A General Steganalysis Method of QR Codes

Jia Chen[1,2], Kunlin Chen[1,2], Yongjie Wang[1,2], Xuehu Yan[1,2(✉)], and Longlong Li[1,2]

[1] National University of Defense Technology, 460 Huangshan Road, Shushan District, Hefei 230037, China
publictiger@126.com

[2] Anhui Key Laboratory of Cyberspace Security Situation Awareness and Evaluation, Hefei 230037, China

Abstract. With the wide application of quick response (QR) codes, its security has been paid more and more attention. There are many steganography schemes to embed the secret message into QR codes, which can be used in terrorist activities, spread viruses, etc. However, there is currently no effective scheme for detecting stego QR code. This paper divides the spatial QR code-based steganography schemes into three categories and then proposes a steganalysis method for QR codes. The method includes detecting stegao codes and recovering pure QR codes, which is realized by the code regeneration, module comparison, and embedded information filtering operations. Our method can perfectly distinguish the stego code and block the transmission of embedded information for the spatial QR code-based steganography schemes. Theoretical analysis and experiments show that the proposed method is feasible, universal, and robust.

Keywords: QR codes · Steganography · Steganalysis · Code regeneration · Protection

1 Introduction

The quick response (QR) codes [1] were invented by Japanese company Denso Wave in 1994 for tracking components in vehicle manufacturing. These barcodes now are widely applied in location, printing, online advertising, mobile payment and Internet commerce, etc. With the popularity of smartphones, QR codes have become a fast and efficient URL connector, known as the "entrance" of the mobile Internet. They are convenient, easy to convey information. Meanwhile, smartphones can quickly and easily use built-in cameras or decoders downloaded from the Internet to decode QR codes.

Supported by the Program of the National University of Defense Technology and the National Natural Science Foundation of China (Number: 61602491).

S. Goel et al. (Eds.): ICDF2C 2022, LNICST 508, pp. 472–483, 2023.
https://doi.org/10.1007/978-3-031-36574-4_28

With the widespread usage and promotion of QR codes, its security issues have attracted more and more attention. In 2010, Kaspersky Lab captured the first attempt to use malicious QR codes for cybercrime, linking the QR codes to malware for Android (OS) and J2ME (Java). A malicious QR code is usually a malicious link embedded in a normal QR code. When users scan it, they jump to malware or a designated website. Recently, vicious crimes based on QR codes have increased, and the common QR code scam are clickjacking, phishing links, and Trojan horse viruses, etc. [2].

Data hiding [3,4] and secret sharing [5,6] are common data protection techniques. However, steganography can also be used to embed malicious information into a QR code. In recent years, more and more researchers have studied QR code-based steganography schemes. Some redesigned the QR code module to embed the secret message, such as [7–11]. The most common method is to implement steganography based on the error correction capability of the QR code [12–17]. There is also a scheme of embedding secret information into padding bits [18]. These QR code-based steganography schemes may be used for terrorist activities, cybercrime, and so on.

Faced with the security issues of QR codes caused by data hiding technology, a steganalysis scheme for QR codes is urgently needed to identify the stego code. The QR code is not only a typical two-dimensional barcode, but also a standard image. Currently, there are many image steganalysis schemes. Early schemes used statistical features for steganalysis [19,20]. Avcibas *et al.* [21] proposed a scheme to detect the stego image with the aid of image quality features and multivariate regression analysis. Later, some researchers proposed more complex feature sets with high dimension to improve the detection performance of steganalysis, such as subtractive pixel adjacency model (SPAM) [22], Spatial Rich Models (SRM) [23], and Discrete Cosine Transform Residual (DCTR) [24], etc. Meanwhile, some feature selection algorithms have also been proposed, such as the Genetic Algorithm (GA) [25], Binary Bat Algorithm (BBA) [26] and so on. Recently, many image steganalysis schemes tend to be implemented based on deep learning [27,28]and convolution neural network [29–31].

