Security and privacy issues related to quick response codes

Pulkit Garg, Saheb Chhabra, Gaurav Gupta, Garima Gupta, Monika Gupta

Chapter 13

SECURITY AND PRIVACY ISSUES RELATED TO QUICK RESPONSE CODES

Pulkit Garg, Saheb Chhabra, Gaurav Gupta, Garima Gupta and Monika Gupta

Abstract Quick response codes are widely used for tagging products, sharing information and making digital payments due to their robustness against distortion, error correction features and small size. As the adoption and popularity of quick response codes have grown, so have the associated security and privacy concerns. This chapter discusses advancements in quick response codes and the major security and privacy issues related to quick response codes.

Keywords: Quick response codes, security, privacy

1. Introduction

During the 1940s, the growing goods and supply chain management industry sought an automated means for tracking goods and maintaining inventories. At the same time, there was a drive to do away with cash registers that required merchants to enter prices manually. The barcode, invented by Woodland and Silver [37] in 1951, provided effective solutions to these problems. Products were labeled with barcodes that were read by optical sensors. The barcodes worked seamlessly with the point-of-sale systems to log products, their prices and other attributes.

Early barcodes had black and white one-dimensional bars that encoded product information. Their popularity led to demands for more storage capacity, increased robustness and smaller size. However, increasing the storage capacity increased barcode size. To address this limitation, multi-dimensional barcodes were created that increased the processing speed by allowing them to be read in multiple directions concurrently. The first two-dimensional barcode was created in 1987. This

was followed by various two-dimensional barcodes that comprised not just bars and boxes, but also unique characters, shapes and patterns.

In the years that followed, there was a need for quick processing barcodes that could be deployed in assembly line environments. The idea was to have a recognizable pattern in a two-dimensional barcode that would enable a scanner to identify the code quickly. Eventually, it was decided that positional information should be incorporated in the code to increase detection speed.

Researchers conducted extensive surveys of the ratios of white to black areas in pictures, posters and other printed items. The least-used ratio of black to white was found to be 1:1:3:1:1, which enabled the determination of the widths of the black and white areas in the position detection patterns. The resulting design, which could be detected rapidly from any direction, was named a quick response (QR) code.

In 1994, QR codes were formally introduced as a substitute for one-dimensional barcodes. These two-dimensional matrix codes encode information using numbers, letters and special characters. Since QR codes store information in both directions, they can store more information than one-dimensional barcodes. QR codes also have desirable characteristics such as high error correction, strong robustness against distortions and small size. At this time, there are 40 versions of QR codes that are used based on the storage and/or error correction requirements of applications.

QR codes are scanned using a mobile or handheld device with a camera/image sensor and a QR code scanning application. The captured image is first processed to extract the QR code from the image. This is accomplished by detecting three distinctive squares in the QR code and single/multiple small squares near the fourth corner. The scanner can extract a correctly-oriented QR code image; if the image is not oriented properly, the viewing angle is adjusted up to a limit to extract the QR code image. The black and white boxes in the QR code are then decoded to read the information embedded in the QR code. The QR code also has error correction data, which are error bytes that enable information recovery when the QR code has physical damage. QR codes have recovery rates of up to 30%, which makes them one of the most robust codes ever invented.

However, QR codes have certain limitations, especially with regard to security and privacy. This chapter discusses advancements in quick response codes and the major security and privacy issues related to quick response codes.

