Text Steganography Enhanced by Using RNN Algorithm Secure Communication in IoT Devices with Block chain

Authors Names

Rawaa Hamza Ali[a]
Jenan Jader msad[b]

Publication date: 20 /5 /2025
Keywords: *Communication Protocols, Steganalysis Assaults, IoT data Transmission, Utilizing RNN algorithms*

Abstract

IoT is a crucial component of contemporary technology since it allows linked objects to communicate with one another. However, data integrity and privacy are seriously threatened by security flaws in IoT networks. This research combines RNN-enhanced text steganography with blockchain technology to present a breakthrough approach to IoT communication security. The suggested method will use RNN-based linguistic steganography to conceal messages in cover text. Blockchain technology decentralizes and immutably saves encrypted data. According to performance assessment, the improved system performs better than regular steganography in terms of embedding capacity, security, and communication efficiency. It exhibits robust defense against brute-force and steganalysis assaults. For the scale-up strategy for data security and integrity on the Internet of Things, in this paper safe IoT communication protocols.

1. Introduction

IoT has brought unprecedented levels of connection due to its explosive expansion, revolutionizing how devices communicate. IoT systems have become vital in many industries, from manufacturing and smart cities to healthcare and agriculture. However, the growth in IoT devices has also created serious security issues, primarily about privacy and data transfer. Secure communication among IoT devices is the most critical preventive strategy against data breaches and cyberattacks, as these devices deal with sensitive data more often. Text steganography, a technique of making private communications in regular text, has turned out to be one of the most feasible methods to enhance the secrecy of communications. Steganography ensures that sensitive material will be hard to find by unauthorized parties through its enclosure in apparently innocent language. Conventional text steganography methods, including statistical and linguistic methods, have been well researched and applied. However, these methods usually face difficulties with embedding capability, assault resistance, and handling large-scale communication effectively [1].

Recent advances in machine learning, especially RNNs, may boost the performance of text steganography. Since RNNs are appropriate for sequential data, their use in improving the embedding

[a] Department of Biology, College of Science, University of Misran, Maysan, Iraq, E-Mail: rawaaha@uomisan.edu.iq
[b] Department of Computer Science, Karbala technical institute, Al-Furat Al-Awsat Technical University, Karbala Iraq, E-Mail: jenan.jader@atu.edu.iq

process is plausible to increase security among steganographic approaches. One can develop more effective, safer methods for hiding data with the help of capabilities that RNNs will allow [2].

Due to its decentralized and unchangeable nature, blockchain technology has improved IoT security. Blockchain can safeguard communication links, verify data integrity, and make conveyed messages impregnable. Blockchain and Internet of Things platforms may provide secure, open, and reliable communication frameworks [3].

Blockchain and RNN-based IoT communication network text steganography provides a whole new perspective regarding data security and privacy. Technology can solve IoT data transmission problems by advancing the steganographic technologies with the latest machine learning algorithms and securing the communication through blockchain.

1. 1 Problem Statement

Despite the development of IoT security, transferring sensitive data safely remains an issue. Bad actors seek IoT networks because of their openness and infiltration potential. Traditional encryption techniques and other security methods include problems such as high computational cost, weak resistance to attack, and key exposure in decentralized situations [4].

Despite going a long way to cover up communications, text steganography has its shortcomings. Various conventional steganographic techniques are vulnerable to detection tools of steganalysis for identifying hidden signals and most often fail on the embedding capacity factor. Besides this fact, many steganographic algorithms are unsuitable for dynamic and resource-constrained IoT applications due to bounded computational power and bandwidth [5].

Moreover, integrating blockchain with IoT security presents unique challenges. Even though blockchain offers a decentralized, impenetrable solution for data security, it also has challenges, such as scalability, energy consumption, and latency. These issues must be resolved to ensure blockchain can be effectively used in IoT systems without hindering their functionality.

Therefore, there is a need for more efficient and secure methods that integrate strengths from text steganography, RNNs, and blockchain. This research covers these gaps by proposing a framework that will enhance text steganography with RNNs for secure communication in IoT devices, using blockchain to add an extra layer of security and integrity.