However, the above steganalysis schemes are not effective when applied to QR codes, and many of them require considerable samples to train the model. Moreover, there is currently no scheme specifically designed to detect stego QR codes. Meanwhile, the special structure of the black and white blocks of the barcode does not have general image statistics and texture features, etc. To solve the increasingly serious security issues of QR codes, and overcome the difficulty that QR code-based steganography schemes are not easy to detect, this paper proposes a general steganalysis method of QR codes. The code regeneration and module comparison operation are used to detect stego codes, and the secret message is filtered to recover pure QR codes. The contributions of this paper are summarized as follows.

1. We review the QR code-based steganography schemes and divide them into three categories according to implementation principles.

2. We design a steganalysis method for QR codes, which contains detecting stegao codes and recovering pure QR codes.
3. Experiments verify the feasibility and robustness of the proposed method, and the robustness is consistent with the robustness of the steganography scheme.

The rest of this paper is organized as follows. In Sect. 2, we briefly introduce the features of the QR code, and review the QR code-based steganography schemes. The proposed method and the theoretical analyses are described in Sect. 3. Section 4 gives experimental results. Finally, conclusions are drawn in Sect. 5.

2 Preliminaries

2.1 QR Code Features

A QR code consists of black and white squares (called modules). Each module represents 1 bit of data, where black (white) modules represent 1 (0), respectively. According to the QR code standard, there are a total of 40 different versions of QR codes. The number of modules in a QR code is determined by the version number v. For a version-v QR code, the number of modules is $(17 + 4v) \times (17 + 4v)$. In addition, the Reed-Solomon code is applied to achieve the error-correction capability of QR codes. Four error-correction levels (L, M, Q, and H) are available, and corresponding error-correction capabilities are about $7\%, 15\%, 25\%$, and 30%, respectively.

Figure 1 shows the structure of a standard version-7 QR code. All modules of a QR code can be divided into two parts: the function pattern and data region. The function pattern contains the quiet zone, finder patterns, separators, timing patterns, and alignment patterns, and is applied to locate and identify the QR code parameters. The data region includes the format information, version information, and data and error-correction codewords. In general, the function pattern of the same version QR code is the same, and the data region determines the essence of the QR code. Through the encoding and decoding phase of the QR code as shown in Algorithm 1, we analyzed that the same content can generate the same QR code with the same version and format information.

2.2 Steganography Based on QR Codes

According to the implementation principles of these schemes and the encoding and decoding characteristics of QR codes, we divide the steganography schemes based on QR codes into three categories:

1. Redesign the modules of the cover QR code to embed secret information [7–11]. A module is a pixel block composed of some pixels. Usually, a module is designed into a 3×3 or 5×5 pixel block. The key pixels remain unchanged, and the secret information is embedded in other pixels.

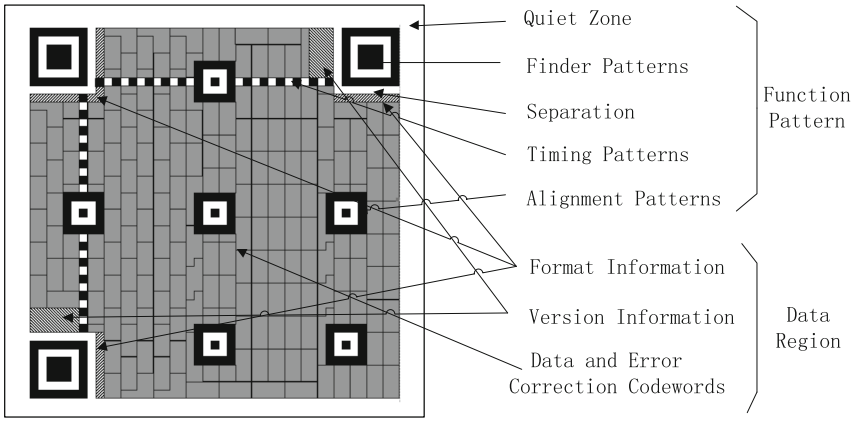

Fig. 1. Structure of a version-7 QR code.

Algorithm 1. The encoding and decoding phase of the QR code.

The encoding phase
Step 1. Analyze the input data stream to determine the type of characters to be encoded. And select the required error correction level.
Step 2. Encode the data into a bitstream with every eight bits as a codeword, and adding padding codewords if necessary.
Step 3. Encode the bitstream with the RS code.
Step 4. Construct the final information and place function patterns in the matrix.
Step 5. Masking the data and error-correction codewords of the symbol.
Step 6. Generate the the format and version information, and then obtain the final matrix.

