2023 62nd Annual Conference of the Society of
Instrument and Control Engineers of Japan (SICE)
September 6-9, 2023. Tsu City, Japan

# Deep photographic steganography using two-dimensional barcodes and with robustness to image perturbations

Yoshinobu Hayakawa[1], Hironori Takimoto[1†] and Akihiro Kanagawa[1]

[1]Faculty of Computer Science and Systems Engineering, Okayama Prefectural University, Okayama, Japan
(Tel: +81-866-94-2004; E-mail: takimoto@c.oka-pu.ac.jp)

**Abstract:** Our final objective is to achieve a solution that avoids visible and unsightly barcodes by invisibly embedding within images 2D barcodes encoded with short-string digital information. This study proposes a deep photographic steganography that uses 2D barcodes and is robust to image perturbations caused by printing and scanning devices. We proposed model training using a distortion network to improve the restoration performance of the 2D barcodes. In addition, the invisibility of 2D barcodes in container images was improved by applying a low-contrast method to the 2D barcodes. The experimental results confirmed the effectiveness of the proposed method in terms of both invisibility and restoration performance.

**Keywords:** Image steganography, deep learning, 2D barcodes

## 1. INTRODUCTION

It is well-known that barcodes are one of the most practical solutions for storing and transmitting short-string data. The most widely used type of visual 2D code is quick response (QR) codes [1]. It requires only simple data-capturing hardware, such as a scanner or camera. Their use has further increased in various industries as a convenient method for contactless data transmission.

The visual appearance of 2D codes are distinct because their presence can easily and clearly be perceived. Though conspicuous appearance may be seen as an advantage in some scenarios, the inflexible aesthetics of visual codes is a challenge in some use cases. There is a desire to develop codes that are less conspicuous or aesthetically variable [2-4]. In general, such techniques involve a tradeoff between aesthetics and performance. The less "code-like" the barcoding is to humans, the more difficult it is for software to locate and decipher the code accurately [5].

On the other hand, steganography is a technology that conceals information by embedding it in other information [6]. Invisible embedding conceals the existence of the secret information itself, thus enabling secure storage and transmission of the data. Recently, steganography for electronic data has been studied for sounds and images, which is used for embedding copyright information.

In recent times, convolutional neural network (CNN) models based on deep learning [7] has become the most influential architecture for addressing computer vision tasks. Baluja proposed "Deep Steganography" [8] based on deep learning. The proposed "Deep Steganography" consists of three networks: a network for feature extraction of secret images, an auto-encoder-based network [9] for embedding, and a restoration network. In addition, the entire network is trained in an end-to-end manner to achieve steganography of images. Compared to existing non-deep-learning steganography [10, 11], Baluja's "Deep Steganography" achieves embedding of a large amount of information within images while maintaining a high degree of invisibility. However, not only Baluja's "Deep Steganography", but also other existing methods [10-14] are based on the assumption that container images are transmitted digitally. Therefore, they are not robust to image perturbations in real-world information transmission methods such as printing or data capturing by cameras/scanners. That is, the technology of steganography has not yet penetrated people's day-to-day living because it is challenging to apply it to more practical and common applications using scanning or printing devices.

Here, we propose photographic steganography for 2D barcodes that considers the image perturbations caused by printing and scanning devices. Fig. 1 shows a basic concept of our proposed image steganography. For our model training with robustness to the image perturbations, we propose an image degradation-aware deep steganography model by adding noise to the container image. In addition, to improve the invisibility of the container image, a low contrast technique is proposed for the 2D barcodes. Our final goal is to achieve a solution that avoids visible and unsightly barcodes by invisibly embedding 2D barcodes with short-string digital information within natural images. Image steganography technology that uses 2D barcodes, and is robust to image perturbations caused by printing and capturing by cameras and scanners, is expected to have various application scenarios.

