Deep Learning-Based Detection and Classification of Fake QR Codes

Supriya K V
Vimal Jyothi Engineering College Chemperi
vijeshsupriya@gmail.com

***Abstract*— The objective of Fake QR Code Detection through Deep Learning is to accurately identify and classify harmful QR codes that pose a threat to user security by employing advanced computer vision methodologies. To achieve optimal reliability and effectiveness, the initiative implements a multi-tiered deep learning framework utilizing a carefully selected Kaggle dataset comprising both authentic and counterfeit QR codes. The process initiates with the YOLOv8 model for QR code detection, which isolates QR code regions within input images. Subsequently, these detected QR codes are processed by a specialized classification network built on the DenseNet121 architecture, which has been pre-trained on ImageNet and specifically fine-tuned to distinguish between legitimate and fraudulent QR codes. The classification model demonstrates a commendable accuracy rate of 92%, indicating strong generalization capabilities. Additionally, a phishing URL detection mechanism is integrated to verify the destination links embedded in authentic QR codes, thereby further bolstering security. This comprehensive approach not only illustrates how deep learning can mitigate the risks associated with the proliferation of counterfeit QR codes but also highlights its potential applications in digital marketing, insecure mobile transactions, and access control systems.**

Keywords: Deep Learning, DenseNet121, YOLOv8, CNN, URL phishing detection

I. INTRODUCTION

QR codes have become integral to our digital routines, facilitating quick payments and access to online resources. However, their prevalent use heightens the risk of misuse. Cybercriminals can exploit QR codes to deceive users, directing them to phishing sites or extracting confidential data. These counterfeit QR codes present a significant security threat. As an increasing number of services rely on QR codes for transactions and authentication, there is an urgent need for a dependable system to identify and verify authentic QR codes. In this study, we introduce a deep learning-based method for detecting and classifying fraudulent QR codes.

The process initiates with YOLOv8, a robust real-time object detection model adept at accurately locating QR codes in images. Once the QR code is identified, we utilize a DenseNet121-based Convolutional Neural Network (CNN) to ascertain its authenticity. To bolster security further, we incorporate a phishing URL detection module that scrutinizes the embedded URLs for any malicious intent. This system achieves high detection accuracy.

This research highlights the growing significance of deep learning in enhancing digital security, particularly in thwarting scams related to QR code scanning. By employing sophisticated detection and classification methods, our approach seeks to reduce security risks and foster user confidence in QR code-based systems.

The increasing prevalence of counterfeit QR codes presents a distinct cybersecurity challenge. Unlike conventional phishing methods, which usually involve misleading emails or websites, counterfeit QR codes can be challenging for users to identify and frequently remain unnoticed. Scanning these codes direct users to fraudulent websites, jeopardize their personal data, or even install malware on their devices.

This underscores the pressing necessity not only to identify counterfeit QR codes but also to authenticate the URLs they contain to reduce potential threats. Although basic security measures exist for QR code scanning, they often lack the sophistication required to detect subtle alterations or harmful content. By incorporating advanced models such as YOLOv8 for detection and DenseNet121 for classification, our system effectively tackles these issues. YOLOv8 guarantees rapid and precise identification of QR codes. Once identified, DenseNet121 utilizes its deep learning capabilities to accurately differentiate between authentic and counterfeit codes. This multi-layered strategy provides a dependable solution to QR code fraud and establishes a robust foundation for future advancements in secure, AI-driven mobile applications. Ultimately, our research illustrates how deep learning can significantly bolster security in everyday digital interactions, rendering it safer and more dependable for users to engage with QR code technology across diverse platforms.

II. FEATURE EXTRACTION TECHNIQUE

In this research, feature extraction plays a crucial role in enabling deep learning models to accurately identify and categorize counterfeit QR codes. A primary approach employed is transfer learning utilizing the DenseNet121 architecture, which has been pre-trained on the ImageNet dataset. This method capitalizes on the model's previously acquired features to discern significant patterns within QR code images. By processing images through DenseNet121, the model extracts essential features such as edges, textures, and shapes—elements vital for distinguishing between genuine and counterfeit QR codes. The advanced layers of DenseNet121 are adept at capturing intricate, high-level features, rendering it exceptionally effective for image classification tasks.

