Copyright Protection for Progressive Image Transmission with QR Code and Secret Sharing Applications

Hsiang-Cheh Huang[1], Yueh-Hong Chen[2], Feng-Cheng Chang[3], and Teng-Kuan Huang[1]

[1] Department of Electrical Engineering, National University of Kaohsiung, Taiwan, R.O.C.
hch.nuk@gmail.com
[2] Dept of Computer Science and Information Engineering, Far East University, Taiwan, R.O.C.
yuehhong@gmail.com
[3] Department of Innovative Information Technology, Tamkang University, Taiwan, R.O.C.
135170@mail.tku.edu.tw

Abstract. Progressive image transmission (PIT) can be commonly encountered in the browsers due to the bandwidth consumption of different users. With the digital nature of images, they can be easily copied and spread, and hence copyright protection of progressively transmitted images would be needed. We make use of the QR code to hide the copyright information, and apply the visual secret sharing method for embedding secret data into different layers of color images for progressive transmission. Simulation results have presented the acceptable quality of marked images for progressive transmission, and the copyright protection with QR code and secret sharing. The proposed technique can be practical and easily implementable for copyright protection of progressive image transmission.

Keywords: progressive transmission, QR code, secret sharing

1 Introduction

Copyright protection is much required for multimedia contents [1], especially for digital images. There are lots of images that can be viewed with browsers from the Internet. Due to the bandwidth requirement, the images can be transmitted progressively and they are shown gradually in the browsers. This kind of scheme is named progressive image transmission (PIT) [2]. Therefore, it would be applicable to hide information relating to copyright owners into progressively transmitted images.

Reversible data hiding [3, 4, 5] is one effective means for copyright protection. We can hide secret information into different layers of PIT. Besides, QR codes [6] are commonly seen today. We may consider using QR codes to represent the copyright information. For enhanced protection capability, and by utilizing the characteristics of PIT, we employ the visual secret sharing (VSS) method [7] for hiding the noise-like patterns corresponding to the QR codes into the images. By doing so, the embedded information can be extracted at the decoder from the marked image. Original images for progressive transmission can be perfectly recovered with reversible data hiding at the receiver. Reconstructed QR code can be captured, and then the webpage relating to the copyright can be accessed instantly.

We briefly describe the use of difference alteration for reversible data hiding in Sec. 2. And then we present the proposed method with QR code and visual secret sharing in Sec. 3. We demonstrate the simulation results in Sec. 4 to show the effectiveness of proposed application. Finally, we address the conclusions in Sec. 5.

2 Reversible Data Hiding with Difference Alteration

Reversible data hiding makes good use of the characteristics of original image for hiding secret data [3, 4, 5]. Due to 'reversibility', secret data can be hidden into original image at the encoder. And at the decoder, with a small amount of overhead for decoding, both the original image and the secret data should be perfectly separated from the marked image. Due to its ease of implementation, in this paper, we propose to integrate reversible data hiding, QR code, and visual secret sharing altogether for protecting the copyright of progressively transmitted images.

Based on the global and local characteristics of original images, researchers utilize the histogram and the difference values to make reversible data hiding possible. With the enhanced performances, researchers tend to use the difference corresponding to original image for data hiding. The difference values come from both the original image and the predicted image relating to the original one. Here, we employ the prediction-based scheme for data hiding. The steps are briefly described as follows.

Steps at the encoder are listed below.

Step 1. Perform prediction in [2] from the original image in the base and enhancement layers for progressive transmission. Obtain the predicted images in the red, green, and blue planes.

Step 2. Calculate the differences between predicted and original images. Generate the three difference histograms relating to each color plane for hiding the secret shares corresponding to the QR code.

Step 3. Choose the embedding level (EL), or a positive integer denoting the portion for intentionally modifying the histogram for secret embedding. The secret shares are hidden into the designated color planes for PIT. In the difference histogram, move the positive part to the right, and the negative part to the left with the EL. Embed the secret shares by following the schemes in [5].