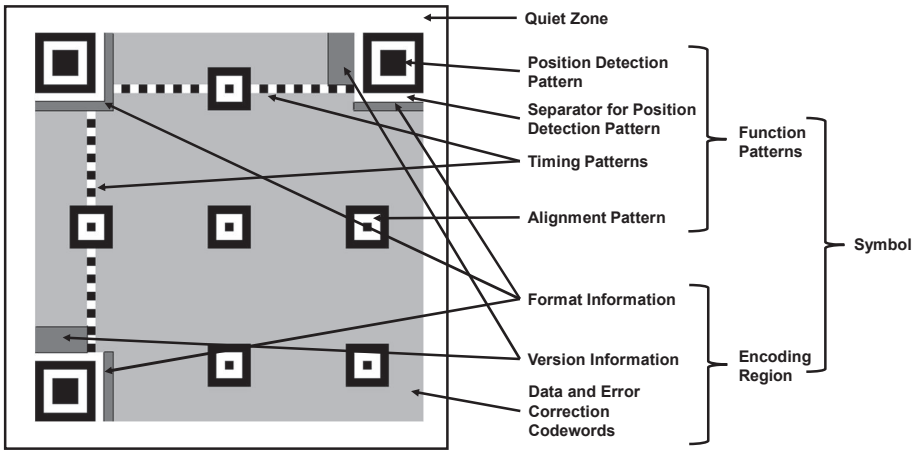

Figure 1. QR code structure [17].

2. QR Code Structure

Figure 1 presents the QR code structure. A QR code comprises black and white square modules that are set in a regular square array. The modules contain encoded information as well as the following function patterns and components:

- **Finder Pattern:** Three finder patterns are embedded in the upper-left, upper-right and lower-left corners of a QR code. These concentric square patterns assist in detecting the QR code position and orientation.
- **Separator:** A separator is an all-white pattern that is located between a finder pattern and the encoding region. The width of the separator is equal to the width of one module.
- **Timing Pattern:** A timing pattern comprises alternating black and white modules. The pattern always starts and ends with a black module. It helps determine the QR code version and identify module positions.
- **Alignment Pattern:** An alignment pattern is a 5×5 module pattern placed in a predefined position in a QR code. It comprises a 3×3 white/light module and a black/dark module in the center. The number of alignment patterns varies according to the QR code version. The first version of the QR code did not have alignment patterns.

- **Encoding Region:** The encoding region contains format information, version information and data and error correction codewords.

- **Quiet Zone:** The quiet zone is a region without markings that completely surrounds a QR code.

- **Data Storage:** QR codes store different types of information using numeric, alphabetic, byte and Kanji formats.

- **Error Correction:** QR codes use the Reed Solomon code to compute error correction bits based on the error correction requirements. Four error correction levels are available: (i) L (7%), (ii) M (15%), (iii) Q (25%) and (iv) H (30%).

- **Masking:** Masking is the inverting of the color of a QR code module. Black modules are converted to white and white modules are converted to black. Mask patterns enable QR codes to be read more easily by scanners. The color of a module after masking is determined by a formula that takes in the coordinates of the module and returns a value of zero or one. If the returned value is zero, the new color of the module is the opposite of its previous color. If the returned value is one, then the color of the module remains the same.

3. QR Code Evolution

QR codes have evolved in three ways: (i) storage capacity, (ii) security and (iii) appearance:

- **Storage Capacity:** Researchers have proposed several solutions to increase the storage capacity of QR codes. Grillo et al. [14] proposed high-capacity colored two-dimensional codes that increase the storage capacity. Vongpradhip [35] developed a multiplexing method to increase storage capacity. Tkachenko et al. [33] suggested using a two-layered QR code in which one QR code can be read by a generic QR code scanner while the other QR code can only be read via a specialized application, thereby increasing the storage capacity and well as security and privacy. Tikhonov [32] created an innovative double-sided QR code that incorporates a QR code and its mirrored version; although this approach has some limitations, it can store two QR codes in a single QR code.

- **Security:** Since QR codes are widely used in digital transactions, government identification cards and other official documents,

it is important that they are secure, non-reproducible and non-forgeable. Gaikwad and Singh [12] proposed an image embedding scheme for hiding QR codes in colored images using half-toning and luminance level control. Secret information is hidden in QR codes using steganography [4, 12]. Watermarks are used to safeguard QR codes from forgery.

- **Appearance:** A standard QR code is a matrix of black and white blocks arranged in a specific manner to store information. However, as QR codes became embedded in advertisements and hoardings, they had to be made attractive instead of just plain black and white. Chu et al. [9] proposed the use of machine-readable halftone QR codes. These QR codes are aesthetic and presentable, but have reduced error correction capabilities. Xu et al. [38] proposed a mechanism to create aesthetically pleasing QR codes while maintaining their robustness up to a certain level.

