Image Processing-based Data Integrity Attack Detection in Dynamic Line Rating Forecasting Applications

Arash Moradzadeh
Faculty of Electrical and Computer Engineering,
University of Tabriz,
Tabriz, Iran
arash.moradzadeh@tabrizu.ac.ir

Hamed Moayyed
GECAD–Research Group on Intelligent Engineering and Computing for Advanced Innovation and Development,
Polytechnic of Porto,
Porto, Portugal
hmoayyed@fe.up.pt

Behnam Mohammadi-Ivatloo
Faculty of Electrical and Computer Engineering,
University of Tabriz,
Tabriz, Iran
bmohammadi@tabrizu.ac.ir

Amjad Anvari-Moghaddam
Department of Energy (AAU Energy),
Aalborg University,
Aalborg, Denmark
aam@energy.aau.dk

Zita Vale
GECAD–Research Group on Intelligent Engineering and Computing for Advanced Innovation and Development,
Polytechnic of Porto,
Porto, Portugal
zav@isep.ipp.pt

Reza Ghorbani
Renewable Energy Design Laboratory (REDLab), Department of Mechanical Engineering
University of Hawaii at Manoa,
Honolulu, HI 96822 USA
rezag@hawaii.edu

***Abstract*— Dynamic line rating (DLR) is considered a key concept in transmission lines that can guarantee the variable nature of renewable energy sources with minimal economic constraints. So far, various schemes have been selected for DLR forecasting that offers acceptable capacity but require measuring instruments and communication networks with precise calibration on the conductor surface, which in addition to high economic costs, are always available for cyber attackers. In this study, to forecast the DLR values, a deep learning-based technique called long short-term memory (LSTM) is proposed. Additionally, a novel data integrity attack detection approach based on image processing is developed to maintain the performance of the forecasting model against cyber-attacks. The LSTM forecasts the DLR values of an overhead transmission line located in Tabriz, Iran, using meteorological parameters as input data. The forecasting results confirm the high performance of the LSTM model with minimal error values. Then, a scaling attack is applied as a known data integrity attack on the input variables of wind speed and wind direction to evaluate the performance of the LSTM network against cyber-attacks. The results of this scenario show that a cyber-attack can significantly reduce the accuracy of the forecasting. To prevent this, the image processing-based technique detects and clearly displays the cyber-attacks in each of the input variables by converting the input data parameters to 2-D images.**

Keywords—Dynamic line rating, forecasting, long short-term memory, image processing, data integrity attack

I. Introduction

The modern power system has significantly witnessed the synergy of renewable energy sources (RES) with transmission and distribution systems. Given recent studies, it reaches 60% of total power generation worldwide by 2050 [1], [2]. Easy access and use of these resources require basic infrastructure in line with the transmission of generated energy by RES with minimal restrictions [3].

Dynamic line rating (DLR) is a key concept in transmission lines that ensures the variable nature of RES without high investment costs and minimal constraints. The DLR has various application aspects, which are discussed in [4], [5] of its technologies for integrating wind turbines in power systems. In the conventional structure, overhead transmission lines operate in a range less than the predetermined rate, i.e., static line rate (SLR) [6], [7]. However, the thermal capacity of overhead transmission lines, according to IEEE 738 and CIGRE standards, is highly affected by environmental and climatic conditions such as wind speed, wind direction, global radiation, temperature, and so on. Therefore, due to the dependence of overhead line capacity on environmental conditions, DLR is able to forecast the thermal capacity of overhead transmission lines in real-time [6]. Online monitoring and real-time forecasting of overhead line's capacity significantly contribute to the integration of RES, especially wind turbines, with the power system with higher reliability and stability, yet at a lower cost. Due to the fact that the DLR mainly depends on environmental and weather conditions, the amount of DLR related to each transmission line can be forecasted based on the available weather conditions and using observed data in meteorological stations available in the region [7], [8].