## 2. PROPOSED METHOD

Our objective is to realize image steganography using 2D barcodes and taking into account the image quality degradation caused by printing and data capturing or scanning devices. First, we assume to use a digital scanner as the scanning device. An overview of the proposed deep learning-based image steganography is shown in Fig. 2. Here, the main challenge of this study is that the decoding procedure needs to recover the hidden information from photos that contain perturbations/distortions

† Hironori Takimoto is the presenter of this paper.

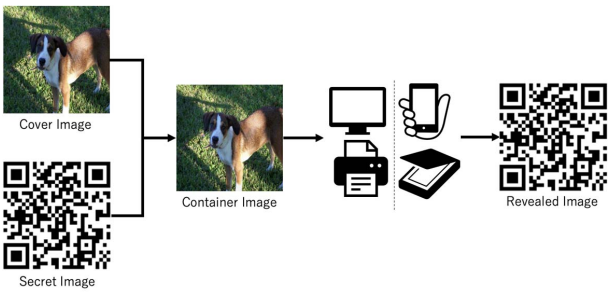


Fig. 1 Overview of our proposed image steganography

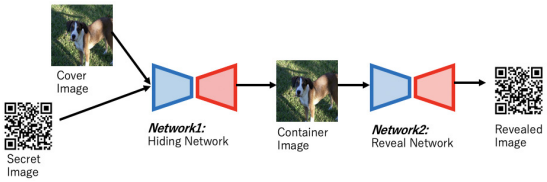


Fig. 2 Pipeline of our proposed deep image steganography

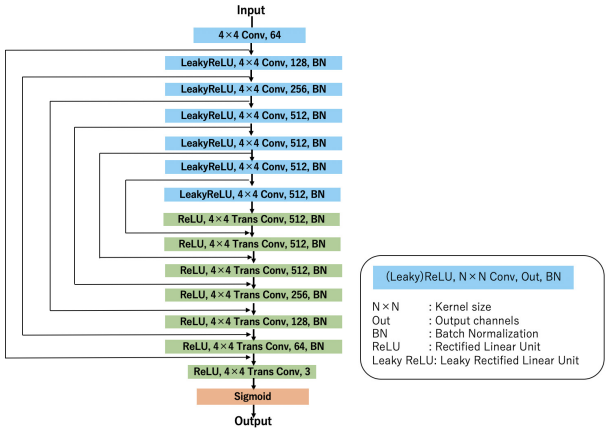


Fig. 3 Architecture of the hiding network

caused by the printing and scanning process. These perturbations/distortions can be divided into three categories according to their sources: distortions from printing (such as color reproduction, ink blurring, and paper color), distortions from scanning devices (including compression, geometric distortion, and noise).

The basic architecture of the proposed image steganography is based on the autoencoder-based "Deep Steganography" proposed by Baluja [8]. In terms of difference from Baluja's model, the proposed model does not include a preparation network that extracts features from the secret image in advance because the same size of secret and cover images can always be used. Therefore, in this study, only the hiding and reveal networks are used to construct the deep network on which the image steganography is based. The hiding and reveal network structures are shown in Fig. 3 and Fig. 4.

The hiding network is a U-Net type convolutional network [15], which generates a container image from the cover and secret images. The image information for a total of six channels, which concatenate the cover and secret images, is input to the hiding network. Conversely, the reveal network restores the revealed image using the container image as a direct input. The reveal network in

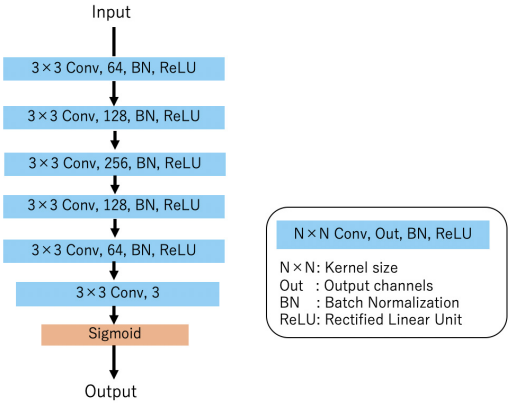


Fig. 4 Architecture of the reveal network

our proposed model consists of six convolutional layers with a kernel size of $3 \times 3$. It should be noted that cover, secret, container, and revealed images are all defined as 8-bit×3-channel RGB images.