Step 4. Reconstruct the marked image by adding the modified difference value back to the original image layer by layer.

Correspondingly, steps at the decoder are listed below.

Step 1. Generate the difference histogram in each layer of received color image.

Step 2. With the provision of EL value, secret bits can be extracted sequentially, and secret shares can be produced from the designated color plane. QR code can be reconstructed subsequently.

Step 3. Recover the original difference histograms corresponding to each color plane in each layer, and add the difference back to obtain the original image in each layer for progressive transmission.

3 Proposed Applications with QR code and Secret Sharing

For the copyright protection, we propose to hide the QR code [6] with the information corresponding to the copyright owner into the progressively transmitted images. In order to convert the QR code into the noise-like patterns, and to consider utilizing different color planes for hiding data, we employ visual secret sharing [7] to produce the shares for further protection. After data hiding, the marked image can be obtained, which is suitable for progressive transmission.

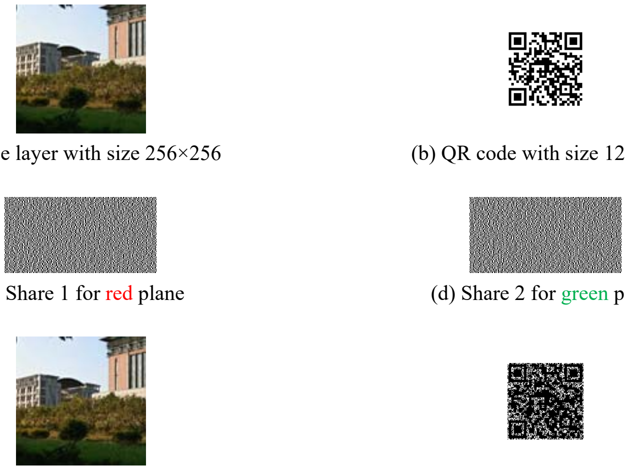
With our application, the maximal capacity in the base and enhancement layers for progressive transmission should be estimated in advance. Next, the size of the QR code can be determined. Later on, by use of (2, 2) visual secret sharing, two shares can be produced, and hence they can be reversibly hidden into original image. After embedding, the marked image can be delivered to the decoder.

Note that after the completion of visual secret sharing, the width of each share gets doubled to its QR code counterpart. Upon completion of data extraction in reversible data hiding, the width of composed QR code is also doubled. Hence, we choose to collect all the odd-numbered columns altogether to obtain the reconstructed QR code. Due to the error correcting capability of QR code, it would be convenient for later use by mobile phones and link to the designated websites to keep the copyright of images.

4 Simulation Results

With the proposed application, we choose the test image `NUK-building`, with the size of 1024×1024, for conducting simulations. The image is taken in the campus of the first author's affiliation, or the campus at National University of Kaohsiung (NUK) by ourselves. With progressive transmission, we set the base layer with the size of 256×256. For the first and second enhancement layers, the sizes are 512×512 and 1024×1024, respectively.

In Fig. 1, the base layer of original image with the size of 256×256 in Fig. 1(a) can be processed firstly. After performing prediction between predicted color planes and original color planes, we can randomly choose the red and green planes for data hiding. By calculating the differences between original and predicted images, the red and green planes can hide 34141 and 34787 bits, respectively, which lead to the maximally allowable capacity of 68928 bits. Hence, we choose the QR code with the size of 120×120, containing the information of the homepage of NUK, in Fig. 1(b). Next, by use of visual secret sharing, the two shares with the sizes of 120×240 are presented in Fig. 1(c) and Fig. 1(d), respectively. We notice that both Share 1 and Share 2 have 120×240×2 = 57600 bits altogether, which is below the maximally allowable capacity. After data embedding, we obtain the marked image in Fig. 1(e). For checking the copyright information contained in the QR code, after performing the reverse operations, both shares can be perfectly extracted, and they are composed to obtain the flattened pattern with the size of 120×240. By gathering the odd-numbered columns altogether, we have the reconstructed QR code in Fig. 1(f). We can then use the mobile phone camera to capture the reconstructed QR code and link to the designated webpage due to the error correcting capability provided by the QR code standard. Even though Fig. 1(b) and Fig. 1(f) are not identical, the homepage of NUK can still be accessed successfully. In addition, with reversible data hiding, original base layer can be recovered at the decoder, which is identical to Fig. 1(a).