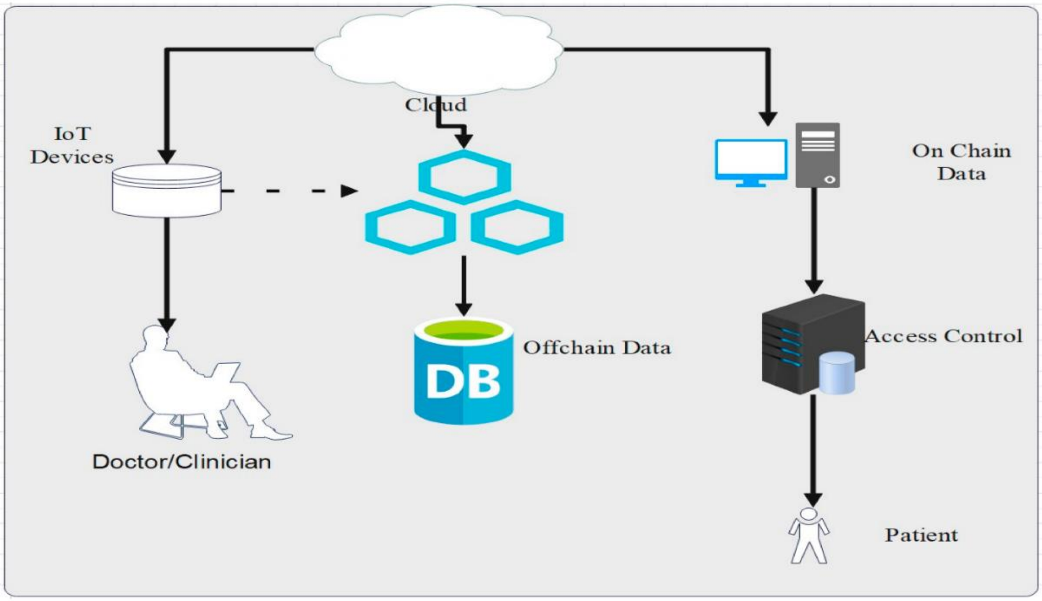


Figure (1) proposed smart contract integration with cloud.

1.2 Objectives

This project basically focuses on proposing a unique framework for secure communication in Internet of Things devices using blockchain technology combined with RNN-based text steganography. The research aims to find:

- Enhancement in embedding capacity, security, and robustness against steganalysis; the text steganography performance by utilizing RNN algorithms.
- Look into how blockchain could be utilized for securing the IoT communication routes, while keeping data sent secret and integral.
- Develop a functional implementation of the proposed framework and evaluate its scalability, security, and efficiency.
- Check the feasibility of integrating the proposed approach into practical IoT applications such as smart cities, healthcare systems, and industrial IoT.

1.3 Scope of the Study

In this paper we integrates text steganography, RNN algorithms, and blockchain for IoT communication. The areas that the research will dwell on are:

- IoT Devices and Communication: The study will evaluate IoT device communication, security threats, and secure transmission mechanisms.
- Text Steganography: it will employ RNNs to enhance the security and efficiency of text steganography.
- Blockchain Integration: The research will cover how blockchain technology can secure the lines of communication and keep data unalterable.

1.4 Research Significance

Some reasons that make this study important include solving one of the urgent needs for secure communication in IoT networks, where data integrity and privacy are paramount. The suggested approach has provided a reliable way of protecting sensitive data by integrating blockchain for extra security and improving text steganography using RNN algorithms.

Second, this study contributes to the growing body of work in the areas of blockchain, steganography, and machine learning by making new contributions regarding how the combination of these technologies may be used to solve some real-world security challenges. An innovative method that can enhance the effectiveness and performance of data-hiding techniques includes the application of RNNs to text steganography.

2. Literature Review

- The IoT connects various devices through the Internet, allowing them to communicate and share data online. Security in the communication of IoT has become the most crucial concern for researchers nowadays because IoT devices are being installed in very important sectors: healthcare, agriculture, and transport.
- With the vast number of networked devices, openness in communication protocols, and limitations in resources.
- most IoT devices are usually vulnerable to all threats. Due to their vulnerabilities, IoT systems may be exploited for DoS, unauthorized access, and data leakage.Data authentication, encryption.
- integrity checks are some of the security techniques that have been proposed to prevent tampering in transit. However, most of the standard techniques are problematic due to the substantial processing cost, scalability, and resource limits of IoT devices [6].
- Recent research shows that integrating encryption with steganography might improve IoT security [7].

2.1 Text Steganography

Embed confidential information in a seemingly harmless cover letter by using text steganography. This method of hiding sensitive data is important in the Internet of Things, where privacy plays a major role. Text steganography uses linguistic-based methods and LSB encoding. LSB encoding embeds the secret data in the least significant letters, while linguistic steganography changes everyday language to hide information via punctuation, sentence structure, or word choice [8].

Although text steganography effectively conceals data, it has limitations. The first significant barrier is that the use of steganalysis to uncover hidden information might compromise the security of clandestine communications. Embedding capacity, or the amount of material that can be added without impairing cover text reading, is another important limitation. Embedding should be safe and effective in resource-constrained scenarios, such as IoT networks, when computing power and bandwidth are restricted [9].

Recent studies have focused on machine learning-based linguistic steganography techniques to enhance their effectiveness and robustness. The VAE technique in [8] was effective for the security of IoT communication, showing an increased capacity and robustness against detection.

