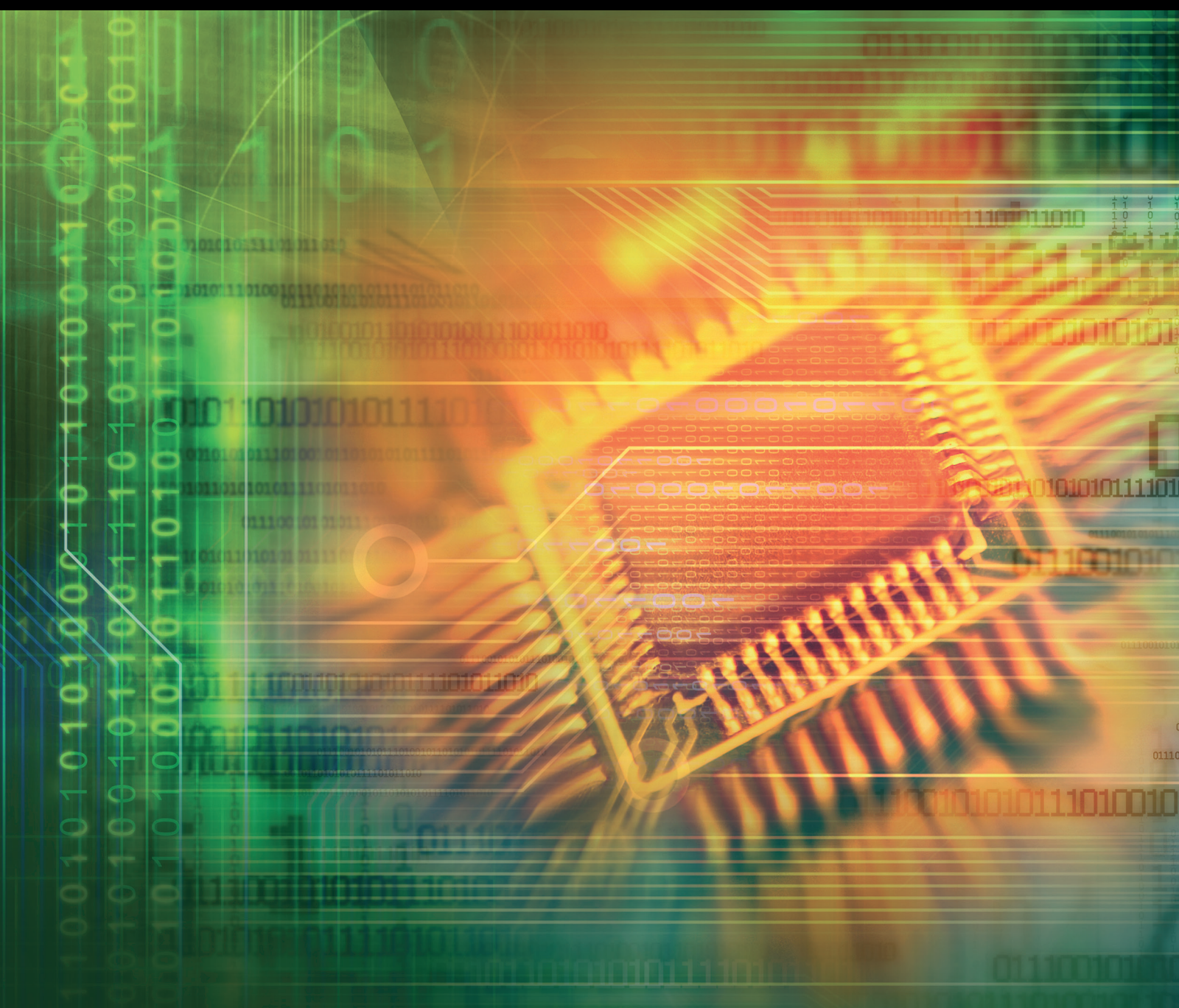
Journal of Electrical and Computer Engineering

Advanced Information Technology Convergence 2017

Lead Guest Editor: Jucheng Yang
Guest Editors: Anthony T. S. Ho, Hui Cheng, Sook Yoon, and Lu Liu



Advanced Information Technology Convergence 2017

Journal of Electrical and Computer Engineering

Advanced Information Technology Convergence 2017

Lead Guest Editor: Jucheng Yang
Guest Editors: Anthony T. S. Ho, Hui Cheng, Sook Yoon, and Lu Liu

Editorial Board

Contents

Hindawi
Journal of Electrical and Computer Engineering
Volume 2017, Article ID 3736075, 2 pages
https://doi.org/10.1155/2017/3736075

Editorial
Advanced Information Technology Convergence 2017

Jucheng Yang,[1] Anthony T. S. Ho,[2] Hui Cheng,[3] Sook Yoon,[4] and Lu Liu[5]

[1]*College of Computer Science and Information Engineering, Tianjin University of Science and Technology, Tianjin, China*
[2]*Department of Computing, School of Electronics and Physical Sciences, University of Surrey, Guildford, UK*
[3]*School of Computing and Mathematical Sciences, Liverpool John Moores University, Liverpool, UK*
[4]*Department of Computer Engineering, Mokpo National University, Jeonnam, Republic of Korea*
[5]*College of Engineering and Technology, University of Derby, Derby, UK*

Correspondence should be addressed to Jucheng Yang; jcyang@tust.edu.cn

Received 3 May 2017; Accepted 4 May 2017; Published 29 May 2017

Nowadays, the tremendous growth and usage of information technologies led to rapid development in the various aspects of advances in convergence and hybrid information technology, such as IT convergence in signal and image processing, human-computer interaction, robotics, transportation system, and health care. The spread of current technologies is more emanative at all stages of research, development, diffusion, and use. Moreover, different regions of research and applications are often integrated together to achieve better performance, solve problems, and restructure systems, as well as improve the computational intelligence in both theoretical and practical aspects. Hence, the convergence of information technologies could lead to the new stage of innovation with significant increasing speed.

This special issue in 2017 is aimed to provide state-of-the-art publication of refereed, high quality original research papers in all branches of the convergence technologies and its applications, such as signal and image processing for IT convergence, web and database technology for IT convergence, IT convergence in health care, robotics, transportation system, and Big Data technology. It provides a platform for researchers to comprehensively share ideas, problems, and solutions related to advanced information technology convergence with various topics.

The special issue consists of 8 papers whose brief summaries are listed below.

"The Channel Compressive Sensing Estimation for Power Line Based on OMP Algorithm" by Y. Zhang et al. analyzes the transmission characteristics of the power line channel and model it with mathematics channel. A new method about the power line channel estimation based on compressive sensing is proposed, which can collect and extract the effective parameters of the power line channel to storage with very little space.

"Study of SAW Based on a Micro Force Sensor in Wireless Sensor Network" by J. Wang et al. investigates wireless sensor network (WSN) acquisition nodes and analyzes the relationship between the frequency and actual pressure values of sensor nodes. Also, the sensitive mechanism of the surface acoustic wave (SAW) based on a micro force sensor is researched, and the principle of least squares method is used to establish a transformation model of frequency and pressure for the SAW sensor.

"Image Encryption Algorithm Based on a Novel Improper Fractional-Order Attractor and a Wavelet Function Map" by J. Zhao et al. presents a three-dimensional autonomous chaotic system with high fraction dimension. The image encryption algorithm is proposed based on the continuous chaos and the discrete wavelet function map.

"Ferrography Wear Particles Image Recognition Based on Extreme Learning Machine" by Q. Li et al. proposes to employ extreme learning machine (ELM) for ferrography wear particles image recognition, which shows its advantages compared to the traditional feedforward neural network based on gradient training algorithms. More specifically, the shape features, color features, and texture features of five typical kinds of wear particles are extracted as the input of the ELM classifier and five types of wear particles are set as the output of the ELM classifier.

"Online Behavior Analysis-Based Student Profile for Intelligent E-Learning" by K. Liang et al. analyzes the relation indicators of E-Learning to build the student profile and gives countermeasures. By adopting the similarity computation and Jaccard coefficient, a system model is designed to clean and dig into the educational data and the students' learning attitude and the duration of learning behavior are also used to establish student profile. Moreover, an intelligent guide model is presented to guide both E-Learning platform and learners to improve learning things according to the E-Learning resources and learner behaviors.

"A Fast and Robust Key Frame Extraction Method for Video Copyright Protection" by Y. Shi et al. proposes a key frame extraction method for video copyright protection. The fast and robust method is based on frame difference with low level features, including color feature and structure feature. A two-stage method is used to extract accurate key frames to cover the content for the whole video sequence.

"Algebraic Cryptanalysis Scheme of AES-256 Using Gröbner Basis" by K. Zhao et al. proposes a zero-dimensional Gröbner basis construction method by choosing suitable term order and variable order after performing an in-depth study on the linear transformation and the system of multivariate polynomial equations of AES-256. Also, an algebraic cryptanalysis scheme of AES-256 using Gröbner basis is proposed based on the detailed construction process of the zero-dimensional Gröbner basis.

"Acoustic Log Prediction on the Basis of Kernel Extreme Learning Machine for Wells in GJH Survey, Erdos Basin" by J. Cao et al. proposes using kernel extreme learning machine (KELM) to predict missing sonic DT logs when only common logs are available. The common logs are set as predictors and the DT log is the target. By using KELM, a prediction model is firstly created based on the experimental data and then confirmed and validated by blind-testing the results in wells containing both the predictors and the target DT values used in the supervised training. Finally the optimal model is set up as a predictor.

Jucheng Yang
Anthony T. S. Ho
Hui Cheng
Sook Yoon
Lu Liu

Hindawi
Journal of Electrical and Computer Engineering
Volume 2017, Article ID 2483586, 8 pages
https://doi.org/10.1155/2017/2483586

Research Article

The Channel Compressive Sensing Estimation for Power Line Based on OMP Algorithm

Yiying Zhang,[1] Kun Liang,[1] Yeshen He,[2] Yannian Wu,[2] Xin Hu,[2] and Lili Sun[2]

[1]*College of Computer Science and Information Engineering, Tianjin University of Science & Technology, Tianjin, China*
[2]*China Gridcom Co., Ltd, Shenzhen, Guangdong, China*

Correspondence should be addressed to Kun Liang; liangkun@tust.edu.cn

Received 12 November 2016; Accepted 28 March 2017; Published 23 April 2017

Academic Editor: Hui Cheng

Power line communication (PLC) can collect information by power line which increases the coverage and connectivity of the smart grid. In this paper, we analyze the transmission characteristics of the power line channel and model it with mathematics channel. The multipath effect of the power line channel is studied with a novel technology named compressive sensing herein. We also proposed a new method to the power line channel estimation based on compressive sensing. We can collect and extract the effective parameters of the power line channel to storage, which only take very little storage space. The simulation results show that the proposed approach can reduce the amount of processing data in the digital signal processing module and decrease the requirement for the hardware.

1. Introduction

Industry 4.0 employs CPS (Cyber-Physical System) to promote industrial production with interconnection and intelligence. And various communication technologies provide important support for the CPS. Power Line Communication, as a special communication technology, not only is designed to transmit electrical energy, but also is used to transmit multiple types of information [1]. However, due to the fact that the power line network is designed for the transmission of electrical energy and works in high electromagnetic phenomena environment, the characteristics of power line channel are different from other conventional communication channel greatly. Power line noise is very complex. It is not a single Gaussian white noise in the other usual communication environments and includes colored background noise and periodic impulse noise (asynchronous or synchronized), as shown in Figure 1.

According to the random in or out access of electrical equipment, PLC has a strong time-varying characteristic [2, 3]. The channel state information is essential for the relevant data detection, quantification, and interference suppression. Therefore, we need to further analyze and conduct research on the transmission characteristics and estimation methods of power line channel [4–6]. Generally, the traditional channel estimation method has three ways. Nonblind channel estimation is the most traditional channel estimation method, which mainly makes use of the pilot signal response channel's features on transmitting terminal. Blind channel estimation is a kind of channel estimation method which does not need to send pilot signal, Semiblind channel estimation is a compromise method between the above two methods [7]. The traditional channel estimation method requires a high speed analog to digital converter. In order to accurately estimate the channel characteristics on receiving terminal, we need to send long pilot signal and collect large sample data. There is no doubt that the hardware complexity and cost of the receiving terminal will increase.

Different from other areas of data compression for universal video, voice, image number, and so on, in order to be able to reliably analyze the power grid state, the data of power system stored after compression must be able to retain the perturbed feature quantities for each frequency band of the power quality [8]. In [8–10], authors adopt the wavelet transform to apply the power quality disturbance data compression and obtained a certain degree of compression. However,

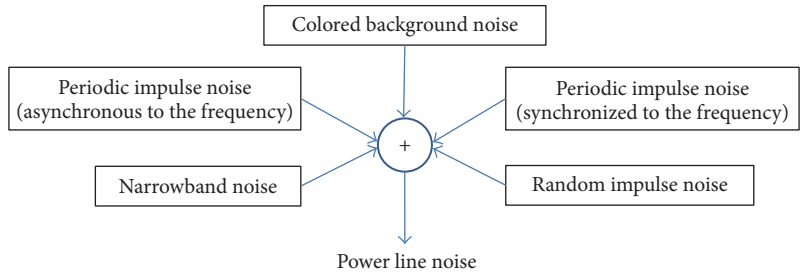


Figure 1: Power line noise.

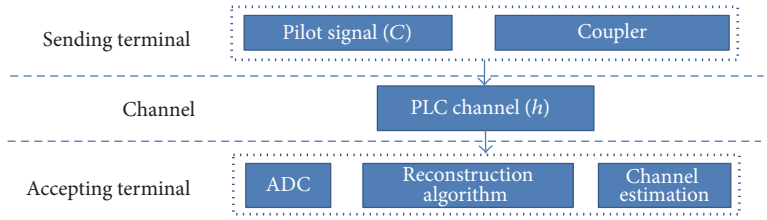


Figure 2: Block diagram of PLC estimation model.

the wavelet transform algorithm is complex, computationally intensive, real-time, and difficult to apply in real-time power quality monitoring system; meanwhile, the wavelet function is not unique, often using different wavelet analysis of the same signal analysis results which may vary greatly without adaptability.

Compression sensing includes two parts: the signal is measured on the measurement vector, and the signal is reconstructed by the measured value [11, 12]. Compression sensing theory shows that if the original signal is sparse on a certain base, the sampling frequency can be greatly reduced, and the original signal can be reconstructed exactly when the constrained equidistant condition between the observation matrix and the transform base is satisfied. The signal is sampled and compressed.

Therefore, researcher suggests that transmission characteristics of the power line channel are time-varying linear channel. We can estimate it based on OFDM pilot signal. However, this channel estimation mechanism ignores ADC device requirements on the receiving terminal. In the wireless communication scenario, a method of wireless channel estimation is based on compressive sensing. By orthogonal matching pursuit (OMP) algorithm on receiving terminal, we reconstruct the transmission characteristics of wireless channel [13–15]. This paper proposed an approach for the power line channel estimation based on compressive sensing. We analyzed the sparse characteristic of power line channel. Send the appropriate pilot signal by compressive sensing technology from the transmitting terminal. After the power line channel delay and attenuation, we extracted the effective features of power line channel to finish the power line channel estimation.

The rest of this paper is organized as follows. Section 2 presents PLC channel estimation model. Section 3 shows compressive sensing estimation channel characteristics. Section 4 describes the simulation in detail and Section 5 evaluates our solution and gives the conclusion.

2. Power Line Communication Channel Estimation Model

Power line communication channel estimation model includes two parts: transmitting terminal and receiving terminals. Transmitting terminal is used to send appropriate pilot signal, amplified and coupled to the power line through the coupling circuit and then is influenced by the actual power line channel environment. Channel estimation at the receiver can get the transmission characteristics of power line channel.

As shown in Figure 2, the transmission signal includes the effective signal and pilot signal, amplified and coupled to the power line through the coupling circuit. The signal is attenuated by the power line channel and the interference of the noise. Through a coupling circuit, receiving terminal does the electrical isolation and receiving and then starts the digital signal processing after A/D (analog-to-digital signal conversion) by ADC [16].

Usually, those residential areas are generally used in the combination of radial and trunk distribution mode. There are a large number of nodes in the power line network, such as the branch structure and the impedance mismatch [17], which are shown in Figure 3.

These nodes cause the transmission signal on the power line to not be able to reach the receiving node directly from the sending node. There will be reflected and standing waves on different paths. The final receiving device received the superimposed signal via reflected and standing wave in the different paths. This makes the power line channel cause multipath effect, and the transmission characteristics show a certain frequency selective fading.

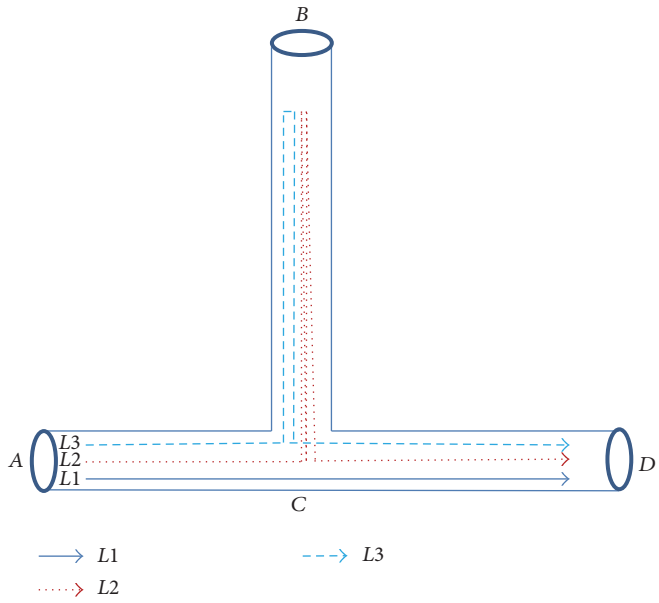


Figure 3: Branch circuit of power line communication.

Not only is the signal on power line directly transmitted from the sending node A to the receiving node D, but also it reflected many times to arrive at the receiving node D, forming the multipath effect. The signals in Figure 3 may have the transmission path as follows: (1) $L1$: $A \rightarrow C \rightarrow D$; (2) $L2$: $A \rightarrow C \rightarrow B \rightarrow C \rightarrow B \rightarrow C \rightarrow D$; (3) $L3$: $A \rightarrow C \rightarrow B \rightarrow C \rightarrow D$.

Since the multipath effect disperses the signal ability and arrives at the receiver with the different signal phase, it seriously influences the accepted effect. When there are n paths, frequency diversity can be achieved by changing the carrier frequency to improve the signal decision rate.

We suppose the channel transfer function of the ith path in multipaths is $H_i(f)$, so transfer function of the power line channel was formulated as follows:

$$H(f) = \sum_i H_i(f), \tag{1}$$

where $H(f)$ present the superposition of multipaths transmission characteristics. According to the reasons of multipath transmission, we analyzed the transmission characteristics on each path. There has been a path delay and the signal is attenuated with the increase of the transmission distance and frequency [18].

According to formula (1), we consider the main parameters affecting the characteristics of each path to establish the power line channel model. Meanwhile, for simulation, we simplify (1) as follows [19]:

$$H(f) = \sum_{i=1}^{N} g_i(f)\, e^{-(\alpha_0+\alpha_1 f^k)d_i} e^{-j2\pi f \tau_i}, \tag{2}$$

in which parameters (a_0, a_1, and k) are obtained by field measurements on the reference channel. Coefficient $g_i(f)$ is the weight of each multipath channel generated randomly between $(-1, 1)$. The parameter d_i is the channel length of each path, with uniform distribution on $(0, L)$. L defined the upper limit of the path length on each scenario. In the power line channel model, main parameters in Table 1 can be used for modeling and analyzing the typical power line channel [8, 20]. Although we reduce parameters, they also can reflect the power line channel characteristics.

Table 1: Parameters of transfer function model.

Model parameters	References
i	The number of paths; when the path is the shortest, $i = 1$
a_1, a_2	Attenuation parameter
k	Attenuation factor index; the typical value is 0.5~1
g_i	Weighted factor of path i; its absolute value is less than or equal to 1
d_i	The length of path i
τ_i	The delay of path i
f	Frequency

The mathematical model of power line channel shows that the power line channel is a multipath channel, which has frequency selective fading. The frequency response function reveals the sparse nature of the transmission characteristics of the power line channel.

3. Compressive Sensing Estimation Channel Characteristics

Due to the electromagnetic phenomena and other external causes, the environments usually affect the performance of

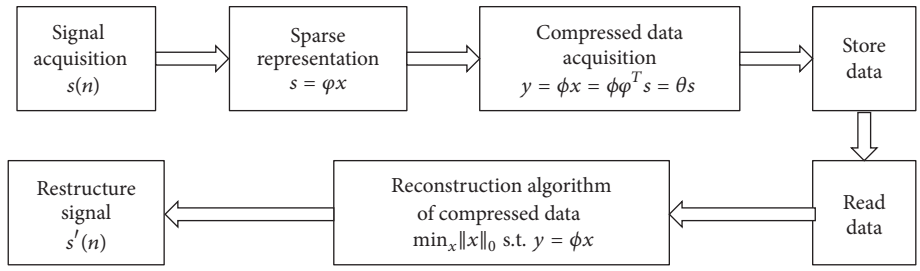


Figure 4: Process of CS.

device in power line communication. Therefore, it is very necessary to evaluate the channel accurately to acquire characteristic parameters of the channel impulse response.

3.1. Compressive Sensing Technology. The process of compress sensing includes three steps: signal sparse representation, data compression, and reconstruction of compressed data as shown in Figure 4.

The compression sensing is a novel information acquisition theory, which mainly consists of two parts: the signal is projected on the measurement vector to obtain the measured value; the signal is reconstructed from the measured value. Usually, the power steady-state harmonic signal can be expressed as

$$f(t) = a_0 \cos(2\pi\gamma_0 t + \theta_0) + \sum_{m=1}^{L} a_m \cos(2\pi\gamma_m t + \theta_m), \quad (3)$$

where a_0, γ_0, and θ_0 are the amplitude, frequency, and phase of the fundamental component; L denotes the number of harmonics; a_m, γ_m, and θ_m denote the amplitude, frequency, and phase of the mth harmonic component. We assume the signal $f(t)$ to be s in time domain. And then, we can start the process of compress sensing as follows.

3.1.1. Signal Sparse Representation. Assume the signal s has no sparsity in its time domain; it can be converted to another domain to obtain the sparsity projection x. Then, we can compress the sparsity x by the compress sensing technology. The transform domain projection process is the process of signal sparse representation, as shown in

$$s = \varphi x, \quad (4)$$

where s is the original signal without sparsity; φ denotes the projection matrix; x is the projection of s in the projection matrix φ, that is, the sparse signals.

3.1.2. Data Compression. Let $x(n)$ be a digital signal sampled by the ADC; the dimension is N. If x is a sparse signal and the sparsity is K ($K \ll N$), that is, there are only K nonzero elements in the signal, then it can be compressed by the compressed sensing technology to reduce the dimension N of the original signal $x(n)$ to the dimension M ($M \ll N$) and then we can get the compressed signal y as shown in

$$y = \phi x = \phi\varphi^T s = \theta s, \quad (5)$$

where y is the compressed signal; ϕ is an opposite observation matrix; x is the discrete signal; s is the original signal.

3.1.3. Reconstruction of Compressed Data. Since the front-end hardware completed the data compression process, it reduces the storage requirements of analysis section. Then, we just focus on the back-end hardware compression algorithm for data recovery reconstruction work. Based on the above compression algorithm, the restore reconstructed of the compressed signal can be realized through 0-minimum-norm by

$$\begin{aligned} \min_x \quad & \|x\|_0 \\ \text{s.t.} \quad & y = \phi x, \end{aligned} \quad (6)$$

where x denotes the sparse signal with reconstruction; y is the restored signal after x's observations; 0-minimum-norm indicates the number of nonzero elements. The results of CS in sampling are as shown in Figure 5.

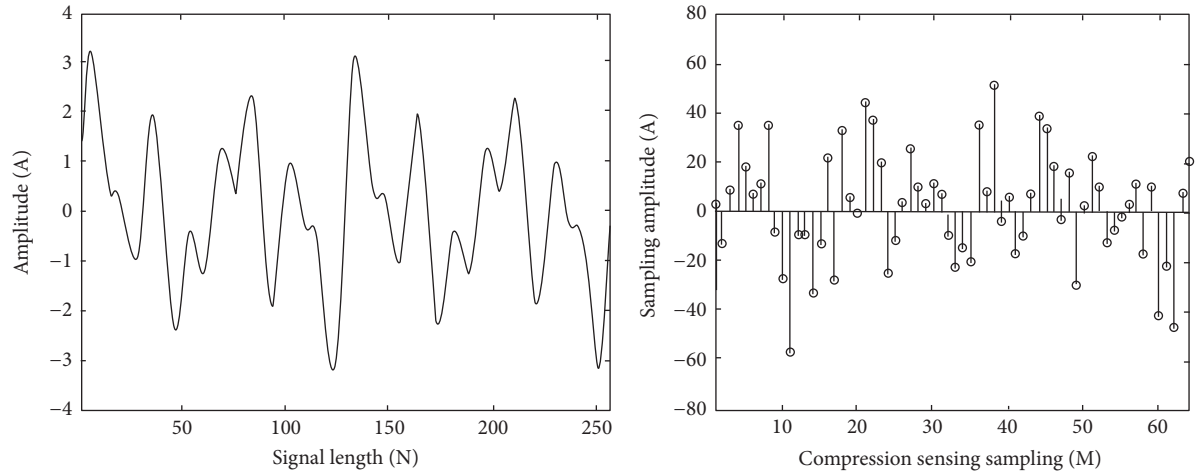
3.2. CS Channel Estimation. The traditional least squares channel estimation response is equal length pilot blocks by transmitting the channel impact, so that the transmitted signal and channel impulse response of linear convolution are converted to circular convolution; received vector can be written as

$$y = p * h + n, \quad (7)$$

where $*$ denotes the circular convolution; P is the transmitted pilot signal.

$$y = Ch + n. \quad (8)$$

After constructing an appropriate pilot signal, it transmits the test pilot signal C and couples power line at the transmitting terminal through couplers. However, the pilot signal is affected due to channel transmission characteristics of the power line and the power line noise. Figure 6 shows the estimation model in the pilot point.



(a) The original signal (b) The sampling signal by CS

Figure 5: Sampling process of CS.

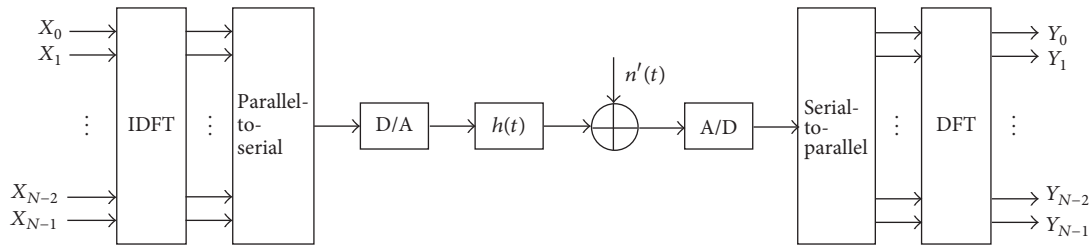


Figure 6: Pilot point channel estimation model.

Therefore, we just focus on the model and disturb signal by noise in the receiving end through couplers as described in

$$\begin{bmatrix} y_0 \\ y_1 \\ \vdots \\ y_{M-2} \\ y_{M-1} \end{bmatrix}_{M\times 1} = \begin{bmatrix} c_0 & & c_1 \\ c_1 & \ddots & c_2 \\ \vdots & & \vdots \\ c_{M-1} & \ddots & c_M \\ c_M & & c_0 \end{bmatrix}_{M\times N} \begin{bmatrix} h_0 \\ h_1 \\ \vdots \\ h_{N-2} \\ h_{N-1} \end{bmatrix}_{N\times 1} + \begin{bmatrix} n_0 \\ n_1 \\ \vdots \\ n_{M-2} \\ n_{M-1} \end{bmatrix}_{M\times 1}. \quad (9)$$

Assume the available power line communication channel characteristics y are at receiving end; we employ the sensing reconstruction algorithm (OMP, Orthogonal Matching Pursuit Algorithm) to estimate the power line channel impulse response $h(t)$.

OMP algorithm is the improved algorithm of MP algorithm. OMP algorithm selects and observes the most closely matched atom signal from the atom library as OM algorithm. The orthogonality will make the selected atom not be repeated in the OMP algorithm iterative process, which ensures the optimality of iteration and thereby reduces the number of iterations and good reconstruction.

The restored reconstruction of OMP is as follows:

(1) Initialization is as follows: residual value $r_0 = y$, index set $\Lambda_0 = \Phi$, and iterations $i = 1$, $\Gamma_0 = \Phi$.

(2) Determine index value: $\lambda_{i+1} = \arg\max|\langle r_i, \tau_j\rangle|$, where τ_j is column j on matrix Φ; determine the position of the corresponding atom, that is, the position of nonzero element: $\{\Lambda_{i+1} = \Lambda_i \cup \lambda_{i+1}\}$, $\{\Gamma_{i+1} = \Gamma_i \cup \tau\lambda_{i+1}\}$.

(3) LS algorithm is used to obtain new estimates:

$$\hat{x}_{i+1} = \arg\min \left\| y - \Gamma_{i+1}\hat{x} \right\| = {\Gamma_{i+1}}^{+} x. \quad (10)$$

in which + is devoted pseudoinverse.

(4) Calculate the new residual value: $r_{i+1} = y - \Gamma_{i+1}\hat{x}_{i+1}$.

(5) Optimize the iterative process: construct loop $i = i + 1$, and then repeat the indexing process until the completion of the required number m of iterations to terminate the iteration.

(6) Complete signal reconstruction: the calculated estimated value satisfies equality as $\hat{x}_{\Lambda_m} = \hat{x}_m$ and $\hat{x}_{\{1,\ldots,2N\}-\Lambda_m} = 0$.

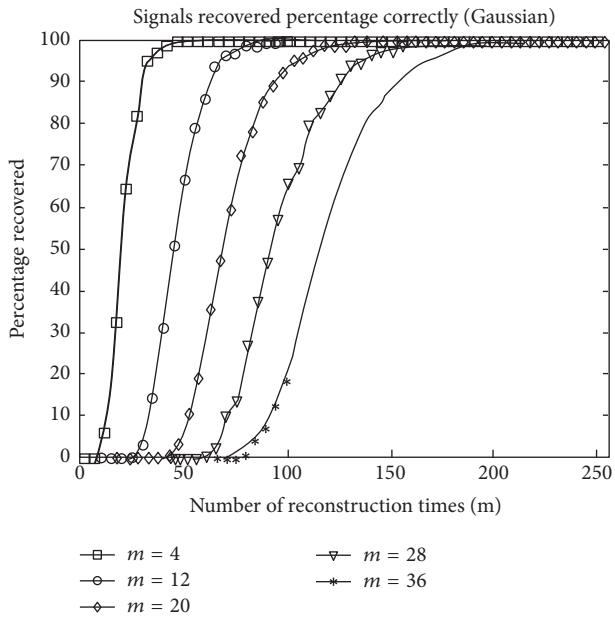


Figure 7: OMP multireconstruction.

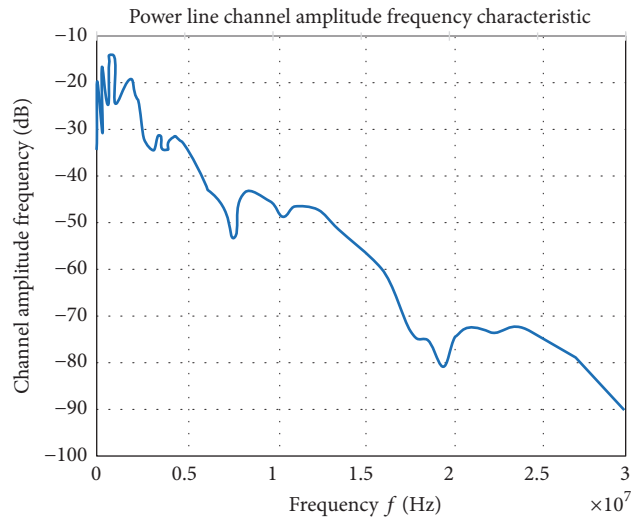


Figure 8: Amplitude frequency response of reference channel.

Table 2: Parameters list.

Parameters	Value
Bandwidth simulation	$B_W = 30$ MHz
Sampling frequency	$f_s = 60$ MHz
Sampling time	$t = 10\,\mu$s

In each interaction, OMP algorithm obtains a nonzero element corresponding position in x and calculates the value of this element. After m iterations, it can get the estimation value $\hat{x}$, and then it estimates the power line channel impulse response. The reconstruction is as shown in Figure 7.

4. Simulation Result

Based on Matlab simulation platform, we built the simulation environment and simulated the power line channel impulse response. PLC channel frequency domain response is in 15 paths, and the longest path is 1000 m in the channel model. And based on the least squares channel estimation of the pilot sequences and CS-based power line channel estimation, we analyze the simulation results under the same conditions.

To build the simulation environment, we refer to the reference communication channel parameters and simulate the time-domain characteristics of power line reference communication channel. The parameters are shown in Table 2.

4.1. Different SNR (Signal to Noise Ratio). Power line noises are very complex; they can be roughly divided into five categories in the time domain: the colored background noise, narrowband noise, asynchronous to power frequency periodic impulse noise, synchronized to power frequency periodic impulse noise, and sudden impulse noise.

In implementation of the project, the average power of noises, the colored background noise, narrowband noise, and asynchronous to power frequency periodic impulse noise, are small. And these three noises time-varying characteristics are weak; they change slowly with time in the entire PLC carrier communication frequency band. Thus, they can be called background noise. Meanwhile, the average power synchronization frequency periodic pulse noise and sudden impulse noise are relatively large. And there are two noises changes, frequently and randomly. They thus are called random impulse noise. Although the random impulse noise appears little, this type of noise greatly affects the quality of communication. It usually causes the narrowband communication interruption. Therefore, we just consider the superposition persistence of background noise in the channel in simulation.

Based on the impulse response of power line channel, we built the suitable pilot signal matrix. The dimensions of fixed reception signal are as follows: M 50 and N 200. And due to the interference of power line channel by background noise, the signal to noise ratio changes are from 5 dB to 30 dB.

As shown in Figures 8 and 9, compared to the traditional least squares channel estimation, CS channel estimation has a better estimation by the compressed sensing technology in the low SNR and hostile environment. The estimation error is less than tenfold the traditional least squares channel estimation algorithm. As the SNR increases and the channel environment tends to be better, the least squares channel estimation and compressive sensing-based channel estimation can achieve good estimation. However, compared to compressive sensing-based channel estimation, the least squares estimation needs longer pilot signal, more data computation, and longer calculation time.

4.2. Different Compression Dimension. Based on the impulse response of power line channel, we built the suitable pilot signal matrix again. For the dimensions of fixed reception signal, we increase M from 50 to 150 gradually and N is at 200.

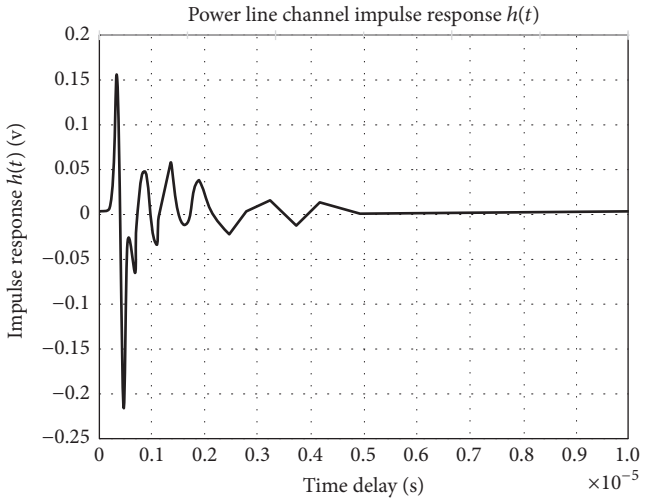


Figure 9: Impulse response of reference channel.

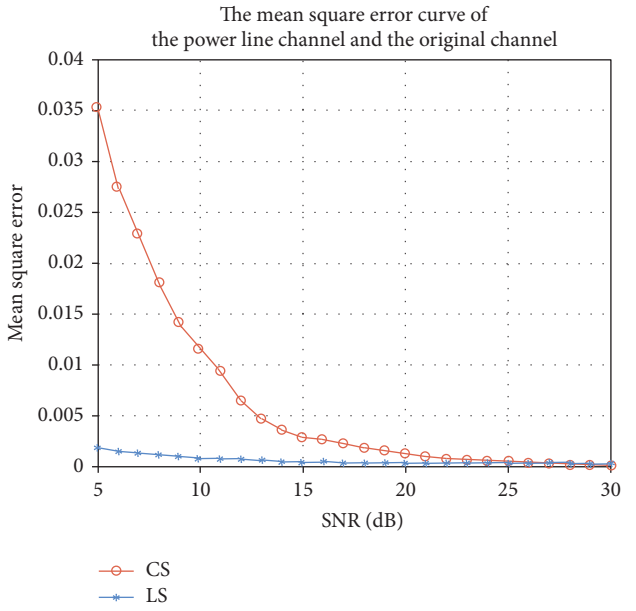


Figure 10: Performance comparison of CS and LS (SNR).

Meanwhile, we added the noise power line channel and fixed the noise ratio at 15 dB.

As shown in Figures 10 and 11, in the unchanged situation of the power line signal to noise ratio, with the increasing of received signals' dimension of M, these two methods performance of power line channel estimation is improved. However, due to the sparsity of power line channel, CS-based power line channel estimation adopts the sparsity to improve the efficient and accurate estimation of the power line channel characteristics, which achieves better channel restoration reconstruction.

