Scientific Research Publishing

International Journal of Intelligence Science, 2024, 14, 49-57
https://www.scirp.org/journal/ijis
ISSN Online: 2163-0356
ISSN Print: 2163-0283

Enhancing Security in QR Code Technology Using AI: Exploration and Mitigation Strategies*

Saranya Vaithilingam, Santhosh Aradhya Mohan Shankar

Department of Information Technology, University of the Cumberlands, Williamsburg, KY, USA
Email: SaraVaithilingam@gmail.com, S.aradhyams@gmail.com

How to cite this paper: Vaithilingam, S. and Shankar, S.A.M. (2024) Enhancing Security in QR Code Technology Using AI: Exploration and Mitigation Strategies. *International Journal of Intelligence Science*, **14**, 49-57.
https://doi.org/10.4236/ijis.2024.142003

Received: January 23, 2024
Accepted: March 23, 2024
Published: March 26, 2024

Abstract

The widespread adoption of QR codes has revolutionized various industries, streamlined transactions and improved inventory management. However, this increased reliance on QR code technology also exposes it to potential security risks that malicious actors can exploit. QR code Phishing, or "Quishing", is a type of phishing attack that leverages QR codes to deceive individuals into visiting malicious websites or downloading harmful software. These attacks can be particularly effective due to the growing popularity and trust in QR codes. This paper examines the importance of enhancing the security of QR codes through the utilization of artificial intelligence (AI). The abstract investigates the integration of AI methods for identifying and mitigating security threats associated with QR code usage. By assessing the current state of QR code security and evaluating the effectiveness of AI-driven solutions, this research aims to propose comprehensive strategies for strengthening QR code technology's resilience. The study contributes to discussions on secure data encoding and retrieval, providing valuable insights into the evolving synergy between QR codes and AI for the advancement of secure digital communication.

Keywords

Artificial Intelligence, Cyber Security, QR Codes, Quishing, AI Framework, Machine Learning, AI-Enhanced Security

1. Introduction

Quick Response (QR) codes represent a form of barcode that is comprised of

*"Enhancing QR Code Security with AI: Exploring Mitigation Strategies" delves into how artificial intelligence can strengthen QR code technology security. It explores strategies to identify and address vulnerabilities through AI-driven solutions, aiming to fortify the robustness of QR code systems.

black and white squares. Users can quickly access information by simply scanning the code with a smartphone camera, eliminating the need to manually type in URLs, Applications, Coupons, Contact details, text messages, and other information making them suitable for a wide range of applications. Their convenience has led to widespread adoption in areas like marketing, ticketing, contactless payments, connecting to an open Wi-Fi network and more. These attributes have led to innovative marketing strategies that effectively communicate sustainability information to consumers [1].

A Quick Response Code has several elements that make its generation and decoding very easy and on-the fly. Due to its low cost, large amount of stored information, and the ability to scan without attaching to a database, the two-dimensional code, they are becoming increasingly popular for a wide range of applications [2]. It consists of Position Markers, Timing Patterns, Format of QR Code, Data in Modules, as well as a Version of the QR code (**Figure 1**).

However, their growing popularity has also made them susceptible to security threats.

2. Problem Statement

It has been found that consumers' attitudes toward and intentions to scan QR codes are significantly influenced by their perceptions of their ease of use and usefulness. The use of QR codes by cybercriminals can spread malware to victims' devices or lead them to phishing websites that steal their credentials, personal information or other sensitive information. Phone calls, text messages, and forcing the device to connect to a specific Wi-Fi network are some of the methods of attack that can be launched with QR codes.

2.1. Quishing

There are usually signs that can help identify a phishing message, such as typographical errors or incorrect domain names, which make them easier to spot.