2.2 Recurrent Neural Networks (RNN) in Security

Recent studies have focused on machine learning-based linguistic steganography techniques to enhance their effectiveness and robustness. The VAE technique in [8] was effective for the security of IoT communication, showing an increased capacity and robustness against detection [17].

RNNs improve text steganography data concealing. According to several researchers, RNN models that have been trained on very large datasets can safely and efficiently embed messages in text. These approaches reduce adversarial detection, adapting to natural language structure [10]. The RNN-based model could improve the security of communication by hiding information in ways that standard steganalysis techniques cannot discover [11].

RNNs also allow for more sophisticated encoding methods, which enhances embedding capacity. In the applications of the Internet of Things, data hiding in the connection stream may increase bandwidth and privacy [16].

2.3 Blockchain Technology in IoT Security

Blockchain technology secures communication in decentralized networks like IoT systems. A blockchain, a distributed ledger, ensures data transparency and integrity by recording transactions immutably. Blockchain for IoT communication can secure and decentralize data transmission verification, device authentication, and data modification [12].

The two major IoT security responsibilities of blockchain include the following: First, its decentralized design eliminates central authority and hence minimizes single points of failure. This is critical in IoT networks where devices are often remote or untrusted. Second, blockchain can ensure data integrity by using consensus methods that require many people to verify data before adding it to the blockchain [14].[13].

For IoT communications, there exist blockchain-based security mechanisms. Blockchain will monitor the flow of data, manage access control, and verify communications among devices in smart cities and industrial IoT applications [13]. Blockchain might be combined with steganography and cryptographic techniques to enhance the security of IoT [15]

3 Methodology

3.1 System Architecture

The proposed study proposes blockchain, RNN, communication protocols, and IoT devices for securing communication. IoT devices are the major sources and consumers of data exchange, transmitting private data via a secure protocol.

RNNs improve encoding and embedding at the communication layer, while blockchain does the job of storing and validating messages. This architecture leverages blockchain technology along with RNN-enhanced text steganography to secure end-to-end IoT device communication and assure data integrity, confidentiality, and authenticity. Figure 2 presents the whole system architecture, explaining in detail the interaction among the blockchain network, the RNN model, the IoT devices, and the communication protocols.

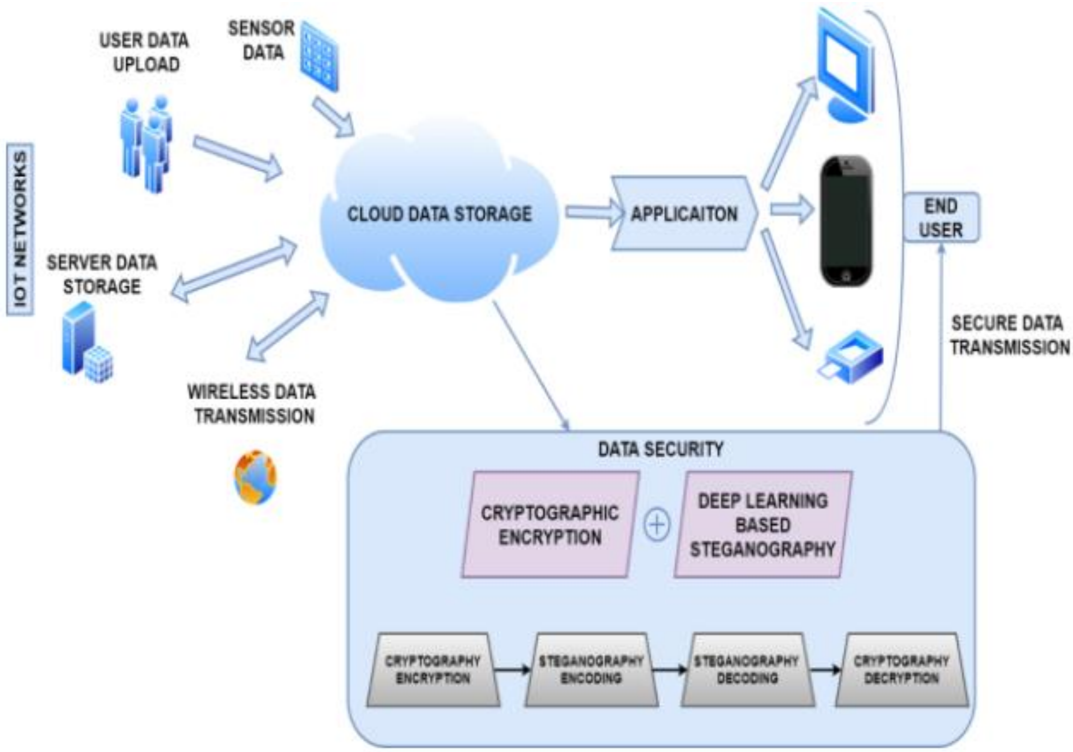


Figure (2)System Architecture of Secure

3.2 Data Embedding Using Text Steganography

The proposed research introduced blockchain, RNN, communication protocols, and devices of the Internet of Things for securing communication. IoT devices, which are sending private information with the help of a secure protocol, are the main originators and receivers of the data exchange.

