Long-Short Term Memory Network-Based Monitoring Data Anomaly Detection of a Long-Span Suspension Bridge

Jianliang Zhang 1, Jian Zhang 1,2,* and Zhishen Wu 1,3

1 School of Civil Engineering, Southeast University, Nanjing 211189, China
2 Jiangsu Key Laboratory of Engineering Mechanics, Southeast University, Nanjing 211189, China
3 Key Laboratory C&PC Structures, Ministry of Education, Southeast University, Nanjing 210096, China
* Correspondence: jian@seu.edu.cn; Tel.: +86-159-5194-158

Abstract: Structural health monitoring (SHM) systems have been widely applied in long-span bridges and a large amount of SHM data is continually collected. The harsh environment of sensors installed at structures causes multiple types of anomalies such as outlier, minor, missing, trend, drift, and break in the SHM data, which seriously hinders the further analysis of SHM data. In order to achieve anomaly detection from a large amount of SHM data, this paper proposes a long-short term memory (LSTM) network-based anomaly detection method. Firstly, the proposed method reduces the workload for preparing training sets. Secondly, the purpose of real-time anomaly detection can be met. Thirdly, the problem of high alarm rate can be avoided by utilizing double thresholds. To validate the effectiveness of the proposed method, a case study of finite element model simulation is firstly introduced, which illustrates the detailed implementation process. Finally, acceleration data from the SHM system of a long-span suspension bridge located in Jiangyin, China is employed. The results show that the proposed method can detect anomaly with high accuracy and identify abnormal accidents such as a ship collision quickly.

Keywords: long-span bridge; SHM system; anomaly detection; LSTM network; double thresholds

1. Introduction

SHM systems can collect structural responses which play an important role in evaluating the health condition and monitoring the exceptional events at any time, such as in ship-bridge collisions. Thus, more and more complex health monitoring systems have been installed on large-scale or critical civil structures [1–4]. In addition, many new detection methods have also been applied to bridge structures [5,6].

Meanwhile, massive SHM data is continually being collected and big data analytics is currently a hot research area. Generally, big data analysis is mainly divided into five steps which include data extraction, data storage, data cleaning, data mining, and data visualization. Among them, data mining is most widely studied, particularly for structural damage detection based on vibration and deformation data [7–10]. Unfortunately, most SHM systems work in complicated and harsh environments, which inevitably results in various abnormal data. According to the official documents, 496 sensors installed in Sutong Bridge collect 11,904 data files every day, and only about 64% data files are in good condition. The remainder of the data files are obviously abnormal in time domain or even missing, which will have a serious impact on data mining and structural health evaluation. Overall, anomaly detection is an important prerequisite for data analysis and the main purpose of this paper is to find a way to detect the anomalous SHM data with high accuracy and in real-time.

The simplest anomaly detection method is to set a static threshold for SHM data. However, detection results deeply depend on professional knowledge. Nevertheless, most traditional machine learning-based anomaly detection methods (such as Cluster, PCA,
SVM, etc.) require enough data which cannot be processed in real time, so these methods cannot be applied to real-time processing time series [11–17].

Recently, deep learning-based methods have increasingly attracted researchers’ attention, which have been applied to all aspects. Kramer [18] utilized an autoregressive neural network to reduce noise and detect anomalies. Tamilselvan and Wang [19] utilized deep belief networks to diagnose failures in aircraft engines and electric power transformers. Abdeljaber et al. [20] utilize one-dimensional convolutional neural networks to detect structural damage. Cha et al. [21] utilized convolutional neural networks to detect crack damage detection. Allen et al. [22] utilized recurrent neural network to automatically detect pixel-level pavement cracks. Some other applications can be found in references [23–28].

Studies on anomaly detection based on deep learning have also made some progress in this field. Kambayashi et al. [29] utilized feed-forward neural networks to reconstruct the original signals; the network is trained by minimizing reconstruction errors. The well-trained network will produce larger reconstruction error with abnormal data input. Kim et al. [30] divides the data into several parts, each of which is reconstructed by deep neural network-based encoder decoder scheme; the part that has larger reconstruction error is identified as abnormal data. Filonov et al. [31] and Tuor et al. [32] utilized the prediction error of recurrent neural network (RNN) to detect the abnormal data successfully. Bao et al. [33] converted SHM data into images, and a depth-restricted Boltzmann machine (RBM) was utilized to identify the abnormal data. Ni et al. [34] used a one-dimensional convolutional neural network to extract the features of input sequences, and the fully connected network was used to recognize the abnormal data. Nanduri et al. [35] uses LSTM and GRU network to predict aircraft’s flight data, and the abnormal data are judged by a given threshold. The anomaly detection methods mentioned above which utilize neural network to reconstruct original data belongs to the offline mode and cannot provide warnings in real-time for abnormal events. Although real-time warnings can be achieved by utilizing the RNN prediction error, the RNN network itself is prone to “gradient disappearance” in the training process. The anomaly detection method which transforms data into an image actually is a kind of anomaly judgment based on computer vision, and a lot of information can be easily lost during the transformation process. The anomaly detection method which uses LSTM and GRU can process monitoring data in real-time, but the threshold given by experience does not make sense.

