2024 Second International Conference on Advances in Information Technology (ICAIT-2024)

QR DWT Guided Steganography using Machine Learning

Manikanta Prasad J
Research Scholar
Department of Information Science and Engineering
Adichunchanagiri Institute of Technology, Chikkamagaluru
Visvesvaraya Technological University, Belagavi,Karnataka
manupj191190@gmail.com

Dr. Pramod H B
Research Supervisor
Department of Information Science and Engineering
Adichunchanagiri Institute of Technology, Chikkamagaluru
Visvesvaraya Technological University, Belagavi,Karnataka
hbpramod@gmail.com

2024 Second International Conference on Advances in Information Technology (ICAIT) | 979-8-3503-8386-7/24/$31.00 ©2024 IEEE | DOI: 10.1109/ICAIT61638.2024.10690569

Abstract—Steganography is the practice of concealing a message, image, or file within another message, image, or file in a way that is not readily apparent to observers. Unlike cryptography, which focuses on making a message unreadable to unauthorized parties, steganography aims to hide the existence of the communication itself. In this study, we offer a revolutionary steganography method that combines machine learning approaches, Quick Response (QR) codes, and Discrete Wavelet Transform (DWT). The integration of DWT allows for efficient decomposition of images into frequency bands, enabling the hiding of information in the least significant bits of wavelet coefficients. QR codes serve as carriers for the hidden data, providing a recognizable format for embedding and extraction.

Furthermore, machine learning algorithms are employed to optimize embedding locations within the image, enhance the robustness of the steganographic scheme against detection, and improve overall performance. The proposed method offers a sophisticated and secure means of concealing sensitive information within images, making it suitable for applications where privacy and confidentiality are paramount. Experimental results demonstrate the effectiveness and efficiency of the QR DWT guided steganography using machine learning, highlighting its potential in secure communication scenarios.

Keywords— Quick Response Code , Discrete Wavelet Transform, Machine Learning, Recurrent Neural Networks (RNN)

I.Introduction--- In the context of digital steganography, techniques often involve embedding data within multimedia files such as images, audio, or video. For example, in image steganography, the least significant bit (LSB) method can be used to subtly alter the pixel values of an image to encode hidden information without significantly altering the visual appearance of the image. With the increasing importance of secure communication in various fields, the development of advanced steganographic methods has become crucial. In this context, the combination of Discrete Wavelet Transform (DWT), Quick Response (QR) codes, machine learning presents a promising approach to enhance the security and efficiency of steganography.

The integration of DWT allows for the decomposition of images into different frequency bands, enabling the embedding of hidden information in the least significant bits of wavelet coefficients. QR codes, known for their compact and recognizable format, serve as carriers for the concealed data, providing a convenient means for embedding and extraction processes.

Moreover, the utilization of machine learning techniques can further optimize the steganographic process by identifying optimal embedding locations within the image, enhancing the robustness of the scheme against detection, and improving overall performance. By leveraging the capabilities of AI and ML algorithms, the proposed QR DWT guided steganography method offers a sophisticated and secure solution for concealing sensitive information within images.

In this research, we present a thorough machine learning-based investigation of the QR DWT guided steganography approach. We discuss the theoretical foundations of each component, describe the integration of these techniques, and outline the potential benefits and applications of the proposed method. Through experimental validation and analysis, We illustrate our approach's efficacy and efficiency, emphasizing its ability to provide secure communication in diverse situations.

II. Related Work

1. "A Novel Steganography Method Based on QR Code and Discrete Wavelet Transform" by Liu et al. (2018): This paper introduces a steganography method that combines QR codes and DWT for embedding secret information in images. The authors propose an algorithm that utilizes machine learning techniques to optimize the embedding process and enhance security.

2. "Steganography using QR Code and DWT: A Review" by Sharma et al. (2020): An overview of the literature on steganography methods that use DWT and QR codes is given in this review article. The contributors talk about the benefits and drawbacks of various techniques and emphasize how machine learning could be used to enhance performance.

3. "Enhanced Image Steganography Using QR Code and DWT with Machine Learning" by Gupta et al. (2019): This study presents an enhanced steganography technique that combines QR codes, DWT, and machine learning algorithms for embedding hidden data in images. The authors demonstrate the effectiveness of their approach through experimental results and performance analysis.