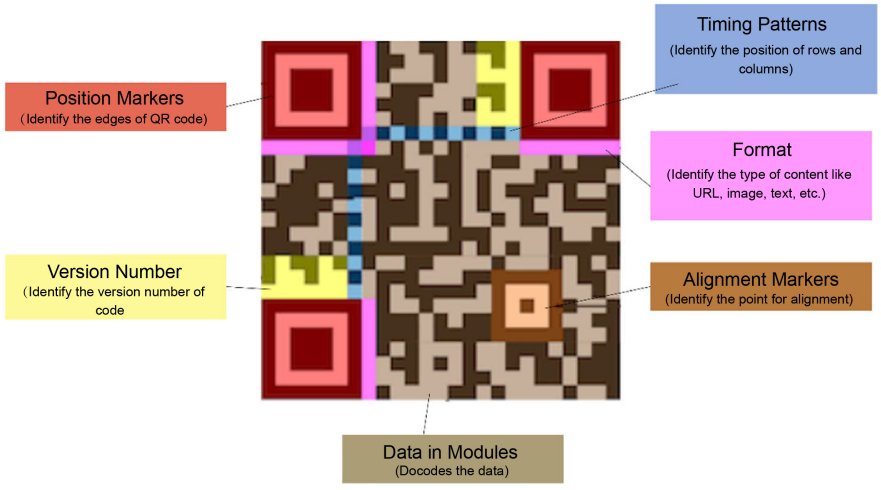

Figure 1. Elements of a quick response code [2].

However, QR codes lack these identifying features, making QR code-based attacks more likely to succeed compared to email-based attacks [3].

One such threat is "Quishing", which is short for QR code Phishing. Quishing attacks use QR codes to deceive users into visiting malicious websites or downloading harmful content, akin to traditional phishing attacks but using QR codes as bait. This type of attack can be particularly effective since QR codes are often trusted by users and offer a convenient alternative to typing, which can lead to complacency among users.

2.2. QRLjacking

Another way hackers leverage malicious QR Codes is through QRLjacking [4]. QRLjacking, which stands for Quick Response Code Login Jacking, refers to an attack in which malicious actors seize control of a user session. They do this to manipulate applications that utilize the "Login with QR code" functionality. The goal is to replace the genuine QR code with the attacker's QR code across all associated applications. It's essential to enhance and bolster QR code security with AI, as these codes can't be stored in databases, are generated on the fly, and are vulnerable to exploitation by malicious hackers [4].

2.3. Tracking and User Profiling

QR codes can track user behavior without storing any personal data. Although the code itself doesn't store user information, it can redirect to an application or URL that does. This process may raise privacy concerns when users are unaware that scanning the code will lead to data collection [4].

2.4. Malware Distribution

A QR code scanned through certain apps can initiate the download of malware onto the user's device. This method can be exploited to install malware on the user's device. Downloading files like images, PDFs, videos, and audio files from untrusted sources or third parties can also lead to malware infections.

3. Frameworks for Enhancing Security Using Artificial Intelligence

The paper presents a cutting-edge concept by introducing unique frameworks that leverage Artificial Intelligence (AI) to bolster the security of QR Codes. This framework is designed to tackle emerging threats such as QRLjacking and Quishing as well as image deconstruction and text confirmation on QR codes, which have been identified as potential vulnerabilities in QR code security. By harnessing the power of AI, this frameworks aim to mitigate these risks and enhance the overall security of QR code interactions on mobile devices like smartphones and tablets.

Coupled with an existing Machine Learning Algorithm by Authors, this framework forms a comprehensive strategy for enhancing QR code security through

the integration of AI technology. By leveraging AI's capabilities for pattern recognition, anomaly detection, and adaptive learning, these frameworks pave the way for a more secure and resilient QR code ecosystem. This research lays the groundwork for future advancements in QR code security, offering promising avenues for further exploration and development in the field.

3.1. NLP Based Framework for AI-Enhanced Security

The first framework focuses on proactive measures, utilizing AI algorithms to monitor and read the text/URL generated by the QR Code before redirecting the User. By analyzing patterns and detecting anomalies through a large NLP dataset, the algorithm can identify suspicious behavior indicative of potential security threats. This proactive approach allows for the early detection and prevention of malicious activities, safeguarding users from potential risks.

The framework has three major components as demonstrated in **Figure 2**, the Smartphone Caching System, the Natural Language Processing (NLP) Algorithm, and a Ranking Aggregation & Scoring System.