To solve the problems mentioned above, this paper proposes a LSTM network-based anomaly detection method, which includes two main steps: (1) an anomaly detection model including input layer, LSTM cycle module, and output layer is built; and (2) judgment criteria of double thresholds corresponding to the detection model is determined. The proposed anomaly detection method only utilizes a small amount of historical normal data in the training process, which is beneficial for SHM data with a large proportion of normal data and greatly reduces the workload of selecting normal historical SHM data in the early stage. In addition, a double thresholds method was proposed to avoid the problem of high alarm rate in the past, and the continuous input character of LSTM network can realize the aim of developing real-time warnings for abnormal events.

This paper is organized as follows. Section 2 introduces the details on the overall framework of the proposed method. Section 3 verifies the feasibility of the proposed method through a case study of finite element model simulation. In Section 4, the effectiveness of the proposed method is experimentally validated by using one day SHM data of a long-span suspension bridge when the accident of ship-bridge collision occurred. Section 5 includes the conclusion with major findings, and suggestions for further work are discussed.

2. Framework of the Proposed Method

The overall framework of the proposed method in this paper for detecting abnormal SHM data is shown in Figure 1. The proposed method mainly consists of four steps: data preprocessing, network prediction, thresholds decision, and abnormal detection. In the section of data preprocessing, the normal data is firstly selected from historical monitoring
data manually, and then the normal monitoring data is divided randomly into three groups, named training sets, validation sets, and threshold sets. The other three steps are detailed as follows.

![Diagram](image.png)

**Figure 1.** The framework of the proposed method.

### 2.1. Network Prediction

The RNN is a neural sequence model that achieves state of the art performance on many important tasks. Most importantly, the RNN models allow us to operate over sequences of vectors which just meet the continuously generation characteristic of SHM data, while the convolutional neural networks (CNN) usually only accepts a fixed-sized vector as input. However, the traditional RNN usually can’t update the neuron parameters since the input sequence in the actual training process is too long [36,37]. LSTM networks differ from standard RNN networks primarily with respect to the use of memory blocks instead of neurons [38], which can solve the problem wherein traditional RNN cannot be trained when the input sequence becomes longer. Therefore, the LSTM network is selected to predict normal monitoring data in this paper.

The monitoring data recorded by sensors is composed of structural response data and random noise, and the structural response data of different channels have different data structures. This will increase the complexity of network and the difficulty of training when the monitoring data of all channels is simulated by a general network. To overcome the above problems, this paper suggests that it is necessary to establish different ‘small’ networks for each channel separately. This can avoid the problem of performance difference of a general network caused by unbalanced dataset.
In practice projects, the positions of many sensors are close (for example, they are installed on the same sling), and they can share a general network since their data structures are similar (In other words, they are highly relevant). Inspired by the covariance-driven random subspace method, the correlation coefficient is utilized to measure the correlation of monitoring data between different channels, and a threshold of correlation coefficient is necessary to determine the number of networks built. The correlation coefficient between two channels can be calculated by Equation (1):

\[
    r_{XY} = \frac{\sum (X_i - \bar{X})(Y_i - \bar{Y})}{\sqrt{\sum (X_i - \bar{X})^2 \sum (Y_i - \bar{Y})^2}}
\]

where \( r \) is correlation coefficient, \( X_i \) and \( Y_i \) are monitoring data of two channels at time point \( i \), \( \bar{X} \) and \( \bar{Y} \) are mean values of monitoring data.

The LSTM network utilized in this paper consists of three parts: the input layer, the LSTM cycle module and the output layer (fully connected layer), as shown in Figure 2. The sets of input sequences, cell states, hidden states, output sequences and target sequences in the LSTM network are denoted as \( X = (x_1, \ldots, x_t, \ldots) \), \( C = (c_1, \ldots, c_t, \ldots) \), \( H = (h_1, \ldots, h_t, \ldots) \), \( \bar{Y} = (\bar{y}_1, \ldots, \bar{y}_t, \ldots) \) and \( Y = (y_1, \ldots, y_t, \ldots) \) separately. The cell state \( c_t \) and hidden state \( h_t \) can be updated by Equation (2), and the output sequence \( \bar{y}_t \) can be calculated by Equation (3):

\[
    f_t = \sigma(W_f \cdot [h_{t-1}, x_t] + b_f)
\]

\[
    i_t = \sigma(W_i \cdot [h_{t-1}, x_t] + b_i)
\]

\[
    o_t = \sigma(W_o \cdot [h_{t-1}, x_t] + b_o)
\]

\[
    c_t = f_t \cdot c_{t-1} + i_t \cdot \tanh(W_c \cdot [h_{t-1}, x_t] + b_c)
\]

\[
    h_t = o_t \cdot \tanh(c_t)
\]

\[
    \bar{y}_t = W_h h_t + b_h
\]

where \( f_t \), \( i_t \) and \( o_t \) are forget gate, input gate and output gate in LSTM structure respectively, and the weights attached to them are \( (W_f, b_f) \), \( (W_i, b_i) \) and \( (W_o, b_o) \). \( \sigma \) denotes the sigmoid function.