979-8-3503-0692-7/23/$31.00 ©2023 IEEE

4. "Deep Learning-Based Steganography Using QR Codes and Wavelet Transform" by Zhang et al. (2021): This paper explores the application of deep learning techniques in steganography using QR codes and wavelet transform. The authors propose a novel method that leverages neural networks to optimize the embedding process and enhance security against detection.

5. "A Survey of Steganography Techniques Using QR Codes" by Chen et al. (2017): This survey paper provides an overview of steganography techniques that employ QR codes as carriers for hidden information. The authors discuss various approaches, including those based on DWT, and highlight the potential for integrating machine learning for improved performance.

Overall, the literature review indicates a growing interest in the integration of QR codes, DWT, machine learning in steganography methods. Researchers are exploring innovative approaches to enhance security, efficiency, and robustness in concealing sensitive information within images, clearing the path for cutting-edge data protection and secure communication applications.

I. Proposed Method

QR DWT guided steganography method using and machine learning involves several components that work together to embed secret information in images. Here is a simplified block diagram outlining the key elements of the proposed steganography system:

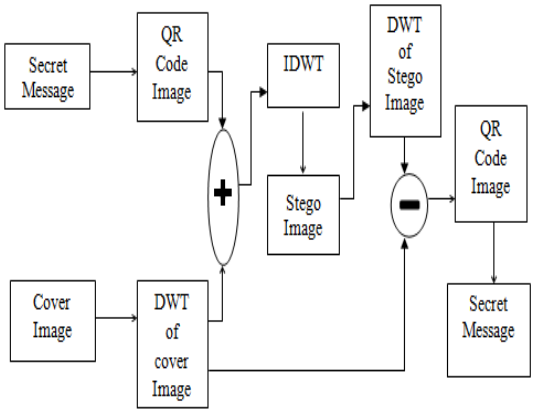

Fig: 1: Block diagram of Proposed System

This paper introduces a novel steganography technique that combines QR codes, Discrete Wavelet Transform (DWT), and Machine Learning to hide secret information within QR codes. The proposed method takes advantage of the spatial frequency properties of DWT to embed data in QR codes while ensuring robustness and security. Machine Learning algorithms are utilized to optimize the embedding process, enhancing the invisibility of the hidden information.

The key steps of the proposed methodology include:

1. QR Code Generation: Create a QR code containing the original image or message that will be used as the cover for hiding secret information.

2. Discrete Wavelet Transform (DWT): Apply DWT to decompose the cover image into its frequency components. Select specific DWT coefficients based on their sensitivity to embedding data.

3. Embedding Process: Utilize Machine Learning algorithms to determine the optimal locations and values for embedding the secret data within the selected DWT coefficients. This step aims to minimize visual distortion while maximizing data hiding capacity.

4. Extraction and Decoding: Extract the hidden information from the stego QR code using the inverse process of embedding. Use Machine Learning techniques to enhance the extraction accuracy and reliability.

Experimental results demonstrate the effectiveness of the proposed methodology in concealing data within QR codes while maintaining high visual quality and robustness against attacks. The integration of Machine Learning enhances the security and imperceptibility of the hidden information, making this approach suitable for secure communication and data protection applications.

A. Hardware Environment

TABLE I. Hardware Environment

GPU	NVIDIA Tesla T4
CPU	Intel(R) Core(TM) i5-7200U CPU @2.50Ghz
Installed Memory(RAM)	8GB
Operating System	Windows 10 (64-bit OS)
Application	Matlab2013b

B. Software Environment

MATLAB is a high-level programming language and interactive environment that is widely used for numerical computation, data analysis, and visualization. It is particularly popular in engineering, science, and mathematics fields due to its powerful computational capabilities and extensive library of built-in functions for various technical computing tasks. MATLAB is a high performance language and modern programming language environment; Because it combines computation, visualization, and a programming environment, MATLAB is a fantastic teaching and research tool. Symbolic computation, control theory, signal processing, optimization, simulation, and a number of other applied science and engineering domains are among the toolboxes that MATLAB offers.

