EURASIP Journal on Wireless Communications and Networking

RESEARCH Open Access

Electromagnetic radiation-based IC device identification and verification using deep learning

Hong-xin Zhang[1,2], Jia Liu[1*], Jun Xu[3], Fan Zhang[4], Xiao-tong Cui[1] and Shao-fei Sun[1]

* Correspondence: 390147588@qq.com
[1]College of Electronic and Information Engineering, Beijing University of Posts and Telecommunications, Beijing 100876, China
Full list of author information is available at the end of the article

Abstract

The electromagnetic radiation of electronic equipment carries information and can cause information leakage, which poses a serious threat to the security system; especially the information leakage caused by encryption or other important equipment will have more serious consequences. In the past decade or so, the attack technology and means for the physical layer have developed rapidly. And system designers have no effective method for this situation to eliminate or defend against threats with an absolute level of security. In recent years, device identification has been developed and improved as a physical-level technology to improve the security of integrated circuit (IC)-based multifactor authentication systems. Device identification tasks (including device identification and verification) are accomplished by monitoring and exploiting the characteristics of the IC's unintentional electromagnetic radiation, without requiring any modification and process to hardware devices, thereby providing versatility and adapting existing hardware devices. Device identification based on deep residual networks and radio frequency is a technology applicable to the physical layer, which can improve the security of integrated circuit (IC)-based multifactor authentication systems. Device identification tasks (identification and verification) are accomplished by passively monitoring and utilizing the inherent properties of IC unintended RF transmissions without requiring any modifications to the analysis equipment. After the device performs a series of operations, the device is classified and identified using a deep residual neural network. The gradient descent method is used to adjust the network parameters, the batch training method is used to speed up the parameter tuning speed, the parameter regularization is used to improve the generalization, and finally, the Softmax classifier is used for classification. In the end, 28 chips of 4 models can be accurately identified into 4 categories, then the individual chips in each category can be identified, and finally 28 chips can be accurately identified, and the verification accuracy reached 100%. Therefore, the identification of radio frequency equipment based on deep residual network is very suitable as a countermeasure for implementing the device cloning technology and is expected to be related to various security issues.

Keywords: Radio frequency identification, Electromagnetic Radiation, Security, Deep learning, Res-net

1 Introduction

In recent years, the physical attack methods for security systems have developed rapidly, making it increasingly difficult for new countermeasures and security measures to keep up with the development [1]. Compared to the mathematical cryptanalysis attacks, implementation attacks present a serious and immediate threat because the strength of the underlying algorithms and protocols is largely irrelevant. The means of attack can be implemented with complex techniques of expensive and highly specialized equipment (such as laser tomography or focused ion beam operation), and also may be implemented with extremely simple and low-cost equipment(such as unintentional information leakage method) [2].

Academic and commercial research organizations are dedicated to studying the physical security of encryption and other security devices. These works focused on the following directions over the past decade: side-channel analysis and failure analysis [3]. Given that many implementation attacks are well within the reach of even modestly funded and minimally equipped individuals, they should be given serious practical consideration when designing modern systems. Cautiously designed methods are (1) assuming that security tokens or other basic system components are affected by forgery, cloning or sensitive data extraction, and (2) taking appropriate solutions to mitigate the associated risks and treating them as an integrated, multi-layered part of the system security architecture.

Machine learning and electromagnetic radiation-based device identification technology enhances existing multifactor authentication schemes for cloning and related threats by authenticating at the physical level of the device. This technique is based on the slight difference in electromagnetic radiation caused by the slight difference in the physical properties. Only accidental electromagnetic leakage of integrated circuits is considered here [4].

Because the technology takes advantage of the inherent properties of the device, it is suitable for security applications involving commercial ICs without requiring changes to any physical device. In addition, preliminary results indicate that the technology can be adapted to existing processes and protocols and is likely to be applicable to a variety of IC devices, for example, general purpose microcontrollers, programmable logic devices, FPGAs, and custom ASICs.

2 Problem description

This work evaluated the applicability of device identification based on deep residual networks (deep learning network) and RF for two distinct but closely related device identification tasks: identification and verification.

(1) Device identification [4]. The identification system uses the SoftMax classifier to identify the corresponding feature map through the device information.
(2) Device verification. The identification system uses a one-to-one comparison to check the authenticity of the device's claimed identity (through the presented digital certificate). As with biometric authentication, the purpose of physical layer device authentication is to prevent two devices from using the same identity [4].

Previous identification efforts have focused on one-to-many identification tasks in wireless network security environments, where a device entering a network needs to be verified as belonging to a pool of authorized devices [4]. However, detecting cloned security tokens (such as smart card-based ID cards or payment devices) requires one-to-one verification. Here, the suitability this paper uses the depth residual network to extract the features assessed for both identification and verification tasks.

3 Physical layer equipment certification system design

This section describes the system design for applying the device identification method based on deep residual network and radio frequency to the above device identification and verification problems [5]. The basic design consists of four modules:

(1) Sensor module. The sensor module is used to collect unintended RF emissions and consists of an oscilloscope and a near-field probe. Used to obtain experimental data.
(2) Deep residual network classification training module. Classify the experimental data and adjust the network parameters.
(3) Feature image visualization module. Extracting the original signals through the residual network and using them to draw a two-dimensional image can help us understand the classification basis of the network.
(4) Verification module. For the identification task, the signal extracted from the device is sent to the network model for identification to verify its identity.

The process framework is shown in Fig. 1.

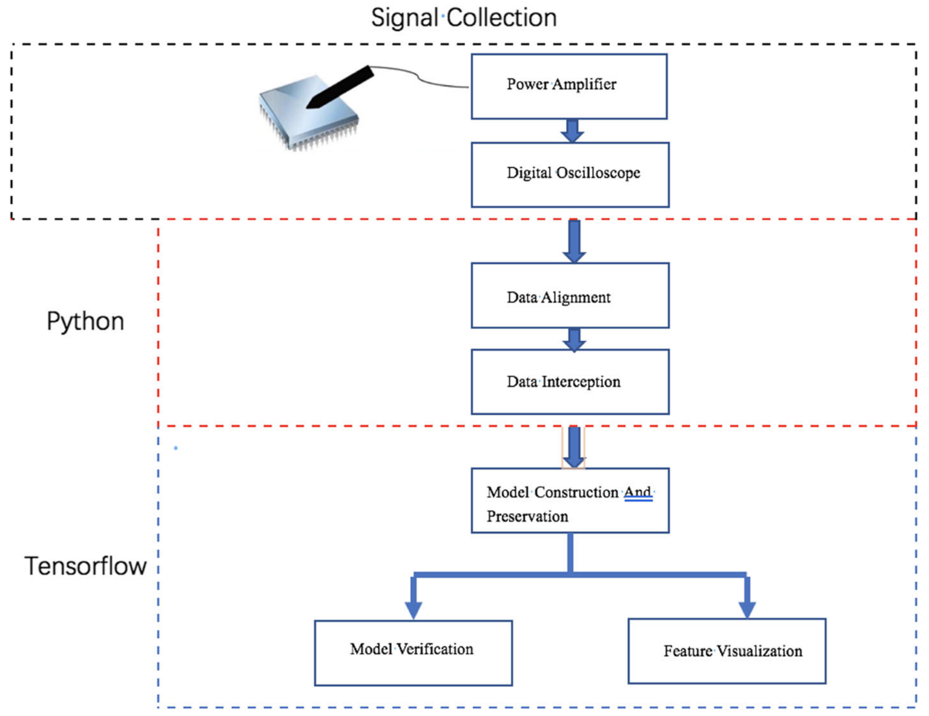


Fig. 1 Certification system process framework

4 Unintentional RF emissions of ICs

It is well known that electronic devices radiate electromagnetic energy (EM) that can interfere with nearby devices. It is for this reason that airline passengers are required to "turn off all portable electronic devices" and consumer electronic products are required to pass certification tests to meet the requirements of the Federal Communications Commission (FCC) [6] or other regulatory standards [4]. Digital devices, including high-frequency clocks and oscillators, are clearly defined as unintentional radiation and require rigorous testing to ensure emissions do not exceed specified levels [4].

