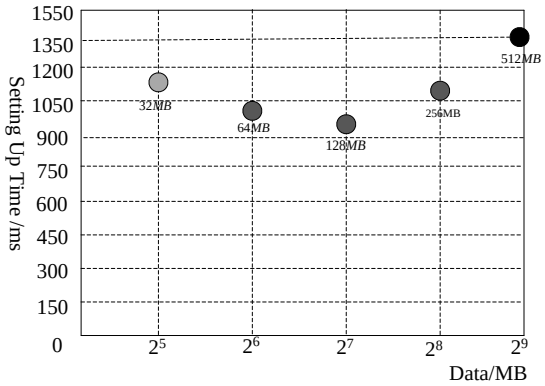



**Figure 1. User feature mining item group continuous network**

Based on the above figure, further establish and standardize the duration of search terms, improve the performance of search terms, so as to better calculate the service background running time, improve the ability of data search, and get good search results [13]. Furthermore, the feature analysis model can be used to judge the likelihood degree of user login information, and on this basis, the dynamic identification of user login digital network can be realized. The tracking user's login digital network user identity is decomposed into three small network user identities [14]. The track moving point sequence, hand shape change sequence and distance sequence between finger and center position in the network user identity are analyzed respectively, and the above feature analysis model is input to judge the likelihood. Taking likelihood as fuzzy membership degree, the fuzzy processing of recognition results is completed, and the sum product reasoning method is used to realize the dynamic collection of user's identity in the digital network. The basic framework of dynamic collection of user identity is shown in the figure.

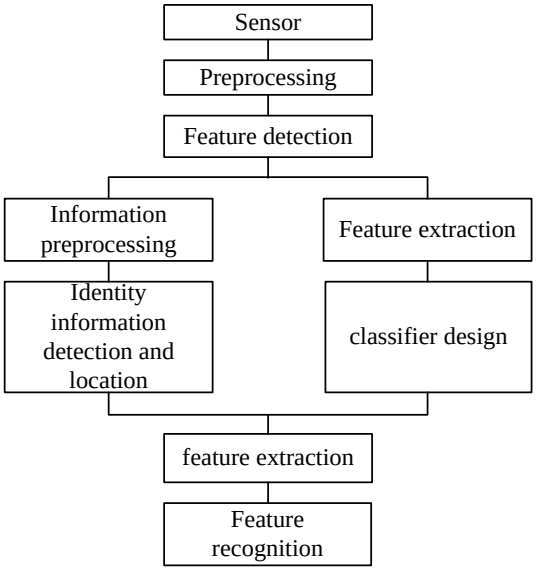



**Figure 2. User identity feature collection steps**

In the user identity feature acquisition step, the network user identity is captured by the sensor such as CCD camera, and then the quality of the network user identity is improved by preprocessing, and then the user identity is located according to the user identity feature detection, and the network user identity is set to the predefined size. the feature extraction is used to extract the effective features to reduce the dimension of the original pattern space, and the classifier is based on the features Make decision classification. Feature recognition also plays a very important role in the research of biometrics and human-computer interaction [15]. The common goal of human-computer interaction is to improve the way of human-computer interaction by studying the input-output technology and the human factors involved in the interaction. In order to make the interface more natural and in line with people's intuitive feelings, people require machines to acquire human skills such as identity recognition, user login and human activities, rather than continue to require people to acquire the same skills as machines. Feature recognition is a typical pattern recognition problem, and the research of biometrics and its solutions help us to solve other related problems in this field.

### 2.2. Network identity feature detection

Based on the above feature collection results, further detection of identity feature information is carried out. According to the characteristics of user's identity, the biometric technology of automatic identification has the characteristics of superior, universal and non-contact operation. Feature recognition technology includes identity detection, identity confirmation and identity identification. Identity detection realizes the automatic collection of the identity of the network user of the withdrawer, and automatically extracts the identity of the network user of the withdrawer's face from the identity of the network user photographed by the pinhole camera, so as to confirm the identity attribute of the withdrawer, realize the positioning of each key point of the identity, effectively separate each component, and further realize the feature extraction of the identity. Identity confirmation is a one-to-one comparison between the identity of the network user of the withdrawal identity department and the identity of the network user in the database, and it can judge whether they are the same person according to their similarity. Identity authentication is to compare the identity of the network user of the withdrawal identity department with the identity of the network user in the database in one to many ways, and identify the identity of the withdrawer according to the comparison results, or find the most similar identity, and output the retrieval results according to the size of the similarity degree. In this paper, a pyramid recognition method based on the extraction of identity features is proposed. By using this method and sub pattern, the identity can be identified efficiently. The flow chart of user authentication is shown in the figure below.