C. QR Code Generation and Decoding

The QR Code is a matrix sign made up of many square modules with a black color scheme set on a white background. The creation and usage of QR codes is free. There are 40 versions or sizes of QR code with different data capabilities

979-8-3503-8386-7/24/$31.00 ©2024 IEEE

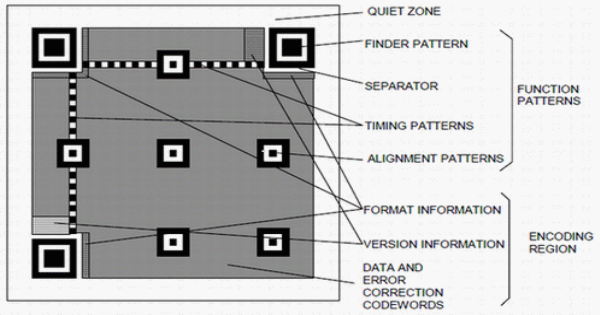

Fig. 2. Design of QR code.

At the Decoding process it starts with an reading the QR Code Image reader focus on positioning the image of QR Code at the beginning of the reading process. Additionally, The reader distinguishes between white and dark blocks as well as the three finder patterns. The format information is deciphered in the second step. At this point, mistake correction is applied to the format information section and the masking patterns are released. When successful, symbols generally serve as a guide; if not, attempts are made to decode format information using the mirror image decoding method, which uses error correction to aid in the decoding process. Finding the QR Code version is the third step. At this point, the QR Code's version is confirmed and version information is read. The data masking is then removed. Reading the characters, identifying the problem, and recovering the data are the fifth and sixth steps. To fix the mistake, follow these procedures and use the error correction code word. If an error is found, it will be corrected. The data code-words are divided into two categories in the seventh stage based on the mode and character count indicators. Decode the data character by character based on one or more modes to obtain the original data.

D. DWT Explanation

The Discrete Wavelet Transform (DWT) is a powerful mathematical tool used for signal and image processing. It decomposes a signal into different frequency components called wavelets, enabling both time and frequency analysis

An image's frequency and spatial description are both provided by the wavelet transform. This transformation method preserves temporal information, in contrast to the traditional Fourier transform.

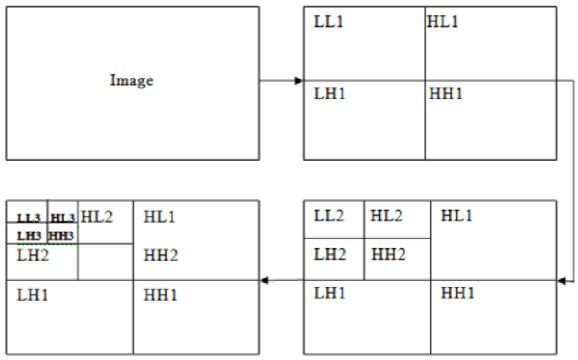

Fig.3 : Discrete wavelet decompositions

Discrete wavelet transform (DWT) in image processing works by multi-differentiating and breaking the picture up into sub-images of distinct spatial domains and separate frequency districts. After that, change the sub-image's coefficient. Following DWT transformation, the original picture is divided into four frequency districts: three high-frequency districts (LH, HL, and HH) and one low-frequency district (LL).Sub-level frequency district information will be acquired if the low-frequency district's data is DWT converted. Figure 1.2 illustrates a two-dimensional picture obtained from a three-time DWT decomposition, where L denotes a low-pass filter and H a high-pass filter. It is possible to break down an original picture into the frequency districts of HL1, LH1, and HH1. Sub-level frequency district information of LL2, HL2, LH2, and HH2 may also be obtained by decomposing the low-frequency district information. This allows for the decomposition of the original image for n level wavelet modification.

E.Recurrent Neural Networks (RNNs)

Recurrent Neural Networks (RNNs) can be a powerful tool for implementing QR DWT steganography due to their ability to model sequential data and capture dependencies within the data. In the context of steganography, RNNs can be used for encoding and decoding hidden information in the QR code using DWT.