Due to the clock distribution, transistor switches, and other integrated circuit activities, currents through the device produce electromagnetic fields that are combined by complex interactions that propagate in the form of time-varying electromagnetic waves through radiation and conduction. The basic properties of these effects are well understood and described by Maxwell's equations.

Most modern integrated circuits, including general purpose microprocessors, are based on complementary metal oxide semiconductor (CMOS) transistor technology. Dynamic power consumption is caused by the internal switching activity of each transistor. Since the switching activity depends on the operations performed and data manipulated, the resulting variations in dynamic power consumption are a source of side-channel information leakage.

At any time, the sum of the current by all logic cells is the total current. Charging and discharging phenomena occur when the transistor is turned on and off. Figure 2 illustrates the principle using a simple CMOS inverter. When the input transitions from 1 to 0, M1 is switched off and M2 is switched on. The cell draws a charging current from a constant voltage power supply to charge the intrinsic and extrinsic capacitances. When the input transitions from 0 to 1, M1 is switched on and M2 is switched off, and the stored energy is discharged through the ground line. Dynamic power consumption changes include state information inside the device.

Over the past decade, more and more people have realized that radiation is not only a source of interference, but also contains useful information about the internal state of the radiation-generating device [7]. This has a profound impact on the physical security of sensitive electronic systems, because in many cases, the state information of leaking is sufficient to infer the exact details of the operation being performed by the device and/or the data it is processing [8, 9]. Recently, in the study, in addition to data- and

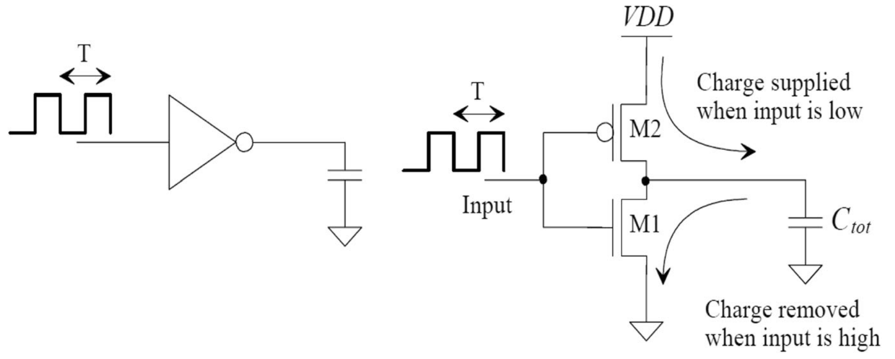


Fig. 2 Dynamic power dissipation of the CMOS inverter

operation-related characteristics, unintentional near-field RF radiation of individual ICs also showed significant device-related characteristics [10].

The most likely source of different leakage between devices is the random process variation introduced during mold manufacturing and packaging [11]. Although the integrated circuit manufacturing process must be accurate, the final device, in a very small range, will still have structural changes (deep sub-micron of modern integrated circuit technology) [4]. As a result, no two chips are exactly the same. As long as the change in the induction process is within acceptable limits, the device will operate correctly from the perspective of the black box function.

The hypothesis of this study is that changes in the manufacturing process of each microcontroller can cause different radiation, and the difference is sufficient to identify the source of radiation [4]. Although this article only studies radiation, the methods used are considered to be applicable to other aspects of channel radiation, such as changes in device power consumption. This method identifies devices with small differences, so it is mainly applied in security.

In order to improve the security of electronic systems, researchers have proposed various methods to take advantage of the changes caused by the little difference between devices. Various methods will be mentioned in Section 5. The method proposed in this paper can identify each individual and improve the security of electronic systems in certain fields, for example, prevent device clone and Trojan and so on. And this method does not need to add other parts, it just uses electromagnetic radiation to complete the accurate memory of each chip.

5 Related research

In order to improve the security of electronic systems, researchers have proposed various methods to take advantage of the changes caused by the slight gap between devices. The aforementioned physical layer device identification technologies include the following: physical unclonable functions (PUFs) [12], RF Certificates of Authenticity (RF-COAs) [13], development of wireless networks with unique radiation information and wireless-based identified devices (i.e., RF fingerprinting) [14].

(1) Physical unclonable functions (PUFs). PUF technology refers to two different methods of device authentication. The first is to add an internal measurement circuit to the integrated circuit that calculates the calculation of the individual function based on the number of failure statistics, propagation delay, or other characteristics that vary with the internal process variations of the electronic device [15]. The second method is to combine a capacitive sensor grid integrated in the top metal layer of the IC with a coating of randomly distributed dielectric particles on top of the IC passivation layer. Conformal coatings require active activation (i.e., application of a specified voltage with a known amplitude and frequency) and response from an internal measurement circuit [16].

(2) RF Certificates of Authenticity (RF-COA). RF-COA technology attaches a three-dimensional randomly shaped conductive or dielectric object to an RFID (radio frequency identification) device. This is similar to a PUF coating performed by an external RFID reader in addition to testing and responding to the rest of the measurements. The RFID reading device includes a dense patch antenna matrix for

transmitting and receiving high-frequency radio frequency signals. The device accesses the RFID and extracts fingerprints to calculate its authenticity [4].

(3) RF-DNA identification technology. Radio frequency DNA identification technology as a physical layer technology enhances the security of various wireless communication devices [4]. Based on filtering, truncation, feature extraction method, and traditional neural network are used for classification and identification in reference [17]. This paper optimizes the recognition algorithm and uses the deep learning algorithm to replace the traditional machine learning algorithm, which improves the accuracy of device recognition.

Compared to PUF and RF-COA technologies, RF-DNA and deep residual network and RF-based device identification technology do not require any modifications to the internal circuitry or external coating of existing electronic devices and are suitable for any commodity integrated circuit. In addition, the measurement for the device is done passively and does not require the device to be equipped with transmitters. Compared with reference [4], the advantage of this article is that it does not need filtering and feature extraction operations to simplify the human operation process and replace the recognition algorithm to increase the accuracy to 100%.

6 Experiment method

All results were obtained by analyzing data from a given number of test devices. The experimental setup and analysis methods used herein are given below.

6.1 Experimental setup

All the processes in the experiment were carried out in office environment. A total of 28 chips of the same model were evaluated. These chips were from 4 different batches, and there are several unique chips per batch. The distribution is shown in Table 1. The conscious choice of models provides varying degrees of similarity, with chips from each model coming from the same manufacturing batch of "EP4CE10E22C8N."

For device control and measurement, the chip is mounted on the evaluation board of the same replaceable chip and the same programming is performed to produce the same operation. Use custom fixtures to secure the board to the measurement stage to minimize any movement during collection or replacement of the chip and use standard laboratory DC power to reduce the effects of uncontrolled voltage fluctuations.

The amplitude response of the unintentional RF signal captured from some of the chips is shown in Fig. 3 (Take one chip for each batch and the order from top to bottom is A1637A, A1431A, A1631A, and A1719A).

Table 1 Chip batch quantity details

Model	Batch	Number (chip)
EP4CE10E22C8N	G CCAAA1637A	5
	G CCAAA1431A	5
	G CCAAA1631A	8
	G CCAAA1719A	10

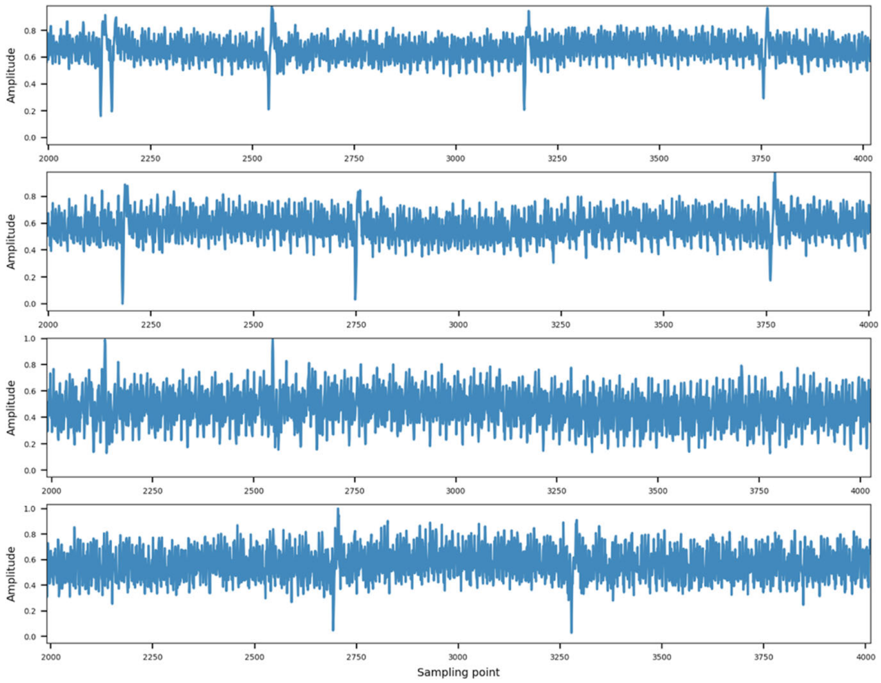


Fig. 3 Signal amplitude response

According to Fig. 3, the average amplitude of the four signals is different and there are peaks at different positions.