3.1.1. Natural Language Processing System

When integrated with Natural Language Processing for Text Extraction and Compositional semantic analysis, the Smartphone Cache can dissect the displayed text and the uniform resource locator embedded in the QR Code. This analysis is then combined with a custom Ranking Aggregation and Scoring mechanism that is an extension to an existing machine learning algorithm by authors [5] to assess the legitimacy of the QR code. The results of this evaluation can be communicated to the user appropriately, flagging any potential security concerns. The Natural Language Processing adds to the number of combinations and permutations that can be leverage for detecting keywords, not just the length of a URL, restricted and special characters in the URL, domain names, host names and can be extended to contact numbers and phone numbers to find legitimacy of the QR codes for other types of data transfers (**Figure 3** and **Figure 4**).

3.1.2. Rank Aggregation and Scoring System

The framework's key component is its reactive strategy, which utilizes AI-based anomaly detection to recognize and respond to security incidents within QR

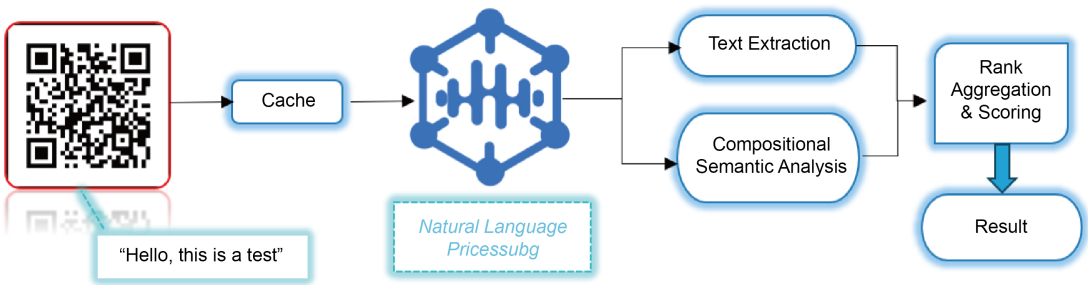

Figure 2. Components of NLP based framework.

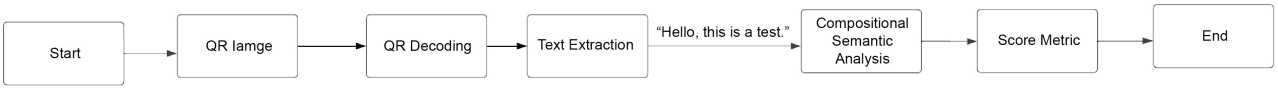

Figure 3. UML for a simple text based QR code decoding.