However, with the growing pilot sequences, the pilot signal-based least squares channel estimation method can achieve good channel estimation. However, compared to the former, the compressed sensing-based power line channel

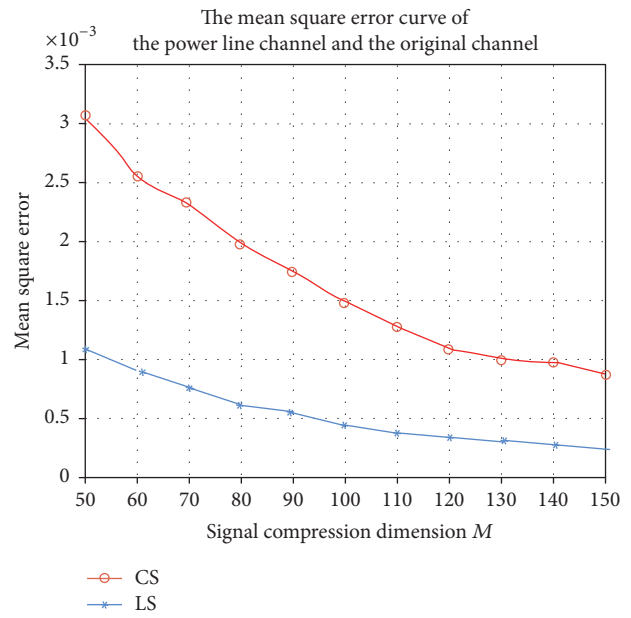


Figure 11: Performance comparison of CS and LS (M).

estimation algorithm has advantages and achieves compression objective data.

5. Conclusion

In this paper, we analyzed the sparsity of power line channel firstly. On this basis, we proposed a method of power line channel estimation based on compressive sensing. The simulation results show that this method used less pilot signal and fewer storage resources. However, the performance of the algorithm is better than the least square channel estimation algorithm. Therefore, the algorithm proposed in this paper has better application prospect.

In the future, we will still research various algorithms to improve the efficiency in compression sensing.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

References

[1] M. Yigit, V. C. Gungor, G. Tuna, M. Rangoussi, and E. Fadel, "Power line communication technologies for smart grid applications: a review of advances and challenges," *Computer Networks the International Journal of Computer & Telecommunications Networking*, vol. 70, no. 10, pp. 366–383, 2014.

[2] S. K. Shen, "Power line communication system and control method thereof," 2016.

[3] A. J. Hicks Iii, B. Davis, G. Howell et al., "Power-line communications," US20160148499, 2016.

[4] B. M. Propp and D. L. Propp, "Power line communication apparatus," U.S. Patent 4,815,106. 1989.

[5] M. Götz, M. Rapp, and K. Dostert, "Power line channel characteristics and their effect on communication system design," *IEEE Communications Magazine*, vol. 42, no. 4, pp. 78–86, 2004.

[6] M. Zamani, Z. Zhang, and C. Li, "Channel estimation for optical orthogonal frequency division multiplexing systems," 2016.

[7] P. L. Zhang, H. X. Zhang, H. D. Liu, Y. J. Zhang, P. F. He, and X. L. Pang, "Particle filtering based channel estimation in OFDM power line communication," *Journal of China Universities of Posts & Telecommunications*, vol. 21, no. 5, pp. 24–30, 2014.

[8] B. Yunus and H. Li, "Analysis of power quality waveform for data transmission efficiency over IEC 61850 communication standard," in *Proceedings of the 1st International Power and Energy Conference (PECon '06)*, pp. 161–166, November 2006.

[9] C. Tse, "Power quality meter and method of waveform anaylsis and compression," 2015.

[10] A. Rahim Abdullah, H. T. N. Ahmad, A. N. Abidullah et al., "Performance evaluation of real power quality disturbances analysis using s-transform," *Applied Mechanics & Materials*, vol. 753, no. 2015, pp. 1343–1348, 2015.

[11] D. L. Donoho, "Compressed sensing," *IEEE. Transactions on Information Theory*, vol. 52, no. 4, pp. 1289–1306, 2006.

[12] R. G. Baraniuk, "Compressive sensing," *IEEE Signal Processing Magazine*, vol. 24, no. 4, pp. 118–124, 2007.

[13] J. A. Tropp and A. C. Gilbert, "Signal recovery from random measurements via orthogonal matching pursuit," *IEEE. Transactions on Information Theory*, vol. 53, no. 12, pp. 4655–4666, 2007.

[14] D. Tralic and S. Grgic, "Signal reconstruction via compressive sensing," in *Proceedings of the 53rd International Symposium (ELMAR '11)*, pp. 5–9, Zadar, Croatia, September 2011.

[15] S. C. Yan and J. Qi, "Research on service impact analysis for power communication network based on N-1 principle," *Advanced Materials Research*, vol. 846-847, pp. 396–399, 2014.

[16] J. Y. Shin and J. C. Jeong, "Power line channel model considering adjacent nodes with reduced calculation complexity due to multipath signal propagation and network size using infinite geometric series and matrices," *Transactions of the Korean Institute of Electrical Engineers*, vol. 58, no. 2, pp. 248–255, 2009.

[17] A. Tomasoni, R. Riva, and S. Bellini, "Spatial correlation analysis and model for in-home MIMO power line channels," in *Proceedings of the 16th IEEE International Symposium on Power Line Communications and Its Applications (ISPLC '12)*, pp. 286–291, March 2012.

[18] J. Matanza, S. Alexandres, and C. Rodríguez-Morcillo, "Advanced metering infrastructure performance using European low-voltage power line communication networks," *IET Communications*, vol. 8, no. 7, pp. 1041–1047, 2014.

[19] Y. Xiao, J. Zhang, F. Pan, and Y. Shen, "Power line communication simulation considering cyclostationary noise for metering systems," *Journal of Circuits, Systems and Computers*, vol. 25, no. 9, Article ID 1650105, 2016.

[20] Y. Wang, Q. D. Wang, X. Z. Hou, H. L. Sun, X. M. Chen, and X. J. Li, "Measurement and research on attenuation characteristics of low voltage power line communication channel," *Advanced Materials Research*, vol. 986-987, pp. 2068–2072, 2014.

Hindawi
Journal of Electrical and Computer Engineering
Volume 2017, Article ID 4967232, 11 pages
https://doi.org/10.1155/2017/4967232

Research Article

Study of SAW Based on a Micro Force Sensor in Wireless Sensor Network

Jun Wang,[1] Yuanyuan Li,[1] Ke Chen,[1] Wenke Lu,[2] Qinghong Liu,[3] Haoxin Zhang,[3] and Huashan Yan[4]

[1] *College of Electronic and Electrical Engineering, Shanghai University of Engineering Science, Shanghai 201620, China*
[2] *Electronics and Information Engineering, Donghua University, Shanghai 201620, China*
[3] *Xi'an Leitong Science & Technology Co., Ltd., Xi'an 710049, China*
[4] *Shanghai Advanced Traction Battery Systems Co., Ltd., Shanghai 201805, China*

Correspondence should be addressed to Yuanyuan Li; liyuanyuanedu@163.com

Received 24 November 2016; Revised 7 March 2017; Accepted 15 March 2017; Published 19 April 2017

Academic Editor: Lu Liu

Wireless sensor network (WSN) technology has increasingly assumed an active role in detection, identification, location, and tracking applications after more than ten years of development. However, its application still suffers from technology bottlenecks, which must be solved and perfected to eliminate the key problems of the technology. This article investigates WSN acquisition nodes and analyzes the relationship between the frequency and actual pressure values of sensor nodes. The sensitive mechanism of the surface acoustic wave (SAW) based on a micro force sensor is researched, and the principle of least squares method is used to establish a transformation model of frequency and pressure for the SAW sensor. According to the model, polyfit function and matrix calculation are selected to solve and calculate the estimate of the polynomial coefficients, which simulate the data acquisition of WSN nodes and draw a polynomial curve fitting. The actual SAW sensor is tested to demonstrate the reasonableness of the device stability in WSNs.

1. Introduction

Wireless sensor network (WSN) technology has various applications in many disciplines and fields, such as communication, embedded computing, data processing, torrent analysis, and sensor technology. A set of integrated sensing, information processing, and communication units of wireless sensor nodes constitute WSNs without infrastructure [1]. Wireless sensor nodes in WSNs monitor and collect data in their coverage areas; they then collaborate with nodes and send the collected data to the coordinator nodes by multihop wireless through transmission channels [2]. The coordinator nodes then use the Internet or other channels to interact with users. WSNs have significant advantages in replacing traditional wired network transmission modes [3]. The important scientific and practical values of WSNs have gained much attention from many researchers and have been recognized as an emerging research field since the 2000s [4]. WSNs mix the logical information and real physical worlds together and transform the interaction between humans and nature [5, 6].

The monitoring environment is currently becoming increasingly complex. Simple data acquired by traditional sensor networks cannot meet the full requirements of environmental monitoring. Achieving fine-grained and accurate monitoring information is urgently needed. Actual application demands indicate that WSNs are usually composed of hundreds of sensor nodes, which are specifically or randomly deployed based on the interest within a particular geographical or physical area. These nodes sense factors in the external world, such as temperature, humidity, pressure, vibration, magnetic field, and light intensity; they also complete observations in target detection, identification, location, and tracking [7–10]. Surface acoustic wave (SAW) is an interdisciplinary subject that includes acoustics, electronics, piezoelectric materials, and semiconductor technology applied in the rapid development of large-scale integrated circuits of microelectronics, computer, silicon micromechanical processing,

semiconductor planar process, and laser technologies. SAW sensors have excellent properties, such as passivity, small size, low cost, excellent temperature stability, high reliability, and high reproducibility, which overcome the complicated algorithms and high power of VLSI [11, 12] and the large size and low reproducibility of optical devices [13]. The development of SAW based on a micro force sensor has been oriented toward intelligent wireless networks [14, 15]. Frequency and pressure conversion in the network optimization problem of SAW pressure sensors has become an urgent research topic. The method of implementing wavelet transform using SAW devices was first proposed by Zhu and Lu. Nowadays, micromanipulation has performed to design the precise pressure device in WSNs [16]. In order to design precise pressure devices in WSNs, micromanipulation is currently performed.

Different devices for intelligent and wireless networks have been developed and integrated. Lü established the force model whose device stability and precision of elastic modulus analysis should be improved [17]. Jungwirth described a micromechanical precision pressure sensor in delay lines [18]. Muntwyler designed a three-axis micro force sensor, which suffers from the problem of measurement uncertainty [19]. The present study constructs a SAW sensor based on a micro force sensor device on two sides and force-measuring elements that use a cantilever beam. The device is also equipped with single channel inductive components, and its electromagnetic field interference is more sensitive than that of others. Two inductors are placed at 90° to decrease the interference between them. A mathematical model is also established to analyze the frequency of the varied pressure. The SAW based on a micro force sensor has good linearity, consistency, and repeatability in performance within the scope of the effective measurement. It also uses the piezoelectric properties and temperature stability of crystals, which enhances the signal processing of this device in terms of its digital features and stable WSN performance.

The velocity and phase of the SAW based on a micro force sensor are changed after sensing the change in the quantity, which is generated by the interdigital transducer (IDT) of the SAW device. The output signal is directly measured by the network analyzer. The rest of this paper is organized as follows: Section 1 presents the background research on WSNs. Section 2 discusses the pressure-sensitive mechanism of a SAW based on a micro force sensor. Section 3 develops a simulation model using the principle of the least squares method. Sections 1–4 shift the focus of the study to the relationship between frequency and pressure, which in turn obtains the relationship between the output signal and sensing volume. Section 5 presents the testing and analysis of the SAW based on a micro force sensor used under different pressure levels. Section 6 analyzes temperature compensation of SAW based on a micro force sensor.

2. WSNs

2.1. Concept of WSNs. WSNs are a multihop self-organizing network system by wireless communication, which is composed of a large number of sensor nodes in monitoring areas [20]. Its purpose is to perceive, collect, and process the information of objects in the network and send it to observers.

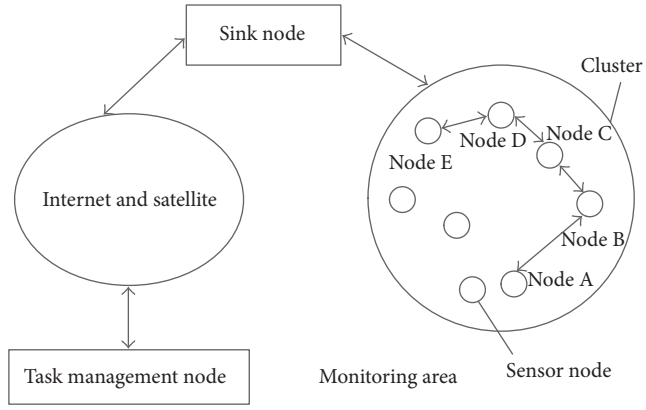


Figure 1: WSN architecture.

The structure of WSNs is shown in Figure 1. Sensor network system usually consists of sensor nodes, sink nodes, and management nodes.

In wireless sensor networks, sensor nodes are deployed in monitoring areas for automatic detection. Each sensor node sends out wireless signals and then constructs a network that supports dynamic topology in a self-organizing manner. In this network, the node has some association with cluster. In the cluster, usually according to certain rules, a sink node (such as nodes A, B, C, D, and E in Figure 1) is to be elected. The data is processed via the Internet or satellite system.

2.2. Wireless Sensor Network Node. Sensor node is the basic unit of wireless sensor network, which is composed of processor module, wireless communication module, sensor module, and power management module as shown in Figure 2. Sensor module is mainly composed of various types of sensors, AD/DC conversion module structure. Due to different physical signals, different types of sensors are used for data acquisition, and then data are transmitted to the processor module for processing. And the processor module is computing core of wireless sensor network node whose design requires miniaturization, low cost, stability, and security. Data communication protocols of sensor network in wireless communication module include physical layer, link layer, network layer, and application layer. The power management module not only provides the necessary energy for operation of sensor nodes, but also provides necessary power management to prolong the lifetime of wireless sensor networks.

WSNs have a very close correlation, and different applications require different network models, hardware platforms, and system software. In the design of sensor nodes, the following aspects should be considered.

(1) Miniaturization. Wireless sensor network node requirements are as small as possible on the volume, without affecting the performance of the system.

(2) Low Cost. Low cost is the basic requirement of WSN node.

(3) Stability and Security. Under conditions of given temperature, humidity, and pressure, each module of sensor node can work normally.

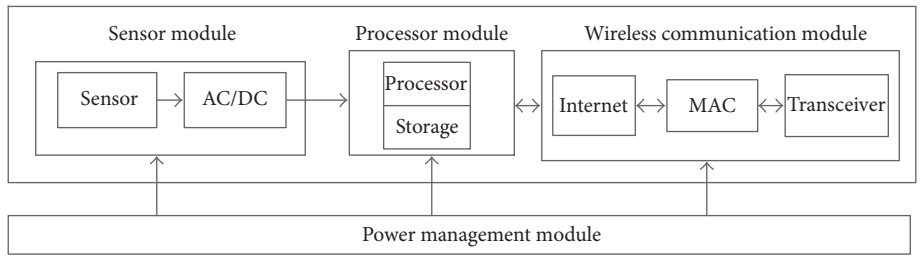


Figure 2: Sensor node architecture.

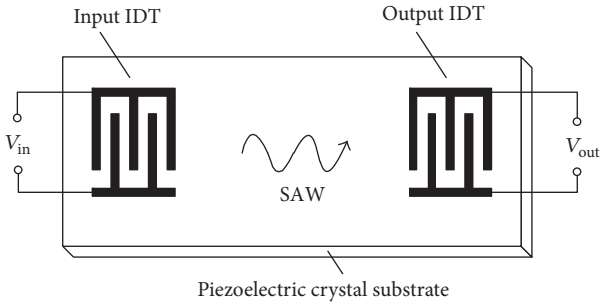


Figure 3: Schematic of the double-ended fixed sheet.

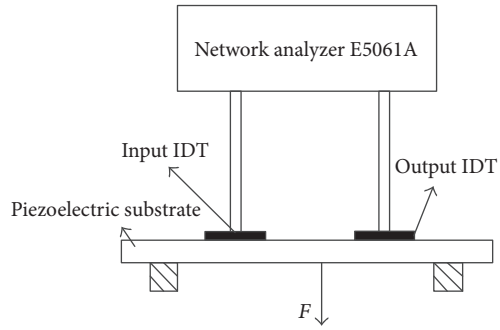


Figure 4: Schematic of the SAW-based micro force sensor.

SAW sensors have excellent properties, such as passivity, small size, low cost, excellent temperature stability, high reliability, and high reproducibility, whose development based on a micro force sensor has been oriented toward intelligent wireless networks. Therefore, it is highly possible to use SAW pressure sensors in wireless sensor networks.

3. SAW Based on a Micro Force Sensor

A SAW sensor is a new type of sensor that combines SAW, thin film, and electronic technology. This sensor translates different physical, chemical, and biomass information around SAW devices into changes in the SAW oscillator frequency by detecting the parameter variation in the frequency to monitor acceleration, temperature, humidity, pressure, shear, and bend. This device also uses the piezoelectric properties and temperature stability of crystals and the frequency signal instead of the conventional pressure sensor with a voltage signal. This approach enhances the signal processing of the device in terms of its digital feature and stable performance. SAW sensor technology is relatively mature at present; researchers have successfully developed pressure, temperature, mass, humidity, and gas sensors.

3.1. Principle of SAW Device. The basic structure of a SAW device is shown in Figure 3. This device manufactures two acoustic electric transducers on the piezoelectric characteristic substrate material-polishing surface, which is defined as the transmitting and receiving IDT (i.e., input and output IDT, resp.). An electrical signal applied on the input IDT generates an opposite polarity potential in two busbars such that an adjacent electric field is generated between two finger pair types. The piezoelectric material surface experiences strain in the electric field, when it affects the substrate with inverse piezoelectric. If the applied electrical signal is alternating, the deformation of the piezoelectric material surface propagates through the piezoelectric material surface; this process is called the SAW excitation process. It can produce an electric charge in certain directions of the piezoelectric materials through the output IDT excitation, which the SAW sensor propagates. Given the presence of the interdigital electrode, the charge accumulates on the electrode such that the output IDT busbars can check the corresponding electrical signal [21].

3.2. Basic Structure and Principle of a SAW Based on a Micro Force Sensor

3.2.1. Basic Structure of a SAW Based on a Micro Force Sensor. The output frequency of the SAW based on a micro force sensor is conducted using the network analyzer equipment E5061A. Force-measuring elements employ a cantilever beam loaded with a pressure of 0 kPa to 20 kPa as shown in Figure 4.

The piezoelectric substrate adopts a cantilever structure where two ends are fixed and the middle is loaded with micro-pressure. The cantilever experiences deformation when micro-pressure is loaded at the middle of the cantilever. The SAW propagation path is consequently changed. Otherwise, the output frequency is also changed and can detect the micro-pressure loaded on the cantilever.

3.2.2. Principle of Operation. The center frequency of the SAW device is f; the equation is as follows:

$$f = \frac{v}{\lambda}, \tag{1}$$

where v is the propagation velocity of the SAW on the surface of the piezoelectric substrate material and λ is the SAW length. Thus

$$v \approx \sqrt{\frac{E}{\rho}}, \tag{2}$$

where E is the elastic modulus of the piezoelectric substrate material and ρ is the density of the piezoelectric substrate material.

Equation (3) can be derived from (1) and (2) as follows:

$$f = \frac{\sqrt{E/\rho}}{\lambda}. \tag{3}$$

Given that the distribution of the IDT fingers is homogeneous, the relationship between the wavelength λ and distance d of the IDT fingers is as follows:

$$\lambda = 2d. \tag{4}$$

v_0 is the propagation velocity of the SAW that does not load the micro-pressure. λ_0, thus, is the SAW center frequency which is written as follows:

$$f_0 = \frac{v_0}{\lambda_0}. \tag{5}$$

The piezoelectric substrate of the cantilever structure experiences deformation when the micro-pressure F_m is loaded on two ends of the cantilever. The formula can be written as follows:

$$\delta = \frac{\Delta d}{d_0}. \tag{6}$$

The relationship between the distance d of the IDT fingers of the SAW device and the piezoelectric substrate deformation δ is as follows:

$$d(\delta) = d_0 + \Delta d = d_0 + \delta d_0 = d_0(1+\delta). \tag{7}$$

The following can be obtained from (4) and (7):

$$\lambda(\delta) = 2d(\delta) = 2d_0(1+\delta) = \lambda_0(1+\delta). \tag{8}$$

Equation (8) shows that when the micro-pressure is loaded at the middle of the cantilever, the SAW length that propagates along the piezoelectric substrate increases.

Equation (1) shows that the micro-pressure loaded on the cantilever changes the material density ρ and velocity of the SAW pressure sensor. The relationship between δ and v can be expressed as follows:

$$v(\delta) = v_0(1 + K\delta), \tag{9}$$

where K is a constant of the piezoelectric substrate material.

The function relationship between the output frequency of the SAW based on a micro force sensor and the piezoelectric substrate deformation can be obtained by substituting (8) and (9) in (5):

$$f(\delta) = \frac{v(\delta)}{\lambda(\delta)} = \frac{v_0(1+K\delta)}{\lambda_0(1+\delta)}. \tag{10}$$

The output frequency Δf is then equal to the following equation:

$$\Delta f = f(\delta) - f_0 = f_0\left(\frac{1+K\delta}{1+\delta} - 1\right) = f_0\frac{\delta(K-1)}{1+\delta}. \tag{11}$$

Given that the cantilever experiences deformation $\delta \ll 1$ at the micro-pressure $1 + \delta \approx 1$, (10) is rewritten as

$$\Delta f = f(\delta) - f_0 \approx f_0\delta(K-1). \tag{12}$$

The following equation is then obtained:

$$f(\delta) = \Delta f + f_0 \approx f_0[1 + \delta(K-1)]. \tag{13}$$

Equation (13) shows that the sensor output frequency changes the variety of cantilever deformation when the substrate material constant is determined. In other words, using the SAW drift output frequency can measure the micro-pressure weight loaded on the sensor cantilever.

4. Creating and Solving the Linear Regression Model of a SAW Based on a Micro Force Sensor

4.1. Establishing the Model. According to the SAW based on a micro force sensor, input variable (micro-pressure) and output variable (frequency) can be recorded. The difference between the input and output variables is the linear function relationship established in what follows. From (13), the function relationship between the micro-pressure loaded on the sensor (F_m) and the difference frequency (Δf) of the output frequency can be written as follows:

$$F(\Delta f) = k_0 + k_1\Delta f + k_2\Delta f^2 + k_3\Delta f^3 + \cdots + k_n\Delta f^n \cdots. \tag{14}$$

The least squares method can be used to solve (14) [22].

Given the experimental data sample ($F_i, \Delta f_i$ $i = 1, 2, \ldots, n$) and setting $n = 6$, (14) is equal to

$$F_i = k_0 + k_1\Delta f_i + k_2\Delta f_i^2 + k_3\Delta f_i^3 + k_4\Delta f_i^4 + k_5\Delta f_i^5 + k_6\Delta f_i^6, \tag{15}$$

where the regression coefficients k_0, k_1, k_2, k_3, k_4, k_5, and k_6 can be estimated using the least squares.

4.2. Least Squares. A series of data pairs, such as ($x_1, y_1, x_2, y_2, \ldots, x_m, y_m$), can generally be obtained using the principle of the least squares method and by researching the relationship of the two variables (x, y). If these points are nearly a straight line, we can set the line equation that describes the data in the x-y Cartesian coordinate system as follows:

$$Y_j = a_0 + a_1X, \tag{16}$$

where a_0 and a_1 are arbitrary real numbers.

Establishing a linear equation to determine a_0 and a_1 is necessary to obtain the sum of squares of the deviations $\sum(Y_i - Y_j)^2$ of the measured value Y_j and the calculated value Y_j from (16) as follows:

$$Q = \sum\left(Y_i - Y_j\right)^2. \tag{17}$$

According to the least squares method, Q is the sum of variance between the predicted dependent variable and its actual value.

The following equation is obtained by substituting (16) in (17):

$$Q = \sum \left(Y_i - a_0 - a_1 X_i\right)^2. \tag{18}$$

The partial derivatives of a_0 and a_1 can be calculated using the function Q, when $\sum(Y_i - Y_j)^2$ is at its minimum. The two partial derivatives are set to equal zero:

$$\left.\frac{\partial Q\left(a_0, a_1\right)}{\partial a_0}\right|_{a_0=\widehat{a_0}} = 0,$$
$$\left.\frac{\partial Q\left(a_0, a_1\right)}{\partial a_1}\right|_{a_1=\widehat{a_1}} = 0. \tag{19}$$

Thus,

$$\sum a_0 + a_1 \sum X_i = \sum Y_i,$$
$$a_0 \sum X_i + a_1 \sum {X_i}^2 = \sum X_i Y_i. \tag{20}$$

The two equations of the unknown a_0 and a_1 can be calculated and (16) solved [23].

4.3. Analysis of Solving the Model. According to the least squares method in (16) to (20), the sum of the variances Q between the predicted value F_i and the actual value F in (15) is given as

$$Q\left(k_0 - k_6\right) = \sum_{i=1}^{N} {\Delta_i}^2 = \sum_{i=1}^{N} \left[F_i - F\right]^2, \tag{21}$$

where N is the sampling point of the independent variables. The least squares estimation therefore calculates the minimum value of Q, which implies that $\widehat{k_0}$, $\widehat{k_1}$, $\widehat{k_2}$, $\widehat{k_3}$, $\widehat{k_4}$, $\widehat{k_5}$, and $\widehat{k_6}$ must be suitable for the following equation:

$$\begin{aligned} Q\left(\widehat{k_0}, \widehat{k_1}, \widehat{k_2}, \widehat{k_3}, \widehat{k_4}, \widehat{k_5}, \widehat{k_6}\right) &= \sum_{i=1}^{N} \left[F_i - F\right]^2 \\ &= \min_{\widehat{k_0}-\widehat{k_i}} \sum_{i=1}^{N} \left[F_i - F\right]^2 = \min_{\widehat{k_0}-\widehat{k_6}} \sum_{i=1}^{N} \left[k_0 + k_1 \Delta f_i + k_2 \Delta {f_i}^2\right. \\ &\quad \left. + k_3 \Delta {f_i}^3 + k_4 \Delta {f_i}^4 + k_5 \Delta {f_i}^5 + k_6 \Delta {f_i}^6 - F\right]^2, \end{aligned} \tag{22}$$

where $\widehat{k_0}$, $\widehat{k_1}$, $\widehat{k_2}$, $\widehat{k_3}$, $\widehat{k_4}$, $\widehat{k_5}$, and $\widehat{k_6}$ are the least squares estimations of k_0, k_1, k_2, k_3, k_4, k_5, and k_6, respectively.

Setting the equations

$$\begin{aligned} \left.\frac{\partial Q\left(k_0, k_1, k_2, k_3, k_4, k_5\right)}{\partial k_0}\right|_{k_0=\widehat{k_0}} &= 0, \\ \left.\frac{\partial Q\left(k_0, k_1, k_2, k_3, k_4, k_5\right)}{\partial k_1}\right|_{k_0=\widehat{k_1}} &= 0, \\ \left.\frac{\partial Q\left(k_0, k_1, k_2, k_3, k_4, k_5\right)}{\partial k_2}\right|_{k_0=\widehat{k_2}} &= 0, \\ \left.\frac{\partial Q\left(k_0, k_1, k_2, k_3, k_4, k_5\right)}{\partial k_3}\right|_{k_0=\widehat{k_3}} &= 0, \\ \left.\frac{\partial Q\left(k_0, k_1, k_2, k_3, k_4, k_5\right)}{\partial k_4}\right|_{k_0=\widehat{k_4}} &= 0, \\ \left.\frac{\partial Q\left(k_0, k_1, k_2, k_3, k_4, k_5\right)}{\partial k_5}\right|_{k_0=\widehat{k_5}} &= 0, \\ \left.\frac{\partial Q\left(k_0, k_1, k_2, k_3, k_4, k_5\right)}{\partial k_6}\right|_{k_0=\widehat{k_6}} &= 0, \end{aligned} \tag{23}$$

we can obtain the following:

$$\begin{aligned} &\sum_{i=1}^{N} \left[\left(\widehat{k_0} + \widehat{k_1}\Delta f_i + \widehat{k_2}\Delta f_i^2 + \widehat{k_3}\Delta f_i^3 + \widehat{k_4}\Delta f_i^4 + \widehat{k_5}\Delta f_i^5 \right.\right. \\ &\quad \left.\left. + \widehat{k_6}\Delta f_i^6\right) - F_i\right] = 0, \\ &\sum_{i=1}^{N} \left[\left(\widehat{k_0} + \widehat{k_1}\Delta f_i + \widehat{k_2}\Delta f_i^2 + \widehat{k_3}\Delta f_i^3 + \widehat{k_4}\Delta f_i^4 + \widehat{k_5}\Delta f_i^5 \right.\right. \\ &\quad \left.\left. + \widehat{k_6}\Delta f_i^6\right) - F_i\right] \Delta f_i = 0, \\ &\sum_{i=1}^{N} \left[\left(\widehat{k_0} + \widehat{k_1}\Delta f_i + \widehat{k_2}\Delta f_i^2 + \widehat{k_3}\Delta f_i^3 + \widehat{k_4}\Delta f_i^4 + \widehat{k_5}\Delta f_i^5 \right.\right. \\ &\quad \left.\left. + \widehat{k_6}\Delta f_i^6\right) - F_i\right] \Delta f_i^2 = 0, \\ &\sum_{i=1}^{N} \left[\left(\widehat{k_0} + \widehat{k_1}\Delta f_i + \widehat{k_2}\Delta f_i^2 + \widehat{k_3}\Delta f_i^3 + \widehat{k_4}\Delta f_i^4 + \widehat{k_5}\Delta f_i^5 \right.\right. \\ &\quad \left.\left. + \widehat{k_6}\Delta f_i^6\right) - F_i\right] \Delta f_i^3 = 0, \\ &\sum_{i=1}^{N} \left[\left(\widehat{k_0} + \widehat{k_1}\Delta f_i + \widehat{k_2}\Delta f_i^2 + \widehat{k_3}\Delta f_i^3 + \widehat{k_4}\Delta f_i^4 + \widehat{k_5}\Delta f_i^5 \right.\right. \\ &\quad \left.\left. + \widehat{k_6}\Delta f_i^6\right) - F_i\right] \Delta f_i^4 = 0, \\ &\sum_{i=1}^{N} \left[\left(\widehat{k_0} + \widehat{k_1}\Delta f_i + \widehat{k_2}\Delta f_i^2 + \widehat{k_3}\Delta f_i^3 + \widehat{k_4}\Delta f_i^4 + \widehat{k_5}\Delta f_i^5 \right.\right. \\ &\quad \left.\left. + \widehat{k_6}\Delta f_i^6\right) - F_i\right] \Delta f_i^5 = 0, \\ &\sum_{i=1}^{N} \left[\left(\widehat{k_0} + \widehat{k_1}\Delta f_i + \widehat{k_2}\Delta f_i^2 + \widehat{k_3}\Delta f_i^3 + \widehat{k_4}\Delta f_i^4 + \widehat{k_5}\Delta f_i^5 \right.\right. \\ &\quad \left.\left. + \widehat{k_6}\Delta f_i^6\right) - F_i\right] \Delta f_i^6 = 0. \end{aligned} \tag{24}$$

Further simplifying the said equations we obtain the following:

$$
\begin{aligned}
&N\widehat{k_0} + \widehat{k_1}\sum_{i=1}^{N}\Delta f_i + \widehat{k_2}\sum_{i=1}^{N}\Delta f^2{}_i + \widehat{k_3}\sum_{i=1}^{N}\Delta f_i{}^3 + \widehat{k_4}\sum_{i=1}^{N}\Delta f_i{}^4 \\
&\quad + \widehat{k_5}\sum_{i=1}^{N}\Delta f_i{}^5 + \widehat{k_6}\sum_{i=1}^{N}\Delta f_i{}^6 = \sum_{i=1}^{N}F_i, \\
&\widehat{k_0}\sum_{i=1}^{N}\Delta f_i + \widehat{k_1}\sum_{i=1}^{N}\Delta f^2{}_i + \widehat{k_2}\sum_{i=1}^{N}\Delta f_i{}^3 + \widehat{k_3}\sum_{i=1}^{N}\Delta f_i{}^4 \\
&\quad + \widehat{k_4}\sum_{i=1}^{N}\Delta f_i{}^5 + \widehat{k_5}\sum_{i=1}^{N}\Delta f_i{}^6 + \widehat{k_6}\sum_{i=1}^{N}\Delta f_i{}^7 = \sum_{i=1}^{N}F_i\Delta f_i, \\
&\widehat{k_0}\sum_{i=1}^{N}\Delta f_i{}^2 + \widehat{k_1}\sum_{i=1}^{N}\Delta f^3{}_i + \widehat{k_2}\sum_{i=1}^{N}\Delta f_i{}^4 + \widehat{k_3}\sum_{i=1}^{N}\Delta f_i{}^5 \\
&\quad + \widehat{k_4}\sum_{i=1}^{N}\Delta f_i{}^6 + \widehat{k_5}\sum_{i=1}^{N}\Delta f_i{}^7 + \widehat{k_6}\sum_{i=1}^{N}\Delta f_i{}^8 = \sum_{i=1}^{N}F_i\Delta f_i{}^2, \\
&\widehat{k_0}\sum_{i=1}^{N}\Delta f_i{}^3 + \widehat{k_1}\sum_{i=1}^{N}\Delta f^4{}_i + \widehat{k_2}\sum_{i=1}^{N}\Delta f_i{}^5 + \widehat{k_3}\sum_{i=1}^{N}\Delta f_i{}^6 \\
&\quad + \widehat{k_4}\sum_{i=1}^{N}\Delta f_i{}^7 + \widehat{k_5}\sum_{i=1}^{N}\Delta f_i{}^8 + \widehat{k_6}\sum_{i=1}^{N}\Delta f_i{}^9 = \sum_{i=1}^{N}F_i\Delta f_i{}^3, \qquad (25) \\
&\widehat{k_0}\sum_{i=1}^{N}\Delta f_i{}^4 + \widehat{k_1}\sum_{i=1}^{N}\Delta f^5{}_i + \widehat{k_2}\sum_{i=1}^{N}\Delta f_i{}^6 + \widehat{k_3}\sum_{i=1}^{N}\Delta f_i{}^7 \\
&\quad + \widehat{k_4}\sum_{i=1}^{N}\Delta f_i{}^8 + \widehat{k_5}\sum_{i=1}^{N}\Delta f_i{}^9 + \widehat{k_6}\sum_{i=1}^{N}\Delta f_i{}^{10} = \sum_{i=1}^{N}F_i\Delta f_i{}^4, \\
&\widehat{k_0}\sum_{i=1}^{N}\Delta f_i{}^5 + \widehat{k_1}\sum_{i=1}^{N}\Delta f^6{}_i + \widehat{k_2}\sum_{i=1}^{N}\Delta f_i{}^7 + \widehat{k_3}\sum_{i=1}^{N}\Delta f_i{}^8 \\
&\quad + \widehat{k_4}\sum_{i=1}^{N}\Delta f_i{}^9 + \widehat{k_5}\sum_{i=1}^{N}\Delta f_i{}^{10} + \widehat{k_6}\sum_{i=1}^{N}\Delta f_i{}^{11} = \sum_{i=1}^{N}F_i\Delta f_i{}^5, \\
&\widehat{k_0}\sum_{i=1}^{N}\Delta f_i{}^6 + \widehat{k_1}\sum_{i=1}^{N}\Delta f^7{}_i + \widehat{k_2}\sum_{i=1}^{N}\Delta f_i{}^8 + \widehat{k_3}\sum_{i=1}^{N}\Delta f_i{}^9 \\
&\quad + \widehat{k_4}\sum_{i=1}^{N}\Delta f_i{}^{10} + \widehat{k_5}\sum_{i=1}^{N}\Delta f_i{}^{11} \\
&\quad + \widehat{k_6}\sum_{i=1}^{N}\Delta f_i{}^{12} = \sum_{i=1}^{N}F_i\Delta f_i{}^6.
\end{aligned}
$$

The following equations are set:

$$
\begin{aligned}
A &= \sum_{i=1}^{N}\Delta f_i, \\
B &= \sum_{i=1}^{N}\Delta f^2{}_i, \\
C &= \sum_{i=1}^{N}\Delta f_i{}^3, \\
D &= \sum_{i=1}^{N}\Delta f_i{}^4, \\
E &= \sum_{i=1}^{N}\Delta f_i{}^5, \\
F &= \sum_{i=1}^{N}\Delta f_i{}^6, \\
G &= \sum_{i=1}^{N}\Delta f_i{}^7, \\
H &= \sum_{i=1}^{N}\Delta f_i{}^8, \\
I &= \sum_{i=1}^{N}\Delta f_i{}^9, \\
J &= \sum_{i=1}^{N}\Delta f_i{}^{10}, \\
K &= \sum_{i=1}^{N}\Delta f_i{}^{11}, \\
L &= \sum_{i=1}^{N}\Delta f_i{}^{12}, \\
M &= \sum_{i=1}^{N}F_i, \\
P &= \sum_{i=1}^{N}F_i\Delta f_i, \\
Q &= \sum_{i=1}^{N}F_i\Delta f_i{}^2, \\
R &= \sum_{i=1}^{N}F_i\Delta f_i{}^3 \\
S &= \sum_{i=1}^{N}F_i\Delta f_i{}^4, \\
T &= \sum_{i=1}^{N}F_i\Delta f_i{}^5, \\
U &= \sum_{i=1}^{N}F_i\Delta f_i{}^6.
\end{aligned} \qquad (26)
$$

Equation (25) can be written as follows:

$$
\begin{aligned}
&N\widehat{k_0} + A\widehat{k_1} + B\widehat{k_2} + C\widehat{k_3} + D\widehat{k_4} + E\widehat{k_5} + F\widehat{k_6} = M, \\
&A\widehat{k_0} + B\widehat{k_1} + C\widehat{k_2} + D\widehat{k_3} + E\widehat{k_4} + F\widehat{k_5} + G\widehat{k_6} = P, \\
&B\widehat{k_0} + C\widehat{k_1} + D\widehat{k_2} + E\widehat{k_3} + F\widehat{k_4} + G\widehat{k_5} + H\widehat{k_6} = Q, \\
&C\widehat{k_0} + D\widehat{k_1} + E\widehat{k_2} + F\widehat{k_3} + G\widehat{k_4} + H\widehat{k_5} + I\widehat{k_6} = R, \\
&D\widehat{k_0} + E\widehat{k_1} + F\widehat{k_2} + G\widehat{k_3} + H\widehat{k_4} + I\widehat{k_5} + J\widehat{k_6} = S,
\end{aligned}
$$

Table 1: Frequency and pressure experiment data.