6.2 Signal collection

The radiation from each chip is collected by using an approach probe connected to the oscilloscope. The probe acts as an antenna for receiving unintended radiation from the device. The test did not directly contact the chip and the distance is 1 cm. All data is acquired at a sampling rate of GSa/s, and an amplifier (PA-303N) is inserted between the probe and the oscilloscope to amplify the signal. The experimental device is shown in Fig. 4 and Fig. 5.

In this study, the device was preheated for 20 min before the signal was collected to stabilize the operating temperature and a regulated power supply was used to provide a stable supply voltage to control the environmental impact. After warming up, each chip repeatedly performs the same operation to collect the same signal. For practical implementation, studies have shown that working within the expected operating temperature and supply voltage range is an effective technique for dealing with environmental fluctuations.

For all operations, the chip is used randomly to prevent any differences related to the acquisition sequence. All acquisition operations did nothing to isolate the data collection system from the background environment noise, and all collections took place in an office environment with a large number of PCs and wireless devices.

6.3 Classification order

In this research scheme, the classification order is first classified for the chip model, and 28 chips can be accurately classified into their specific batch, and then the chip-

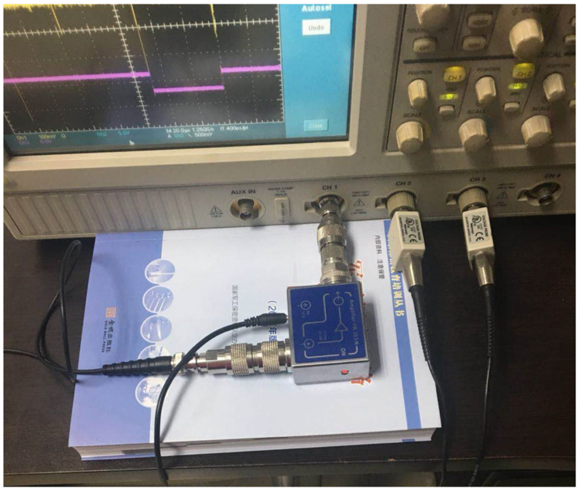


Fig. 4 The amplifier of PA-303N

chip detailed classification of the subordinate chips is performed for each batch. Through this classification method, we can understand the chip model, and we can know which chip is working.

6.4 Datasets and input

In this experiment, each of our chips was individually set to one class. The data required for training is completely collected by the laboratory. As stated in the paper, we have 28 chips to collect data; each chip collects 20,000 pieces of data, so there are 560, 000 pieces of data as data sets. Among the 20,000 pieces of data collected by each chip,

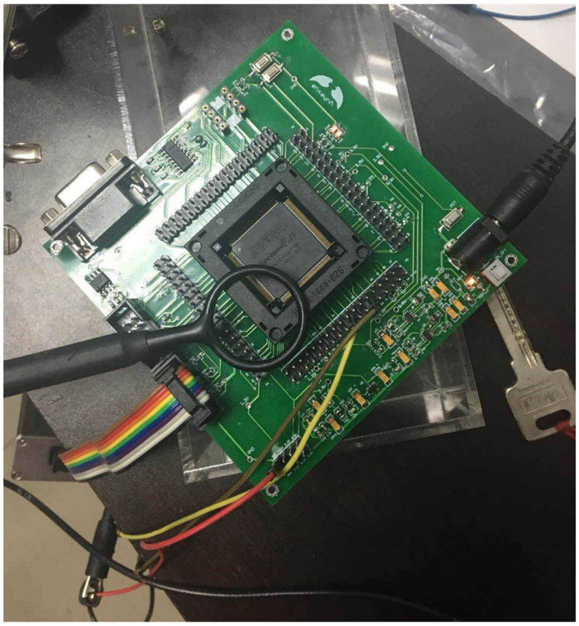


Fig. 5 Probe connector and chip

we set 90% for the training set and 10% for the verification set. Thus, the training set has a total of 504,000 pieces of data, and the validation set has a total of 56,000 pieces of data (Table 2). Because the study protects device clones, we need to accurately and one-to-one identify all chips. So we will use all the chips in the network training.

The original signal has 9604 points. When we input the network, we convert the video signal into a two-dimensional signal by method function named numpy.reshape() in python.

6.5 Devices for training

The equipment used during the training is configured as follows: GPU: NVIDIA GeForce GTX 1080 Ti. The CPU is Intel(R) Xeon(R) and CPU: E5-2678 v3 @ 2.50 GHz. When using this equipment to train, the accuracy and loss reach a steady state during training which needs 2 h. If a logistic regression algorithm is used, the training usage time is 20 min. But the final accuracy is very different. When we judge whether the model is suitable, we judge based on the combination of final accuracy and time.

6.6 Network

The training process of the neural network includes a forward propagation process and a back-propagation process [18]. The neural network training algorithm is mainly based on the gradient descent back-propagation algorithm. The algorithm updates the parameters according to the gap between the training samples and the expected output. The parameters that need to be updated include the convolution kernel parameters and the down-sampling network weights, full connectivity layer network weights, and layer bias parameters [19, 20]. The difference between the training sample and the expected output is typically evaluated using a loss function; the loss function is calculated for each layer, and the parameters are updated in a direction that causes the loss function to decrease, such that the final output is close to the desired output. In order to increase the frequency of updating parameters, we generally use the gradient descent method to train the network. The global squared error loss function of n samples can be defined as:

$$J(k, \alpha, w, b) = 1/2n \sum_{i=1}^{N} \|t_n - y_n\|^2 \tag{1}$$

The error signal is then conducted to the front layer according to the chain law of the derivation.

The layer network parameters are updated by the calculated loss function for the partial derivatives of parameters k, α, w, and b. Layer l parameter update:

Table 2 Data distribution

Number of chips	Number of data/chip	Training set/chip	Validation set/chip
28	20,000	18,000	2000
	Total number of data	Total training set	Total validation set
	560,000	504,000	56,000

$$k_{ij}^{l} = k_{ij}^{l} - \eta \frac{\partial J}{\partial k_{ij}^{l}} \tag{2}$$

$$b_{ij}^{l} = b_{ij}^{l} - \eta \frac{\partial J}{\partial b_{ij}^{l}} \tag{3}$$

Layer m full connection parameter update:

$$w_{ij}^{m} = w_{ij}^{m} - \eta \frac{\partial J}{\partial w_{ij}^{m}} \tag{4}$$

$$b_{ij}^{m} = b_{ij}^{m} - \eta \frac{\partial J}{\partial b_{ij}^{m}} \tag{5}$$

Among them, η is the learning rate, the speed of controlling the gradient is lowered, and the learning rate is too large, which easily leads to the inability to converge.

The training process of the network is actually an approximation process for the implicit mapping between input and output, but this process is difficult to optimize in a very deep network. The deep residual network uses the residual block approach to try to solve this problem and achieves good results. As shown in Fig. 6, the basic model of the residual block, $H(x)$ is the learned feature information, $F(x)$ is the general neural network feature information, and x is the shallower feature information. By adding $F(x)$ and x, it is possible to eliminate the defect that the deep layer cannot learn the feature information as the number of network layers deepens, so that the network always has information to learn.

In this paper, we use the residual network, and the number of network layers is 22 layers. Except for the first layer and the last layer, each of the 2 layers constitutes a residual block. The structure is presented in Figs. 7 and 8.

The specific parameters are shown in Table 3.