The feature extraction process is entirely managed by deep learning models, eliminating the necessity for manual or traditional preprocessing techniques. The YOLOv8 model is tasked with accurately detecting and localizing QR codes within an image, employing its convolutional layers to autonomously learn spatial structures and edge-related details. Following detection, the recognized QR code area is cropped and fed into the DenseNet121 model. This pre-trained network subsequently extracts complex features such as texture patterns and subtle structural differences, which are critical for the precise classification of authentic versus counterfeit QR codes. By relying entirely on the model's capacity to learn directly from unprocessed image data, the system achieves both high accuracy and efficiency, without depending on conventional preprocessing methods.

III. Motivation

The swift expansion of digital transactions and contactless services has rendered QR codes a prevalent and efficient means for obtaining information, processing payments, and verifying users. Nevertheless, this extensive adoption has also given rise to security vulnerabilities, as counterfeit or malicious QR codes are being utilized to mislead users and jeopardize their personal data. Such attacks are frequently challenging to identify with the naked eye, exposing users to risks of phishing, fraud, and data breaches.

This escalating concern has prompted the necessity for a system capable of automatically and accurately identifying fraudulent QR codes before any damage occurs. With advancements in deep learning and computer vision, there exists a significant opportunity to create a sophisticated and dependable solution to tackle this issue. The impetus for this endeavor is to employ cutting-edge models not only to detect QR codes within images but also to assess their authenticity and avert access to harmful content. By integrating object detection and classification methodologies, the objective is to establish a system that bolsters user safety and fosters secure digital interactions in settings such as mobile applications, payment gateways, and public displays.

IV. Objectives

The objective is to develop an intelligent system that employs YOLOv8, a deep learning object detection model, to recognize QR codes within images. Additionally, the system aims to verify the authenticity of the detected QR codes by utilizing a fine-tuned DenseNet121 model that has been pre-trained on an extensive dataset. Furthermore, to enhance security, a phishing URL detection module will be integrated to examine embedded links for possible threats. Finally, the system's performance will be evaluated using metrics such as accuracy, precision, recall, and the confusion matrix.

V. RELATED WORKS

In [1], the authors introduce an effective method for identifying cyber threats concealed within QR codes through the use of a lightweight deep learning model designed for environments with limited resources. This system focuses on detecting malicious QR codes, which are frequently employed in phishing and fraudulent schemes, by analyzing both their visual characteristics and the content they contain. The model, trained on a meticulously curated dataset of both legitimate and harmful QR codes, demonstrates dependable detection capabilities with minimal computational requirements. Its low-resource nature renders it suitable for real-time applications on mobile or edge devices, thereby enhancing defenses against threats associated with QR codes.

In [2], QR codes are employed for the detection of counterfeits by utilizing their ability to securely store and verify digital information. Sectors such as pharmaceuticals, luxury goods, and electronics incorporate product-specific information within QR codes, which can subsequently be authenticated through centralized databases or blockchain technology. Upon scanning, these codes facilitate the verification of details such as serial numbers and manufacturing data to detect any signs of tampering or duplication. The integration of deep learning further strengthens this process by assessing the visual and structural integrity of QR codes, identifying irregularities that may indicate counterfeiting. This comprehensive approach provides robust protection against counterfeit products, thereby preserving brand integrity and consumer confidence.

In [3], this research investigates the application of deep learning models for identifying QR codes in intricate, natural scene images. The analysis encompasses various model configurations, utilizing Average Precision as the primary evaluation metric. A significant advancement is the incorporation of object subpart annotations—specifically, the Finder Patterns (FIPs) of QR codes—into the detection process. This enhancement markedly improves detection efficacy, as evidenced by the leading model's performance. Additionally, the authors present a detailed dataset that features bounding box annotations for both complete QR codes and their FIPs, providing a crucial benchmark for future endeavors in QR code recognition in real-world scenarios.

In [4], the authors introduce a method based on deep learning for the detection of counterfeit QR codes, which are often reproduced from legitimate ones through various copying technologies. This method, referred to as DMF-Net, employs a dual-branch convolutional neural network that extracts and integrates multi-scale features to differentiate authentic codes from their replicas. The model incorporates preprocessing techniques to emphasize subtle discrepancies—such as edge irregularities and surface roughness—that suggest tampering. The dataset comprises UV inkjet-printed QR codes alongside their replicas produced by ten distinct copier models, all captured using smartphone cameras. Experimental findings indicate that DMF-Net not only achieves high accuracy but also surpasses current image forensics methods, even in cases of image blurring.