F_m (kPa)	f (MHz)	f (MHz)	Δf (Hz)
0	40.784663	40.784744	81
1	40.788365	40.788453	88
2	40.787996	40.788086	90
3	40.788788	40.788881	93
4	40.790232	40.790326	94
5	40.789643	40.789746	103
6	40.788437	40.788542	105
7	40.790993	40.791100	107
8	40.788762	40.788871	109
9	40.790272	40.790385	113
10	40.790215	40.790331	116
11	40.788104	40.788221	117
12	40.788600	40.788721	121
13	40.789033	40.789155	122
14	40.788988	40.789112	124
15	40.787255	40.787383	128
16	40.788580	40.788712	132
17	40.784916	40.785051	135
18	40.786062	40.786201	139
19	40.786068	40.786211	143
20	40.785977	40.786124	147

$$\begin{aligned} E\widehat{k_0} + F\widehat{k_1} + G\widehat{k_2} + H\widehat{k_3} + I\widehat{k_4} + J\widehat{k_5} + K\widehat{k_6} &= T, \\ F\widehat{k_0} + G\widehat{k_1} + H\widehat{k_2} + I\widehat{k_3} + J\widehat{k_4} + K\widehat{k_5} + L\widehat{k_6} &= U. \end{aligned} \tag{27}$$

Solving (27) yields the estimated value $\widehat{k_0}$–$\widehat{k_6}$ of the parameters k_0–k_6 of the regression analysis model shown in (15). The input and output variable regression of the SAW based on a micro force sensor can be calculated by solving (15).

4.4. Model Solution

4.4.1. Experimental Setup. On the basis of previous study, different size sensors were fabricated. Then, the network analyzer E5061A is used for testing (Figure 6).

Force-measuring elements employ a cantilever beam loaded with a pressure of 0 kPa to 20 kPa; a pressure of 1 kPa is added to the beam each time. Because of the fluctuation of the frequency in the measurement, it is necessary to read the data after a period of time, and the more the data is, the more accurate the frequency conversion formula will be.

Environment of equipment is not complicated; the test can be operated on the experimental platform. And there is no special requirement for operators; they need to operate carefully.

4.4.2. Experimental Data. The experimental data were measured in the laboratory as shown in Table 1 [24]. F_m (kPa) is the acting force on the piezoelectric substrate, f is the minimum and maximum frequencies tested by the network analyzer, and Δf is the difference between the maximum and minimum frequencies.

4.4.3. Selecting the Degree of Polynomial Fitting. This study uses six-degree polynomial fitting, which can be proven directly by the polynomial fitting procedure three to seven times. The main program is as follows:

x = [81, 88, 90, 93, 94, 103, 105, 107, 109, 113, 116, 117, 121, 122, 124, 128, 132, 135, 139, 143, 147];

y = [0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20];

P = zeros(5, 7); % Define the matrix size

for k = 2 : 6; % 3 to 7 times fitting

[Pt, S] = polyfit(x, y, k); % Polynomial fitting

$P(k-1, 1 : k+1) = Pt$; % Assign Pt to matrix P

Y = polyval(Pt, x, S); % Calculate the fitting values of x

$Dt(k-1)$ = std($Y-y$); % Calculate the standard deviation between the fitting value and original data

end

Results are as follows:

Columns 1 to 5

0.576165303485416

0.405216710673834

0.393676218911461

0.364152373789325

0.347679434090903.

The variance decreases rapidly when the polynomial number is more than 5. The increase in the number also quickly decreases the errors. Thus, a six-degree polynomial fits the laboratory data.

4.4.4. Solving the Polyfit Function. This study constructs an analytic function based on the principle of curve fitting, which is the polynomial $y = a_1x^n + a_2x^{n-1} + \cdots + a_nx + a_{n+1}$. This function ensures that the original discrete points on the data set are as close as possible to the given value. After solving the function, the following fitted values are obtained:

$$\begin{aligned} p = {} & 4.192893268467821e-09, \\ & -2.793471478615071e \\ & -06, 7.674258962870516e-04, \\ & -0.111309364487564, 8.994744948450235, \\ & -3.839297860714657e \\ & +02, 6.758923327690160e+03, \end{aligned} \tag{28}$$

$$\begin{aligned} y = {} & [0.000000004192893268467821 08, \\ & -0.000027934714786150705 4, \\ & 0.00076742589628705159 5, \\ & -0.111309364487563539, 8.99474494845023465, \\ & -383.929786071465742, 6758.92332769015957]. \end{aligned}$$

% in the form of diminishing a dimension provides the fitting polynomial coefficients.

4.4.5. Matrix Calculation. Solving (16) requires the calculation of an approach to a computed matrix in MATLAB. The obtained results are given polynomial coefficients in the form of an increasing dimension number.

The value of $\widehat{k_0}$–$\widehat{k_6}$ is as follows:

$$\begin{aligned} x1 &= 6633.023822460154, \\ &\quad - 384.0079835318029, 8.905647996212356, \\ &\quad - 0.114164102269569, 0.000710263767188689, \\ &\quad - 0.000002698678654041, 0.0000000040823517085. \end{aligned} \tag{29}$$

The results of y that retain 18 significant figures are as follows:

$$\begin{aligned} y &= 6.633023822460154e + 3, \\ &\quad - 3.840079835318029e \\ &\quad + 2, 8.905647996212356, \\ &\quad - 0.114164102269569, 0.710263767188689e \\ &\quad - 3, -0.2698678654041e - 5, 0.40823517085e \\ &\quad - 8. \end{aligned} \tag{30}$$

5. Fitting Results and Curve

The following arithmetic formula is obtained using the matrix method to solve the final frequency pressure polynomial:

$$\begin{aligned} F(\Delta f) &= 6.6330 \times 10^3 - 3.8401 \times 10^2 \Delta f_i \\ &\quad + 8.9056 \Delta f_i^2 - 0.1142 \Delta f_i^3 + 0.7102 \\ &\quad \times 10^{-3} \Delta f_i^4 - 0.2698 \times 10^{-5} \Delta f_i^5 + 0.4082 \\ &\quad \times 10^{-8} \Delta f_i^6. \end{aligned} \tag{31}$$

The polyfit function method can be used to solve the same equation:

$$\begin{aligned} F(\Delta f) &= 6.7589 \times 10^3 - 3.8392 \times 10^2 \Delta f_i \\ &\quad + 8.9947 \Delta f_i^2 - 0.1113 \Delta f_i^3 + 0.7674 \\ &\quad \times 10^{-3} \Delta f_i^4 - 0.2793 \times 10^{-5} \Delta f_i^5 + 0.4193 \\ &\quad \times 10^{-8} \Delta f_i^6. \end{aligned} \tag{32}$$

The polyfit function is a curve fitting function that uses the least square parameter in MATLAB. Its principle is to construct an analytic function or polynomial through the discrete points on the data set and ensure that the original discrete points approach the infinity of the given value. The matrix function uses the matrix arithmetic method to solve a data set, which belongs to the method of linear algebra. Using two methods to calculate the frequency and pressure conversion algorithm results in a generally consistent trend in this study with a certain range of error.

In the picture, the data are as follows:

(1) (0, 81)
(2) (1, 88)
(3) (2, 90)
(4) (3, 93)
(5) (4, 94)
(6) (5, 103)
(7) (6, 105)
(8) (7, 107)
(9) (8, 109)
(10) (9, 113)
(11) (10, 116)
(12) (11, 117)
(13) (12, 121)
(14) (13, 122)
(15) (14, 124)
(16) (15, 128)
(17) (16, 132)
(18) (17, 135)
(19) (18, 139)
(20) (19, 143)
(21) (20, 147).

Figure 7 shows the polynomial simulating curve. The small red circle shows the relationship between the experimental values of the frequency difference and the experimental values of the pressure. The black line shows the relationship between the experimental values of the frequency difference and the pressure fitting values. The polyfit function also exhibits better polynomial fitting performance than the matrix calculation when the experiment data are significantly large. Unlike other published approaches, the small circle distribution is successfully simulated through the polynomial curve fitting. The normal interfacial stress sensor cannot measure a stress range less than 11 kPa. We designed the SAW based on a micro force sensor, which is based on the polyfit function and matrix calculation to overcome precisely this shortcoming. The sensor has better anti-interference and higher accuracy than others, can measure a range of 0 kPa to 20 kPa of microstress, and has good linearity (Figure 5).

6. Temperature Compensation

In this paper, a new type of SAW sensors is based on $LiNbO_3$. In order to ensure accuracy of data in the measurement, it is necessary to analyze the temperature compensation. The same reference device and the original measuring device are arranged in parallel. The output difference frequency method

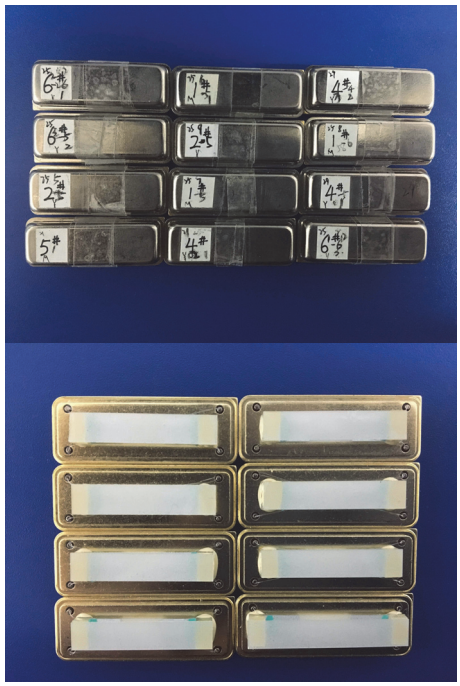


Figure 5: Physical maps of SAW based on a micro sensor.

Figure 6: The connection of a sensor and the network analyzer.

is adopted to eliminate the interference of temperature, humidity, and noise, as shown in Figure 8.

The output frequency of a SAW sensor is F_1, T_1 is the initial temperature, T_2 is the ambient temperature, ΔT is the difference temperature between the initial temperature and ambient temperature, and β_1 is the temperature coefficient of a SAW sensor. ΔF is the difference output frequency between one sensor and the reference sensor; then (33) is given as

$$F_1 = F_{01} + \Delta F + \beta_1 (T_2 - T_1) = F_{01} + \Delta F + \beta_1 \Delta T, \quad (33)$$

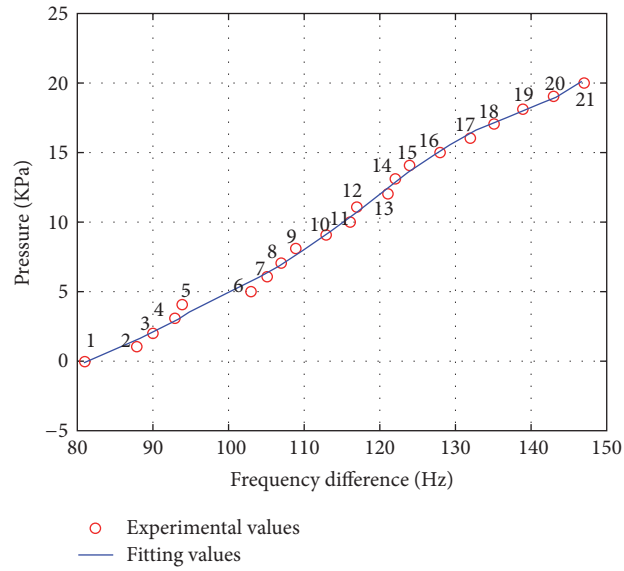


Figure 7: Fitting curve of the frequency difference and pressure of a SAW based on a micro force sensor.

where F_{01} is the initial frequency of the output of the sensing device without loading micro-pressure in temperature T_1. The output frequency of the reference SAW sensor is F_2; the formula can be written as follows:

$$F_2 = F_{02} + \beta_2 \Delta T, \quad (34)$$

where F_{02} is the initial frequency of the output of the reference device without loading micro-pressure in temperature T_2 and β_2 the temperature coefficient of a reference SAW sensor.

The difference frequency (ΔF) between F_1 and F_2 can be calculated:

$$\Delta F = F_1 - F_2 = F_{01} - F_{02} + \Delta F + (\beta_1 - \beta_2) \Delta T. \quad (35)$$

When β_1 and β_2 are equal, the difference of the output frequency of sensors is only related to the difference of temperature between the initial temperature and ambient temperature ΔT; then the reference device can completely compensate the influence of temperature on the sensing device.

Due to the difference of SAW devices, temperature coefficients cannot be equal. However, the sensor and the reference sensor have the same material, design, and fabrication; a certain amount of error will not affect the system so that the temperature compensation of SAW sensors can be fully realized.

7. Conclusion

WSNs have an active role in the detection of seismic and electromagnetic parameters, temperature, humidity, noise, light intensity, pressure, soil composition, size of a moving object, and speed and direction of the surrounding environment. As a new sensor type, the SAW based on a micro force sensor has high precision, small size, and high reliability

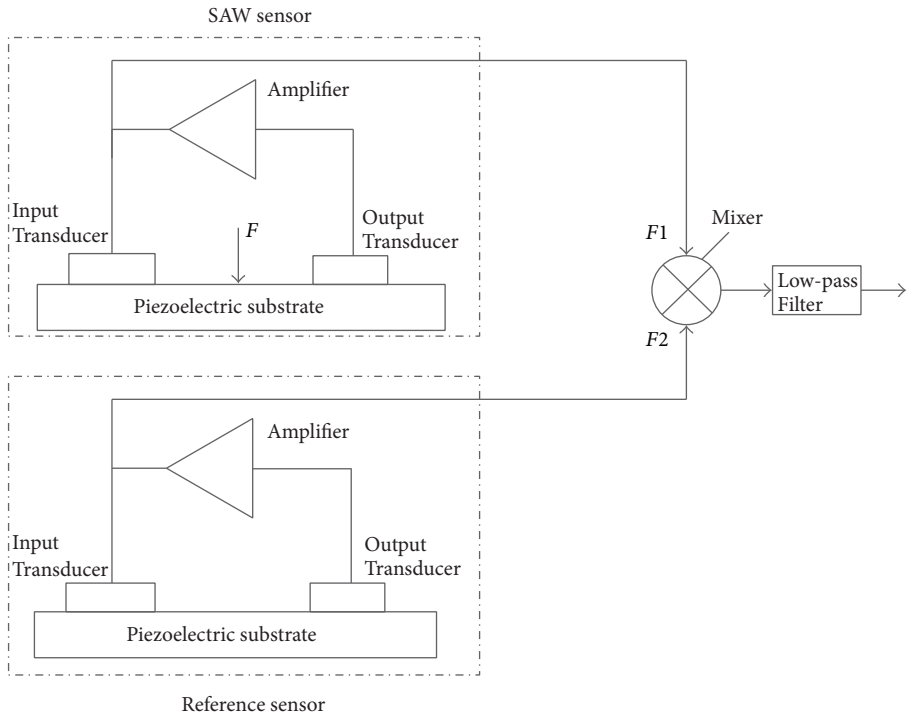


Figure 8: Principles of temperature compensation for SAW sensors.

characteristics in line with the high demand for sensors in the rapid development of WSNs.

This paper presents two different methods of analyzing the frequency and pressure conversion optimization algorithm of a SAW based on a micro force sensor. The polyfit function and matrix calculation, which are based on WSNs, SAW detection, and least squares method, have practical applications in the data acquisition of the proposed sensor in WSN nodes.

The study also proposes the pressure difference and frequency conversion method based on the relationship between the frequency and actual pressure data. The difference in the frequency data for different pressure values can also be established through the least squares model. The best estimate for the value of the polynomial coefficients and optimized model can be obtained after determining the minimum sum of the squares of the difference between the predicted and actual values. This approach decreases the measurement error and improves the advantages and competitiveness of the SAW-based micro force sensor in WSNs. SAW sensors in different WSN nodes use the piezoelectric properties and temperature stability of the crystal and the frequency signal instead of the conventional pressure sensor with a voltage signal. This approach enhances the signal processing of the device in terms of its digital feature and stable performance. Nevertheless, several fundamental problems still need to be solved, such as using more than one polynomial function in the fitting curve, expanding the scope of the pressure, and increasing the sampling data. Further studies on these issues should be undertaken in the future.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

Authors' deepest gratitude goes first and foremost to Professor Chuangchun Zhu, and the authors acknowledge the National Natural Science Foundation of China (no. 61274078), National Basic Research Program of China Textile Industry (no. J201608), and Research and Innovation Project of Graduate Students of Shanghai University of Engineering Science (E3-0903-16-01182) for the financial support and technical assistance.

References

[1] J. V. Nickerson and S. Olariu, "Protecting with sensor networks: attention and response," in *Proceedings of the 40th Annual Hawaii International Conference on System Sciences (HICSS '07)*, January 2007.

[2] A. Kishtwal, J. Singh, and R. Bhatt, "A review: wireless sensor networks (WSN) and security aspects," *International Journal of Engineering Research & Technology*, vol. 3, no. 1, pp. 223–228, 2014.

[3] B. Tang, Q. Huang, L. Deng, and Z. Liu, "Research progress and challenges of wireless sensor networks for machinery equipment condition monitoring," *Journal of Vibration, Measurement and Diagnosis*, vol. 34, no. 1, pp. 1–7, 2014.

[4] T. Cui, L. Chen, and T. Ho, "Energy efficient opportunistic network coding for wireless networks," in *Proceedings of the 27th IEEE Communications Society Conference on Computer Communications (INFOCOM '08)*, pp. 361–365, April 2008.

[5] V. Ugrinovskii, "Conditions for detectability in distributed consensus-based observer networks," *IEEE Transactions on Automatic Control*, vol. 58, no. 10, pp. 2659–2664, 2013.

[6] H. Dong, Z. Wang, and H. Gao, "Distributed H-infinity filtering for a class of markovian jump nonlinear time-delay systems over lossy sensor networks ," *IEEE Transactions on Industrial Electronics*, vol. 60, no. 10, pp. 4665–4672, 1999.

[7] D. Liao and K. Sarabandi, "Optimization of low-profile antennas for applications in unattended ground sensor networks," in *Proceedings of the IEEE Antennas and Propagation Society International Symposium*, pp. 783–786, Albuquerque, NM, USA, July 2006.

[8] J. Tokyo, "The future of technology," *Global Electronics China*, vol. 1, no. 5, pp. 4–500, 2007.

[9] J. Su, H. Qiao, Z. Ou, and Y. Zhang, "Sensor-less insertion strategy for an eccentric peg in a hole of the crankshaft and bearing assembly," *Assembly Automation*, vol. 32, no. 1, pp. 86–99, 2012.

[10] Q. Li, B. Shen, Y. Liu, and T. Huang, "Event-triggered H∞ state estimation for discrete-time neural networks with mixed time delays and sensor saturations," *Neural Computing and Applications*, pp. 1–11, 2016.

[11] C. Y. Xiong, J. W. Tian, and J. Liu, "A note on 'Flipping structure: an efficient VLSI architecture for lifting-based discrete wavelet transform'," *IEEE Transactions on Signal Processing*, vol. 54, no. 5, pp. 1910–1916, 2006.

[12] X. Tian, L. Wu, Y.-H. Tan, and J.-W. Tian, "Efficient multi-input/multi-output VLSI architecture for two-dimensional lifting-based discrete wavelet transform," *IEEE Transactions on Computers*, vol. 60, no. 8, pp. 1207–1211, 2011.

[13] W. Lu, L. Kuang, X. Lü, C. Zhu, T. Zhang, and J. Zhang, "Solution of some problems of single-scale wavelet transform processor using a magnetostatic surface wave device," *Metrology and Measurement Systems*, vol. 19, no. 4, pp. 685–692, 2012.

[14] D. S. Ballantine, R. M. White, S. J. Martin et al., *Acoustic Wave Sensor: Theory, Design, and Physic-Chemical Applications*, Academic Press, 1997.

[15] L. Xu, Y. Liu, and X. Fu, "Effects of the van der waals force on the dynamics performance for a micro resonant pressure sensor," *Shock and Vibration*, vol. 2016, Article ID 3426196, 11 pages, 2016.

[16] W. K. Lu, C. C. Zhu, J. H. Liu, and Q. Liu, "Implementing wavelet transform with SAW elements," *Science in China, Series E: Technological Sciences*, vol. 46, no. 6, pp. 627–638, 2003.

[17] X. Z. Lü, *Interfacial Stress Sensor for Artificial Skin Application*, Donghua University, 2012.

[18] M. Jungwirth, H. Scherr, and R. Weigel, "Micromechanical precision pressure sensor incorporating SAW delay lines," *Acta Mechanica*, vol. 158, no. 3-4, pp. 227–252, 2002.

[19] S. Muntwyler, F. Beyeler, and B. J. Nelson, "Three-axis micro-force sensor with sub-micro-Newton measurement uncertainty and tunable force range," *Journal of Micromechanics and Microengineering*, vol. 20, no. 2, Article ID 025011, pp. 3165–3170, 2010.

[20] Z. Cheng, *Research on Wireless Sensor Network Node Based on CC2431*, University of Science and Technology of China, Hefei, China, 2009 (Chinese).

[21] A. Binder, G. Bruckner, N. Schobernig, and D. Schmitt, "Wireless surface acoustic wave pressure and temperature sensor with unique identification based on LiNbO3," *IEEE Sensors Journal*, vol. 13, no. 5, pp. 1801–1805, 2013.

[22] W. K. Lu, C. C. Zhu, J. F. Zhang, C. Shi, and X. Z. Lü, "Study of small size wavelet transform processor and wavelet inverse-transform processor using SAW devices," *Measurement*, vol. 44, no. 5, pp. 994–999, 2011.

[23] K. Z. Zhou, *Least-Square Method*, Longmen Joint Press, 1951 (Chinese).

[24] Y. Y. Li, W. K. Lu, C. C. Zhu et al., "Acoustic electric generation for Morlet wavelet transform of surface acoustic wave device," *Research Journal of Applied Sciences, Engineering and Technology*, vol. 5, no. 4, pp. 1203–1207, 2013.

Hindawi
Journal of Electrical and Computer Engineering
Volume 2017, Article ID 8672716, 10 pages
https://doi.org/10.1155/2017/8672716

Research Article

Image Encryption Algorithm Based on a Novel Improper Fractional-Order Attractor and a Wavelet Function Map

Jian-feng Zhao,[1] Shu-ying Wang,[2] Li-tao Zhang,[3] and Xiao-yan Wang[1]

[1]*Department of Information Engineering, Henan Polytechnic, Zhengzhou, China*
[2]*Department of Minzu, Huanghe Science and Technology College, Zhengzhou, China*
[3]*Department of Mathematics and Physics, Zhengzhou Institute of Aeronautical Industry Management, Zhengzhou 450015, China*

Correspondence should be addressed to Shu-ying Wang; wsy0707@126.com

Received 12 November 2016; Revised 21 January 2017; Accepted 8 February 2017; Published 22 March 2017

Academic Editor: Jucheng Yang

This paper presents a three-dimensional autonomous chaotic system with high fraction dimension. It is noted that the nonlinear characteristic of the improper fractional-order chaos is interesting. Based on the continuous chaos and the discrete wavelet function map, an image encryption algorithm is put forward. The key space is formed by the initial state variables, parameters, and orders of the system. Every pixel value is included in secret key, so as to improve antiattack capability of the algorithm. The obtained simulation results and extensive security analyses demonstrate the high level of security of the algorithm and show its robustness against various types of attacks.

1. Introduction

With rapid development of communications, network security of information has become increasingly important for many applications. While high redundancy for image and multimedia information is challenging traditional cryptography algorithms [1, 2], chaotic attractors have orbital pseudorandom properties, good unpredictability, highly sensitivity for initial conditions, topological transitivity features, and so on. These characters indicate that chaos-based cryptosystem is a research hotspot in multimedia security area [3]. In 1949, Shannon created confusion and diffusion in the world of cryptography [4]. To overcome high redundancies and strong correlations of digital images, chaos has been widely applied in traditional encryption algorithm [5–13]. Research proposed that one-dimensional chaotic system has low security [14, 15]. With higher dimension, chaotic attractor occupies more space and winding complexly. The most complex attractor has much more complex output signals so that encryption effect would be better, whereas three-dimensional autonomous chaotic systems with higher fractal dimension are rare [16].

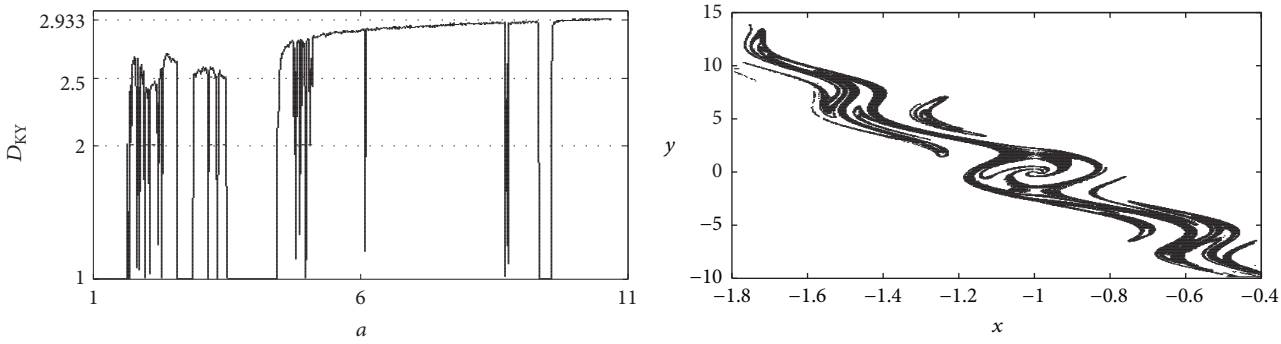
Comparing with integer-order chaotic system, the fractional-order chaotic system is not only related to parameters of the system, but also closely linked with fractional orders of system. Improper fractional-order chaotic system, therefore, has strong nonlinear characters and complexity. In secret communication, it can enhance the density and security so as to enormously increase the difficulty of unmasking signals. The algorithm shows greater application value in communication field [17, 18].

The rest of this paper is organized as follows: Section 2 describes a novel complex attractor. In Section 3, the chaos-based encryption algorithm is proposed. The numerical experimental results of performance analysis are given in Section 4. Finally, Section 5 contains conclusion and perspectives.

2. Improper Fractional-Order Chaotic Flow

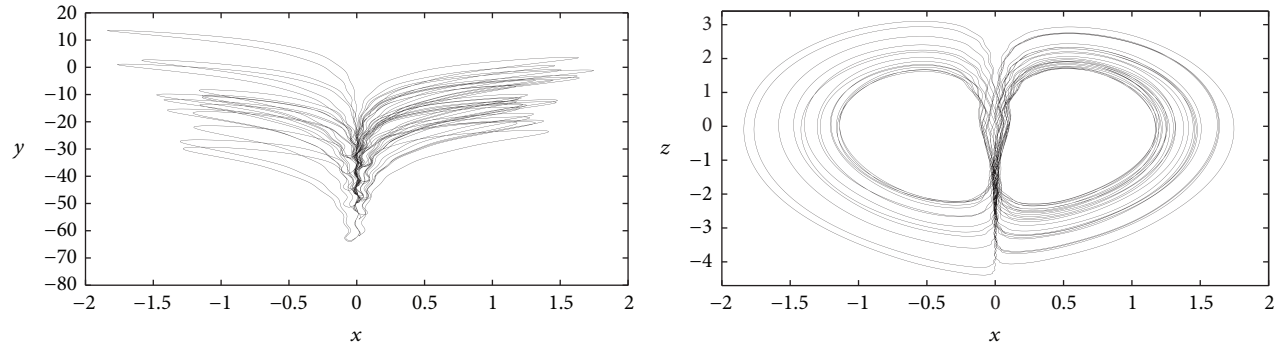
A new three-dimensional autonomous chaotic system with high fraction dimension is constructed, of which the governing fractional-order equation is

$$\frac{d^{q_1}x}{dt^{q_1}} = xz + b\sin(x + y + z),$$
$$\frac{d^{q_2}y}{dt^{q_2}} = az - by,$$



(a) Lyapunov dimensions (b) Poincaré sections of the maximally complex attractor

Figure 1: Chaotic characters of the novel attractor with $q_1 = q_2 = q_3 = 1$.



(a) x-y phase plane (b) x-z phase plane

Figure 2: The fractional-order chaos with $q_1 = 1.01$, $q_2 = 1.1$, and $q_3 = 1.11$.

$$\frac{d^{q_3} z}{dt^{q_3}} = 1 - cx^2, \tag{1}$$

where $X = (x, y, z)^T$ are state variables and a, b, c are parameters. Three fractional orders are q_1, q_2, q_3; if $\max(q_1, q_2, q_3) < 1$, system (1) is a true fractional-order system, if $q_1 = q_2 = q_3 = 1$, system (1) is an integer-order system, and if $\max(q_1, q_2, q_3) > 1$, system (1) is an improper fractional-order system. Based on stability theory and numerical analysis of fractional-order system, when $(a, b, c) = (6, 5, 0.12)$ and $(q_1, q_2, q_3) = (1, 1, 1)$, the Lyapunov dimension D_{KY} is shown in Figure 1(a) with varying parameter a in interval $[1, 11]$. Almost all D_{KY} of chaotic attractors are larger than 2.5. With increasing control parameters, D_{KY} reaches as high as 2.9336 at some special parameters. As shown in Figure 1(b), the Poincaré section of the maximally complex attractor has hierarchical structure composed of dense points. When $(q_1, q_2, q_3) = (1.01, 1.1, 1.11)$, the improper fractional-order chaos presents interesting and complex dynamic behavior represented in Figure 2.

3. Image Encryption Algorithm

Algorithm process is shown in Figure 3.

Encryption Procedure. Image encryption algorithm mainly consists of two processes: confusion and diffusion.

Step 1 (pixel confusion). Suppose that the size of plaintext image is $L = M \times N$. Scanning the plaintext image line by line in order to obtain pixel matrix P is as follows:

$$P = \begin{bmatrix} P(1) & P(2) & \cdots & P(N) \\ P(N+1) & P(N+2) & \cdots & P(2N) \\ \vdots & \vdots & \vdots & \vdots \\ P((M-1)N+1) & P((M-1)N+2) & \cdots & P(L) \end{bmatrix}. \tag{2}$$

In confusion procedure, the wavelet function map is taken as follows [21]:

$$x_{n+1} = k \cdot \left(1 - x_n^2\right) \cdot e^{-(x_n+\mu)^2/2}, \tag{3}$$

where $n \in N$ is the number of iterations. For numerical simulations, we take the initial value of the discrete system (3) as $x_0 = 0.3$, parameter $k = 1.33$, and $\mu = -0.6$. The chaotic characteristics of wavelet function map are shown in Figure 4(a), and its interesting bifurcation diagram varying with $\mu \in [-0.77, -0.29]$ is displayed in Figure 4(b).

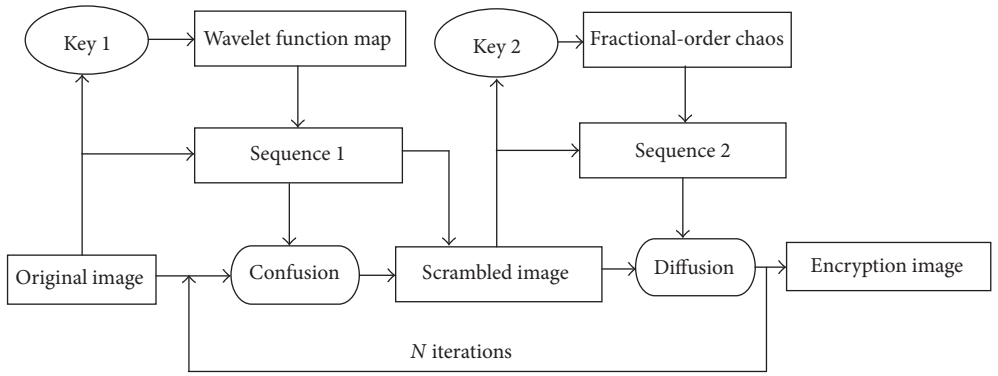
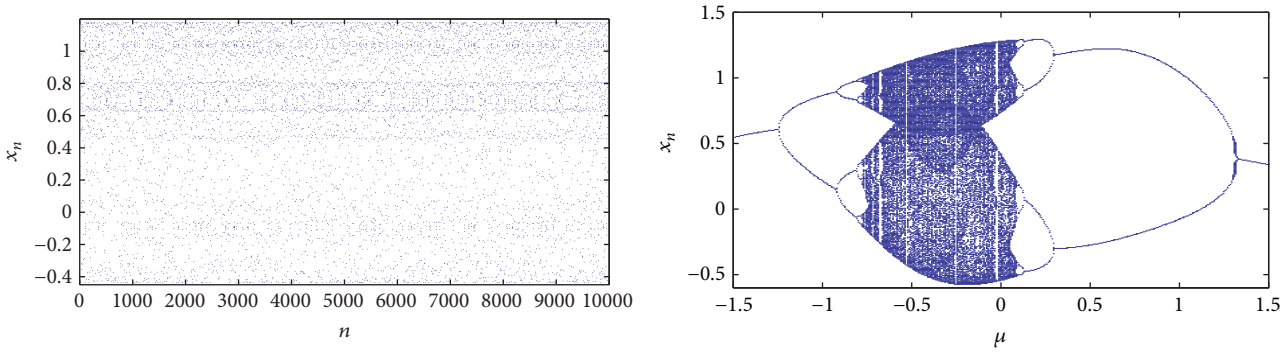


Figure 3: Encryption process.



(a) Wavelet function map

(b) Bifurcation of wavelet function map

Figure 4: Wavelet function map.

To improve the sensitivity of original image to encryption image, secret keys are distracted by plain image. In confusion procedure, $T = \mathrm{mod}\left(\sum_{i=1}^{L} P(i), L\right)/(L-1)$ is initial vector of wavelet function map. Sequence $x(n)$ is rearranged by wavelet function map so as to engender position matrix $lx(n)$. Then $lx(n)$ is used to confuse position of image pixels and get matrix $\{C(i) \mid i = 1, 2, \ldots, L\}$. Finally matrix $\{C(i) \mid i = 1, 2, \ldots, L\}$ is transformed into permutation image C of size $M \times N$.

Step 2 (pixel diffusion). Confusion only changes the position of pixel point while the pixel value is fixed, so the attacker may break down the algorithm though the statistics.

In diffusion, T is used to disturb parameter $a = a + T$ of system (1). Then the chaos generates chaotic sequences and makes N_0 times preiteration to eliminate some harmful effect of chaos transient process. Matrix B is created and initialized as an empty sequence. State vector $\{x(1), x(2), x(3)\}$ is generated in every iteration and a parameter $m = \mathrm{mod}\left(\mathrm{abs}(x(1) + x(2) + x(3)), 3\right)$ is derived. Then, matrix B is assigned according to parameter m. When $m = 0$, $B = \{B, x_1, x_2\}$, when $m = 1$, $B = \{B, x_1, x_3\}$, and when $m = 2$, $B = \{B, x_3, x_1\}$.

In every interaction, sequence B has strong randomness after $2L + N_0$ times iteration. Then B is preprocessed in the following form:

$$K(i) = \mathrm{mod}\left(\mathrm{temp}, 256\right), \quad i = 1, 2, \ldots, L, \tag{4}$$

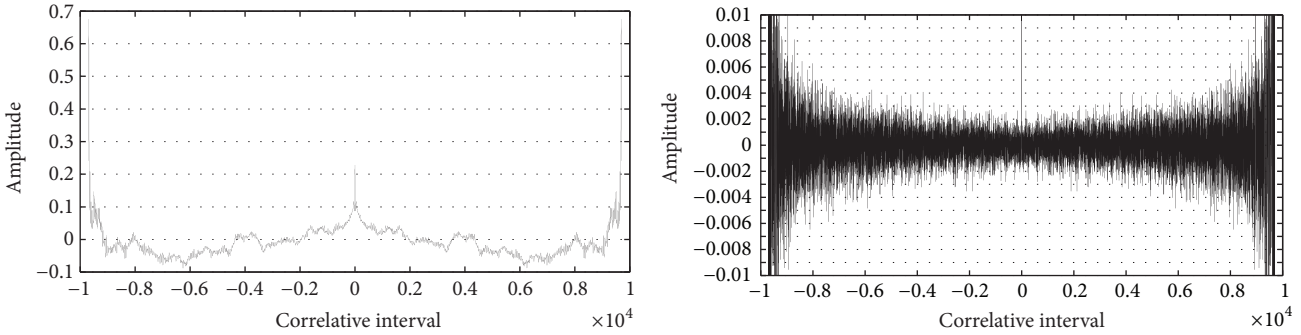
where $\mathrm{Temp} = \mathrm{floor}\left((|B(i)| - \mathrm{floor}\left(|B(i)|\right)) \times 10^m\right)$, $|x|$ is absolution of x, and $\mathrm{floor}\,(x)$ expresses downrounding. The positive integer $m = 12$. The autocorrelation of sequence B focuses on the interval $[-0.1, 0.1]$ and is shown in Figure 5(a), whereas the autocorrelation of sequence K after the pretreatment focuses on a smaller interval $[-0.003, 0.003]$ processed in Figure 5(b).

