NTU Journal of Engineering and Technology (2026) 5 (1) : 1-10
DOI: https://doi.org/10.56286/ntujet.v5i1

IRAQI Academic Scientific Journals

P-ISSN: 2788-9971 E-ISSN: 2788-998X
NTU Journal of Engineering and Technology
Available online at: https://journals.ntu.edu.iq/index.php/NTU-JET/index

A Classification Model to Detect Malicious Software in QR Code

Naseem Nawful Maree[1]
[1]Programmer, Directorate of Treasury of Nineveh, Ministry of Finance, Mosul, Iraq
Naseemswe87@gmail.com

Article Informations

Received: 08-05- 2025,
Revised: 08-08- 2025,
Accepted: 01-09-2025,
Published online: 22-03-2026

Corresponding author:
Name: Naseem Nawful Rashad
Affiliation : Nineveh Treasury
Email: naseemswe87@gmail.com

Key Words:
QR Code,
CNN,
malicious,
benign,
deep learning.

A B S T R A C T

Quick Response (QR) codes have become very popular in making payments, marketing/authentication, and are frequently used with malicious intent by cybercriminals using them to inject malicious URLs to steal information or install malware. The current study is concerned with malicious QR codes detection with deep learning. A balanced data set of 316,254 benign and 316,254 malicious URLs were turned into an image of QR code to train a Convolutional Neural Network (CNN). On the validation set, the model attained 99.62% accuracy and on the test set, the model attained 100% accuracy, absolute precision, recall and F1 scores. Average processing speed is 61ms per batch which allows real time scanning. CNN was able to outperform other probabilistic models because of its high performance implying that further comparisons can be carried out in future. This work brings to the fore an efficient, scalable solution devised to identify malicious QR codes and enhance the security in the current contactless digital environment.

1. Introduction

Over the past few years, with the advent of the QR codes (quick response) in multiple areas of life (including finance, marketing, healthcare and education), data sharing and interactivity between users has become approachable. Nevertheless, security vulnerabilities have been generated through this feature as well. Cybercriminals have also taken advantage of QR codes by putting malicious links that result in phishing, malware downloads and even stealing computers. This is a concerning pattern that has elicited serious issues in cyber security, especially in terms of detection and defining malicious QR codes [1].

Historical modes of detection like URL black listing are not effective in detection of novel threats, as they depend on the ones that have been detected and registered. This weakness emphasizes the necessity of smarter and data-driven solutions that would be able to surpass familiar threats[2].

Considering this distinction, this paper presents a new deep learning-based model that is used to categorize the QR codes into two groups: benign and malicious. The primary objectives of the study are to make QR code use more secure as an area of interest by attempting to perform more profound textual readings of URLs, as well as take advantage of the aesthetic qualities of QR code images. The dataset was prepared on the basis of URLs collected online in the free sources like Kaggle and it was transformed into QR images to be used in training and testing. The offered approach focuses on the visual characteristics of QR codes, which introduces a twist to the threat detection. The present work adds to the design and implementation The Convolutional Neural Network (CNN) model is trained on QR image classification, the balanced and labeled dataset of the malicious and benign QR codes is created, and detailed evaluation will be provided. The article identifies the possibility of combining deep learning and cybersecurity tools to decrease the threat of malicious QR codes [3].

1.1. Deep learning in QR code Classification

Deep learning, an interesting area of machine learning has achieved remarkable advances in numerous classification problems, particularly with image and text recognition. It is a good candidate to classify QR codes because of its capability to identify complicated patterns of huge data sets. With QR codes, deep learning has the capability of analyzing the visual characteristics of a QR code and determine its security. CNNs have also become an effective QR code classifier, particularly in cyber security. Since QR codes have become very common in online communications, they have been victims of cybercriminals who use them in advanced phishing attacks. The only issue is in finding a decent way of detecting and analyzing these QR codes which can be rather difficult when incorporated into pictures and in high-traffic systems like email servers. This study emphasizes on CNN to detect QR codes, whereby the principal objective is to differentiate between nonmalicious and malicious codes. Recurring optimizations of the CNN model produced striking prediction accuracy during the initial phases of the model although it experienced overfitting as it becomes more complicated. This brings out the necessity of a well-balanced training process to sustain performance. Finally, the research paper has shown good evidence that CNNs have the potential to enhance email security systems to QR code-based phishing attacks, and it emphasizes the importance of maintaining constant optimization of models to match the increase in cyber threats [4 , 5].

1.2. Image-Based Malware Classification

- QR codes are used to convert features to CNN format.
- These codes have been used with varied success with CNN architectures, and are unable to perform well with certain datasets, or perform better than more conventional algorithms on other datasets, resulting in worse performance. [6].

