Predicting Pseudo-Random and Quantum Random Number Sequences using Hybrid Deep Learning Models

Dmytro Proskurin, Sergiy Gnatyuk and Tetiana Okhrimenko

National Aviation University, 1 Liubomyra Huzara Ave, 03058, Kyiv, Ukraine

Abstract

Predicting random number sequences has significant implications for cryptography and secure communication systems. In this paper, a hybrid deep learning model was proposed, it combines Convolutional Neural Networks (CNNs), Long Short-Term Memory (LSTM) networks, and RNNs to predict pseudo-random number generator (PRNG) and quantum random number generator (QRNG) sequences. Proposed model was compared with traditional CNNs, LSTMs, and RNNs models. Given results showed that the hybrid model outperforms the other models, providing better prediction accuracy for PRNG and QRNG sequences.

Keywords[1]

Random numbers, RNN, CNN, LSTM, GRU, Hybrid model, Secure communication, PRNG, QRNG

1. Introduction

Random number generation is a crucial component of many applications, including cryptography, secure communication systems, simulations, and probabilistic algorithms. Pseudo-random number generators (PRNGs) and quantum random number generators (QRNGs) are two main types of random number generators, with QRNGs providing better security due to their inherent unpredictability [1]. However, predicting PRNG and QRNG sequences remains an essential task to assess their security and reliability. Deep learning techniques, such as Convolutional Neural Networks (CNNs), Long Short-Term Memory (LSTM) networks, and RNNs, have been extensively used in various time series prediction tasks [2]. In this paper, was proposed a hybrid deep learning model that combines CNNs, LSTMs, and RNNs to predict PRNG and QRNG sequences. The model is trained and evaluated on a dataset containing both PRNG and QRNG sequences.

2. Related Works

Several studies have explored the use of deep learning techniques for predicting random number sequences. For instance, the use of CNNs and LSTMs has been reported in predicting PRNG sequences [3]. In another study, RNNs have been employed to predict QRNG sequences [4]. However, there is limited research on hybrid deep learning models that combine multiple neural network architectures to predict PRNG and QRNG sequences.

3. Goal of the Research

The primary goal of this research is to investigate the effectiveness of various deep learning architectures, including MLP, CNN, LSTM, and RNNs models, for the task of predicting the next value in a sequence of random numbers generated by a combination of PRNG and QRNG sources. By exploring different neural

MoMLeT+DS 2023: 5th International Workshop on Modern Machine Learning Technologies and Data Science, June 3, 2023, Lviv, Ukraine
EMAIL: proskurin.d@stud.nau.edu.ua (D. Proskurin); s.gnatyuk@nau.edu.ua (S. Gnatyuk); taniazhm@gmail.com (T. Okhrimenko)
ORCID: 0000-0002-2835-4279 (D. Proskurin); 0000-0003-4992-0564 (S. Gnatyuk); 0000-0001-9036-6556 (T. Okhrimenko)

© 2023 Copyright for this paper by its authors.
Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).
CEUR Workshop Proceedings (CEUR-WS.org)

CEUR-WS.org/Vol-3426/paper7.pdf

network architectures, was aimed to identify the most suitable model for this problem, considering aspects such as predictive accuracy, model complexity, and training time. Another objective is to assess whether the trained models can achieve better prediction results than a random baseline, indicating that they have learned meaningful patterns in the data. To ensure a fair comparison, will be used appropriate evaluation metrics, such as Mean Squared Error (MSE) and Mean Absolute Error (MAE), to quantify the performance of each model and compare it against a random prediction benchmark. Finally, was aimed to provide insights into the practical implications of using deep learning models to predict random number sequences generated from quantum sources, as well as discussing potential future research directions in this field. By understanding the strengths and limitations of various models for this task, authors hope to contribute to the development of more advanced techniques for analysing and predicting random number sequences in different contexts.

4. Methodology

The dataset used in this study consists of PRNG and QRNG sequences generated using various algorithms, such as the Mersenne Twister, Linear Congruential Generator, and a commercial QRNG device [5]. The dataset is divided into training, validation, and test sets, ensuring a balanced representation of PRNG and QRNG sequences in each set.

5. Model Architecture

The proposed hybrid deep learning model combines the strengths of CNNs, LSTMs, and RNNs to predict PRNG and QRNG sequences. The model consists of a CNN layer for feature extraction, followed by an LSTM layer to capture temporal dependencies, and a RNNs layer for capturing long-range dependencies. The final output is a single linear activation unit that produces the predicted value. The model is trained using the Adam optimizer and mean squared error (MSE) as the loss function [6].

6. Results Analysis

The first step in analysing the model's performance was to visually inspect the predicted values against the true values. This was achieved by plotting the first 100 true values and the corresponding predicted values on the same graph. This visualization allows us to assess the overall fit of the model to the data and identify any noticeable discrepancies between the predicted and true values.