So far, various studies have proposed different techniques for DLR forecasting. In [9], the DLR forecasting has been performed based on the ampacity probabilistic forecasting. This study forecasts the DLR values by avoiding the network operators' risk in high-risk situations. The DLR forecasting in [10] has been done using a variety of regression models, including multivariate polynomial regression, an hourly normalization, and an autoregressive integrated moving average. Estimation of DLR values for transmission lines has been performed using meteorological data combined with computational fluid dynamics of wind simulation in [11]. DLR forecasting considering the cyber-security of input data has been done in [5] by developing a hybrid scheme based on deep learning applications. In [12], machine learning techniques have been suggested for 27 hours ahead of DLR forecasting related to two transmission lines studied in Northern Ireland. In [13], the application of DLR expansion technology in non-thermally limited long lines has been evaluated by considering the correlation between effective variables such as temperature, conductor resistance and voltage drop in the overhead transmission lines. The results of that study show an increase of 17% and 12% for 69 kV and 138 kV lines, respectively, without the need to upgrade the substation equipment. In [14], four various machine learning procedures forecast the day-ahead DLR by considering meteorological data as input variables. A novel model based on dynamic stochastic general equilibrium has been developed in [15] to forecast DLR. The proposed model is based on stochastic volatility and is utilized for real-time forecasting. In [16], DLR forecasting in real-time has been done using 110 kV transmission line data and techniques based on a live simulation model and a systematic deviation correction approach based on the Tabu search algorithm. Quantitative regression and super-density regression methods have been proposed in [17] for very short-term risk-averse stochastic DLR forecasting. In [18], modeling uncertainties related to meteorological variables and presenting an accurate trend of DLR forecasting related to overhead transmission lines have been performed via the fuzzy theory. Stability evaluation of transmission lines equipped with a DLR technology has been developed in [19] based on a Markov model. In [20], decision tree-based learning models such as AdaBoost, Gradient Boosting (GBoosting), XGBoost, CatBoost, and Light Gradient Boosted Machine have been applied to forecast the DLR values associated with two overhead transmission lines in Iran.

A review of the literature shows the background of the DLR forecasting process, so it can be seen that various techniques have been devoted to forecasting DLR with different accuracies and applications. However, each of the utilized methods suffers from problems that reduce the accuracy of the forecasted results. As mentioned in the literature, the DLR values have a high correlation with meteorological variables. Time-series model is also one of the most important features of meteorological data used in DLR forecasting that has not been modeled in any of the solutions employed in the reviewed studies. In addition, modern power/energy systems have a significantly high volume of data, and cyber-security and the prevention of cyber-attacks are among the most important issues that must be considered today in a diversity of applications associated with power systems. However, this problem has not been addressed in any of the reviewed studies and the performance of the suggested technique against cyber-attacks has not been evaluated.

The rest of this paper is organized as follows: Section II introduces the developed methodologies. Cyber-attack modeling is represented in Section III. The results of DLR forecasting and data integrity attack detection are presented in different scenarios in Section IV. Section V presents the conclusion of the paper.

II. Methodologies

In this paper, the prediction of DLR values in transmission lines is done based on one of the well-known and robust deep learning applications named LSTM. Then, during a separate scenario, the cyber-attack injects into the input parameters to evaluate the performance of the LSTM network against false data. Finally, the data visualization procedure is proposed to diagnosis cyber-attacks in each of the input variables. In the continuation of this section, each of the LSTM and data visualization techniques is introduced in detail.

A. *Long short-term memory (LSTM)*

LSTM is a useful recurrent neural network (RNN) structure of deep learning applications that was first suggested in 1997 [21]. This algorithm was able to dramatically compensate for RNN limitations such as the vanishing gradients issues via allowing gradients to pass unaltered. In addition, time-series modeling, forecasting, categorization, and modeling of linear and nonlinear relationships are other applications of the LSTM [22]. Typically, most conventional machine learning and deep learning procedures are not able to model and extract features from time-series data during the training stage. While, the LSTM can retain information about previous states and receive acceptable training in the face of high-dimensional data that requires prior state knowledge. Each LSTM unit consists of four main variables called internal memory, forget gate (f_t), input gate (i_t), and output gate (o_t). The first gate in this architecture is the forget gate, which determines the amount of data kept from the latest c_{t-1} status. The mathematical formulations of the LSTM architecture is described as follows [23], [24]:

$$f_t = \sigma(W_{lf} l_t + W_{mf} m_{t-1} + b_f) \tag{1}$$

$$i_t = \sigma(W_{li} l_t + W_{mi} m_{t-1} + b_i) \tag{2}$$

$$o_t = \sigma(W_{lo} l_t + W_{mo} m_{t-1} + b_o) \tag{3}$$

$$a_t = tanh(W_{la} l_t + W_{ma} m_{t-1} + b_a) \tag{4}$$

$$c_t = c_{t-1} \phi f_t + i_t \phi a_t \tag{5}$$

$$m_t = o_t \phi \tanh c_t \tag{6}$$

where σ demonstrates the logistic sigmoid function, c_t and a_t denote the memory cell and the hidden vector, respectively. $W_{l*} = \{W_{lf}, W_{li}, W_{la}, W_{lo}\}$ and $W_{m*} = \{W_{mf}, W_{mi}, W_{ma}, W_{mo}\}$ represent the trainable weights corresponding to the respective gates. b_f, b_i, b_o, and b_a shows the output biases. Operator ϕ shows the Hadamard product. Table I shows the parameters set for the LSTM model in this paper.