(a) Base layer with size 256×256

(b) QR code with size 120×120

(c) Share 1 for red plane

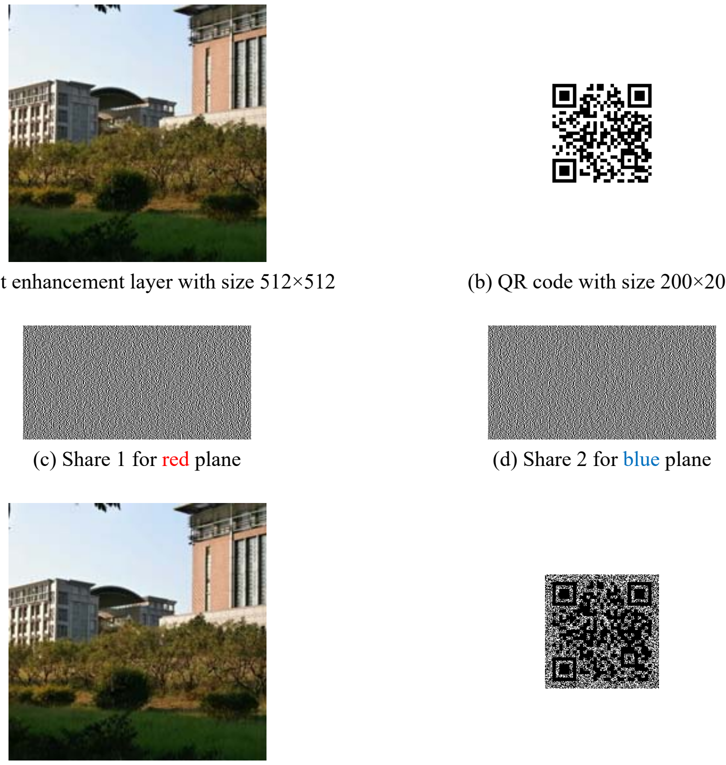
(d) Share 2 for green plane

(e) Marked image, max. capacity of 68928 bit @ 31.96 dB

(f) Reconstructed QR code

Fig. 1. Simulations with the base layer with size 256×256 for test image `NUK-building`.

By following the similar manner, we can perform data embedding in the enhancement layers in Fig. 2 and Fig. 3, respectively. For demonstrations, we choose the homepage of College of Engineering of NUK to present the QR code in the first enhancement layer, and the homepage of Department of Electrical Engineering of NUK to present the QR code in the second enhancement layer, respectively. It follows the hierarchical structure of the university with the similar concept to PIT. In Fig. 2, we can randomly choose the red and blue planes for data hiding. By calculating the differences between original and predicted images, the red and blue planes can hide 149038 and 140907 bits, respectively, which lead to the maximally allowable capacity of 289945 bits in Fig. 2(a). Hence, we choose the QR code in Fig. 2(b) with the size of 200×200 for producing the two shares in visual secret sharing in Fig. 2(c) and Fig. 2(d). Each share has the size of 200×400, and both shares have 160000 bits altogether, which is below the maximally allowable capacity. After embedding, we have the marked image in Fig. 2(e). We follow the reverse procedures to obtain the reconstructed QR code in Fig. 2(f). With the help of mobile phone camera, the reconstructed QR code is recognizable and the webpage of College of Engineering of NUK can be accessed. Besides, with reversible data hiding, the first enhancement layer can be recovered at the decoder, which is identical to Fig. 2(a).