1.3. Adversarial Attacks and QR Codes

- Familiarize with side effects Side effects are the manipulation of input data to confuse a machine learning model, in particular in image classification. Models may misclassify images due to these attacks and this is extremely dangerous in applications like facial recognition and self driving vehicles where it is crucial to be accurate.
- The purpose of the QR code: QR code is a barcode with two dimensions and can include the information in the form of a URL or a text. These are commonly applied in many ways altogether such as marketing to payment systems. Nevertheless, the vulnerability to malicious attackers is a new issue, since a distorted QR code will deceive the image classification model even though the scanner will still be able to read it.
- Adversarial QR codes: Recent studies have proposed another method to generate an adversarial QR code which can be scanned by devices and yet cause the image classification model to misclassify the image. This is done through incorporation

of side effects on the QR code enabling it to operate normally and conceal evil motives.

- Weight in design: The effectiveness of the conflicting QR codes lies in the fact that they are able to make a compromise in terms of visibility and the misleading classification models. The researchers experimented with the various shapes and intensity of colors of the QR patches to balance it and discovered that circular patches tend to be better opposed to other shapes in terms of adverse influence.
- Implications to Malware Classification: One should learn to understand how useful malware classification systems can be used in relation to QR codes. This knowledge can help researchers to come up with better detection systems to ensure users are not attacked by malicious codes when they realize the power of QR coded attacks.
- Future research directions: The research paper suggests that the study further conducts research on the effect of the length of QR codes on their adverse influence and the enhancement of scanning ranges and angles. These are relevant in order to enhance the security of QR codes applications in realms [7, 8].

1.4. Research Contribution

This paper presents an image based approach. To detect malicious QR codes. As a contrast to analyzing text-based URLs or exploring complicated traffic of the network, we transform the latter into QR code images and feed the CNNs with them. This is a new method whereby the visual aspect of the QR codes is used to detect possible threats. It is a significant move towards cyber security particularly against phishing and malware that may be concealed under QR codes. Our model is efficient and user friendly as it demonstrates high accuracy and can be scanned in real-time [9].

1.5. Research Objectives

The primary objective of the study is to develop a strong and scalable model of classification that will be capable of differentiating between benign and malicious QR codes with only a glance at their visual features. The following are the exact objectives we set: - To obtain a balanced data on QR code images of tagged URLs. The materials used will be as follows: - Constructing and training a CNN model to properly classify these images. - Evaluate the performance of the model based on standard accuracy, precision, recall, and F1 score-Show the feasibility of image-based QR code threat detection when implemented into practice, namely in the mobile and lightweight environments [10].

1.6. Significance of the Study

This research is important because it is the first application of image-based machine learning with the aim of combating the increasing problem of harmful QR codes in our online communications. With QR codes getting more popular in different fields of practice, including finance, healthcare, marketing and education, the possibility of abuse creates a cause of great security concern. The study is already a valid and viable solution as it presents a deep learning-based classification framework capable of identifying threats concealed within QR codes. Having amazing detection accuracy and compatibility with both mobile and embedded systems, it comes out as a useful tool to enhance cyber security both personally and within organizations [11].

1.7. Research Question

Assessment of URLs -With the recent awareness of the growing risks of security that are linked to the embedded QR codes, the present study attempts to answer certain research questions that respond to the scope and objectives of the work. The goal is to explore the efficiency and performance of deep-learning models, in particular, CNN, to identify malicious QR codes. Consequently, the following questions inform the research. Which method can be used to identify the malicious and benign QR codes using the CNN-based method? What is the possible solution to converting URLs into QR codes and analysing them using deep learning methods? The formulation of such questions also allows the study to focus on the technical and practical aspects of the study of QR code maliciousness, and it gives a distinct aspect of the creation of QR code of URLs to aid in the recognition process[12].

2. Related Work

Classification of QRs, particularly the ones obtained as a result of converting URLs, has emerged as a subject of heated research, where the focus has been on enhancing the level of security and accuracy of managing the data. A number of studies pursued the idea of machine learning to successfully categorize QR codes, solve such issues as noise interference, and identify malicious URLs. The following sections will outline some of the important findings of the available literature [13].

