# Multi-secret Steganography in QR Codes

KATARZYNA KOPTYRA, MAREK R. OGIELA
AGH University of Krakow,
30 Mickiewicza Ave, 30-059 Krakow,
POLAND

*Abstract:* - This paper presents a steganographic scheme that conceals two independent secrets in a single QR code. The method uses two embedding algorithms which operate in separate domains. The first algorithm embeds the secret information into segments. The resulting code is then passed to the second method which modifies some modules to hide another secret, exploiting the error correction feature of QR codes. In this way, the secret messages do not overlay and are both possible to recover. The secrets may be retrieved separately as their embedding areas are different. The presented approach is an example of multi-secret steganography which may be used for confidential data transfer.

*Key-Words:* - QR code, steganography, multi-secret, information hiding, security, privacy, secret communication, hidden channel.

Received: March 9, 2024. Revised: September 6, 2024. Accepted: October 9, 2024. Published: November 27, 2024.

## 1 Introduction

QR codes are a popular medium for short message storage, [1]. They are commonly used in commerce, public services, personal applications, posters, and many more. The prevalence of QR codes results from their design suited for machine reading, that facilitates decoding with mobile devices.

QR codes appear very characteristic because they are built from modules—white and black (or sometimes bright and dark) squares. Additionally, the code contains some specific patterns that help with localization and decoding, presented in Figure 1.

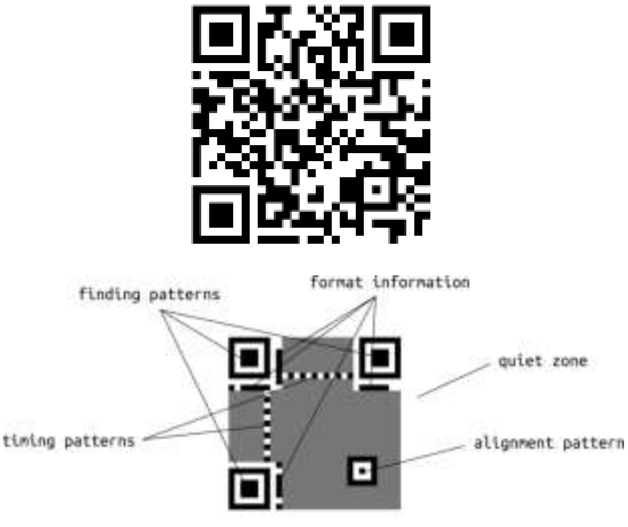

Fig. 1: An example of a QR code (top); Reserved areas of a QR code (bottom)

The creation of a QR code is a quite complex process that consists of a few steps, including data analysis, data encoding, error correction coding, structure of final message, module placement in matrix, data masking, and format and version information. During these phases, the input data are analyzed to check which modes (data types) are optimal, and which version (size) of QR code should be used. The encoded data are placed in the code outside reserved areas presented in Figure 1.

Considering the current state of the research field, there are a few ideas of steganography in QR codes. Data hiding is usually realized with an error correction mechanism. It is a part of the QR standard [1] designed to repair some discrepancies that may occur during scanning. Thanks to error correction, a specific number of modules may be damaged and the content is still possible to recover. This feature precipitated new steganographic algorithms based on introducing deliberate errors to the code, [2], [3], [4], [5], [6], [7], [8]. These methods use secret sharing or rely on the secret key, and frequently deal with Reed-Solomon codewords.

Other approaches to information hiding in QR codes can also be listed. One idea uses a segmentation feature [9] to conceal secret information. It is done by injecting additional segments into regular data. Another algorithm creates a QR code that reveals different information when scanned in a mirror, [10]. There are also techniques of using subcells which serve as a second storage level, [11], [12]. Many more techniques adapted a number of approaches to utilize QR codes in steganography, [13], [14], [15], [16], [17].

As can be seen, various methods of QR code steganography hide data in several ways. This paper aims to propose a scheme for multi-secret steganography that uses different embedding areas for secret messages. The proposed scheme uses two data-hiding methods for concealing and recovering the secrets. The novelty lies in applying multi-secret steganography for a single QR code which gives two separate communication channels.

## 2 Problem Formulation

The problem we want to solve is the design of a multi-secret steganography system, which allows to hide at least two different secrets in one QR code. The main assumptions are: there is a single carrier and multiple secret messages. Such a scheme should be able to conceal secret messages in a QR code and retrieve them back.

### 2.1 Model

The model of this system is composed of two complementary algorithms for embedding and extracting the secrets. They are presented in Figure 2.