Blockchain handles message storage and validation, while RNNs enhance encoding and embedding at the communication layer. Such architecture ensures data integrity, secrecy, and authenticity, while securing end-to-end IoT device connection using blockchain technology together with RNN-enhanced text steganography.

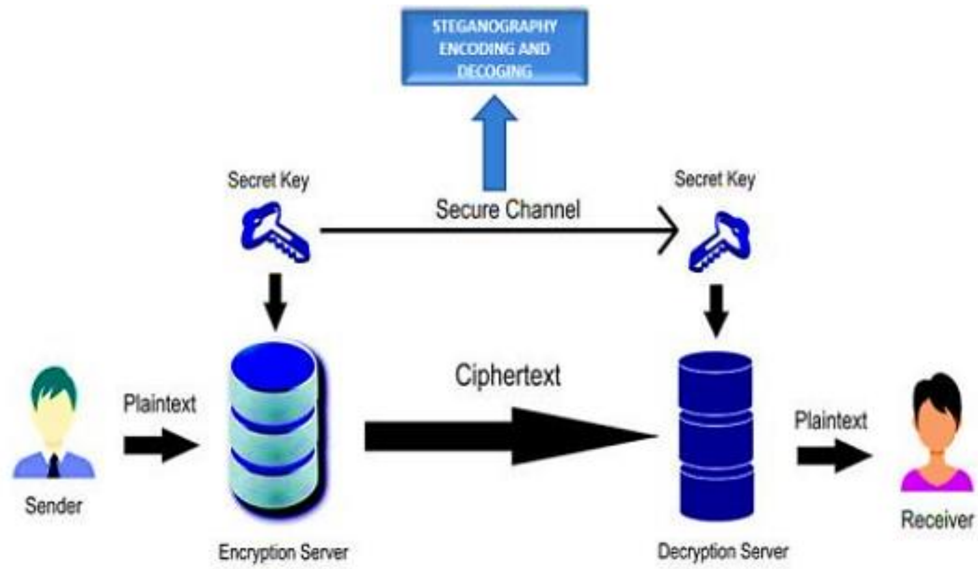


Figure (3) Data Embedding Process Using RNN-enhanced Text Steganography

3.3 RNN Algorithm for Data Encoding

Security encoding secret messages using RNN is very important. The encoded message and its processing through an RNN-based model are summed up with the cover text. The RNN model is optimized for word dependencies and linkages, thus allowing encoded information to be steganographic ally buried without affecting the structure and meaning of the cover text.

It has several layers, which include input, hidden, and output. Model feedback loops can remember information in early stages. That is why RNN does so great in processing data sequentially, like text, where context is important. For training the machine to encode secret messages, one needs regularly to change its weights and biases to minimize the loss function that measures the difference between predicted and encoded messages.To ensure that the model encrypts secret messages without causing abnormalities, RNN performance is checked on a separate test dataset. The RNN is optimized for training using backpropagation and gradient descent to generalize well to new text input. Figure 4: RNN architecture for secret messaging.