2.1. Imporving QR Codes Image

Smart devices present the information to the consumers in a simple and fast manner, fueling AQR codes and mobile marketing. They promote marketing campaigns and aims and enable one to network, interact, persuade and transform wide groups via integrating both offline and online platforms. QR codes have become a ubiquitous element of digital transactions with a quick proliferation in the banking, e-commerce, health care and authentication systems. Attackers however use QR codes to insert malicious web links and malware exposing users to phishing attacks, fraud and unauthorized access of information. In contrast to conventional hyperlinks, harmful QR codes are hard to identify by use prior to scanning and this makes them even more appealing to cybercriminals. This loophole has contributed to more and more attacks involving the QR codes and there is a dire need to have a higher level of security which would be in position to monitor any ill intent in the QR codes. In a bid to solve these issues, this paper suggests a CNN-based classification model of automatically and correctly differentiating between benign and malicious QR codes. The proposed model enhances the security against the QR code-based cyber threats by exploiting the visual and structure features of the QR images to offer a scalable solution. This is not only because the approach is targeted at high detection accuracy, but also to provide efficiency, which is appropriate with real-time mobile applications [14].

2.2. QsecR: Secure QR Code Scanner for Malicious URL Detection

The emergence of malicious URLs that cybercriminals utilize to execute phishing attacks, deliver malicious software and defraud the user has become the largest cybersecurity threat in the modern age and this has been the cause of financial, as well as, identity theft in most instances. Since the QR codes have gained a lot of popularity in encoding URLs, attackers have discovered new means of concealing malicious links in these seemingly innocent codes. The standard QR scanners are usually used based on blacklist detection that is ineffective to identify emerging or latent dangers. To overcome this issue, the recent studies have presented QsecR a secure and privacy-aware Android QR code scanner that employs the novel approaches based on machine learning to provide the methods of static feature classification QsecR is able to detect 39 classes of features, such as blacklist, lexical, host-based, and content-based features, and to achieve good accuracy and precision of 93.50 and 93.80, respectively, with a minimum number of permission requirements making the system both secure and respectful towards the privacy of users. [15].

2.3. An Efficient to Classify the Type of Noises in QR Code using machine learning

It has been demonstrated in previous research that there are various methods to enhance the security and readability of QR codes. They suggested a hybrid scheme to categorize the noise of QR code images, and integrate convolutions, support vector machines (SVM) and logistic fields. Their approach was aimed at enhancing the awareness of noisy QR codes by eliminating the histogram-based tasks and resolving the image distortion. Although the study of theirs has significant contributions to the strength of QR codes in harsh visual conditions, it does not talk directly about the security implication of malicious QR content. Conversely, our study is about transitioning noisy classification to deep learning-based cyber competition in classifying QR codes as malicious or benign. An example of a CNN architecture that we use on a dataset of QR codes retrieved through Kaggle is that each code is associated with a real-world URL with a threat level associated with it. This will help more in our system in order to guard our users against phishing and malicious attacks in the form of malicious QR codes. Thus, our work builds a continuation of the earlier works by focusing on the security of QR codes instead of enhancing readability [13].

2.4. Cyber-Threat for Detection System Using Multi-Model Image Representation

By analyzing network traffic data, the authors suggested a hybrid framework of cyber threat detection of Android applications. Their network converts the network packets to text and image representations, which are Word2vec and SIFT/ORB, respectively. The traffic then undergoes a CNN with machine learning models to decide whether it is a benign or malicious traffic. Despite the amazing accuracy on both CIC-AAGM2017 and CicMalMalroid2020 data sets, this approach will need robust combination of engineering and other processing strengths. Our research, on the other hand, is more succinct and relies on a closer examination of URLs and how to transform them into QR codes and use their visual hierarchy to classify them. This approach does not require either traffic level or packet level analysis but rather aims at the visual complexity and entropy of the QR code to detect possible malware. It provides a competitive performance and ensures that the computational costs are low and the preparation pipeline is simple to use, so our model is suitable in a real-time or embedded scenario [16].

2.5. Evaluating Detection Malicious URL Using Machine Learning

A lot of research has been done addressing the issue of identifying and categorizing malicious URLs. Another interesting article published in Sensors (2022) utilized common machine learning models, including random forests, gradient boosting, and SVM to detect malicious URLs with the help of manually obtained textual features. In as much as this method was promising when it came to accuracy and simplicity in use, it was restricted to text input and it did not consider other forms of representation like visual encoding. Conversely, according to a recent study published on the platform Electronics (2025) the authors explored the methods of quantum machine learning (QML) to classify malicious URLs. The authors compared quantum SVM (QSVM) and CNN (QCNN) with their classical counterparts. They discovered that QSVM was more effective than traditional SVM, and QCNN did not differ significantly with normal CNN. Nonetheless, the study also identified shortcomings of existing quantum machines more so in the aspect of scalability and time run. Unlike these methods, our study brings about the idea of using QR code images in classifying URLs, which is based on their visual characteristics. CNN is used to determine the structural trends of the QR codes, which can help to understand the nature of the URL. Our approach of transforming text-related information into a visual medium gives a different view on URL classification, which, in a traditional text-based or quantum approach is difficult to attain [17].