B. *Data visualization*

Data visualization is based on visual information and uses it to present a fast and efficient method of sharing information globally. The aim of data visualization is to simplify data so that the human brain can easily understand and reason it. However, to achieve this goal, it needs to be transformed into a visual context, like an image. So, when the data becomes manageable, patterns, trends, and even unusual values can be easily spotted in the massive data. As mentioned earlier, this is the most important goal of data simplification. Sensitivity to visual processing is higher in the human brain than in any

TABLE I. THE LSTM MODEL PARAMETERS

Layer (type)	Output Shape
Directional	22
Dropout_1 (Dropout)	0.3
Flatten_1 (Flatten)	22
Dense_1 (Dense)	14
Output (Dense)	16

other sense, and in the act of understanding, visual processing is considered to have "broadband" availability. In practice, what is obtained with these tools must be easily understood by all people, and only in this way are these computational tools useful. In the real world, however, we have a wide range of massive data, and this goal is rarely achieved. Representative methods are not able to establish a basic and effective correlation of the qualitative information contained in these data. Therefore, the visualization approach could play an important role in data analysis in various applications.

Modern power systems generate a huge amount of information and require power system engineers and operators to analyze this information in detail. In power systems with thousands of buses, the main challenge is to present the generated data in such a way that operators can intuitively and quickly assess the state of the system. This is especially true when analyzing the relationships between power flows on the grid and the capacity of the transmission system. This need becomes even more acute when a single entity, such as an independent operator, operates a much larger system. To generate a lot of information, there are various computing processors in power systems that utilize different complex algorithms consisting of considerable data in the case of control to operate. In control centers, the data is extracted from the devices used in a power system. Then the analysis process of these outputs is done by the operators. After this analysis, the relevant results are obtained and on the basis of these results, appropriate actions are taken while the time is limited.

A visualization approach, such as physically grasping these internal representations, is very likely to make significant progress in understanding. So far, few studies in the field of power and energy systems have applied the data visualization approach [25], [26]. However, this must be achieved in different applications. To this end, the authors recently introduced a novel visualization approach that easily detects the location of short circuit faults in power transformer windings [27]. The results presented in this study emphasize the effectiveness of the data visualization approach. In the present work, we have implemented this procedure in detecting cyber-attacks on DLR parameters. In the following, this visualization technique is explained in detail.

III. Cyber-attack modeling

Data integrity attack is based on the destruction of measured values and mainly targets the measured data in the system in order to make the performance of the system difficult by changing the relevant parameters. This type of attack can easily be implemented in all parts of the power and energy systems that have sensors and measuring equipment [5]. In this paper, a false data injection attack is modeled and applied as a known example of a data integrity attack on meteorological data, which are the input variables of DLR measurements.

Scaling attack is one of the most common forms of false data injection attack modeling that has been applied to wind speed and wind direction parameters in this paper. Decreasing and increasing the actual measurements of the data during the attack based on the tuned scaling parameters, is the basis of this type of attack [28]. In this study, modeling the scaling attack is performed by decreasing and increasing the wind speed and wind direction values by 5%, so that the average data is maintained. The mathematical modeling of a scaling attack is as follows [29]:

$$\bar{Q}_t = (1+\lambda_S) \times Q_t \quad for\ t_s < t < t_e \tag{7}$$

where Q_t is the main dataset, $\bar{Q}_t$ shows the manipulated dataset under the scaling attack, λ_S denote the attack parameters, t_s represent the start time of the scaling attack, and finally, t_e indicates the end time of the attack.