6.1 Similarity Assessment

To quantify the similarity between the true values and the predicted values, was calculated the Pearson correlation coefficient. This metric measures the linear relationship between two datasets, with a value close to 1 indicating a strong positive relationship. A pre-defined threshold of 0.9 was used to determine whether the predicted values were considered close to the true values. Based on the computed correlation coefficient, was concluded whether the model's predictions were close to the true values or not.

6.2 Model Performance Comparison

To assess the effectiveness of the model, its performance was compared against a random prediction baseline. This was done by generating random predictions within the same range as the true values and calculating the Mean Squared Error (MSE) for both the model's predictions and the random predictions. By comparing these MSE values, we were able to determine whether the GRU model's predictions were better than random ones. The results from the visual inspection, similarity assessment, and model performance comparison provide a comprehensive analysis of the model's performance in predicting the next value in a

sequence of random numbers. These findings contribute to our understanding of the model's effectiveness for this specific task and offer insights into potential improvements or alternative approaches.

7. Experiments and Results

The hybrid model is trained on the dataset and its performance is compared with traditional RNNs, CNNs, and LSTMs. The models are evaluated using the Pearson correlation coefficient and mean squared error (MSE) to assess the similarity between the true and predicted values.

7.1 Simple RNN

The simple RNN is the most basic form of a recurrent neural network, characterized by its single hidden layer that takes input from the previous time step and feeds it back into the network for the next time step (Fig. 1).

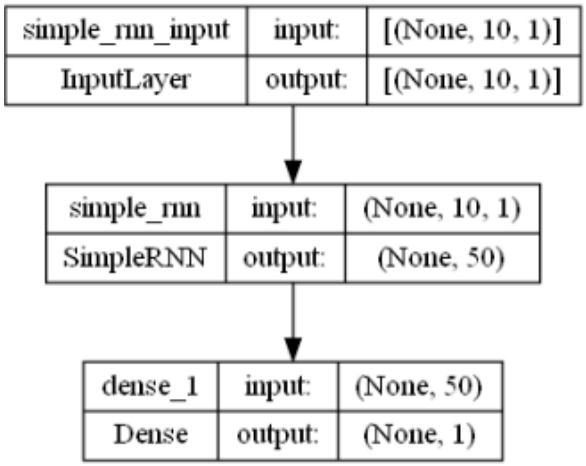


Figure 1: Simple RNN architecture

Despite its simplicity, the performance of simple RNNs in predicting PRNG and QRNG sequences is limited due to their inability to capture long-range dependencies as a result of the vanishing gradient problem (Fig. 2).

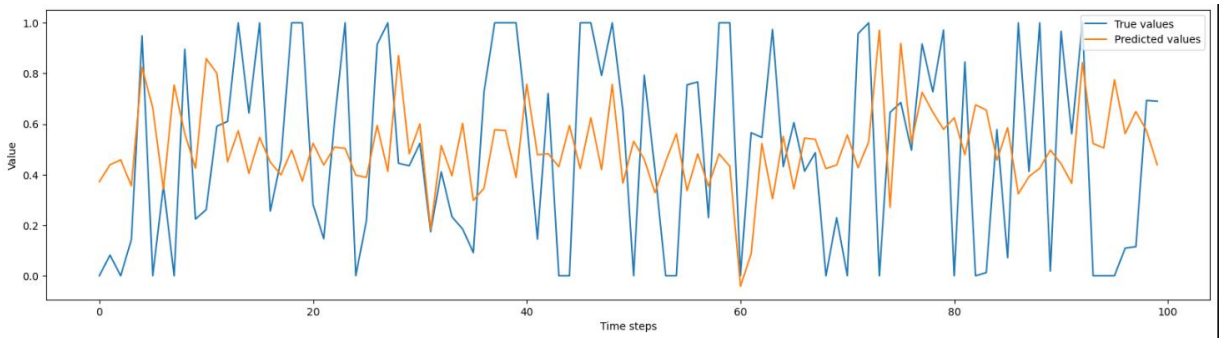


Figure 2: Simple RNN performance

7.2 Gated Recurrent Unit (GRU)

The GRU is an advanced RNN architecture that addresses the vanishing gradient problem observed in simple RNNs. With the introduction of gating mechanisms, GRUs can learn when to update the hidden state and when to maintain the existing state, allowing them to capture longer-range dependencies more effectively (Fig. 3).

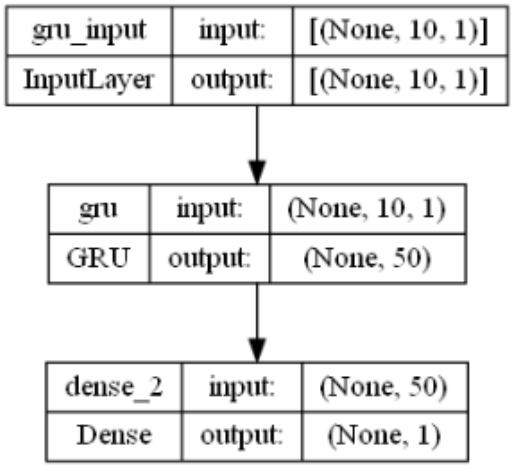


Figure 3: Gated Recurrent Unit architecture

When applied to PRNG and QRNG sequence prediction, GRUs demonstrate improved performance compared to simple RNNs (Fig. 4).