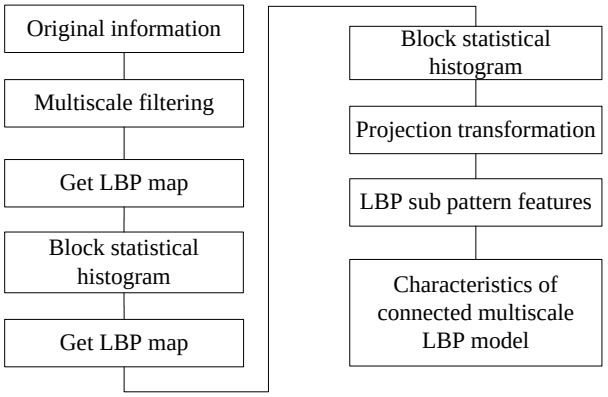



**Figure 3. User authentication flow chart**

The specific extraction steps of sub pattern features can be obtained from the graph:

A. Select the filter with strong desiccation effect to filter and decompose the network user identity carefully, remove the redundant impurities, and then build the low-dimensional network user identity with multi-scale space;

B. Operators are used to calculate the dimension of users' identities in different scales, so as to obtain the feature spectrum data;

C. By dividing the different feature spectrum, we can get the module area with non repetition attribute and count the histogram data in the area;

D. The sub module features of different regions can be obtained by mapping the operator rectangles of different regions with projection method;
E. By splicing the sub module features of all regions, multi-scale sub module sequences can be obtained, and the identity can be identified with this feature vector.
In the process of constructing feature recognition and feature values, we need to choose the number of network user identities and the size of decomposition area according to the actual situation of different people. The most common method combined with feature attribute extraction algorithm is network user identity attribute extraction algorithm. Based on the above algorithm, the quantitative feature histogram of remote sensing network user identity is further standardized. Without affecting the detected network user identity features, the induced changes of the identified network user identity features and their influence degree, projection interference and component jitter are de noised. In the process of network user identity recognition, it is necessary to display the surrounding information through the quantitative histogram of network user identity. Combined with the principle of convolution layer, the characteristic attributes of network user identity are collected, and a convolution kernel of 3 * 3 is established to convolute the 5 * 5 network user identity, which can effectively reduce the resolution frequency of attribute network user identity and reduce its sensitivity to displacement change. Combined with offset transfer, the required behavior characteristics of network user identity are obtained through activation curve. Specific principle:

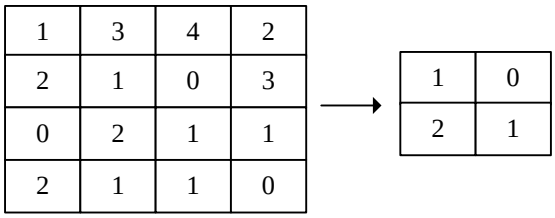



**Figure 4. Principle of identity information feature transfer**

Furthermore, the data information of network user's identity collected and uploaded after landslide disaster is calculated by combining Internet code programming technology, video broadcasting technology, information base analysis and processing technology, and DSP embedded technology to complete the actual scene of network user's identity display and corresponding switching. In order to obtain the identity features accurately, it is necessary to analyze the whole network user identity, both the modules and some areas in detail, so as to extract the important features. The digital sequence of histogram can be obtained by using the distribution mode of network user identity pyramid. After projection transformation, the identity features can be extracted, which are called multi-scale sub pattern features. When the feature spectrum in the network structure is divided, there will be detection areas with different overlapping attributes. These areas can be characterized by different local features in the form of histograms, and the features can be displayed in the form of histograms. The areas with higher dimensions can be classified and dimensioned down, thus the features of each sub module can be obtained. The multi-scale network user identity can be obtained by combining the characteristics of all the sub modules of identity network user identity. The network user identity is used as the feature vector to describe the identity characteristics of the whole identity network user. In order to verify the rationality of the design of the feature recognition technology based on, we use the data in the standard identity database to verify the rationality of the technology. From the identity database, 40 detection values of network user's identity areas are selected, including expression change, posture change and angle change. The size of network user's identity is 90 × 110. Each one, three and five network user identities of these 40 people are taken as the training samples, and the remaining network user identities are taken as the samples for experimental test. The traditional identification technology is compared with the identification technology in this paper, and the network identification information base is established, as shown in Table 1.