2.6. Survey of Malicious Software Detection Systems

In the recent times, numerous works have been carried out in the deep learning field to enhance malware and phishing detection. As an example, Alshamrani et al. (2022) developed a vision-based phishing detection scheme, which takes advantage of deep CNNs, and concerns visualization of screenshots of web pages. Their model was based on smart transfer learning to identify malicious websites with the analysis of image characteristics, and it actually excelled in phishing categories. On the same note, Alshehri et al. (2023) created a malware detection system based on blockchain that is adapted to IoT applications, which combines CNNs with blockchain technology to guarantee secure and lightweight threat classification even in low-resource contexts. However, our study is unique since it transforms URLs into QR code images and classifies them using deep learning models. It is a novel methodology that integrates both text and image-based data representation, which offers one of the more effective and powerful methods of identifying malicious URLs. In contrast to the past practices, that only use visual screen shots or network behaviors, our QR code classification plan enhances abstraction and becomes less vulnerable to evasion strategies. Python implementation and the quality of the results we obtained actually demonstrate the feasibility of our suggested approach [18].

2.7. Comparison of Related Studies

Our literature review indicates that there are several strategies meant to enhance the processing of QR code, its detection and classification in different security models. As an illustration, the research papers referred to in Sections 2.1 and 2.3 are aimed at enhancing the clarity of visual representation of QR codes by addressing various image noise types. Although these measures are sure to be helpful in making the system more readable and reliable when it comes to capturing images, they fail to resolve the security risks that are created by malicious QR codes. Conversely, the articles in the parts 2.2 and 2.5 are aimed at detecting malicious content using standard or quantum-enhanced machine learning models. Yet, they are predominantly based on textual URL characteristics, which is why they are not very effective in fighting wily concealed threats of visual formats. Our study, in turn, takes a different direction, transforming URLs into QR code pictures and classifying them with the help of CNN, namely, images. The strategy of visualization has a number of benefits: it does not have the disadvantage of depending on the extraction of features of text, it cannot be evaded, and this approach is applicable in real-time. In our comparative study, we indicate that prior investigations did not offer direct QR based threat assessment or were quite complicated in their pre-processing. The distinctive feature of our approach is the delivery of a lightweight scalable, and efficient framework, integrating deep learning with cybersecurity, which enables the superior identification of unhealthy QR patterns.

Table 1: Comparison of Related Studies

Ref.	Study & Method	Strengths / Limitations	Comparison with Our Work
[14]	Imporving QR Code (CNN + SVM)	Focuse imporiving reading QR Code, not focused on security	Our study focuses on malicious QR detection
[15]	QsecR (Static Feature ML)	Accurate (93.5%), privacy-aware, but text-based only	Our model uses image-based QR analysis for robustness
[13]	Hybrid Noise	Improves noisy QR	We address malicious

	Detection (CNN + Histograms)	readability, not security-focused	threats, not just visual clarity
[16]	Cyber-Threat Detection (Hybrid ML)	High accuracy, but requires complex preprocessing	Our pipeline is simpler and more suitable for real-time use
[17]	Quantum ML (QSVM, QCNN)	Explores novel quantum methods; limited scalability	Our approach is more deployable and resource-efficient

2.8. Limitations of Previous Studies

As much as research conducted in the past provided valuable information regarding the analysis of QR codes and malware detection, it is possible to say that it also had a number of constraints. To start with, much of the studies were based on small or unbalanced data sets, which may undermine the models and reduce their overall fit. Two, several tasks require artisanal or manual engineers that in most instances cannot replicate such intricate shapes and lines in QR code images. Third, some of the works addressed the indirect issues related to the topic of the matter such as noise detection or phishing in general, rather than malicious QR codes. These limitations prove that the previous methods were too narrow or lacked the adequate generalization. This paper on the contrary introduces a CNN-based approach where the images of the QR codes are directly compared thus providing a more accurate and scalable approach to distinguish the benign and malicious QR codes.