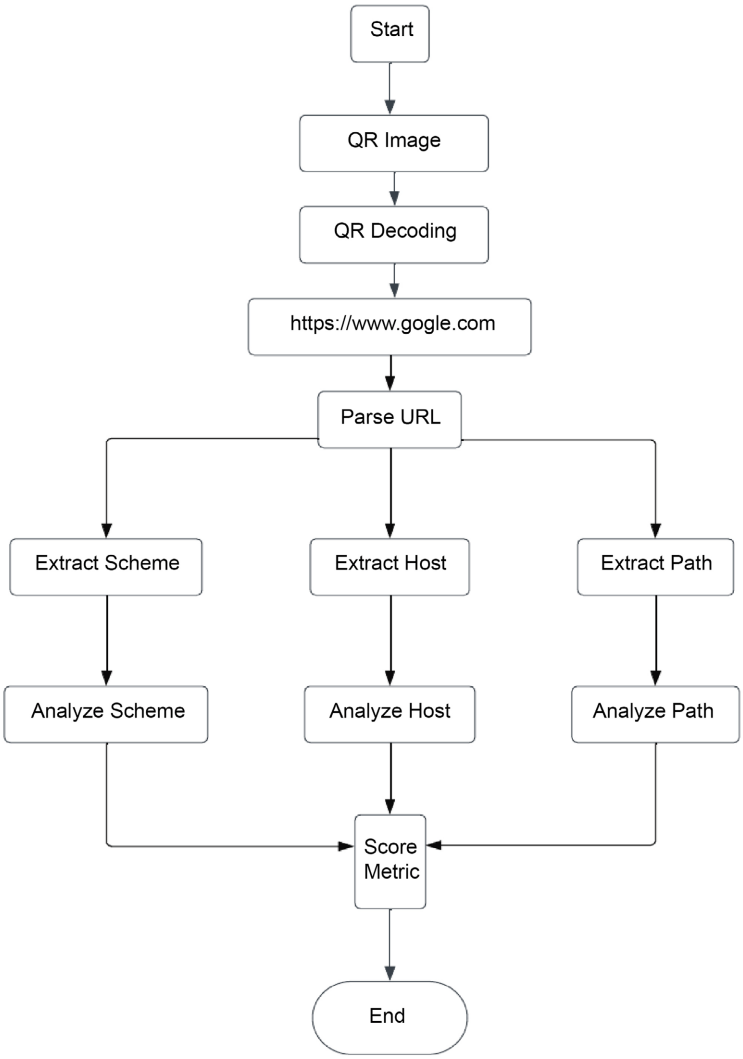

Figure 4. UML for a URL based QR code decoding.

code interactions. This approach incorporates machine learning algorithms developed by the authors [5], allowing the system to analyze past incidents and adjust its defenses to address evolving threats. This adaptive capability enhances the system's effectiveness in identifying and mitigating future security breaches. The framework builds upon the foundation of the Secure QR code scanner, which originally focused on detecting malicious uniform resource locators (URLs) using machine learning, as outlined by Pawar *et al.*

In the expanded framework, alongside the natural language processing (NLP) service, new features such as sentiment analysis and entity identification have been incorporated. By utilizing machine learning to derive insights and correla-

tions from unstructured text data, including overall sentiments and identified entities, the framework can evaluate the sentiment associated with the extracted or decoded content. Furthermore, the service can be trained to recognize specific entities, differentiating between entities without needing to dissect their lexical features, hosts, or content characteristics, as suggested by the authors [5]. This approach facilitates a more effective scoring system, ensuring a consistent differentiation between benign and malicious QR codes by analyzing their overall content and utilizing user-defined criteria to identify suspicious or malicious keywords through learning mechanisms (**Figure 5**).

3.2. Benefits of NLP Based Framework

By implementing this framework as a patch to the operating system, it streamlines the process of navigating to a secure QR Code Reader on the smart device,