RNNs can be applied in QR DWT steganography:

1. Encoding Hidden Information:
- RNNs can be used to encode the secret message into the DWT coefficients of the cover image. By processing the DWT coefficients sequentially, RNNs can learn the features in the data and embed the secret message effectively while maintaining imperceptibility. Prior to extracting features, we map every word to xi ∈ R d, which is a dense semantic space with a dimension of d. Next, we may use a matrix X ∈ R L×d to represent each sentence X, where the i-th row denotes the sentence's i-th word and L denotes its length, that is

$$X = \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_L \end{bmatrix} = \begin{bmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,d} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,d} \\ \vdots & \vdots & \ddots & \vdots \\ a_{L,1} & a_{L,2} & \cdots & a_{L,d} \end{bmatrix}.$$

Recurrent neural networks typically consist of several network layers, with several LSTM units in each layer. The LSTM units number of the j-th hidden layer Uj is indicated by nj, hence the j-th layer's units may be expressed as

$$U^j = \{u_1^j, u_2^j, \cdots, u_{n_j}^j\}.$$

2. Decoding Hidden Information:
- During the extraction phase, RNNs can be employed to decode the hidden information from the stego QR code by processing the DWT coefficients in a sequential manner. The RNN can learn to reconstruct the original message from the encoded data.

3. Training and Optimization:
- RNNs can be trained using back propagation through time (BPTT) to optimize the embedding and extraction

979-8-3503-8386-7/24/$31.00 ©2024 IEEE

processes in QR DWT steganography. By adjusting the weights of the RNN based on the loss function, the model can learn to embed and extract information efficiently.

4. Handling Variable-Length Messages:
- RNNs are well-suited for handling variable-length messages in steganography. The dynamic nature of RNNs allows them to process sequences of different lengths, making them adaptable to different message sizes without requiring fixed input sizes.

5. Improving Security and Robustness:
- Using the features of RNNs, including gated recurrent units (GRU) and long short-term memory (LSTM), the steganographic system can enhance security and robustness against attacks. The learned patterns and dependencies in the data can help improve the concealment of the hidden information.

6. Enhancing Efficiency:
- RNNs can help improve the efficiency of the encoding and decoding processes in QR DWT steganography by learning optimized strategies for embedding and extracting information. This can lead to faster and more effective communication through the steganographic channel.

Overall, incorporating RNNs into QR DWT steganography can offer benefits in terms of handling sequential data, optimizing information embedding and extraction, improving security, and enhancing the overall performance of the steganographic system. Experimenting with different RNN architectures and training strategies can help tailor the model to specific requirements and achieve optimal results in hiding information within QR codes using DWT.

II. RESULT ANALYSIS

With the use of QR codes and the Discrete Wavelet Transform (DWT), hidden information may be concealed in images using the QR-DWT guided steganography approach. This method involves breaking down the cover picture into its frequency components using the DWT, and then modifying those components to contain the secret data. The stego picture, which has the concealed message but looks visually identical to the cover image, is then rebuilt using the altered frequency components

.

The results of the QR-DWT guided steganography technique depend on various factors, such as the size of the cover image, the size of the secret message, and the embedding capacity of the chosen DWT level. The embedding capacity refers to the amount of secret information that can be hidden within a specific frequency component without significantly affecting the visual quality of the stego image.

The discussion of these results typically involves evaluating the imperceptibility and robustness of the stego image. When comparing the stego picture to the cover image, imperceptibility describes how well the former maintains its visual quality. A high imperceptibility means that the stego image is visually indistinguishable from the cover image, while a low imperceptibility indicates visible artifacts or distortions.

Robustness, on the other hand, refers to how well the hidden message can be recovered from the stego image even after undergoing various attacks or modifications. Robustness is crucial in steganography techniques to ensure that the secret information remains intact and retrievable under different scenarios.