IV. DLR forecasting and data integrity attack detection results

In this study, the results are presented in two different scenarios including DLR forecasting and data integrity attack detection. Each of these scenarios is described as follows:

A. First scenario: DLR forecasting

In this study, forecasting of DLR is done by employing the well-known LSTM technique. The overhead transmission line located in Tabriz, Iran has been selected as the case study [5]. Thus, the meteorological data associated with this region, which are observed by the meteorological station, are considered as the input dataset. The transmission line understudy has specifications such as 8 spans, length of 40.50 km, a diameter of 31.5 mm, and maximum heat capacity of 75 ° C. The meteorological data used also include wind speed, wind direction, temperature, humidity, and solar radiation at 40 m altitude for the years of 02/11/2011 to 01/07/2012 with a sampling resolution of 10 minutes. The LSTM network training is performed by 75% of the desired data and network testing is performed by the remaining 25% of the data. After completion the training and test process, the network performance for each stage is analyzed by different performance evaluation indicators such as correlation coefficient (R^2), mean square error (MSE), root mean square error (RMSE), and mean absolute percentage error (MAPE). Each of these indicators analyses the results in a specific way. Thus, the maximum values of R^2 and the minimum values of error indices express the best state of the forecasting model. The mathematical calculation for each of these metrics is denoted in [22].

The designed network is trained using the provided data and in this process, the training results of the LSTM network are presented in Table II. The results show that the network was able to model the behavioral pattern of the input data in an acceptable way to forecast the corresponding DLR values. After evaluating the results of the training process and saved the designed network, the test data is considered as network input to perform the test phase. This process is based on the patterns identified from the input data so that the saved network can forecast the DLR values of the test input data. Fig. 1 provides a general comparison of the actual DLR values and forecasted DLR values by the LSTM in the test phase. The results presented in Fig. 1 clearly show that the LSTM can to forecast the DLR values with less difference than the actual values. The correlation between the actual and forecasted DLR values is seen in this figure. In addition, since the input parameters did not have any preprocessing technique, so can emphasize the high performance of the LSTM in forecasting DLR values. Introduced performance evaluation indicators can be used to more accurately evaluate the forecasting results. Table III examines the results of the LSTM test phase based on performance evaluation indicators.

TABLE II. Evaluating the LSTM network results in the training phase

R^2 **(%)**	**MSE**	**RMSE**	**MAPE**
99.39	4.6841	2.1643	8.2578

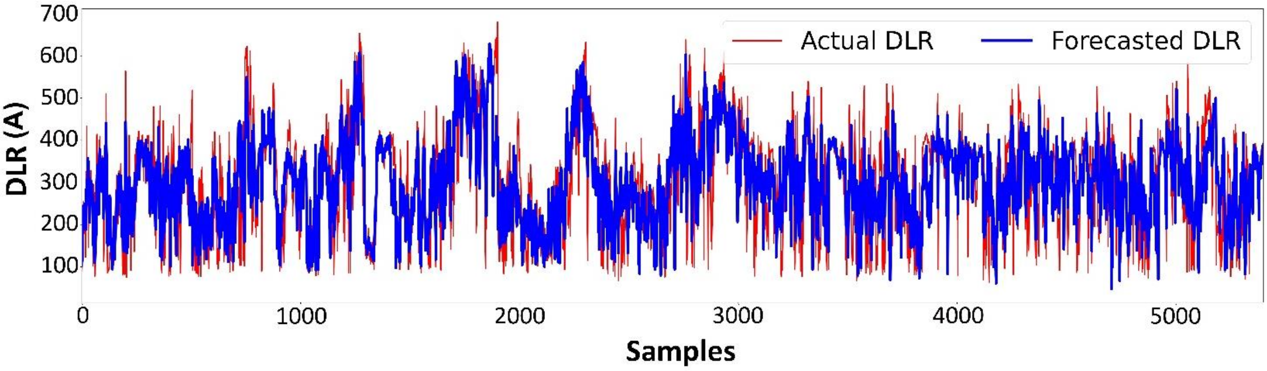


Fig. 1. Comparison of actual DLR values and forecasted DLR values at the LSTM test stage

TABLE III. EVALUATING THE LSTM NETWORK RESULTS IN THE TEST PHASE

R^2 (%)	MSE	RMSE	MAPE
99.11	187.21	13.68	24.19

The results presented in Table III also show that the network can forecast the DLR parameters with acceptable accuracy. Each of the evaluation metrics is computed based on the relationship between the real measurements and the forecasted DLR parameters and evaluates the performance of forecasting model. However, knowing the minimum and maximum error intervals in the forecast parameters can provide a better overview of the forecast process and the performance of the network in the test phase. Fig. 2 provides the error histogram for the LSTM network in the test phase. The results presented in this figure show that the minimum and maximum error prediction intervals of the LSTM network are in the worst case between -62 and 78. Excluding the difference between the actual and forecasted DLR values from this error interval, indicates disturbances and a decrease in the correlation between the input variables. As such, this condition mainly occurs in cyber-attacks such as false data injection attack. Accordingly, to evaluate the performance of the proposed model against cyber-attacks, it is necessary to use false data to test the LSTM network. The next scenario addresses this issue by applying a scaling attack on the input variables and proposes a data integrity attack detection approach based on image processing.