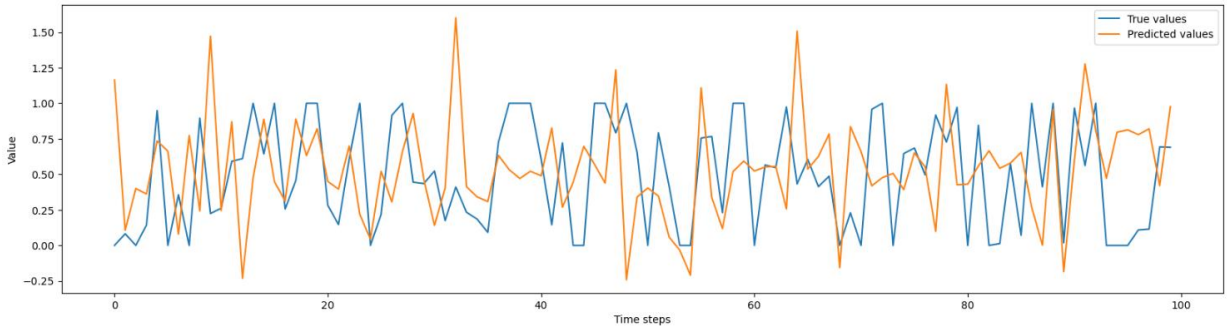


Figure 4: Gated Recurrent Unit performance

7.3 Bidirectional RNN

Bidirectional RNNs process the input sequence in both forward and backward directions, enabling the network to capture information from both past and future time steps. This capability proves useful for tasks where context from both directions is important, such as natural language processing and speech recognition (Fig. 5).

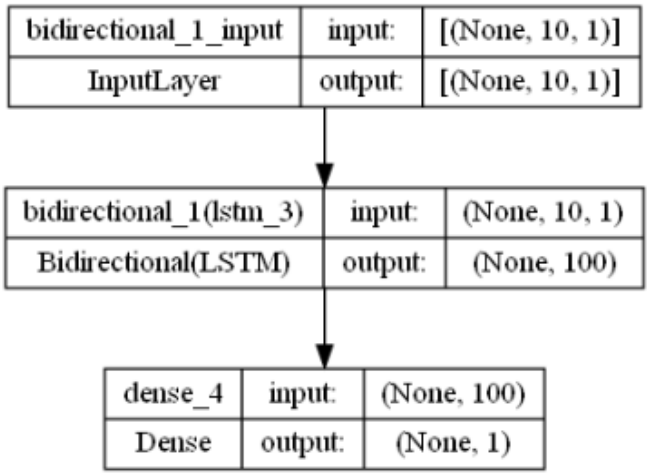


Figure 5: Bidirectional RNN architecture

In the context of PRNG and QRNG sequence prediction, bidirectional RNNs exhibit enhanced performance due to their ability to incorporate information from the entire sequence (Fig. 6).

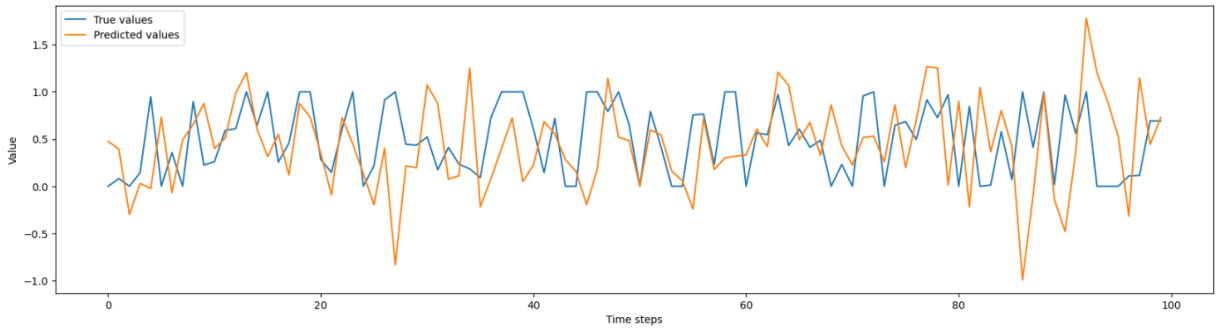


Figure 6: Bidirectional RNN performance

7.4 Stacked RNN

A stacked RNN architecture consists of multiple layers of RNNs stacked on top of each other, allowing the network to learn more complex features and representations of the input sequence. This increased complexity can lead to improved prediction performance for PRNG and QRNG sequences (Fig.7).