3. Research Method

This paper is pragmatic in determining QR code malware through deep learning. The study commences with a balanced data set collection consisting of tagged URLs which indicate safe and malicious links. To achieve quality and availability, the dataset was sourced on the Kaggle platform. The dataset was converted to URLs to QR code image by activating the QR code library in Python. These images were then placed in two folders a structured directory format so that benign code and malicious code is well defined. Although the past researches to identify malicious URLs and QR code were mainly based on the use of string analysis, network traffic, or traditional machine learning techniques, they are usually limited in terms of generalization, scalability, and real-time functionality. The present work presents a novel image-based methodology that transforms URLs into the images of QR code and classifies them with the help of CNN. Our method will take advantage of the graphics layout of QR codes which detects threats effectively unlike traditional methods giving a fresh angle in cyber security. The principal objectives of the study are to make a balanced set of QR code images based on tagged URLs, to design and train a powerful CNN model, and to evaluate its performance with references to such aspects as the precision, the accuracy, the recall and the F1 score.The critical analysis of the research, through red comparison of the existing methods and focusing on the limitations, will prove the practical feasibility and effectiveness of image-based QR code threat detection [19 , 20] .

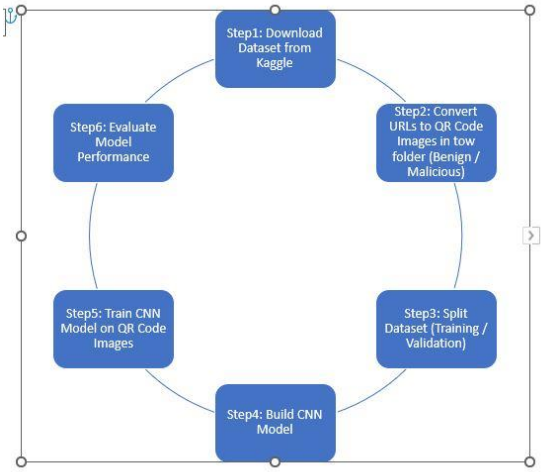

Fig. 1. Steps of research method.

3.1. Download Dataset

The dataset, benign, phishing, malware and exclusions were initially borrowed off the ISCX-WAL-2016 dataset to create URLs. The malware blacklist dataset was used to include additional URLs with phishing and malware to cover more of malicious examples. In order to increase the number of benign URLs, the Git repository data of Faizan was taken. The phishtank and phishstorm databases were used to add additional phishing URLs. The URLs in all these various sources were initially tabulated in individual data frames, after which they were combined into one big dataset by tagging with the URL and the corresponding class and hence consistency as well as uniqueness. The data set in this study is a balanced data of 632,508 unique URLs, half benign (316, 254) and the other half malicious (316,254). It was compiled by combining two publicly available datasets at Kaggle. The initial dataset consists of 450,176 URLs out of which about 77 contain benign and 23 malicious URLs. The second data set consists of 651,191 URLs, which are benign, phishing, exception, and malware. To create a balance, the combined dataset has more malicious

samples of the second source and some benign samples of the first one were deleted. The last data set is in the form of one CSV file with three columns: the URL, a label with either benign or malicious, and a binary result column (where 0 is benign and 1 malicious). The proposed model and evaluation is based on this data set, so the data set applied in this study is not conclusive, but it can be extended in the future. The dataset was created by transforming benign and malicious URLs into QR code images; therefore, the same can be done to any new URLs that will be gathered in the future. [21].

3.2. QR Code Generation

Within our labeled dataset, the URL of each particular data point was translated into a QR code image as per Python QRCODE library. A written script was used to manipulate the data and save the produced QR codes in two separate folders benign and malicious, respectively, according to their labels. The complete time spent to create the QR code was about 18,076 seconds (5 hours). The resulting data had a total size of 583.67 MB, benign folder size was 285.02 MB, and malicious was 298.65 MB. This made it possible to apply image-based classification methods rather than defaulting to the old method of traditional text-based URL analysis [19].

3.3. Model Design and Training

A CNN was specifically designed and trained to recognize QR code images The structure of the model was a set of convolutions and pooling layers followed with dense layers where dropouts were used to evaluate the performance of the model using metrics like the accuracy, the precision, and the F1 score [3, 22].

3.4. Technical Depth

The proposed CNN model was applied on the deep learning system by Kera. The structure is formed by three convolutional blocks with 32, 64, and 128 filters with respective 3×3 kernels and ReLU activation fused, and then it is topped by 2×2 sized max-pooling layers to further reduce the spatial dimensions. To classify the benign and malicious QR code, the extracted feature maps are flattened and input to a dense layer of 128 neurons with ReLU and dropout loss rate of 0.5 is used to reduce overfitting The final output layer is a single neuron with a sigmoid activation function generalization improvement such as data enhancements are shown.

