Counterfeit IC Detection Research Based on BP-AdaBoost Model and Genetic Algorithm

Junyan Liu, Xiongwei Li, Linyun Liu, Zhihui Wang, Panfei Du, Kang Li

ABSTRACT

In view of the increasingly prominent problems exposed by chips in integrated circuits and the destructive problems of traditional chip detection methods, a BP-AdaBoost neural network model based on genetic algorithm optimization was proposed and applied to chip detection and classification. By using electromagnetic probes to collect the electromagnetic signals generated by different chips in the same operating state and using the electromagnetic radiation signals as the basis for chip identification and classification, the signals are put into the BP-AdaBoost model optimized by genetic algorithm for learning and training. Experimental results show that this method has good effect in the application of chip recognition and classification.

KEYWORDS

Chip Inspection, Bypass Signal, Neural Network, Adaptive Boosting Algorithm, Genetic Algorithm.

INTRODUCTION

With the rapid development and wide application of electronic products, various
problems existing in integrated circuit chips have been exposed and are increasingly valued by people [1]. For these chip products that do not meet the original design specifications or are not authorized, we call them "Pseudo Chips [2]". In some important fields, the safety and reliability of IC chips are crucial. Once the problematic chip has a safety problem or failure during operation, it is very likely to bring huge economic losses and even more serious consequences. Therefore, how to effectively detect the chip is a very important issue.

However, the manufacturing methods of pseudo chips are becoming more and more concealed, and it is not an easy task to detect the chip with low cost, high efficiency and precision. Some of these problems are hidden deep, and it is difficult for us to find them by conventional means. The problems in the chip are manifold. At present, there are many different test methods for detecting various abnormalities in the chip. The detection methods are different according to the nature of the problem. The main detection methods can be divided into two categories, namely physical detection methods and electrical detection methods [2]. Physical detection methods have certain limitations, most of which are destructive to the chip, and have high detection cost, long time, and low detection efficiency. It can't be done automatically, and it depends on man-made standard operation. Although the electrical testing method has low cost and simple operation, the electrical parameters of the chip vary greatly, making it difficult to determine whether it is aging or the cause in the process and it is difficult to detect the subtle problems in the chip.

Therefore, some scholars proposed to achieve the purpose of detecting chips from the perspective of bypass signal analysis [3]. In this paper, we use electromagnetic probes and oscilloscopes to obtain the electromagnetic bypass signals released by the chip in the execution of specific operations, and then introduce neural networks to learn and recognize them [4]. BP neural network can show good results in most classification tasks. In order to make the neural network achieve a better learning effect, we can further introduce genetic algorithms and ensemble learning methods [5]. The genetic algorithm realizes the optimization by simulating the natural selection of biological evolution theory and the biological evolution process of genetic mechanism, so as to prevent the BP neural network from falling into the local optimal situation. The AdaBoost algorithm uses the BP neural network as a weak learner to form a strong learner through continuous iterative training. The ensemble learning can achieve the effect that one person is smarter than the sum of wisdom of all people by combining multiple weak learners.
RELATED THEORIES

BP-AdaBoost Model

BP (Back Propagation) neural network can handle any complex pattern classification problem and also has better multi-dimensional function mapping ability. It can realize the process of continuous learning and improvement by forward propagation of signals and back propagation of errors. In this paper, the BP neural network with the structure shown in Figure 1, which is used as a weak learner to learn the processed digital signals.

The forward propagation of the BP neural network can be expressed by the following formula:

\[ H_j = f \left( \sum_{i=1}^{n} w_{ij} x_i - b_j \right) \quad j = 1, 2, \ldots, n \]  

(1)
Among them: \( x \) is the eigenvalue of the input; \( H_j \) is the predicted output of the hidden layer; \( O_k \) is the final output of the neural network; \( W_{ij} \) is the weight between the input layer and the hidden layer; \( W_{jk} \) is the weight between the hidden layer and the output layer Value; \( b_j \) is the threshold of the hidden layer; \( b' \) is the threshold of the output layer. \( f \) is the activation function, this article chooses the Sigmoid function:

\[
f(x) = \frac{1}{1 + e^{-x}}
\]

(3)

Backpropagation can be expressed by the following formula. After repeated iterations, the information in the signal is learned into the parameters of the neural network:

\[
e_k = \frac{1}{2}(Y_k - O_k)^2 \quad k = 1,2,...,m
\]

(4)

\[
w = w + \eta \frac{\partial e}{\partial w}
\]

(5)

\[
b = b + \eta \frac{\partial e}{\partial b}
\]

(6)

In the formula: \( e_k \) is the square loss function of the predicted output \( O_k \) and the label \( Y_k \); \( \eta \) is the learning rate of the neural network.