4. Key Issues

Key issues related to QR codes include their use in authentication, QR-code-based attacks, and security and privacy.

4.1 Authentication with QR Codes

Counterfeiting of documents, brands and security packaging is one of the fastest growing economic crimes. Holograms and special inks are extensively used to combat the counterfeiting of documents and products. The availability of inexpensive mobile phones, advancements in imaging technology and ease of use have led to QR codes being used to authenticate documents and products. QR codes are easy to generate and authenticate.

Lu et al. [25] proposed a secure mobile phone payment authentication scheme using visual cryptography and aesthetic QR codes. Yahya et al. [39] developed a mobile app for authenticating academic certificates. Student information is encoded in QR codes that are printed on certificates; the certificates are validated by scanning the printed QR codes. Warasart and Kuacharoen [36] implemented a solution for authenticating paper documents. A signed message is stored in a QR code that is printed on a document at creation; the integrity of the document is verified by checking the message stored in the QR code. Arkah et al. [3] created a watermarking scheme for QR codes used to authenticate electronic color documents. Keni et al. [18] developed a QR code for product authentication that is less expensive and more effective than

traditional RFID-based solutions. Several other QR code designs have been developed for authenticating documents and products [2, 5, 7, 22].

4.2 Attacks Using QR Codes

QR codes can be used as attack vectors. The following attacks involving QR codes are feasible:

- **Cross-Site Scripting:** A QR code can be leveraged to execute program-based and cross-site scripting attacks. A QR code can be encoded with a URL containing an alert message that executes an exploit. When a victim accesses the URL via the QR code, the alert message executes an exploit on the victim's web browser or computer system.

- **Command Injection:** A QR code can be input as a command-line argument that enables an attacker to change the content of the QR code or attach malicious QR code over the original code. The malicious QR code can execute commands on the victim's computer system, including installing a rootkit or spyware or launching a denial-of-service attack.

- **Malware Propagation:** An attacker can encode a URL to a rogue website in a QR code. When the QR code is scanned, a connection is established to the rogue website from where malware is downloaded to the victim's computer system. In October 2011, Kaspersky Labs identified malicious sites containing QR codes for portable applications (e.g., Jimm and Opera Mini) with Trojans that sent instant messages to premium-rate numbers.

- **Malicious Pixels in QR Codes:** Kieseberg et al. [19] describe two techniques for contaminating QR code pixels for use as an attack vector. One technique involves the creation of a malicious QR code that looks similar to the original QR code. The other technique involves changing only one pixel at a time.

Attacks can also be perpetrated using barcodes that are printed with QR codes. Lee et al. [21] developed black and white two-dimensional barcodes that provide authorization using a digital signature algorithm (KCDSA). Huang et al. [16] employed a reversible data hiding technique to embed QR code in an image while preserving its integrity properties.

4.3 Security and Privacy of QR Codes

The widespread application of QR codes raises several security and privacy concerns. The easy access of information stored in QR codes is a major problem.

Considerable research has focused on using cryptography to maintain security and privacy [1, 10, 11, 15, 26, 27]. Mendhe et al. [28] proposed a three-layered QR code based message sharing system that uses a combination of cryptography and steganography. The data to be shared is encrypted using the RSA algorithm and encoded in the QR code along with a randomly-initialized pixel or mask image.

Nguyen et al. [29] designed watermark QR codes that are sensitive to printing and scanning. The technique, which does not affect readability, replaces the background of a monochrome QR code with a random texture that is clearly visible when the QR code is reproduced. Liu et al. [24] developed a secure, visual QR code that ensures the authenticity of the encoded data. A hash of a message is created and encrypted using a private key. The message is then encoded in the QR code and fused with an image. The encrypted hash is watermarked in the QR code. At the time of decoding, the hash of the encoded message is matched against the hash obtained by decrypting the watermarked string.

Zhang et al. [40] proposed a two-level QR code that stores public and private data. Public data is easily decoded using a common barcode scanner. Private data is encoded by swapping black modules in the original QR code with textured patterns. The textured patterns are sensitive to printing and scanning processes, enabling the authenticity of the QR code to be determined.