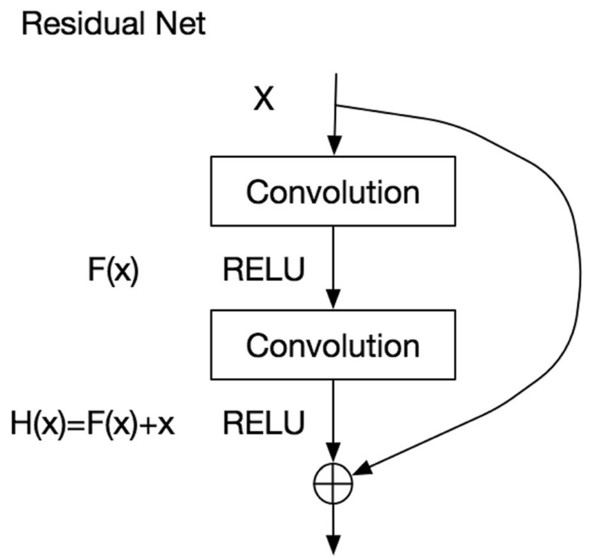


Fig. 6 Residual block model

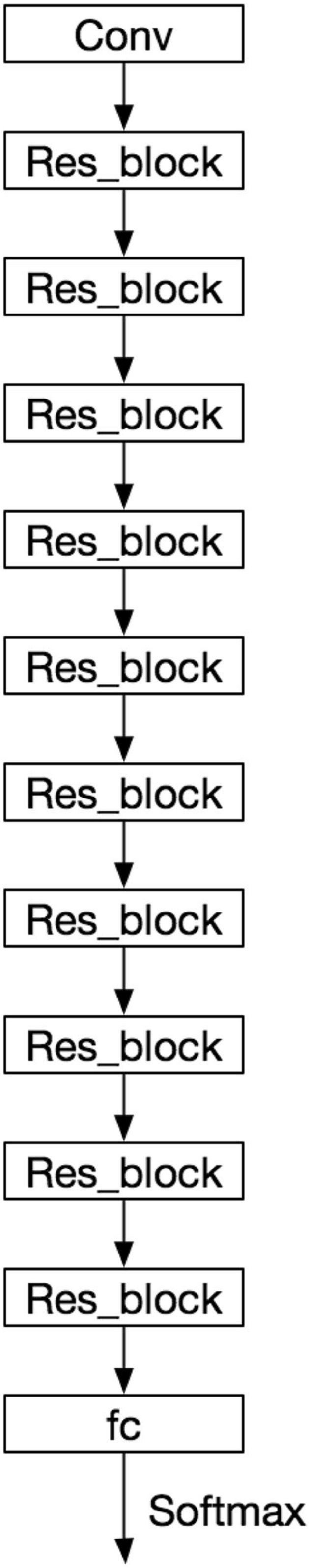


Fig. 7 Network structure

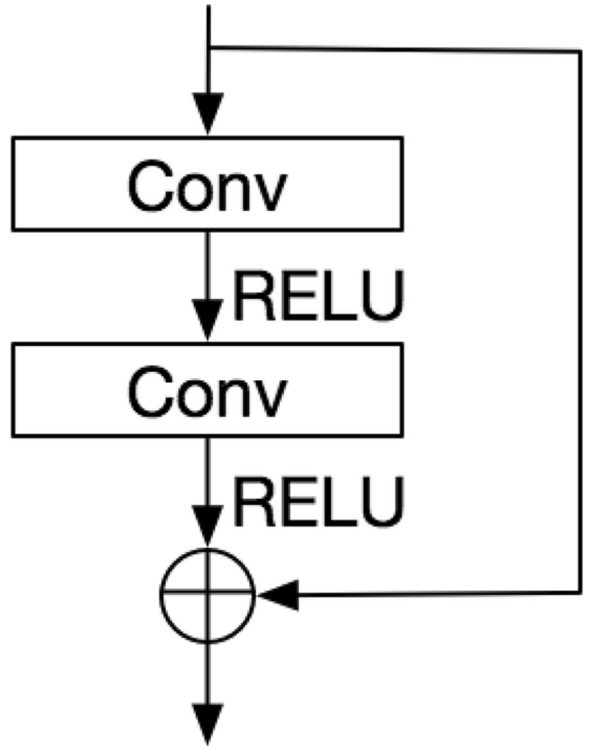


Fig. 8 Residual block

In the parameters, the "[1, 3, 16]" is mean: convolution kernel is [3], the step is 1, and filter number is 16.

According to the same network structure of this article, we designed 12 layers, 18 layers, and 22 layers of networks to compare. The results of the comparison are presented in Figs. 9 and 10.

According to the above four figures, the 22-layer and 18-layer are significantly better than the 12-layer network, and the 22-layer is slightly better than the 18-layer network. In the time comparison, as shown in Fig. 11 below, training time has been automatically generated based on the training data by Tensorboard.

Table 3 Specific parameters

Layer_name	Parameters
Conv	[1, 3, 16]
Res_block	[1, 3, 16]
Res_block	[1, 3, 16]
Res_block	[1, 3, 16]
Res_block	[1, 3, 16]
Res_block	[1, 3, 16]
Res_block	[3,3,1,32]
Res_block	[3,3,1,32]
Res_block	[3,3,1,32]
Res_block	[3,3,1,32]
Res_block	[3,3,1,32]

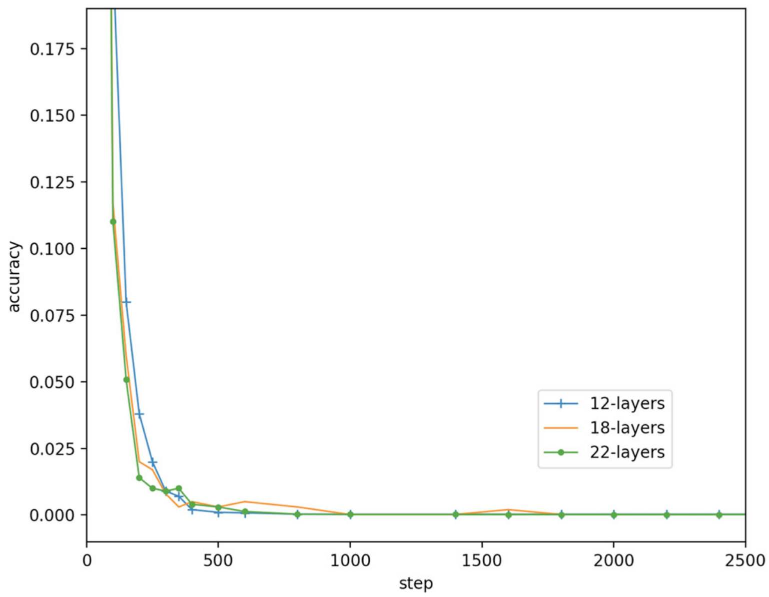


Fig. 9 Loss under different layers

It can be seen from the figure that training to the same steps requires less time for the 12 layers, but the time required for the 18 layers and the 22 layers is almost the same. If we continue to deepen the network layers, the final result will not be much improved, and the time will slowly increase. Therefore, the article selects the 22-layer network finally.