**Table 1. Network identity information base**

| | Parameter | Expression change | Postural change | Angle change |
|---|---|---|---|---|
| 1 Training Sample | Recognition rate | 0.72 | 0.81 | 0.92 |
| | Feature dimension | 388 | 596 | 752 |
| 3 Training Sample | Recognition rate | 0.81 | 0.94 | 1.24 |
| | Feature dimension | 488 | 708 | 904 |
| 5 Training Sample | Recognition rate | 0.89 | 0.99 | 1.05 |
| | Feature dimension | 1400 | 2718 | 3541 |

Based on the information in the above table, it can provide a reference for the user's network identity recognition, so as to better guarantee the effect of identity recognition.

### 2.3. The realization of automatic identification of network identity

The windowing method is used to denoise the user's behavior characteristics and remove the interference of signal projection. The sensor data is extracted from the rectangular window, and the feature vector is constructed to represent the user's behavior, and the corres-

ponding standard deviation is established. Among them, the standard deviation is one of the statistical characteristics, which effectively reflects the discrete degree of sensor data. As people are in the state of static behavior, the acceleration data is basically unchanged, while the standard value is 0, while people's acceleration data constantly changes in the process of movement, and the standard value is greater than 0. The specific calculation formula is:

$$a=\bigcap \lim_{x\to\infty} x\sqrt{\frac{1}{S}\sum_{i=1}^{S}\left(A_i-1\right)^2} \tag{3}$$

Where s is the number of samples; a is the average value of samples. According to formula (3), the static and dynamic behaviors of users can be distinguished. Further, the identification skewness is calculated, which can measure the skew direction of the acceleration sensor data distribution, analyze the gravity direction schematic diagram, and identify the user's behavior according to the coordinate axis skewness. The specific calculation formula is as follows:

$$P=\frac{S\sum_{i=1}^{s}\left(A_i-x\right)^3}{(S-1)(S-2)a^3} \tag{4}$$

According to the formula skewness, the user network behavior can be distinguished effectively. It is an important statistical feature to calculate the peak time of user's network login. The peak change curve can directly reflect the change degree of all signals at the peak of the data curve. The specific calculation formula is as follows:

$$Q=\frac{\sum_{i=1}^{s}\left(A_i-x\right)^4 n_i}{Sa^4} \tag{5}$$

Where: Ni is the sample interval. This formula can effectively distinguish user behavior actions. The correlation coefficient can be used to measure the linear correlation between variables. The specific calculation formula is as follows:

$$W_{AB}=\frac{\sum_{i=1}^{s}A_i\left(B_i-\overline{B}\right)}{\sqrt{\sum_{i=1}^{s}\left(A_i-1\right)^2}\sqrt{\sum_{i=1}^{s}\left(B_i-\overline{B}\right)^2}} \tag{6}$$

Where a and B represent the variable of correlation coefficient respectively. According to the formula and the correlation coefficient of gravity YZ, the user behavior can be effectively distinguished. Under the occlusion condition, the skewness can measure the skewness of acceleration data distribution, so as to analyze the gravity direction diagram, and distinguish the user's forward and backward behaviors according to different axis skewness. The specific calculation formula is as follows:

$$T=\frac{n\sum_{i=1}^{s}\left(z_i-\overline{z}\right)^3}{(n-1)(n-2)d^3} \tag{7}$$

Where, represents the number of samples; $\overline{z}$ represents the average value of samples; D represents the standard deviation. The formula for standard deviation is as follows:

$$k=\sqrt{\frac{1}{n}\sum_{i=1}^{n}\left(z_i-\overline{z}\right)^2} \tag{8}$$

Based on the above algorithm, after coordinating the detection of different characteristic units of network identity, the dynamic coordination in the process of completing the task of network identity recognition is further carried out. Five agents with different functions are constructed to complete different identification processes. Each agent completes its own task. After making the identification result of "yes" or "no" locally, the result is submitted for judgment and the overall identification result is made through the final decision. According to the above multi-path discrimination, the user local feature recognition path is optimized, and the specific recognition process is shown in the figure.