During diffusion, first pixel of permutation image C is encrypted as follows:

$$\begin{aligned} C(1) &= [C(1) + K(1)] \bmod 256 \\ &\quad \oplus [C(L) + K(1 + L + T)] \bmod 256. \end{aligned} \tag{5a}$$

However, for pixel at position $i > 1$, pixel substitution is made according to

$$\begin{aligned} C(i) &= [C(i) + K(i)] \bmod 256 \\ &\quad \oplus [C(i-1) + K(i + L + T)] \bmod 256, \\ &\qquad i = 1, 2, \ldots, L. \end{aligned} \tag{5b}$$



(a) Autocorrelation of sequence B

(b) Autocorrelation of improved sequence K

Figure 5: Autocorrelation of sequences.

Then sequence $\{C(i),\ i = 1, 2, \ldots, L\}$ is conversed into matrix with size of $M \times N$.

Decryption is inverse operation of encryption process. Decryption image D is scanned line by line to get sequence $\{D(i) \mid i = 1, 2, \ldots, L\}$ $(L = M \times N)$.

$$\begin{aligned} \text{temp} &= C(i) \oplus [C(i-1) + K(i+L+T)] \bmod 256, \\ D(i) &= [\text{temp} - K(i)] \bmod 256, \\ & \qquad i = L, L-1, \ldots, 2, \end{aligned} \tag{6a}$$

$$\begin{aligned} \text{temp} &= C(1) \oplus [C(L) + K(1+L+T)] \bmod 256, \\ D(1) &= [\text{temp} - K(1)] \bmod 256. \end{aligned} \tag{6b}$$

Then, inverse scrambling operation for matrix $\{D(i) \mid i = 1, 2, \ldots, L\}$ is made. Firstly, sequence $x(n)$ is generated by wavelet function map to produce position matrix $lx(n)$. Then $lx(n)$ is arranged by the same law so as to get position matrix $llx(n)$. At last we use $llx(n)$ to confuse pixel position of image D to get matrix $\{E(i) \mid i = 1, 2, \ldots, L\}$ and change matrix E into $M \times N$ two-dimension matrix to observe final decrypted image.

4. Numerical Simulation and Performance Analysis

The proposed encryption technique is implemented in MATLAB 7.1. In the experiment, different types of digital images are tested, such as gray image, binary image, and color image.

4.1. 3D Histogram Analysis. Histogram is a graphical representation of the pixels intensity distribution of an image, and it can measure the capacity of resisting attack. The gray Lena image of size 256×256 is encrypted as shown in Figure 6(c) and the 3D histogram of the encrypted Lena image is shown in Figure 6(d). The binary image has only two colors and is sensitive to the change of pixel. 3D histograms of a binary image are encrypted and encrypted binary images are demonstrated in Figures 7(b) and 7(d), respectively. Figure 8(a) shows the color image and its RGB histograms; Figure 8(b) shows the encrypted color image of Figure 8(a) and its RGB histograms. The histogram of the encrypted image is fairly uniform and significantly different from that of the original image, so the information is unpredictable and histogram attack can be avoided.

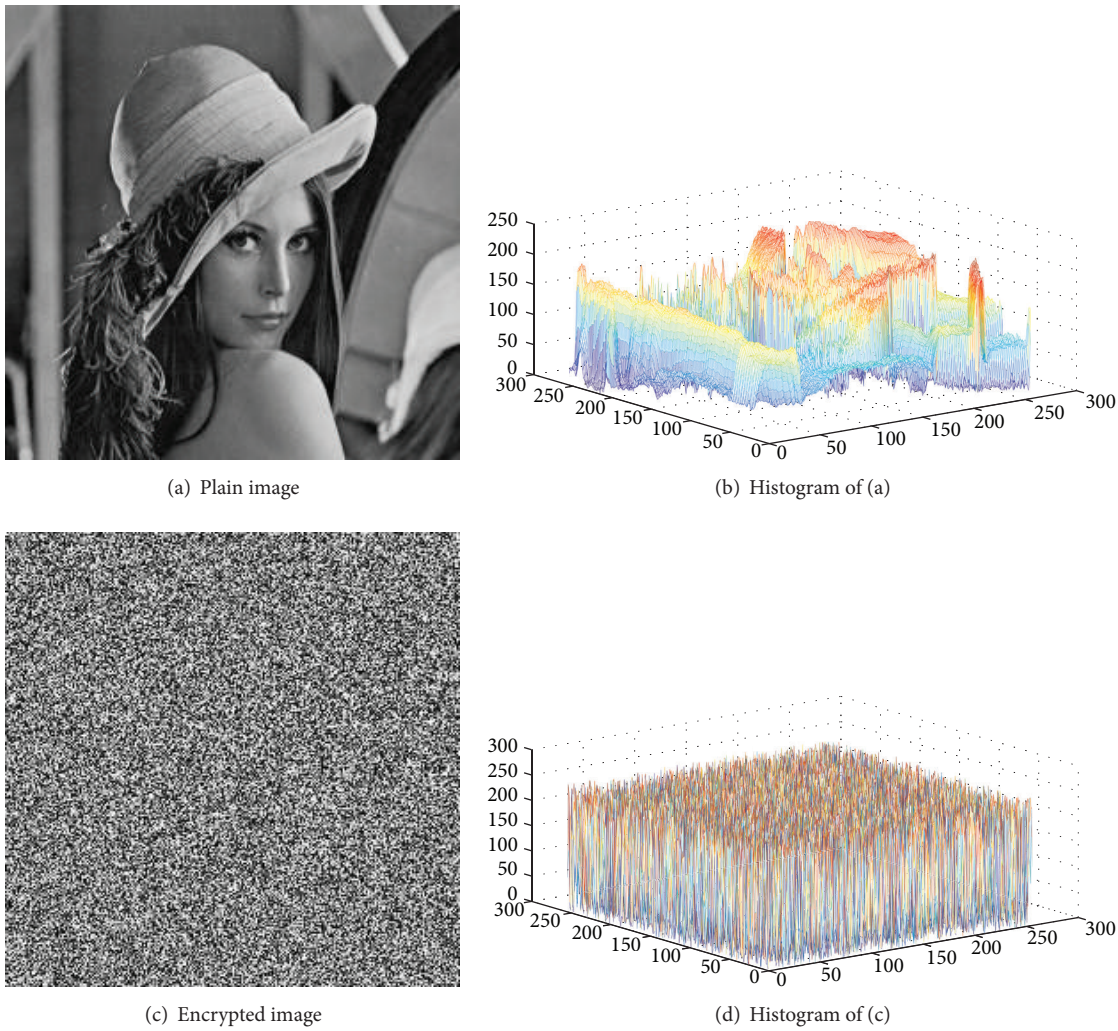
4.2. Information Entropy. Information entropy, firstly proposed by Shannon in 1949, is a significant property that reflects the randomness and the unpredictability of an information source [4]. With bigger entropy image has more uniform gray distribution. The entropy $H(x)$ is defined by the following formula: $H(x) = -\sum_{i=1}^{n} p(x_i)\log_2 p(x_i)$, where $p(x_i)$ denotes the probability of symbol x_i. When $p(x_i) = 1/256$, the 256×256 gray image has maximum entropy of 8. Entropy of gray Lena image and binary image is 7.447144 and 0.593165, respectively, while its encryption is 7.988847 and 7.972069, respectively. Considering RGB components of color image Lena, average information entropy of the color Lena and encrypted color Lena is 7.198813 and 7.997281, respectively. It is obvious that the entropies of the cipher images are very close to the theoretical value of 8, which means that the encryption algorithm has ability of resisting statistical attack.

4.3. Correlation Coefficients of Adjacent Pixels. In the section, we aim at checking up the correlation of two adjacent pixels between the original image and encrypted image. In this simulation, randomly selected 1000 pairs of adjacent pixels (horizontally, vertically, and diagonally) are determined. The correlation coefficient between two adjacent pixels in an image is determined according to the following formula:

$$R_{xy} = \frac{\text{Conv}(x, y)}{\sqrt{D(x)}\sqrt{D(y)}}, \tag{7}$$

where

$$\begin{aligned} E(x) &= \frac{1}{N}\sum_{i=1}^{N} x_i, \\ D(x) &= \frac{1}{N}\sum_{i=1}^{N} [x_i - E(x)]^2, \\ \text{Conv}(x, y) &= \frac{1}{N}\sum_{i=1}^{N} [x_i - E(x)]\,[y_i - E(y)]. \end{aligned} \tag{8}$$



(a) Plain image

(b) Histogram of (a)

(c) Encrypted image

(d) Histogram of (c)

FIGURE 6: The gray Lena image.

Figure 9 displays correlation coefficients of adjacent pixels in four directions of Lena plain image and cipher image. The result emphasizes that there is hardly any correlation of adjacent pixels in encryption images. Correlation coefficients of the encrypted Lena image are smaller than other methods shown in Table 1. The statistical properties of original image have randomly spread to encryption image.

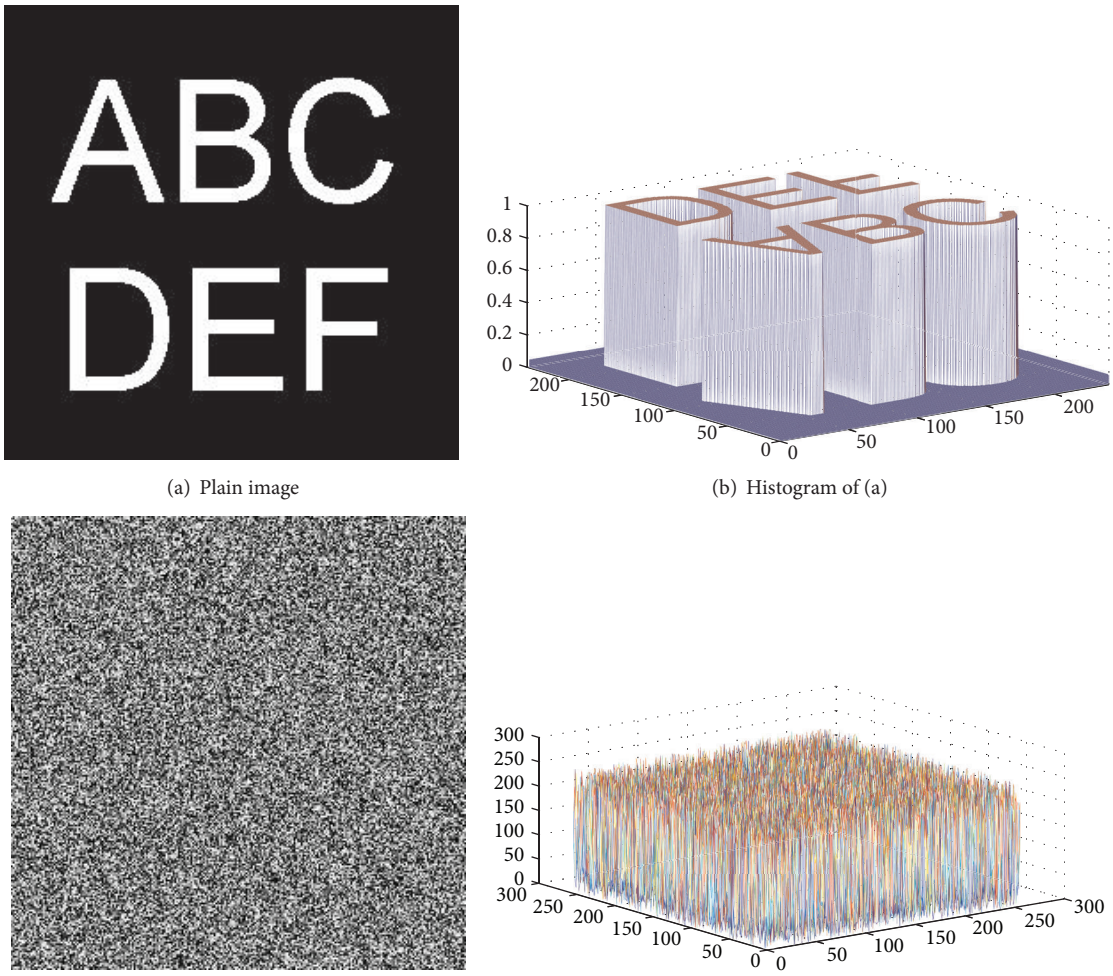
4.4. Resistance to Differential Attack. The attacker may observe the change of decryption by the tiny change of plaintext to find the correlation between plain image and cipher image. Based on principles of cryptology, a good encryption algorithm should be sensitive to plaintext sufficiently. In general, attacker makes a slight change (e.g., modify only one pixel) for plaintext to find out some relationships between plain image and encrypted image. If tiny change of original image can bring great changes to cipher image, the effect of differential attack will be reduced. Sensitivity of the plaintext encryption algorithm can be quantified by NPCR (number of pixels changing rate) and UACI (unified average changing intensity). They are defined as follows:

$$D(i,j) = \begin{cases} 0, & C_1(i,j) = C_2(i,j), \\ 1, & C_1(i,j) \neq C_2(i,j), \end{cases}$$

$$\text{NPCR} = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} D(i,j) \times 100\%, \tag{9}$$

$$\text{UACI} = \frac{1}{255 \times M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} \left| C_1(i,j) - C_2(i,j) \right| \times 100\%,$$

where $C_1(i, j)$ and $C_2(i, j)$ indicate pixel value of two encryption images at location (i, j). M and N present number of rows and columns of the original image.



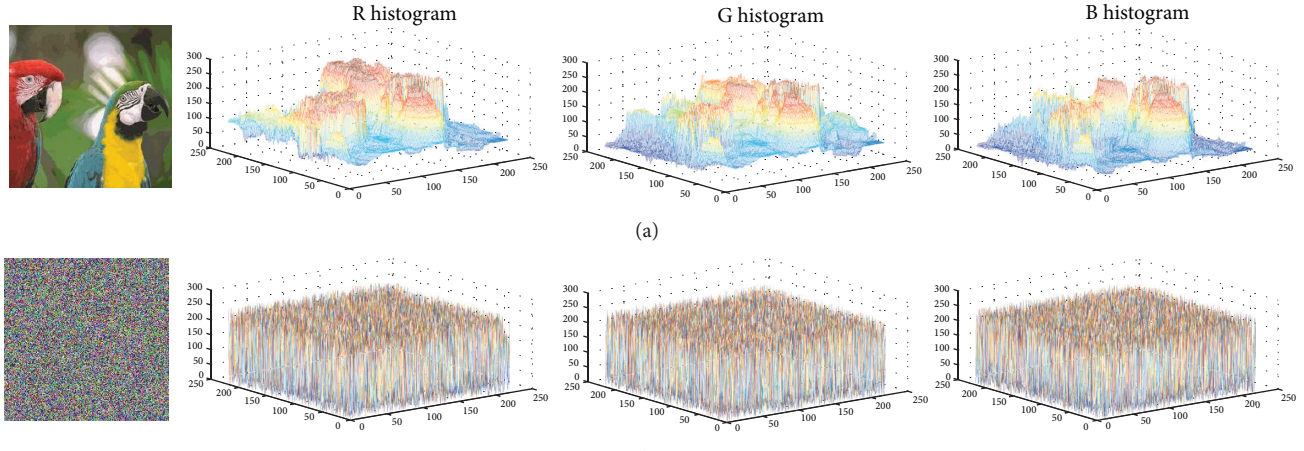
(a) Plain image

(b) Histogram of (a)

(c) Encrypted image

(d) Histogram of (c)

Figure 7: The binary image.



(a)

(b)

Figure 8: The color parrot image: (a) the plain image and its RGB histograms; (b) the encrypted image and its RGB histograms.

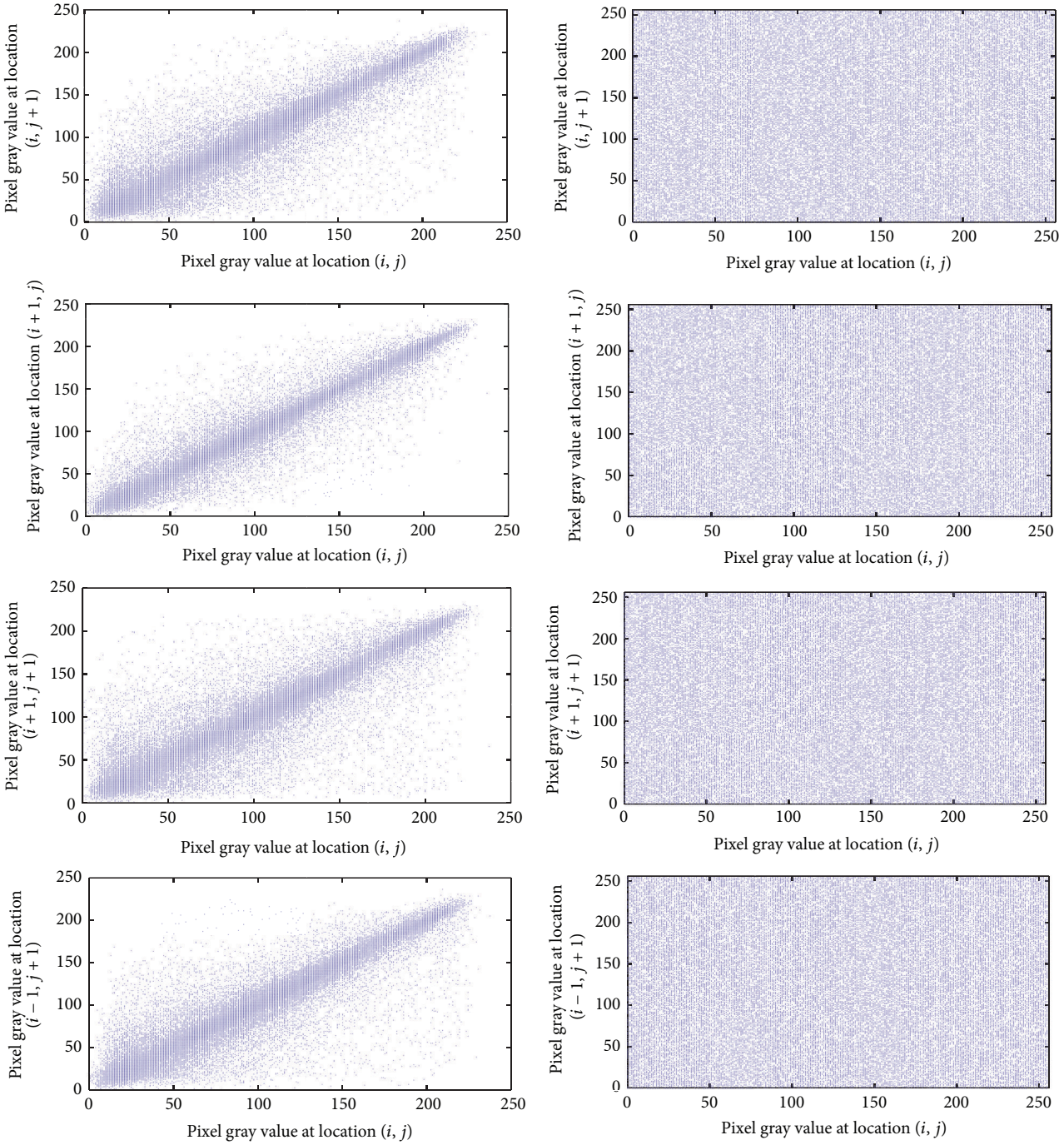


Figure 9: Correlation coefficients of original and encryption image: horizontal; vertical; diagonal; counterdiagonal.

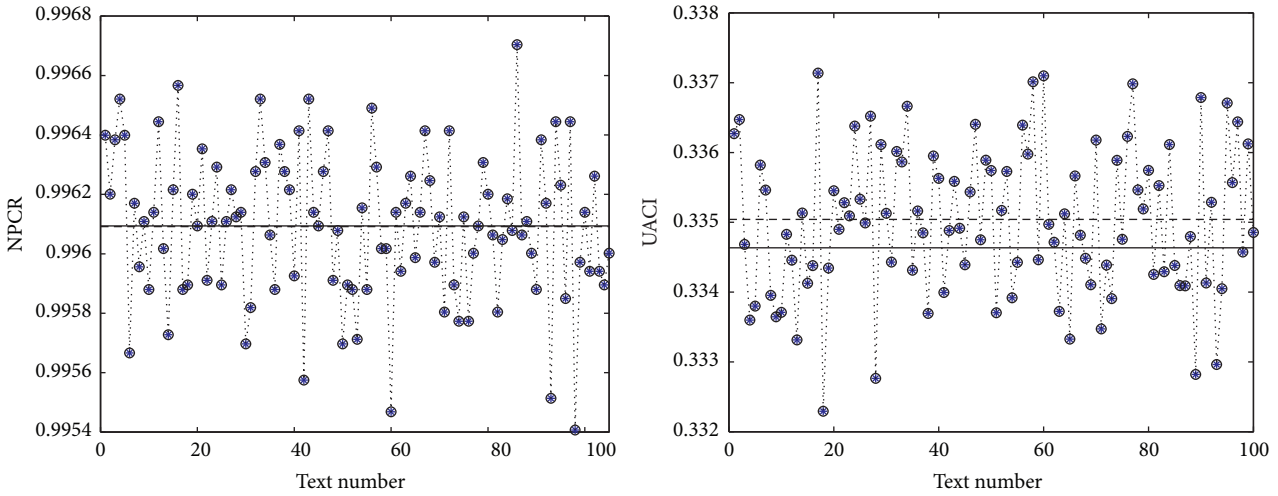
The ideal expectations of NPCR and UACI can be calculated by the following simplified formulas:

$$\begin{aligned} \mathrm{NPCR_E} &= \left(1 - 2^{-n}\right) \times 100\%, \\ \mathrm{UACI_E} &= \frac{1}{2^{2n}} \frac{\sum_{i=1}^{2^n-1} i\,(i+1)}{2^n - 1} \times 100\% \\ &= \frac{1}{3}\left(1 + 2^{-n}\right) \times 100\%, \end{aligned} \tag{10}$$

where n is the number of bits used to represent the different bit planes of an image. For gray scale image parameter $n = 8$ (8 bits per pixel). Hence expected NPCR and expected UACI are $\mathrm{NPCR_E} = 99.6094\%$ (horizontal solid line in Figure 10(a)) and $\mathrm{UACI_E} = 33.4635\%$ (horizontal solid line in Figure 10(b)), respectively. From the above formula we can see that relation $\mathrm{NPCR_E} + 3\mathrm{UACI_E} = 2$, so any value of the ideal expectations can illustrate the capability of algorithm to attack resisting plaintext.

Table 1: Correlation coefficient of different plain image and cipher image.

Plain image	Horizontal	Vertical	Diagonal	Counterdiagonal
Gray Lena				
Plain image	0.972953	0.970462	0.916925	0.938441
Encrypted image	-4.097226×10^{-5}	1.158832×10^{-4}	4.620716×10^{-5}	4.539076×10^{-4}
Encrypted image [19]	0.000417	−0.002048	−0.001554	
Encrypted image [20]	0.023	0.028	0.023	
Binary image				
Plain image	0.915352	0.922622291	0.868221	0.857255
Encrypted image	-3.811868×10^{-6}	-7.131676×10^{-4}	-9.372164×10^{-4}	-3.496642×10^{-4}
Color parrot				
R				
Plain image	0.945140	0.950725	0.919702	0.937272
Encrypted image	−0.001678	3.514572×10^{-4}	-9.329940×10^{-4}	-4.626904×10^{-5}
G				
Plain image	0.948746	0.941403	0.910118	0.929873
Encrypted image	-8.326210×10^{-4}	-4.626904×10^{-5}	1.484844×10^{-5}	6.479456×10^{-4}
B				
Plain image	0.956960	0.924891	0.924891	0.941023
Encrypted image	-7.902728×10^{-6}	1.1520873×10^{-4}	9.66501×10^{-4}	-1.766560×10^{-4}



(a) Number of pixels changing rate

(b) Unified average changing intensity

Figure 10: Measured sensitivity of cipher image to plain image.

In this experiment, one hundred groups of Lena images are encrypted. In every group image, one is original image and the other is original image with only one changed pixel value (including border points and intermediate points, each time the changed amount is only 1). Then the test results are shown in Figure 10; every value fluctuates up and down near ideal value. The average values are $\overline{\text{NPCR}} = 99.6091\%$ (horizontal dotted line in Figure 10(a)) and $\overline{\text{UACI}} = 33.5038\%$ (horizontal dotted line in Figure 10(b)), respectively. Obviously the given encryption algorithm greatly improves the sensitivity of plaintext, thereby enhancing capacity of resistance to differential attacks.

4.5. Key Sensitivity Test. Lena gray image is used to make experimental analysis. With right key, the decrypted image is clear and correct without any distortion in Figure 11(a). Decryption using keys with slight mismatch is performed so as to evaluate the key sensitivity. With a subtle change, the new key $q_1 = 1.01000000001$, and the decrypted image is incorrect, proposed in Figure 11(b). Subtle change of key

(a) Decrypted image (b) Error decrypted image

Figure 11: The decrypted Lena image.

yields greatly different decrypted images. It is fully convincing that the algorithm has steady and superior secure performance in the first encryption round and will well resist differential attack.

4.6. Algorithmic Complexity Analyses. The time complexity of an algorithm quantifies the amount of time taken by an algorithm to run as a function of the size of the input to the problem. The time complexity is commonly described using the big-O notation, which suppresses multiplicative constants and lower order terms. Time complexity of generating key is $O(M \cdot N)$. The maximum complexity chaos and wavelet function map generate chaos sequences with time complexities $O(T_1^2)$ and $O(T_2^2)$, respectively. Pixel diffusion and substitution have the same time complexity $O(M \cdot N)$. At each step, the worst total time complexity is

$$\begin{aligned} &O(M \times N) + O\left(T_1^2\right) + O\left(T_2^2\right) + O(M \times N) \\ &\quad = O(T), \end{aligned} \tag{11}$$

where $T = \max\{M \cdot N, T_1^2, T_2^2\}$. T_1 and T_2 represent iterate numbers of maximum complexity chaos and wavelet function map, respectively.

5. Conclusion

This paper presents a novel fractional-order complex attractor with high fraction dimension, and the preprocessed chaotic sequence has good random character. Secret key is disturbed by every order and pixel value of plaintext; thus slight change of plaintext can bring vast differentness in encrypted image. Theoretical analysis and experimental results indicate that the encryption algorithm has some good characters, such as resistance for different attack, better information entropy, and low coefficient correlation. Comparing with some chaos-based algorithms, the estimated results demonstrate the strong capabilities and the effectiveness of the proposed algorithm. The time complexity of the algorithm is proposed and an example is investigated to verify its validity and practicability. Our future works will focus on video encryption using fractional-order chaotic system.

Conflicts of Interest

The authors declare that they have no competing interests.

Acknowledgments

This research is supported by NNSFs of China (Grant no. 11501525), Science & Technology Innovation Talents in Universities of Henan Province (Grant no. 16HASTIT040), Teacher Education Curriculum Reform of Henan Province (Grant no. 2017-JSJYYB-190), Project of Youth Backbone Teachers of College and Universities in Henan Province (Grant nos. 2013GGJS-142 and 2015GGJS-179), and Basic & Advanced Technological Research Project of Henan Province (Grant no. 162300410261).

References

[1] B. Schneier, *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, John Wiley & Sons, New York, NY, USA, 2nd edition, 1996.

[2] J. Daemen and V. Rijmen, *The Design of Rijndael: AES-The Advanced Encryption Standard*, Springer, Berlin, Germany, 2002.

[3] L. Kocarev, G. Jakimoski, T. Stojanovski, and U. Parlitz, "From chaotic maps to encryption schemes," in *Proceedings of the IEEE International Symposium on Circuits and Systems (ISCAS '98)*, pp. 514–517, IEEE, Monterey, Calif, USA, June 1998.

[4] C. E. Shannon, "Communication theory of secrecy systems," *The Bell System Technical Journal*, vol. 28, no. 4, pp. 656–715, 1949.

[5] N. K. Pareek, V. Patidar, and K. K. Sud, "Discrete chaotic cryptography using external key," *Physics Letters. A*, vol. 309, no. 1-2, pp. 75–82, 2003.

[6] X. Wang and L. Teng, "An image blocks encryption algorithm based on spatiotemporal chaos," *Nonlinear Dynamics. An International Journal of Nonlinear Dynamics and Chaos in Engineering Systems*, vol. 67, no. 1, pp. 365–371, 2012.

[7] S. Behnia, A. Akhshani, H. Mahmodi, and A. Akhavan, "A novel algorithm for image encryption based on mixture of chaotic maps," *Chaos, Solitons & Fractals*, vol. 35, no. 2, pp. 408–419, 2008.

[8] D. Xiao, X. Liao, and P. Wei, "Analysis and improvement of a chaos-based image encryption algorithm," *Chaos, Solitons & Fractals*, vol. 40, no. 5, pp. 2191–2199, 2009.

[9] X.-Y. Wang and X.-M. Bao, "A novel block cryptosystem based on the coupled chaotic map lattice," *Nonlinear Dynamics*, vol. 72, no. 4, pp. 707–715, 2013.

[10] G. Jakimoski and L. C. Kocarev, "Analysis of some recently proposed chaos-based encryption algorithms," *Physics Letters. A*, vol. 291, no. 6, pp. 381–384, 2001.

[11] S. Behnia, A. Akhshani, H. Mahmodi, and A. Akhavan, "A novel algorithm for image encryption based on mixture of chaotic maps," *Chaos, Solitons & Fractals*, vol. 35, no. 2, pp. 408–419, 2008.

[12] O. Mirzaei, M. Yaghoobi, and H. Irani, "A new image encryption method: parallel sub-image encryption with hyper chaos," *Nonlinear Dynamics*, vol. 67, no. 1, pp. 557–566, 2012.

[13] Y. Wang, K.-W. Wong, X. F. Liao, and G. R. Chen, "A new chaos-based fast image encryption algorithm," *Applied Soft Computing*, vol. 11, no. 1, pp. 514–522, 2011.

[14] A. I. Ismail, A. Mohammed, and D. Hossam, "A digital image encryption algorithm based a composition of two chaotic Wavelet function map," *International Journal of Network Security*, vol. 11, no. 1, pp. 1–10, 2010.

[15] R. Rhouma and S. Belghith, "Cryptanalysis of a new image encryption algorithm based on hyper-chaos," *Physics Letters, Section A: General, Atomic and Solid State Physics*, vol. 372, no. 38, pp. 5973–5978, 2008.

[16] X.-F. Li, K. E. Chlouverakis, and D.-L. Xu, "Nonlinear dynamics and circuit realization of a new chaotic flow: a variant of Lorenz, Chen and Lü," *Nonlinear Analysis. Real World Applications. An International Multidisciplinary Journal*, vol. 10, no. 4, pp. 2357–2368, 2009.

[17] J. F. Zhao, S. Y. Wang, Y. X. Chang, and X. F. Li, "A novel image encryption scheme based on an improper fractional-order chaotic system," *Nonlinear Dynamics*, vol. 80, no. 4, pp. 1721–1729, 2015.

[18] X. Wu, H. Wang, and H. Lu, "Modified generalized projective synchronization of a new fractional-order hyperchaotic system and its application to secure communication," *Nonlinear Analysis. Real World Applications*, vol. 13, no. 3, pp. 1441–1450, 2012.

[19] O. Mannai, R. Bechikh, H. Hermassi, R. Rhouma, and S. Belghith, "A new image encryption scheme based on a simple first-order time-delay system with appropriate nonlinearity," *Nonlinear Dynamics*, vol. 82, no. 1-2, pp. 107–117, 2015.

[20] Q. Liu, P.-Y. Li, M.-C. Zhang, Y.-X. Sui, and H.-J. Yang, "A novel image encryption algorithm based on chaos maps with Markov properties," *Communications in Nonlinear Science and Numerical Simulation*, vol. 20, no. 2, pp. 506–515, 2015.

[21] W.-B. Yu and X.-P. Wei, "Bifurcation diagram of a wavelet function," *Acta Physica Sinica*, vol. 55, no. 8, pp. 3969–3973, 2006.

Hindawi
Journal of Electrical and Computer Engineering
Volume 2017, Article ID 3451358, 6 pages
https://doi.org/10.1155/2017/3451358

Research Article

Ferrography Wear Particles Image Recognition Based on Extreme Learning Machine

Qiong Li, Tingting Zhao, Lingchao Zhang, Wenhui Sun, and Xi Zhao

College of Computer Science and Information Engineering, Tianjin University of Science and Technology, Tianjin 300457, China

Correspondence should be addressed to Xi Zhao; xi.zhao@tust.edu.cn

Received 25 November 2016; Accepted 13 February 2017; Published 21 March 2017

Academic Editor: Hui Cheng

The morphology of wear particles reflects the complex properties of wear processes involved in particle formation. Typically, the morphology of wear particles is evaluated qualitatively based on microscopy observations. This procedure relies upon the experts' knowledge and, thus, is not always objective and cheap. With the rapid development of computer image processing technology, neural network based on traditional gradient training algorithm can be used to recognize them. However, the feedforward neural network based on traditional gradient training algorithms for image segmentation creates many issues, such as needing multiple iterations to converge and easy fall into local minimum, which restrict its development heavily. Recently, extreme learning machine (ELM) for single-hidden-layer feedforward neural networks (SLFN) has been attracting attentions for its faster learning speed and better generalization performance than those of traditional gradient-based learning algorithms. In this paper, we propose to employ ELM for ferrography wear particles image recognition. We extract the shape features, color features, and texture features of five typical kinds of wear particles as the input of the ELM classifier and set five types of wear particles as the output of the ELM classifier. Therefore, the novel ferrography wear particle classifier is founded based on ELM.

1. Introduction

Wear particle analysis for machine condition monitoring and fault diagnosis is not a new topic in tribology. Roylance et al. [1] pioneered computer wear pattern recognition research direction by establishing the computer aided visual engineering (CAVE) to extract the wear particles' Fourier factor, roundness factor, and edge details. Then, they used these features to classify portion wear particles [2–7]. Hamblin and Stachowiak proposed the spike parameter to extract characteristics of abrasive particles via adequate description of wear debris boundary in multiscale [8]. Xu et al. [9] developed a set of wear particle image analysis system through the integration of neural network and expert system, which can realize the interactive wear particles image automatic recognition. Tian et al. [10] and Peng and Kirk [11] employed laser scanning confocal microscopy to acquire three-dimensional particle images. The scanning method provides surface information from the analysis of wear surface morphology, which facilitates better understanding of wear features and wear level. Stachowiak et al. [12] utilized an automated classification system to analyze and identify fatigue, abrasive, and adhesive wear particles. Such analysis and identification operations were fulfilled mainly based on the analyses of the area perimeter, elongation parameters, convexity, and surface texture. van Otterlo [13] distinguished different points on the curve of an object boundary by means of the proposed parameters, which might represent points with respect to a reference position in polar coordinate system. This approach provided a unified theoretical basis for analyzing shape similarity according to the proposed parametric contour representations. Laghari and Memon developed an automatic analysis system, KBWPAS, to reduce the dependence on domain experts [14]. Wang combined principal component analysis and gray relational analysis to optimize the parameters of features of wear particles [15]. Wang and Yin used wear particle shape, color, and surface texture parameters as input vectors and introduced radial basis function neural network to conduct automatic classification and identification on wear particle [16]. Gu

applied support vector machine to ferrography wear particle pattern recognition and built wear particle classifier based on supper vector machine [17]. Yuan and Yan took surface texture and surface roughness as the important indicators of three-dimensional surface characteristic and adopted artificial intelligent neural network method to identify wear particle type, which efficiently improved accuracy of wear particle classification [18]. Luo et al. proposed to use principal component analysis to extract characteristic parameters of wear particles and then introduced BP neural network to conduct automatic classification on wear particles. This method optimized parameters firstly, which yielded better classification rate compared to traditional BP neural network [19]. Zhou et al. used the same method to optimize parameters of wear particle features and applied the improved genetic algorithms to the LS-SVM's parameter optimization, thus improving wear particle recognition rate [20].

At present, a lot of image classification algorithms have been proposed, among which the neural network based image classification algorithms are widely used. However, the traditional feedforward neural networks need many iterations to converge and are easy to fall into the local optimum in the procession of image classification, which seriously limit its development and application. On the other hand, the extreme learning machine as a new machine learning algorithm has become more and more popular due to its few adjustable parameters, fast learning speed, and good generalization performance. However, the effectiveness of the application of ELM to the field of image processing of iron spectrum abrasive particles is open to be investigated. In this paper, we present the method to apply the extreme learning machine to the recognition of wear particles.

The rest of the paper is organized as follows. Section 2 introduces principles and methods used in this paper. In Section 3, we describe the proposed method. In Section 4, we describe the experiments. Section 5 finalizes the paper with the conclusions.

2. Principle and Method

2.1. Characteristic Parameters of Wear Particles. Generally, characteristic parameters play important role in the final result of wear particles recognition. Although the obtained ferroscope images of wear particles are not three-dimensional, the size, texture, and color features are enough for typical wear particles recognition.