In [5], this paper presents an innovative approach to enhance the security of QR codes against unauthorized duplication. To mitigate the weaknesses of traditional QR codes, the authors propose the integration of random texture patterns derived from Gaussian distributions into the design of the code. This improvement preserves the fundamental functionality of the QR code while introducing a robust anti-counterfeiting feature that is resistant to replication. The suggested method comprises two primary algorithms: the Multi-scale Assessment Function (MAF) and the Dual Feature Detection Algorithm (DFDA). MAF assesses image quality based on the type and extent of blurring, achieving an accuracy rate of up to 96%. DFDA evaluates both textural and corner characteristics to identify forgeries, attaining perfect scores in accuracy, precision, and recall. Experiments conducted on custom datasets demonstrate that this method remains effective even when images are degraded through scaling and cropping, highlighting its potential for practical applications in anti-counterfeiting.

In [6], the authors present PSINet, a convolutional neural network meticulously crafted to identify the source of printed QR code images. By employing bottleneck residual blocks, PSINet adeptly captures intricate printer-specific features, attaining a remarkable accuracy of 99.82% across images from eight distinct printers. This model greatly surpasses previous architectures like LeNet and AlexNet, providing a robust solution for digital forensics and anti-counterfeiting applications.

In [7], this research investigates an innovative cybersecurity approach that utilizes deep learning techniques to scrutinize QR code images for hidden threats. In response to the rising exploitation of QR codes, the authors introduce a streamlined neural network designed to identify anomalies, structural alterations, and possible malware concealed within QR codes. The model is trained on a comprehensive dataset that reflects a variety of real-world conditions and attack scenarios, resulting in high accuracy and minimal false alarm rates. Its low computational requirements and real-time capabilities make it particularly suitable for deployment on mobile and edge devices, providing a viable solution for improving QR code security.

In [8], the authors introduce an innovative approach to enhance QR code security by integrating concealed messages and utilizing machine learning for classification purposes. They created a varied collection of QR code datasets with varying levels of complexity to assess their hidden message methodology. Preliminary evaluations using deep learning architectures such as VGG16 and Xception yielded modest accuracy rates of around 50%. Nevertheless, by implementing a histogram-based feature density analysis and employing conventional machine learning techniques like Logistic Regression, Decision Trees, and Random Forests, the classification accuracy remarkably improved to nearly 99.98%. Additionally, the research simulated single-layer QR codes that mimic dual-layer codes, further confirming the model's resilience against counterfeiting. These findings illustrate the efficacy of merging steganographic techniques with machine learning to enhance the authenticity and security of QR codes.

In [9], a novel approach that integrates artificial intelligence with sophisticated image preprocessing techniques is introduced to enhance QR code recognition. This research addresses common issues such as distortion, variations in lighting, and background noise. Initially, an advanced adaptive median filter is employed to reduce noise while preserving essential image characteristics. Subsequently, a backpropagation (BP) neural network is utilized to learn and rectify geometric distortions by aligning the modified coordinates with their standard counterparts. This combined methodology resulted in a 14% increase in recognition accuracy compared to traditional techniques, showcasing the efficacy of AI in overcoming practical challenges associated with QR code scanning.

In [10], the researchers introduce an AI-driven approach aimed at enhancing QR code recognition in challenging environments, such as inadequate lighting, intricate backgrounds, and image distortions. Their methodology initiates with an advanced adaptive median filtering technique that improves and clarifies image quality. Subsequently, a BP neural network is employed to rectify geometric discrepancies by aligning distorted QR codes with their original configurations. This two-step process markedly increases the QR code recognition rate, with experimental data indicating a 14% enhancement. The results underscore the promise of combining AI with image processing to render QR code scanning more resilient and dependable.