The encoding phase
Step 1. Identifie all black and white modules.
Step 2. Decode the format and version information.
Step 3. Remove the mask pattern.
Step 4. Recover the data and error correction codewords.
Step 5. Check the error with error-correcting codewords.
Step 6. Decode the data codewords.

2. Utilize error correction mechanism of the QR code [12–17]. The secret information is embedded by modifying the QR code modules within the scope of fault tolerance. During decoding, the RS code can correct data errors and recover the correct information.
3. Take advantage of the redundancy of the QR code. The padding bits are added in each data block if there are insufficient data bits. When constructing the final information, remainder bits are filled if needed. The secret information is embedded utilizing these redundant and meaningless bits [18].

3 The Proposed Method

3.1 The Steganalysis Method for QR Codes

In the proposed method, we first detect the stego code, and then recover the pure QR code. Among the three types of QR code-based steganography schemes summarized above, the embedding method based on the redesigned cover module is easy to see the difference from the standard QR code. So the embedded information is directly filtered to recover the pure QR code. For the remaining two categories, the QR code cannot be determined from the appearance to be abnormal. Therefore, it is necessary to judge the stego code first, and then filter out the embedded information. The flow chart of the proposed method is shown in Fig. 2.

The detailed steps of the proposed method are described in Algorithm 2. Given a cover QR code, first identify whether it is stego code. If the QR code is abnormal in appearance, we directly filter out embedded information by code regeneration. The so-called code regeneration operation, specifically, decodes the QR code to obtain the cover content, version, and format information, and then regenerates a pure QR code (called re-code) based on these information. The original QR code becomes a stego code after embedding secret information. The re-code is the same as the original QR code in the module distribution. As a result, the re-code blocks the transmission of secret information to protect the QR code.

In proposed method, we detect the stego QR codes using the code regeneration and module difference rate (MDR), if the stego code cannot be determined directly. First, perform the code generation operation to obtain the re-code. Then compare the re-code with all modules of the cover code to calculate the MDR. Finally, set the threshold t, and the stego code is distinguished based on MDR and t. If this code is a stego code, output the pure re-code to filter the embedded information. Otherwise, this code can be used directly without security issues.

3.2 Theoretical Analysis

Feasibility. Filtering embedded information is based on code regeneration operation, and the detection process also depends on the code regeneration operation. Therefore, the key to the feasibility of the proposed method lies in whether the code regeneration operation can be realized. According to the encoding and decoding processes of the QR code as shown in Algorithm 1, the generation of QR code is related to cover content, version, error correction capability, and mask. Given the same cover content, then select the same version and error correction capability. Eight kinds of mask patterns are fixed, and an optimal one is selected based on the evaluation. Therefore, when the content, version, and format information are the same, the QR code is unique. Based on the uniqueness of QR codes, we can implement the proposed method.