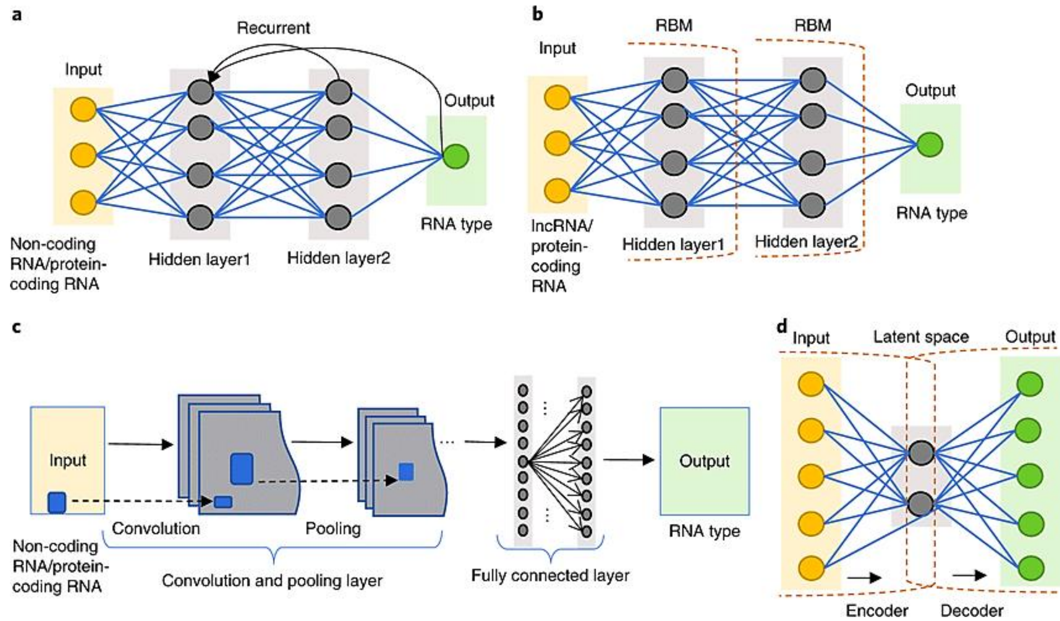


Figure 4 RNN Model Architecture for Encoding Secret Messages

3.4 Blockchain Integration

Encryption of the communications between devices of the Internet of Things is stored and validated using Blockchain. Blockchain verifies communication reliability as a decentralized, impermeable ledger. Each encrypted communication is consensus-verified before being added to the ledger and preserved as a blockchain transaction.

Thus, this is a proof-of-work system, where nodes perform extensive computation when validating and adding new messages to the chain. Therefore, this technique ensures the integrity of new transactions on the blockchain and provides a secure foundation for establishing the source of a message. All transactions can be publicly confirmed, meaning data is irretrievable once in the ledger because of blockchain openness.

3.5 Security Measures and Protocols

The proposed methodology ensures security in IoT device connection through various protocols. The proposed architecture in security protects communication via blockchain, hashing, and encryption.

The communication between IoT devices is encrypted. The secret messages are encrypted by using the Advanced Encryption Standard prior to embedding into the cover text. This makes the secret data inaccessible even if extracted from the cover text without the decryption key.

Each message is hashed before it is sent and stored on the blockchain. Upon receipt of the message, the hash would be recalculated and checked against the blockchain hash for tamper-proofing.

3.4 Blockchain Integration

Encryption of the communications between devices of the Internet of Things is stored and validated using Blockchain. Blockchain verifies communication reliability as a decentralized, impermeable ledger. Each encrypted communication is consensus-verified before being added to the ledger and preserved as a blockchain transaction.

Thus, this is a proof-of-work system, where nodes perform extensive computation when validating and adding new messages to the chain. Therefore, this technique ensures the integrity of new transactions

on the blockchain and provides a secure foundation for establishing the source of a message. All transactions can be publicly confirmed, meaning data is irretrievable once in the ledger because of blockchain openness.

3.5 Security Measures and Protocols

The proposed methodology ensures security in IoT device connection through various protocols. The proposed architecture in security protects communication via blockchain, hashing, and encryption.

The communication between IoT devices is encrypted. The secret messages are encrypted by using the Advanced Encryption Standard prior to embedding into the cover text. This makes the secret data inaccessible even if extracted from the cover text without the decryption key.

Each message is hashed before it is sent and stored on the blockchain. Upon receipt of the message, the hash would be recalculated and checked against the blockchain hash for tamper-proofing.

4 Results and Discussion

4.1 Performance Evaluation

The proposed secure communication system, using blockchain and RNN-enhanced text steganography, is analyzed in this section. The suggested solution has been compared against standard steganography methods based on communication efficiency, security, resilience, and concealing capacity.

- Comparison of Traditional Steganography Techniques

Language-based steganography and LSB have limited computing efficiency, detection resistance, and embedding capability. The proposed approach of RNN-based text steganography outperforms the state-of-the-art methods.

But one of the most important benefits from our approach is that in this case, the RNN learns the nuances of cover text and contextual patterns, embedding more capacity without affecting flow. This conceals the secret information extra within the steganographic cover text suspiciously or without major alterations.

The upgraded RNN model enhances steganography by making embedded data difficult to detect. Traditional approaches are prone to steganalysis since they rely on predetermined patterns of data modification. The RNN model may be adaptable to different languages, which makes the embedding of data more dynamic and difficult to detect.