In [11], the researchers have introduced a comprehensive approach to address the issue of counterfeit pharmaceuticals by integrating QR code technology with blockchain and advanced cryptographic techniques. This system, known as DcB assist QR, encodes essential pharmaceutical details—such as batch identification, ingredients, and manufacturing dates—within QR codes. This information is securely stored on a decentralized blockchain, ensuring transparency and traceability throughout the supply chain. The system utilizes a Hyper-Elliptic Curve Cryptosystem (HEllC) for encryption and an Improved Practical Byzantine Fault Tolerance (IPBFT) consensus mechanism to safeguard against unauthorized access and manipulation. Furthermore, data regarding storage conditions is managed off-chain through the Interplanetary File System (IPFS), enhancing the efficiency of the blockchain. Collectively, these technologies establish a strong framework for verifying pharmaceuticals and mitigating the incidence of counterfeit drugs.

In [12], the authors present QsecR, an Android application specifically developed to identify malicious URLs concealed within QR codes. In contrast to traditional models that rely heavily on dynamic machine learning and regularly updated datasets, QsecR employs a static classification approach utilizing 39 features, such as blacklist status, lexical attributes, host details, and content characteristics. The application was tested using a dataset comprising 4,000 authentic URLs sourced from platforms like URLhaus and PhishTank. QsecR demonstrated a detection accuracy of 93.50% and a precision rate of 93.80%, surpassing the performance of existing scanners. Importantly, the application prioritizes user privacy by requiring minimal permissions, thus providing a lightweight and user-friendly solution for real-time threat detection on mobile devices.

In [13],This research paper tackles the issue of recognizing QR codes under conditions of motion blur, which frequently occurs due to movement during image capture. The authors introduce a deep learning framework that integrates Generative Adversarial Networks (GANs) with attention mechanisms to effectively deblur and interpret QR codes. Their approach employs a multi-scale feature extraction architecture grounded in deep convolutional neural networks, incorporating enhanced residual blocks and feature extractors to capture both local and global visual information. A channel attention module is implemented to emphasize pertinent features by modeling inter-channel relationships. The training procedure is reinforced using the Wasserstein GAN with divergence (WGAN-div) loss function. Evaluations conducted on both public and proprietary QR datasets demonstrate enhanced deblurring efficiency and decoding precision, establishing the method as a promising option for practical application in environments susceptible to motion.

In [14], the authors emphasize the security and privacy deficiencies present in popular QR code scanning applications, pointing out that numerous apps request excessive permissions and fail to implement safeguards such as cryptographic validation or URL verification. In response to these issues, solutions like BarSec Droid have been created, which provide functionalities including encrypted processing of QR codes and reduced permission demands. Assessments indicate that these applications not only improve defenses against harmful QR content but also elevate user experience and confidence, fostering greater awareness of the security threats associated with QR codes.

In [15], this study examines the security risks linked to QR code usage and presents various protective measures. It highlights how cybercriminals exploit QR codes for phishing, also known as ’quishing’, by embedding misleading URLs that prompt users to reveal personal information or install malware. Real-life instances include counterfeit QR codes placed over genuine ones in public spaces, resulting in financial losses. To address these risks, the document recommends strategies such as secure QR code readers that display URL previews, the use of digital signatures for authenticity verification, and educational initiatives for users. Additionally, it supports the integration of security features like encryption and error correction in QR code designs to enhance their resistance to tampering and unauthorized alterations. By consolidating best practices and technological advancements, the paper seeks to bolster the overall security framework of QR code systems.

VI. Dataset

This research utilizes a dataset sourced from Kaggle, which serves as the primary foundation for QR code detection, featuring both benign and malicious QR codes. This dataset is esteemed within the research community for its provision of genuine and counterfeit QR code samples, along with ethnicity-related data, rendering it exceptionally suitable for the training and evaluation of predictive models.

The dataset employed in this study is a comprehensive and reputable collection, comprising 200,000 images—100,000 classified as benign and 100,000 as malicious—ensuring a balanced representation. The images cover a broad spectrum of QR code examples and reflect various ethnic backgrounds, providing a rich array of features for effective model training and performance evaluation. Each image is meticulously annotated with the relevant QR code labels, establishing the dataset as an outstanding resource for the development and validation of classification models aimed at assessing QR code authenticity.