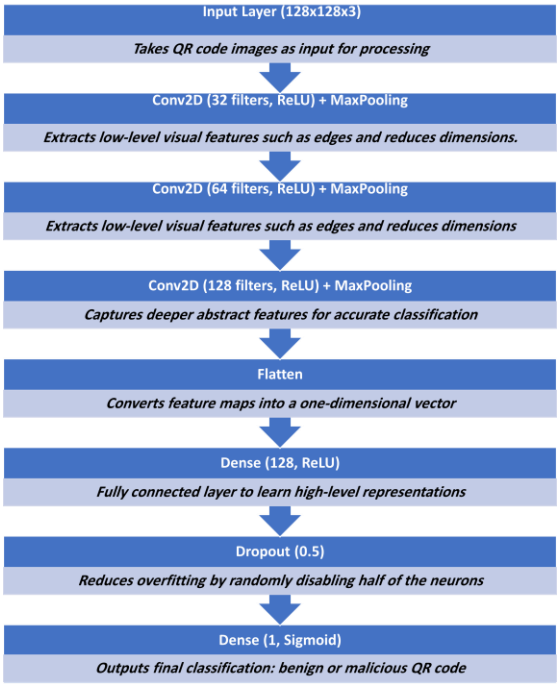

Fig. 2. Technical Depth.

4. Results and Discussion

The sample of the present study is a balanced sample consisting of 632,508 unique URLs which are evenly spread and balanced among benign URLs.

4.1. Training and Validation Accuracy

Training and validation accuracy during the epoch were used in order to monitor the learning progress of the model. The training and the validation accuracies were very high with more than 98 percent during the first epoch. The proximity of these two data points implies that this model learns efficiently and extrapolates well on unknown information. It indicates that the model is not overfitted and can be relied on to accurately work on new QR code images.

4.2. Training and Validation Loss

The values of the losses substantiate the performance of the model, and they were observed with epochs. The loss values are minimal, validation loss is a little less than training loss. The values of the low loss indicate that the model predictions are very close to the real labels. The small gap between training and validation loss is beneficial to state that the model is highly efficient and resistant.

4.3. Evaluation Metrics

We had a further glance at the performance of our CNN model with the classification of QR codes.

To achieve this, we applied some of the measures, which include accuracy, precision, recall, and F1 scores. The findings were encouraging and the model made the following results:

- ✓ Accuracy: 99.96%
- ✓ Precision: 99.92%
- ✓ Recall: 99.91%
- ✓ F1 Score: 99.91%

These data indicate that this model is highly useful in the separation of benign and malicious QR codes as Figure 3 demonstrates.

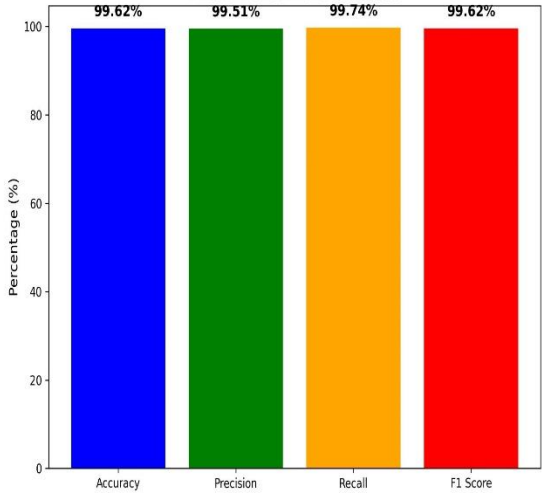

Fig. 3. Evaluation Metrics.

4.4. Confusion Matrix Analysis

Figure 4 indicates the confusion of the model in prediction. It points out real the positives, real negatives, false positives and false negatives:

- The true positives (malicious QR codes that are correctly identified) and true negatives(benign QR codes that are correctly identified) are very high.
- The high rate of correct results and low rate of wrongful results proves the power and validity of the model in practice.

4.5. Results

The findings indicate that the deep learning and CNNs in particular can generate extremely high rates of correct classification of malicious and benign QR codes, and the model can achieve more than 99.9% accuracy on validation through controlled experimental conditions, involving an equal set of malicious and benign QR codes. The results indicate that the model is an effective and good generalizer to untried before QR code images. These are promising results, yet it should be born in mind that there are limitations to such research: the test was run on designed QR codes, but not on the live scanning programs that might introduce certain additional variability.