(a) First enhancement layer with size 512×512

(b) QR code with size 200×200

(c) Share 1 for red plane

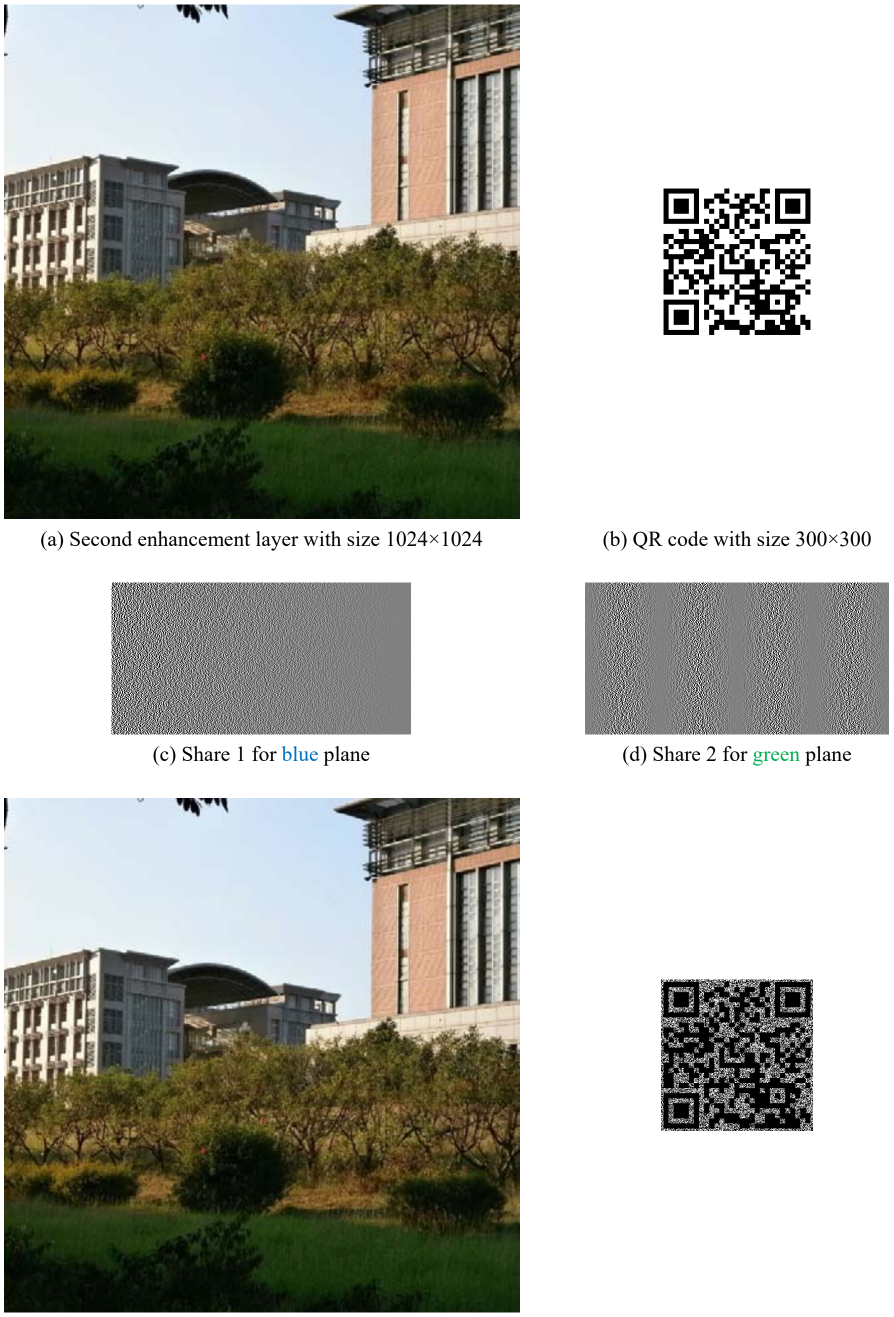
(d) Share 2 for blue plane

(e) Marked image, max. capacity of 289945 bit @ 33.18 dB

(f) Reconstructed QR code

Fig. 2. Simulations with the first enhancement layer with size 512×512 for test image `NUK-building`.