**Figure 2.** The architecture of long short-term memory (LSTM) network.
The prediction process of LSTM network can be abbreviated as: \( \tilde{y}_t = \text{LSTM}(x_t, \Theta) \), where \( \Theta \) denotes the trainable parameters. The training process of LSTM networks is equivalent to finding a set of training parameters to satisfy:

\[
\Theta_T = \arg \max_{\Theta} P(\tilde{y}_t | x_t, \Theta)
\]  

(4)

During the training process of LSTM network, the mean square error on training sets and validation sets are expressed as \( J_t \) and \( J_v \) separately. If \( J_t \) was greater than \( J_v \), and both \( J_t \) and \( J_v \) tend to be stable with increase of the number of iterations (epochs), the training processes are usually considered as well convergence. The mean square error can be calculated by Equation (5):

\[
J = \sum_i (y_i - \tilde{y}_i)^2
\]

(5)

2.2. Dual Thresholds

As mentioned earlier, for all of the training sets, validation sets and threshold sets are picked out from historical normal SHM data. The well-trained LSTM network will then perform good prediction ability with normal target sequences and poor prediction ability with abnormal target sequences, as shown in Figure 3. Therefore, the prediction error of well-trained LSTM network can reflect the anomalous possibility of target sequences, and the prediction error of each sampling point in target sequences can be calculated by Equation (6):

\[
E_i = |y_i - \tilde{y}_i|
\]

(6)

where \( E_i \), \( y_i \), and \( \tilde{y}_i \) are the prediction error, target value, and prediction value of sampling point \( i \).

![Figure 3. The prediction result of the LSTM network.](image)

In order to avoid the problem of high alarm rate caused by the traditional point by point comparison of prediction error and threshold, this paper proposes a dual thresholds strategy to detect abnormal monitoring data. In the two-threshold strategy, the length of the target sequence needs to be determined firstly, which can be set according to actual requirements. Secondly, the first threshold is determined and it is compared by the prediction error of each sampling point in target sequence. Thirdly, the second threshold is determined, and it is compared by the number of sampling points in target sequence that prediction error exceeds the first threshold. Finally, the target sequence can be considered normal when the number of sampling points in target sequence where the prediction error exceeds the first threshold is less than the second threshold. Otherwise, it is considered abnormal. The above identification process of normal target sequence can be expressed briefly by Equation (7):

\[
n(E_i > \lambda_T) < n_T
\]

(7)
where \( \lambda_T \) is the first threshold and \( n_T \) is the second threshold. \( n(E_i > \lambda_T) \) denotes the number of sampling points wherein the prediction error exceeds the first threshold.

The probability of the occurrence event is the largest among all possible events according to the maximum likelihood estimation, so this paper reversely solves the two thresholds by maximizing the threshold set without occurrence of anomalies (or minimizing the occurrence of anomalies in threshold set). The anomalous probability of threshold sets can be obtained via statistics analysis. For generalization performance of two thresholds, it is important to avoid using training sets and validation sets instead of threshold sets, and which is selected from historical normal SHM data. To facilitate the expression of the following formulas, the number and length of target sequences in threshold sets are recorded as \( N \) and \( L \), respectively.

First of all, all input sequences in threshold sets are fed into well-trained LSTM network, and the prediction error of all sampling points in each target sequences can be obtained. Then, the prediction errors of each target sequence are fitted by normal distribution, which is often used to simulate monitoring data. The parameters of normal distribution can be gained by utilizing maximum likelihood estimation (MLE) method. According to the probability distribution equation of normal distribution, the probability that the prediction error at sampling point \( i \) is larger than the first threshold can be expressed as:

\[
P_i(E_i > \lambda_T | (u, \Sigma)) = 2(1 - \Phi(\frac{\lambda_T - u}{\Sigma}))
\]

where \( P_i \) denotes the probability of anomaly occurring at sampling point \( i \), \( \Phi(\bullet) \) denotes the probability distribution equation of standard normal distribution. \( (u, \Sigma) \) denotes the two parameters of normal distribution. \( \lambda_T \) is the first threshold, and \( \lambda_T \in [0, E_{\text{max}}] \). \( E_{\text{max}} \) is the maximum prediction error in the threshold sets.

According to the probability of anomaly occurring at each sampling point, the anomalous probability of each target sequence can be obtained by utilizing binomial distribution analysis technique:

\[
P_S(n(E_i > \lambda_T) > n_T | (u, \Sigma), L) = \sum_{j=N_T+1}^{L} \frac{L!}{j!(L-j)!} p_i^j (1 - p_i)^{L-j}
\]

where \( P_S \) denotes the anomalous probability of each target sequence. \( n_T \) is the second threshold, and \( n_T \in [0, L] \).

According to the anomalous probability of each target sequence, the anomalous probability of threshold sets can be expressed as:

\[
P_T(n(n(E_i > \lambda_T) > n_T) > 1 | (u, \Sigma), L, N) = 1 - (1 - P_S)^N
\]

where \( P_T \) denotes the anomalous probability of threshold sets.