Lin et al. [23] employed steganography to prevent unauthorized access to private information stored in QR codes. The approach embeds a confidential message in the data codewords of the public message QR tag and makes no modifications to the other QR code regions. In the final QR code, the hidden information can only be extracted using a private key whereas public information is easily decoded using a normal scanner.

Krombholz et al. [20] demonstrated that malicious links to phishing sites can be embedded in QR codes. They analyzed attack scenarios in various applications of QR codes and identified design requirements for rendering QR codes secure and usable. Rogers [30] revealed a vulnerability in how Google Glass interprets QR codes. He showed that a Google Glass device could scan a QR code that would force it to connect to a hostile access point and root access could be gained to the device without the wearer's knowledge.

Interestingly, QR codes are now being placed on headstones. The QR codes typically point to websites where information, pictures and videos of the departed persons are posted. Gotved [13] discussed the privacy concerns of sharing such information in public spaces.

Bani-Hani et al. [6] discussed the privacy risks associated with QR codes. They demonstrated how sensitive user information could be stolen and how privacy rights can be violated by malicious code that runs in the background. They developed a secure system for QR code generation and scanning to address these problems. Vidas et al. [34] showed that a URL embedded in a QR code could take a smartphone user to a website that installs a malicious application that accesses and exfiltrates private user data.

5. Innovative Applications

This section highlights three innovative applications of QR codes.

5.1 Self-Authenticating Documents

Paper document fraud is easily perpetrated using high-resolution scanners and printers. At this time, few, if any, mobile systems are available for detecting fraudulent paper documents in real time. The available systems have low accuracy, do not incorporate biometric authentication and typically require manual intervention. QR codes with security features, including biometric data, signed document content hashes and encryption, could be embedded in paper documents when they are created. A smartphone application could be used to quickly scan QR codes and verify the authenticity of the paper documents.

5.2 Color QR Codes

Limited storage capacity is limiting new applications of QR codes. Research is underway to use colors in QR codes to increase storage capacity. However, the robustness of color QR codes is an open problem.

A key hurdle is color selection. In general, the robustness of color QR codes is affected by color shifting and variations in illumination. To address these problems, QR code colors should be chosen to maximize their distances in the RGB and CMYK color spaces.

Another problem is cross-channel interference, which is the mixing of colors that occurs during the printing process. Cross-module interference is a problem that occurs when a high-density color QR code is printed using a low-resolution color printer. It affects QR code robustness because the colors tend to bleed into neighboring modules.

5.3 Anti-Counterfeiting QR Codes

QR codes are easily reproduced, replaced and forged. Current anti-counterfeiting solutions use sophisticated methods that are inefficient and not scalable. Special patterns can be employed to render QR codes non-reproducible, non-replaceable and non-forgeable, but modified QR code readers would be needed to extract, decode and verify the embedded information.

6. Conclusions

QR codes are seeing myriad applications, but serious concerns are being raised about the security, privacy and authenticity of the information embedded in QR codes. This chapter has discussed advancements in QR code technology as well as strategies for implementing security and privacy features in QR codes. Of course, the challenge is to provide these features without reducing storage capacity and error correction capabilities.

Future research will focus on implementing anti-counterfeiting techniques for QR codes. Also, it will focus on the digital forensic aspects of copied, manipulated and forged QR codes.

References

[1] M. Ahamed and H. Mustafa, A secure QR code system for sharing personal confidential information, *Proceedings of the International Conference on Computer, Communications, Chemical, Materials and Electronic Engineering*, 2019.

[2] C. Allen and A. Harfield, Authenticating physical locations using QR codes and network latency, *Proceedings of the Fourteenth International Joint Conference on Computer Science and Software Engineering*, 2017.

[3] Z. Arkah, L. Alzubaidi, A. Ali and A. Abdulameer, Digital color document authentication using QR codes based on digital watermarking, *Proceedings of the International Conference on Intelligent Systems Design and Applications*, pp. 1093–1101, 2018.

[4] A. Arya and S. Soni, Enhanced data security in quick response (QR) code using image steganography technique with DWT-DCT-SVD, *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, vol. 3(5), pp. 59–65, 2018.