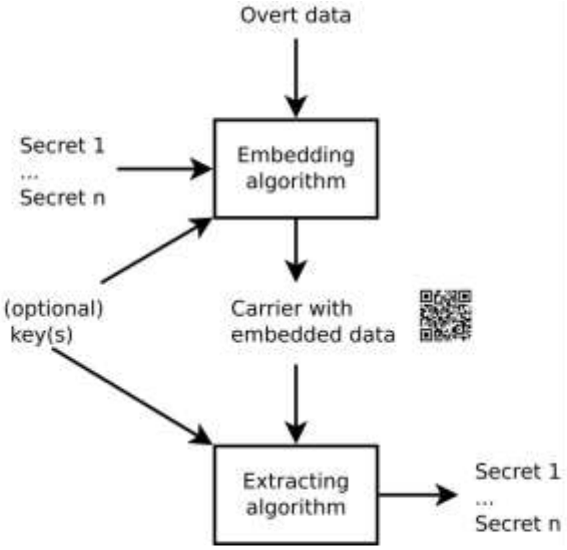

Fig. 2: A model of multi-secret steganographic scheme for QR codes

Secrets are passed to the embedding algorithm which generates a QR code with hidden data. Optional keys may be used for denoting specific secret positions in the carrier. The cover with concealed secrets is then passed to the extracting algorithm that returns the secrets back. If keys were used during embedding, they are again utilized during extraction.

There are multiple possible algorithms that may be applied to the presented model. It is required that both methods use separate embedding regions so that the secrets do not overlap. In this way, all hidden data are possible to extract without loss. The chosen methods for this paper are: hiding data in empty segments and modified modules. The details are presented in section 3.

## 3 Problem Solution

The presented solution is for a single carrier and two secrets. The embedding algorithm uses two steganographic methods: hiding data in empty segments and in modified modules. These methods have been chosen because their embedding areas do not overlap. The first steganographic method introduces additional segments to the QR code. They contain no data but encode secret bits with their type. The second steganographic method relies on an error correction mechanism for data hiding. Secret encoding is done by introducing some alterations that are later repaired during QR decoding.

The embedding process works as follows. In the beginning, the first secret is presented as a binary string. Then, for each two bits, one empty segment is created. Secret bits are encoded in segment type, i.e. numeric for 00, alphanumeric for 01, byte for 10, and kanji for 11. These empty segments are then mixed with regular segments that contain the overt message. An additional key may indicate how these segments are arranged. In this way initial QR code is generated. Currently, the code contains only one payload. To conceal the second secret, we cast it into a binary string. Then we modify the non-reserved modules of the QR code. The locations of such modifications may be indicated with an optional secret key. These errors will be rectified later during decoding in the error correction process.

The extracting process is complementary and works as follows. To reveal the first secret, we need to decode segments and filter them to retain only empty ones. If an optional key was used during embedding, it indicates segment position during decoding as well. Then, depending on segment types, we assemble bits and translate them to the first message. Recovering the second secret requires the identification of damaged modules. It may be done by generating a new code with identical data, version, and error correction level as the stego-code. The difference between the codes constitutes our second secret. Alternatively, error positions may be indicated with an optional key. In such a case, it is not necessary to recreate the whole code from scratch.

For instance, if our first secret is ":)" and our second secret is ":(", we may present them in binary format as follows: 0011101000101001 and 0011101000101000. This example does not use optional keys. In the first embedding method we created eight empty segments of types: numeric, kanji, byte, byte, numeric, byte, byte, and alphanumeric. These segments are mixed with segments of a regular message. The intermediate code is shown in Figure 3 (a). When the code was created, we flipped non-reserved segments if the bit of the second secret was equal to 1. When the bit was 0, the module remained unchanged. In this way, we altered six modules to hide the second secret. The result is presented in Figure 3 (b). In this example, the modules were modified from the bottom right, but other starting points are also possible, because with error correction any modules may be damaged, providing that their number is below the allowed limit.

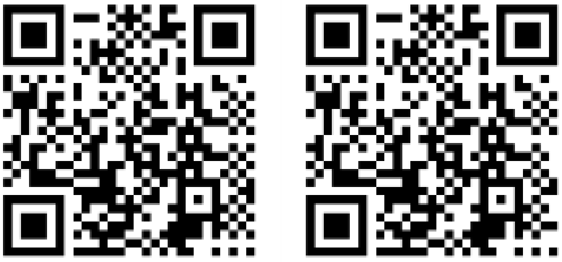

Fig. 3: (a) QR code with a single secret hidden in segments; (b) QR code with two secrets hidden in segments and in modules

The recovery phase of the first secret requires segment analysis. There is one segment with a regular message and eight empty segments. We read their types, which are numeric, kanji, byte, byte, numeric, byte, byte, and alphanumeric, then we translate them to bits, from which we obtain 0011101000101001. To reveal the second secret, we need to detect damaged modules. Therefore we recreated the code with the same settings and compared the result with input data. The analysis showed that bits on positions 2, 3, 4, 6, 10, 12 were flipped. From this information, we may deduce the second secret: 0011101000101000. Subsequent modules were untouched, so they denote null-termination of the string.