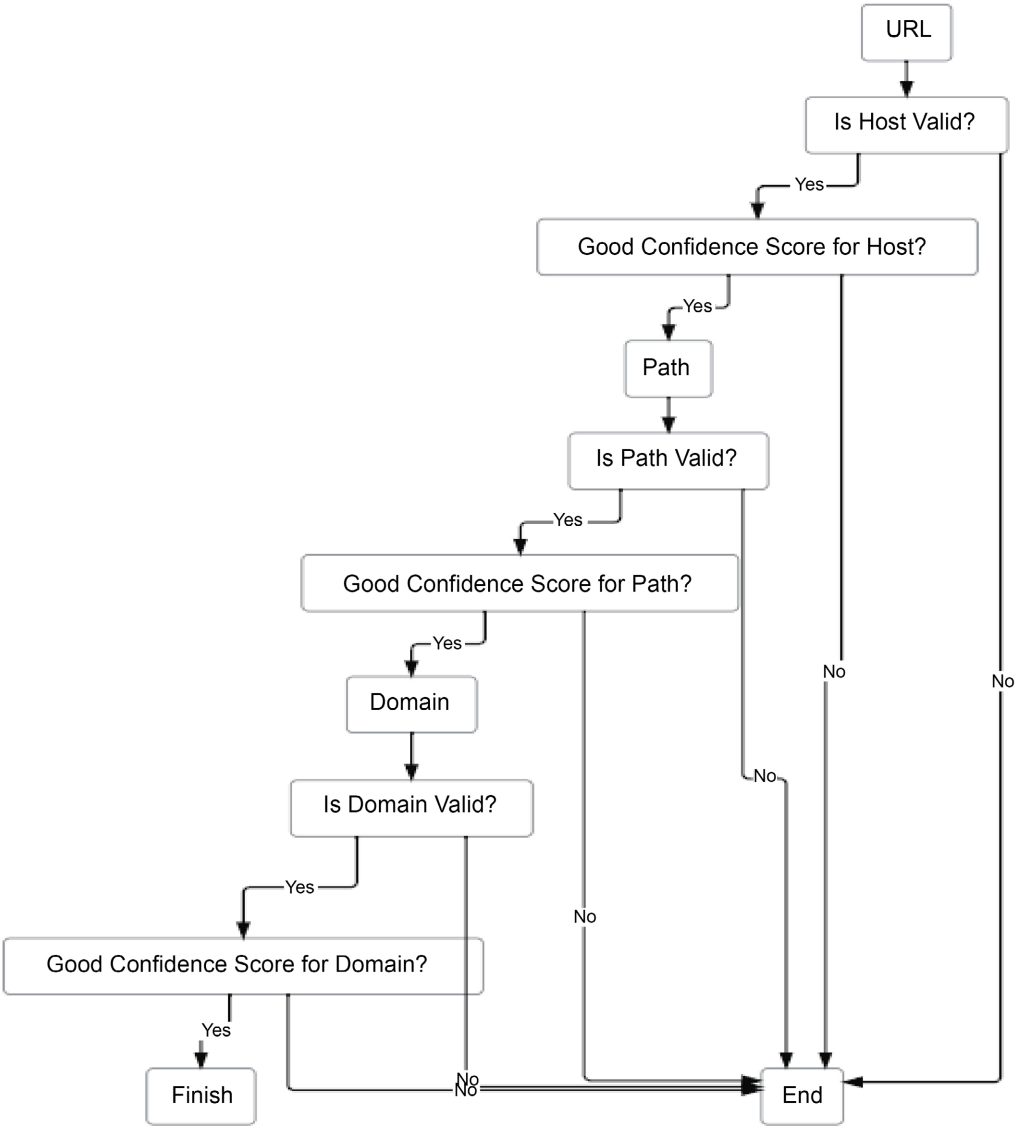

Figure 5. Example of a scoring system using URL.

saving valuable time. Furthermore, this framework can be expanded to recognize company logos embedded in the QR Code, providing additional context or personalized experiences associated with the brand. This integration of image recognition with QR code information extraction demonstrates how AI can enhance the understanding and utilization of encoded data, leading to a more comprehensive and secure user experience.

3.3. Limitations of NLP Based Framework

The time it takes for Natural Language Processing (NLP) to analyze a sentence can vary depending on several factors, including the complexity of the sentence, the size of the dataset being processed, the specific NLP techniques and algorithms used, and the computational resources available.

For simple sentences and small datasets, NLP processing can be relatively quick, often taking just a fraction of a second. However, for more complex sentences or larger datasets, the processing time can be longer, ranging from a few seconds to several minutes or more, especially when dealing with tasks like language translation, sentiment analysis, or advanced semantic analysis. When it comes to QR codes, the amount of text involved is typically limited to a few characters. As a result, the processing time for NLP tasks related to QR codes may be relatively short, with computational power and chip capabilities of the smart device being the primary limiting factors in the near future.

One potential limitation of the framework described is its reliance on the efficiency of the Rank Aggregation and Scoring Mechanism. The effectiveness of this mechanism depends on the thoroughness of the keyword vetting process, which can impact the reliability of the scoring system. Therefore, careful attention to the selection and validation of keywords is essential for ensuring the accuracy and usefulness of the scoring mechanism in the context of QR code security.

4. Potential Impact of AI-Enhanced Security

Authors [6] recommend educating users about the risks associated with scanning codes from untrusted sources and the importance of using secure QR code scanning software. They advocate for providing clear instructions on how to identify and avoid potentially harmful QR codes. While the suggested framework can improve security by promoting the adoption of AI and best practices, these technologies could have wider implications for smartphone operations, societal aspects, and user attitudes towards QR code usage.

4.1. Impact on Image and Processing Capabilities of Smartphones

While some significant improvements to Image processing and storage have been added through the application of AI for recognition of scenes, objects and image resolution improvement from a low quality to higher resolution, these measures are meagerer than what we seek to accomplish with detecting mali-

ciousness in QR codes. Image processing programs can significantly impact smartphone performance. These programs often require substantial computational resources, including CPU power and memory, to perform tasks such as image capture, editing, and analysis. As a result, running intensive image processing tasks can consume battery life and slow down the device, especially if the smartphone's hardware is not optimized for such tasks [5]. Additionally, the continuous processing of images in the background can lead to increased heat generation, potentially affecting the overall stability and longevity of the smartphone. To mitigate these impacts, smartphone manufacturers often optimize their devices' hardware and software to handle image processing efficiently, but the performance can still be influenced by the complexity and demands of the image processing algorithms being used.