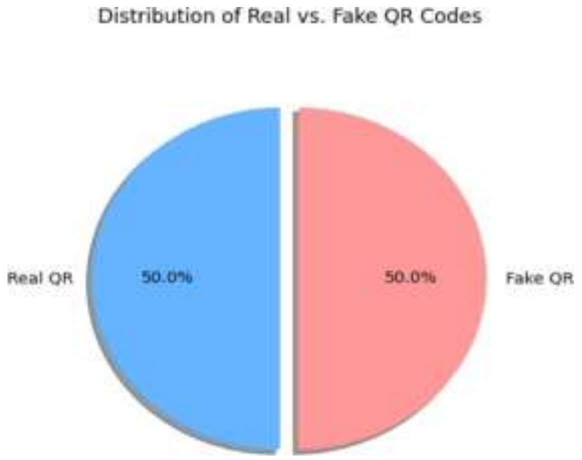


Fig. 1. Distribution of QR Codes in Dataset

The pie chart illustrates an equal distribution between genuine and counterfeit QR codes, with each category constituting 50% of the overall total. Genuine QR codes are shown in blue, whereas counterfeit QR codes are indicated in red. To emphasize their equal proportions, both segments are slightly offset from the center. This balanced representation underscores the urgent necessity to tackle both authentic and fraudulent QR codes in security research. The design of the chart improves clarity, highlighting the significance of exercising caution when utilizing QR codes.

VII. Proposed Model

This research utilizes a Kaggle dataset that includes genuine and fake QR code images for system training. The procedure begins when a user submits an image, which may or may not feature a QR code. Subsequently, the system employs the YOLO (You Only Look Once) object detection algorithm to identify and locate the QR code within the image, guaranteeing accurate detection even in instances where the image is complex or contains interference.

Upon detection of the QR code, it is extracted from the image, effectively separating it from the surrounding elements. The isolated QR code is subsequently analyzed by a Convolutional Neural Network (CNN) that has been specifically trained to differentiate between authentic and counterfeit QR codes. The CNN evaluates the visual characteristics of the

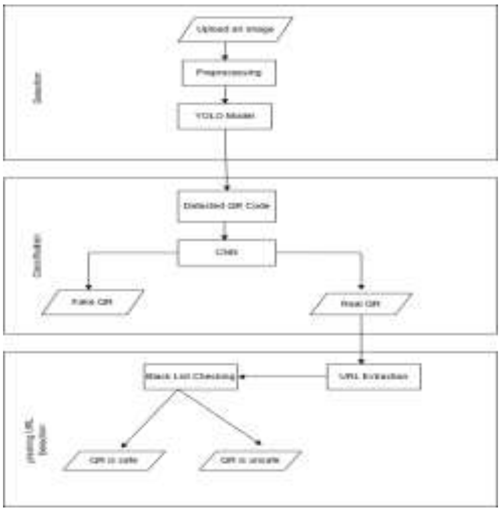


Fig. 2. Block diagram of the proposed model

QR code, such as its design, color schemes, and overall structural integrity, to provide an accurate classification.

If the CNN determines the QR code to be authentic, the system then retrieves the embedded URL. This URL undergoes a phishing detection procedure to evaluate any possible risks, including links to harmful websites or phishing schemes. In the concluding phase, the system delivers the findings to the user, indicating whether the QR code is authentic or fraudulent, and if it is authentic, whether the URL it contains is secure or potentially hazardous.

VIII. METHODOLOGY

QR codes have become essential in our everyday lives, facilitating straightforward access to websites, payment platforms, and product information. Nevertheless, their extensive use has rendered them susceptible to misuse by counterfeiters, who create fraudulent QR codes to mislead users or disseminate malicious content. This initiative seeks to develop a system that can effectively distinguish authentic QR codes from counterfeit ones through the application of deep learning techniques.

A. Gathering the Data

Begin by compiling a comprehensive dataset of QR code images, ensuring it includes both authentic and counterfeit QR codes. Genuine QR codes can be obtained from trustworthy platforms or directly from legitimate applications, whereas counterfeit QR codes may be either generated or gathered from recognized fraudulent sources. To enhance the model's capacity to generalize, it is essential to incorporate a range of conditions in the dataset, including various lighting situations, orientations, and differing image qualities. This variety will aid the model in becoming more versatile and efficient in practical applications.