Unlike the first threshold, both the second threshold and the length of target sequences are determined according to actual requirements. Since the target sequences of threshold set are collected from normal historical normal SHM data, the value of the first threshold should minimize the anomalous probability of threshold sets for any given length of target sequences and the second threshold. In other words, the value of first threshold need to satisfy the following Equation (11):

\[
\lambda_T = \arg\min_{\lambda_T} P_T
\]

The values of the first threshold can be obtained from Equations (8)–(10):

\[
\lambda_T = E_{\text{max}}
\]
In order to minimize the anomalous probability of each target sequence in the threshold set, the second threshold can be obtained from Equation (12) for the first threshold determined:

\[ n_T = P_i(E_i > E_{\text{max}}) * L \]  

(13)

2.3. Anomaly Detection and Evaluation Criteria

After the two thresholds are determined, the abnormal data can be identified from current monitoring data. Firstly, the current monitoring data needs to be recombined into input sequences and target sequences according to network requirements. Then, the input sequences are fed into the predictive network and the prediction error of the target sequences is calculated. Finally, we can easily identify abnormal monitoring data by comparing prediction error of target sequences with dual thresholds.

In order to evaluate the performance of the proposed anomaly detection method, the concepts of anomaly rate (AR), anomaly detection rate (ADR), and anomaly detection accuracy (ADA) are introduced. Anomaly rate is the ratio of the abnormal target sequences number to the total of target sequences number. Anomaly detection rate is the rate of identified abnormal target sequences number to the total of target sequences number. Anomaly detection accuracy is the ratio of the identified abnormal target sequences number to the actual abnormal target sequences number. In addition, the concepts of classical precision (P), recall (R), and accuracy (A) are also introduced. The detection results of target sequences are only included normal and abnormal, which belongs to the two-classification problem. The abnormal sequences are set as positive, and the normal sequences are set as negative. TP means the number of abnormal sequences identified as positive, FP means the number abnormal sequences identified as negative, FN means the number of normal sequences identified as positive, and TN means the number normal sequences identified as negative. AR, ADR, P, R, and A can be calculated as follows:

\[
\text{AR} = \frac{\text{TP} + \text{FP}}{\text{TP} + \text{TN} + \text{FP} + \text{FN}} \\
\text{ADR} = \frac{\text{TP} + \text{FN}}{\text{TP} + \text{FP} + \text{FP} + \text{FN}} \\
\text{ADA} = \frac{\text{TP} + \text{FN}}{\text{TP} + \text{FP}} \\
\text{P} = \frac{\text{TP}}{\text{TP} + \text{FP}} \\
\text{R} = \frac{\text{TP}}{\text{TP} + \text{FN}} \\
\text{A} = \frac{\text{TP} + \text{TN}}{\text{TP} + \text{TN} + \text{FP} + \text{FN}}
\]

(14)

3. Case Study 1: Numerical Example

3.1. Structural Response Simulation and Data Preprocessing

To validate the effectiveness of the proposed method, a case study of finite element model simulation is firstly introduced. Compared with the SHM data of real structures, various types of anomalies can be easily added to finite element model response which will benefit for the accurate human labeled. A simply supported H-beam with length of 1.2 m is considered in this study. The cross-sectional area and inertial moment of the beam are 24.37 cm\(^2\) and 999.97 cm\(^4\), respectively. The 1/6 span, 2/6 span, 3/6 span, 4/6 span, and 5/6 span of the beam are simultaneously excited by white Gaussian noise. At the same time, the structure response of these excitation points is collected with 50 Hz sampling frequency, and five normal structural responses with 500,000 sampling points are obtained. In order to increase the difficulty of anomaly detection, noise with 20 signal-to-noise ratios (SNR) is added to these responses, and these noise-added responses are named as \(XA\), \(XB\), \(XC\), \(XD\), and \(XE\), respectively.
In order to better illustrate the effectiveness of the anomaly detection method proposed in this paper, the five simulated responses need to be split into training sets, validation sets, and test sets. Before the sets are established, five simulated responses are continuously intercepted into the input sequences by a time window of 270 sampling points with an interval of 250 sampling points. Taking response \( XA \) as an example, the number of input sequences is 1999. These input sequences are randomly assigned to four sets, and the number of input sequences in training sets, validation sets, threshold sets and test sets are 760, 39, 400, and 800 separately. The target sequence corresponding to each input sequence consists of the last 250 sampling points of input sequences.

In order to verify the universality of the proposed anomaly detection method, six kinds of abnormal patterns are designed for each test set, which are outlier (Type 2), minor (Type 3), missing (Type 4), trend (Type 5), drift (Type 6), and break (Type 7), respectively, as shown in Figure 4. The method of building abnormal input sequences and corresponding abnormal target sequence is to replace normal data with abnormal data. As a result of each test set, the abnormal pattern of input sequences 1–100 is type 2, 141–240 is type 3, 281–380 is type 4, 421–520 is type 5, 561–660 is type 6, 701–800 is type 7. The unchanged input sequences are labeled as normal (Type1).

![Figure 4. Six typical anomaly patterns of acceleration data.](image)

3.2. Network Training and Two Thresholds Determination

To determine the number of LSTM networks established, the correlation coefficients of abnormal input sequences in the five test sets are shown in Figure 5. Since the noise ratio of the response is 20%, the threshold for the correlation coefficient is set at 80%. According to the calculation results in Figure 5, five LSTM networks need to be established to predict the above five response data, and they are named Net1, Net2, Net3, Net4, and Net5.