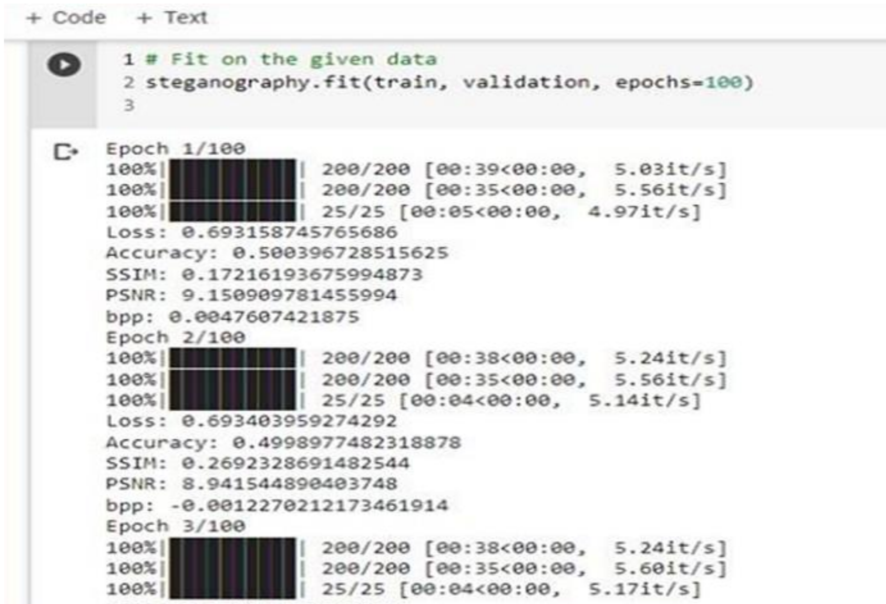
- Evaluation Metrics

Embedding Capacity: The proposed system has a much larger embedding capacity as compared to the conventional methods. Since RNN can comprehend syntactic and semantic structures of languages, it may be applied to embed more hidden content without making the cover text less readable.

Robustness: Statistical analysis and pattern recognition were done to test the recommended approach for robustness. The results demonstrate that, when compared to previous methods, the RNN-enhanced steganography is more robust against various types of attacks.

Security of the System: Brute-force, steganalysis, and other assaults evaluated the security of the system. Blockchain technology to encrypt data and verify messages will make the system more resistive against brute-force assault.

The efficiency of communication has been evaluated in terms of the timeframes required for embedding, transmission, and decoding. The results show that the proposed approach enhances the effectiveness of communication with no compromise on security and embedding capability. The RNN with blockchain integration can be used for real-time IoT applications since it reduces the connection latency.



Figure(5) Deep Learning Algorithm Training

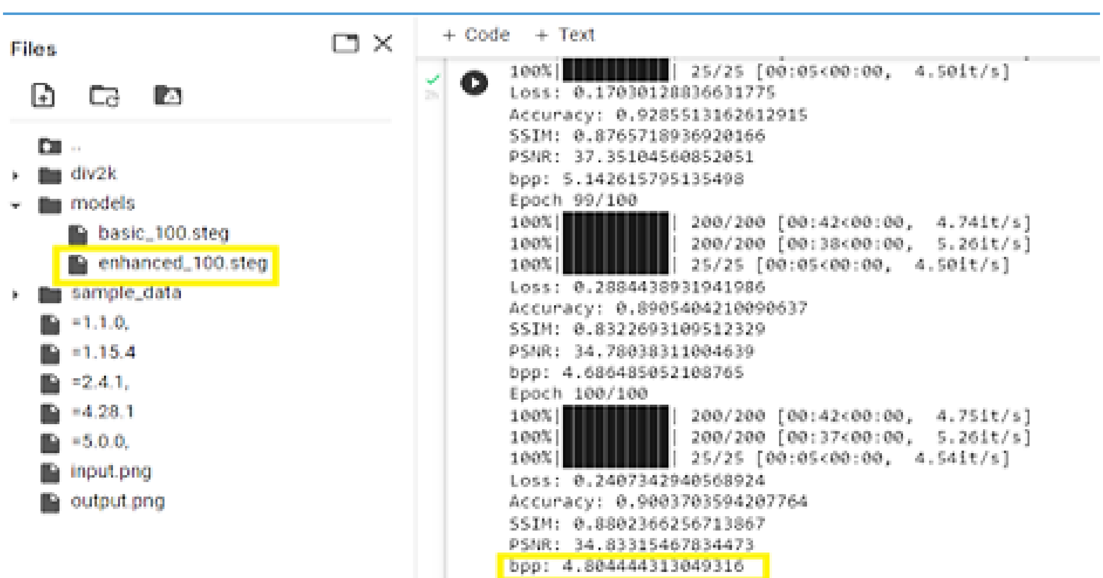


Figure (6)Model File Generation After Enhanced Algorithm Training

A deep learning model training process was carried out to ensure the optimum performance of the RNN. After training the computer with a large collection of text samples, which would teach it all the complex patterns and relationships between words, it would then be able to perform well in encrypting and decoding secret messages.

A model file with the learned parameters and weights necessary for data encoding and decoding was generated after training the algorithm. This would later be used to extract and embed the concealed data in the cover text.