[5] E. Ayeleso, A. Adekiigbe, N. Onyeka and M. Oladele, Identity card authentication system using a QR code and smartphone, *International Journal of Science, Engineering and Environmental Technology*, vol. 2(9), pp. 61–68, 2017.

[6] R. Bani-Hani, Y. Wahsheh and M. Al-Sarhan, Secure QR code system, *Proceedings of the Tenth International Conference on Innovations in Information Technology*, 2014.

[7] A. Banu, K. Ganagavalli and G. Ramsundar, QR code based shopping with secure checkout for smartphones, *Journal of Computational and Theoretical Nanoscience*, vol. 15(5), pp. 1545–1550, 2018.

[8] T. Bui, N. Vu, T. Nguyen, I. Echizen and T. Nguyen, Robust message hiding for QR code, *Proceedings of the Tenth International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, pp. 520–523, 2014.

[9] H. Chu, C. Chang, R. Lee and N. Mitra, Halftone QR codes, *ACM Transactions on Graphics*, vol. 32(6), article no. 217, 2013.

[10] Z. Cui, W. Li, C. Yu and N. Yu, A new type of two-dimensional anti-counterfeit code for document authentication using neural networks, *Proceedings of the Fourth International Conference on Cryptography, Security and Privacy*, pp. 68–73, 2020.

[11] R. Dudheria, Evaluating features and effectiveness of secure QR code scanners, *Proceedings of the International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery*, pp. 40–49, 2017.

[12] A. Gaikwad and K. Singh, Information hiding using image embedding in QR codes for color images: A review, *International Journal of Computer Science and Information Technologies*, vol. 26(1), pp. 278–283, 2015.

[13] S. Gotved, Privacy with public access: Digital memorials in quick response codes, *Information, Communication and Society*, vol. 18(3), pp. 269–280, 2015.

[14] A. Grillo, A. Lentini, M. Querini and G. Italiano, High capacity colored two-dimensional codes, *Proceedings of the International Multiconference on Computer Science and Information Technology*, pp. 709–716, 2010.

[15] V. Hajduk, M. Broda, O. Kovac and D. Levicky, Image steganography using QR code and cryptography, *Proceedings of the Twenty-Sixth International Conference on Radioelectronics*, pp. 350–353, 2016.

[16] H. Huang, F. Chang and W. Fang, Reversible data hiding with histogram-based difference expansion for QR code applications, *IEEE Transactions on Consumer Electronics*, vol. 57(2), pp. 779–787, 2011.

[17] International Organization for Standardization, ISO/IEC Standard 18004: Information Technology – Automatic Identification and Data Capture Techniques – QR Code Bar Code Symbology Specification, Geneva, Switzerland, 2000.

[18] H. Keni, M. Earle and M. Min, Product authentication using hash chains and printed QR codes, *Proceedings of the Fourth IEEE Annual Consumer Communications and Networking Conference*, pp. 319–324, 2017.

[19] P. Kieseberg, S. Schrittwieser, M. Leithner, M. Mulazzani, E. Weippl, L. Munroe and M. Sinha, Malicious pixels using QR codes as an attack vector, in *Trustworthy Ubiquitous Computing*, I. Khalil and T. Mantoro (Eds.), Atlantis Press, Paris, France, pp. 21–38, 2012.

[20] K. Krombholz, P. Fruhwirt, P. Kieseberg, I. Kapsalis, M. Huberand and E. Weippl, QR code security: A survey of attacks and challenges for usable security, *Proceedings of the International Conference on Human Aspects of Information Security, Privacy and Trust*, pp. 79–90, 2014.

[21] J. Lee, T. Kwon, S. Song and J. Song, A model for embedding and authorizing digital signatures in printed documents, *Proceedings of the International Conference on Information Security and Cryptology*, pp. 465–477, 2002.

[22] O. Lewis and S. Thorpe, Authenticating motor insurance documents using QR codes, *Proceedings of the Southeast Conference*, 2019.

[23] P. Lin and Y. Chen, QR code steganography with secret payload enhancement, *Proceedings of the IEEE International Conference on Multimedia and Expo Workshops*, 2016.