The advantage of the residual neural network is that it can automatically extract the feature map suitable for the classification target through a very deep network depth. Our method takes into account the time consumption while deepening the depth. The

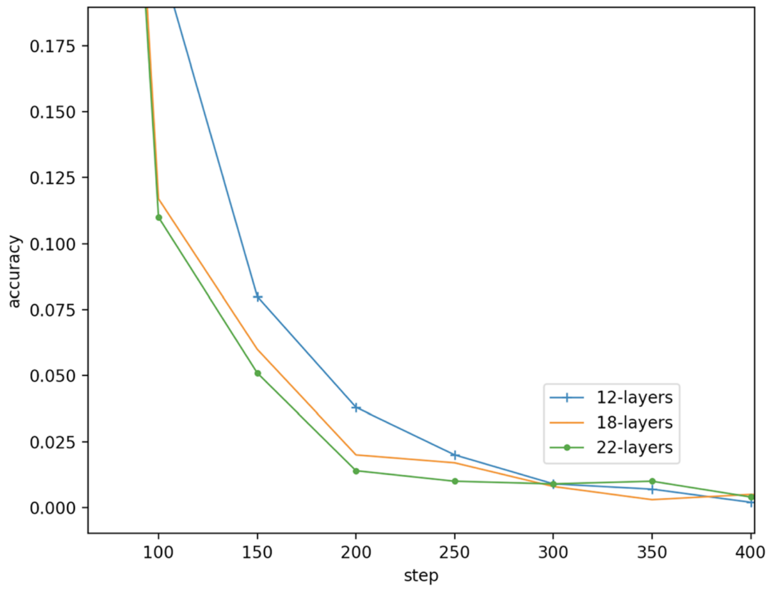
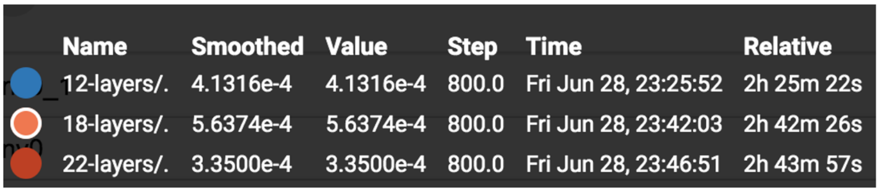


Fig. 10 Details of loss under different layers



	Name	Smoothed	Value	Step	Time	Relative
●	12-layers/.	4.1316e-4	4.1316e-4	800.0	Fri Jun 28, 23:25:52	2h 25m 22s
●	18-layers/.	5.6374e-4	5.6374e-4	800.0	Fri Jun 28, 23:42:03	2h 42m 26s
●	22-layers/.	3.3500e-4	3.3500e-4	800.0	Fri Jun 28, 23:46:51	2h 43m 57s

Fig. 11 Training time under different layers

design of the number of convolution kernels can ensure that the number of parameters will not explode with deepening the depth.

7 Results

7.1 The result of training using the original signal

In this study, the signal was amplified only when the signal was acquired, and then no subsequent processing was performed on the signal. In the case of the original SNR, the 20-layer depth residual neural network was used to classify and identify the chip.

The classifier achieves 100% batch classification and 100% chip-chip specific classification under the collected SNR (no enhancement). In this way, the overall average recognition rate reaches 100%. The feature maps that were generated autonomously by the last convolutional layer are shown in Fig. 12.

Figure 12 is a final classification feature map of four batches that from top to bottom are A1431, A1631, A1637, and A1719 batches. As can be seen from the figure, the overall amplitude of A1431 and A1631 is higher, while the average amplitude of the second half of A1431 is higher, and the average amplitude of the first half of A1631 is

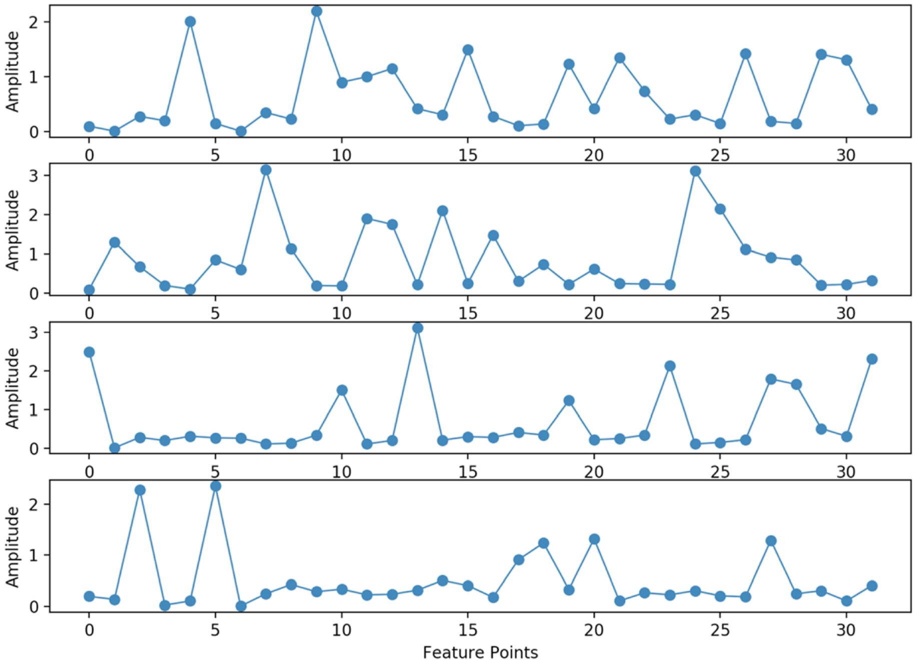


Fig. 12 Batch map

higher. A1637 and A1719 had overall low amplitude, of which all A1637 are in a low-amplitude state, A1719 central amplitude increases, and the rest is in a low-amplitude state.

Figure 13 is the batch chip feature map of A1431. As can be seen from the figure, the amplitude of each chip in the batch is not repeated and opposite, so that five chips are separated.

Figure 14 is the batch chip feature map of A1631. As can be seen from the figure, most of the chips in the batch are in a low-amplitude state, and the feature points in the high-amplitude state are in different ranges, thereby separating the batch of 8 chips.

Figure 15 shows the A1719 batch chip. For the batch chip, except for a few chips which have a lower amplitude, the other chips are generally in a relatively high-amplitude state. It can be seen from the figure that the amplitude direction and shape are different in the high-amplitude state. Thereby, different chips are separated.

Figure 16 is the batch chip feature map of A1637. It can be seen from the figure that the classification algorithm can be classified and identified according to the range and number of feature points in the high-amplitude state.

In this way, 100% recognition accuracy can be achieved under the original conditions without signal enhancement, and the results show that the device can achieve great performance without additional optimization.

In order to test the recognition results of untrained chips, we deliberately use the chip that has never been trained by the networks. I used 27 chips for training and used one of the A1719 batches without trained chips for testing. In the training process, 4 batches are classified first, and then 9 chips are classified according to specific chips (only 9 chips are used in the A1719 batch, the remaining chip test).

The final test result is that the accuracy of the chip classification of A1719 batch is 94.73% and classification into a specific chip is 76.K68% (Figs. 17 and 18).