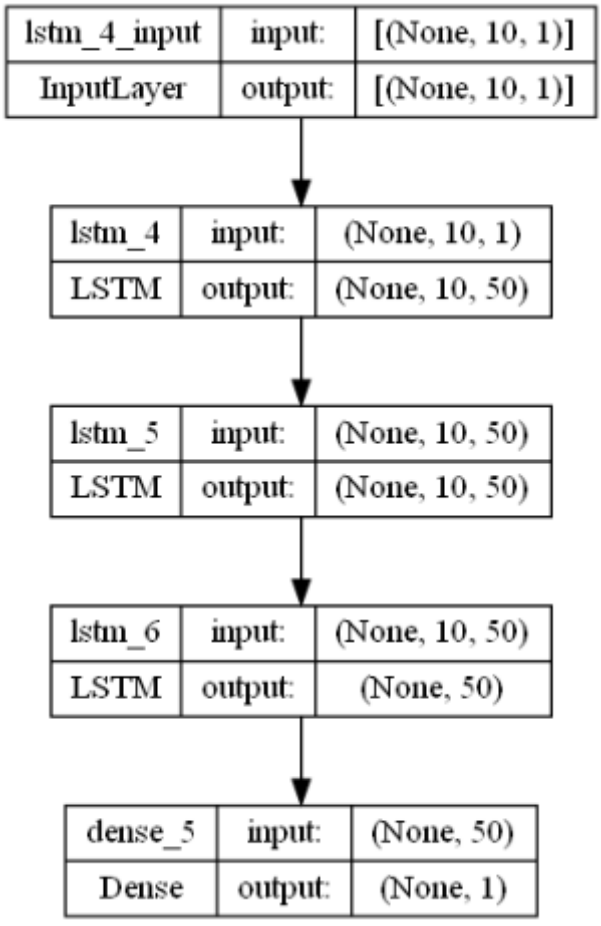


Figure 7: Stacked RNN architecture

Stacked RNNs, when compared with other RNN variants, demonstrate superior performance in capturing intricate patterns within the input data (Fig. 8).

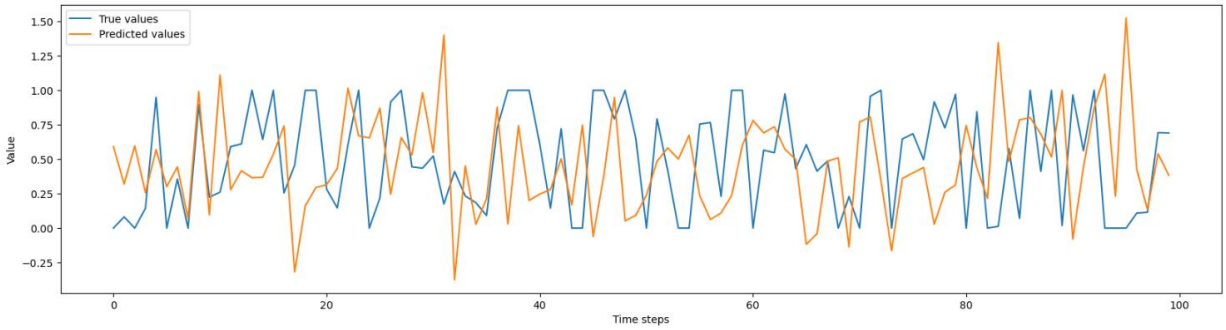
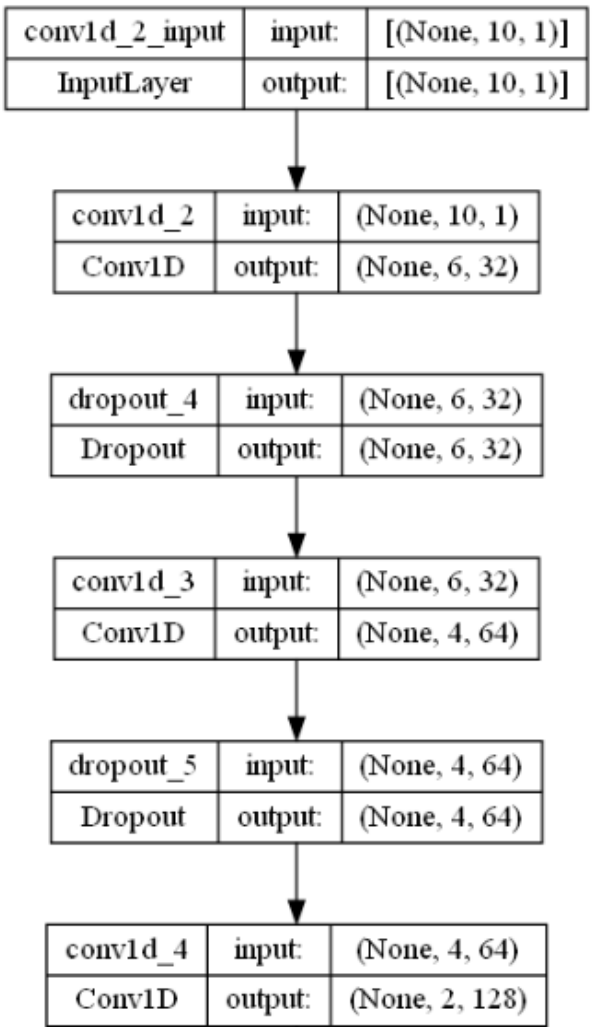