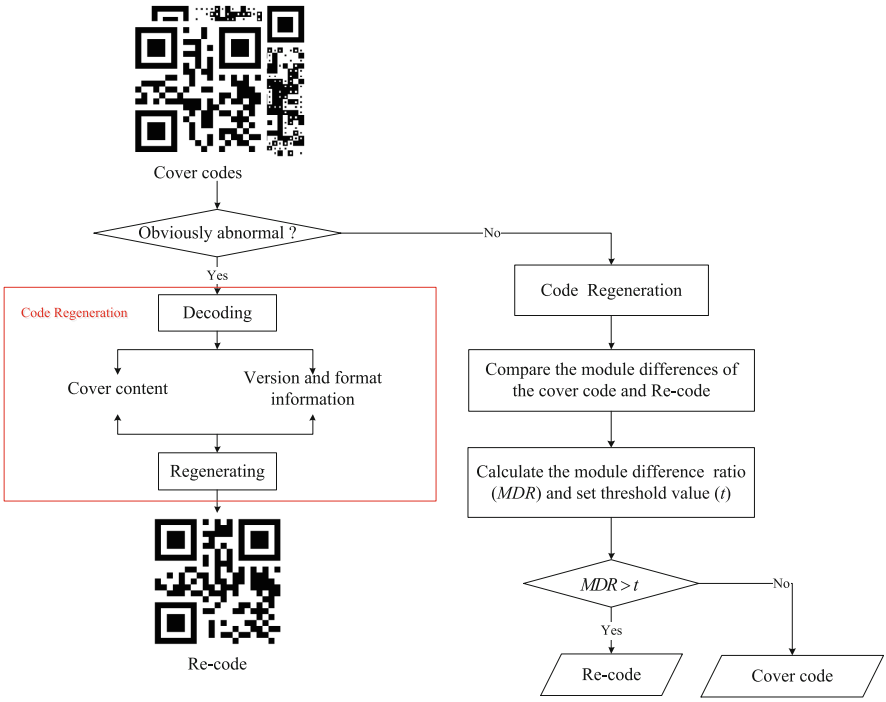

Fig. 2. The flowchart of the protection for QR codes.

Algorithm 2. The process of protection method for QR codes.

Input: A cover QR code.
Output: A secure QR code.

Step 1. Decode the cover QR code to obtain the cover content, version, and format information.
Step 2. Regenerate the re-code based on the decoded information.
Step 3. Determine whether the cover code is a stego code. If it can be determined directly, go to Step 6; otherwise, go to Step 4.
Step 4. Compare the re-code with all modules of the cover code to calculate the MDR, and set the threshold t.
Step 5. If $MDR \geq t$, go to Step 6; otherwise, go to Step 7.
Step 6. Output the re-code.
Step 7. Output the cover QR code.

Universality. The QR code-based steganography schemes are divided into three categories according to the implementation principles. Our proposed method is applicable to all three types of stego QR codes. On the one hand, the code regeneration operation is carried out directly to recover a standard pure QR code for the abnormal code. On the other hand, the detection of the stego code

depends on our steganalysis scheme for codes without obvious abnormalities. The embedded secret information will cause changes in QR code module. As long as the module changes, it will be successfully captured by our steganalysis scheme. Therefore, the proposed method can be applied to the protection of all QR codes. In addition, the idea of our proposed method can also be used to protect all barcodes.

Robustness. The robustness of our proposed method depends on the robustness of decoding. As long as a standard decoder can decode a QR code, we can perform steganalysis and protection. Generally, the QR code-based steganography schemes will ensure that the QR code can be decoded normally to reduce the probability of being discovered. So the stego code has good robustness and can resist various noise and other attacks. In our proposed method, the robustness of steganography determines the robustness of steganalysis. As long as the stego code can be decoded normally, our scheme is effective.

Threshold Estimation. Embedding secret information will cause changes to the QR code cover module, but this change will be within the error correction capability to ensure correct decoding. So based on the number of modules used for error correction, we can roughly estimate the upper limit of the threshold t as shown in 1. Where n represents the total number of modules, and ecc denotes each error correction level provides error-correction capabilities ($L \sim 7\%$, $M \sim 15\%$, $H \sim 25\%$, $Q \sim 30\%$).

$$t_h = \frac{\lfloor n \cdot ecc \times 8/2 \rfloor}{(17+4v)(17+4v)} = \frac{\lfloor 4 \times n \cdot ecc \rfloor}{(17+4v)(17+4v)} \tag{1}$$

Generally, there are no error modules for electronically printed QR codes. That is, the error rate is 0. In addition, our proposed method adopts the module difference rate instead of the pixel difference rate, which can also overcome the interference caused by noise, blur, printing, etc. Because the change of a pixel will not affect the recognition of the module. Therefore, we set the lower limit of the threshold $t_l = 0.01$. In summary, if $0.01 \leq MDR \leq \frac{\lfloor 4 \times n \cdot ecc \rfloor}{(17+4v)(17+4v)}$, it means that the QR code is embedded with secret information.

4 Experimental Results and Comparison

In this section, to verify the effectiveness of the proposed method, experiments are given for each type of stego code in Python and executed on a PC with a 3.40 GHz CPU and 16.0 GB of RAM running the Windows 7 operating system. Since some steganographic algorithms based on QR codes are not open source, the test sample codes used in the experiment are screenshots from the corresponding papers.