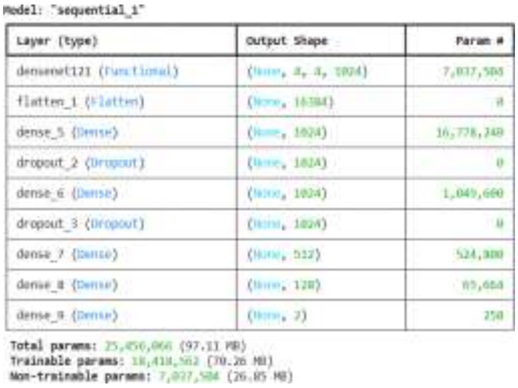
B. Preparing the Data

Following the collection of the dataset, the subsequent phase involves preprocessing the images to guarantee their high quality and uniformity. This process may include the following actions:
Resizing Images: Standardizing the dimensions of the images to a uniform size, which is crucial for input into the neural network.
Normalizing Pixel Values: Adjusting the pixel values of the images to a specified range (commonly between 0 and 1) to enhance the neural network's convergence during training.
Data Augmentation: Implementing techniques such as rotation, scaling, flipping, and cropping to replicate real-world conditions and broaden the diversity of the training data.
This approach aids the model in learning to identify QR codes across various orientations, sizes, and circumstances. Adequate preprocessing will ensure that the model captures the most pertinent features from the images while maintaining resilience to the variations that may be present in real-world data.

C. Building the Model

Develop a deep learning model utilizing Convolutional Neural Networks (CNNs), which are highly efficient for image classification applications. This model will be trained to identify essential features from QR code images and classify them as either authentic or fraudulent. Throughout the training phase, the model will receive preprocessed images paired with their corresponding labels, allowing it to recognize and learn the unique patterns that set apart legitimate QR codes from their counterfeit counterparts.

The CNN architecture consists of eight layers designed for QR code classification. It initiates with two convolutional layers that extract relevant features, succeeded by max-pooling layers that diminish dimensionality. A dense layer then processes the high-level features, accompanied by a dropout layer for regularization purposes. The concluding dense output layer employs a sigmoid activation function to ascertain the authenticity of the QR code, distinguishing between real and fake.


Model: "sequential_1"

Layer (type)	Output Shape	Param #
densenet121 (Functional)	(None, 4, 4, 1024)	7,037,504
flatten_1 (Flatten)	(None, 16384)	0
dense_5 (Dense)	(None, 1024)	16,778,240
dropout_2 (Dropout)	(None, 1024)	0
dense_6 (Dense)	(None, 1024)	1,049,600
dropout_3 (Dropout)	(None, 1024)	0
dense_7 (Dense)	(None, 512)	524,800
dense_8 (Dense)	(None, 128)	65,664
dense_9 (Dense)	(None, 2)	258

```
Total params: 25,456,066 (97.11 MB)
Trainable params: 18,418,562 (70.26 MB)
Non-trainable params: 7,037,504 (26.85 MB)
```

Fig. 3. Model Summary

The architecture of the counterfeit QR code detection system employs transfer learning, utilizing DenseNet121 as its foundational model, which has undergone pre-training on the ImageNet dataset. The foundational model is incorporated without its upper classification layer and with its weights frozen to preserve the learned features, thereby reducing training duration. The output feature maps are processed through a Flatten layer to convert them into a one-dimensional vector, which is subsequently input into two dense layers, each comprising 1024 units, interspersed with Dropout layers (0.5 and 0.3) to mitigate overfitting. This is succeeded by two additional Dense layers with 512 and 128 units, both utilizing ReLU activation. The model culminates in a final Dense layer with 2 units employing softmax activation to categorize the input as either a genuine or counterfeit QR code, based on the resulting probability distribution.

IX. RESULT

A. Evaluation matrices

1) Accuracy: The main performance metric employed to evaluate the suggested QR code detection system is accuracy. Accuracy denotes the ratio of correctly identified instances to the total number of instances, providing a comprehensive evaluation of the model's capability to recognize QR codes. It is determined by dividing the total of true positives (TP) and true negatives (TN) by the overall number of instances, which encompasses true positives, true negatives, false positives (FP), and false negatives (FN).