The AdaBoost algorithm is an iterative algorithm evolved from the Boosting algorithm and belongs to the Boosting algorithm series [6]. Compared with the Boosting algorithm, there are some improvements. This paper uses the AdaBoost
algorithm to train the BP neural network for multiple rounds to form several weak classifiers, and finally forms a higher-precision strong classifier by weighting these weak classifiers.

When training the first round of weak classifiers, initialize the training sample weights:

\[ D = (w_1, w_2, \ldots, w_N) \quad w_i = \frac{1}{N}, i = 1, 2, \ldots, N \]  

(7)

Training the weak classifier:

\[ G_m(x) : \chi \rightarrow [0, 1] \]  

(8)

The error value of the weak classifier determines the weight of this weak classifier:

\[ e_m = P(G_m(X) \neq y) = \sum_{i=1}^{N} w_m I(G_m(x_i) \neq y_i) \]  

(9)

\[ a_m = \frac{1}{2} \log \frac{1 - e_m}{em} \]  

(10)

After training a weak classifier, the weight of the training sample is updated according to the training effect for the training of the next weak classifier:

\[ w_{i,m+1} = w_{i,m} \exp[-y_i a_m G_m(x)] \]  

(11)

After rounds of iterations, multiple weak classifiers are obtained and linearly combined to obtain the final strong classifier:
Genetic algorithm is a parallel and random search for the optimal method. For non-convex functions, it can find the optimal in the global. In this paper, the genetic algorithm is used to find the initial weights and thresholds of the BP neural network that are closest to the global optimum before learning the samples using the BP-AdaBoost model. The basic flow chart of its optimization is shown in Figure 2:

\[ G(x) = a_1 G_1(x) + a_2 G_2(x) + \cdots + a_m G_m(x) \]  

(12)
The initial population is composed of a certain number of coding individuals. The genes of each individual are arranged into a one-dimensional array in the order of input layer to hidden layer weight, hidden layer threshold, hidden layer to output layer weight and output layer threshold by real coding.

The fitness indicates the individual's ability to survive in the problem space. Since the larger the error, the worse the individual's ability to adapt, so the reciprocal of the error is selected as the individual's fitness:

\[
    f = \frac{1}{\sum_{i=1}^{n} \text{abs}(y_i - o_i)}
\]

(13)

Using the method of roulette for selective replication, the probability of each individual entering the next generation is equal to the ratio of its fitness value to the sum of individual fitness values of the entire population:

\[
    P_i = \frac{f_i}{\sum_{j=1}^{N} f_j}
\]

(14)

EXPERIMENTAL PROCESS AND RESULT ANALYSIS

Experimental Configuration

The configuration of the experimental bypass signal acquisition platform is shown in Figure 3. For the electromagnetic probes, we selected the RF2 near-field probe set of LangerEMV technology company in Germany, and the digital sampling oscilloscope used the TektronixDPO4104 digital sampling oscilloscope of American Tektronix. During the experiment, the LabView program development environment was used to write a virtual instrument control program for the collected signals on the PC and control the configuration information of the relevant tests.
Experimental Process

SIGNAL ACQUISITION

Select two different models of 51 series single-chip microcomputer chips STC89C52RC and STC89C51RC to make labels (0/1), collect 100 sets of electromagnetic signals released when performing the same operation under the same operating state, and remove the noise through wavelet transform [7-8] Get training samples, and select 50 of them as the test set, used to detect the recognition effect of the method on the chip.