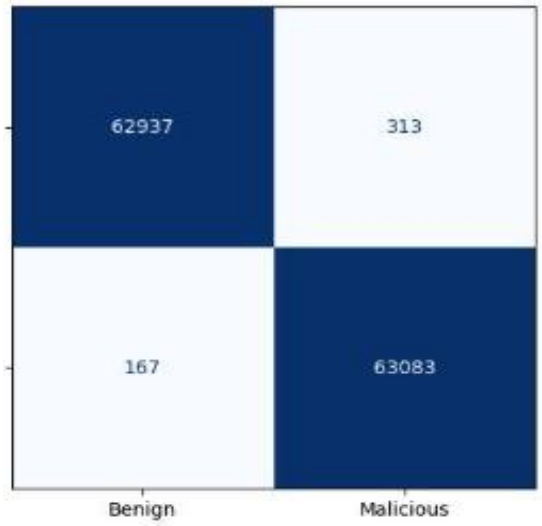

Fig. 4. Confusion Matrix Analysis.

Compared to the previous researches, which used small or biased data sets and classical machine learning methods, our method makes use of a big balanced data set and automated feature learning a gap in the research. In addition, we also conduct quantitative performance assessment as compared to the earlier study which lacked an in-depth analysis, which is to be carried out in future. To better bring our findings into a more topical language, we compare our CNN-based approach with the previous state of the art literature which is described in Section 2. The previous studies, such as Improving QR Code Readability, were mainly on how to enhance the scanning mechanism, but not on the issue of security [2.1]. Similarly, the hybrid noise detection structure [2.3] was devised to classify and thwart visual distortions, and not harmful threats. Even though hybrid ML methods [2.4] were rather precise, they require complicated preprocessing processes, and hence limiting their use to real-time. In addition to this, quantum-based methods [2.5] have introduced novel methods, but these are also affected by the issue of scalability and distribution. Instead, our CNN-based model is capable of not only recognizing malicious QR codes hence 99.9 percent accuracy, a balanced dataset, but also at a more deployable and resource efficient solution with end-to-end pipeline. This comparison will reflect the practical significance and advantages of our proposed approach in relation to the conventional approaches to it, and will also provide a definite point of departure to future research in the sphere of QR code security.

5. Conclusion

Our model, using the strength of CNN, will place QR codes under normal and malicious classification. We selected a dataset and

downloaded it, transforming it to the image format to utilize the spatial tasks, enabling the CNN to learn complicated representations. Our experimental findings demonstrated that our model has a high level of performance, with the accuracy of 99.96 being particularly high when it comes to identifying normal code as well as phishing code. These results indicate that CNNs can be used to detect minute variations within the structure of visual QR codes that are unfamiliar to the human eye. The model however was not so good in detecting malware meaning some threats which are advanced and challenging can still go unnoticed. This limitation is an indication of the fact that more improvements are required, perhaps with the help of data augmentation, multi-model or incorporation of pertinent metadata. Notwithstanding this restriction, CNN model is still a powerful tool in real-time screening of QR codes particularly when it is applied in mobile or cloud-based scanning systems. Finally, the findings of this research support the idea that deep learning, in particular, CNNs are efficient to make sure that QR codes are used safely. Intelligent systems will help make the digital space safer by properly detecting malicious patterns behind QR codes. With the rise in the application of the QR code in several sectors, there is a greater need to upscale our security against cyber-attacks. This study is not only adding value to the QR code, but also provides the foundation of the further development of automated visual threat recognition.

References

[1] M. Sarkhi and S. Mishra, "Detection of QR Code-based cyberattacks using a lightweight deep learning model," Eng. Technol. Appl. Sci. Res., vol. 14, no. 4, pp. 15209–15216, Aug. 2024, doi: 10.48084/etasr.7777.

[2] S. Choudhary and A. Sharma, "Data science approach for malware detection," J. Phys.: Conf. Ser., vol. 1804, no. 1, p. 012196, Feb. 2021, doi: 10.1088/1742-6596/1804/1/012196.

[3] M.-J. Tsai, Y.-C. Lee, and T.-M. Chen, "Implementing deep convolutional neural networks for QR code-based printed source identification," Algorithms, vol. 16, no. 3, p. 160, Mar. 2023, doi: 10.3390/a16030160.

[4] D. O. Do Rosario Lourenco, M. V. H. Sai Sriraj, K. K. Thambi, and V. Ranjan, "Malicious URLs and QR code classification using machine learning and deep learning techniques," in Proc. 3rd Asian Conf. Innov. Technol. (ASIANCON), Ravet, India, Aug. 2023, pp. 1–10, doi: 10.1109/ASIANCON58793.2023.10270125.

[5] J. Ford and H. S. Berry, "Feasibility of machine learning-enhanced detection for QR code images in email-based threats," in Proc. Cyber Awareness Res. Symp. (CARS), Grand Forks, ND, USA, Oct. 2024, pp. 1–9, doi: 10.1109/CARS61786.2024.10778732.