During the training processes, the basic parameters of the five designed networks are set as follows: the input and output dimensions of the networks are 270 and 250, respectively, the batch size is 256, dropout is 0.3, and epoch is 20. The activation function of the fully connection layer is linear function, the loss function is the mean square error (MSE). These networks are trained using Adam optimizer. The mean square errors on training sets and validation sets of each network are shown in Figure 6. It can be seen that all of these networks converge gradually with increasing of iterations (epochs).
Table 3.3.

| Item | Threshold |
|------|-----------|
|      | Net1      | Net2     | Net3     | Net4     | Net5     |
| \( \lambda_s \) (m/s²) | 10.6       | 11.1     | 16.1     | 14.4     | 9.7      |

3.3. Results and Analysis

After the networks are trained and the two thresholds are determined, the anomaly data in the target sequences of test sets can be identified. Similarly, the prediction errors need to be averaged by a five-sampling-point sliding window with a stride of five sampling points to get the prediction errors. In order to increase the stability of the detection results, the prediction errors of each input sequence are averaged by a five-sampling-point sliding window with a stride of one sampling point. Then the first threshold can be calculated by Equation (15), and the results corresponding to Net1-Net5 are shown in Table 1. According to Equation (13), the value of second thresholds corresponding to Net1–Net5 are all calculated as one.

\[
\lambda_s = \max((E_i + E_{i+1} + E_{i+2} + E_{i+3} + E_{i+4})/5) \ i \in [1, 246]
\]

\[
\lambda_T = \max(\lambda_s) \ s \in [1, 400]
\]

Figure 5. The correlation coefficients between original signals.

Figure 6. The training processes of built networks.
point. The anomaly detection results are shown in Table 2. From Table 2, we can find that the detection results are essentially in agreement with the correlation coefficients in Figure 5. In other words, the number of trained LSTM networks must be equal to the number of channels for multi-channel data with weak correlation.

Table 2. Anomaly detection results of test sets.

| Responses | AR | ADR     |
|-----------|----|---------|
|           |    | Net1 | Net2 | Net3 | Net4 | Net5 |
| XA        | 38.75% | 39.38% | 40.63% | 39.75% | 39.13% | 39.00% |
| XB        | 98.75% | 98.75% | 40.88% | 99.00% | 39.13% | 98.88% |
| XC        | 98.38% | 98.38% | 98.13% | 98.25% | 38.75% | 98.88% |
| XD        | 38.75% | 38.63% | 39.75% | 39.00% | 38.75% | 38.63% |

In order to further illustrate the effectiveness of the proposed anomaly detection method in identifying various abnormal patterns, Table 3 shows the detection results of six abnormal patterns in each test set. From the Table 3, it can be seen that the proposed method can achieve good detection results for six abnormal patterns. Precision, recall, and accuracy are calculated to evaluate the overall performance of the proposed method in each test set, as shown in Figure 7, and the actual anomaly layout and the detection results are compared in Figure 8.

Table 3. Anomaly detection results of six types of abnormal patterns.

| Abnormal Patterns | AR (Type) | ADR (Type)     |
|-------------------|-----------|----------------|
|                   |           | Net1-XA | Net2-XB | Net3-XC | Net4-XD | Net5-XE |
| Type1             | 6.25%     | 6.38%  | 6.63%  | 6.38%  | 6.25%  | 6.25%  |
| Type2             | 6.00%     | 6.00%  | 6.25%  | 5.88%  | 5.63%  | 6.00%  |
| Type3             | 5.75%     | 5.63%  | 5.88%  | 6.50%  | 5.55%  | 5.88%  |
| Type4             | 8.00%     | 8.63%  | 9.13%  | 8.75%  | 8.38%  | 7.83%  |
| Type5             | 6.50%     | 6.50%  | 6.75%  | 7.25%  | 6.75%  | 6.88%  |
| Type6             | 6.25%     | 6.25%  | 6.25%  | 6.25%  | 6.25%  | 6.25%  |

Figure 7. The precise (P), recall (R) and accuracy (A) of the detection results.
4. Case Study 2: Experimental Example of a Long Span Suspension Bridge

4.1. Background

To further illustrate the extensive applicability of the proposed method, the acceleration data of a long-span suspension bridge located in Jiangyin, China is employed. According to historical official records, the Jiangyin Bridge was hit by a ship in 2 June 2005, and the impact location on the main girder of the bridge is shown in Figure 9. Figure 10 shows the typical response data of the accelerometers on the suspender, girder and main cable which are closest to the ship impact position, respectively. As can be seen from Figure 10, the acceleration data of the suspenders is most sensitive to ship impact accidents. Therefore, the accident of ship collision can be easily identified based on suspenders’ acceleration data. A total of 12 accelerometers are installed on the suspenders of Jiangyin Bridge, as shown in Figure 9.
4.2. Data Preprocessing

In this section, the suspender acceleration data from 1 June to 2 June 2005 is employed. The calculated correlation coefficients of 12 channels are shown in Figure 11, and the maximum correlation coefficient of different channels is 0.729. The threshold for the correlation coefficient should be determined according to the proportion of noise in the response data. Here, 80% is adopted as a rule of thumb. Therefore, it is necessary to train 12 different LSTM networks to correspondingly detect anomaly in 12 channels, and these networks are named as LSTM1~LSTM12, respectively. To create training sets, validation sets, threshold sets, and test sets, the acceleration data of 12 channels is continuously intercepted into the input sequences by a time window of 1050 sampling points with an interval of 1000 sampling points. The training sets, validation sets, and threshold sets were randomly selected from the normal input sequences on 1 June 2005. For each channel, the number of input sequences in training sets, validation sets, and threshold sets are 342, 18 and 36 respectively. All of the input sequences on 2 June 2005 are utilized as the test sets, and the number of input sequences is 4320. The target sequence corresponding to each input sequence consists of the last 1000 sampling points of input sequences.