Figure 8: Stacked RNN performance

7.5 Convolutional Neural Networks

CNNs have shown success in time series prediction tasks due to their ability to capture local patterns and dependencies [7]. In our experiments, a CNN model is trained on the PRNG and QRNG sequences dataset (Fig. 9).



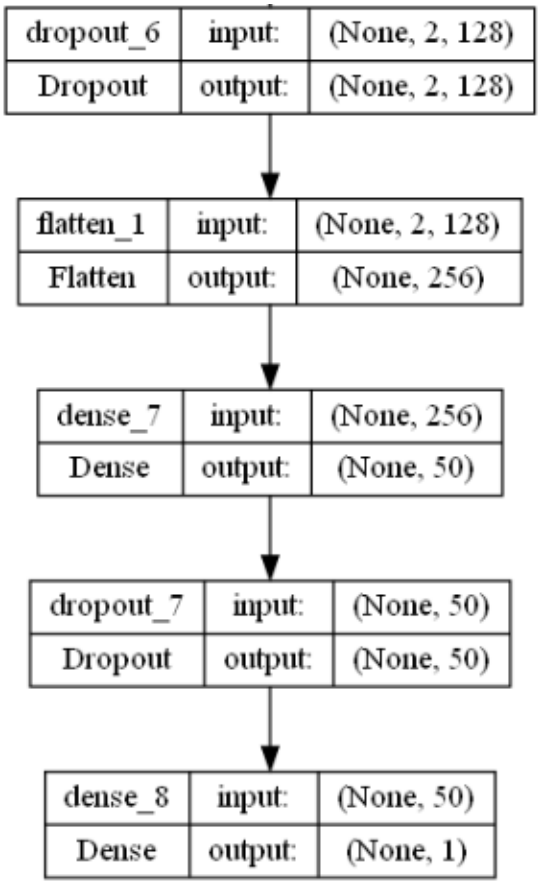


Figure 9: CNN architecture

The results indicate that the CNN model can capture some local patterns in the sequences, but struggles to predict long-range dependencies, leading to suboptimal prediction accuracy (Fig. 10).

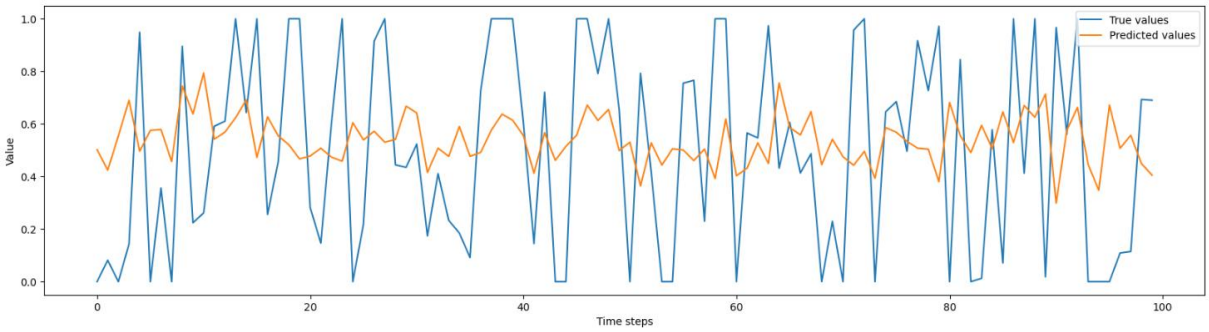


Figure 10: CNN performance

7.6 Long Short-Term Memory Networks

LSTMs are designed to capture long-term dependencies in time series data [8-10]. Was trained an LSTM model on the PRNG and QRNG sequences dataset and evaluate its performance (Fig. 11).