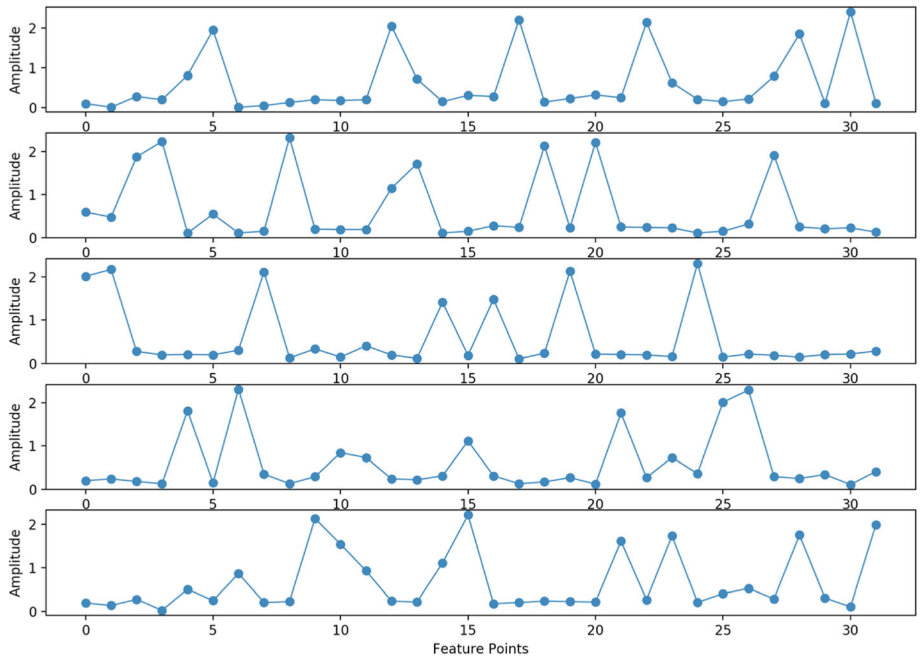


Fig. 13 batch chip feature map of A1431

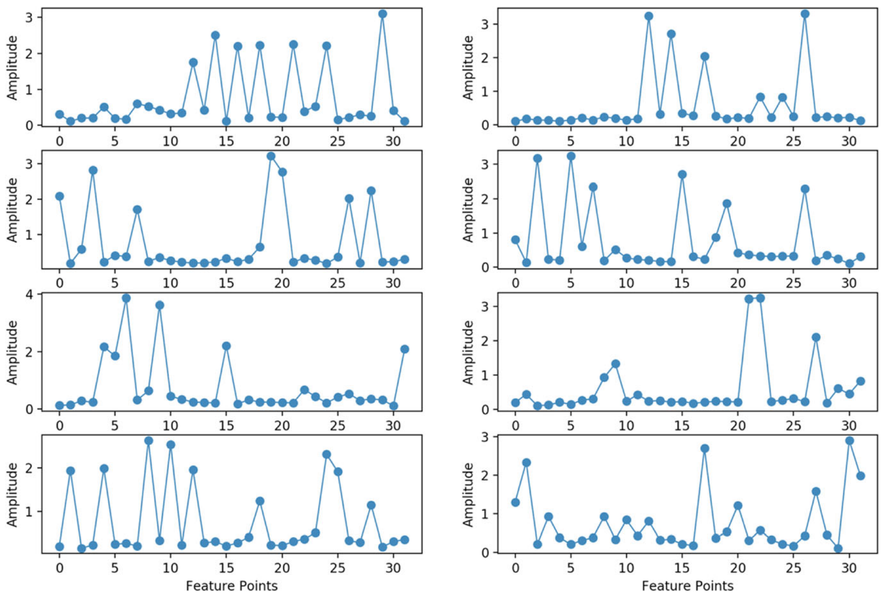


Fig. 14 batch chip feature map of A1631

The reason for the high accuracy of classification into specific batches is the similarity between the chips of each batch. However, when the individual chips of the same batch are classified individually, the reason for the low accuracy is that the chips have independent features, and the difference between these independent features is little, so it is easy to make mistakes.

The result is that the network usually classifies it as a chip with similar characteristics. Often two chips are similar, so when using 10 pieces of data for classification, after statistics, the maximum number of chips divided into one chip usually does not exceed

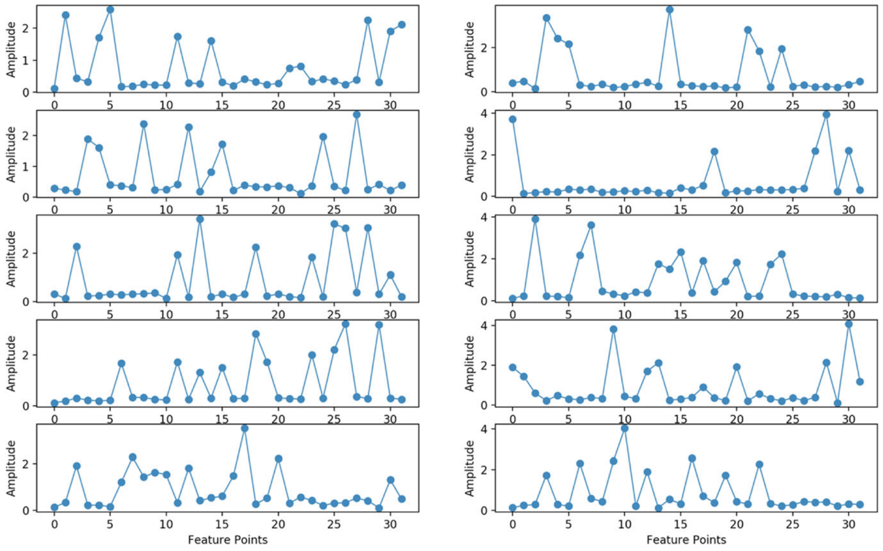


Fig. 15 batch chip feature map of A1719

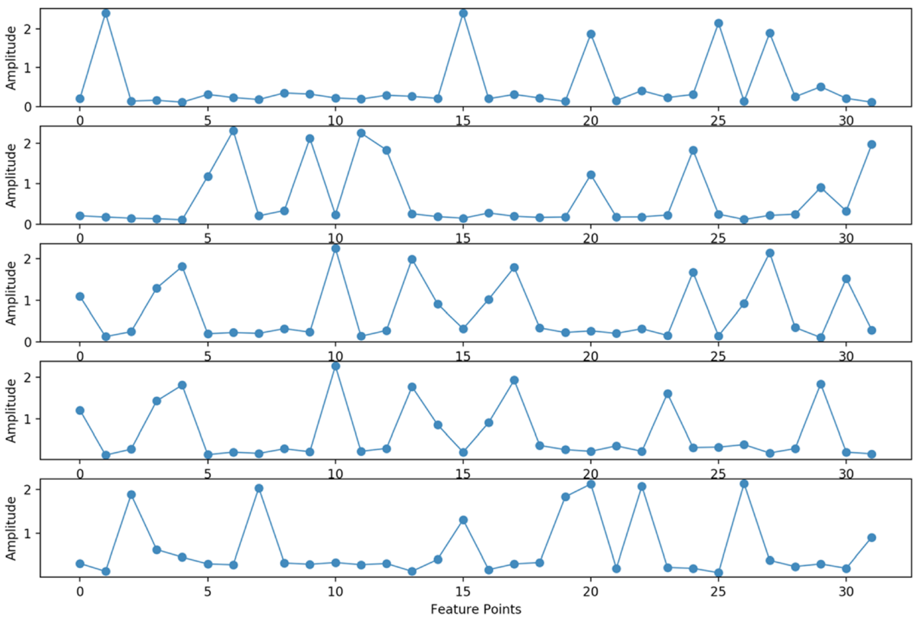


Fig. 16 batch chip feature map of A1637

8.5 pieces of data. By statistically calculating the classification results of multiple pieces of data, the chips that have never been trained can be excluded.

7.2 The results using different a SNR signal

In order to detect the anti-noise performance of the signal, we artificially add noise to the original signal without any operation. In this way, we get the datasets under different noise interferences: SNR = 22, SNR = 18, SNR = 14, SNR = 10, SNR = 6, SNR = 2, and SNR = − 2 were generated for 6 different signal-to-noise ratio signals, and network training was performed. Anti-noise performance can be understood by training and testing different SNR datasets. SNR is calculated using the following formula. The final result is shown in Fig. 19, and Fig. 20.

$$\mathrm{SNR} = 101_g\left(\frac{\mathrm{signal\_original}}{\mathrm{noise\_added}}\right) \tag{6}$$

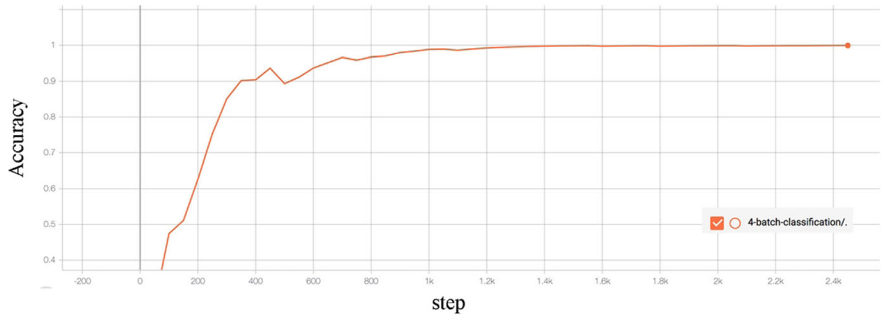


Fig. 17 Training accuracy of classification into 4 categories

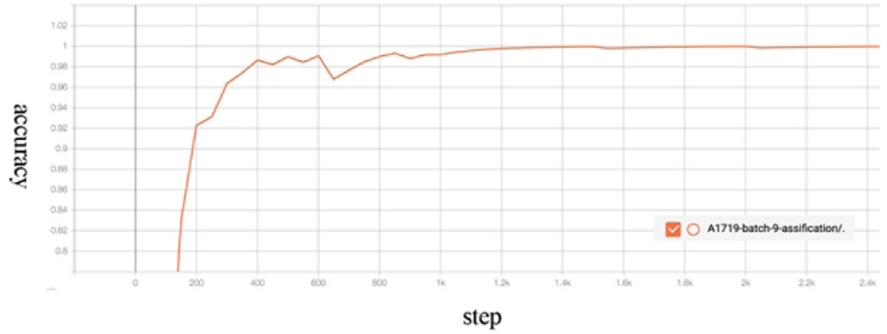


Fig. 18 Training accuracy of classification into 9 individual chips

Figure 19 shows the variation of the accuracy with SNR in the four categories of classification tasks.