4.3. Network Training and Dual Thresholds Determination

The Adam optimization strategy is adopted to train the 12 LSTM networks. The input and output dimensions of these networks are set to 1050 and 1000 separately, and other
parameters have the same setting with Section 3.2. The mean square errors on training sets and validation sets of networks are shown in Figure 12. It can be seen that the prediction errors on training sets is greater than the prediction errors on validation sets, and both of them tend to be stable with increasing of iterations (epochs), which means that the training results are pretty good.

Figure 12. The training and validation processes.

Similar to the case study of finite element model simulation in Section 3, the prediction error are firstly averaged by a five-time-point window. The first thresholds corresponding to LSTM1-LSTM12 can be obtained by Equation (15), as shown in Table 4. all of the second thresholds corresponding to LSTM1-LSTM12 are calculated as 1.

Table 4. The first threshold of LSTM1~LSTM12.

| Model   | $\lambda_T (10^{-3} \text{ m/s}^2)$ | Model   | $\lambda_T (10^{-3} \text{ m/s}^2)$ | Model   | $\lambda_T (10^{-3} \text{ m/s}^2)$ |
|---------|---------------------------------|---------|---------------------------------|---------|---------------------------------|
| LSTM 1  | 15.4                            | LSTM 5  | 18.2                            | LSTM 9  | 16.9                            |
| LSTM 2  | 19.8                            | LSTM 6  | 20.7                            | LSTM 10 | 52.4                            |
| LSTM 3  | 13.6                            | LSTM 7  | 13.3                            | LSTM 11 | 49.3                            |
| LSTM 4  | 16.2                            | LSTM 8  | 17.0                            | LSTM 12 | 46.7                            |

4.4. Result and Discussion

The human labeled results and networks detection results of 12 channels are compared in Figure 13. The ship collision accidents can be quickly located while the acceleration data of 12 channels are detected as anomaly at the same time point. The accuracy of detection results in each channel are given in Table 5, and it can be seen that the proposed method performs well in real bridge data processing and exception event warning.
In order to illustrate the advantages of the anomaly identification method in this paper in workload, the data set preparation method in this paper is compared with [31]. Firstly, this paper only needs to prepare normal dataset, while [31] prepares both normal and abnormal datasets. Secondly, each channel in this paper establishes a “small” network independently, so there is no need to pay attention to the balance of data between channels, while [31] needs to pay attention to this aspect. Finally, the data structure of each channel is relatively fixed, so only a few sample data are needed to learn the “small network”.

### Table 5. The ADA of 12 channels.

| Sensors | ADA (%) | Sensors | ADA (%) | Sensors | ADA (%) |
|---------|---------|---------|---------|---------|---------|
| Channel 1 | 99.5 | Channel 5 | 99.7 | Channel 9 | 99.9 |
| Channel 2 | 99.5 | Channel 6 | 99.9 | Channel 10 | 96.9 |
| Channel 3 | 99.2 | Channel 7 | 98.8 | Channel 11 | 97.7 |
| Channel 4 | 99.3 | Channel 8 | 99.0 | Channel 12 | 97.4 |

In order to better explain the mechanism of proposed method, an anomaly detection example for two target sequences in this case study is shown in Figure 14. The left ordinate is the value corresponding to the target sequences and the output sequences, and the right ordinate is the value corresponding to the prediction error and the first threshold. As can be seen from Figure 14, the prediction errors of more than 50 sampling points in both target sequences exceed the first threshold, so both target sequences are judged as anomalies. If a single threshold is used, both target sequences will alarm for more than 50 times, which is obviously unreasonable.

![Figure 13. The detection results of SHM data (-A symbolizes the results with human labeled, -D symbolizes the detected results).](image-url)

![Figure 14. An example of anomaly detection with proposed method.](image-url)
Figure 14. An example of anomaly detection with proposed method.

5. Conclusions

The main contribution of this paper is to propose an anomaly detection method based on LSTM network. First, a small amount of historical normal data is used to train the network. Then, the prediction error of the well-trained network can be utilized to detect the anomaly. The feasibility of the method has been verified by two case studies of finite element simulation and real suspension bridge SHM data successively. Compared with other anomaly detection methods, the major and novel contributions here are as follows:

- An anomaly detection method based on LSTM network is proposed, which not only achieve the requirement of real-time identification, but also reduces the workload of preparing training sets.
- The correlation coefficient is used to determine the number of networks that need to be established. The problem of performance differences of networks in different channels caused by unbalanced dataset can be avoided by establishing the “small” concept for each channel.
- A double thresholds method was proposed to avoid the problem of high alarm rate in the past.
- The anomaly detection method is applied to the acceleration data of Jiangyin Bridge, and the ship collision accident of Jiangyin Bridge is successfully detected, which proves the application potential of this method in the structural warning system.