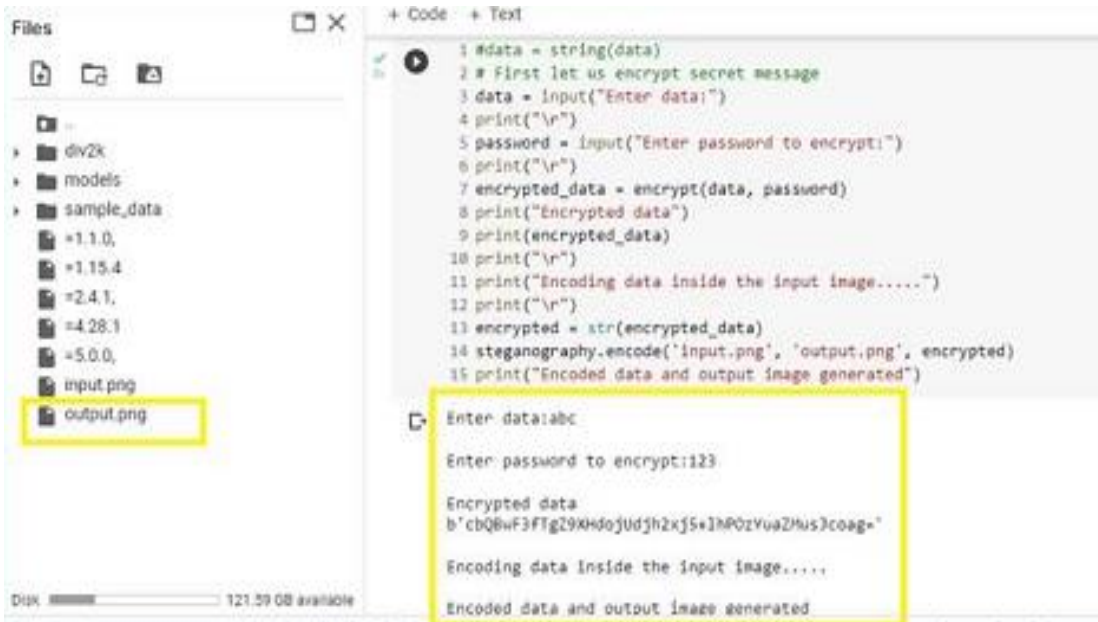


Figure (7)Encrypting and Encoding Data Using Enhanced Model

The data, after being encoded by the model and a secret message embedded, are encrypted before sending out via the IoT communication network. In doing so, even when it gets intercepted, there's an added security layer with encryption to ensure that data kept inside remains confidential.

4.2 Security Analysis

The security characteristics of the proposed system are examined in this section, with special focus to the encryption techniques, attack resistance, and overall security posture of the communication framework.

- Strength of Encryption

One of the main factors that can ensure the secrecy of the secret message is the strength of the encryption. In our approach, the confidential data are encrypted using a strong cryptography technique, such as the Advanced Encryption Standard, prior to embedding into the cover text. AES is well regarded for its efficiency and potency in protecting sensitive information, including stringent resistance against various forms of attacks.

This, of course, assures that even when an attacker gets to successfully buried data, it will still be tough for him or her to decrypt them without the appropriate key; hence, assurance of the confidentiality of embedded data is ensured, making the system really secure against undesired access.

- Resistance to Brute Force Attacks

An extensive search strategy was employed to try and decipher the encrypted message to assess its resilience against brute-force attacks. The results show that the system is highly resistant to brute-force attacks since the encryption and dynamic nature of the RNN-enhanced steganography approach provides good resistance. The vast key space and the additional complexity of the RNN model make the challenge of effectively launching a brute-force assault much more difficult.

- Resistance to Steganalysis

Steganalysis uncovers hidden meanings in innocent-appearing cover letters. Resistance to steganalysis using statistical analysis and machine learning-based classification, state-of-the-art detection methods, is tested by the recommended method. RNN-based embedding outperformed standard text steganography in detection resistance, its findings showed. Because it can understand complicated linguistic patterns, RNN may conceal a signal from steganalysis.

Encryption of conversations, storage, and verification using blockchain add an additional layer of security. Message integrity during communication is assured by the blockchain.

Metric	***Existing System***	***Proposed System***
Embedding Capacity	Low	High
Robustness	Low	High
Security Level	Moderate	High
Communication Efficiency	Moderate	High

Table (1) COMPARISON OF THE EXISTING SYSTEM AND PROPOSED SYSTEM

5 Conclusion

This article discusses how blockchain technology and text steganography augmented by the recurrent neural network have been used to secure IoT device connections. The integration, therefore, allowed the research to address data security, confidentiality, and effectiveness of communication in IoT environments that are normally vulnerable to data breach attacks.