Among the shape and size factors of wear particles, area, perimeter, equivalent circle diameter, circularity, aspect ratio, concavity, and so on are commonly used features to be extracted from the color images, which are captured via the microscope. These shape and size parameters can be further approximated by converting the sample color image into binary image with the values of 0 and 1.

Besides the shape and size parameters, texture is also very important in image analysis. The texture is the description of the pixel distribution of a picture in gray space. Machines or equipment with a pair of relatively moving contact surfaces for long-time operation tends to produce wear particles. Usually, the surface texture provides statistical information of the wear state in the machinery operation process. Textural features are investigated by using the distribution function to analyze the gray level of the characteristic region of wear particles. Among the parameters of wear particles, two of the characteristic features are employed to distinguish the surface texture, namely, roughness and directivity. Gray level cooccurrence matrix (GLCM) [21] is commonly used to describe the surface textural factors of wear particles. The textural features, including energy, entropy, dependency, inertia moment, and stability, can be extracted by employing the GLCM. However, the connection between the obtained textural features and human vision perceptual system has not been established. Based on the psychological representation of human vision perception to the texture, Tamura et al. proposed the expression of the textural feature, Tamura textural feature [22], which can be used to extract six properties of the textural features, contrast ratio, roughness, direction level, regularity, linearity, and coarseness. Moreover, we have found that HoG gives a good simulation of the variation of the particle images [23]. The histogram of oriented gradient for the local region of the wear particle images can be calculated by using HoG.

Color feature is another kind of significant properties to analyze wear particle images. The color factor is important for the identification of the red oxides, black oxides, and fatigued copper wear particles. By analyzing the color of the wear particles, mechanical abrasion degree can be predicted. The image commonly consisted of three-primary colors of red (R), green (G), and blue (B). In the RGB space, the three-color factors of R(i, j), G(i, j), and B(i, j) denote the color features of wear particles. After the images of wear particles are processed, the first-order and second-order statistical values (mean and variance) of R(i, j), G(i, j), and B(i, j) and the third-order color matrix of the HSV color space are extracted as the color characteristic parameters.

2.2. Extreme Learning Machine. The extreme learning machine (ELM) algorithm was originally proposed by Huang et al. [24–27]. The method is proved to be a universal approximator given enough hidden neurons [28]. It works as follows.

Consider a set of N distinct samples (x_i, t_i) with $x_i \in R^d$ and $t_i \in R^c$. Then a single layer feedforward network with L hidden neurons is modeled as

$$\sum_{i=1}^{L} \beta_i \phi\left(\mathbf{w_i x_j} + b_i\right), \quad j \in [1, N] \tag{1}$$

with ϕ being an activation function, $\mathbf{w_i}$ the input weights, b_i the biases, and β_i the output weights.

In the case where the single layer feedforward network would perfectly approximate the data, the errors between the estimated outputs y_i and the targets t_i are zero, and the relation between inputs, weights, and targets is

$$\sum_{i=1}^{L} \beta_i \phi\left(\mathbf{w_i x_j} + b_i\right) = t_i, \quad j \in [1, N] \tag{2}$$

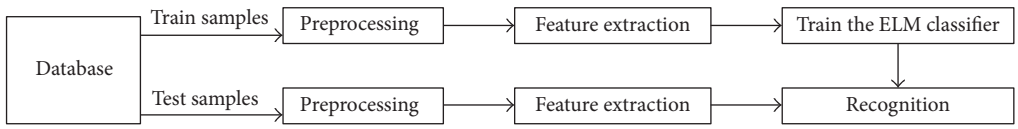


Figure 1: Wear particles recognition based on ELM

which can be written compactly as $\mathbf{H}\beta = \mathbf{T}$, with

$$\mathbf{H} = \begin{pmatrix} \phi(\mathbf{w_1}\mathbf{x_1} + b_1) & \cdots & \phi(\mathbf{w}_L\mathbf{x_1} + b_L) \\ \vdots & \ddots & \vdots \\ \phi(\mathbf{w_1}\mathbf{x}_N + b_1) & \cdots & \phi(\mathbf{w}_L\mathbf{x}_N + b_L) \end{pmatrix} \quad (3)$$

$$\beta = \left(\beta_1^T \cdots \beta_L^T\right),$$

$$T = \left(t_1^T \cdots t_N^T\right).$$

Finding the output weights β from the hidden layer outputs $\mathbf{H}$ and targets is a linear regression problem. In the general case of $N \neq d$, a minimum L^2-norm solution is given by the Moore-Penrose generalized inverse, or pseudoinverse, of the matrix $\mathbf{H}$ denoted as $\mathbf{H}\dagger$ [29]. The training of ELM requires no iterations, and the most computational efficient part is the calculation of the pseudoinverse of the matrix $\mathbf{H}_{(NsL)}$, which makes ELM an extremely fast artificial neural networks method.

3. Proposed Method

Extreme learning machine (ELM) is a new machine learning algorithm. It is increasingly favored by many researchers due to its simple structure, fast learning speed, and good generalization performance. This part will introduce extreme learning machine (ELM) method into the wear particles image recognition. The specific flow chart is shown in Figure 1

The exact procedures are as follows: The first four steps are image preprocessing as shown in Figure 2, which include the steps of 3D media filter, K-means clustering segmentation, region growing, morphology expansion, and erosion; the fifth step is feature extraction and the last step is recognition.

Step 1 (the three-dimensional median filter [30]). Apply the median filter to the three components of RGB color images; then use the relevant algorithms incorporating three components to get three-dimensional image of median filter. The change of the picture is shown in Figure 3.

Step 2 (K-means clustering segmentation [31]). K-means clustering is used to segment wear particles images in Lab color mode. The calculation of 3D color images needs more computer memory and is time consuming, but the characteristic information of 3D color images contributes to the wear particles recognition. Compared with three-dimensional color images, two-dimensional color images not only have quick computing speed, but also can be well segmented. We apply K-means clustering to the two-dimensional color images; then we can get the wear particle image that contains the color information. We choose the Lab color mode for its relatively small mutual association between three components. As (a, b) component represents the color change and L component represents the change of brightness in a Lab mode image, we use (a, b) component for K-means clustering. Firstly, the input of wear particle image is transformed from RGB space to Lab space. Randomly generate three initial clustering points for K-means clustering algorithm. At last, the cluster region with the most complete target region is selected as the target segmentation region.

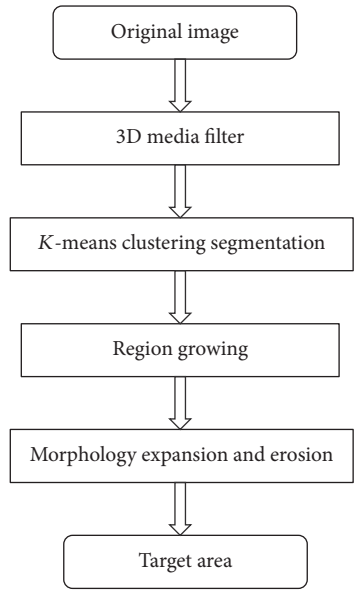


Figure 2: Image preprocessing.

Step 3 (region growing [32]). K-means clustering cannot extract the target area and just simply labeled it. After clustering, we use region growing method to extract the interested area and remove the grains around it.

Step 4 (morphology expansion and erosion). Corrosion and expansion are two important operations of mathematical morphology, which can make the segmentation target area closing, remove the holes in the target area, and make the segmentation region more even. The area that we are interested in extracted by region growing may have holds and rough edges. It requires using mathematical morphology method for further processing in order to get a complete wear particle image. The changes of the processed image are shown in Figure 4.

Step 5 (feature extraction). Due to the fact that different wear particles have different characteristics as shown in Figure 3, different characteristic parameters need to be extracted for recognition. The most obvious characteristic of red oxide is color, so we extract the first-order origin matrix, second-order center matrix, and third-order center matrix of H, S,

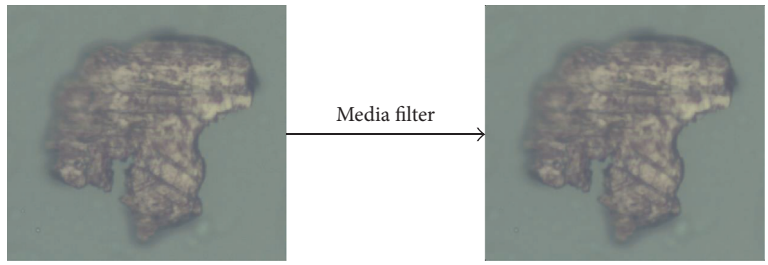


Figure 3: The three-dimensional median filter.

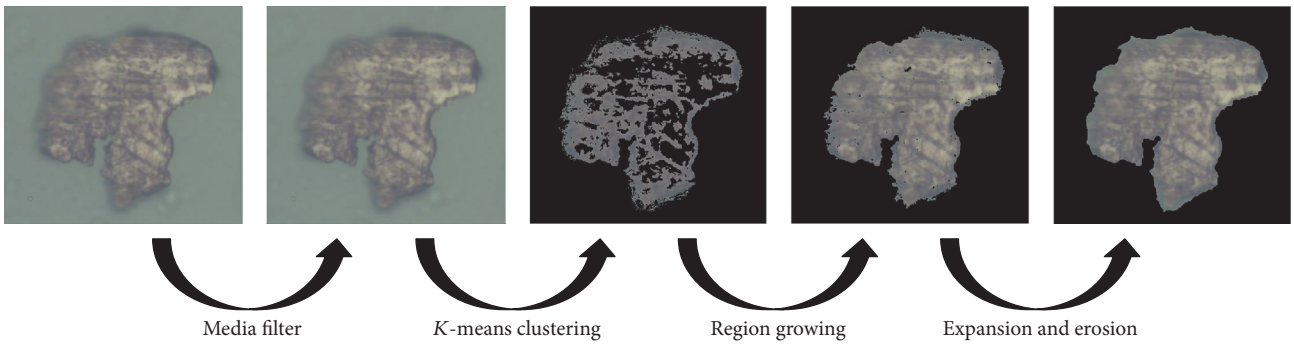


Figure 4: Changes of the image in the preprocessing.

and V components in the HSV color space as red oxide's feature. Fatigue wear particles showed very similar morphological characteristics. The majority of fatigue wear particles are laminar particles. They had smooth flat surfaces and irregular contours. Based on the characteristics of fatigue wear particle, its HoG feature is extracted for classification. For the cutting wear particle, its shape feature is obvious. We get its area, perimeter, equivalent diameter, roundness, aspect ratio, and concavity which is due to the reflection of light and another important basis to recognize the spherical particles. This method uses the following characteristics of spherical particles to identify them: area, perimeter, equivalent diameter, roundness and slenderness ratio, concavity, energy, entropy, moment of inertia, local stability, R mean value, G mean value, and B average value as well as R, G, and B standard deviation. The surface of fatigue wear is relatively rough, characterized by severe galling, parallel scratches, or partial oxidation and irregular edge contour. As scratch is an important feature to recognize fatigue wears, we extracted its Tamura features.

Step 6 (using extreme learning machine for recognition). We use the extracted features to train the ELM classifier and then use the trained network for wear particle recognition.

4. Experiments

4.1. Experimental Database. In this paper, the experimental database was collected from Guangdong provincial Key Laboratory of Petrochemical Equipment Fault Diagnosis. Lubricating oil samples of petrochemical plant machinery were adopted to make ferrogram through using analytical ferrograph. Through a double light microscope, the morphological features and distribution were observed and the database was set up by shooting featured particles' images trough CDD. The database consists of five typical ferrography abrasive particles, with totally 149 particles pictures. There are 33 red oxide images, 42 fatigue wear particles images, 29 cutting wear particles images, 18 spherical wear particles images, and 27 severe sliding wear particles images. The size of the images is 1024 × 768. Five kinds of wear particles are shown in Figure 5.

Table 1: Average recognition rate.

Training percentage (%)	Average recognition rate (%)		
	70	80	90
Red oxide	90.00	100	100
Fatigue	80.77	91.25	100
Cutting	77.78	88.33	100
Spherical	100	100	100
Severe sliding	85.00	100	100

4.2. Results of Experiments. We conduct five experiments; each experiment only recognizes one of the five wear particles. Take the red oxide as an example; we extract color characteristics of all particles and use the ELM to classify them into two categories, red oxide and non-red oxide; thus we recognize the red oxide. According to this method, we recognize fatigue, cutting, and spherical and severe sliding wear particles.

To test the performance of the proposed method, three sets of experiments had been carried out for one kind wear particle. 70%, 80%, and 90% of each type of wear particles images are used for training and the rest of them for test. The result of the experiments is shown in Table 1.

Table 2: Average recognition rate of three classifiers (%).

classifier and training percentage (%)	BP				SVM				ELM			
	70	80	90	Average training time (s)	70	80	90	Average training time (s)	70	80	90	Average training time (s)
Red oxide	99.44	100	100	0.26	84.62	87.50	90.00	0.19	90.00	100	100	**0.14**
Fatigue	82.00	88.78	90	1.43	76.00	76.00	80.00	0.22	80.77	91.25	100	**0.18**
Cutting	85.00	92.00	95.00	0.19	87.50	90.00	90.00	0.09	77.78	88.33	100	**0.07**
Spherical	87.40	95.00	97.00	0.28	80.00	82.00	85.00	0.15	100	100	100	**0.13**
Severe sliding	83.00	88.00	94.05	0.21	78.95	88.89	91.57	0.11	85.00	100	100	**0.07**

Red oxide Fatigue Cutting Spherical Severe sliding

Figure 5: Five kinds of wear particles.

We compared the proposed method with two other classification methods, which are BP [33] and SVM [34]. We use the same features which we used to train the ELM to train the BP and SVM and then test them with the same samples. Table 2 shows that the recognition rates for training images and the average training time.

4.3. Discussion. Table 1 shows the results of the experiments. The recognition rate of red oxide, spherical wear particles, and severe sliding wear particles is great and can reach 100%. The reason why the recognition rate of cutting wear particles is not as good as the above three classifications is the shape features which we have chosen. For some short, thick, and big cutting wear particles, its aspect ratio is not obvious. The computer may mix the cutting wear particles with parts of fatigue wear particles and severe sliding wear particles so that it leads to the low recognition rate. However, for the fatigue wear particles, because the scratched parts of wear particles may not be obvious or not too many and Tamura features cannot represent it well, it causes the relatively low recognition rate.

As we extract different features for different wear particles, the average training time of the five wear particles is different. we can see from Table 2 that ELM has a good time efficiency. For the same kind of wear particle, the BP's recognition rate is close to ELM, but its time efficiency is much lower than ELM. Among the three kinds of classifiers the SVM's performance is the lowest on both recognition rate and time efficiency.

5. Conclusion

In this paper, ELM is introduced into the wear particles image recognition. Different from traditional method, each time only one of the five wear particles is recognized. This avoids the simultaneous extraction of various wear particle characteristics, resulting in redundancy features, and achieves better classification results. However, as shown from the experimental results, the recognition rate of fatigue and cutting wear particles are to be improved. Future work will include how to get robust wear particle features and improve the recognition rate based on ELM.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was supported by the National Natural Science Foundation of China under Grant no. 61502338 and no. 61502339, the 2015 Key Projects of Tianjin Science and Technology Support Program no. 15ZCZDGX00200, the Open Fund of Guangdong Provincial Key Laboratory of Petrochemical Equipment Fault Diagnosis no. GDUPTKLAB201504, and the Fund of Tianjin Food Safety & Low Carbon Manufacturing Collaborative Innovation Center.

References

[1] B. J. Roylance, I. A. Albirdewi, and M. S. Laghari, "Computer-aided vision engineering (CAVE): quantification of wear particle morphology," *Lubrication Engineering*, vol. 50, no. 2, pp. 111–116, 1994.

[2] S. Raadnui and B. J. Roylance, "The classification of wear particle shape," *Lubrication Engineering*, vol. 51, no. 5, pp. 432–437, 1995.

[3] K. K. Yeung, A. J. McKenzie, D. Liew, and G. A. Luoma, "Development of computer-aided image analysis for filter debris analysis," *Lubrication Engineering*, vol. 50, no. 4, pp. 293–299, 1994.

[4] F. T. Barwell, "The contribution of particle analysis to the study of wear of metals," *Wear*, vol. 90, no. 1, pp. 167–181, 1983.

[5] A. D. H. Thomas, T. Davies, and A. R. Luxmoore, "Computer image analysis for identification of wear particles," *Wear*, vol. 142, no. 2, pp. 213–226, 1991.

[6] T. Pancewicz and I. Mruk, "Holographic contouring for determination of three-dimensional description of surface roughness," *Wear*, vol. 199, no. 1, pp. 127–131, 1996.

[7] T. B. Kirk, G. W. Stachowiak, and A. W. Batchelor, "Fractal parameters and computer image analysis applied to wear particles isolated by ferrography," *Wear*, vol. 145, no. 2, pp. 347–365, 1991.

[8] M. G. Hamblin and G. W. Stachowiak, "A multi-scale measure of particle abrasivity, and its relation to two-body abrasive wear," *Wear*, vol. 190, no. 2, pp. 190–196, 1995.

[9] K. Xu, A. R. Luxmoore, L. M. Jones, and F. Deravi, "Integration of neural networks and expert systems for microscopic wear particle analysis," *Knowledge-Based Systems*, vol. 11, no. 3-4, pp. 213–227, 1998.

[10] Y. Tian, J. Wang, Z. Peng, and X. Jiang, "A new approach to numerical characterisation of wear particle surfaces in three-dimensions for wear study," *Wear*, vol. 282-283, pp. 59–68, 2012.

[11] Z. Peng and T. B. Kirk, "Computer image analysis of wear particles in three-dimensions for machine condition monitoring," *Wear*, vol. 223, no. 1-2, pp. 157–166, 1998.

[12] G. P. Stachowiak, G. W. Stachowiak, and P. Podsiadlo, "Automated classification of wear particles based on their surface texture and shape features," *Tribology International*, vol. 41, no. 1, pp. 34–43, 2008.

[13] P. J. van Otterlo, *A Contour Oriented Approach to Digital Shape Analysis*, Kluver, Amsterdam, The Netherlands, 1988.

[14] M. S. Laghari and Q. A. Memon, "Knowledge based wear particle analysis," *International Journal of Information Technology*, vol. 1, no. 3, pp. 91–95, 2004.

[15] J. Q. Wang and X. L. Wang, "A wear particle identification method by combining principal component analysis and grey relational analysis," *Wear*, vol. 304, no. 1-2, pp. 96–102, 2013.

[16] W. H. Wang and Y. H. Yin, "Abrasive identification system based on radial basis function neural network," *Tribology*, vol. 123, no. 4, pp. 340–343, 2003.

[17] D. Q. Gu, "Ferrography wear pattern recognition based on support vector machine," *China Mechanical Engineering*, vol. 17, no. 13, pp. 1391–1394, 2006.

[18] C. Q. Yuan and X. P. Yan, "Recognition of the type of abrasive," *Lubrication*, vol. 32, no. 3, pp. 21–23, 2007.

[19] B. H. Luo, Y. W. Huang, and Y. F. Liu, "Wear particles identification based PCA-BP neural network," *Lubrication*, vol. 35, no. 6, pp. 117–120, 2010.

[20] W. Zhou, B. Jing, and S. Deng, "Aeroengine abrasive identification based on IGA and LS-SVM," *Lubrication*, vol. 38, no. 1, pp. 14–18, 2013.

[21] R. M. Haralick, I. Dinstein, and K. Shanmugam, "Textural features for image classification," *IEEE Transactions on Systems, Man and Cybernetics*, vol. 3, no. 6, pp. 610–621, 1973.

[22] B. H. Tamura, S. Mori, and T. Yamawaki, "Texture features corresponding to visual perception," *IEEE Transactions on Systems, Man, and Cybernetics*, vol. 8, no. 6, pp. 460–473, 1978.

[23] N. Dalal and B. Triggs, "Histograms of oriented gradients for human detection," in *Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR '05)*, vol. 1, pp. 886–893, IEEE, San Diego, Calif, USA, June 2005.

[24] G.-B. Huang, Q.-Y. Zhu, K. Z. Mao, C.-K. Siew, P. Saratchandran, and N. Sundararajan, "Can threshold networks be trained directly?" *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 53, no. 3, pp. 187–191, 2006.

[25] G.-B. Huang, Q.-Y. Zhu, and C.-K. Siew, "Extreme learning machine: theory and applications," *Neurocomputing*, vol. 70, no. 1–3, pp. 489–501, 2006.

[26] Y. Miche, M. van Heeswijk, P. Bas, O. Simula, and A. Lendasse, "TROP-ELM: a double-regularized ELM using LARS and Tikhonov regularization," *Neurocomputing*, vol. 74, no. 16, pp. 2413–2421, 2011.

[27] G.-B. Huang, H. Zhou, X. Ding, and R. Zhang, "Extreme learning machine for regression and multiclass classification," *IEEE Transactions on Systems, Man, and Cybernetics, Part B: Cybernetics*, vol. 42, no. 2, pp. 513–529, 2012.

[28] G.-B. Huang, L. Chen, and C.-K. Siew, "Universal approximation using incremental constructive feedforward networks with random hidden nodes," *IEEE Transactions on Neural Networks*, vol. 17, no. 4, pp. 879–892, 2006.

[29] C. R. Rao and S. K. Mitra, *Generalized Inverse of a Matrix and Its Applications*, John Wiley & Sons, Berkeley, Calif, USA, 1971.

[30] W. Yu, Y. Ma, L. Zheng et al., "Research of improved adaptive median filter algorithm," in *Proceedings of the 2015 International Conference on Electrical and Information Technologies for Rail Transportation (EITRT '15)*, Springer, Hunan Province, China, 2016.

[31] J. A. Hartigan and M. A. Wong, "A K-means clustering algorithm," *Applied Statistics*, vol. 28, no. 1, pp. 100–108, 2013.

[32] S.-Y. Wan and W. E. Higgins, "Symmetric region growing," *IEEE Transactions on Image Processing*, vol. 12, no. 9, pp. 1007–1015, 2003.

[33] D. E. Rumelhart, G. E. Hinton, and R. J. Williams, "Learning representations by back-propagating errors," in *Neurocomputing: Foundations of Research*, pp. 533–536, MIT Press, Cambridge, Mass, USA, 1986.

[34] C. Cortes and V. Vapnik, "Support-vector networks," *Machine Learning*, vol. 20, no. 3, pp. 273–297, 1995.

Hindawi
Journal of Electrical and Computer Engineering
Volume 2017, Article ID 9720396, 7 pages
https://doi.org/10.1155/2017/9720396

Research Article

Online Behavior Analysis-Based Student Profile for Intelligent E-Learning

Kun Liang,[1] Yiying Zhang,[1] Yeshen He,[2] Yilin Zhou,[3] Wei Tan,[2] and Xiaoxia Li[2]

[1]*College of Computer Science and Information Engineering, Tianjin University of Science & Technology, Tianjin 300222, China*
[2]*China GRIDCOM Co., Ltd., Shenzhen 518031, China*
[3]*Xiamen Great Power Geo Information Technology Co. Ltd., Xiamen, Fujian 361000, China*

Correspondence should be addressed to Yiying Zhang; yiyingzhang@tust.edu.cn

Received 15 November 2016; Accepted 23 February 2017; Published 13 March 2017

Academic Editor: Sook Yoon

With the development of mobile platform, such as smart cellphone and pad, the E-Learning model has been rapidly developed. However, due to the low completion rate for E-Learning platform, it is very necessary to analyze the behavior characteristics of online learners to intelligently adjust online education strategy and enhance the quality of learning. In this paper, we analyzed the relation indicators of E-Learning to build the student profile and gave countermeasures. Adopting the similarity computation and Jaccard coefficient algorithm, we designed a system model to clean and dig into the educational data and also the students' learning attitude and the duration of learning behavior to establish student profile. According to the E-Learning resources and learner behaviors, we also present the intelligent guide model to guide both E-Learning platform and learners to improve learning things. The study on student profile can help the E-Learning platform to meet and guide the students' learning behavior deeply and also to provide personalized learning situation and promote the optimization of the E-Learning.

1. Introduction

As an effective way for education, the E-Learning supported more knowledge and skills than the traditional education and also is beyond the restriction of time and space based on new information and communication technologies [1]. MOOC (massive open online courses) is a representative online education platform. And the Coursera is the largest MOOC platform in the world, established by the USA top universities network learning platform. At present, there are about 1563 courses and more than 17 million registered students on the platform. Based on edX, the largest MOOC platform (http://www.xuetangx.com) is developed by Tsinghua University, in China. It has about 3 million members which are from more than 200 countries and regions [2].

E-Learning education has had a rapid development. Figure 1 shows that the number of Chinese E-Learning users reached 90.992 million in 2015, which is with an annual growth rate of 56%; it will grow to 120 million people by 2017.

However, although more and more people are concerned about the E-Learning platform, there are only 7%–9% learners who completed MOOC's course according to Coursera statistics data [3]. Therefore, it is very necessary to improve the quality of learning and optimize the teaching mechanism to push the course accurately. The student profile is a novel method to analyze the basic information and learn the behavior of online learners. Through the establishment of student profile, it is to achieve personalized situation construction and learn process guidance, which plays a positive role in promoting online learning.

The student profile is a figure portrait analysis based on the big data and labeling. We collect, process, and analyze the data generated in the learners' behavior, for an information description of individual students or groups. According to the theory of behavioral psychology, use of the student profile to analyze the data on student behavior can reflect the students' behavior characteristics and psychodynamics. For example, the Education Big Data Research Institute of

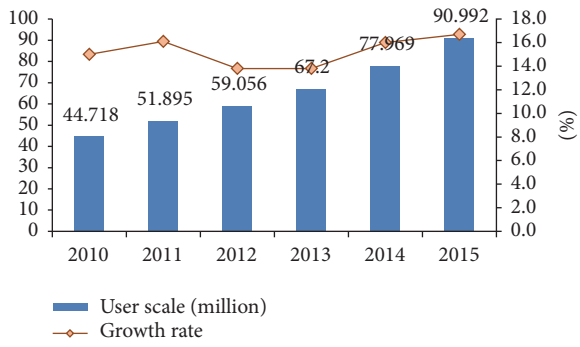


Figure 1: 2010–2015 E-Learning user scale.

UESTC (University of Electronic Science and Technology of China) cooperate with other departments in developing the Student Profile System, which can give an early warning about failing the exam [4]. Similarly, Southwest Jiaotong University collected and analyzed the big data drawn students on campus "behavior track" model to predict students' future development [5]. In foreign countries, researchers have proved that using the big data to analyze the students' learning behavior such as reading course information online, submitting homework, and exchanging detected the warning information in poor learning performance. According to this warning information, the teachers made recommendations for improvement and given some guidance, to ensure that the students learn effectively. However, "student profile" has been applied in the education field; the big data profile technology combined with education has a very important practical significance.

In view of the E-Learning data, we use the big data technology to analyze the E-Learning characteristic, and the main research contents of this paper are as follows: (1) analysis of factors affecting the student profile. The students are classified according to age, and then we define the relations between student behavior and duration; (2) building a student profile model. We collected and preprocessed data and dug out the connection on the students' learning behavior attributes by the Jaccard algorithm, to form the student profile finally; (3) analysis on the student profile. It is to contribute to the E-Learning platform to better understand the learning behavior of students.

2. The Definition of the Student Profile

The student profile described the learning characteristics from multidimensions and multiangle. It includes the analysis indicators and influencing factors, such as student behavior, data collection, data cleaning, and student profile building and analyzing [6].

2.1. Student Definition. The main research on the student profile is the students in the school or E-Learning platform. Assume the student set as follows:

$$S = \left\{ s_i^j \mid s_1^j, s_2^j, \ldots, s_n^j \right\}, \quad (1)$$

Table 1: Learners' age segment table.

Years	Symbol	Example
<17	a	It means student s_1 is under the 17 years
18–24	b	It means student s_2 is 18–24 years
25–34	c	It means student s_3 is 25–34 years
35–54	d	It means student s_4 is 35–54 years
>55	e	It means student s_5 is over 55 years

Table 2: Preset 12 kinds of online learning behavior.

ID	Learning behavior
$b1$	Browse learning goals
$b2$	Text learning
$b3$	Multimedia learning
$b4$	Practice online
$b5$	Search & view reference
$b6$	Make notes
$b7$	Download courseware
$b8$	Question online
$b9$	Exchange interaction
$b10$	Communicate through E-mail
$b11$	Rest or listen to music
$b12$	Talk about QQ when learning

where s_i^j indicates the students classified by age; i means the individual; j denotes the student age level (for convenience, the superscript is usually omitted as s_i), and there are 5 types of students classified in different age, which includes less than 17 years old, 18–24 years old, 25–34 years old, 35–54 years old, and over 55 years old, as shown in Table 1.

According to age, we can predict learner profile information and further dig into the characteristics of students learning.

2.2. Definition of Learning Behavior. The online learning behavior is the kinds of learning behavior under the network environment. We focus on digging out the characteristics of learners from online learning behavior after analysis, in order to understand the student's performance. The core of learning behavior is the operation of online learning behaviors [7, 8]. For example, learner clicks on a course, browses the page, plays the video, and downloads the relevant courseware. The "click" and "download" are the two operations about learning behaviors. The behavior set (behavior) in the student profile is defined as

$$B = \left\{ b_i \mid b_1, b_2, \ldots, b_n \right\}, \quad (2)$$

where b_i indicates varieties of behavior and includes 12 kinds of learning behaviors, such as learning goal, text learning, online practice, and making notes, as shown in Table 2.

Since the online learning is the period of time process with online learning behavior, it is an important parameter to evaluate the quality of online learning. In particularly, it

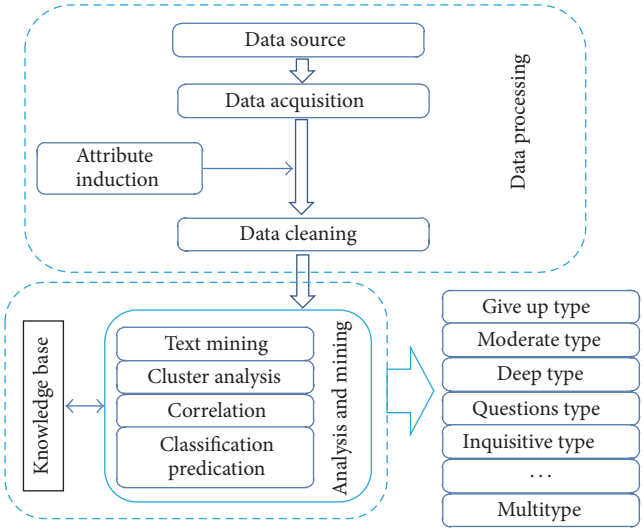


Figure 2: Student profile model.

reflects the degree of focus on learning. The duration set (timeslot) in student profile is defined as follows:

$$T = \{t_i \mid t_1, t_2, \ldots, t_n\}, \tag{3}$$

where t_i indicates various of durations; it is divided into periods as 1–10 minutes, 10–20 minutes, 20–30 minutes, 30–40 minutes, 40–50 minutes, 50–60 minutes, and so forth.

According to the above definitions, $s_1 \cdot b_i$ means the behavior b_i of the student s_1. We suppose behavioral differences $\Delta b = s_1 \cdot b_i - s_2 \cdot b_i$; it represents the students' differences in a certain behavior. For example, suppose college learner s_1, job learner s_2, and online training b_1. We adopt $\Delta b = s_1 \cdot b_1 - s_2 \cdot b_1$ to analyze the differences between college learner and job learner in the behavior of the training online.

3. Student Profile Model

The student profile has a complete model to guide us to analyzing the students' online learning process. The student profile model (Figure 2) includes data collection, data cleaning, and portrait analysis. Firstly, data collection can obtain the original data by means of E-Learning platform or questionnaire survey. Secondly, we utilize the attribute reduction to clean the original data and then employ the Jaccard coefficient algorithm for data analysis and data mining. Finally, we label the students according to results of the analysis in order to form the student profile. Simultaneously, we build the knowledge base (KB) for storage of knowledge sheet about the student profile [9]. In student profile model, KB is parallel to the data mining level and interaction. From the knowledge base, we take some of the student profile set to dig into and analyze and store the results in the KB. Therefore, the KB of the student profile has the self-growth and self-perfection ability.

3.1. Data Acquisition. Data acquisition includes four categories, such as student user registration data, web log data, learning behavior data, and learning content preference data. The student user registration data is mainly analysis on the characteristics of the learners, including user name, sex, date of birth, geography, occupation, and hobbies. The web log data reflects the operation of E-Learning platform, including active number, page views, access time, activation rate, and learning path. The learning behavior data is helpful for statistics analysis of online learning performance, including learning time, learning activities, learning resources, and examination results. The learning content preference data can be used to analyze the preference of courses or teachers, including browse/collection content, review content, and interactive content. It can be helpful for pushing the course accurately.

3.2. Data Cleaning. Data cleaning preprocesses the original data, removes redundant data, retains the useful data for the analysis, and organizes the data into a standard format. Because the interference of abnormal values often results in data mining distortion [10–12], data cleaning improves the accuracy of data analysis and ensures the reliability of data mining.

Attribute induction is the most important process of collecting the data source pretreatment. Suppose the original data field to $\{G_1, G_2, \ldots, G_{N_G}\}$, where N_G is the dimension of the original data field. Set the vector A, where $A \in \{G_1, G_2, \ldots, G_n\}$ and A means desirable property. By the property statute of data preprocessing to give all the desired properties, the attribute induction method is defined as sig, cleaning the data to get the following results:

$$\{A_1, A_2, \ldots, A_{N_A}\} = \text{sig}\{G_1, G_2, \ldots, G_n\}, \tag{4}$$

in which N_A is an important property for the dimension data field. In our solution, we calculate the importance of the property and select the same behavior analysis related to the desired attributes. Our solution does not deal with the concrete implementation of the attribute induction about sig.

4. Student Profile Analysis

In this section, we calculate the similarity in the behavior set of different students, through the Jaccard coefficient similarity algorithm compared with the online behavior characteristics and duration of learners, similar properties classified as a class, and the difference properties classified to different classes.

4.1. Student Behavior Feature Similarity Calculation. Similarity among the behavioral characteristics of different students objects belongs to nonnumeric objects; we adopt Jaccard coefficient calculated similarity [13, 14]. The similarity formula is as follows:

$$r_{ijk} = \text{Jaccard}\left(s_i \cdot b_k, s_j \cdot b_k\right) = \left|\frac{s_i \cdot b_k \cap s_j \cdot b_k}{s_i \cdot b_k \cup s_j \cdot b_k}\right|, \tag{5}$$

where $s_i \cdot b_k$ and $s_j \cdot b_k$ represent the behavior b_k of students s_i and s_j. Suppose the student s_i belongs to KB; we compare

```
(1) Input: ss //ss is a set of students
(2) Output: R[i][j]
(3) /*similarity of behavior characteristics
    between student i and j.*/
(4) Dim R As Float[][]; //similarity matrix R
(5) Dim i, j, n As int;
(6) Dim k As float;
(7) Begin
(8) n = ss.length;
(9) // get the number of Student set
(10) For i = 0 To n {
(11)   For j = i + 1 To n {
(12)     For k = 0 To |B|
(13)  //|B| is the number of behavior types
(14)     {
(15)     r[i][j][k] = Jaccard(ss[i][j][k]);
(16)     }
(17)     R[i][j] = Sim(ss[i], ss[j])
(18) }}
(19) Return R
(20) End
```

Algorithm 1: Jaccard coefficient algorithm.

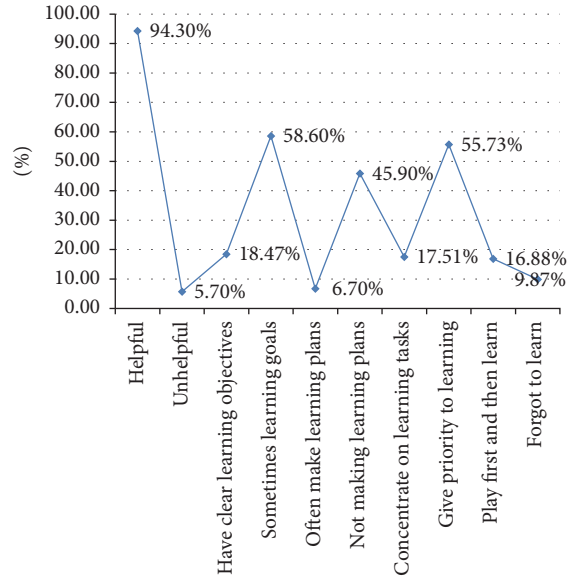


Figure 3: Learning attitude analysis.

s_j to s_i. If s_j and s_i similarity difference is too large, it will be added to the KB as a new class.

User similarity is defined as

$$R_{ij} = \mathrm{Sim}\left(s_i, s_j\right) = \frac{1}{M}\sum_{k=1}^{M} r_{ijk}, \tag{6}$$

in which $\mathrm{Sim}(s_i, s_j)$ indicates the similarity between students s_i and s_j; M indicates the behavior dimension attributes of student set S; r_{ijk} represents the similarity about property k between students s_i and s_j, and $i \neq j$.

According to similarity calculation, we obtain $\mathrm{Matrix}_{\mathrm{sim}}$ as follows:

$$\mathrm{Matrix}_{\mathrm{sim}} = \begin{bmatrix} 1 & R_{12} & R_{13} & & \cdots & \cdots & R_{1N} \\ 0 & 1 & R_{23} & \cdots & \cdots & \cdots & R_{2N} \\ 0 & 0 & 1 & & \cdots & \cdots & R_{3N} \\ & \vdots & & \ddots & & \vdots & \\ & & & & 1 & \vdots & \vdots \\ & & & \cdots & 0 & \ddots & R_{N-1,N} \\ 0 & & & & 0 & 0 & 1 \end{bmatrix}. \tag{7}$$

It is an upper triangular matrix, where $0 < R_{ij} < 1$, R_{ij} denoted line i and row j, and it is the similarity of behavior characteristics between student i and student j.