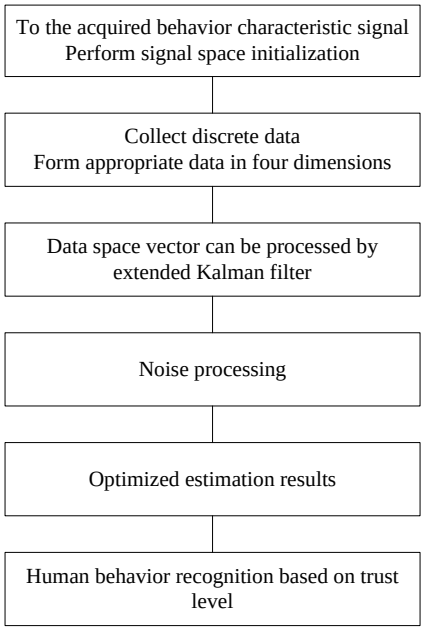



**Figure 5. Local feature recognition process**

According to the identification process shown in Figure 4, the trust level of each component in the data space can be set, and each level can be de dried to obtain the optimal feature data, and the user behavior can be identified under the component trust level. The camera collects the identity of the network user, the fingerprint reader reads the fingerprint information, and transmits it

to the In DSP, firstly, DSP detects the identity of the incoming network user, and checks whether there is identity, fingerprint network user identity and identity card information. If there is, it divides the identity, fingerprint and main feature information of the ID card of the withdrawer and extracts the feature. The extracted identity, fingerprint and identity card feature information is compared with the information in the database to determine the similarity If the similarity is greater than the specified threshold, the identification is successful. Otherwise, the identification fails and the identity, fingerprint and ID card network user identity of the withdrawer are recorded and compared with the network user identity of the criminal in the database. If there is a network user identity matching with it, it is reported to the police. The specific principle of network identity verification and recognition is shown in the following figure:

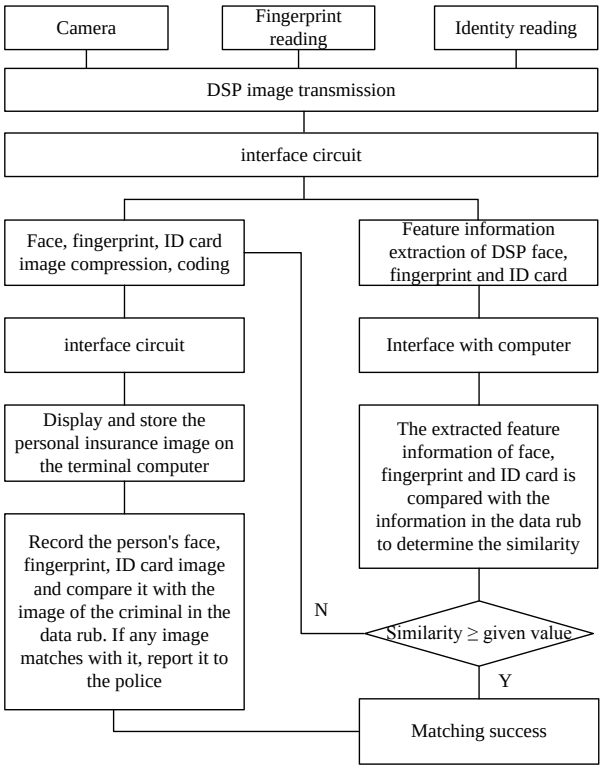



**Figure 6. Steps of automatic identification of user identity**

Based on the above steps, it can effectively realize the automatic identification of the artificial intelligence method in 5g network, improve the identification accuracy, simplify the identification process, reduce the identification time, and improve the overall operation efficiency.