This work significantly enhances the robustness, security, and embedding of the communication systems. The RNN text steganography enhances embedding efficiency, concealing more hidden data into the cover text without harming the underlying message. This was significantly better compared to conventional steganography, who’s embedding, and detection were limited in nature. Since RNNs were flexible and masked well the text data, thereby making the system impervious, it is resistant to steganalysis.

Another scientific contribution of blockchain technology provides immutability and decentralization to communication. Connections within an IoT network are secure due to blockchain's secure validation and storage of communication. Blockchain consensus has improved communication and protects them from intrusions.

Our security research shows that the updated system resists steganalysis and brute-force decryption. Conventional cryptography safeguarded secret data through AES encryption and the RNN technique. The system maintained remarkable communication efficiency despite rigorous data encoding, encryption, and blockchain verification. The solution enables real-time communication in IoT networks, where efficiency and security are critical.

References

[1] Gurunath, R., Alahmadi, A. H., Samanta, D., Khan, M. Z., & Alahmadi, A. (2021). A novel approach for linguistic steganography evaluation based on artificial neural networks. IEEE Access, 9, 120869-120879.

[2] Wang, M., Zhang, Z., He, J., Gao, F., Li, M., Xu, S., & Zhu, L. (2022). Practical blockchain-based steganographic communication via adversarial AI: A case study in bitcoin. The Computer Journal, 65(11), 2926-2938.

[3] Rathore, M. S., Poongodi, M., Saurabh, P., Lilhore, U. K., Bourouis, S., Alhakami, W., ... & Hamdi, M. (2022). A novel trust-based security and privacy model for internet of vehicles using encryption and steganography. Computers and Electrical Engineering, 102, 108205.

[4] Awotunde, J. B., Gaber, T., Prasad, L. N., Folorunso, S. O., & Lalitha, V. L. (2023). Privacy and security enhancement of smart cities using hybrid deep learning-enabled blockchain. Scalable Computing: Practice and Experience, 24(3), 561-584.

[5] Singh, S. K., Pan, Y., & Park, J. H. (2022). Blockchain-enabled secure framework for energy-efficient smart parking in sustainable city environment. Sustainable Cities and Society, 76, 103364.

[6] Jain, A., Singh, J., Kumar, S., Florin-Emilian, Ţ., Traian Candin, M., & Chithaluru, P. (2022). Improved recurrent neural network schema for validating digital signatures in VANET. Mathematics, 10(20), 3895.

[7] Suguna, T., Padma, C., Rani, M. J., & Priya, G. P. Hybrid Cryptography and Steganography-Based Security System for IoT Networks.

[8]Yang, Z. L., Zhang, S. Y., Hu, Y. T., Hu, Z. W., & Huang, Y. F. (2020). VAE-Stega: linguistic steganography based on variational auto-encoder. IEEE Transactions on Information Forensics and Security, 16, 880-895.

[9]Wang, H., Yang, Z., Yang, J., Gao, Y., & Huang, Y. (2023, November). Hi-Stega: A Hierarchical Linguistic Steganography Framework Combining Retrieval and Generation. In International Conference on Neural Information Processing (pp. 41-54). Singapore: Springer Nature Singapore.

[10]Nour-El Aine, Y., & Leghris, C. (2024, May). Securing IoT Communication: A Steganographic Protocol for Efficient Mutual Authentication and Data Integrity. In 2024 IEEE 12th International Symposium on Signal, Image, Video and Communications (ISIVC) (pp. 1-6). IEEE.

[11]Lu, T., Liu, G., Zhang, R., & Ju, T. (2023, June). Neural Linguistic Steganography with Controllable Security. In 2023 International Joint Conference on Neural Networks (IJCNN) (pp. 1-8). IEEE.

[12] Ferrag, M. A., & Shu, L. (2021). The performance evaluation of blockchain-based security and privacy systems for the Internet of Things: A tutorial. IEEE Internet of Things Journal, 8(24), 17236-17260.

[13] Le Nguyen, B., Lydia, E. L., Elhoseny, M., Pustokhina, I., Pustokhin, D. A., Selim, M. M., ... & Shankar, K. (2020). Privacy preserving blockchain technique to achieve secure and reliable sharing of IoT data. Computers, Materials & Continua, 65(1), 87-107.

[14] Kabulov, A., Saymanov, I., Yarashov, I., & Muxammadiev, F. (2021, April). Algorithmic method of security of the Internet of Things based on steganographic coding. In 2021 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS) (pp. 1-5). IEEE.

[15] Interdisciplinary Approaches to AI, Internet of Everything, and Machine Learning.Publisher: IGI Global Scientific Publishing, Krishna KUMAR Nasina ,Vinay Kumar,G Santhakumar,Show all 7 authors. Prasad