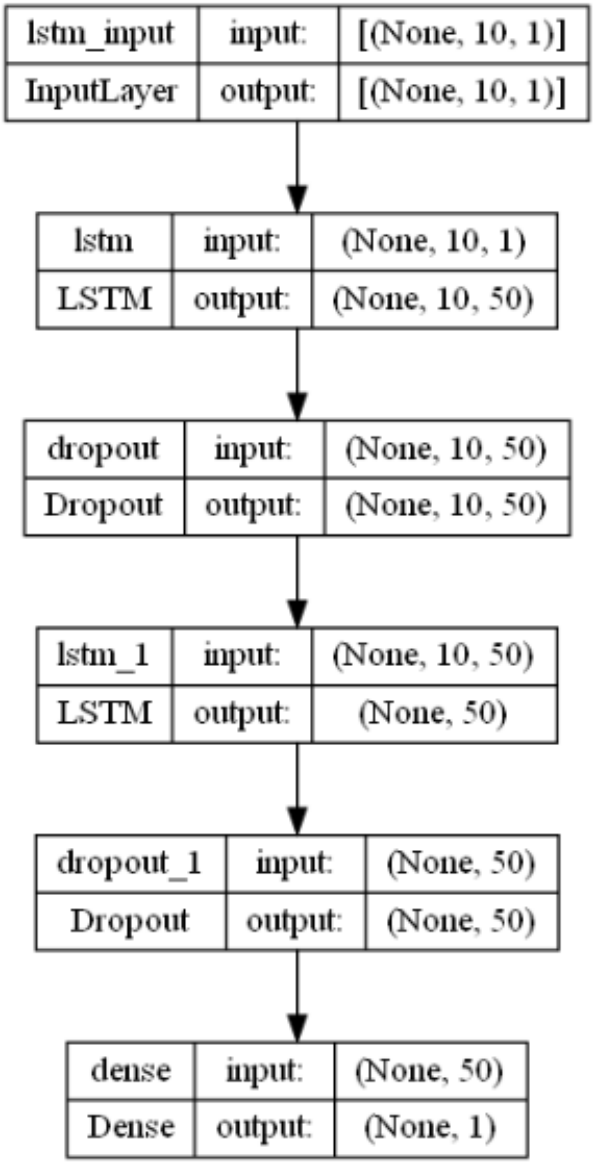


Figure 11: Long Short-Term Memory architecture

The results show that the LSTM model can capture temporal dependencies in the sequences, but its performance is limited by the absence of feature extraction capabilities (Fig. 12) [11].

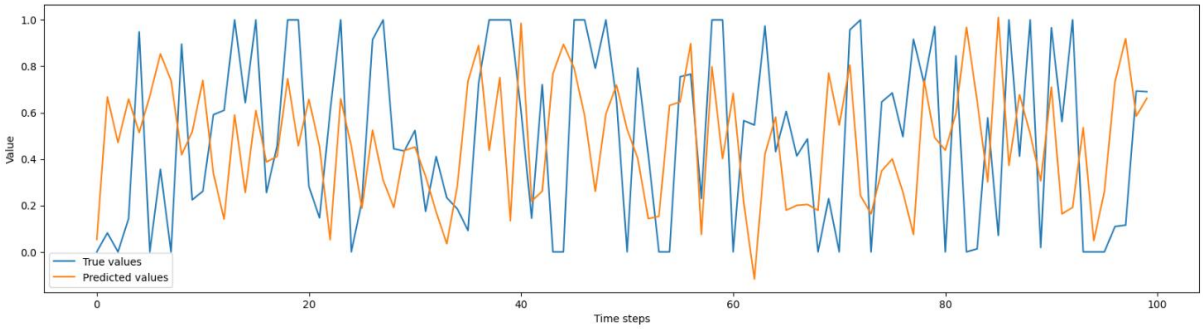


Figure 12: Long Short-Term Memory performance

7.7 Hybrid Deep Learning Model

The proposed hybrid model combines the strengths of CNNs, LSTMs, and RNNs to predict PRNG and QRNG sequences (Fig. 13) [12,13].