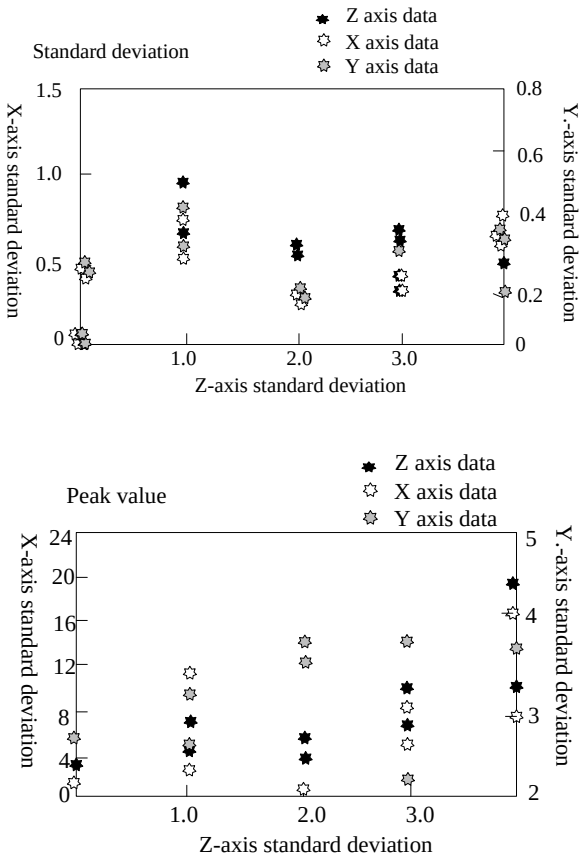
## 3. Analysis of Experimental Results

In order to verify the actual application effect of artificial intelligence method in 5g network identity automatic recognition for comparative detection, in order to guarantee the experimental detection effect, first set the experimental environment and parameters uniformly, and the specific experimental detection information is shown in the table below:

**Table 2. Experimental parameter settings**

| Parameter | Index |
|---|---|
| CPU | Intel Core |
| Processor | 64 |
| Graphics card | NAIDIA |
| Built-in | USB3.0 Bus |
| OS | WIN8.1 |

Based on the above experimental environment, further discrete processing is carried out for the collected user local feature information in 5g network environment, respectively detecting and judging the data standard deviation, skewness, peak value and correlation coefficient of user behavior, as shown in the figure below.



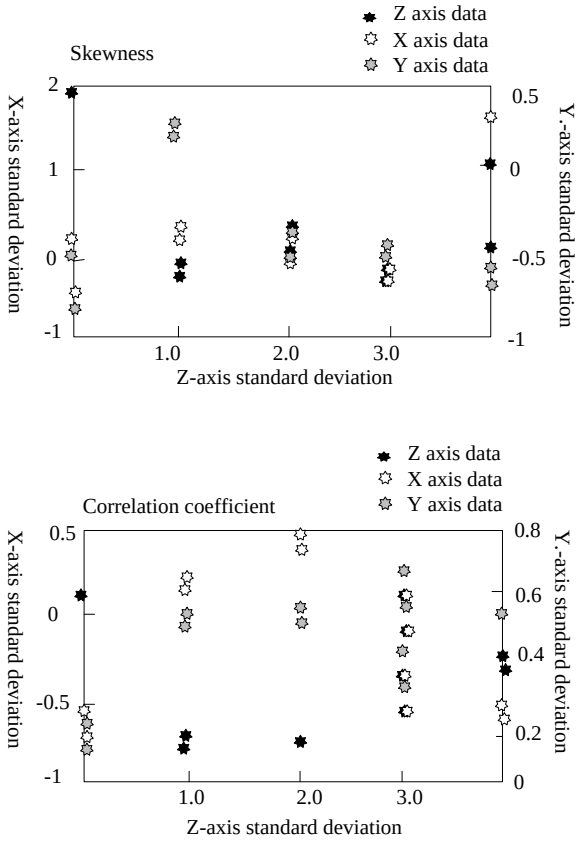



**Figure 7. Local identification results**

Based on the above detection results, further compare the recognition accuracy of the traditional method and the recognition method in this paper, and record the detection results, as shown in the following figure.

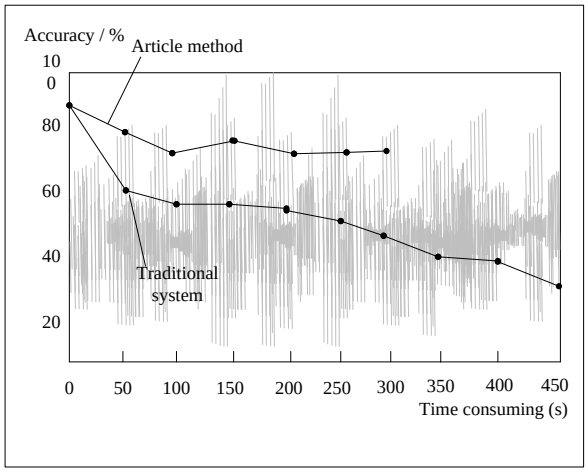



**Figure 8. Comparison test results**

Observing Fig. 6 and Fig. 7 for analysis, it can be found that compared with the traditional method, the proposed artificial intelligence method in 5g network identity automatic recognition has higher accuracy, less time-consuming and higher practicability and effectiveness. Fully meet the research requirements.