In the proposed method, each network needs to be trained by factoring in the image quality degradation caused by printing and scanning devices. We insert a distortion network between the hiding and reveal networks to simulate image quality degradation (that potentially could be) caused by printing and scanning processes. The distortion network adds noise simulated by a Gaussian noise model (sampling standard deviation U[0, 0.1]) to the container image. The two networks can learn to resist image quality degradation with the help of the distortion network.

Our proposed model consisting of two networks is trained end-to-end by optimizing the following loss function $L$.

$$L(c, c', s, s') = L_H(c, c') + \beta \times L_R(s, s') \tag{1}$$

The $L_H$, which is the mean squared error of the pixel values between the cover image $c$ and the container image $c'$, is defined by

$$L_H(c, c') = ||c - c'|| \tag{2}$$

where $\beta$ is a hyperparameter that determines the weights of the restoration. The $L_R$, which is the mean squared error of the pixel values between the secret image $s$ and the revealed image $s'$, is defined by

$$L_R(s, s') = ||s - s'|| \tag{3}$$

Next, the range of pixel values representing the 2D barcode is compressed by:

$$s'_{ij} = \begin{cases} x & if \quad s_{ij} < x \\ s_{ij} & if \quad x \leq s_{ij} < 255 - x \\ 255 - x & \text{otherwise} \end{cases} \tag{4}$$

where $s_{ij}$ is the RGB value of pixel $(i, j)$, and $x$ is a parameter in the range between 0 and 127. This is a low-contrast 2D barcode to improve the invisibility of the 2D codes in the container image.

Fig. 5 Example of QR code used for our experiments

## 3. EXPERIMENT

### 3.1. Experimental setup

To validate the effectiveness of the proposed method, we performed experiments using real data and devices. The images included in the following datasets were used as cover images.

– The images of dogs and cats included in the "Dogs vs. Cats" Kaggle dataset [16]
– Human face images included in "Labeled Faces in the Wild dataset (LFW dataset) [17]"

For training the deep steganography model, 1650 images from both dataset were used as cover images. The remaining images were used for testing.

In contrast, 1650 barcode images are used for model training. These barcodes were generated by error correction level $M$ (correctable up to approximately 15%). An example of the generated barcode is shown in Figure 5. The barcodes contain random alphanumeric information of 30-100 characters.

As parameters for model training, the batch size was set to 6, the number of epochs to 150, the optimization method was Adam, and the learning rate was set to 0.001. The size of the cover image and the 2D barcode image was 512 x 512 pixels. The parameter for the loss function was set to $\beta = 0.3$. The parameter $x$ for low-contrast 2D codes was empirically set to 100.

The outline of the evaluation experiment is described as follows. First, the steganography model is trained end-to-end using training images. Next, the evaluation images are input to the hiding network to obtain a container image. Note that a distortion network is not applied to the evaluation images. The container image is then printed using a printer. The printed container image is captured by the scanner and cropped manually. Finally, the cropped container image is input to the Reveal network to extract the 2D barcode as a revealed image. The extracted 2D barcode was decoded by using an iPhone SE to evaluate whether the Reveal network correctly recovered the 2D barcodes. A 2D barcode recovery was defined as successful if the embedded alphanumeric characters were decoded correctly.

An EPSON LP-S7160 was used as a printer for printing container images. A color laser paper (PLUS PP-120-WH-T) was used as the printing paper. For scanning, we used a Brother MFC-L8610CDW to capture the printed images. The resolution of the capture was 300 dpi.