Jaccard coefficient algorithm is described as shown in Algorithm 1.

According to the result of Jaccard coefficient algorithm, we can label the learners. Suppose that the calculation is from two dimensions about learning behavior and duration. The student could be labeled "depth learning type" if learning performance takes more than 60 minutes. Similarly, the student could be labeled "tasted type" if learning performance takes less than 10 minutes. Additionally, based on the frequency of online question and online training, we labeled "inquisitive type," "application type," and "perseverance type." The specific labeling method does not repeat them here. We only proposed Jaccard coefficient algorithm and labeling idea for readers.

4.2. Learning Attitude Analysis. The students' learning attitude makes a difference to learning effect. We collected data from 18–24-year-old student group and statistically analyzed it, such as whether having the clear learning goal or not and whether having the learning plan or not. As shown in Figure 3, it reflects the learners' subjective initiative and recognition to E-Learning courses, which contributes to analyzing the interference factors of E-Learning.

In the 18–24-year-old group, there are about 94.3% learners who believed that E-Learning courses are helpful for them. There are 18.47% learners who have the clear learning objectives, and 58.6% learners have clear learning objectives occasionally. This ratio reflects that most students are quite blindly taking the E-Learning course. There are 45.9% learners who have no learning plan, and 55.73% learners are learning online while doing other things, such as QQ chat and listening to music. According to Figure 3, we can conclude that E-Learning course requires definite objective, inner motive, synchronous feedback, and independence of the learners. Since the online learners have much recognition of online courses, the E-Learning platform has the broader prospects for development.

4.3. Duration Analysis of Online Learning Behavior. The learning behavior of online learners is diversity. To a certain

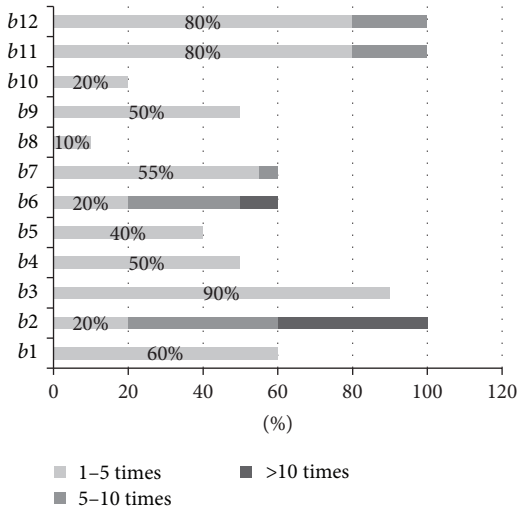


Figure 4: Learners' online learning behavior statistics.

extent, the frequency of learning behavior reflects the attention of learners to the learning resources. According to the frequency statistics [15], we analyzed which course resources are more likely to be accepted by the learners as shown in Figure 4.

In Figure 4, behaviors 1–7 are an independent learning behavior. Behaviors 8–11 are an interactive learning behavior. Behaviors 11-12 have nothing to do with learning. Most learners browse the text and make notes frequently; therefore the text resource is the most popular type of resources. About 90% learners will first browse multimedia resources. Only 50% of the learners will participate in online exercises and only 1–5 times. About 60% learners will choose to view the learning objectives before studying the course, and the number of views is generally less than 5 times. 80% learners will rest; listen to music; or QQ chat 1–5 times during the learning process. This shows that most learners have a sense of learning strategies. They are interested in multimedia resources, but they are more used to learning through reading text resources. Online interactive learning behavior is low [16, 17]. Learning in the network easily causes fatigue and is affected by chat and other factors.

4.4. Intelligent Learning Guide

4.4.1. Achievement Predicting. MOOC is a popular E-Learning platform, whose importance is reflected in the pass rate of the course. In view of the low pass rate on MOOC [15, 18], it is supposed that a course is expected to be predicting whether the learner will eventually get the certificate according to the characteristics of the learner's behavior. And we also try to verify the previous analysis and conclusions.

We suppose that the behavioral data was collected from the registered learners on Data Structures and Algorithm Analysis (DSAA) course for the first 5–7 weeks. After filtering the behavior of unregistered learners in the data record, the sample statistics are shown in Table 3.

Table 3: Number of samples.

Course	1–5 weeks	1–6 weeks	1–7 weeks
DSAA	9401	9543	9990

Define each course having i learners and each learner having n characteristic values

$$C = \{C_1, \ldots, C_n\} \in R^{i \times n}. \tag{8}$$

Predictive value is

$$P = f(C) \in R^i, \quad p \in \{0, 1\}, \tag{9}$$

in which C_n denotes a course; $p = 0$ means it is unlikely to get a certificate, and $p = 1$ means you might get a certificate; and $f(C)$ are a predictive function.

We have chosen the characteristic values of the courses, and they have an impact on result about learner's study. From Table 2, they are the number of text learning behaviors ($b2$), the number of multimedia learning behaviors ($b3$), the number of online practice behaviors ($b4$), the number of download courseware behaviors ($b7$), and the number of online questions behaviors ($b8$).

According to this course, the data set is divided into training set, validation set, and test set randomly; the ratio is 3 : 1 : 1. To use the training parameters with the training set for each experiment, select the optimal parameters for the validation set, and then use the test set to calculate the indicators. We used three classification models: linear discriminant analysis (LDA), logistic regression (LR), and linear support vector machine (LSVM). They are used to predict the course, and the experimental results are shown in Table 4.

The experimental results show that the three classifiers show consistent performance, and the accuracy is higher. Figure 5 shows the time series changes of the predicted F-core by DSAA course. According to the learners' learning behaviors in the first half of the semester, we accurately predicted the final study results, whether it can obtain the certificate [2]. In fact, if a learner performs well in the first half of the semester, it is shown that he is firm and capable. He is more likely than others to get the certificate finally.

4.4.2. Emotional Guide Analysis. Achievement prediction can help E-Learning platform to discover the abnormal situation, so as to timely intervention and guidance for students. Because online learners are mainly independent learners, they are in isolation and lack emotional communication, which makes them lack emotional support and have difficulty in maintaining long-term learning enthusiasm [19]. It is an effective way to solve the emotional deficiency by constructing an intelligent learning guiding mechanism in the student profile and providing some emotional help and support services to the learners during the learning process [20].

According to the E-Learning resources and learners' behaviors, we can present an evaluation model supported by the duration, frequency of access, concentration, and

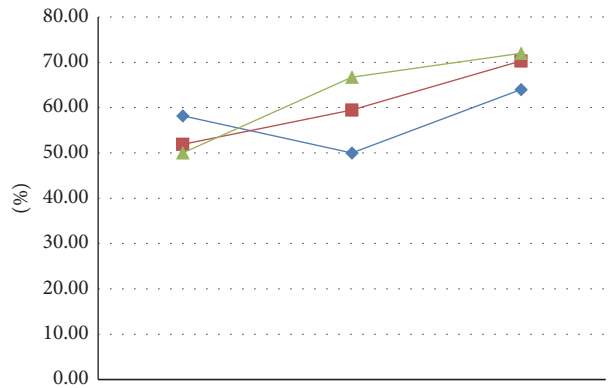


Figure 5: Sequential variation of DSAA course.

Table 4: Comparison of the forecasting results.

Course	Classifier	Accuracy	Precision	Recall	F-score
DSAA	LDA	99.6	50.0	88.9	64.0
	LR	99.5	65.0	76.5	70.3
	LSVM	99.7	64.3	81.8	72.0

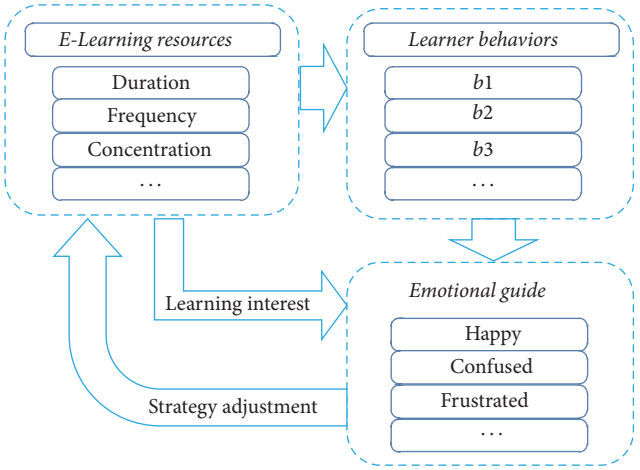


Figure 6: Emotional evaluation model.

other parameters to evaluation learners' emotion as shown in Figure 6.

5. Conclusion

In this paper, we deeply study the online learning behavior and build the student profile with big data processing technology. Firstly, we analyze the characteristics of learners and the factors that influence the learning behavior and use the method of attribute reduction to cleaning the data. Then, we calculate the similarity of students' behavior and use the Jaccard coefficient algorithm to classify the students. Finally, the student profile has been established as well as visual analysis. We confirm that E-Learning course requires definite objective, inner motive, synchronous feedback, and independence of the learners. The student profile helps the student to understand their learning situation, to find their own problems, and to improve the completion rate of online courses. With the continuous accumulation of education data and in-depth development, the student profile is bound to promote the healthy development of E-Learning. In the future, we will conduct in-depth study on the fragmentation of knowledge aggregation online.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Acknowledgments

This work was supported by the Tianjin University of Science and Technology Youth Innovation Foundation (no. 2016LG28).

References

[1] T.-H. Wang, "Developing an assessment-centered e-Learning system for improving student learning effectiveness," *Computers & Education*, vol. 73, pp. 189–203, 2014.

[2] Z. Jiang, Y. Zhang, and X. Li, "Learning behavior analysis and prediction based on MOOC data," *Journal of Computer Research and Development*, vol. 52, no. 3, pp. 614–628, 2015.

[3] C. Bo, M. Wang, A. I. Mørch, N.-S. Chen, Kinshuk, and J. M. Spector, "Research on E-Learning in the workplace 2000–2012: a bibliometric analysis of the literature," *Educational Research Review*, vol. 11, pp. 56–72, 2014.

[4] M. Raspopovic and A. Jankulovic, "Performance measurement of e-learning using student satisfaction analysis," *Information Systems Frontiers*, pp. 1–12, 2016.

[5] C. G. Brinton, S. Buccapatnam, M. Chiang, and H. V. Poor, "Mining MOOC Clickstreams: on the relationship between learner behavior and performance: computer science," https://arxiv.org/abs/1503.06489.

[6] T. Sinha, "'Your click decides your fate': leveraging clickstream patterns from MOOC videos to infer students' information processing & attrition behavior," https://arxiv.org/abs/1407.7143.

[7] Y. Liu and H. Feng, "An empirical study on the relationship between metacognitive strategies and online-learning behavior & test achievements," *Journal of Language Teaching and Research*, vol. 2, no. 1, pp. 990–992, 2011.

[8] S. Dumais, R. Jeffries, D. M. Russell et al., "Understanding user behavior through log data and analysis," in *Ways of Knowing in HCI*, pp. 349–372, Springer, New York, NY, USA, 2014.

[9] I. Jo, T. Yu, H. Lee, and Y. Kim, "Relations between student online learning behavior and academic achievement in higher education: a learning analytics approach," in *Emerging Issues in Smart Learning*, Lecture Notes in Educational Technology, pp. 275–287, Springer, Berlin, Germany, 2015.

[10] I. H. Witten and E. Frank, *Data Mining: Practical Machine Learning Tools & Techniques with Java Implementations*, vol. 13, no. 4, Morgan Kaufmann, Burlington, Mass, USA, 2011.

[11] D. Agrawal, C. Budak, A. El Abbadi, T. Georgiou, and X. Yan, "Big data in online social networks: user interaction analysis to model user behavior in social networks," in *Databases in Networked Information Systems*, vol. 8381 of *Lecture Notes in Computer Science*, pp. 1–16, Springer International Publishing, 2014.

[12] Y. Ar and E. Bostanci, "A genetic algorithm solution to the collaborative filtering problem," *Expert Systems with Applications*, vol. 61, pp. 122–128, 2016.

[13] J. Santisteban and J. Tejada-Cárcamo, "Unilateral weighted Jaccard coefficient for NLP," in *Proceedings of the 14th Mexican International Conference on Artificial Intelligence (MICAI '15)*, pp. 14–20, IEEE, Cuernavaca, Mexico, October 2015.

[14] X. Xian, F. Chen, and J. Wang, "An insight into campus network user behavior analysis decision system," in *Proceedings of the 2nd International Symposium on Computer, Consumer and Control (IS3C '14)*, pp. 537–540, Taichung, Taiwan, June 2014.

[15] H. Khalil and M. Ebner, "'How satisfied are you with your MOOC?'—a research study about interaction in huge online courses," *Journalism & Mass Communication Quarterly*, vol. 5, no. 12, pp. 629–639, 2016.

[16] D. Hempel, S. Sinnathurai, S. Haunhorst et al., "Influence of case-based e-learning on students' performance in point-of-care ultrasound courses: a randomized trial," *European Journal of Emergency Medicine*, vol. 23, no. 4, pp. 298–304, 2016.

[17] D. D. Prior, J. Mazanov, D. Meacheam, G. Heaslip, and J. Hanson, "Attitude, digital literacy and self efficacy: flow-on effects for online learning behavior," *Internet and Higher Education*, vol. 29, pp. 91–97, 2016.

[18] L. Geoffrey, *From E-Reading to E-Learning: A Pedagogical Framework for Online Learning*, 2016.

[19] Huang, *Research on Learner's Emotion Modeling and Its Application in E-Learning*, Central China Normal University, Wuhan, China, 2014.

[20] S. Bhuta, A. Doshi, U. Doshi, and M. Narvekar, "A review of techniques for sentiment analysis of Twitter data," in *Proceedings of the International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT '14)*, pp. 583–591, IEEE, Ghaziabad, India, February 2014.

Hindawi
Journal of Electrical and Computer Engineering
Volume 2017, Article ID 1231794, 7 pages
https://doi.org/10.1155/2017/1231794

Research Article

A Fast and Robust Key Frame Extraction Method for Video Copyright Protection

Yunyu Shi,[1] Haisheng Yang,[2] Ming Gong,[2] Xiang Liu,[1] and Yongxiang Xia[1]

[1]*School of Electronic and Electrical Engineering, Shanghai University of Engineering Science, Shanghai, China*
[2]*Shanghai Media Group, Shanghai, China*

Correspondence should be addressed to Xiang Liu; morningcall@sues.edu.cn

Received 25 November 2016; Accepted 12 February 2017; Published 9 March 2017

Academic Editor: Hui Cheng

The paper proposes a key frame extraction method for video copyright protection. The fast and robust method is based on frame difference with low level features, including color feature and structure feature. A two-stage method is used to extract accurate key frames to cover the content for the whole video sequence. Firstly, an alternative sequence is got based on color characteristic difference between adjacent frames from original sequence. Secondly, by analyzing structural characteristic difference between adjacent frames from the alternative sequence, the final key frame sequence is obtained. And then, an optimization step is added based on the number of final key frames in order to ensure the effectiveness of key frame extraction. Compared with the previous methods, the proposed method has advantage in computation complexity and robustness on several video formats, video resolution, and so on.

1. Introduction

Video data has been increased rapidly due to rapid development of digital video capture and editing technology. Therefore, video copyright protection is an emerging research field and has attracted more and more attention. Digital video watermark is a traditional method for video copyright protection. However there are some faults about the above method and it is not suitable for huge video data on the Internet.

Key frame extraction is a powerful tool that implements video content by selecting a set of summary key frames to represent video sequences. Most of the existing key frames extraction methods are not suitable for video copyright protection, as they do not meet specific requirements.

Generally, key frame extraction techniques can be roughly categorized into four types [1], based on shot boundary, visual information, movement analysis, and cluster method. And then sometimes it could be completed in compressed domain [2]. Nowadays, cluster-based methods are mostly applied in video content analysis research. In these methods, key frame extraction is usually modeled as a typical clustering process that divides one video shot into several clusters and then one or several frames are extracted based on low or high level features [3–6]. The methods in compressed domain usually are not suitable for diverse formats of videos from the Internet. Transcoding may increase time complexity and inaccuracy.

How to achieve a meaningful key frame is an important problem in various communities. The focus of the work is to represent the video content adequately and fast [7, 8]. In this paper, an active detection method is proposed. First, the key frame is defined for video copyright protection. And then, a key frame extraction algorithm based on two-step method with low level features is proposed.

The distinct features of our algorithm are as follows. (1) The definition of key frame is specific for video copyright protection. (2) The method is with lower computation complexity. (3) The method is robust for online videos regardless of video formats, video resolution, and so on.

The rest of the paper is organized as follows. The proposed key frame extraction method is presented in Section 2, while experimental results are listed in Section 3. Finally the conclusions are drawn in Section 4.

32.jpg 33.jpg

34.jpg 35.jpg

Figure 1: Four frames with low gray value extracted from a tested video.

2. The Proposed Key Frame Extraction Method

2.1. Definition of Key Frame for Video Copyright Protection. There are some distinct features about the key frame for video copyright protection. So, the key frame for video copyright protection is defined firstly before video preprocessing and key frame extracting.

The key frames should meet the following three conditions.

(1) The gray value of a key frame is within a certain range to allow viewers to have subjective perception about the video content. Four images with low gray value in Figure 1 are extracted from a single video, which is difficult for almost viewers to recognise the content.

(2) The final key frame sequence must be arranged in chronological order consistent with original video sequence, in order to satisfy temporal features and to be different from the short promotion trailer.

(3) Appropriate redundancy of some key frames is allowed to ensure the periods or intervals along the processing of video content. Figure 2 indicates the condition by selecting four images from a tested video, which are with similar content, that is to say, one judge in the show every once in a while.

In general, radio and television programs need to convey certain visual content; that is, video images that are too dark or too bright do not meet these subjective feelings. Four images in Figure 1 are extracted form a tested video, which are always too dark for viewers to perceive the video content. The phenomenon is sometimes with gradual transitions of shots. In order to distinguish and program trailers and other programs, the intervals between extracted key frames must be consistent with the frames from the original video. As online video piracy is often divided into smaller video files for playback, thus mastering the key frame extraction should allow appropriate redundancy to ensure a period of time. Taking the talent show as an example, the moderator reviewing screen may arise for every player in a game situation, as shown in Figure 2; then the time of video frames' critical information is reserved for the key frame extraction processing.

2.2. Two-Stage Method for Key Frame Extraction. Figure 3 is the key frame extraction overall flowchart for digital video copyright protection. First, a digital video is decomposed into video frames. The downloaded video from the network includes several video formats, such as f4v, flv, and mp4. In order to improve the universality of video key extraction algorithm, the present method does not consider the specific format and video stream structure, and the video is decoded before the processed video frame decomposition. It is seen from Figure 3 that the program to extract key frame is divided into two steps. Firstly, alternative key frame sequence based on the color characteristics of the original difference

Figure 2: Four frames with similar content extracted from a tested video.

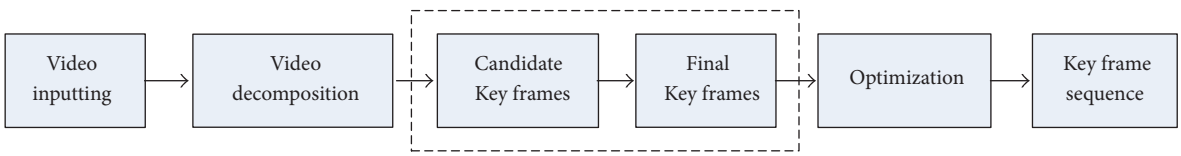


Figure 3: Flowchart of the proposed key frame extraction method.

between video frames is obtained; then key frame sequence is got according to the structure characteristic differences between alternative key frames sequence, and finally it is determined by the number of key frames in order to ensure the effectiveness of key frames.

Based on the above considerations, the frame difference method is used to extract key frames by analyzing the presence of spatial redundancy and temporal redundancy. In order to improve operational efficiency, it is worth mentioning that this method is different from the traditional shot segmentation method [9], for that the traditional approach is to conduct a video shot segmentation, then to extract key frames from each shot, and finally to compose key frame sequence of the video. In this method, the segmentation is not considered and then to extract key frames directly from the video.

2.2.1. Alternative Key Frame Sequence Based on Color Features. Color is one of the important properties of the image and is often used to characterize the statistics of the image [10, 11], and even for some specified domain video, color information can be expressed directly semantics, such as soccer video, usually on behalf of green grass. In addition, different color space of the sensory perception of visual effects is inconsistent. In order to achieve an effective balance between the key frame extraction efficiency and the speed, the RGB color space is used and the color histogram for each frame is calculated. Then the color histogram difference between adjacent frames is adopted in the present method, as shown in Figure 4.

Based on the number of key frames, color feature extraction method for video sequence obvious video content conversion has a good ability to judge, but to little effect, or change the gradient color; light detection effect is not ideal, because the color histogram for pretty gradients and lighting effects such as gradients are very sensitive to the frame between a few dozen frames of video content; despite little change between adjacent frames, the significant changes between color histogram features are occurring. As previously stressed, in order to quickly and effectively perform key frame extraction, the video shot segmentation will not be adopted directly. Although motion estimation, optical flow analysis, and motion modeling method are effective in the previous method, the time complexity is also too high; these problems have a serious impact on the practical application of copyright in video monitoring.

2.2.2. Final Key Frame Sequence Based on Structure Features. Figure 5 is a key frame sequence optimization based on structural features. The program uses the first frame extraction based on color features alternate key and then extracted key frames to optimize based on structural features; that is, the

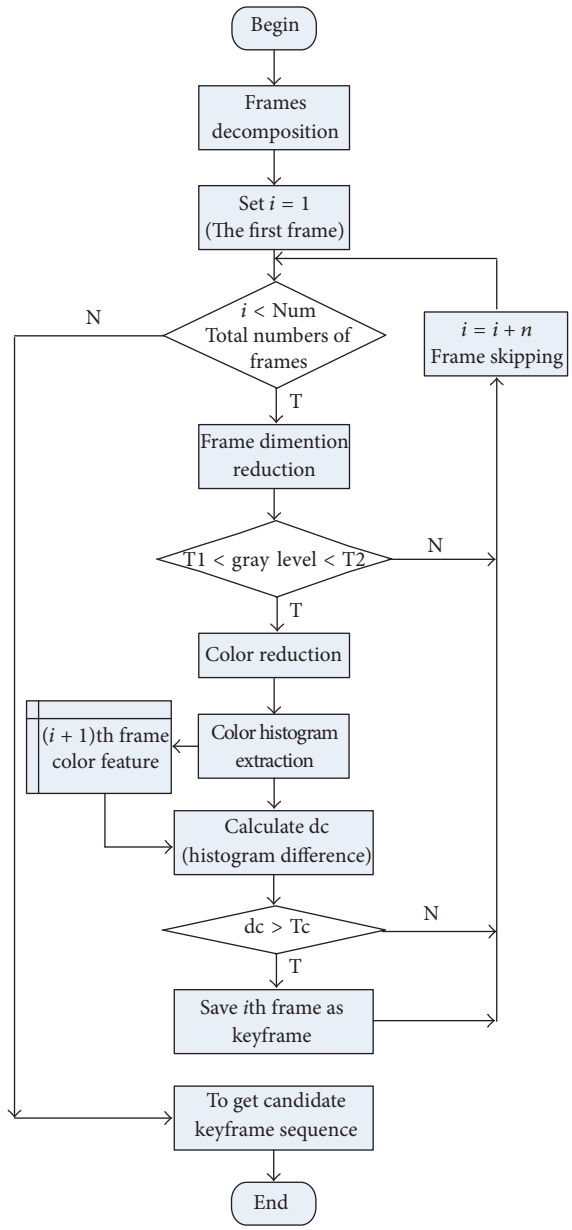


Figure 4: Flowchart of generating candidate key frame sequence.

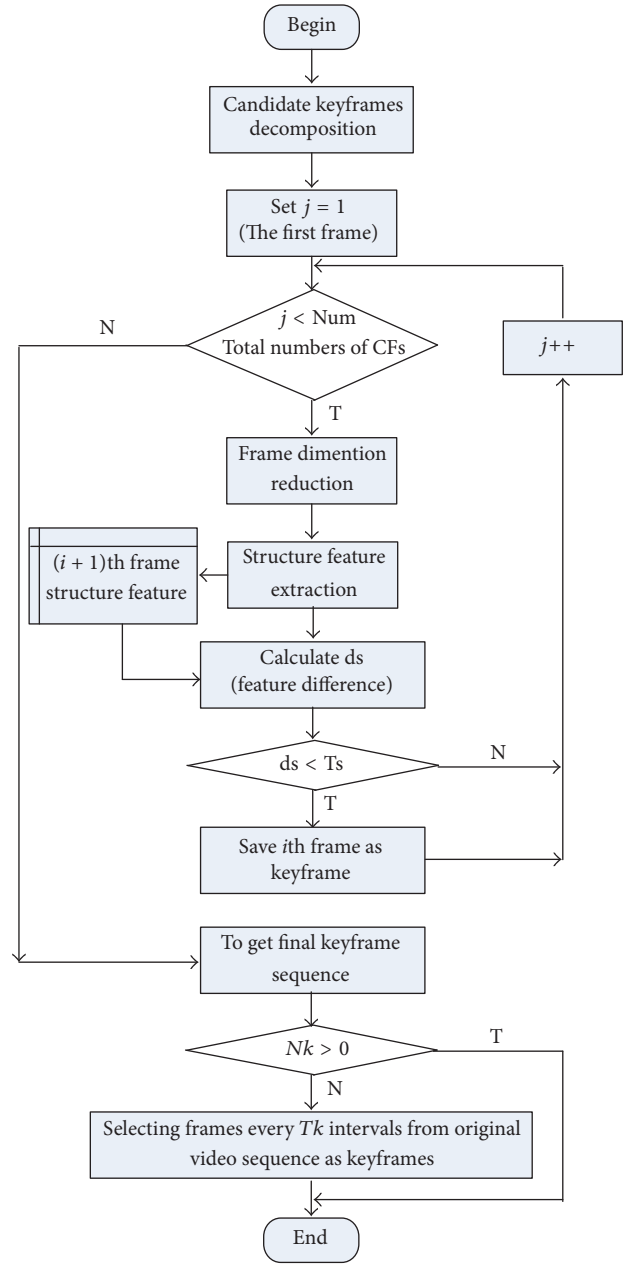


Figure 5: Flowchart of generating final key frame sequence and optimization based on key frames number.

alternative key frame structure similarity between adjacent frames is determined to further reduce key frames.

The method is derived from the structural similarity evaluation method for image quality evaluation [12] and is a measure of the similarity of the two images; the value closer to 1 indicates that the two images' quality is more similar. Structural similarity theory states that natural image signal is highly structured and that there is a strong correlation between pixels, especially airspace closest pixels; this correlation contains important information visual objects in the scene structure. Human visual system (HVS) main function is to extract structured information from view; it can be used as a measure of structural information perceived image quality of approximation. In this scenario, the structure is similar to the concept introduced to the key frame optimization process; thereby removing the extraction of the frame structure information is not sensitive to this problem based on color feature key.

The program uses only similarity index structure similar to the structure of the components. From the perspective of an image composition, structural information is defined as an independent component from brightness and contrast in the theory of structural similarity index. And it could reflect the properties of objects in the scene. The covariance is selected as a structural similarity metric. The main calculation is as follows.

Figure 6: Examples of alternative key frames.

Covariance as a structural similarity measure for the image block x, y of the correlation coefficient, namely, the covariance of x and y, is calculated as

$$\sigma_{xy} = \frac{1}{N-1}\sum_{i-1}^{N}(x_i - \mu_i)(y_i - \mu_i), \quad (1)$$

where N is the number of the patches and μ_i is the average value.

In the alternative key frame sequence, the front frame could be as the original image, and the adjacent frame is set as the test image. According to the two corresponding image blocks at the same position x (in the original image) and y (in the test image), the structure similarity component between the two image blocks is calculated as (x, y):

$$s(x, y) = \frac{\sigma_{xy} + C}{\sigma_x \sigma_y + C}, \quad (2)$$

where $C = ((KL)^2/2)$, $K \ll 1$, $L \in (0, 255]$ and σ_x, σ_y are x and y variance, respectively.

If the component values of $s(x, y)$ are small, then the distinction between the contents of the information is not; at the same time they do not have to be retained as a key frame, which can be extracted only as a key frame is optimized.

2.3. Optimization Based on the Number of Key Frames. After extracting alternative key frames based on color features and key frames based on structural features, the number of key frames will be determined to meet the demand. If no key frame is extracted from a video, then it will extract the appropriate number of key frames from the original video, in accordance with isochronous interval. Usually this occurs in the lens without the division, such as newscasts broadcast of a piece with only anchor shot. There are no significant changes in color and structural features between video frames.

3. Experiments and Analysis

The method is applied to a lot of online videos downloaded from several video websites and the digital linear tapes are from Shanghai Media Group. The algorithm was implemented in C++ and OpenCV 2.0, and then the experiments were conducted on a Windows 7 system with an Intel i7 processor and 16 GB RAM.

Firstly, we took television show "SUPER DIVA" to verify the effectiveness and robustness of the proposed method. More than 20 versions of the copies or near-duplicates were downloaded, which may be different in video formats (.mp4, .rm, .wmv, .flv, etc.), spatial resolutions (1920 ∗ 1080, 1080 ∗ 720, 720 ∗ 576, etc.), video lengths (such as short clips cut from a full video), and so on. The results which are got from the downloaded video with mp4 format are partly shown in Figures 6 and 7.

From Figure 6, we could see that most key frames are covering the video content exactly. There are also some frames similar with content, such as the three frames in the 2nd and 3rd row. The difference among these frames is color background, especially the bubble lights. So the final key frames are extracted based on the structural difference from the alternative key frames, as shown in Figure 7. In general, these final key frames meet the three conditions mentioned in Section 2. The frame content could be viewed definitely and their order consisted with the original video, and there

Figure 7: Examples of final key frames extracted from Figure 6.

Figure 8: Three sets of key frames from different versions of the tested video.

is appropriate redundancy, such as the third frame in the 1st row and the last frame in the 3rd row.

Secondly, three different versions of SUPER DIVA were tested to get the final key frames. They are different in formats or resolutions and are noted in V1 (.mp4, 640 ∗ 352), V2 (.flv, 608 ∗ 448), and V3 (.avi, 512 ∗ 288). The results are partly shown in Figure 8. It should be noted that the frames listed in Figure 8 are cropped to the same size for the appearance. Generally, each set of key frames are consistent with others, especially with almost the same video content and the same time line. The reason for the different key frames may be because of the same feature difference thresholds, Tc and Ts.

Thirdly, the optimization step based on the number of key frames was tested and the results are listed in Figure 9. The original video is a short promotion trailer about a famous movie. There's almost no feature difference among these original frames, only the mouth movements and few hand movements of the introducer. So no key frames are extracted based on the color and structure information. Therefore, the optimization based on the a fixed time interval is needed in order to satisfy the key frame demand and ensure the following processes for video copyright detection.

4. Conclusions

A key frame extraction method based on frame difference with low level features is proposed for video copyright protection. Exactly, a two-stage method is used to extract accurate key frames to cover the content for the whole video sequence. Firstly, an alternative sequence is obtained

Figure 9: Optimized key frames based on the frame number.

based on color characteristic difference between adjacent frames from original sequence. Secondly, the final key frame sequence is obtained by analyzing structural characteristic difference between adjacent frames from the alternative sequence. And thirdly, an optimization step based on the number of final key frames is added in order to ensure the effectiveness for video copyright protection processes. Tested with several television videos with different content, formats, and resolutions, it is shown that the proposed method has advantages in computation complexity and robustness on several video formats, video resolution, and so on. In the future the adaptive threshold is the primary research point.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

Shanghai College Young Teachers Training Program (no. ZZGCD15002) and Local Colleges and Universities' Capacity Construction Project of Shanghai Science and Technology Commission (no. 15590501300) are gratefully acknowledged.

References

[1] J. M. Zhang, H. Y. Liu, and S. M. Sun, "Keyframe extraction based on improved ant algorithm and agglom erative," *Computer Engineering and Applications*, vol. 49, no. 3, pp. 222–225, 2013.

[2] X. Guo and F. Shi, "Quick extracting keyframes from compressed video," in *Proceedings of the 2nd International Conference on Computer Engineering and Technology (ICCET '10)*, pp. V4163–V4165, Chengdu, China, April 2010.

[3] S. Angadi and V. Naik, "Entropy based fuzzy C means clustering and key frame extraction for sports video summarization," in *Proceedings of the 5th International Conference on Signal and Image Processing (ICSIP '14)*, pp. 271–279, January 2014.

[4] Q. Guo, C. Zhang, Y. Zhang, and H. Liu, "An efficient SVD-based method for image denoising," *IEEE Transactions on Circuits & Systems for Video Technology*, vol. 26, no. 5, pp. 868–880, 2016.

[5] J. Peng and Q. Xiao-Lin, "Keyframe-based video summary using visual attention clues," *IEEE Multimedia*, vol. 17, no. 2, pp. 64–73, 2010.

[6] L. Liu and G. Fan, "Combined key-frame extraction and object-based video segmentation," *IEEE Transactions on Circuits & Systems for Video Technology*, vol. 15, no. 7, pp. 869–884, 2005.

[7] M. Chatzigiorgaki and A. N. Skodras, "Real-time Keyframe extraction towards video content identification," in *Proceedings of the 16th International Conference on Digital Signal Processing (DSP '09)*, pp. 68–73, grc, July 2009.

[8] S. Lei, G. Xie, and G. Yan, "A novel key-frame extraction approach for both video summary and video index," *The Scientific World Journal*, vol. 2014, Article ID 695168, 9 pages, 2014.

[9] J. Li, Y. Ding, Y. Shi, and Q. Zeng, "DWT-based shot boundary detection using Support Vector Machine," in *Proceedings of the 5th International Conference on Information Assurance and Security (IAS '09)*, pp. 435–438, September 2009.

[10] Z. Sun, K. Jia, and H. Chen, "Video key frame extraction based on spatial-temporal color distribution," in *Proceedings of the 4th International Conference on Intelligent Information Hiding and Multiedia Signal (IIH-MSP '08)*, pp. 196–199, August 2008.

[11] J. Zhang, X. Jiang, G. Li, and L. Jiang, "Key frame extraction based on particle swarm optimization," *Journal of Computer Applications*, vol. 31, no. 2, pp. 358–361, 2011.

[12] Y. Shi, Y. Ding, R. Zhang, and J. Li, "Structure and hue similarity for color image quality Assessment," in *Proceedings of the International Conference on Electronic Computer Technology (ICECT '09)*, pp. 329–333, February 2009.

Hindawi
Journal of Electrical and Computer Engineering
Volume 2017, Article ID 9828967, 9 pages
https://doi.org/10.1155/2017/9828967

Research Article

Algebraic Cryptanalysis Scheme of AES-256 Using Gröbner Basis

Kaixin Zhao,[1] Jie Cui,[2] and Zhiqiang Xie[2]

[1]*Department of Computer Science and Technology, Henan Institute of Technology, Xinxiang 453003, China*
[2]*School of Computer Science and Technology, Anhui University, Hefei 230039, China*

Correspondence should be addressed to Jie Cui; cuijie@mail.ustc.edu.cn

Received 22 October 2016; Accepted 22 January 2017; Published 23 February 2017

Academic Editor: Jucheng Yang

The zero-dimensional Gröbner basis construction is a crucial step in Gröbner basis cryptanalysis on AES-256. In this paper, after performing an in-depth study on the linear transformation and the system of multivariate polynomial equations of AES-256, the zero-dimensional Gröbner basis construction method is proposed by choosing suitable term order and variable order. After giving a detailed construction process of the zero-dimensional Gröbner basis, the necessary theoretical proof is presented. Based on this, an algebraic cryptanalysis scheme of AES-256 using Gröbner basis is proposed. Analysis shows that the complexity of our scheme is lower than that of the exhaustive attack.

1. Introduction

On October 2, 2000, the Rijndael algorithm, which was designed by Daemen and Rijmen, was determined by the National Institute of Standards and Technology (NIST) for the Advanced Encryption Standard (AES) [1]. It has been of concern to the cryptographic community since the Rijndael algorithm was proposed, and there have been many attack methods. However, there is no successful attack on the full Rijndael algorithm up to now [2, 3].

Cryptanalysis and cryptography not only are mutually antagonistic, but also promote each other. Because of the great advantages of algebraic cryptanalysis technology, it has become a hot research topic in recent years. Algebraic attack is mainly composed of two steps: the first step is to establish a system of algebraic equations to describe the relationship among the plaintext, the ciphertext, and the key in cryptographic algorithm; the second step is to solve the system of equations to obtain the key by some of the known plaintext-ciphertext pairs. The first step has already obtained some research results, and many scholars have proposed many kinds of equation systems of AES algorithm [4, 5]. In the second step, the multivariate equation system is still a problem to be solved. Although solving the multivariate equation system is an NP-hard problem, the complexity of solving a sparse overdetermined system of equations is far lower than that of the NP-hard problem.

At present, the methods of solving the high order multivariate equation system mainly include XL, XSL, and Gröbner basis. Since the algebraic expression of AES algorithm is sparse and structured, it is inefficient to apply XL attacks directly. In 2002, Courtois et al. proposed an XSL attack method and claimed to break the key length of 256-bit AES algorithm in theory. However, the number of linear independent equations generated by XSL attacks in the academic field is disputed, and the validity of the attack is questioned [6, 7]. Gröbner basis is an effective method for solving the high order multivariate equation system, which is proposed by Buchberger. Its essence is to set up a set of arbitrary ideals in polynomial rings, describe and compute a set of generators with good properties, and then study the ideal structure and carry out the ideal computation [3].