Figure 3 shows the experimental results of the proposed protection method for stego codes based on module redesign. Figure 3 (a) is a nested QR code captured from [9]. The outer QR code encodes the URL "https://www.yzu.edu.tw", and the inner QR code is the URL "https://www.youtube.com/watch?v=9i_UQC4znvu". Figure 3 (c) is the re-code based on the outer QR code. Figure 3 (e) shows a two-level QR code taken from [10]. Figure 3 (g) is the re-code according the public-level message "cover Response Code 1". Figure 3 (a) and (e) are obviously abnormal QR codes. Figure 3 (c) and (g) are re-code which remove the embedded content. Figure 3 (b), (d), (f) and (h) are the decoding of Fig. 3 (a), (c), (e) and (g), respectively. From the decoding result, the re-code and cover code can carry the same information and achieve the same function.

Figure 4 shows the experimental results for stego QR codes based on error correction mechanism and encoding redundancy. Figure 4 (a) is a version 1-L stego code based on error correction mechanism captured from [14]. Its public message is the URL "fcu.edu.tw", and the embedded secret is the number "29", which requires a specific decoder to decode it. Figure 4 (b) shows a secure QR code generated based on public message. Figure 4 (c) shows the different modules marked in red modules between the cover code and re-code, and $MDR = 7.710\%$. Figure 4 (d) is a version 40-M QR code embedded with secret message. Its public message is "guofangkejidaxuedianziduikangxueyuan", and the secret message "This the a secret.0000..." is embedded in the padding bits of the QR code. Figure 4 (e) shows the re-code. Figure 4 (f) displays the different modules with 5.471%.

Experiments for robustness verification were conducted. The cover QR codes of the steganalysis samples are all derived from QR code-based steganography schemes related papers of. Experiments show that our method can accurately distinguish stego codes from all samples, and the embedded messages can be filtered through code regeneration. The robustness of the proposed protection method is consistent with the robustness of the corresponding steganography scheme. As long as the stego QR code can be decoded by a standard decoder, our proposed method can work successfully.

Table 1 compares the properties of classic image steganalysis schemes with our method. The schemes in [21,23,27,29] are classic image steganalysis methods and require many samples to train the model. However, when they are applied to QR code detection, the effect of steganalysis is not ideal. Our scheme adopts code regeneration operation, only one cover QR code is needed to realize real-time protection, and the detection effect is perfect.

Fig. 3. The proposed protection method for stego codes based on module redesign. (a) shows the nested code taken from [9]. (b) is the result of decoding (a). (c) is the re-code. (d) presents the decoding result of (c). (e) is the stego code taken from [10]. (f) shows the decoding result of (a). (g) is the re-code. (h) displays the result of decoding (g).

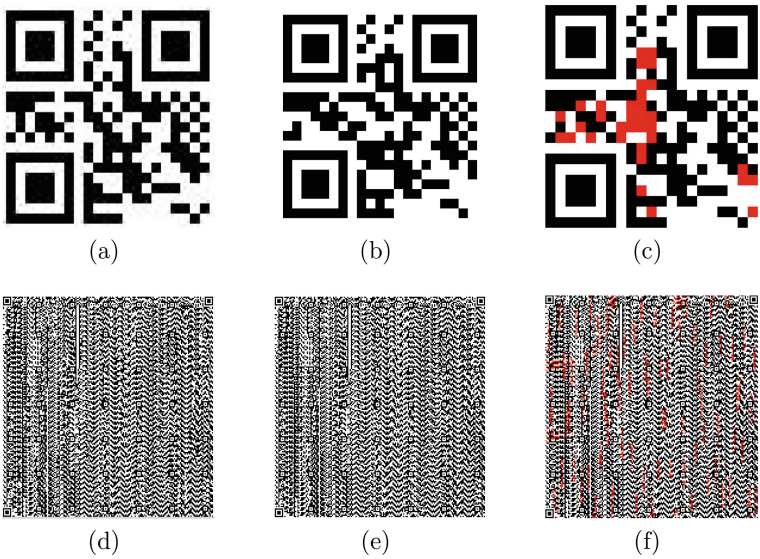

Fig. 4. The proposed protection method for stego codes. (a) − (c) are based on error correction mechanism, and (d) − (f) are based on the padding code. (a) shows the cover code taken from [14]. (b) is the re-code. (c) displays the differences between (a) and (b) with $MDR = 7.710\%$. (d) is the cover code from [18]. (e) is the re-code. (f) shows the differences between (d) and (e) with $MDR = 5.471\%$.