To sum up, both secret messages reside in separate regions and their lossless recovery is possible. Created codes adhere to QR standards and may be decoded with a regular QR reader. Then only the overt message is revealed. Thanks to this, the proposed approach may find application in steganographic scenarios, like hidden communication channels.

# 4 Conclusion

The steganographic scheme presented in this paper places two secret messages in different areas of a QR code. Both secrets may be revealed independently as they do not interfere. The first secret (hidden in segments) is characterized by high robustness. This is because it is stored in a code together with regular content, thereby being protected with an error correction mechanism as well. Conversely, for the second secret, error correction is used for embedding data. For this reason, the code needs to be distortion-free to recover this secret.

The presented system belongs to generative steganography methods. It means that the embedding algorithm does not receive an empty cover as input. Instead, the algorithm receives both overt and covert data needed to create a carrier. The final QR code with hidden secrets is generated as output.

Our system may also be used for secret sharing [18], [19], [20], [21]. After the secret is divided, the shares are placed in separate regions of a QR code. To decode the secret, both parts must be extracted, and then combined. This increases the security of the system because both shares must be found by an adversary to recover the final message. Of course in this case the QR code has to be intact as well.

The capacity of a multi-secret steganographic scheme is higher than that of a single-secret. The reason is that more regions of a QR code are utilized. Nonetheless, the capacity of both messages is limited in their own ways. The maximum length of the first secret depends on the version and error correction level of a QR code. With the highest version and lowest level of error correction, we are able to store a few hundred bytes [9]. The maximum length of the second secret is constrained by the error correction level—a trait of the QR code selected during generation. The highest level is able to correct up to 30% of errors, so this is the value that can be considered the capacity of the second secret.

QR codes are very popular and useful media for short message storage, [22]. Their ubiquity makes them interesting carriers for data-hiding purposes. One of the most important advantages of QR codes in steganography is that they are not only digital carriers. The code may be printed and its payload is still decodable, even if some parts of the code are damaged or obscured. Such a feature opens a lot of future directions for information hiding, as the structure of QR codes offers diverse embedding areas. This gives the possibility of combining a multitude of techniques and creating better algorithms.

*References:*

[1] Denso Wave Incorporated. QRcode.com, [Online]. http://www.qrcode.com/en/ (Accessed Date: August 18, 2024).

[2] Chow, Y.; Susilo, W.; Yang, G.; Phillips, J.G.; Pranata, I.; Barmawi, A. Exploiting the error correction mechanism in QR codes for secret sharing. In *Proceedings of the Lecture Notes in Computer Science, Information Security and Privacy: 21st Australasian Conference, ACISP 2016, Proceedings, Part I*, Melbourne, Australia, 2016; Vol. 9722, pp. 409–425. https://doi.org/10.1007/978-3-319-40253-6_25.

[3] Chow, Y.W.; Susilo, W.; Baek, J., Covert QR Codes: How to Hide in the Crowd. In *International Conference on Information Security Practice and Experience*; Melbourne, Australia, 2017; pp. 678–693. https://doi.org/10.1007/978-3-319-72359-4_42.

[4] Chiang, Y.J.; Lin, P.Y.; Wang, R.Z.; Chen, Y.H. Blind QR Code Steganographic Approach Based upon Error Correction Capability. *KSII Transactions on Internet and Information Systems 2013*, vol. 7 no. 10, pp. 2527–2543. https://doi.org/10.3837/tiis.2013.10.012.

[5] Cheng, Y.; Fu, Z.; Yu, B. Improved Visual Secret Sharing Scheme for QR Code Applications. IEEE Trans. Inf. Forensics Secur. 2018, vol. 13, no. 9, pp. 2393–2403. https://doi.org/10.1109/TIFS.2018.2819125.

[6] Lin, P.Y.; Chen, Y.H.; Lu, E.J.L.; Chen, P.J. Secret Hiding Mechanism Using QR Barcode. In *Proceedings of the 2013 International Conference on Signal-Image Technology & Internet-Based Systems (SITIS)*, Kyoto, Japan, 2–5 December 2013; pp. 22–25. https://doi.org/10.1109/SITIS.2013.15.

[7] Bui, T.V.; Vu, N.K.; Nguyen, T.T.; Echizen, I.; Nguyen, T.D. Robust Message Hiding for QR Code. In *Proceedings of the 2014 Tenth International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP)*, Kitakyushu, Japan, 27–29 August 2014; pp. 520–523. https://doi.org/10.1109/IIH-MSP.2014.135.