B. *Second scenario: Image processing-based data integrity attack detection*

TABLE IV. PERFORMANCE EVALUATION OF THE LSTM NETWORK IN DLR FORECASTING BY FALSE DATA

Attack description	R^2 (%)	MSE	RMSE	MAPE
Decrease 5 % wind speed	96.61	347	18.62	41.24
Increase 5 % wind speed	96.23	298	17.26	37.41
Decrease 5 % wind direction	21.52	8362	91.44	100.2
Increase 5 % wind direction	94.74	675	25.98	79.62

In this scenario, the scaling attack, as described in Section 3, is applied separately to the input variables (test data) of wind speed and wind direction. Then, the DLR forecasting is performed using false data as LSTM input variables. Table IV presents the results of DLR forecasts using false data. The results presented in Table IV show that the implemented cyber-attack on the input data was able to break the correlation between the input variables. Thus, at this stage of forecasting, the accuracy of the model compared to the clean state of the data has been greatly reduced and the error values of forecasting have been increased. Like the first scenario, Fig. 3 shows the distribution of the forecasting error associated with this scenario in the form of an error histogram.

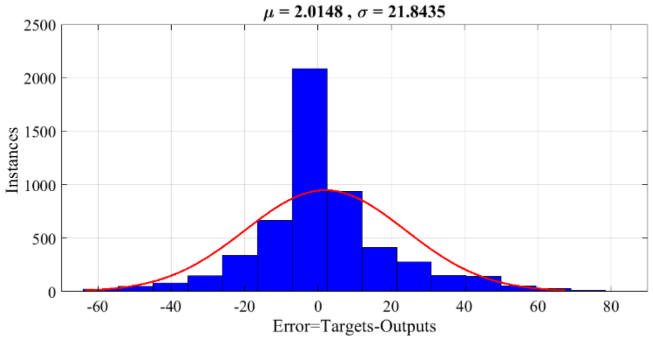


Fig. 2. Distribution of the LSTM network errors in the test process in the form of error histogram

As shown in Fig. 3, at this point, the forecasted DLR error values are out of the range specified in the original model test process. This trend indicates that input variables are involved in the problems that reduce the correlation between them. In this paper, this correlation was damaged by a data integrity attack. As mentioned in the literature, the main purpose of this scenario was to provide a data integrity attack detection approach based on image processing. Thus, the proposed technique accurately identifies the cyber-attack applied to the input variable and clearly displays the changes resulting from the attack compared to the clean state of the input variables. The basis of the proposed image processing technique is the conversion of input parameters into 2-D images. So, in the first step, the parameters related to the clean state are converted from the variables of wind speed and wind direction to 2-D images. Then, 2-D images corresponding to the attacked parameters are generated. Finally, the discrepancy between the healthy and false state images clearly indicates an attack on the input data. Fig. 4 shows 2-D images of clean states related to the test data of wind speed and wind direction.

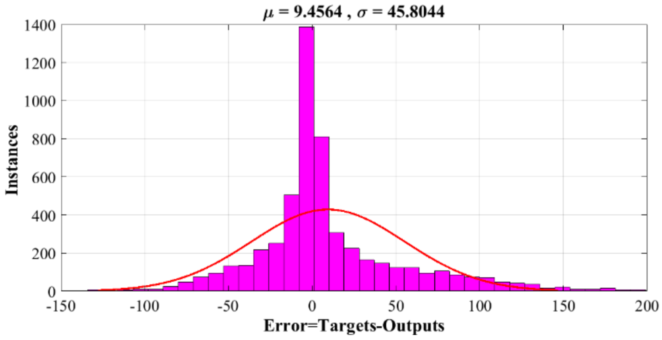
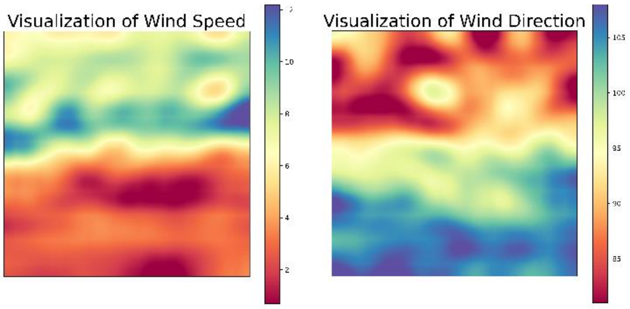