## 4. Concluding Remarks

In order to better realize the accurate identification of network identity users, a method of industrial intelligence in 5g network identity automatic identification is proposed. The physical interaction and field description method are introduced into the abstract domain space. The identity features are represented by data field, and the data are self-organized and clustered by the interaction and movement of data, so as to realize the nonlinear transformation In this way, the dimension of identity data can be reduced and the sample database of data field sorted by the most potential function can be established. Based on the improved evidence theory of feature recognition, the identity is fused to get accurate user identity. The experimental results show that the method can automatically identify the user's identity, and the efficiency and speed of identification are effectively improved. In the next step, we will consider how to build a large sample database automatically, and test the algorithm recognition rate and recognition time under the condition of large sample database, so as to improve the time efficiency of automatic dimensionality reduction.

## References

[1] Victor Henrique Alves Ribeiro, Gilberto Reynoso Meza, Leandro dos Santos Coelho. Comparison of different classifiers for automatic target recognition systems. IEEE Latin America Transactions. 2018, 16(1), 13-18.

[2] Ke Xiao, Liang Gong, Michel Kadoch. Opportunistic multicast NOMA with security concerns in a 5G massive MIMO system. IEEE Communications Magazine. 2018, 56(3), 91-95.

[3] Tadas Rimavičius, Adas Gelžinis, Antanas Verikas, et al. Automatic benthic imagery recognition using a hierarchical two-stage approach. Signal Image and Video Processing. 2018, 12(11), 1-8.

[4] Lee Shengchieh, Wang Jhingfa, Chen Miaohia. Threshold-based noise detection and reduction for automatic speech recognition system in human-robot interactions. Sensors. 2018, 18(7), 2068.

[5] Raja J., Gunasekaran K., Pitchai R. Prognostic evaluation of multimodal biometric traits recognition based human face, finger print and iris images using ensembled SVM classifier. Cluster Computing. 2019, 22(1), 1-14.

[6] Dai Yueyue, Xu Du, Maharjan Sabita, et al. Blockchain and deep reinforcement learning empowered intelligent 5G beyond. IEEE Network. 2019, 33(3), 10-17.

[7] Petya Puncheva-Michelotti, Sarah Hudson, Marco Michelotti. The role of proximity to local and global citizens in stakeholders' moral recognition of corporate social responsibility. Journal of Business Research. 2018, 88(8), 234-244.

[8] Matsangidou Maria, Otterbacher Jahna, Ang Cheesiang, et al. Can the crowd tell how I feel? Trait empathy and ethnic background in a visual pain judgment task. Universal Access in the Information Society. 2018, 36(4), 1-13.

[9] Ahmed Murkaz, Riaz Hussain, Junaid Ahmed, et al. An intra–inter-cell device-to-device communication scheme to enhance 5G network throughput with delay modeling. Telecommunication Systems. 2018, 69(4), 461-475.

[10] Adel A Ahmed, Abdullah Ahmad. A comprehensive survey on handover management for vehicular ad hoc network based on 5G mobile networks technology. Transactions on Emerging Telecommunications Technologies. 2018, 30(5), 1-19.

[11] Mudassar Ali, Saad Qaisar, Muhammad Naeem, et al. Resource allocation for licensed and unlicensed spectrum in 5G heterogeneous networks. Transactions on Emerging Telecommunications Technologies. 2018, 29(6), e3299.

[12] Qi Yan, Wei Chen, Vincent Poor. Big data driven wireless communications: a human-in-the-loop pushing technique for 5G systems. IEEE Wireless Communications. 2018, 25(1), 64-69.

[13] Chen Min, Qian Yongfeng, Hao Yixue, et al. Data-driven computing and caching in 5G networks: architecture and delay analysis. IEEE Wireless Communications. 2018, 25(1), 70-75.

[14] Trung Kien Vu, Mehdi Bennis, Merouane Debbah, et al. Ultra-reliable communication in 5G mm wave networks: a risk-sensitive approach. IEEE Communications Letters. 2018, 22(4), 1-4.

[15] Lorenzo Fernandez Maimo, Angel Luis Perales Gomez, Felix J. Garcia Clemente, et al. A self-adaptive deep learning-based system for anomaly detection in 5G networks. IEEE Access. 2018, 6(99), 7700-7712.