[6] A. Khadilkar and M. Stamp, "Image-based malware classification using QR and Aztec codes," arXiv preprint, Dec. 2024, doi: 10.48550/arXiv.2412.08514.

[7] A. Chindaudom, P. Siritanawan, K. Sumongkayothin, and K. Kotani, "Surreptitious adversarial examples through functioning QR code," J. Imaging, vol. 8, no. 5, p. 122, Apr. 2022, doi: 10.3390/jimaging8050122.

[8] K. Vasilas, E. Makris, C. Pavlatos, and I. Maglogiannis, "NCC—An efficient deep learning architecture for non-coding RNA classification," Technologies, vol. 13, no. 5, p. 196, May 2025, doi: 10.3390/technologies13050196.

[9] Y. M. Latha and B. S. Rao, "Advanced denoising model for QR code images using Hough transformation and convolutional neural networks," Trait. Signal, vol. 40, no. 3, pp. 1243–1249, Jun. 2023, doi: 10.18280/ts.400342.

[10] S.-Y. Yang, H.-C. Jan, C.-Y. Chen, and M.-S. Wang, "CNN-based QR code reading of package for unmanned aerial vehicle," Sensors, vol. 23, no. 10, p. 4707, May 2023, doi: 10.3390/s23104707.

[11] S. Wang, Z. Li, and X. Zhao, "The application of convolutional neural network in malware images classification," in Proc. Int. Conf. Public Art Human Develop. (ICPAHD), Kunming, China, 2022, doi: 10.2991/assehr.k.220110.047.

[12] J. Rasheed, A. B. Wardak, A. M. Abu-Mahfouz, T. Umer, M. Yesiltepe, and S. Waziry, "An efficient machine learning-based model to effectively classify the type of noises in QR code: A hybrid approach," Symmetry, vol. 14, no. 10, p. 2098, Oct. 2022, doi: 10.3390/sym14102098.

[13] A. S. Rafsanjani, N. B. Kamaruddin, H. M. Rusli, and M. Dabbagh, "QsecR: Secure QR code scanner according to a novel malicious URL detection framework," IEEE Access, vol. 11, pp. 92523–92539, 2023, doi: 10.1109/ACCESS.2023.3291811.

[14] F. Ullah et al., "Cyber-threat detection system using a hybrid approach of transfer learning and multi-model image representation," Sensors, vol. 22, no. 15, p. 5883, Aug. 2022, doi: 10.3390/s22155883.

[15] L. Eze, U. B. Chaudhry, and H. Jahankhani, "Quantum-enhanced machine learning for cybersecurity: Evaluating malicious URL detection," Electronics, vol. 14, no. 9, p. 1827, Apr. 2025, doi: 10.3390/electronics14091827.

[16] M. Alshomrani et al., "Survey of transformer-based malicious software detection systems," Electronics, vol. 13, no. 23, p. 4677, Nov. 2024, doi: 10.3390/electronics13234677.

[17] "Python QR code generator," [Online]. Available: https://pypi.org/project/qrcode/ [Accessed: Month Day, Year].

[18] "Benign and malicious URLs dataset," [Online]. Available: https://www.kaggle.com/datasets/samahsadiq/benign-and-malicious-urls/data [Accessed: Month Day, Year].

[19] A. Minocha, A. Goyal, and R. Gandhi, "Recognition of valid QR codes with machine learning," in Proc. IEEE 13th Int. Conf. Commun. Syst. Netw. Technol. (CSNT), Jabalpur, India, Apr. 2024, pp. 724–730, doi: 10.1109/CSNT60213.2024.10546171.

[20] [20] A. Khadilkar and M. Stamp, "Image-based malware classification using QR and Aztec codes," arXiv preprint, Dec. 2024. [Online]. Available: https://doi.org/10.48550/arXiv.2412.08514

[21] "Python QR code generator," [Online]. Available: https://pypi.org/project/qrcode/ [Accessed: Month Day, Year].

[22] "Benign and malicious URLs dataset," [Online]. Available: https://www.kaggle.com/datasets/samahsadiq/benign-and-malicious-urls/data [Accessed: Month Day, Year].

[23] A. Minocha, A. Goyal, and R. Gandhi, "Recognition of valid QR codes with machine learning," in Proc. IEEE 13th Int. Conf. Commun. Syst. Netw. Technol. (CSNT), Jabalpur, India, Apr. 2024, pp. 724–730, doi: 10.1109/CSNT60213.2024.10546171.