Figure 20 shows the classification accuracy change image under different SNRs. The xlabel is the number of trainings and the ylabel is the accuracy.

As can be seen from Fig. 19 and Fig. 20, the network performance is still very good when SNR = 22, 18, and 14. When the SNR = 10 or less, the accuracy begins to decrease rapidly. When the SNR = − 2, the accuracy rate drops to 35.08%. From these data, the noise immunity of this technology is very good, and it is not necessary to pay attention to the environmental impact when collecting signals.

In order to observe the error between the chips, a network confusion matrix with SNR = 22 is made. As shown in Table 4.

It can be known from the confusion matrix that the A1719 batch is similar to the A1631 batch and is prone to misjudgment. The rest of the chips are more likely to be

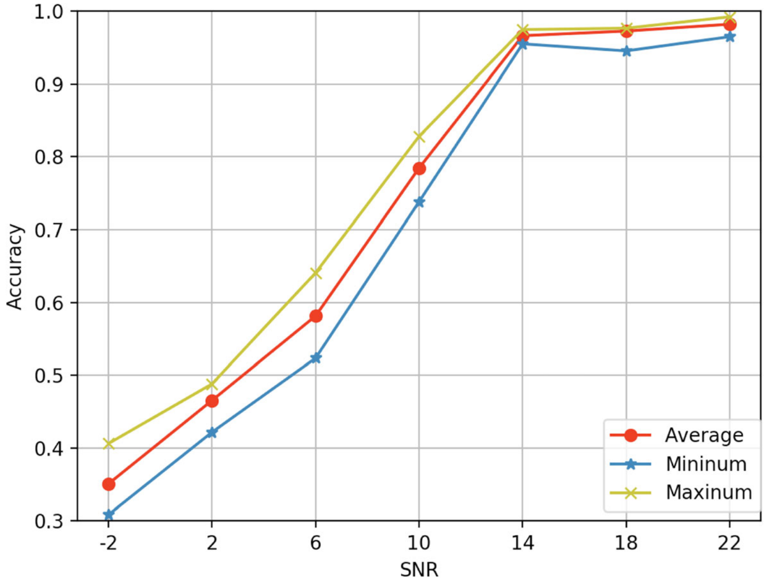


Fig. 19 Accuracy under different SNRs

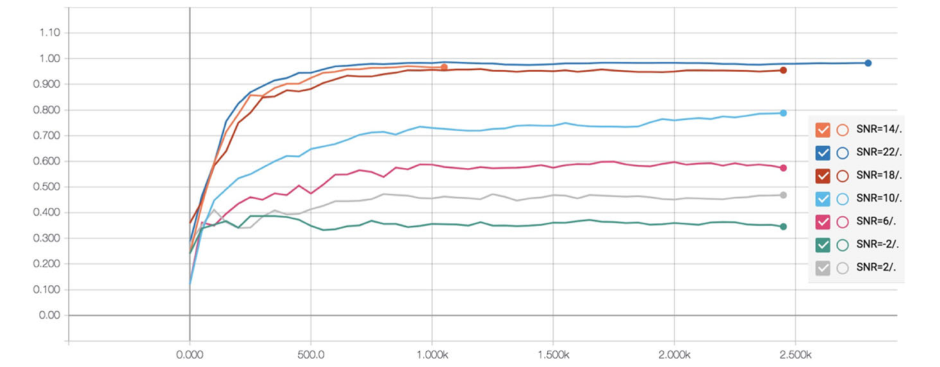


Fig. 20 Classification accuracy change under different SNRs

randomly misjudged. The reason should be the result of noise masking useful information.

7.3 The results using different algorithms

The SNR = 22 data set is used, different algorithms for training are used, and the results are compared.

In order to compare with the logistic regression, we extracted the features of the signal. When extracted features, we divide the original data set into 9 segments and extract the above 12 features in each segment to form a feature set. The 12 features are standard deviation, variance, skewness, and kurtosis of the instantaneous frequency, instantaneous phase, and instantaneous amplitude. The result is the accuracy is 61.3% finally. The result is shown in Fig. 21.

When using SVM for training, different kernel functions are used for comparison, such as RBF, linear, and sigmoid kernel functions. The data set uses three methods. The first is the original data set, without feature extraction (Since there are too many points, only the first 1000 points are used here.). The second is a data set that extracts only 12 features (12 features are the mean, variance, kurtosis, and skewness in the three domains of time domain, frequency, and phase). The third is to divide the original data set into 9 segments and extract the above 12 features in each segment to form a feature set.

The final result is shown in the Table 5, Table 6, and Table 7.

Table 4 Confusion matrix

	Forecast results				Actual total	Recall (%)
Actual results	14003	34	106	22	14165	98.86
	91	7036	9	2	7138	97.95
	403	18	11155	1	11577	96.35
	40	3	1	7076	7120	99.38
Forecast total	14537	7091	11271	7101	40000	
Accuracy (%)	96.33	99.22	98.97	99.65		

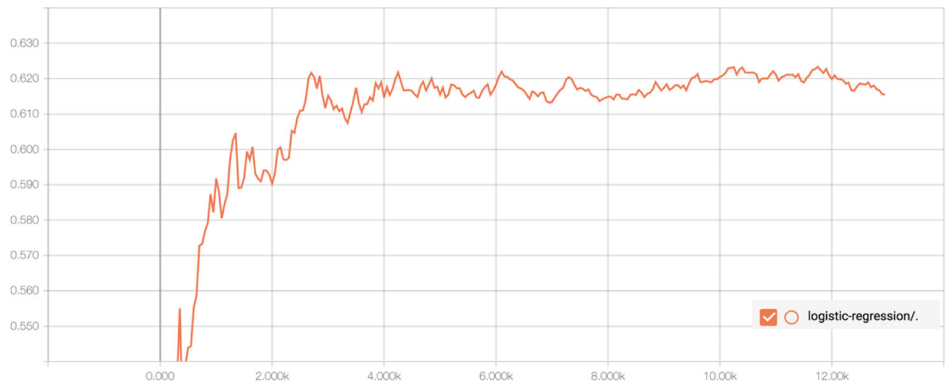


Fig. 21 The result of logistic regression

From the above results, it can be seen that the optimal result is to use the third data set and the kernel is RBF and gamma is 0.5. The optimal result is that the verification accuracy is 63%.

Because the difference between the chips is very small, the machine learning algorithm relies heavily on manual feature extraction and the depth of the general model is very shallow, so the result of the machine learning algorithm is not good.

Deep learning can continuously extract different features between categories through a very deep model, make full use of the computing power of the computer, and solve the problem of small difference in artificial feature extraction. Therefore, the final result of deep learning is excellent, far better than SVM.

The results of all methods are compared as shown in Table 8.

Compared with the results in other literatures and traditional machine learning, the main advantages of this algorithm are as follows:

1. The original signal acquisition does not require any additional processing and even does not require filtering to achieve very good results.

2. After the original signal is acquired, no artificial extraction feature is needed, which avoids the unnecessary influence caused by human intervention, and simplifies the operation process and reduces the manual operation time.

3. The algorithm classification can not only classify chips of different batches of the same model, but also classify and identify the same batch of chips of the same model. In this way, you can know which model a particular chip belongs to, and which specific chip in which batch get the most detailed information.

Table 5 Results using the first dataset

Kernel	**Gamma**			
	0.1		**1**	
	Training accuracy	**Verification accuracy**	**Training accuracy**	**Verification accuracy**
RBF	0.31	0.27	0.39	0.24
Sigmoid	0.25	0.23	0.27	0.22
Linear	0.79		0.1	

Table 6 Results using the second dataset

Kernel	Gamma					
	0.1		1		10	
	Training accuracy	Verification accuracy	Training accuracy	Verification accuracy	Training accuracy	Verification accuracy
RBF	0.51	0.49	0.55	0.51	0.89	0.58
Sigmoid	0.39	0.38	0.42	0.39	0.77	0.1

During a limited trial, no statistical difference in performance was observed when the specified response region changed to include sub-regions of very different microcode-indicating sequences. This indicates that the technique can be implemented in any manner, where a portion of other authentication processes or protocol communications can be intercepted. Further improvements in performance can be obtained by more carefully selecting or defining responses that emphasize device sub-circuits with high inter-device variability, such that the classification algorithm more determines its classification results. However, it is believed that for many applications, this approach has provided sufficient performance without further performance improvements through response optimization.