4.2. Impact of QR Code Security on Society and Users

The prevalence of QR codes in everyday life is due to their user-friendly nature. As technology advances, people find it increasingly convenient to incorporate QR codes into their routines. However, the emergence of malicious codes has led to hesitancy in using them, stemming from concerns about identity theft. When users are assured that QR codes have been fortified with security measures, they are more inclined to trust and utilize them without reservation. Consequently, this can result in greater integration of QR codes across various domains such as digital payments, ticketing, and accessing information. This heightened security can be seamlessly implemented through the utilization of AI. Strengthened QR codes serve to safeguard users' personal and sensitive data by ensuring the legitimacy and security of scanned information, thereby diminishing the risk of identity theft or unauthorized data breaches. By fostering a more secure environment for QR code usage, users can benefit from a more efficient and seamless experience when interacting with QR codes, confident in the reduced likelihood of encountering security vulnerabilities.

5. Conclusion

Despite the widespread use of QR codes, end users encounter several challenges, particularly due to the absence of measures to identify defective or untrusted QR codes. To address this issue and minimize future security risks, it is essential to combine this evolving framework with best practices for training users, particularly in age groups that are more vulnerable to Quishing [3]. By integrating these approaches, strategies can be developed to mitigate potential security vulnerabilities. However, it's important to note that while advanced machine learning algorithms have the potential to improve security, they may also pose challenges for small devices with limited computing power, potentially reducing their efficiency and responsiveness [7]. Despite these challenges, further research into machine learning algorithms holds promise for enhancing QR code security in the future.

Acknowledgements

We would like to extend my sincere gratitude to Dr. Jamia Mills for her invaluable assistance and guidance in shaping the ideas presented in this work. Her expertise and insights have been instrumental in refining the concepts and ensuring the quality of this research. We are truly grateful for her support and mentorship throughout this endeavor.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Bashir, H. (2022) Leveraging Technology to Communicate Sustainability-Related Product Information: Evidence from the Field. *Journal of Cleaner Production*, **362**, Article ID: 132508. https://doi.org/10.1016/j.jclepro.2022.132508

[2] Huo, L., Zhu, J., Singh, P.K. and Pavlovich, P.A. (2021, January 1) Research on QR Image Code Recognition System Based on Artificial Intelligence Algorithm. *Journal of Intelligent Systems*, **30**. https://doi.org/10.1515/jisys-2020-0143 https://www.degruyter.com/document/doi/10.1515/jisys-2020-0143/html

[3] Posey, B. (2022, August 5) Understanding QR Code Security Issues for Enterprise Devices. https://www.techtarget.com/searchmobilecomputing/tip/Understanding-QR-code-security-issues-for-enterprise-devices

[4] Malwarebytes (2023, December 15) QR Code: How They Work and How to Stay Safe? https://www.malwarebytes.com/cybersecurity/basics/what-is-a-qr-code

[5] Sarker, I.H., Hoque, M.M., Uddin, M.K. and Alsanoosy, T. (2021) Mobile Data Science and Intelligent Apps: Concepts, AI-Based Modeling and Research Directions. *Mobile Networks and Applications*, **26**, 285-303. https://doi.org/10.1007/s11036-020-01650-z

[6] Morikawa, C., Kobayashi, M., Satoh, M., Kuroda, Y., Inomata, T., Matsuo, H., Miura, T. and Hilaga, M. (2021) Image and Video Processing on Mobile Devices: A Survey. *The Visual Computer*, **37**, 2931-2949. https://doi.org/10.1007/s00371-021-02200-8

[7] Daengsi, T., Pornpongtechavanich, P. and Wuttidittachotti, P. (2021) Cybersecurity Awareness Enhancement: A Study of the Effects of Age and Gender of Thai Employees Associated with Phishing Attacks. *Education and Information Technologies*, **27**, 4729-4752. https://doi.org/10.1007/s10639-021-10806-7