[8] Huang, P.C.; Chang, C.C.; Li, Y.H.; Liu, Y. High-payload secret hiding mechanism for QR codes. Multimed. Tools Appl. 2019, vol. 78, no. 19, pp. 22331–22350. https://doi.org/10.1007/s11042-019-7600-x.

[9] Koptyra, K.; Ogiela, M. Information Hiding in QR Codes using Segment Manipulation. In *Proceedings of the 2024 IEEE International Conference on Pervasive Computing and Communications Workshops and other Affiliated Events (PerCom Workshops)*, Biarritz, France, 2024; pp. 397–400. https://doi.org/10.1109/PerComWorkshops59983.2024.10502885.

[10] Alexey, T. On Double-Sided QR-Codes, 2019, [Online]. https://www.researchgate.net/publication/331165555_On_Double-Sided_QR-Codes (Accessed Date: March 25, 2024).

[11] Teraura, N.; Sakurai, K. Information Hiding in Subcells of a Two-Dimensional Code. In *Proceedings of the 1st IEEE Global Conference on Consumer Electronics* 2012, GCCE, Tokyo, Japan, 2–5 October 2012; pp. 652–656. https://doi.org/10.1109/gcce.2012.6379943.

[12] Uttarwar, S.V.; Bagade, A.M. Two-Level QR Code for Secured Message Sharing and Document Authentication. *International Journal of Advanced Research in Computer and Communication Engineering* 2017, vol. 6, no. 6, pp. 508–511. https://doi.org/10.17148/IJARCCE.2017.6689 .

[13] Rani, M.M.S.; Euphrasia, K.R. Data Security Through QR Code Encryption And Steganography. *Adv. Comput. Int. J. (ACIJ)*, 2016, vol. 7, no. 1/2. https://doi.org/10.5121/acij.2016.7201.

[14] Chen, W.Y.; Wang, J.W. Nested image steganography scheme using QR-barcode technique. *Opt. Eng.*, 2009, vol. 48, no. 5, 057004. https://doi.org/10.1117/1.3126646.

[15] Chung, C.H.; Chen, W.Y.; Tu, C.M. Image hidden technique using QR-Barcode. In *Proceedings of the Fifth International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, Kyoto, Japan, 12–14 September 2009; pp. 522–525. https://doi.org/10.1109/IIH-MSP.2009.119.

[16] Dey, S.; Mondal, K.; Nath, J.; Nath, A. Advanced Steganography Algorithm Using Randomized Intermediate QR Host Embedded

With Any Encrypted Secret Message: ASA_QR Algorithm. *Int. J. Mod. Educ. Comput. Sci. (IJMECS)*, 2012, vol. 4, no. 6, pp. 59-67. https://doi.org/10.5815/ijmecs.2012.06.08.

[17] Wu, W.C.; Lin, Z.W.; Wong, W.T. Application of QR-Code Steganography Using Data Embedding Technique. In *Information Technology Convergence, Lecture Notes in Electrical Engineering*; Springer: Amsterdam, The Netherlands, 2013; Vol. 253, pp. 597-605. https://doi.org/10.1007/978-94-007-6996-0_63.

[18] Shamir, A. How to Share a Secret. *Commun. ACM* 1979, vol. 22, no. 11, pp. 612–613. http://doi.org/10.1145/359168.359176.

[19] Blakley, G.F. Safeguarding cryptographic keys. In: National Computer Conference, 1979, *American Federation of Information Processing Societies — Conference Proceedings*, Vol. 48 (1979), AFIPS Press, Montvale, New Jersey, pp. 313–317.

[20] Koptyra, K.; Ogiela, M.R. Subliminal Channels in Visual Cryptography. *Cryptography* 2022, vol. 6, no. 3, 46. https://doi.org/10.3390/cryptography6030046.

[21] He, J.; Dawson, E. Multistage secret sharing based on one-way function. *Electron. Lett.*, 1994, vol. 30, no. 19, pp. 1591–1592.

[22] Ricson, E. 61+ QR Code Usage Statistics 2024: Latest Facts and Insights. 2024, [Online]. https://www.qrcode-tiger.com/qr-code-statistics-2022-q1 (Accessed Date: September 5, 2024).

### Contribution of Individual Authors to the Creation of a Scientific Article (Ghostwriting Policy)

- Katarzyna Koptyra: conducted investigation and developed methodology, and conceptualization. formal analysis, writing - original draft.
- Marek R. Ogiela: supervision, validation, writing - original draft.

### Sources of Funding for Research Presented in a Scientific Article or Scientific Article Itself

This work has been supported by the funds of the Polish Ministry of Education and Science assigned to AGH University of Krakow. Research project supported by program „Excellence initiative – research university" for the AGH University of Krakow.

### Conflict of Interest

The authors have no conflicts of interest to declare.

### Creative Commons Attribution License 4.0 (Attribution 4.0 International, CC BY 4.0)