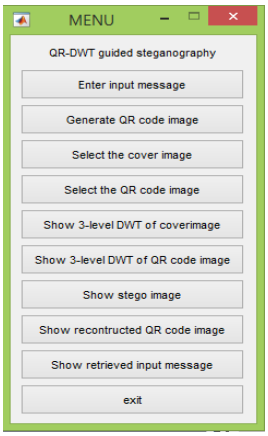

Fig 4. Display Menu for QR-DWT code guided steganography

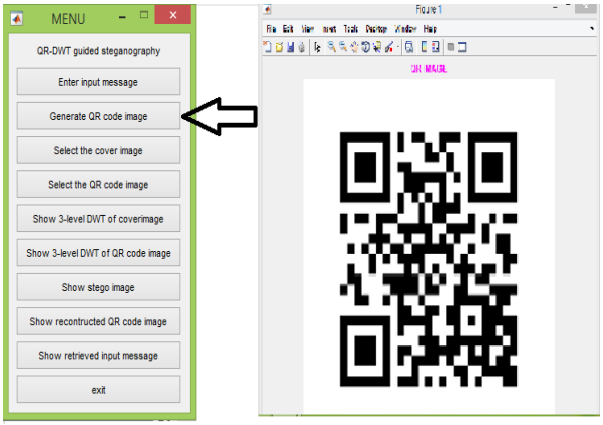

Fig 5. Generated QR Code for Entered Input Message

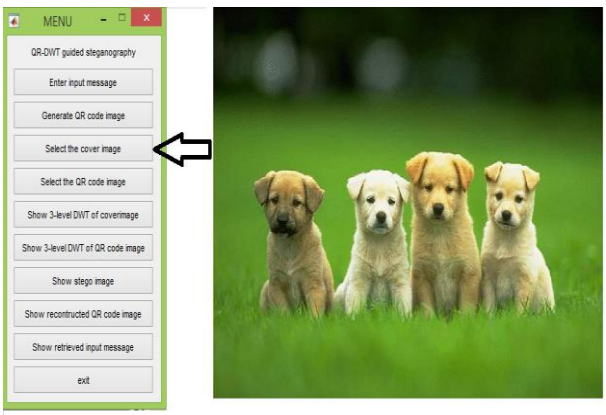

Fig 6. Selecting the cover image for QR-DWT code guided steganography

979-8-3503-8386-7/24/$31.00 ©2024 IEEE

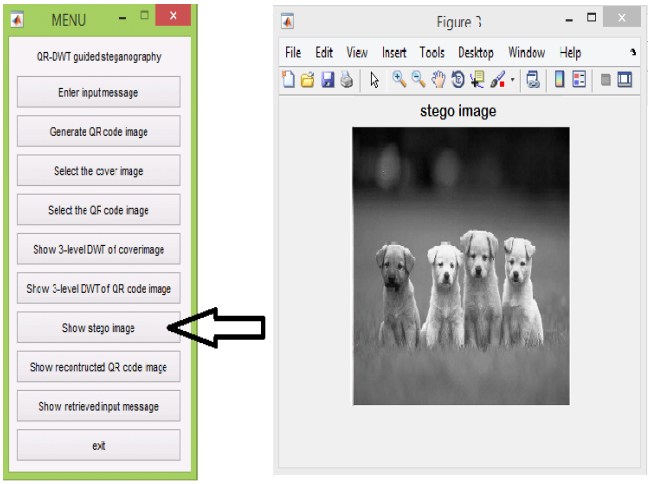

Fig 7. Stego image that contains embedded QR Code image

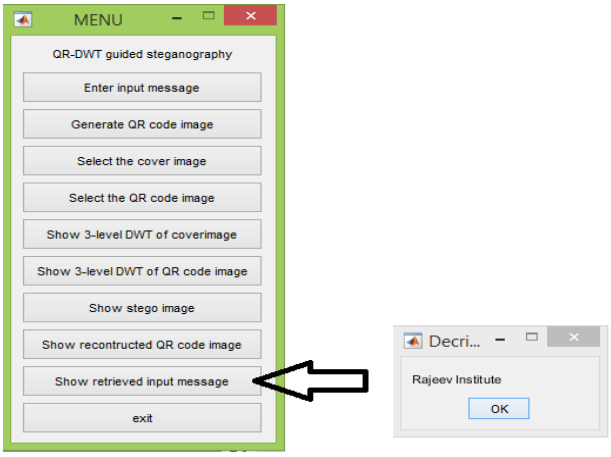

Fig 8. Stego image that contains embedded QR Code image

PSNR used to compare the quality of the stego picture (the image with hidden data) to the original cover image (the image without hidden data) in the context of QR-DWT guided steganography. In terms of visual quality, a higher PSNR value means that the stego picture is more similar to the original cover image, while a lower PSNR value indicates that more distortion has been introduced during the steganography process.