In Fig. 3, by following the operations in Fig. 1 and Fig 2 respectively, it reveals the results with the second enhancement layer. In order to differentiate from the color planes for embedding in Fig. 1 and Fig. 2, we can randomly choose the blue and green planes for hiding the shares in VSS. By calculating the differences between original and predicted images in this layer, the blue and green planes can hide 617546 and 662139 bits, respectively, which lead to the maximally allowable capacity of 1279685 bits in Fig. 3(a). Hence, we choose the QR code in Fig. 3(b) with the size of 300×300 for producing the two shares in visual secret sharing in Fig. 3(c) and Fig. 3(d). Each share has the size of 300×600, and both shares have 360000 bits altogether, which is below the maximally allowable capacity. After embedding, we have the marked image in Fig. 3(e) with good quality. Embedded shares are imperceptible . We follow the reverse procedures to obtain the reconstructed QR code in Fig. 3(f). With the help of mobile phone camera, the reconstructed QR code is recognizable and the webpage of Department of Electrical Engineering of NUK can be accessed. Also, with the procedures of reversible data hiding at the decoder, the second enhancement layer can be recovered, which is identical to Fig. 3(a).



(a) Second enhancement layer with size 1024×1024

(b) QR code with size 300×300

(c) Share 1 for blue plane

(d) Share 2 for green plane

(e) Marked image, max. capacity of 1279685 bit @ 34.29 dB

(f) Reconstructed QR code

Fig. 3. Simulations with the second enhancement layer with size 1024×1024 for test image `NUK-building`.

From the demonstrations of progressive image transmission with QR code and secret sharing from Fig. 1 to Fig. 3, it reveals the applicability for copyright protection in each layer for progressive transmission. The size of the QR code, and consequently the sizes of the shares in visual secret sharing, can be determined by the copyright owner under the condition to fall within the maximally allowable capacity. Reconstructed QR code from the composition of secret shares may look different from the embedded QR code. Even so, with the error correcting capability provided by the QR code, we can still use the mobile phone camera to capture the reconstructed QR code and link to the designated webpage of the copyright owner.

5 Conclusions

In this paper, we propose the application of copyright protection for progressive image transmission with QR code and visual secret sharing. Reversible data hiding algorithm is selected to hide the secret shares corresponding to the QR codes relating to copyright owners. For progressive image transmission, the secret shares can be respectively hidden into the base and enhancement layers of original color images. After the progressive reception of images, the shares corresponding to each layer can be composed altogether to produce the reconstructed QR codes. Users can use the mobile phone camera to scan the reconstructed QR codes and then link to the websites of copyright owners. With the proposed application in this paper, it can be practical and easily implementable for copyright protection of progressive image transmission.

Acknowledgement

The authors would like to thank Ministry of Science and Technology (Taiwan, R.O.C.) for supporting under Grants MOST 105-2221-E-390-022 and MOST 106-2221-E-390-024.

References

1. Chen, Y.H., Huang, H.C.: Coevolutionary Genetic Watermarking for Owner Identification. Neural Computing and Applications, 26, 291–298 (2015)
2. Lin, Y.C.: Reversible Data Hiding for Progressive Image Transmission. Signal Processing: Image Communication, 26, 628–645 (2011)
3. Wang, J., et al.: Rate and Distortion Optimization for Reversible Data Hiding Using Multiple Histogram Shifting. IEEE Trans. Cybernetics, 47, 315–326 (2017)
4. Huang, H.C., et al.: Reversible Data Hiding with Histogram-based Difference Expansion for QR Code Applications. IEEE Trans. Consumer Electronics, 57, 779–787 (2011)
5. Huang, H.C., Chang, F.C.: Hierarchy-based Reversible Data Hiding. Expert Systems with Applications, 40, 34–43 (2013)
6. ISO/IEC 18004: Information Technology – Automatic Identification and Data Capture Techniques – QR Code Bar Code Symbology Specification (2015)
7. Naor, M., Shamir, A.: Visual Cryptography. Lecture Notes in Computer Science, 950, 1–12 (1995)