Table 1. Comparisons of the proposed method and classic image steganalysis schemes.

	Based method	Main Detection Object	The steganalysis effect for QR codes	Number of samples required
[21]	Image quality metrics	Image	Not ideal	Many
[23]	Rich models	Image	Not ideal	Many
[27]	Deep learning	Image	Not ideal	Many
[29]	Convolutional Neural Network	Image	Not ideal	Many
Our	Code regeneration	Barcodes	Perfect	One

5 Conclusion

This paper proposes a general steganalysis method of QR codes. We apply the code regeneration and module comparison operation to distinguish the stego QR codes. Furthermore, the embedded message can be filtered out by code regeneration to recover the pure QR code. The proposed method can effectively determine the stego QR code and block the transmission of secret messages. The accuracy of steganalysis is almost 100%, and the proposed method has a perfect effect on QR code protection. In future work, researchers could attempt to extend this method to other barcode protection, design a model to protect all barcodes, and further focus on studying steganalysis methods based on deep learning for QR codes.

References

1. JTC1/SC, I.: Information technology - automatic identification and data capture techniques - QR code 2005 bar code symbology specification (2006)
2. Arntz, P.: QR code scams are making a comeback (2020). https://blog.malwarebytes.com/scams/2020/10/qr-code-scams-are-making-a-comeback/
3. Shi, Y.Q., Li, X., Zhang, X., Wu, H.T., Ma, B.: Reversible data hiding: advances in the past two decades. IEEE Access **4**, 3210–3237 (2016). https://doi.org/10.1109/ACCESS.2016.2573308
4. Ma, K., Zhang, W., Zhao, X., Yu, N., Li, F.: Reversible data hiding in encrypted images by reserving room before encryption. Inf. Forensics Secur. IEEE Trans. **8**, 553–562 (2013). https://doi.org/10.1109/TIFS.2013.2248725
5. Yan, X., Lu, Y., Yang, C.N., Zhang, X., Wang, S.: A common method of share authentication in image secret sharing. IEEE Trans. Circ. Syst. Video Technol. **31**, 2896–2908 (2020)
6. Yan, X., Lu, Y., Liu, L., Song, X.: Reversible image secret sharing. IEEE Trans. Inf. Forensics Secur. **15**, 3848–3858 (2020). https://doi.org/10.1109/TIFS.2020.3001735
7. Mohamed Amin, M., Salleh, M., Ibrahim, S., Katmin, M.: Stenography: random LSB insertion using discrete logarithm, pp. 234–238 (2003)