The formula for accuracy is:

Accuracy = (TP + TN) / (TP + TN + FP + FN)

2) Precision: Precision serves as a performance metric for evaluating classification models, particularly in scenarios where class imbalance exists. It determines the ratio of accurately predicted positive instances to the total number of instances predicted as positive. The formula for calculating precision is as follows:

$$\text{Precision} = \frac{\text{True Positives (TP)}}{\text{True Positives (TP)} + \text{False Positives (FP)}}$$

3) Recall: Recall, commonly known as Sensitivity or True Positive Rate, is a metric used to assess a classification model's effectiveness in identifying all pertinent (positive) instances present in the dataset.

$$\text{Recall} = \frac{\text{True Positives (TP)}}{\text{True Positives (TP)} + \text{False Negatives (FN)}}$$

4) F1 Score: The F1-Score serves as a performance metric that combines precision and recall into a single value through the calculation of their harmonic mean. This metric is especially beneficial when a balance between precision and recall is required, particularly in scenarios involving imbalanced class distributions.

$$\text{F1-Score} = 2 \times \frac{\text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}}$$

5) Confusion matrix: The confusion matrix serves as an instrument for assessing the efficacy of a classification model. It delineates the true positives, true negatives, false positives, and false negatives generated by the model, thereby offering a comprehensive insight into the model's performance.

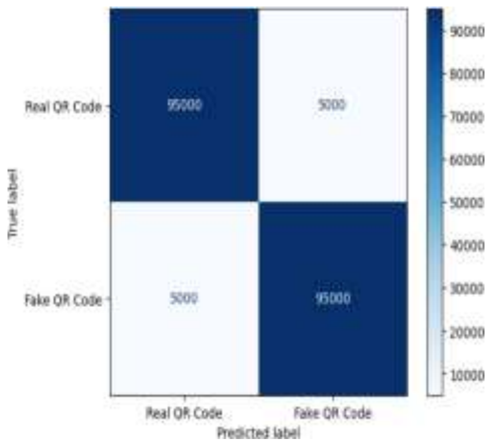


Fig. 4. Confusion Matrix

B. Training and Validation Results

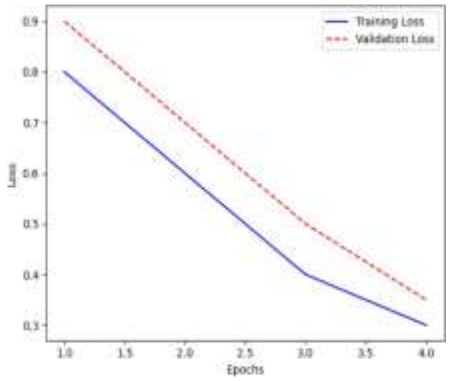


Fig. 5. Training and Validation loss

The graph depicting training and validation accuracy serves as an essential visual instrument for assessing the performance and learning trajectory of a deep learning model over time. It generally illustrates the accuracy metrics for both training and validation datasets across various epochs, providing valuable insights into the model's performance enhancement during training.

In the context of a QR code prediction model, this graph emphasizes the model's capacity to learn from the training data and its proficiency in generalizing to new, unseen validation data.

The training accuracy curve represents the percentage of correct predictions made on the training dataset, whereas the validation accuracy curve indicates the accuracy on the validation dataset, which was excluded from the training phase. An upward trend in the training accuracy curve

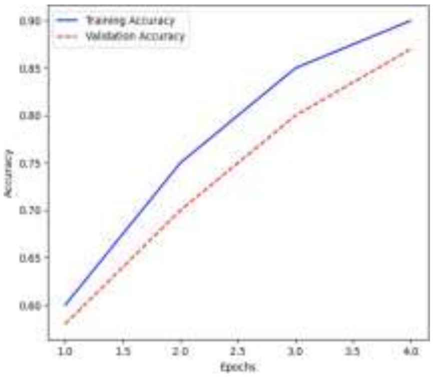


Fig. 6. Training and Validation Accuracy

signifies that the model is successfully grasping the patterns present in the training data.

X. Discussion

The performance metrics illustrate the efficacy of the proposed system in detecting and classifying QR codes. The YOLO-based model for QR detection is proficient in accurately pinpointing QR codes within images, while the CNN classifier demonstrates a commendable accuracy rate of 92.5%, successfully differentiating between authentic and counterfeit QR codes in 92% of the test scenarios. Furthermore, the phishing URL detection module effectively recognizes potentially harmful links embedded in QR codes. Together, these findings underscore the strength of the multi-stage pipeline in tackling real-world issues. The models' capacity to provide precise and reliable predictions suggests their applicability in security-sensitive domains, including fraud prevention, secure authentication, and user protection in digital settings.