[24] S. Liu, J. Zhang, J. Pan and C. Weng, SVQR: A novel secure visual quick response code and its anti-counterfeiting solution, *Journal of Information Hiding and Multimedia Signal Processing*, vol. 8(5), pp. 1132–1140, 2017.

[25] J. Lu, Z. Yang, L. Li, W. Yuan, L. Li and C. Chang, Multiple schemes for mobile payment authentication using QR codes and visual cryptography, *Mobile Information Systems*, vol. 2017, article no. 4356038, 2017.

[26] S. Maheswari and D. Hemanth, Frequency domain QR code based image steganography using the Fresnelet transform, *AEU International Journal of Electronics and Communications*, vol. 69(2), pp. 539–544, 2015.

[27] V. Mavroeidis and M. Nicho, Quick response code secure: A cryptographically-secure anti-phishing tool for QR code attacks, *Proceedings of the International Conference on Mathematical Methods, Models and Architectures for Computer Network Security*, pp. 313–324, 2017.

[28] A. Mendhe, D. Gupta and K. Sharma, Secure QR code based message sharing system using cryptography and steganography, *Proceedings of the First International Conference on Secure Cyber Computing and Communications*, pp. 188–191, 2018.

[29] H. Nguyen, A. Delahaies, F. Retraint, D. Nguyen, M. Pic and F. Morain-Nicolier, A watermarking technique to secure printed QR codes using a statistical test, *Proceedings of the IEEE Global Conference on Signal and Information Processing*, pp. 288–292, 2017.

[30] M. Rogers, Hacking the Internet of Things for Good, Lookout, San Francisco, California (`www.slideshare.net/LookoutInc/hacking-the-internet-of-things-for-good`), 2013.

[31] J. Swartz, The growing "magic" of automatic identification, *IEEE Robotics and Automation*, vol. 6(1), pp. 20–23, 1999.

[32] A. Tikhonov, On Double-Sided QR-Codes, arXiv: 1902.05722 (`arxiv.org/abs/1902.05722`), 2019.

[33] I. Tkachenko, W. Puech, O. Strauss, C. Destruel, J. Gaudin and C. Guichard, Rich QR code for multimedia management applications, *Proceedings of the International Conference on Image Analysis and Processing*, pp. 383–393, 2015.

[34] T. Vidas, E. Owusu, S. Wang, C. Zeng, L. Cranor and N. Christin, QRishing: The susceptibility of smartphone users to QR code phishing attacks, in *Financial Cryptography and Data Security*, A. Adams, M. Brenner and M. Smith (Eds.), Springer, Berlin Heidelberg, Germany, pp. 52–69, 2013.

[35] S. Vongpradhip, Using multiplexing to increase information in QR codes, *Proceedings of the Eighth International Conference on Computer Science and Education*, pp. 361–364, 2013.

[36] M. Warasart and P. Kuacharoen, Paper-based document authentication using digital signatures and QR codes, presented at the *International Conference on Computer Engineering and Technology*, 2012.

[37] N. Woodland and B. Silver, Classifying Apparatus and Method, U.S. Patent No. 2,612,994, October 7, 1952.

[38] M. Xu, Q. Li, J. Niu, H. Su, X. Liu, W. Xu, P. Lv, B. Zhou and Y. Yang, ART-UP: A novel method for generating scanning-robust aesthetic QR codes, *ACM Transactions on Multimedia Computing, Communications and Applications*, vol. 17(1), article no. 25, 2021.

[39] Z. Yahya, N. Kamarzaman, N. Azizan, Z. Jusoh, R. Isa, M. Shafazand, N. Salleh and S. Mokhtaruddin, A new academic certificate authentication using leading-edge technology, *Proceedings of the International Conference on E-Commerce, E-Business and E-Government*, pp. 82–85, 2017.

[40] B. Zhang, K. Ren, G. Xing, X. Fu and C. Wang, SBVLC: Secure barcode-based visible light communications for smartphones, *IEEE Transactions on Mobile Computing*, vol. 15(2), pp. 432–446, 2016.