OPTIMIZATION OF NEURAL NETWORK PARAMETERS

According to the order of neural network input layer to hidden layer weights, hidden layer thresholds, hidden layer to output layer weights, and output layer thresholds, it is arranged into a one-dimensional array, which is used as a chromosome, and the initial population is put into the genetic algorithm for optimization. The initial population is set with 10 individuals, the crossover rate is set to 0.6, the mutation rate is set to 0.001, and the iteration is 200 times. Using the global search ability of the genetic algorithm, the global optimal solution of the problem space is obtained.
SAMPLE LEARNING

The genetic algorithm optimization result is used as the initial weight of the BP neural network, and the BP neural network is used as the weak classifier. The number of input layer nodes is the dimension of the training sample, the number of output layer nodes is 1, the number of hidden layer nodes is the square root of the product of the number of input layer nodes and the number of output layer nodes, the learning rate is 0.015, and the number of weak learner trainings is 10000 times, set 6 weak classifiers to learn and recognize the characteristic signals of the chip.

MODEL EFFECT TEST

Put 50 prepared test data into the trained model for classification, and judge the effect of the model in chip bypass signal recognition based on error value and classification accuracy.

Effect Evaluation of Classification

In order to test the classification effect of the model in chip detection, we use absolute error and accuracy as the evaluation indicators of the model:

(1) Absolute error:

\[
ER = \frac{1}{n} \sum_{i=1}^{n} |Y_i - O_i|
\]  
(17)

(2) Correct rate:

\[
ACC = \frac{\sum_{i=1}^{N} I(G_m(x_i)=O)}{N}
\]  
(18)
Experimental Results

The comparison of error and classification effect is shown in Figure 4 and Table I:

![Figure 4. Error diagram.](image)

| Evaluation          | Absolute error | Correct rate |
|---------------------|----------------|--------------|
| BP neural network   | 0.00527430     | 92%          |
| Mean value of weak classifier | 0.00338526     | 96%          |
| GA-BP-AdaBoost      | 0.00269622     | 98%          |

**Result Analysis**

From the data of the experimental results, the BP-AdaBoost model optimized by genetic algorithm has a relatively high accuracy rate for learning and identifying the
bypass signal in the chip. The weak classifier (BP) is optimized by genetic algorithm, its effect is greater than that of BP neural network.

At the same time, it can be seen that the recognition rate achieved by different base classifiers is uneven. Through ensemble learning methods, we can avoid the situation that a single weak learner does not have a good effect on individual samples. After the integration of AdaBoost algorithm, the effect is obviously better.

CONCLUSION

In this paper, the BP neural network with good learning classification ability and nonlinear mapping ability is used as the learner, and the genetic algorithm is used to obtain the initial weights and thresholds of the BP neural network. Under the influence of the AdaBoost algorithm, the two are combined to form an optimized BP-AdaBoost model, which is used to identify and classify chip bypass signals. The experimental results show that this method shows higher accuracy. It is in line with the actual situation and can be used for IC chip detection and recognition.

ACKNOWLEDGMENTS

Corresponding author: Xiongwei Li. This work was financially supported by National Natural Science Foundation of China (61602505, 61271152, 51377170).

REFERENCES

1. Hu Kaibo, Zhang Qian. Risks of the US military integrated circuit supply chain and its countermeasures [J]. China Integrated Circuit, 2013, 22(3): 24-30.

2. Tehranipoor M, Salmani H, Zhang X. Integrated Circuit Authentication: Hardware Trojans and Counterfeit Detection[M].2013: 138-146.

3. Ye Lin. Electronic component failure prediction technology and its application based on bypass signal analysis [D]. South China University of Technology, 2017.
4. Yan Fei, Hu Yuping. ECG signal classification method based on superimposed denoising automatic encoder combined with deep neural network[J]. Computer Applications and Software, 2019, 36(04): 178-185.

5. Wang Kai, Tang Shihua, Wang Jiangbo, Xiao Yang, Rong Jing, Wang Wenguang. Application of dam deformation based on GA-BP-AdaBoost strong prediction model [J]. Journal of Guilin University of Technology, 2019, 39(02): 415-419.

6. Zhou Zhihua. Machine learning[M]. Beijing: Tsinghua University Press, 2017:97-114,171-188.

7. Huang Juan, Gao Jing, Zhang Ling. Research on the method of bearing fault feature signal extraction based on wavelet denoising and HHT transform [J]. Machine Tool and Hydraulics, 2020, 48(10): 50-55.

8. Yu Wei, Han Qiang, Ma Jingjing. EEG signal processing method based on EMD and SVM [J]. Journal of Kunming University of Science and Technology (Natural Science Edition), 2012, 37(6): 38-42.