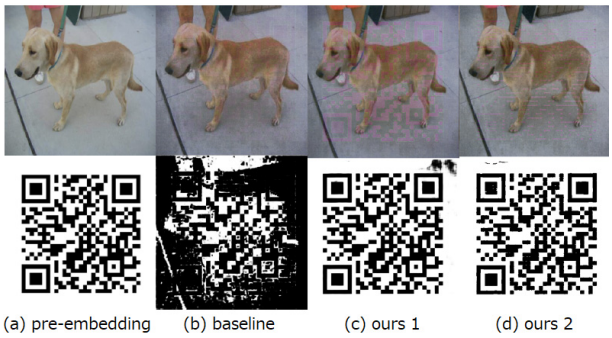


Fig. 6 Comparison of container and revealed images (sample 1)

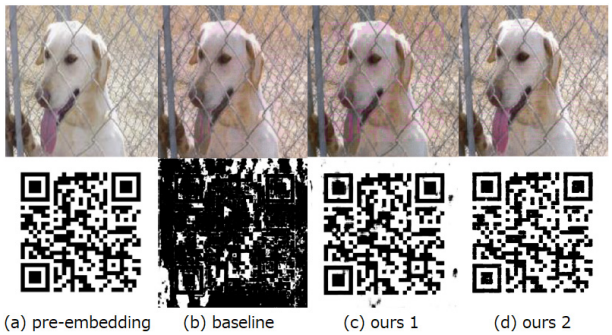


Fig. 7 Comparison of container and revealed images (sample 2)

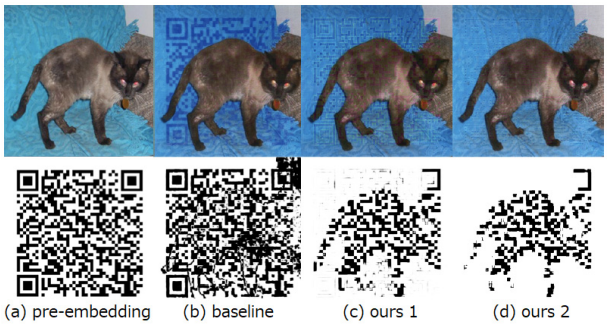


Fig. 8 Comparison of container and revealed images (sample 3)

### 3.2. Results and discussion

To validate the effectiveness of the methods we have proposed in this paper, we compare the performance of the following three models.

– **baseline**
– **ours-1** : Baseline with a distortion network
– **ours-2** :Baseline with a distortion network and low-contrast barcodes

Baseline is Baluja's Deep steganography method without the preparation network. In other words, the baseline is representative of conventional deep steganography methods.

The results of the experiment are shown in Figs. 6, 7, and 8. Table 1 also shows the results indicating whether the embedded 2D barcodes could be correctly recovered (decoded). Figures 6, 7, and 8 show from left to right the pre-embedding images, and the revealed images after applying a baseline method and our two proposed methods,

Table 1 Decoding results for extracted 2D barcodes

| | baseline | ours-1 | ours-2 |
|---|---|---|---|
| sample 1 | × | ○ | ○ |
| sample 2 | × | ○ | ○ |
| sample 3 | × | × | × |

ours-1 and ours-2. In the first column of each figure, the top row is the cover image, and the bottom row is the Secret image. In columns 2 to 4, the top row is the container image, and the bottom row is the revealed image.

First, the embedded information could not be decoded correctly for all the evaluation images when using the baseline. On the other hand, the proposed method was able to correctly decode the embedded information for some samples. Thereafter, training the steganographic model with the addition of Gaussian noise by a distortion network improved its robustness against degradation due to printing and scanning. When comparing the results of the two proposed methods (ours-1 and-2), the number of samples that could be decoded was the same. However, when comparing the container image generated by each method with the cover image, it was subjectively confirmed that the container image of ours-2 was more similar to the cover image. This means that the low contrast reduced the visibility of the 2D barcode in the container image.

Although the proposed method improved the restoration performance, half of all images could be restored as readable 2D barcodes when printed or scanned. It means that the performance of the proposed method is currently insufficient for practical use. In addition, the factors that cause image degradation in practical use vary depending on the means of usage and environment. For example, in image capturing with a camera, the set-up of the environment, such as the brightness, can be a significant factor in image quality degradation. In future works, robustness against various degradation factors should be evaluated, and further improvements in restoration performance and generalizability are required.