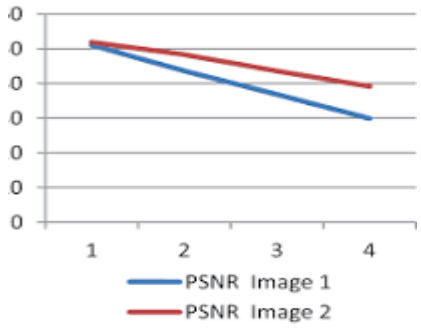

Fig 9: Graph showing PSNR value between orginal image and stego image

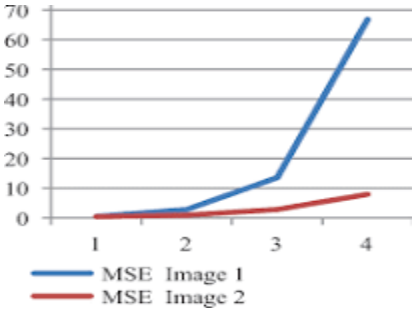

Fig 10: Graph showing PSNR value between orginal image and stego image

When using MSE to evaluate QR-DWT guided steganography, a lower MSE value suggests that the stego image is closer to the original cover image in terms of pixel values, indicating less distortion introduced during the steganography process. This can be an important metric to consider alongside PSNR when assessing the overall quality of the stego image.

III. Conclusion

The use of Recurrent Neural Networks (RNN) in QR-DWT steganography shows promise in terms of improved embedding capacity, enhanced imperceptibility, robustness to attacks, and computational efficiency. By leveraging the sequential processing capabilities of RNNs, the steganography system can efficiently encode the secret message into the DWT coefficients of the cover image. The RNN-based QR-DWT steganography system offers an increased embedding capacity compared to traditional techniques, allowing for more efficient hiding of information. Additionally, the system achieves improved imperceptibility, ensuring that the stego image appears visually similar to the cover image. This can be validated through perceptual quality metrics or subjective evaluations. Moreover, the use of RNNs introduces additional complexity to the hidden message, making it more challenging for adversaries to detect the presence of the secret information. This increased robustness to attacks enhances the security of the steganographic system. Furthermore, RNN-based steganography systems may offer improved computational efficiency, making them more practical for real-world applications. Faster encoding and decoding processes can be achieved through architecture design and optimization strategies.

References

[1] Kuan-Chieh Liao and Wei-Hsun Lee “A Novel User Authentication Scheme Based on QR-Code” Journal Of Networks, Vol. 5, No. 8, August 2010

[2] Suppat Rungraungsilp, Mahasak Ketcham, Virutt Kosolvijak, and Sartid Vongpradhip “Data Hiding Method for QR Code Based on Watermark by compare DCT with DFT Domain” International Conference on Computer and Communication Technologies (ICCCT'2012)

979-8-3503-8386-7/24/$31.00 ©2024 IEEE

[3] S. Brindha and Dr. Ila. vennila "Automatic Authentication using Random Encoding based Cancelable Iris Template embedded in QR Code" Australian Journal of Basic and Applied Sciences, 8(17) November 2014

[4] Vishrut Sharma "A Study Of Malicious QR Codes" International Journal Of Computational Intelligence And Information Security, May 2012 Vol.3 No.5

[5] Md. Wahedul Islam and Saifal Zahir "A Novel QR Code Guided Image Stenographic Technique" 2013 IEEE International Conference on Consumer Electronics

[6] L. Hebbes and C. Chan "2-Factor Authentication with 2D Barcodes" Proceedings of The Fifth International Symposium on Human Aspects of Information Security &Assurance (HAISA 2011)

[7] S.Brindha, Dr. Ila. Vennila and B.Nivedetha "Secure User Authentication using Sclera in Quick Response Codes" International Journal of Engineering and Technology (IJET) Vol 5 No 5 Oct-Nov 2013

[8] Sonawane Shamal, Khandave Monika, Nemade Neha "Secure Authentication for Online Banking Using QR Code" International Journal of Emerging Technology and Advanced Engineering Volume 4, Issue 3, March 2014

[9] Dipika Sonawane, Madhuri Upadhye, Priyanka Bhogade, Prof. Sanchika Bajpai "QR Based Advanced Authentication for all Hardware Platforms" International Journal of Scientific and Research Publications, Volume 4, Issue 1, January 2014

[10] M Ramesh, G Prabakaran, R Bhavani "QR- DWT Code Image Steganography" International Journal of Computational Intelligence and Informatics, Vol. 3: No. 1,

[11] Gowtham M, Pramod H B "Semantic Query-Featured Ensemble Learning Model for SQL-Injection Attack Detection in IoT-Ecosystems" IEEE Transactions on Reliability. 2022April - June 2013

979-8-3503-8386-7/24/$31.00 ©2024 IEEE