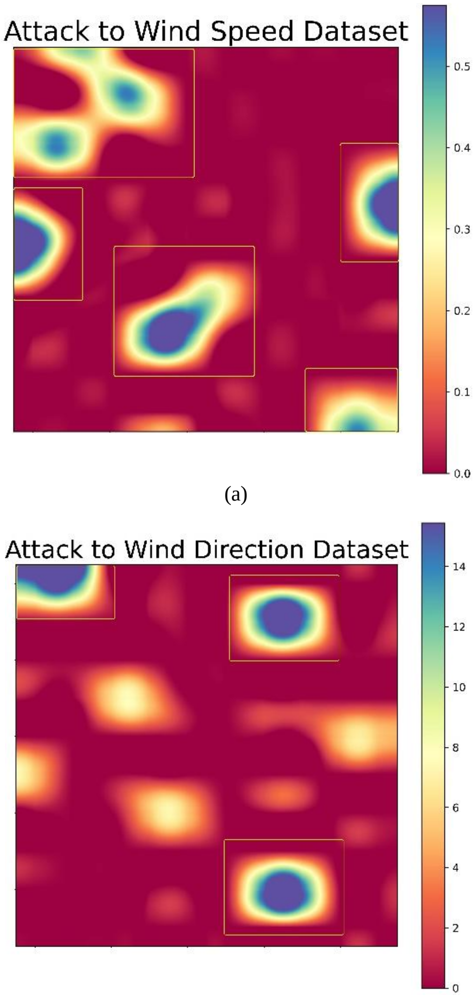
Fig. 3. Distribution of the LSTM network errors in the test process by false data in the form of error histogram



(a) (b)

Fig. 4. 2-D images of test data in the clean state; (a) wind speed, (b) wind direction

As can be seen in Fig. 4, the parameters related to each of the variables of wind speed and wind direction have been converted into 2-D color images, and the color variation in these shapes is due to the variation in the data parameters. Images of false test data are now generated to clearly see the difference in parameters caused by the cyber-attack. Fig. 5 shows the cyber-attacks detected in the test data. The results presented in Fig. 5, show that the proposed image processing technique was able to detect and clearly display the designed cyber-attack by plotting the difference between the parameters of the healthy state and the false state related to the input data. In each of the figures related to the variables of wind speed and wind direction, changes due to cyber-attack on the parameters are clearly observed.



(a)

(b)

Fig. 5. Detection of cyber-scaling attack in parameters related to test data; (a) wind speed, (b) wind direction

V. Conclusion

Ensuring the nature of the RES variable with minimal economic constraints has clarified the concept of DLR and increased its forecasting importance. However, cyber-attacks can be considered a major threat to the security of the data used and the results of the forecasting. In this paper, in order to forecast the DLR values in overhead transmission lines, a deep learning-based DLR forecasting procedure named LSTM and a cyber-attack detection scheme based on image processing were developed. The LSTM technique was trained using climatic variables observed by meteorological stations installed in the city of Tabriz in Iran to forecast the DLR parameters of an overhead transmission line in this region. The results of the predictions related to the training and test processes of the LSTM network were analyzed using different performance evaluation indices, and the presented results emphasized the high capability of the developed LSTM technique. However, the performance of the forecasting model against cyber-attacks was analyzed. To do this, the scaling cyber-attack was applied as a data integrity attack to the input variables of wind speed and wind direction. Then, false data were used as input to the forecasting model. The forecasting results had low accuracy and high error, which showed a lower correlation between input variables. Due to the high volume of data and maintaining the average parameters in the modeled cyber-attack, detecting the designed attack required an intelligent technique. The proposed image processing technique, with a high ability to convert numerical parameters to 2-D images with high color resolution, was able to display any changes in parameters with certain color schemes and was therefore used to detect data integrity attack in this paper. In the first step of the detection process, the parameters related to the clean state of the input data were converted to 2-D images. It then detects the cyber-attack applied to each input variable by forming 2-D images of the false data and finding the difference between them and the clean data. Finally, the presented results were emphasized the high performance of the developed image processing method in data integrity attack detection.

References

[1] "IRENA (2018), Global Energy Transformation: A roadmap to 2050, International Renewable Energy Agency, Abu Dhabi." .

[2] O. Sadeghian *et al.*, "A comprehensive review on energy saving options and saving potential in low voltage electricity distribution networks: Building and public lighting," *Sustainable Cities and Society*, vol. 72, p. 103064, Sep. 2021, doi: 10.1016/j.scs.2021.103064.