## 4. CONCLUSIONS

This study proposed deep photographic steganography that uses 2D barcodes and is robust to image perturbations caused by printing and scanning devices. First, model training with a distortion network was used to improve the restoration performance of 2D barcodes. Next, the invisibility of 2D barcodes in container images was improved by a low contrast technique. From the results of evaluation experiments, the proposed method's effectiveness was confirmed in terms of both invisibility and restoration performance.

## REFERENCES


[1] QR codes. https://www.denso-wave.com/en/technology/vol1.html, 2023/2/29

[2] Z. Yang, Y. Bao, C. Luo, X. Zhao, S. Zhu, C. Peng, Y. Liu, and X. Wang, "ARTcode: Preserve Art and Code In Any Image", *Proc. of UbiComp 2016*, pp. 904–915, 2016.

[3] M. Xu, Q. Li, J. Niu, X. Liu, W. Xu, P. Lv, and B. Zhou, "ART-UP: A Novel Method for Generating Scanning-robust Aesthetic QR codes", *arXiv preprint*, arXiv:1803.02280, 2018.

[4] X. Xu, H. Su, Y. Li, X. Li, J. Liao, J. Niu, P. Lv, and B. Zhou, "Stylized Aesthetic QR Code", *IEEE Trans. Multimedia*, Vol. 21, No. 8, pp. 1960–1970, 2019.

[5] Y. Takeuchi, "Ninja Codes: Exploring Neural Generation of Discreet Visual Codes", *Proc. of Conference on Human Factors in Computing Systems (CHI 2021)*, No. 224, 2021.

[6] T. Morkel, J. H. Eloff, and M. S. Olivier, "An overview of image steganography", *Proc. of the Fifth Annual Information Security South Africa Conference*, pp. 1–11, 2005.

[7] Y. LeCun, Y. Bengio, and G. Hinton, "Deep learning", *Nature*, Vol. 521, pp. 436–444, 2015.

[8] S. Baluja, "Hiding images in plain sight: Deep steganography", *Proc. of 31st Conference on Neural Information Processing Systems*, Vol. 30, pp. 2069–2079, 2017.

[9] G. E. Hinton and R. R. Salakhutdinov, "Reducing the dimensionality of data with neural networks", *Science*, Vol. 313, pp. 504–507, 2006.

[10] N. F. Johnson and S. Jajodia, "Exploring Steganography: Seeing the Unseen", *Computer*, Vol. 31, No. 2, pp. 26–34, 1998.

[11] L. M. Marvel, C. G. Boncelet, and C. T. Retter, "Spread Spectrum Image Steganography", *IEEE Transactions on Image Processing*, Vol. 8, No. 8, pp. 1075–1083, 1999.

[12] H. Shi, J. Dong, W. Wang, Y. Qian, and X. Zhang, "Ssgan: Secure Steganography Based on Generative Adversarial Networks", *In Advances in Multimedia Information Processing*, pp. 534–544, 2018.

[13] D. Volkhonskiy, I. Nazarov, and E. Burnaev, "Steganographic Generative Adversarial Networks" *arXiv preprint*, arXiv:1703.05502, 2017.

[14] K. A. Zhang, A. C. Infante, L. Xu, and K. Veeramachaneni, "Steganogan: High Capacity Image Steganography with Gans", *arXiv preprint*, arXiv:1901.03892, 2019.

[15] O. Ronneberger, P. Fischer, and T. Brox, "U-Net:Convolutionalnetworksforbiomedical imagesegmentation", *Proc. of International Conference on Medical Image Computing and Computer Assisted Intervention*, pp. 234–241, 2015.

[16] Kgggle.com, "Dogs vs. Cats", https://www.kaggle.com/competitions/dogs-vs-cats/overview, 2023/2/29.

[17] G. B. Huang, M. Ramesh, T. Berg, and E. Learned-Miller, "Labeled Faces in the Wild: A Database for Studying Face Recognition in Unconstrained Environments", *University of Massachusetts, Amherst, Technical Report*, pp. 7–49, 2007.