Gröbner basis is a standard representation method of polynomial ideals, which has some useful properties [8]. Gröbner basis exists in any ideal, and the Gröbner basis of any ideal can be computed by the Buchberger algorithm or F4 or F5 algorithm [6]. Lexicographic order is a commonly used elimination order. The coefficient matrix of the basis is triangular when using lexicographical Gröbner basis in the computation, and the last row solves single-variable equations. This is the reason why lexicographical Gröbner

basis can solve the equation system. But the direct computation of lexicographic Gröbner basis will produce excessive coefficients.

Common practice is to compute the total degree order Gröbner basis of the ideal firstly and then convert the total degree order Gröbner basis to lexicographical Gröbner basis using Gröbner basis conversion algorithm. Gröbner basis conversion algorithms include the Gröbner Walk [7] and the FGLM algorithm [6]. Compared with the Gröbner Walk, FGLM algorithm is simple and efficient, but the FGLM algorithm only works for zero-dimensional ideals [9, 10]. Therefore, constructing the zero-dimensional Gröbner basis of AES algorithm is crucial to implement Gröbner basis cryptanalysis. In 2013, the zero-dimensional Gröbner basis construction method of Rijndael-192 was proposed [11]. However, how to construct the zero-dimensional Gröbner basis of AES-256 and how to apply Gröbner basis cryptanalysis to AES-256 are still open questions. In this paper, the authors perform some particular studies on the linear transformation and the system of multivariate polynomial equations of AES-256 and propose its zero-dimensional Gröbner basis construction method through choosing suitable term order and variable order. After presenting the construction method of the Gröbner basis, the authors give the necessary theoretical proof. Moreover, the authors propose an algebraic cryptanalysis of AES-256 using Gröbner basis. Analysis suggests that the complexity of our scheme is lower than the exhaustive attack. The main contributions are given as follows:

(1) The zero-dimensional Gröbner basis construction method is proposed by choosing suitable term order and variable order.

(2) The necessary theoretical proof is given, and it shows that the set of polynomials is a zero-dimensional Gröbner basis.

(3) The effective algebraic cryptanalysis scheme of AES-256 using Gröbner basis is proposed.

The rest of this paper is formed as follows. The mathematical model of AES-256 is shown in Section 2. Section 3 demonstrates the Gröbner basis theory. The equation system of AES-256 is given in Section 4. In Section 5, the Gröbner basis construction method of AES-256 and the algebraic cryptanalysis scheme of AES-256 are proposed. Finally, the paper is concluded in Section 6.

2. Mathematical Model of AES-256

The block length and key length of AES can be specified independently as 128 bits, 192 bits, or 256 bits, and the corresponding round time is 10, 12, or 14. Each round consists of 4 transformations: the S-box substitution (ByteSub), ShiftRow, MixColumn, and AddRoundKey. With AES starting from the AddRoundKey, with 13 rounds of iteration, the final round is equal to the round with the MixColumn step removed. AES is an iterated block cipher with a variable block length and a variable key length. In this paper, both the block length and the key length are specified to 256 bits.

2.1. S-Box Substitution. The S-box transformation is a nonlinear byte substitution, operating on each of the state bytes independently. The S-box is invertible and is constructed by the composition of two transformations:

(1) Seeking the inverse operation of multiplication in $\mathrm{GF}(2^8) = Z_2[x]/(x^8 + x^4 + x^3 + x + 1)$ field, that is, input $\omega \in \mathrm{GF}(2^8)$ and output $\upsilon \in \mathrm{GF}(2^8)$, to meet

$$\omega * \upsilon = 1 \bmod \left(x^8 + x^4 + x^3 + x + 1\right), \tag{1}$$

then

$$\upsilon = \omega^{-1} = \begin{cases} \omega^{254}, & \omega \neq 0, \\ 0, & \omega = 0. \end{cases} \tag{2}$$

(2) Let element components of $x = \upsilon$ in $\mathrm{GF}(2)^8$ be $(x_7, x_6, x_5, x_4, x_3, x_2, x_1, x_0)$; the affine transformations are as follows:

$$y = \mathrm{La} \times x + \text{“63”} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} x_7 \\ x_6 \\ x_5 \\ x_4 \\ x_3 \\ x_2 \\ x_1 \\ x_0 \end{bmatrix} + \begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \end{bmatrix}. \tag{3}$$

The selection of constant “63” is to ensure the S-box is not a fixed point $S(a) = a$ and an opposite fixed point $S(a) = \overline{a}$. S-box has the ability to resist linear attacks and differential attacks [1].

2.2. ShiftRow and MixColumn Transformations. The 4×8-byte matrix is obtained by S-box substitution, where $S_{i,j}$ is the byte in the ith row and the jth column, $0 \le i \le 3$, $0 \le j \le 7$. SR (ShiftRow) shift i bytes to the left for the ith row of the matrix:

$$\begin{bmatrix} s_{0,0} & s_{0,1} & s_{0,2} & s_{0,3} & s_{0,4} & s_{0,5} & s_{0,6} & s_{0,7} \\ s_{1,0} & s_{1,1} & s_{1,2} & s_{1,3} & s_{1,4} & s_{1,5} & s_{1,6} & s_{1,7} \\ s_{2,0} & s_{2,1} & s_{2,2} & s_{2,3} & s_{2,4} & s_{2,5} & s_{2,6} & s_{2,7} \\ s_{3,0} & s_{3,1} & s_{3,2} & s_{3,3} & s_{3,4} & s_{3,5} & s_{3,6} & s_{3,7} \end{bmatrix} \longrightarrow \begin{bmatrix} s_{0,0} & s_{0,1} & s_{0,2} & s_{0,3} & s_{0,4} & s_{0,5} & s_{0,6} & s_{0,7} \\ s_{1,1} & s_{1,2} & s_{1,3} & s_{1,4} & s_{1,5} & s_{1,6} & s_{1,7} & s_{1,0} \\ s_{2,2} & s_{2,3} & s_{2,4} & s_{2,5} & s_{2,6} & s_{2,7} & s_{2,0} & s_{2,1} \\ s_{3,3} & s_{3,4} & s_{3,5} & s_{3,6} & s_{3,7} & s_{3,0} & s_{3,1} & s_{3,2} \end{bmatrix}. \tag{4}$$

MC (MixColumn) transforms the independent operation of each column for the purpose of causing confusion. Each

byte in each column is mapped to the new value; this value is 4 bytes in the column with the function obtained. Transformation is as follows:

$$\begin{bmatrix} s'_{0,0} & s'_{0,1} & s'_{0,2} & s'_{0,3} & s'_{0,4} & s'_{0,5} & s'_{0,6} & s'_{0,7} \\ s'_{1,0} & s'_{1,1} & s'_{1,2} & s'_{1,3} & s'_{1,4} & s'_{1,5} & s'_{1,6} & s'_{1,7} \\ s'_{2,0} & s'_{2,1} & s'_{2,2} & s'_{2,3} & s'_{2,4} & s'_{2,5} & s'_{2,6} & s'_{2,7} \\ s'_{3,0} & s'_{3,1} & s'_{3,2} & s'_{3,3} & s'_{3,4} & s'_{3,5} & s'_{3,6} & s'_{3,7} \end{bmatrix} = D \cdot \begin{bmatrix} s_{0,0} & s_{0,1} & s_{0,2} & s_{0,3} & s_{0,4} & s_{0,5} & s_{0,6} & s_{0,7} \\ s_{1,0} & s_{1,1} & s_{1,2} & s_{1,3} & s_{1,4} & s_{1,5} & s_{1,6} & s_{1,7} \\ s_{2,0} & s_{2,1} & s_{2,2} & s_{2,3} & s_{2,4} & s_{2,5} & s_{2,6} & s_{2,7} \\ s_{3,0} & s_{3,1} & s_{3,2} & s_{3,3} & s_{3,4} & s_{3,5} & s_{3,6} & s_{3,7} \end{bmatrix}, \tag{5}$$

where

$$D = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix}. \tag{6}$$

For mathematical convenience, we use a column vector instead of the original matrix to represent intermediate states and keys. The mapping relationship between the elements in column vector and the elements in the original matrix is as follows:

$$\varphi : F^{4\times 8} \longrightarrow F^{32},$$

$$\begin{pmatrix} s_{0,0} & s_{0,1} & s_{0,2} & s_{0,3} & s_{0,4} & s_{0,5} & s_{0,6} & s_{0,7} \\ s_{1,0} & s_{1,1} & s_{1,2} & s_{1,3} & s_{1,4} & s_{1,5} & s_{1,6} & s_{1,7} \\ s_{2,0} & s_{2,1} & s_{2,2} & s_{2,3} & s_{2,4} & s_{2,5} & s_{2,6} & s_{2,7} \\ s_{3,0} & s_{3,1} & s_{3,2} & s_{3,3} & s_{3,4} & s_{3,5} & s_{3,6} & s_{3,7} \end{pmatrix} \longmapsto \tag{7}$$

$$(s_{0,0}, s_{1,0}, \ldots, s_{0,1}, s_{1,1}, \ldots)^T.$$

The finite field GF(2^8) is denoted as F in this paper. Introducing a 32×32 0-1 transformation matrix M_{SR}, the SR transform is equivalent to left multiplication by the matrix M_{SR}. There is only one element in each column and each row of the matrix is 1 and all the others are 0. Similarly, by introducing a new transformation matrix M_{MC}, the MC transform is equivalent to left multiplication by the matrix M_{MC}. The construction principle of M_{MC} is $M_{\mathrm{MC}} = D \otimes I_8 \in F^{32\times 32}$, where $\otimes$ denotes tensor product and I_8 denotes 8-order identity matrix. The composite transformation of the SR transform and the MC transform is denoted as M, and then $M = M_{\mathrm{MC}} \cdot M_{\mathrm{SR}}$. It is easy to get

$$M = M_{\mathrm{MC}} \cdot M_{\mathrm{SR}}$$

$$= \begin{bmatrix}
02&00&00&00&00&03&00&00&00&00&01&00&00&00&00&01&00&00&00&00&00&00&00&00&00&00&00&00&00&00&00&00\\
01&00&00&00&00&02&00&00&00&00&03&00&00&00&00&01&00&00&00&00&00&00&00&00&00&00&00&00&00&00&00&00\\
01&00&00&00&00&01&00&00&00&00&02&00&00&00&00&03&00&00&00&00&00&00&00&00&00&00&00&00&00&00&00&00\\
03&00&00&00&00&01&00&00&00&00&01&00&00&00&00&02&00&00&00&00&00&00&00&00&00&00&00&00&00&00&00&00\\
00&00&00&00&02&00&00&00&00&03&00&00&00&00&01&00&00&00&00&01&00&00&00&00&00&00&00&00&00&00&00&00\\
00&00&00&00&01&00&00&00&00&02&00&00&00&00&03&00&00&00&00&01&00&00&00&00&00&00&00&00&00&00&00&00\\
00&00&00&00&01&00&00&00&00&01&00&00&00&00&02&00&00&00&00&03&00&00&00&00&00&00&00&00&00&00&00&00\\
00&00&00&00&03&00&00&00&00&01&00&00&00&00&01&00&00&00&00&02&00&00&00&00&00&00&00&00&00&00&00&00\\
00&00&00&00&00&00&00&00&02&00&00&00&00&03&00&00&00&00&01&00&00&00&00&01&00&00&00&00&00&00&00&00\\
00&00&00&00&00&00&00&00&01&00&00&00&00&02&00&00&00&00&03&00&00&00&00&01&00&00&00&00&00&00&00&00\\
00&00&00&00&00&00&00&00&01&00&00&00&00&01&00&00&00&00&02&00&00&00&00&03&00&00&00&00&00&00&00&00\\
00&00&00&00&00&00&00&00&03&00&00&00&00&01&00&00&00&00&01&00&00&00&00&02&00&00&00&00&00&00&00&00\\
00&00&00&00&00&00&00&00&00&00&00&00&02&00&00&00&00&03&00&00&00&00&01&00&00&00&00&01&00&00&00&00\\
00&00&00&00&00&00&00&00&00&00&00&00&01&00&00&00&00&02&00&00&00&00&03&00&00&00&00&01&00&00&00&00\\
00&00&00&00&00&00&00&00&00&00&00&00&01&00&00&00&00&01&00&00&00&00&02&00&00&00&00&03&00&00&00&00\\
00&00&00&00&00&00&00&00&00&00&00&00&03&00&00&00&00&01&00&00&00&00&01&00&00&00&00&02&00&00&00&00\\
00&00&00&00&00&00&00&00&00&00&00&00&00&00&00&00&02&00&00&00&00&03&00&00&00&00&01&00&00&00&00&01\\
00&00&00&00&00&00&00&00&00&00&00&00&00&00&00&00&01&00&00&00&00&02&00&00&00&00&03&00&00&00&00&01\\
00&00&00&00&00&00&00&00&00&00&00&00&00&00&00&00&01&00&00&00&00&01&00&00&00&00&02&00&00&00&00&03\\
00&00&00&00&00&00&00&00&00&00&00&00&00&00&00&00&03&00&00&00&00&01&00&00&00&00&01&00&00&00&00&02\\
00&00&00&01&00&00&00&00&00&00&00&00&00&00&00&00&00&00&00&00&02&00&00&00&00&03&00&00&00&00&01&00\\
00&00&00&01&00&00&00&00&00&00&00&00&00&00&00&00&00&00&00&00&01&00&00&00&00&02&00&00&00&00&03&00\\
00&00&00&03&00&00&00&00&00&00&00&00&00&00&00&00&00&00&00&00&01&00&00&00&00&01&00&00&00&00&02&00\\
00&00&00&02&00&00&00&00&00&00&00&00&00&00&00&00&00&00&00&00&03&00&00&00&00&01&00&00&00&00&01&00\\
00&00&01&00&00&00&00&01&00&00&00&00&00&00&00&00&00&00&00&00&00&00&00&00&00&02&00&00&00&00&03&00\\
00&00&03&00&00&00&00&01&00&00&00&00&00&00&00&00&00&00&00&00&00&00&00&00&00&01&00&00&00&00&02&00\\
00&00&02&00&00&00&00&03&00&00&00&00&00&00&00&00&00&00&00&00&00&00&00&00&00&01&00&00&00&00&01&00\\
00&00&01&00&00&00&00&02&00&00&00&00&00&00&00&00&00&00&00&00&00&00&00&00&00&03&00&00&00&00&01&00\\
00&03&00&00&00&00&01&00&00&00&00&01&00&00&00&00&00&00&00&00&00&00&00&00&00&00&00&00&00&00&02&00\\
00&02&00&00&00&00&03&00&00&00&00&01&00&00&00&00&00&00&00&00&00&00&00&00&00&00&00&00&00&00&01&00\\
00&01&00&00&00&00&02&00&00&00&00&03&00&00&00&00&00&00&00&00&00&00&00&00&00&00&00&00&00&00&01&00\\
00&01&00&00&00&00&01&00&00&00&00&02&00&00&00&00&00&00&00&00&00&00&00&00&00&00&00&00&00&00&03&00
\end{bmatrix}. \tag{8}$$

Thus, the linear transformation consisting of the SR transform and the MC transform can be expressed as

$$\begin{aligned}&\left(s''_{0,0}, s''_{1,0}, \ldots, s''_{0,1}, s''_{1,1}, \ldots\right)^T \\ &\quad = M \cdot \left(s_{0,0}, s_{1,0}, \ldots, s_{0,1}, s_{1,1}, \ldots\right)^T.\end{aligned} \tag{9}$$

2.3. AddRoundKey. In this operation, a round key is applied to the state by a simple bitwise EXOR. The round key is derived from the cipher key by means of the key schedule. It can be denoted as $Y = X \oplus K$, where K is the round key.

2.4. Key Schedule Algorithm. Key schedule consists of two modules: key expansion and round key selection. The block length and key length are denoted as N_b and N_k, respectively, and the unit is a 4-byte word. That is, N_b = block length/32 and N_k = key length/32. The number of rounds is denoted by R.

For AES-256, $N_b = 8$, $N_k = 8$, and $R = 14$. The key expansion of AES-256 is to extend eight 4-byte key words into 90 4-byte words $W[\cdot]$, where $W[0], \ldots, W[7]$ is the cipher key. The expansion algorithm is as shown in Algorithm 1.

3. Gröbner Basis Theory

Let R be a ring; for a nonempty ideal $I \subset R$, its Gröbner basis is generally not unique [12, 13]. The Gröbner basis is related to the selection of term orders. Related definitions are given below.

Definition 1. Order $\leq$ on a set $T(R)$ is called term order, if and only if $\leq$ is a linear order, and satisfies two properties:

(1) For all $t \in T(R)$, $t \geq 1$.

(2) For any $s, t_1, t_2 \in T(R)$, if $t_1 \leq t_2$, then $st_1 \leq st_2$.

In a term order $\leq$, the largest element of a polynomial p is called the head term of p, denoted as $\mathrm{HT}(p)$.

The set of natural numbers is $\mathbb{N}$, and n is a given positive integer, and $x_1, x_2, \ldots, x_n$ are n variables in ring R. Let the set of terms be

$$T(R) = \left\{x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n} \mid \alpha_i \in \mathbb{N},\ i = 1, 2, \ldots, n\right\}. \tag{10}$$

That is, $T(R)$ is the power product set of n variables. The degree of term $t = x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n} \in T(R)$ is denoted as $\deg(t) = \sum_{i=1}^{n} \alpha_i$. Let $X = (x_1, x_2, \ldots, x_n)$; then, the definitions of three common term orders will be given below.

Definition 2. $T(R)$ $x_1 > x_2 > \cdots > x_n$ on lexicographical order, denoted as lex, is defined as follows.

For $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n)$, $\beta = (\beta_1, \beta_2, \ldots, \beta_n) \in \mathbb{N}^n$, then $X^\alpha <_{\text{lex}} X^\beta \Leftrightarrow$ let $\alpha_j = \beta_j$, $j = 0, 1, \ldots, k$, and $\alpha_{k+1} < \beta_{k+1}$ $(\alpha_0 = \beta_0)$, where $0 \leq k \leq n-1$.

Definition 3. $T(R)$ $x_1 > x_2 > \cdots > x_n$ on degree lexicographical order, denoted as deglex, is defined as follows.

For $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n)$, $\beta = (\beta_1, \beta_2, \ldots, \beta_n) \in \mathbb{N}^n$, then

$$X^\alpha <_{\text{deglex}} X^\beta \Longleftrightarrow \begin{cases} \sum_{i=1}^{n} \alpha_i < \sum_{i=1}^{n} \beta_i & \text{or} \\ \sum_{i=1}^{n} \alpha_i = \sum_{i=1}^{n} \beta_i, & \text{and according to the lexicographic order.} \\ X^\alpha <_{\text{lex}} X^\beta \end{cases} \tag{11}$$

Definition 4. $T(R)$ $x_1 > x_2 > \cdots > x_n$ on degree reverse lexicographical order, denoted as degrevlex, is defined as follows.

For $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n)$, $\beta = (\beta_1, \beta_2, \ldots, \beta_n) \in \mathbb{N}^n$, then

$$\begin{aligned}&X^\alpha <_{\text{degrevlex}} X^\beta \Longleftrightarrow \\ &\sum_{i=1}^{n} \alpha_i < \sum_{i=1}^{n} \beta_i, \\ &\text{or } \sum_{i=1}^{n} \alpha_i = \sum_{i=1}^{n} \beta_i, \\ &\alpha_n = \beta_n, \ldots, \alpha_{i+1} = \beta_{i+1},\ \alpha_i \neq \beta_i,\ \alpha_i > \beta_i, \text{between } \alpha \text{ and } \beta, \text{the first different coords from right side}, \alpha_i > \beta_i.\end{aligned} \tag{12}$$

Definition 5. Let R be a ring and let I be one nonzero ideal in R, $G = \{g_1, \ldots, g_m\} \subset I$. G is called the Gröbner basis of ideal I if and only if

$$\left\langle \mathrm{HT}(g_1), \ldots, \mathrm{HT}(g_m) \right\rangle = \left\langle \{\mathrm{HT}(p) : p \in I\} \right\rangle. \tag{13}$$

The Gröbner basis of any nonzero ideal can be obtained by using the Buchberger algorithm [12]. In the implementation of the Buchberger algorithm, the Buchberger rule can be used to eliminate unnecessary polynomials [12, 14]. Based on the Buchberger rule, the following conclusions can be obtained.

Theorem 6. *Let G be a set of polynomials, $H = \{HT(f) : f \in G\}$; if all elements in H are pairwise prime, then G is a Gröbner basis.*

Proof. See [15]. □

A zero-dimensional ideal is an ideal that has a finite number of solutions over the closure of the field. It usually

```
(1) for (i = 8; i < 90; i + +) do
(2)   if i %8 = 0 then
(3)     W[i] = W[i − 8] ⊕ BS(RotByte(W[i − 1])) ⊕const(i/8);
(4)   else
(5)     W[i] = W[i − 8] ⊕ W[i − 1];
(6)   end if
(7) end for
(8) return W[8], W[9], . . . , W[89];
```

Algorithm 1: Key expansion algorithm of AES-256.

is advantageous to have this property for Gröbner basis computations. By using Corollary 6.56 of [16], we can determine whether an ideal I is zero-dimensional. Below we state a reduced version of this corollary.

Theorem 7. *Let G be a Gröbner basis of the ideal I; then, $\dim(I) = 0$ if and only if, for any $1 \le i \le n$, there exists a polynomial $g \in G$, so that $HT(g) = x_i^{d_i}$.*

4. Equation System of AES-256

Let $((p_0, \ldots, p_{31}), (c_0, \ldots, c_{31})) \in F^{32} \times F^{32}$ be a known pair of plaintext and ciphertext in this paper. We call $x_{i,j}$ the jth element of the output of the AddRoundKey in the ith round transformation. We denote by $k_{i,j}$ the jth element of the ith round key. It is easy to see that $k_{0,j}$ denotes the cipher key, $0 \le i \le 14, 0 \le j \le 31$. The equation system on GF(2^8) consists of the following four parts:

(1) Initial round (round 0) equations and the cipher equations:

$$\begin{aligned} x_{0,0} + k_{0,0} + p_0 = 0 \quad & x_{14,0} + c_0 = 0 \\ \vdots \quad & \vdots \\ x_{0,31} + k_{0,31} + p_{31} = 0 \quad & x_{14,31} + c_{31} = 0. \end{aligned} \tag{14}$$

(2) The equations of intermediate rounds, that is, the encryption equation of the ith round, $1 \le i \le 13$:

$$\begin{pmatrix} x_{i,0} + k_{i,0} \\ x_{i,1} + k_{i,1} \\ \vdots \\ x_{i,31} + k_{i,31} \end{pmatrix} + M \cdot \begin{pmatrix} S(x_{i-1,0}) \\ S(x_{i-1,1}) \\ \vdots \\ S(x_{i-1,31}) \end{pmatrix} = 0. \tag{15}$$

(3) The equations of the final round:

$$\begin{pmatrix} x_{14,0} + k_{14,0} \\ x_{14,1} + k_{14,1} \\ \vdots \\ x_{14,31} + k_{14,31} \end{pmatrix} + M_{\mathrm{SR}} \cdot \begin{pmatrix} S(x_{13,0}) \\ S(x_{13,1}) \\ \vdots \\ S(x_{13,31}) \end{pmatrix} = 0. \tag{16}$$

(4) Key scheduling equations:

$$\begin{pmatrix} k_{i,0} \\ k_{i,1} \\ k_{i,2} \\ k_{i,3} \\ k_{i,4} \\ k_{i,5} \\ \vdots \\ k_{i,31} \end{pmatrix} = \begin{pmatrix} k_{i-1,0} + S(k_{i-1,29}) + \xi^{i-1} \\ k_{i-1,1} + S(k_{i-1,30}) \\ k_{i-1,2} + S(k_{i-1,31}) \\ k_{i-1,3} + S(k_{i-1,28}) \\ k_{i-1,4} + k_{i,0} \\ k_{i-1,5} + k_{i,1} \\ \vdots \\ k_{i-1,31} + k_{i,27} \end{pmatrix}, \tag{17}$$

where ξ^{i-1} $(1 \le i \le 14)$ is a round constant.

5. Algebraic Cryptanalysis Scheme of AES-256

Definition 8. Denote the finite domain GF(2^8) as F; the multivariate polynomial ring on F, R is defined as

$$R := F\left[x_{i,j}, k_{i,j} : \{0 \le i \le 31, 0 \le j \le 14\}\right]. \tag{18}$$

To construct AES-256 Gröbner basis, the multivariate equation system obtained in Section 4 must be improved to meet the requirements of Gröbner basis; that is, the head terms of the polynomial on the left-hand side of the equation are pairwise prime.

5.1. The Gröbner Basis Construction Method of AES-256. The Gröbner basis of AES-256 is constructed as follows.

Step 1. The purpose of this step is to construct the polynomial set of the S-box and the inverse S-box. In this step, we make use of the algebraic expression of the S-box and the inverse S-box.

AES S-box is constructed based on evident mathematical theory, so it can be written in the form of an algebraic expression. The sparse algebraic expression of the S-box in F is as follows:

$$\begin{aligned} & S : F \longrightarrow F, \\ & x \longmapsto \\ & 05x^{FE} + 09x^{FD} + F9x^{FB} + 25x^{F7} + F4x^{EF} + B5x^{DF} + B9x^{BF} + 8Fx^{7F} + 63. \end{aligned} \tag{19}$$

Table 1: Coefficients of algebraic expression of AES inverse S-box (Hex).

C (mn)	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	52	F3	7E	1E	90	BB	2C	8A	1C	85	6D	C0	B2	1B	40	23
1	F6	73	29	D9	39	21	CF	3D	9A	8A	2F	CF	7B	04	E8	C8
2	85	7B	7C	AF	86	2F	13	65	75	D3	6D	D4	89	8E	65	05
3	EA	77	50	A3	C5	01	0B	46	BF	A7	0C	C7	8E	F2	B1	CB
4	E5	E2	10	D1	05	B0	F5	86	E4	03	71	A6	56	03	9E	3E
5	19	18	52	16	B9	D3	38	D9	04	E3	72	6B	BA	E8	BF	9D
6	1D	5A	55	FF	71	E1	A8	8E	FE	A2	A7	1F	DF	B0	03	CB
7	08	53	6F	B0	7F	87	8B	02	B1	92	81	27	40	2E	1A	EE
8	10	CA	82	4F	09	AA	C7	55	24	6C	E2	58	BC	E0	26	37
9	ED	8D	2A	D5	ED	45	C3	EC	1C	3E	2A	B3	9E	B7	38	82
A	23	2D	87	EA	DA	45	24	03	E7	C9	E3	D3	4E	DD	11	4E
B	81	91	91	59	A3	80	92	7E	DB	C4	20	EC	DB	55	7F	A8
C	C1	64	AB	1B	FD	60	05	13	2C	A9	76	A5	1D	32	8E	1E
D	C0	65	CB	8B	93	E4	AE	BE	5F	2C	3B	D2	0F	9F	42	CC
E	6C	80	68	43	09	23	C5	6D	1D	18	BD	5E	1B	B4	85	49
F	BC	0D	1F	A6	6B	D8	22	01	7A	C0	55	16	B3	CF	05	00

The nonsparse algebraic expression of the inverse S-box contains 255 terms. The coefficients of the algebraic expression of AES inverse S-box are shown in Table 1. The abbreviated form of the algebraic expression of AES inverse S-box can be expressed as follows:

$$S^{-1} : F \longrightarrow F,$$
$$x \longmapsto \sum_{i=0}^{254} c_i x^i, \tag{20}$$

where c_i is the coefficient of the term with degree i.

Step 2. The purpose of this step is to construct the polynomial set of linear transformations (i.e., ShiftRow and MixColumn). In this step, we use the equation system given in Section 4.

By (14), the plaintext equations, that is, the initial round equation system, can be obtained as (21), and the ciphertext equations can be obtained as (22). Hence,

$$x_{0,i} + k_{0,i} + p_i = 0, \quad p_i \in F, 0 \le i \le 31, \tag{21}$$

$$x_{14,i} + c_i = 0, \quad c_i \in F, 0 \le i \le 31. \tag{22}$$

Since $x_{0,i}$ and $k_{0,i}$ have the same degree, the head term of polynomials in (21) is $x_{0,i}$ or $k_{0,i}$. If the selected term order is $x_{0,i} < k_{0,i}$, then the head term of polynomial is $k_{0,i}$, $0 \le i \le 31$. For (22), the head term of polynomial is $x_{14,i}$, $0 \le i \le 31$.

It is needed to improve (15) and (16) to meet the requirements of Gröbner basis. From (15), it is easy to get 24 polynomial equations of round i $(1 \le i \le 13)$ as shown in

$$\begin{pmatrix} S(x_{i-1,0}) \\ S(x_{i-1,1}) \\ \vdots \\ S(x_{i-1,31}) \end{pmatrix} + M^{-1} \cdot \begin{pmatrix} x_{i,0} + k_{i,0} \\ x_{i,1} + k_{i,1} \\ \vdots \\ x_{i,31} + k_{i,31} \end{pmatrix} = 0. \tag{23}$$

Similarly, from (16), the 32 polynomial equations of the final round can be obtained as shown in

$$\begin{pmatrix} S(x_{13,0}) \\ S(x_{13,1}) \\ \vdots \\ S(x_{13,31}) \end{pmatrix} + M_{\mathrm{SR}}^{-1} \cdot \begin{pmatrix} x_{14,0} + k_{14,0} \\ x_{14,1} + k_{14,1} \\ \vdots \\ x_{14,31} + k_{14,31} \end{pmatrix} = 0. \tag{24}$$

For degree lexicographical order, the head term of polynomial in (23) and (24) is $x_{i,j}^{254}$, $0 \le i \le 13$, $0 \le j \le 31$. It is easy to see that the head term has no nontrivial common factor; that is, the greatest common factor is 1.

Step 3. The purpose of this step is to construct the polynomial set of the key schedule algorithm. In this step, we also use the equation system given in Section 4.

In order to get the polynomial Gröbner basis of the whole encryption algorithm, the equation system of the key schedule algorithm needs to be improved. It is easy to deduce (25) from (17). Hence,

$$\begin{pmatrix} k_{i,0} \\ k_{i,1} \\ k_{i,2} \\ k_{i,3} \\ k_{i,4} \\ k_{i,5} \\ \vdots \\ k_{i,31} \end{pmatrix} = \begin{pmatrix} k_{i-1,0} \\ k_{i-1,1} \\ k_{i-1,2} \\ k_{i-1,3} \\ k_{i-1,4} \\ k_{i-1,5} \\ \vdots \\ k_{i-1,31} \end{pmatrix} + \begin{pmatrix} S(k_{i-1,29}) \\ S(k_{i-1,30}) \\ S(k_{i-1,31}) \\ S(k_{i-1,28}) \\ k_{i,0} \\ k_{i,1} \\ \vdots \\ k_{i,27} \end{pmatrix}$$

$$+\begin{pmatrix} \xi^{i-1} \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}. \tag{25}$$

In order to ensure that the head terms of key schedule polynomials are pairwise prime, applying the inverse S-box transformation to (25) is needed. The transformation results are shown in

$$\begin{pmatrix} S^{-1}\left(k_{i,0}+k_{i-1,0}+\xi^{i-1}\right) \\ S^{-1}\left(k_{i,1}+k_{i-1,1}\right) \\ S^{-1}\left(k_{i,2}+k_{i-1,2}\right) \\ S^{-1}\left(k_{i,3}+k_{i-1,3}\right) \\ k_{i,4}+k_{i-1,4} \\ k_{i,5}+k_{i-1,5} \\ \vdots \\ k_{i,31}+k_{i-1,31} \end{pmatrix} + \begin{pmatrix} k_{i-1,29} \\ k_{i-1,30} \\ k_{i-1,31} \\ k_{i-1,28} \\ k_{i,0} \\ k_{i,1} \\ \vdots \\ k_{i,27} \end{pmatrix} = 0. \tag{26}$$

According to the algebraic expression of the inverse S-box, all the equations included in (26) can be obtained. If the selected term order is

$$\begin{aligned} &k_{i,31} > k_{i,30} > \cdots > k_{i,0} > k_{i-1,31} > \cdots > k_{i-1,1} \\ &\quad > k_{i-1,0}, \end{aligned} \tag{27}$$

where $1 \le i \le 14$, then the set of polynomial head terms of the key schedule equation (26) is

$$\left\{k_{i,j}^{254}, k_{i,h} : 1 \le i \le 14, 0 \le j \le 3, 4 \le h \le 31\right\}. \tag{28}$$

It is easy to see that the elements of the head term set have no nontrivial common factor.

Step 4. The purpose of this step is the reasonable selection of term order and variable order. If we choose a degree lexicographical order over reasonable variable order, we can make the polynomial head terms of the whole encryption algorithm pairwise prime.

The left-hand sides of (21), (22), (23), (24), and (26) constitute a set of polynomials denoted as A, and the degree lexicographical order $<_A$ over the following variable order makes the head terms of polynomials in A pairwise prime. Hence,

$$\begin{aligned} &\underbrace{x_{0,0} < \cdots < x_{0,31}}_{\text{initial round state variables}} < \underbrace{k_{0,0} < \cdots < k_{0,31}}_{\text{initial key variable}} \\ &< \underbrace{k_{1,0} < \cdots < k_{1,31}}_{\text{first round key variables}} < \cdots \\ &< \underbrace{k_{14,0} < \cdots < k_{14,31}}_{\text{last round key variables}} \\ &< \underbrace{x_{1,0} < \cdots < x_{1,31}}_{\text{first round internal state variables}} < \cdots \\ &< \underbrace{x_{13,0} < \cdots < x_{13,31}}_{\text{11th round internal state variables}} \\ &< \underbrace{x_{14,0} < \cdots < x_{14,31}}_{\text{ciphertext variables}}. \end{aligned} \tag{29}$$

After these four steps, the polynomial set A in the term order $<_A$ is a Gröbner basis of the ideal $\langle A\rangle$ in ring R. The following will give the relevant properties and their theoretical proof.

5.2. The Properties of AES-256 Gröbner Basis. Gröbner basis is the standard notation of polynomial ideal, and there are two useful properties: (1) given a Gröbner basis of an ideal, it is effective to determine whether a polynomial belongs to the ideal; (2) for reasonable term order, the ideal type can be calculated effectively, and the polynomial equation systems deduced from these ideals can be solved. The polynomial set A contains 720 polynomials, where 384 polynomials are with the degree 254 and 336 are linear polynomials that contain 720 variables $x_{i,j}, k_{i,j}, 0 \le i \le 14, 0 \le j \le 31$. For polynomial set A, there are the following conclusions.

Theorem 9. *The set of polynomials A is a Gröbner basis relative to degree lexicographical order $<_A$.*

Proof. Relative to the term order $<_A$, the head term set of polynomials in (21) is $H_1 = \{k_{0,i} : 0 \le i \le 31\}$, the head term set of polynomials in (22) is $H_2 = \{x_{14,i} : 0 \le i \le 31\}$, the head term set of polynomials in (23) and (24) is $H_3 = \{x_{i,j}^{254} : 0 \le i \le 13, 0 \le j \le 31\}$, and the head term set of polynomials in (26) is $H_4 = \{k_{i,j}^{254}, k_{i,h} : 1 \le i \le 14, 0 \le j \le 3, 4 \le h \le 31\}$, so the head term set of polynomials A is $H = H_1 \cup H_2 \cup H_3 \cup H_4$. Since, $\forall a, b \in H, \gcd(a, b) = 1$, elements in H are pairwise prime. According to Theorem 6, it can be obtained that the set of polynomials A is a Gröbner basis relative to term order $<_A$. □

Theorem 9 indicates that the set of polynomials A is a Gröbner basis of ideal $\langle A\rangle$ in ring R. This provides the possibility of carrying out the ideal calculation of AES-256.

Theorem 10. *The ideal $\langle A\rangle$ generated by Gröbner basis A of AES-256 is zero-dimensional.*

(1) list the equation system of AES-256 algorithm;
(2) select a known plaintext and ciphertext pair, and substitute it into the equation system;
(3) construct Gröbner basis Ggrelex of the ideal relative to degree lexicographical order using the method in Section 5.1;
(4) judge the solution structure of the Gröbner basis. Because the equation system contains the field equation, the equation is finite or no solution.
(5) **if and only if** Ggrelex = (1) **then**
(6) the equation system is no solution;
(7) **if** it is no solution, **then**
(8) select another plaintext and ciphertext pair to return to Step (3);
(9) **else** continue;
(10) **end if**
(11) **end if**
(12) convert degree lexicographical Gröbner basis Ggrelex to lexicographical Gröbner basis Glex by using FGLM algorithm;
(13) solve the key variables;
(14) verify the correctness of key by applying plaintext, ciphertext and key to AES-256 algorithm;
(15) **return** the key value;

Algorithm 2: Algebraic cryptanalysis algorithm of AES-256.

Proof. The variable set of the AES-256 equation system is $V = \{x_{i,j}, k_{i,j} : 0 \le i \le 14, 0 \le j \le 31\}$, so the number of variables is $|V| = 720$. It can be seen from the proof process of Theorem 9 that the head term set of polynomials set A is H. $\forall x \in V$, there exists $1 \le d \le 254$ satisfying $x^d \in H$; that is, all variables are in the form of a certain number of times in H. Based on this, for any variable x, there exists a polynomial $g \in A$, so that $\mathrm{HT}(g) = x^d$. According to Theorem 7, it is obvious that $\dim(\langle A \rangle) = 0$; that is, the ideal $\langle A \rangle$ generated by the Gröbner basis A is zero-dimensional. □

Theorem 10 points out that the Gröbner basis A constructed by this paper is zero-dimensional. Due to the term order conversion algorithm FGLM can convert any term order Gröbner basis of zero-dimensional ideal into lexicographical Gröbner basis, so the FGLM algorithm can convert degree lexicographical Gröbner basis A into lexicographical Gröbner basis. The construction of zero-dimensional Gröbner basis is helpful to simplify Gröbner basis calculation, which makes it possible to reduce the complexity of solving multivariate equation system.