[3] H. Teimourzadeh, A. Moradzadeh, M. Shoaran, B. Mohammadi-Ivatloo, and R. Razzaghi, "High Impedance Single-Phase Faults Diagnosis in Transmission Lines via Deep Reinforcement Learning of Transfer Functions," *IEEE Access*, vol. 9, pp. 15796–15809, 2021, doi: 10.1109/ACCESS.2021.3051411.

[4] S. Madadi, B. Mohammadi-Ivatloo, and S. Tohidi, "Dynamic Line Rating Forecasting Based on Integrated Factorized Ornstein-Uhlenbeck Processes," *IEEE Transactions on Power Delivery*, vol. 35, no. 2, pp. 851–860, Apr. 2020, doi: 10.1109/TPWRD.2019.2929694.

[5] A. Moradzadeh, M. Mohammadpourfard, I. Genc, Ş. S. Şeker, and B. Mohammadi-Ivatloo, "Deep learning-based cyber resilient dynamic line rating forecasting," *International Journal of Electrical Power & Energy Systems*, vol. 142, p. 108257, Nov.

2022, doi: 10.1016/j.ijepes.2022.108257.

[6] W. B2.43, *Guide for thermal rating calculations of overhead lines*, no. December. Cigré, 2014.

[7] D. A. Douglass *et al.*, "A Review of Dynamic Thermal Line Rating Methods With Forecasting," *IEEE Transactions on Power Delivery*, vol. 34, no. 6, pp. 2100–2109, Dec. 2019, doi: 10.1109/TPWRD.2019.2932054.

[8] A. Mansour Saatloo, A. Moradzadeh, H. Moayyed, M. Mohammadpourfard, and B. Mohammadi-Ivatloo, "Hierarchical Extreme Learning Machine Enabled Dynamic Line Rating Forecasting," *IEEE Systems Journal*, pp. 1–11, 2021, doi: 10.1109/JSYST.2021.3128213.

[9] R. Dupin, A. Michiorri, and G. Kariniotakis, "Optimal Dynamic Line Rating Forecasts Selection Based on Ampacity Probabilistic Forecasting and Network Operators' Risk Aversion," *IEEE Transactions on Power Systems*, vol. 34, no. 4, pp. 2836–2848, 2019, doi: 10.1109/TPWRS.2018.2889973.

[10] J. Zhan, C. Y. Chung, and E. Demeter, "Time Series Modeling for Dynamic Thermal Rating of Overhead Lines," *IEEE Transactions on Power Systems*, vol. 32, no. 3, pp. 2172–2182, May 2017, doi: 10.1109/TPWRS.2016.2596285.

[11] A. W. Abboud, J. P. Gentle, T. R. McJunkin, and J. P. Lehmer, "Using Computational Fluid Dynamics of Wind Simulations Coupled With Weather Data to Calculate Dynamic Line Ratings," *IEEE Transactions on Power Delivery*, vol. 35, no. 2, pp. 745–753, Apr. 2020, doi: 10.1109/TPWRD.2019.2925520.

[12] J. L. Aznarte and N. Siebert, "Dynamic Line Rating Using Numerical Weather Predictions and Machine Learning: A Case Study," *IEEE Transactions on Power Delivery*, vol. 32, no. 1, pp. 335–343, Feb. 2017, doi: 10.1109/TPWRD.2016.2543818.

[13] L. Dawson and A. M. Knight, "Applicability of Dynamic Thermal Line Rating for Long Lines," *IEEE Transactions on Power Delivery*, vol. 33, no. 2, pp. 719–727, Apr. 2018, doi: 10.1109/TPWRD.2017.2691671.

[14] R. Dupin, G. Kariniotakis, and A. Michiorri, "Overhead lines Dynamic Line rating based on probabilistic day-ahead forecasting and risk assessment," *International Journal of Electrical Power & Energy Systems*, vol. 110, pp. 565–578, Sep. 2019, doi: 10.1016/j.ijepes.2019.03.043.

[15] S. Madadi, B. Mohammadi-Ivatloo, and S. Tohidi, "Probabilistic Real-Time Dynamic Line Rating Forecasting Based on Dynamic Stochastic General Equilibrium With Stochastic Volatility," *IEEE Transactions on Power Delivery*, vol. 36, no. 3, pp. 1631–1639, Jun. 2021, doi: 10.1109/TPWRD.2020.3012205.