The limitation of the algorithm proposed in this paper is as follows: The current method records the features of each chip, and when a new chip is added, it is necessary for retraining. This issue needs to be improved.

8 Conclusion and discussion

An unintended EM radiation of IC possesses a feature that is a rich source of distinguishing information for device identification. The experimental results demonstrate the applicability of deep residual neural networks in identifying and verifying device identification tasks. In experimentally collecting signals, this technique can correctly identify all devices. Under the condition of the original signal-to-noise ratio analysis, the correct recognition success rate is maintained at 100%. Comparing the main references, the correct rate is higher when the SNR is far less than the reference. This technology is expected to be used in anti-cloning and related security applications that require unique IC device identification. In addition, superior performance indicates that the technology can accommodate less than ideal conditions and provide acceptable

Table 7 Results using the third dataset

Kernel	Gamma					
	0.1		0.5		1	
	Training accuracy	Verification accuracy	Training accuracy	Verification accuracy	Training accuracy	Verification accuracy
RBF	0.61	0.60	0.68	0.63	0.73	0.63
Kernel	Gamma					
	2		5		10	
	Training accuracy	Verification accuracy	Training accuracy	Verification accuracy	Training accuracy	Verification accuracy
RBF	0.77	0.59	0.83	0.48	0.88	0.36

Table 8 The results of the methods

Method	SVM	Logistic regression	This paper
Accuracy	63%	61.3%	99.63%

performance. The limitation of this method is that the time consumption during training is more than that of traditional machine learning methods.

In order to fully understand the applicability of this method in practical security implementation, there is still a lot of work to be done. The ability to distinguish between devices by inherent characteristics is guessed intuitively, and these characteristics are very difficult to present. However, further analysis and experimentation are needed to confirm this. Other areas that require further research include:

(1) Results of the algorithm when different sensor modules or sensor positioning is changed;
(2) Scalability for very large databases.

9 Supplementary information

Supplementary information accompanies this paper at https://doi.org/10.1186/s13638-020-01808-z.

Additional file 1. Accessories

Abbreviations

IC: Integrated circuit; RF: Radio frequency; FPGA: Field-programmable gate array; ASIC: Application-specific integrated circuit; FCC: Federal Communications Commission; EM: Electromagnetic; CMOS: Complementary metal oxide semiconductor; PUF: Physical unclonabel functions; RF-COA: RF Certificates of Authenticity; RES_block: Residual block; Conv: Convolution layer; RELU: Rectified Linear Unit

Acknowledgements

This work has been supported by The National Natural Science Foundation of China under Grants 61571063 and Beijing Natural Science Foundation under Grants 3182028.

Authors' contributions

ZH, XJ, and ZF conceived of the study and participated in its design. CX participated in the data collection work. SS participated in the design of the study. LJ participated in data preprocessing, experimental design, network model design, and implementation. ZH reviewed the manuscript. All authors read and approved the final manuscript.

Funding

This work has been supported by The National Natural Science Foundation of China under Grants 61571063 and Beijing Natural Science Foundation under Grants 3182028.

Availability of data and materials

Data sharing is available by emailing the first author (hongxinzhang@bupt.edu.cn).

Competing interests

There are no competing interests in this study.

Author details

[1]College of Electronic and Information Engineering, Beijing University of Posts and Telecommunications, Beijing 100876, China. [2]Beijing Key Laboratory of Work Safety Intelligent Monitoring, Beijing University of Posts and Telecommunications, Beijing 100876, China. [3]Beijing Institute of Spacecraft System Engineering, Beijing 100086, China. [4]College of Computer Science and Technology, Zhejiang University, Zhejiang 310058, China.

Received: 22 January 2020 Accepted: 20 September 2020
Published online: 19 October 2020

References

1. D. Hu, D.T. Ma, H. Gong, Z. Ma, A physical layer security authentication method based on PUF [J]. Information Network Security 20(01), 61–66 (2020)
2. W.J. Li, AES energy analysis attack under simulated power collection platform[J]. Shandong Industrial Technology 14, 250–251 (2017)

3. D. Li, G.F. Dai, H.G. Hu, N.H. Yu, Side channel attacks against real RFID tags [J]. Journal of Cryptography 6(03), 383–394 (2019)
4. William E. Cobb, Eric D. Laspe, Rusty O. Baldwin, intrinsic physical-layer authentication of integrated circuits IEEE TRANSA CTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 7, NO. 1, FEBRUARY 2012
5. A. Jain, A. Ross, S. Prabhakar, An introduction to biometric recognition. IEEE Trans. Circuits Syst. Video Technol. 14(1), 4–20 (2004)
6. Federal Communications Commission (FCC), Code of Federal Regulations, Title 47 2009
7. C. Paar, T. Eisenbarth, M. Kasper, T. Kasper, and A. Moradi, "Keeloq and side-channel analysis-evolution of an attack," in FDTC, L. Breveg- lieri, S. Gueron, I. Koren, D. Naccache, and J.-P. Seifert, Eds. Los Alamitos, CA: IEEE Comput. Soc. Press, 2009, pp. 65–69.
8. Wang X, Zhou Q , Harer J , et al. Deep learning-based classification and anomaly detection of side-channel signals [C]// Cyber Sensing 2018. 2018.
9. Y.J. Xiao, W.Y. Xu, Z.H. Jia, et al., NIPAD: a non-invasive power-based anomaly detection scheme for programmable logic controllers [J]. Frontiers of Information and Electronic Engineering: English 18, 534 (2017)
10. W. Cobb, E. Garcia, M. Temple, R. Baldwin, and Y. Kim, "Physical layer identification of embedded devices using RF-DNA finger- printing," in Proc. 2010 Mil. Commun. (MILCOM2010) Conf., 2010, pp. 682–687.
11. R. Maes, P. Tuyls, *Secure integrated circuits and systems, I. Ver- bauwhede, Ed* (Springer, New York, 2010)
12. R. Pappu, B. Recht, J. Taylor, N. Gershenfeld, Physical one-way functions. Science 297(5589), 2026–2030 (2002)
13. G. DeJean and D. Kirovski, "RF-DNA: Radio-frequency certificates of authenticity," in CHES, ser. Lecture Notes in Computer Science, P. Paillier and I. Verbauwhede, Eds. New York: Springer, 2007, vol. 4727, pp. 346–363.
14. B. Danev, T. Heydt-Benjamin, and S. Čapkun, USENIX Association, "Physical-layer identification of RFID devices," in Proc. 18th Conf. USENIX Security Symp., 2009, pp. 199–214.
15. J. Zhang, Y. Xu, Y.T. Mei, A PUF-based lightweight RFID security authentication protocol for low-cost tags [J]. Journal of Anhui Vocational College of Water Resources and Hydropower 19(02), 48–51 (2019)
16. M.H. Ameri, M. Delavar, J. Mohajeri, Provably secure and efficient PUF-based broadcast authentication schemes for smart grid applications [J]. Int. J. Commun. Syst. 32, 8 (2019)
17. X.L. Wang, Y.F. Zhang, H.X. Zhang, X.F. Wei, G.Y. Wang, Identification and authentication for wireless transmission security based on RF-DNA fingerprint. EURASIP J. Wirel. Commun. Netw. 2019(1), 1–12 (2019)
18. Zhao B , Zhu L , Ma Z , et al. Object detection based on multi-channel deep CNN [C]// 2018 14th International Conference on Computational Intelligence and Security (CIS). IEEE Computer Society, 2018.
19. L. Duan, *Reserch on bioelectrical signal recognition for smarter healthcare [D]* (Beijing University of Posts and Telecommunications, Beijing, 2018)
20. F. Jiang, Y. Fu, B.B. Gupta, et al., Deep learning based multi-channel intelligent attack detection for data security [J]. IEEE Transactions on Sustainable Computing, 1–1 (2018)

Publisher's Note

Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.