5.3. The Algebraic Cryptanalysis Scheme and Its Complexity. The algebraic cryptanalysis algorithm of AES-256 is shown in Algorithm 2.

The maximum degree when computing the Gröbner basis is no more than N, where N is the number of the unknown variables in the equation system, so the upper bound of complexity of computing Gröbner basis is $O(2^N)$. Since the upper bound of the complexity of our scheme depends on the complexity of the Gröbner basis computation, the upper bound of the complexity of our scheme is $O(2^N)$. It can be seen from [17] that the complexity of exhaustively solving the equation system is $O(N2^N)$. It is obvious that the complexity of our scheme is less than the complexity of exhaustive attack, which indicates that our scheme is a successful attack scheme. Moreover, taking into account the sparse and overdefined features of AES-256 equation system, the actual complexity will be far less than the exhaustive attack.

Not all equations are always true in the equation system. For an S-box, there is an equation whose true probability is 255/256. For the full AES-256, the true probability of this kind of equation is 1/9. It needs 9 plaintext and ciphertext pairs to conduct computation 9 times in Step 3, and the equation system will have a finite set of solutions.

6. Conclusions

Based on the characteristics of the round transformation in AES-256, the ShiftRow and MixColumn transformations are merged into left multiplication by a matrix M, making it in the form of linear transformation. In further research on AES-256, the linear transformation and multivariate equation system of AES-256 are further studied. The Gröbner basis is proposed and constructed by choosing reasonable term order and variable order. At the same time, we point out and prove that the Gröbner basis is zero-dimensional. Based on this, the Gröbner basis attack scheme is proposed, and the attack complexity is far lower than the brute force attack. Taking into account the fact that the complexity of our scheme is very high, our research results have a theoretical value. However, the discovery of the zero-dimensional Gröbner basis of AES-256 has guiding significance for further study on efficient Gröbner based attack scheme. The complexity of FGLM and the effectiveness of Gröbner basis attack still need to be further studied.

Competing Interests

The authors declare that they have no competing interests.

Acknowledgments

This work was supported by the National Natural Science Foundation of China (no. 61502008), the Key Scientific Research Project of Henan Higher Education (no. 16A520084), the Natural Science Foundation of Anhui

Province (no. 1508085QF132), and the Doctoral Research Start-Up Funds Project of Anhui University.

References

[1] J. Daemen and V. Rijmen, *The Design of Rijndael: AES—The Advanced Encryption Standard*, Springer Science & Business Media, 2013.

[2] A. Hashemi and D. Lazard, "Sharper complexity bounds for zero-dimensional Gröbner bases and polynomial system solving," *International Journal of Algebra and Computation*, vol. 21, no. 5, pp. 703–713, 2011.

[3] M. Bardet, J.-C. Faugère, and B. Salvy, "On the complexity of the F_5 Gröbner basis algorithm," *Journal of Symbolic Computation*, vol. 70, pp. 49–70, 2015.

[4] A. Bogdanov and V. Rijmen, "Linear hulls with correlation zero and linear cryptanalysis of block ciphers," *Designs, Codes and Cryptography*, vol. 70, no. 3, pp. 369–383, 2014.

[5] Y. Sasaki, "Known-key attacks on rijndael with large blocks and strengthening shiftrow parameter," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. 95, no. 1, pp. 21–28, 2012.

[6] C. Cid and G. Leurent, "An Analysis of the XSL Algorithm," in *Advances in cryptology—ASIACRYPT 2005*, vol. 3788 of *Lecture Notes in Comput. Sci.*, pp. 333–352, Springer, Berlin, Germany, 2005.

[7] S. Murphy and M. Robshaw, "Comments on the security of the AES and the XSL technique," *Electronic Letters*, vol. 39, no. 1, pp. 36–38, 2003.

[8] J. Buchmann, A. Pyshkin, and R.-P. Weinmann, "A zero-dimensional Gröbner basis for AES-128," *Lecture Notes in Computer Science*, vol. 4047, pp. 78–88, 2006.

[9] S. Ghosh and A. Das, "An improvement of linearization-based algebraic attacks," in *Security Aspects in Information Technology*, vol. 7011 of *Lecture Notes in Computer Science*, pp. 157–167, Springer, 2011.

[10] M. R. Z'Aba, K. Wong, E. Dawson, and L. Simpson, "Algebraic analysis of small scale LEX-BES," in *Proceedings of the 2nd International Cryptology Conference: Curve is an Art, Cryptology is a Science (Cryptology '10)*, pp. 77–82, Universiti Teknikal Malaysia Melaka, Melaka, Malaysia, July 2010.

[11] J. Cui, L. Huang, H. Zhong, and W. Yang, "Algebraic attack on Rijndael-192 based on Grobner basis," *Acta Electronica Sinica*, vol. 41, no. 5, pp. 833–839, 2013.

[12] S. N. Ahmad and N. Aris, "The Gröbner package in Maple and computer algebra system for solving multivariate polynomial equations," *Academic Journal UiTM Johor*, vol. 10, pp. 156–174, 2011.

[13] M. Bardet, J. C. Faugere, and B. Salvy, "On the complexity of the F_5 Gröbner basis algorithm," *Journal of Symbolic Computation*, vol. 70, pp. 49–70, 2015.

[14] V. Gerdt and R. La Scala, "Noetherian quotients of the algebra of partial difference polynomials and Gröbner bases of symmetric ideals," *Journal of Algebra*, vol. 423, pp. 1233–1261, 2015.

[15] J. Buchmann, A. Pyshkin, and R.-P. Weinmann, "Block ciphers sensitive to Gröbner basis attacks," in *Topics in Cryptology—CT-RSA 2006*, vol. 3860 of *Lecture Notes in Comput. Sci.*, pp. 313–331, Springer, Berlin, Germany, 2006.

[16] D.-M. Li, J.-W. Liu, and W.-J. Liu, "W-Gröbner basis and monomial ideals under polynomial composition," *Applied Mathematics A*, vol. 26, no. 3, pp. 287–294, 2011.

[17] J.-C. Faugère and A. Joux, "Algebraic cryptanalysis of Hidden Field Equation (HFE) cryptosystems using Gröbner bases," in *Proceedings of the Annual International Cryptology Conference (CRYPTO '03)*, vol. 2729 of *Lecture Notes in Computer Science LNCS*, pp. 44–60, Springer, Santa Barbara, Calif, USA, 2003.

Hindawi
Journal of Electrical and Computer Engineering
Volume 2017, Article ID 3824086, 7 pages
https://doi.org/10.1155/2017/3824086

Research Article

Acoustic Log Prediction on the Basis of Kernel Extreme Learning Machine for Wells in GJH Survey, Erdos Basin

Jianhua Cao, Yancui Shi, Dan Wang, and Xiankun Zhang

College of Computer Science and Information Engineering, Tianjin University of Science and Technology, Tianjin, China

Correspondence should be addressed to Jianhua Cao; caojh@tust.edu.cn

Received 24 November 2016; Accepted 22 January 2017; Published 22 February 2017

Academic Editor: Hui Cheng

In petroleum exploration, the acoustic log (DT) is popularly used as an estimator to calculate formation porosity, to carry out petrophysical studies, or to participate in geological analysis and research (e.g., to map abnormal pore-fluid pressure). But sometime it does not exist in those old wells drilled 20 years ago, either because of data loss or because of just being not recorded at that time. Thus synthesizing the DT log becomes the necessary task for the researchers. In this paper we propose using kernel extreme learning machine (KELM) to predict missing sonic (DT) logs when only common logs (e.g., natural gamma ray: GR, deep resistivity: REID, and bulk density: DEN) are available. The common logs are set as predictors and the DT log is the target. By using KELM, a prediction model is firstly created based on the experimental data and then confirmed and validated by blind-testing the results in wells containing both the predictors and the target (DT) values used in the supervised training. Finally the optimal model is set up as a predictor. A case study for wells in GJH survey from the Erdos Basin, about velocity inversion using the KELM-estimated DT values, is presented. The results are promising and encouraging.

1. Introduction

Oil and gas exploration in sedimentary basins is very complicated, since all the targets are buried underground and they cannot be viewed or touched directly. So all the properties for the buried targets have to be predicted or estimated by using modern electrical or magnetic tools. The physical properties of the geologic formations include pore-fluid pressure, rock lithology, porosity, permeability, and oil or water saturation. Nowadays the conventional tool for characterizing these geophysical properties is well logging, and some logs such as gamma ray (GR), dual induction log, formation density (DEN) compensated, deep resistivity (REID), self-potential (SP), and sonic log (DT) are usually recorded. Among them, the sonic log (DT) has largely been used to predict rock porosity, to perform petrophysical analysis, or to carry out well-to-seismic inversion.

Owing to historical operation mistakes or recording loss, the sonic log may not be available in well logging suites. The traditional way solving this problem is to transform the DEN or REID log to DT log based on some experimental formula built between these logs. It might be feasible for some area, but sometimes the errors are unacceptable.

Artificial intelligence techniques have the advantage in connecting unrelated parameters and solving nonlinear problems. Such techniques, including BP neural network, fuzzy reasoning, or evolutionary computing for data analysis and interpretation have become effective tools in the workflow for well drilling and reservoir characterization [1–10]. However, traditional neural networks have many known drawbacks in the learning process, such as multiple local minima, slow learning speed, and poor generalization performances [11].

Extreme learning machine (ELM) is a single-hidden layer feed-forward neural network (SLFN) proposed by Huang et al. [12, 13]. The ELM approach to training SLFN consists in the random generation of the hidden layer weights, followed by solving a linear system of equations by least-squares for the estimation of the output layer weights. This learning strategy is very fast and gives good prediction accuracy. Theoretically and practically, this algorithm can produce good generalization performance in most cases and can

learn thousands of times faster than conventional popular learning algorithms for feed-forward neural networks [14]. A lot of real-life applications [15–18] have already demonstrated advantages of using basic ELM. A kernel-based ELM (KELM) has also been developed lately [19], where the hidden layer feature mapping is determined by the kernel matrix. In this version, only the kernel function and its parameters are needed to be defined; the number of hidden nodes is not required. With the use of kernel function, KELM is expected to achieve better generalization performance than basic ELM. Furthermore, as randomness does not occur in KELM, the chance of result variations could be reduced [20].

In this paper, kernel-based extreme learning machine is used to predict missing sonic (DT) logs when only common logs (e.g., natural gamma ray—GR, bulk density—DEN, or deep resistivity—REID) are available. By using KELM, we first create and train a supervised network model based on experimental data and then confirm and validate the model by blind-testing the results. The optimal model is at last applied to wells containing the predictor data but with lack of DT log. We use this workflow in GJH survey from Erdos Basin and the KELM-estimated DT logs are then integrated in the seismic inversion to identify the sandstone reservoir.

The rest of this paper proceeds as follows. Section 2 gives a short review of ELM and KELM. Section 3 describes the experiments using KELM, including the data preparation, parameter selection, and model validation. Section 4 gives the prediction application in GJH survey. Finally, Section 5 gives the conclusion of this work.

2. Methodology

In this study, the kernel extreme learning machine (KELM) is employed to predict the DT logs for the wells in GJH survey. So we present an overview of the ELM and kernel-based ELM as follows.

2.1. ELM. The classical ELM was proposed for SLFNs by Huang et al. [12, 13]. Different from BP network, the input weights and biases of ELM are randomly assigned and need not be fine-tuned within the training phase, and the output weights can be determined analytically by finding the least-square solution. The prediction of ELM is given by

$$f_L(\mathbf{x}) = \sum_{i=1}^{L} \boldsymbol{\beta}_i \mathbf{h}_i(\mathbf{x}) = \mathbf{h}(\mathbf{x})\,\boldsymbol{\beta}, \tag{1}$$

where $\boldsymbol{\beta} = [\boldsymbol{\beta}_1, \ldots, \boldsymbol{\beta}_L]^T$ is the weight vector connecting the hidden node and the output nodes and $\mathbf{h}(\mathbf{x}) = [\mathbf{h}_1(\mathbf{x}), \ldots, \mathbf{h}_L(\mathbf{x})]^T$ is the output of the hidden layer with respect to the sample $\mathbf{x}$. Since the weights and biases are initially assigned for the hidden layer, when the activation function is set, $\mathbf{h}(\mathbf{x})$ is determined and need not be tuned. And the only unknown parameter is $\boldsymbol{\beta}$, which can be solved as constrained optimization problem:

$$\text{Minimize:} \quad \left\|\mathbf{H}\boldsymbol{\beta} - T\right\|_p^{\alpha 1} + \frac{C}{2}\left\|\boldsymbol{\beta}\right\|_q^{\alpha 2}, \tag{2}$$

where C is control parameter for a tradeoff between structural risk and empirical risk, T is the target output for the network. And when $p, q = F$ and $\alpha 1, \alpha 2 = 2$, a popular and efficient closed-form solution for $\boldsymbol{\beta}$ is

$$\boldsymbol{\beta} = \begin{cases} \mathbf{H}^T\left(C\mathbf{I} + \mathbf{H}\mathbf{H}^T\right)^{-1} T & N \geq L \\ \left(C\mathbf{I} + \mathbf{H}\mathbf{H}^T\right)^{-1} \mathbf{H}^T T & N \leq L \end{cases} \tag{3}$$

2.2. KELM. As proposed in Huang et al. [19], if $\mathbf{h}(\cdot)$ is unknown, that is, an implicit function, one can apply Mercer's conditions on ELM and define a kernel matrix for ELM that takes the form

$$\begin{aligned} &\mathbf{K}_{\text{ELM}} = \mathbf{H}\mathbf{H}^T: \\ &\mathbf{K}_{\text{ELM}_{i,j}} = \mathbf{h}\left(\mathbf{x}_i\right) \cdot \mathbf{h}\left(\mathbf{x}_j\right) = \mathbf{k}\left(\mathbf{x}_i, \mathbf{x}_j\right), \end{aligned} \tag{4}$$

where $\mathbf{k}(\mathbf{x}_i, \mathbf{x}_j)$ is a kernel function. Many kernel functions can be used in kernel-based ELM, such as linear, polynomial, and radial basis function, so that we can obtain the kernel form of the output function as follows:

$$f_L(\mathbf{x}) = \begin{bmatrix} \mathbf{k}\left(\mathbf{x}, \mathbf{x}_1\right) \\ \vdots \\ \mathbf{k}\left(\mathbf{x}, \mathbf{x}_N\right) \end{bmatrix} \left(C\mathbf{I} + \mathbf{K}_{\text{ELM}}\right)^{-1} T \tag{5}$$

Similar to the SVM, $\mathbf{h}(\mathbf{x})$ need not be known; instead, its kernel can be provided (e.g., Gaussian kernel $\mathbf{k}(\mathbf{u}, \mathbf{v}) = \exp(\|\mathbf{u}-\mathbf{v}\|^2/\sigma)$). The optimal penalty parameter C and kernel width s are determined by try and error way. Node number of the hidden layer L need not be available beforehand either. The experimental and theoretical analysis of Huang et al. showed that KELM produces improved generalization performance over the SVM/LS-SVM [21].

For the given type of the kernel function, the training dataset, and the initial parameters of the network, the following steps are considered.

Step 1. Initiate the population based on the kernel function.

Step 2. Evaluate the fitness function of each parameter.

Step 3. The optimal parameters of kernel function can be determined. Then, based on the optimized parameters, the hidden layer kernel matrix is computed.

Step 4. Determine the final output weights.

3. Experimental Study

3.1. Problem Description and Related Work. Well logging is the practice of making a detailed record of the geologic formations penetrated by a borehole. Normally the log is based on the physical measurements made by instruments lowered into the borehole. According to the geophysical properties of the rocks, the logs are always classified as follows: electrical logs, porosity logs, lithology logs, and miscellaneous logs. Sonic log (DT) belongs to the porosity logs, and it provides a formation interval transit time, which

typically varies lithology and rock texture, especially porosity for the rocks. Gamma ray log is a log of the natural radioactivity of the formation along the borehole, measured in API units, particularly useful for distinguishing between sands and shales in a siliciclastic environment. This is because sandstones are usually nonradioactive quartz, whereas shales are naturally radioactive due to potassium isotopes in clays and adsorbed uranium and thorium.

The main datasets used in this study include acoustic log (DT), the gamma ray (GR), the resistivity log (REID), which represents the variation of the electric resistivity, the density (DEN), which records the density variation with depth in the borehole, and the self-Potential (SP), a measurement of natural electric potential. These geophysical parameters DT, GR, REID, DEN, and SP are intrinsically linked, since each of them reflects some physical property of the same rock layer. Take sandstone as an example. Pores are sure to exist at the sandstone interval, and if the pores are not filled with other types of tight materials, fluid is the only also important stuffing. There might be oil or gas and water as well. Since the fluid has different physical parameters than the surrounding sandstone, obvious differences will be recorded on the measuring logs: lower GR, lower DT, higher REID, lower DEN, and abnormal change on SP. Thus just observing the characters of the logs, especially those abnormal changes, the experienced researchers have confidence to tell the geological information along the borehole. And then some researchers try to build theoretical relationships between the logs. Thousands of experiments result in empirical equations. For example, DEN could be transformed using DT log when DEN is missing and the relation is defined as Gardener formula [6]:

$$\mathrm{DEN} = \alpha \mathrm{DT}^{-\beta}, \tag{6}$$

where, α, β are the coefficients and their values are up to the core tests for the studied area.

In this study, the key we focus on is the DT log, and we want to find the optimal way to get the DT log when it is missing.

The sonic log (DT) is very important in petroleum exploration phase. One way for using DT is to estimate rock porosity, which is the critical parameter for the reservoir evaluation, and identify the fluid information along the borehole. Additionally, since DT log has both time and velocity information, it becomes the reliable key for the time-depth conversion when using seismic data to interpret structures and geological mapping. In one word, the DT log is indispensable for the geophysical and geological study.

But there has always been imperfection, and sometimes, owing to operation mistake or recording loss, DT log may not be available in some wells. One solution for obtaining the DT log is to carry out empirical transformation from other logs, and the model is built by experiment analysis. The formula is just for specific field condition, and it can not be used for all the formation conditions. For instance, Faust formula is just for DT calculation using REID log, and cases [7] have shown that the formula is not suitable when fluid exits in the formation. So another study to synthesize missing DT is to use soft-computing methods, such as artificial neural network, gene expressing programming, and fuzzy reasoning. ANN (artificial neural network) has been frequently used in petrophysical properties estimation, and results show satisfied performances when choosing proper models and parameters [8, 9, 16]. The most important property of ANNs is their ability to approximate virtually any function in a stable and efficient way. By using ANNs, it is possible to create a platform on which different models can be constructed. Baziar et al. [22] tested coactive neurofuzzy inference system which combines fuzzy model and neural network in permeability prediction in a tight gas reservoir and gained convincing results.

Since DT has intrinsic links with the other geophysical logs, researchers often use logs like GR, REID, and so forth as the original inputs and the DT as outputs. Linear and nonlinear relationships have been set up using the soft-computing methods. But the results are not always satisfied. Thus our purpose is to build an optimal and reliable relationship between those geophysical logs and DT log.

In this paper, we investigate the capability of a kernel extreme learning machine in building the nonlinear mathematical model that best explains DT (target) as a function of GR, REID, DEN, and SP (predictors).

3.2. Data Preparation. In order to validate the use of KELM in the context of log data recorded in oil and gas wells, we employed datasets obtained from seven wells drilled in the GJH survey in Erdos Basin.

The study involves the following well logging parameters: gamma ray (GR), deep resistivity (REID), self-potential (SP), formation density (DEN), and sonic log (DT). Among the wells, wells of YQ2, Y209, S211, S212, and S215 have full suites of well logs, while DT log is not available in the other two wells (S219 and S205). According to the evaluation conclusion for the logging process, we choose the farther four wells as training dataset sources and well S215 as the testing dataset. Shanxi group of the Permian formation is set as the analysis interval. Logs of GR, REID, SP, DEN, and DT in the interval from the mentioned four wells are collected and grouped as training dataset, while logs of well S215 as the validation target.

Figure 1 is the example of logs showing of well YQ2 in the Shanxi group of Permian formation ranging from 2700 to 2798 meters. The lithology includes sandstone, mudstone, and thin coal layer, and it is easy to differentiate them from the GR log. Coal layer has very low GR and DEN response and abnormal high DT and REID. Thus, for the same type of rocks, these logs have close geophysical link, which is the foundation for DT prediction using these logs.

We select data in the same interval from the four wells of YQ2, Y209, S210, and S212 as the training samples. To ensure the quality of the logs, we use caliper log (CAL) as the reference. Constant diameter of the wellbore (described by CAL) means good environment for the other suite of logs. Totally about 40,000 data items are available for the training process.

To speed up the convergence of the gradient descent algorithm, data normalization is mandatory for the performance. And the above-mentioned logs have different measurement units. All of the logs are normalized before formally inputting

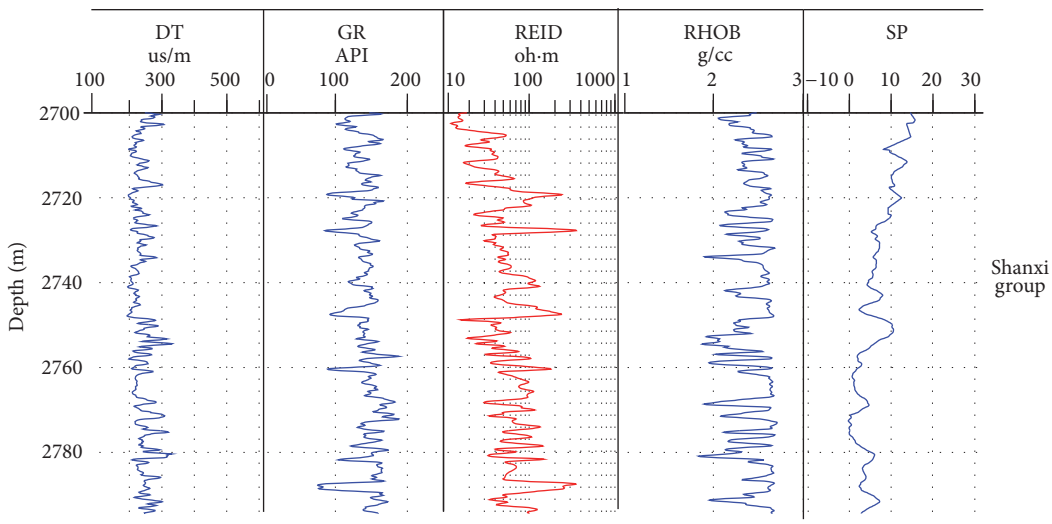


Figure 1: Logs showing of well YQ2 in the Shanxi group of Permian formation.

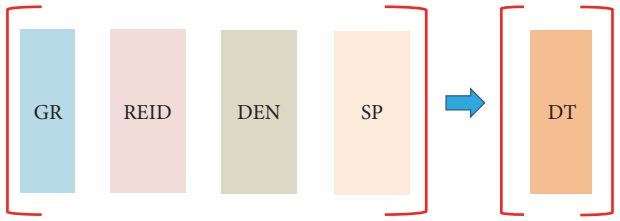


Figure 2: Example of multi-input versus single-output sonic log prediction using KELM. Details about the well logging parameters depicted in the figure are given in text.

into the network. The normalized variable has the following form:

$$X_{\text{new}} = \frac{X_{\text{old}} - \min X}{\max X - \min X}, \tag{7}$$

where X stands for logs of GR, AC, DEN, REID, and SP. The new normalized variable X_{new} takes the range from 0 to 1 for all the parameters.

In KELM network learning, the output model is created by learning patterns from the training examples provided. Therefore, the training dataset should be carefully chosen in order to provide correct examples. And noise should be removed from the samples; otherwise errors may affect the final performance.

3.3. KELM Model Training. For the KELM network model, there are totally four input neurons and one target at the output layer. The four inputs include GR, REID, SP, and DEN logs, and the main task is to build reliable prediction model between these inputs logs and DT log (shown as Figure 2). Gaussian radial basis kernel function is used because it usually produces good results and outperforms other functions for regression.

In the algorithms of KELM, two hyperparameters, namely, the regularization factor (C) and the basis width parameter of the kernel function ($s2$), are necessary. To select the best values for these hyperparameters, leave-one-out cross-validation (LOOCV) is usually applied [9]. In the preliminary experiment, the KELM model achieves the best performance when the values of C and s are set to (10, 1), so these values are finally chosen in our experiment.

The quality of the trained model is evaluated based on the prediction accuracy. The Mean Squared Error (MSE) is computed as the average over all squared deviations of the predictions from the real values.

After training, the model could be presented in the following form:

$$Y = \begin{bmatrix} K(X, x_1) \\ \cdots \\ K(X, x_n) \end{bmatrix} \boldsymbol{\beta}, \tag{8}$$

where $K(*)$ is the Gaussian radial basis kernel function, n is the number of training data, and β is the trained weight matrix of the model based on the training data. By providing unseen input data X to the model, the corresponding model output Y can be predicted.

Furthermore, in order to testify the advantages of KELM, BP network algorithm is used in the model training and testing process to compare with KELM. Backpropagation (BP) feed-forward network is the most commonly used ANN approach, and it is also criticized on its difficulty to decide learning rates, being easy to be stuck on local minimums, overfit problems, and being time-consuming [11].

Table 1 shows the results on testing data. Accuracy, MSE, and training time are three factors in comparison, and the values are obtained by averaging estimations of the samples in well YQ2. The table shows the accuracy, Mean Squared Error (MSE), and total time in seconds for the two processing approaches, respectively. Best results are achieved by KELM with an accuracy of 0.906, mean absolute error of 0.423%, and fast learning speed (23 seconds).

Table 1: Comparison of porosity prediction performance results on KELM against BP methodology for well YQ2. The comparison strata belong to the Shanxi group of the Permian formation.

Algorithm	Accuracy	MSE (%)	Training time (s)
BP	0.752	1.812	912
KELM	0.906	0.423	23

3.4. KELM Model Validation and Prediction. Through the above-mentioned training process, the KELM model for predicting DT is established finally. Although the training dataset has almost 40,000 data points, the training task costs very short time and the performance is satisfying. To validate the KELM model, we use well S215 as blind well. The four logs are collected and processed for the well, and then we input them into the model and keep the network parameters. Since the data for validation is small group with nearly 6000 samples, the process only costs 6 seconds and one predicted DT is generated. In well S215, there has been DT log, so that the predicted DT can be used in comparison with the real DT. Figure 3 shows the comparison result. The curve with the red color is the predicted one from KELM model, and the curve with the blue color stands for the recorded DT log. It is easy to see that the total changing trend and the finest part are almost the same; thus the model is qualified in this study and is reliable to be a predictor.

In this study, DT log is missing in the two wells of S219 and S205. Here the KELM model is then recommended to do the prediction task for the two wells. Luckily, the four input logs (GR, REID, DEN, and SP) are guaranteed in both of the wells. Using the same noise-filtering and normalization step in the training and validating step, we firstly input the four predictor logs of well S219 into the model and generate DT log for this well. And then we repeat the steps for the well S205 and also get the DT log. Figure 4 shows the predicted DT log for well S219 in the Shanxi group of Permian formation.

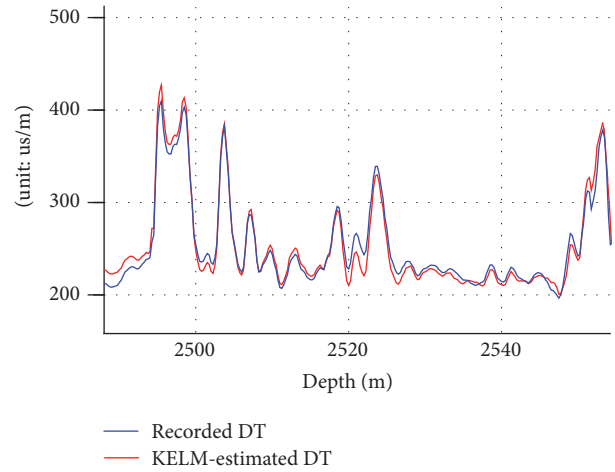


Figure 3: Logs comparison in Shanxi group of Permian formation in well S215.

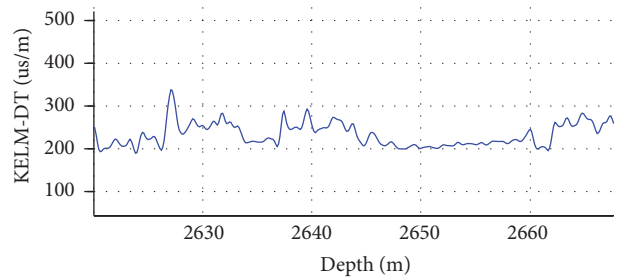


Figure 4: Estimated DT log using KELM model (colored in blue) for S219.

4. KELM-Estimated DT Application

The above analysis has shown the reliability and accuracy of the KELM-based prediction model. All of the 7 wells in the studied area have DT logs now, although two of them are generated using KELM model.

In reservoir description phase, seismic profiles are just wiggle-based and not so convenient for researchers to understand and identify the potential fluid zone. Thus transforming the wiggle shape of seismic sections into velocity or lithological profiles are the necessary step in seismic interpretation. That goal of transformation in geophysical process is the seismic inversion. Since DT log has time unit and velocity information, while seismic data is just in time unit, in the inversion task, DT can be used to do the well-to-seismic calibration and mark the reservoir interval. Here we just focus on the KELM-estimated DT application in the seismic inversion other than discussing the complex inversion technique.

Figure 5 shows part section of the seismic inversion result for line 400 using the predicted DT log of well S205. The inversion result is colored, and the color stands for the velocity change within the Permian formation. Warm color of red and yellow is the high velocity area, while the cold color of green and blue is the relatively low velocity area. Since the rocks within the interval have the difference in velocity reference, the color changes can be viewed as the lithology component difference. Normally sandstone has higher velocity than mudstone, and coal layer has the lowest velocity character. Therefore warm color in the section represents the sandstone area, while the pure blue color is the index of coal layer. So when interpreting the inversion result with the geological reference, we may divide the interval into three parts: the upper part-I, which is mainly composed of sandstone and mudstone and the farther is richer, the middle part-II, with upper half-dominant coal layer and lower half-dominant sandstone, and the lower part-III, which has almost the same bedding principal as the middle part, with thinner sandstone and coal layer. The estimated DT log is inserted as color plot and the meaning of color ranges is the same as the inversion section. It almost matches the section in color resolution, and that is the normal phenomenon. DT log has finer sample interval than the section, and, for the section, more focus will be directed to the horizontal color difference interpretation. The continuous horizontal color zones mean a lot for the geologists and engineers.

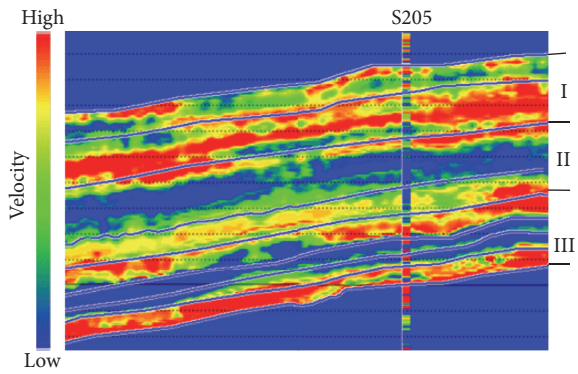


Figure 5: KELM-based inverted velocity section crossing well S205.

5. Conclusions

This paper discusses kernel extreme learning machine as a tool for predicting the sonic log in gas/oil wells based on other available common logs. Strict steps including data normalization, training set selection, and optimization of the ELM parameters are very important for deciding the prediction power, the generalization capability, and the complexity of the derived regression model. Extensive applications are carried on to investigate the prediction power of model-predicted DT log use for seismic inversion.

The method presented here is not limited to modeling DT logs only. It can be extended, with appropriate modifications of the algorithm, in any area of well logging studies, where missing log values are needed. Thus, we offer a blueprint for future similar applications.

Competing Interests

The authors declare that they have no conflict of interests.

Acknowledgments

This work is supported by National Natural Science Foundation of China (no. 61402331). The Foundation of Educational Commission of Tianjin City, China (Grant no. 20140803) also funded this research.

References

[1] A. F. Al-Anazi and I. D. Gates, "Support vector regression to predict porosity and permeability: effect of sample size," *Computers and Geosciences*, vol. 39, pp. 64–76, 2012.

[2] J. Asadisaghandi and P. Tahmasebi, "Comparative evaluation of back-propagation neural network learning algorithms and empirical correlations for prediction of oil PVT properties in Iran oilfields," *Journal of Petroleum Science and Engineering*, vol. 78, no. 2, pp. 464–475, 2011.

[3] M. Baneshi, M. Behzadijo, M. Schaffie, and H. Nezamabadi-Pour, "Predicting log data by using artificial neural networks to approximate petrophysical parameters of formation," *Petroleum Science and Technology*, vol. 31, no. 12, pp. 1238–1248, 2013.

[4] C. Cranganu and M. Breaban, "Using support vector regression to estimate sonic log distributions: a case study from the Anadarko Basin, Oklahoma," *Journal of Petroleum Science and Engineering*, vol. 103, pp. 1–13, 2013.

[5] S. Chikhi and M. Batouche, "Probabilistic neural method combined with radial-bias functions applied to reservoir characterization in the Algerian Triassic province," *Journal of Geophysics and Engineering*, vol. 1, no. 2, pp. 134–142, 2004.

[6] H. Khoshdel and M. A. Riahi, "Multi attribute transform and neural network in porosity estimation of an offshore oil field—a case study," *Journal of Petroleum Science and Engineering*, vol. 78, no. 3-4, pp. 740–747, 2011.

[7] J. R. Hearst, P. H. Nelson, and F. L. Paillet, *Well Logging for Physical Properties*, John Wiley & Sons, 2000.

[8] A. Kouider El Ouahed, D. Tiab, A. Mazouzi, and A. J. Safraz, "Application of artificial intelligence to characterize naturally fractured reservoirs," Paper SPE 84870, 2013.

[9] A. Ouenes, "Practical application of fuzzy logic and neural networks to fractured reservoir characterization," *Computers & Geosciences*, vol. 26, no. 8, pp. 953–962, 2000.

[10] R. S. Zazoun, "Fracture density estimation from core and conventional well logs data using artificial neural networks: the Cambro-Ordovician reservoir of Mesdar oil field, Algeria," *Journal of African Earth Sciences*, vol. 83, pp. 55–73, 2013.

[11] R. B. C. Gharbi and G. A. Mansoori, "An introduction to artificial intelligence applications in petroleum exploration and production," *Journal of Petroleum Science and Engineering*, vol. 49, no. 3-4, pp. 93–96, 2005.

[12] G.-B. Huang, Q.-Y. Zhu, and C.-K. Siew, "Extreme learning machine: a new learning scheme of feedforward neural networks," in *Proceedings of the IEEE International Joint Conference on Neural Networks*, pp. 985–990, Budapest, Hungary, July 2004.

[13] G.-B. Huang, Q.-Y. Zhu, and C.-K. Siew, "Extreme learning machine: theory and applications," *Neurocomputing*, vol. 70, no. 1–3, pp. 489–501, 2006.

[14] H. Zhong, C. Miao, Z. Shen, and Y. Feng, "Comparing the learning effectiveness of BP, ELM, I-ELM, and SVM for corporate credit ratings," *Neurocomputing*, vol. 128, pp. 285–295, 2014.

[15] J. B. Butcher, D. Verstraeten, B. Schrauwen, C. R. Day, and P. W. Haycock, "Reservoir computing and extreme learning machines for non-linear time-series data analysis," *Neural Networks*, vol. 38, pp. 76–89, 2013.

[16] J. Cao, J. Yang, Y. Wang, D. Wang, and Y. Shi, "Extreme learning machine for reservoir parameter estimation in heterogeneous sandstone reservoir," *Mathematical Problems in Engineering*, vol. 2015, Article ID 287816, 10 pages, 2015.

[17] R. Minhas, A. Baradarani, S. Seifzadeh, and Q. M. Jonathan Wu, "Human action recognition using extreme learning machine based on visual vocabularies," *Neurocomputing*, vol. 73, no. 10–12, pp. 1906–1917, 2010.

[18] R. Moreno, F. Corona, A. Lendasse, M. Graña, and L. S. Galvão, "Extreme learning machines for soybean classification in remote sensing hyperspectral images," *Neurocomputing*, vol. 128, pp. 207–216, 2014.

[19] G.-B. Huang, D. H. Wang, and Y. Lan, "Extreme learning machines: a survey," *International Journal of Machine Learning and Cybernetics*, vol. 2, no. 2, pp. 107–122, 2011.

[20] S. Shamshirband, K. Mohammadi, H.-L. Chen, G. N. Samy, D. Petković, and C. Ma, "Daily global solar radiation prediction from air temperatures using kernel extreme learning machine: a case study for Iran," *Journal of Atmospheric and Solar-Terrestrial Physics*, vol. 134, pp. 109–117, 2015.

[21] G.-B. Huang, H. Zhou, X. Ding, and R. Zhang, "Extreme learning machine for regression and multiclass classification," *IEEE Transactions on Systems, Man, and Cybernetics, Part B: Cybernetics*, vol. 42, no. 2, pp. 513–529, 2012.

[22] S. Baziar, M. Tadayoni, M. Nabi-Bidhendi, and M. Khalili, "Prediction of permeability in a tight gas reservoir by using three soft computing approaches: a comparative study," *Journal of Natural Gas Science and Engineering*, vol. 21, pp. 718–724, 2014.