Despite the aforementioned advantages of the proposed method, this paper only considers the time-domain data itself. In the next step, structural parameters such as frequency, mass, and stiffness will be introduced as input of network to improve the detection effect of the anomaly.

In addition, the anomaly of SHM data are either caused by abrupt change of structure performance and external load or by the faults of sensors themselves. The former can reflect the structural characteristics and needs to be accurately captured. The latter has no practical significance and needs to be repaired. Therefore, the question concerning how to effectively distinguish the two types of anomalies will be the focus of future work.

Author Contributions: Investigation, J.Z. (Jianliang Zhang); Supervision, J.Z. (Jian Zhang) and Z.W. All authors have read and agreed to the published version of the manuscript.

Funding: The research presented was financially supported by the Key R&D Program of Jiangsu (No. BE2020094) and National Key R&D Program of China (No. 2020YFC1511900).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.
Acknowledgments: This research is supported by Southeast University.

Conflicts of Interest: The authors declare no conflict of interest.

References
1. Inman, D.J. Damage prognosis for aerospace, civil and mechanical systems. Damage Progn. Aerosp. Civ. Mech. Syst. 2005, 6531, 714–724.
2. Farrar, C.R.; Czarnecki, J.J.; Sohn, H.; Hemez, F.M. A review of structural health monitoring literature 1996–2001. In Proceedings of the Third World Conference on Structural Control, Como, Italy, 7–12 April 2002.
3. Li, S.; Li, H.; Liu, Y.; Lan, C.; Zhou, W.; Ou, J. SMC structural health monitoring benchmark problem using monitored data from an actual cable-stayed bridge. Struct. Control Health Monit. 2013, 21, 156–172. [CrossRef]
4. Wu, Z.S.; Zhang, J.; Noori, M. Fiber-Optic Sensors for Infrastructure Health Monitoring, Volume I: Introduction and Fundamental Concepts, 1st ed.; Momentum Press: Boulder, CO, USA, 2019.
5. Tian, Y.D.; Zhang, C.; Jiang, S.; Zhang, J.; Duan, W.H. Noncontact cable force estimation with unmanned aerial vehicle and computer vision. Comput.-Aided Civ. Infrastruct. Eng. 2021, 36, 73–88. [CrossRef]
6. Jiang, S.; Zhang, J. Real-time crack assessment using deep neural networks with wall-climbing unmanned aerial system. Comput.-Aided Civ. Infrastruct. Eng. 2020, 35, 549–564. [CrossRef]
7. Xia, Q.; Cheng, Y.Y.; Zhang, J.; Zhu, F.Q. In-service condition assessment of a long-span suspension bridge using temperature-induced strain data. J. Bridge Eng. 2016, 22, 04016124. [CrossRef]
8. Zhang, J.; Tian, Y.D.; Yang, C.Q.; Wu, B.T.; Wu, Z.S.; Wu, G.; Zhang, X.; Zhou, L.M. Vibration and deformation monitoring of a long-span rigid-frame bridge with distributed long-gauge sensors. J. Aerosp. Eng. 2017, 30, B4016014. [CrossRef]
9. Zhang, J.; Guo, S.L.; Zhang, Q.Q. Mobile impact testing for structural flexibility identification with only a single reference. Comput.-Aided Civ. Infrastruct. Eng. 2015, 30, 703–714. [CrossRef]
10. Zhang, J.; Wan, C.; Sato, T. Advanced markov chain monte carlo approach for finite element calibration under uncertainty. Comput.-Aided Civ. Infrastruct. Eng. 2013, 28, 522–530. [CrossRef]
11. Keogh, E.; Lin, J.; Lee, S.H.; Herle, H.V. Finding the most unusual time series subsequence: Algorithms and applications. Knowl. Inf. Syst. 2007, 11, 1–27. [CrossRef]
12. Ma, J.; Ma, J.; Perkins, S.; Perkins, S. Time-series novelty detection using one-class support vector machines. In Proceedings of the International Joint Conference on Neural Networks, Portland, OR, USA, 20–24 July 2003.
13. Markus, G.; Seiichi, U. A comparative evaluation of unsupervised anomaly detection algorithms for multivariate data. PLoS ONE 2016, 11, e0152173.
14. Chen, J.; Wang, L.; Hu, Q. Machine learning-based anomaly detection of ganglia monitoring data in HEP Data Center. EPJ Web Conf. 2020, 245, 07081. [CrossRef]
15. Tian, Z.; Wang, Y.; Ti, Z. Anomaly detection of target dynamics based on clustering. In Proceedings of the—2018 15th International Symposium on Pervasive Systems, Algorithms and Networks, I-SPAN 2018, Yichang, China, 16–18 October 2018; Institute of Electrical and Electronics Engineers Inc.: New York, NY, USA, 2019; pp. 287–291.