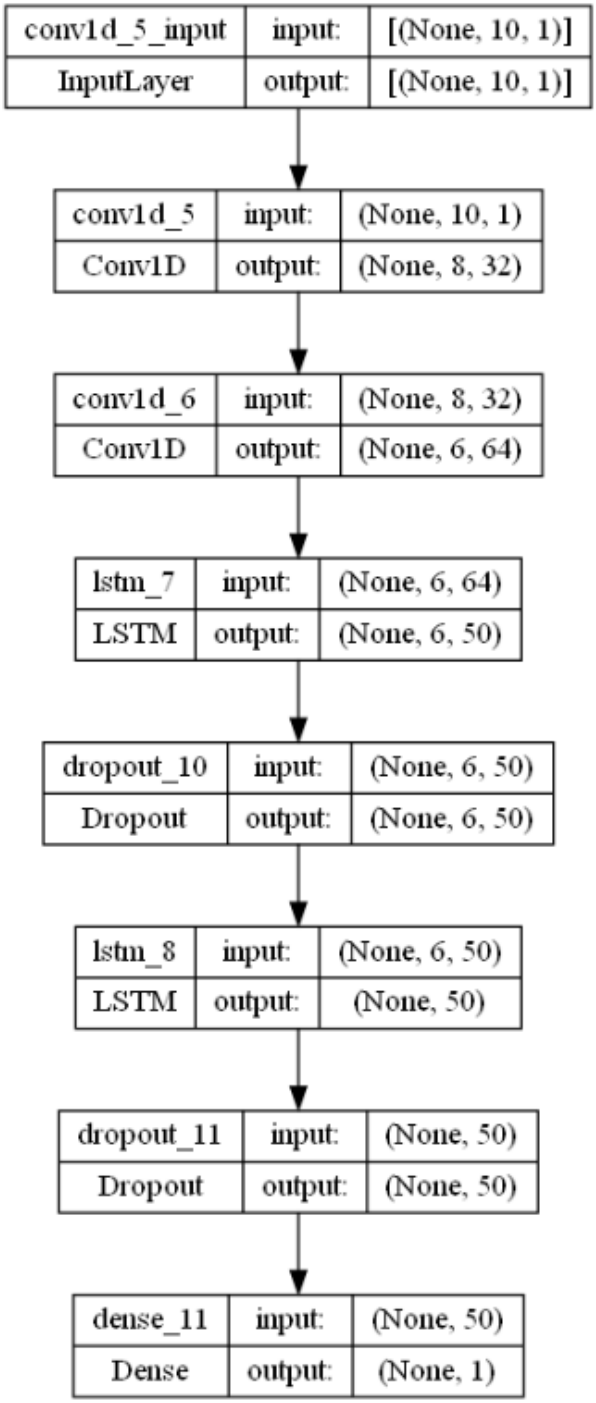


Figure 13: Hybrid Deep Learning architecture

The model's performance is compared with the other models, and the results show that the hybrid model outperforms the traditional CNNs, LSTMs, and RNNs models, providing better prediction accuracy for PRNG and QRNG sequences (Fig. 14).

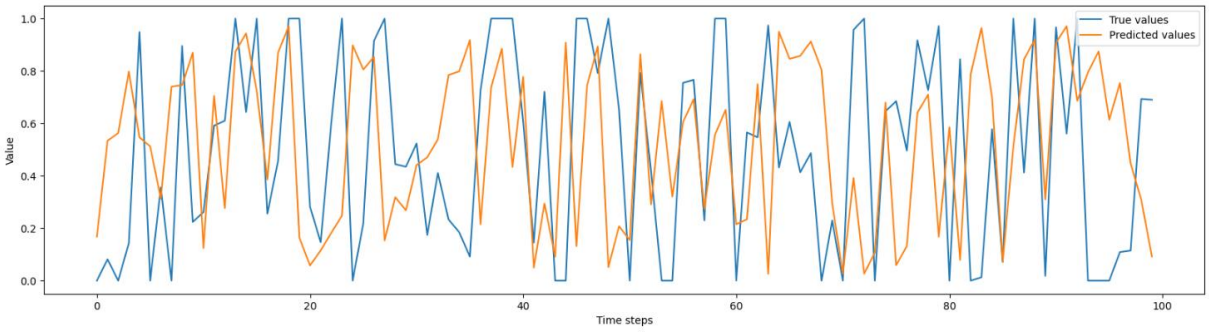


Figure 14: Hybrid Deep Learning performance

It can be observed numerous instances where the models were able to predict the exact value or a very close trend in PRNG and QRNG sequences (Fig. 15, 16). These instances demonstrate the effectiveness of the models in understanding the underlying patterns and dependencies within the data, as well as their capability to generalize and make accurate predictions on unseen data.

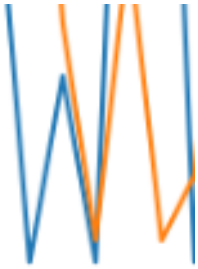


Figure 15: Exact match 1

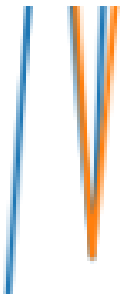


Figure 16: Exact match 2

Furthermore, it was observed that the models were often able to predict a close trend in the sequences, even if the exact value was not pinpointed (Fig.17).

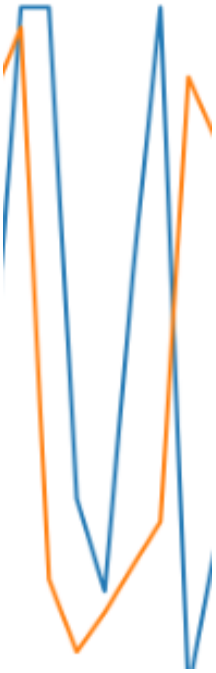


Figure 17: Close trend example

This indicates that the models have a strong grasp of the overall dynamics and structure of the data, enabling them to generate predictions that closely follow the actual trajectory of the PRNG and QRNG sequences [14-16]. This level of trend identification can prove beneficial in scenarios where understanding the general direction or pattern of the data is more critical than pinpointing individual values [17].