[16] Y. Cheng, P. Liu, Z. Zhang, and Y. Dai, "Real-Time Dynamic Line Rating of Transmission Lines Using Live Simulation Model and Tabu Search," *IEEE Transactions on Power Delivery*, vol. 36, no. 3, pp. 1785–1794, Jun. 2021, doi: 10.1109/TPWRD.2020.3014911.

[17] A. Kirilenko, M. Esmaili, and C. Y. Chung, "Risk-Averse Stochastic Dynamic Line Rating Models," *IEEE Transactions on Power Systems*, vol. 36, no. 4, pp. 3070–3079, Jul. 2021, doi: 10.1109/TPWRS.2020.3045589.

[18] H. Shaker, M. Fotuhi-Firuzabad, and F. Aminifar, "Fuzzy dynamic thermal rating of transmission lines," *IEEE Transactions on Power Delivery*, vol. 27, no. 4, pp. 1885–1892, Oct. 2012, doi: 10.1109/TPWRD.2012.2193672.

[19] H. Shaker, H. Zareipour, and M. Fotuhi-Firuzabad, "Reliability Modeling of Dynamic Thermal Rating," *IEEE Transactions on Power Delivery*, vol. 28, no. 3, pp. 1600–1609, Jul. 2013, doi: 10.1109/TPWRD.2013.2252204.

[20] A. Ahmadi, M. Nabipour, B. Mohammadi-Ivatloo, and V. Vahidinasab, "Ensemble Learning-based Dynamic Line Rating Forecasting under Cyberattacks," *IEEE Transactions on Power Delivery*, pp. 1–1, 2021, doi: 10.1109/TPWRD.2021.3056055.

[21] S. Hochreiter and J. Schmidhuber, "Long Short-Term Memory," *Neural Computation*, vol. 9, no. 8, pp. 1735–1780, Nov. 1997, doi: 10.1162/neco.1997.9.8.1735.

[22] A. Moradzadeh, S. Zakeri, M. Shoaran, B. Mohammadi-Ivatloo, and F. Mohammadi, "Short-term load forecasting of microgrid via hybrid support vector regression and long short-term memory algorithms," *Sustainability (Switzerland)*, vol. 12, no. 17, p. 7076, Aug. 2020, doi: 10.3390/su12177076.

[23] A. Moradzadeh, B. Mohammadi-ivatloo, K. Pourhossein, and A. Anvari-Moghaddam, "Data Mining Applications to Fault Diagnosis in Power Electronic Systems: A Systematic Review," *IEEE Transactions on Power Electronics*, vol. 37, no. 5, pp. 1–1, May 2021, doi: 10.1109/tpel.2021.3131293.

[24] A. Moradzadeh, H. Moayyed, K. Zare, and B. Mohammadi-Ivatloo, "Short-term electricity demand forecasting via variational autoencoders and batch training-based bidirectional long short-term memory," *Sustainable Energy Technologies and Assessments*, vol. 52, p. 102209, Aug. 2022, doi: 10.1016/j.seta.2022.102209.

[25] P. Cuffe and A. Keane, "Visualizing the Electrical Structure of Power Systems," *IEEE Systems Journal*, vol. 11, no. 3, pp. 1810–1821, Sep. 2017, doi: 10.1109/JSYST.2015.2427994.

[26] V. Miranda, P. A. Cardoso, R. J. Bessa, and I. Decker, "Through the looking glass: Seeing events in power systems dynamics," *International Journal of Electrical Power and Energy Systems*, vol. 106, pp. 411–419, Mar. 2019, doi: 10.1016/j.ijepes.2018.10.024.

[27] A. Moradzadeh, H. Moayyed, B. Mohammadi-Ivatloo, G. B. Gharehpetian, and A. P. Aguiar, "Turn-to-Turn Short Circuit Fault Localization in Transformer Winding via Image Processing and Deep Learning Method," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 7, pp. 4417–4426, Jul. 2021, doi: 10.1109/TII.2021.3105932.

[28] M. Cui, J. Wang, and M. Yue, "Machine Learning-Based Anomaly Detection for Load Forecasting Under Cyberattacks," *IEEE Transactions on Smart Grid*, vol. 10, no. 5, pp. 5724–5734, Sep. 2019, doi: 10.1109/tsg.2018.2890809.

[29] S. Sridhar and M. Govindarasu, "Model-based attack detection and mitigation for automatic generation control," *IEEE Transactions on Smart Grid*, vol. 5, no. 2, pp. 580–591, Mar. 2014, doi: 10.1109/TSG.2014.2298195.