16. Wang, W.; Liu, J.; Pitsilis, G.; Zhang, X. Abstracting massive data for lightweight intrusion detection in computer networks. Inf. Sci. 2018, 433–434, 417–430. [CrossRef]
17. Arul, M.; Kareem, A. Data Anomaly Detection for Structural Health Monitoring of Bridges using Shapelet Transform. Smart Struct. Syst. 2022, 29, 93–103.
18. Kramer, M.A. Autoassociative neural networks. Comput. Chem. Eng. 1992, 16, 313–328. [CrossRef]
19. Tamilselvan, P.; Wang, P. Failure diagnosis using deep belief learning based health state classification. Reliab. Eng. Syst. Saf. 2013, 115, 124–135. [CrossRef]
20. Abdeljaber, O.; Avcı, O.; Kiranyaz, S.; Gabbouj, M.; Inman, D.J. Real-time vibration-based structural damage detection using one-dimensional convolutional neural networks. J. Sound Vib. 2017, 388, 154–170. [CrossRef]
21. Cha, Y.J.; Choi, W.; Buyukozturk, O. Deep learning-based crack damage detection using convolutional neural networks. Comput.-Aided Civ. Infrastruct. Eng. 2017, 32, 361–378. [CrossRef]
22. Zhang, A.; Wang, K.C.; Fei, Y.; Liu, Y.; Chen, C.; Yang, G.; Li, J.Q.; Yang, E.; Qiu, S. Automated pixel-level pavement crack detection on 3d asphalt surfaces with a recurrent neural network. Comput.-Aided Civ. Infrastruct. Eng. 2018, 34, 213–229. [CrossRef]
23. Brownjohn, J.; Au, S.; Zhu, Y.; Sun, Z.; Li, B.; Bassitt, J.; Hudson, E.; Sun, H. Bayesian operational modal analysis of jiangyin yangtze river bridge. Mech. Syst. Signal Process. 2018, 110, 210–230. [CrossRef]
24. Xiang, X.Z.; Lv, N.; Guo, X.L.; Wang, S.; Abdulmotaleb, E.S. Engineering vehicles detection based on modified faster R-CNN for power grid surveillance. Sensors 2018, 18, 2258. [CrossRef]
25. Grzegorz, P. Multi-sensor data integration using deep learning for characterization of defects in steel elements. Sensors 2018, 18, 292.
26. Cortez, B.; Carrera, B.; Kim, Y.J.; Jung, J.Y. An architecture for emergency event prediction using lstm recurrent neural networks. Expert Syst. Appl. 2017, 97, 315–324. [CrossRef]
27. Tang, P.J.; Wang, H.L.; Sam, K. Deep sequential fusion lstm network for image description. Neurocomputing 2018, 312, 154–164. [CrossRef]
28. Rao, G.Z.; Huang, W.H.; Feng, Z.X.; Cong, Q. Lstm with sentence representations for document-level sentiment classification. *Neurocomputing* **2018**, *308*, 49–57. [CrossRef]
29. Kambayashi, Y.; Winiwarter, W.; Arikawa, M. Outlier detection using replicator neural networks. In *International Conference on Data Warehousing and Knowledge Discovery*; Springer: Berlin/Heidelberg, Germany, 2002; pp. 170–180.
30. Kim, C.; Lee, J.; Kim, R.; Park, Y.; Kang, J. DeepNAP: Deep neural anomaly pre-detection in a semiconductor fab. *Inf. Sci.* **2018**, *457–458*, 1–11. [CrossRef]
31. Filonov, P.; Lavrentyev, A.; Vorontsov, A. Multivariate industrial time series with cyber-attack simulation: Fault detection using an LSTM-based predictive data model. *arXiv* 2016, arXiv:1612.06676.
32. Tuor, A.; Kaplan, S.; Hutchinson, B.; Nichols, N.; Robinson, S. Deep learning for unsupervised insider threat detection in structured cybersecurity data streams. *arXiv* 2017, arXiv:1710.00811.
33. Bao, Y.; Tang, Z.; Li, H.; Zhang, Y. Computer vision and deep learning–based data anomaly detection method for structural health monitoring. *Struct. Health Monit.* **2018**, *18*, 401–421. [CrossRef]
34. Ni, F.T.; Zhang, J.; Noori, M.N. Deep learning for data anomaly detection and data compression of a long-span suspension bridge. *Comput. Civ. Infrastruct. Eng.* **2020**, *35*, 685–700. [CrossRef]
35. Nanduri, A.; Sherry, L. Anomaly detection in aircraft data using Recurrent Neural Networks (RNN). In *Proceedings of the 2016 Integrated Communications Navigation and Surveillance (ICNS)*, Herndon, VA, USA, 19–21 April 2016.
36. Siegelmann, H.T.; Sontag, E.D. On the computational power of neural nets. *J. Comput. Syst. Sci.* **1995**, *50*, 132–150. [CrossRef]
37. Bengio, Y. Learning long-term dependencies with gradient descent is difficult. *IEEE Trans. Neural Netw.* **1994**, *5*, 157–166. [CrossRef] [PubMed]
38. Hochreiter, S.; Schmidhuber, J. Long short-term memory. *Neural Comput.* **1997**, *9*, 1735–1780. [CrossRef] [PubMed]