Conclusions and Future Work

In this paper, was presented a novel hybrid deep learning model that combines the strengths of Convolutional Neural Networks (CNNs), Long Short-Term Memory (LSTM) networks, and RNNs to predict Pseudo-Random Number Generator (PRNG) and Quantum Random Number Generator (QRNG) sequences. Our results demonstrate that the hybrid model outperforms traditional CNNs, LSTMs, and RNNs models in terms of prediction accuracy for both PRNG and QRNG sequences.

As part of the future work, it is planned to explore other hybrid model architectures that could further enhance the performance of our current model. Also was aimed to investigate the use of additional features, such as information from the frequency domain, to improve the prediction capabilities of our model. Furthermore, authors intend to study the generalizability of our hybrid model to other sequence prediction tasks. These tasks may include predicting cryptographic keys, secure communication protocols, and other security-related applications. Additionally, will be considered the development of more robust and efficient training strategies to ensure that proposed model remains effective even in the face of rapidly evolving security threats. By continuing to enhance and refine our hybrid deep learning model, authors hope to contribute to the advancement of secure communications and data protection in the digital age.

Acknowledgements

This work is carried out within the framework of research grant №0122U002361“Intelligent system of secure packet data transmission based on reconnaissance UAV”, funding by the Ministry of Education and Science of Ukraine during 2022-2023.

References

[1] M. Herrero-Collantes, J. C. Garcia-Escartin, “Quantum random number generators”, Reviews of Modern Physics, Vol. 89, 2017, art. 015004.

[2] I. Goodfellow, Y. Bengio, A. Courville, “Deep Learning”, MIT Press, 2016.

[3] J. Wang, M. J. Pérez-Jiménez, “Forecasting Sunspot Numbers with LSTM”, International Conference on Membrane Computing, Springer, Cham, 2016, pp. 153-166.

[4] A. Vaswani, N. Shazeer, N. Parmar et al, “Attention is all you need”, Advances in neural information processing systems, Vol. 30, 2017, pp. 5998-6008.

[5] G. Marsaglia, “Random Number Generators”, Journal of Modern Applied Statistical Methods, Vol. 2, 2003, pp. 2-13.

[6] D. P. Kingma, J. Ba, Adam, “A method for stochastic optimization”, arXiv preprint arXiv:1412.6980, 2014.

[7] Y. LeCun, Y. Bengio, G. Hinton, “Deep learning”, Nature, Vol. 521, 2015, pp. 436-444.

[8] S. Hochreiter, J. Schmidhuber, “Long short-term memory”, Neural computation, Vol. 9, 1997, pp. 1735-1780.

[9] Imanbayev A., Tynymbayev S., Odarchenko R. et al, “Research of Machine Learning Algorithms for the Development of Intrusion Detection Systems in 5G Mobile Networks and Beyond”, Sensors, 2022, Vol. 22, issue 24, art. 9957.

[10] I. Sutskever, O. Vinyals, Q. V. Le, “Sequence to sequence learning with neural networks, Advances in neural information processing systems”, Vol. 27, 2014, pp. 3104-3112.

[11] J. Chung, C. Gulcehre, K. Cho, Y. Bengio, “Empirical evaluation of gated recurrent neural networks on sequence modelling”, arXiv preprint arXiv:1412.3555, 2014.

[12] Azarov I., Gnatyuk S., Aleksander M., Azarov I., Mukasheva A. “Real-time ML Algorithms for the Detection of Dangerous Objects in Critical Infrastructures”, CEUR Workshop Proceedings, 2023, Vol. 3373, pp. 217-226.

[13] Iashvili G., Avkurova Z., Iavich M., Bauyrzhan M., Gagnidze A., Gnatyuk S. “Content-Based Machine Learning Approach for Hardware Vulnerabilities Identification System”, Lecture Notes on Data Engineering and Communications Technologies, Vol. 83, pp. 117-126, 2021.

[14] J. Aldama, S. Sarmiento, I. H. López Grande, S. Signorini, L. T. Vidarte and V. Pruneri, “Integrated QKD and QRNG Photonic Technologies,” in Journal of Lightwave Technology, vol. 40, no. 23, pp. 7498-7517, 1 Dec.1, 2022.

[15] Faure E., Shcherba A., Vasiliu Y., Fesenko A. “Cryptographic key exchange method for data factorial coding”, CEUR Workshop Proceedings, 2020, Vol. 2654, pp. 643-653.

[16] R. Kuang, D. Lou, A. He, C. McKenzie and M. Redding, “Pseudo Quantum Random Number Generator with Quantum Permutation Pad,” 2021 IEEE International Conference on Quantum Computing and Engineering (QCE), Broomfield, CO, USA, 2021, pp. 359-364.

[17] M. Gupta and M. J. Nene, “Random Sequence Generation using Superconducting Qubits,” 2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV), Tirunelveli, India, 2021, pp. 640-645.