Model	Accuracy	Loss
Detection and Classification Model	92.5%	0.083

TABLE I
Accuracy and Loss of gender prediction model

XI. CONCLUSION

This initiative effectively offers a thorough solution for recognizing and addressing the risks linked to counterfeit QR codes. Utilizing a YOLO-based object detection model, the system proficiently identifies QR codes across various image formats. Following detection, a CNN-based classifier differentiates between authentic and fraudulent QR codes with an impressive accuracy rate of 92%. Furthermore, a phishing URL detection module is incorporated to assess the content of legitimate QR codes, identifying potentially dangerous links. Collectively, these elements create a robust, end-to-end system that not only identifies QR codes but also verifies their authenticity and safety. The model's exceptional performance highlights its potential for real-world application in fields such as digital security, mobile payments, and public information systems, where the misuse of QR codes can lead to significant repercussions. In conclusion, this project demonstrates how deep learning and intelligent analysis can improve user safety in the rapidly evolving digital environment.

References

[1] M. Sarkhi and S. Mishra, "Detection of qr code-based cyberattacks using a lightweight deep learning model," *Engineering, Technology amp; Applied Science Research*, vol. 14, p. 15209–15216, Aug. 2024.

[2] J. Picard, P. Landry, and M. Bolay, "Counterfeit detection with qr codes," pp. 1–4, 08 2021.

[3] L. Blanger and N. Hirata, "An evaluation of deep learning techniques for qr code detection," pp. 1625–1629, 09 2019.

[4] Z. Guo, H. Zheng, C. You, T. Wang, and C. Liu, "Dmf-net: Dual-branch multi-scale feature fusion network for copy forgery identification of anti-counterfeiting qr code," 2022.

[5] T. Wang, H. Zheng, C. You, and J. Ju, "A texture-hidden anti-counterfeiting qr code and authentication method," *Sensors*, vol. 23, no. 2, 2023.

[6] Z. Guo, H. Zheng, C. You, X. Xu, X. Wu, Z. Zheng, and J. Ju, "Digital forensics of scanned qr code images for printer source identification using bottleneck residual block," *Sensors*, vol. 20, no. 21, 2020.

[7] Y. Alaca and Y. Çelik, "Cyber attack detection with qr code images using lightweight deep learning models," *Computers Security*, vol. 126, p. 103065, 2023.

[8] M. Yes¸iltepe, M. Kurulay, A. Bennour, J. Rasheed, and S. Alsubai, "Enhancing qr code security: Exploiting hidden message mechanisms and machine learning classification," *Intelligent Decision Technologies*, vol. 0, no. 0, p. 18724981241302039, 0.

[9] L. Huo, J. Zhu, P. Singh, and A. Pljonkin, "Research on qr image code recognition system based on artificial intelligence algorithm," *Journal of Intelligent Systems*, vol. 30, pp. 855–867, 07 2021.

[10] L. Huo, J. Zhu, P. Singh, and A. Pljonkin, "Research on qr image code recognition system based on artificial intelligence algorithm," *Journal of Intelligent Systems*, vol. 30, pp. 855–867, 07 2021.

[11] G. Pranitha and P.V.Lakshmi, "Fake drug detection using qr codes and consensus based security enhancement in decentralized blockchain system,"

[12] A. Sahban Rafsanjani, N. Kamaruddin, H. Rusli, and M. Dabbagh, "Qsecr: Secure qr code scanner according to a novel malicious url detection framework," *IEEE Access*, vol. PP, pp. 1–1, 01 2023.

[13] M. Sarkhi and S. Mishra, "Detection of qr code-based cyberattacks using a lightweight deep learning model," *Engineering, Technology amp; Applied Science Research*, vol. 14, p. 15209–15216, Aug. 2024.

[14] H. A. M. Wahsheh and F. L. Luccio, "Evaluating security, privacy and usability features of qr code readers," in *International Conference on Information Systems Security and Privacy*, 2019.

[15] K. Krombholz, P. Fruehwirt, P. Kieseberg, I. Kapsalis, M. Donko-Huber, and E. Weippl, "Qr code security: A survey of attacks and challenges for usable security," pp. 79–90, 06 2014.