8. Tkachenko, I., Puech, W., Destruel, C., Strauss, O., Gaudin, J.M., Guichard, C.: Two-level QR code for private message sharing and document authentication. IEEE Trans. Inf. Forensics Secur. **11**, 1 (2016). https://doi.org/10.1109/TIFS.2015.2506546
9. Chou, G.J., Wang, R.Z.: The nested QR code. IEEE Sig. Process. Lett. **27**, 1230–1234 (2020). https://doi.org/10.1109/LSP.2020.3006375
10. Cheng, Y., Fu, Z., Yu, B., Shen, G.: A new two-level QR code with visual cryptography scheme. Multimedia Tools Appl. **77**(16), 20629–20649 (2018). https://doi.org/10.1007/s11042-017-5465-4
11. Baharav, Z., Kakarala, R.: Visually significant QR codes: image blending and statistical analysis, pp. 1–6 (2013). https://doi.org/10.1109/ICME.2013.6607571
12. Chiang, Y.J., Lin, P.Y., Wang, R.Z., Chen, Y.H.: Blind QR code steganographic approach based upon error correction capability. KSII Trans. Internet Inf. Syst. **7**, 2527–2543 (2013). https://doi.org/10.3837/tiis.2013.10.012
13. Bui, T., Vu, N., Nguyen, T., Echizen, I., Nguyen, T.: Robust message hiding for QR code, pp. 520–523 (2014). https://doi.org/10.1109/IIH-MSP.2014.135
14. Huang, P.C., Li, Y.H., Chang, C.C., Liu, Y.: Efficient scheme for secret hiding in QR code by improving exploiting modification direction. KSII Trans. Internet Inf. Syst. **12**(5), 2348–2365 (2018)
15. Lin, P.Y., Chen, Y.H.: High payload secret hiding technology for QR codes. EURASIP J. Image Video Process. **2017**(1), 1–8 (2017)
16. Wan, S., Lu, Y., Yan, X., Ding, W., Liu, H.: High capacity embedding methods of QR code error correction, pp. 70–79 (2018). https://doi.org/10.1007/978-3-319-72998-5_8
17. Liu, S., Fu, Z., Yu, B.: A two-level QR code scheme based on polynomial secret sharing. Multimedia Tools Appl. **78**, 21291–21308 (2019). https://doi.org/10.1007/s11042-019-7455-1
18. Tan, L., Lu, Y., Yan, X., Liu, L., Chen, J.: (2, 2) threshold robust visual secret sharing scheme for QR code based on pad codewords. In: Yang, C.-N., Peng, S.-L., Jain, L.C. (eds.) SICBS 2018. AISC, vol. 895, pp. 619–628. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-16946-6_50
19. Luo, X., Liu, F., Lian, S., Yang, C., Gritzalis, S.: On the typical statistic features for image blind steganalysis. IEEE J. Sel. Areas Commun. **29**, 1404–1422 (2011)
20. Li, F., Zhang, X.: Steganalysis for color images based on channel co-occurrence and selective ensemble. J. Image Graph. (2015)
21. Avcibas, I., Memon, N., Sankur, B.: Steganalysis using image quality metrics. IEEE Trans. Image Process. **12**(2), 221–229 (2003). https://doi.org/10.1109/TIP.2002.807363
22. Kodovsky, J., Pevný, T., Fridrich, J.: Modern steganalysis can detect YASS, vol. 7541, p. 754102 (2010). https://doi.org/10.1117/12.838768
23. Fridrich, J., Kodovsky, J.: Rich models for steganalysis of digital images. IEEE Trans. Inf. Forensics Secur. **7**(3), 868–882 (2012). https://doi.org/10.1109/TIFS.2012.2190402
24. Holub, V., Fridrich, J.: Low-complexity features for jpeg steganalysis using undecimated DCT. IEEE Trans. Inf. Forensics Secur. **10**(2), 219–228 (2015). https://doi.org/10.1109/TIFS.2014.2364918
25. Song, S.K., Gorla, N.: A genetic algorithm for vertical fragmentation and access path selection. Comput. J. **43**(1), 81–93 (2000). https://doi.org/10.1093/comjnl/43.1.81

26. Liu, F., Yan, X., Lu, Y.: Feature selection for image steganalysis using binary bat algorithm. IEEE Access **8**, 4244–4249 (2020). https://doi.org/10.1109/ACCESS.2019.2963084
27. Ni, J., Ye, J., YI, Y.: Deep learning hierarchical representations for image steganalysis. IEEE Trans. Inf. Forensics Secur. 12, 2545–2557 (2017). https://doi.org/10.1109/TIFS.2017.2710946
28. Yang, L., Cao, X., He, D., Wang, C., Wang, X., Zhang, W.: Modularity based community detection with deep learning (2016)
29. Wei, L., Gao, P., Jia, L., Liu, M.: Image steganalysis based on convolution neural network. Appl. Res. Comput. **1**, 235–238 (2019)
30. Li, L., Zhang, W., Qin, C., Chen, K., Zhou, W., Yu, N.: Adversarial batch image steganography against CNN-based pooled steganalysis. Sign. Process. **181**, 107920 (2021). https://doi.org/10.1016/j.sigpro.2020.107920
31. Chen, B., Li, H., Luo, W., Huang, J.: Image processing operations identification via convolutional neural network. Sci. Chin. (Inf. Sci.) **63**(03), 275–281 (2020)