17th International Conference on Machine Vision Applications (MVA)
Fully Online, July 25–27, 2021.

Information Hiding Using a Coded Aperture as a Key

Tomoki Minamata, Shoma Ishida, Hiroki Hamasaki
Kagoshima University, Japan
{sc117071, sc115029, sc114048}@ibe.kagoshima-u.ac.jp

Hiroshi Kawasaki
Kyushu University, Japan
kawasaki@ait.kyushu-u.ac.jp

Hajime Nagahara
Osaka University, Japan
nagahara@ids.osaka-u.ac.jp

Satoshi Ono
Kagoshima University, Japan
ono@ibe.kagoshima-u.ac.jp

Abstract

This paper proposes a visual information hiding technique using coded apertures as a key. In general, a watermark embedded as high-frequency components is difficult to extract if it is captured outside of the focal rength and defocus blur occurs. Installation of a coded aperture (CA) into the camera is a simple solution to mitigate the difficulty and several attempts are conducted to make better design for stable extraction. To the contrary, our motivation is to design a specific CA as well as information hiding scheme, where secret information can be decoded only if an image with hidden information is captured with the key aperture whose characteristic is matched with the information hiding scheme. The proposed technique designs the key aperture patterns and information hiding scheme through evolutionary multi-objective optimization so as to minimize the decryption error of a hidden image when using the key aperture while minimizing the accuracy when using other apertures. Experimental results have shown that the proposed information hiding technique was more secure than a password-based system which uses case-insensitive eight alphanumeric characters.

1 Introduction

Coded aperture based techniques are one of the representative area of computational photography, which integrates imaging device (hardware) and image processing technique (software) to achieve better photography than ever. A coded aperture is a non-circular 2D pattern mask which is inserted into the aperture position of the camera for various purposes [1–7], *e.g.*, deblurring, super-resolution, all-focus image production, light-field capturing, and so on.

One of the promising fields where computational photography is expected to be applied is watermarking and information hiding. Pramila *et al.* and Hamasaki *et al.* proposed methods to extend the range of angles or depths at which watermarks can be extracted using focal stack imaging and coded apertures, respectively [8, 9]. In our method, we also propose a method for information hiding; however, to the contrary, our purpose is to use a CA as a key for decoding. Possible scenario is that the watermarked image can be correctly decoded only if it is captured by the camera which is equipped with specific CA as a key. The proposed method embeds a secret image to a cover image by adding carefully designed perturbations and applying deconvolution with a key apreture as a kernel. These processes make the image with the secret information look like a random dot pattern. Decoding the hidden information is difficult when using well-known coded apertures for deblurring such as [1] or even when capturing at focal length. To enhance the confidentiality, the proposed method simutaneously optimizes the perturbation pattern and the key CA pattern suitable for the above purpose using Evolutionary Multi-objective Optimization (EMO) algorithm where the margin of the decryption error between the key and other apertures is maximized and the error of the key are minimized.

The followings are the contributions of this paper.

- To the best of our knowledge, this is the first study to employ a coded aperture as a key for information hiding.
- The proposed method optimizes the perturbation pattern for information hiding and the key CA pattern. Both factors are simultaneously optimized by EMO.
- Experiments showed that the proposed method achieved more secure than a case-insensitive eight alphanumeric character password.

2 Related work

Few studies have devoted to the applications of computational photography to digital watermarking and information hiding. Pramila et al. proposed a watermark extraction method that captures a focal stack of the watermarked image to extend the capturing angle of watermarked images [8]. Hamasaki et al. proposed a coded aperture imaging method to extend the depth

of field for watermark extraction by designing an aperture suitable for watermark extraction from blurred images [9]. Wengrowski et al. approximate the transformation function between a display and a camera using deep neural networks [10]. Unlike these methods, the proposed method is a new information hiding technique that takes advantages of the difficulty of watermark extraction.

On the other hand, in the field of visual cryptography, there have been several studies using various media as keys. Yamamoto et al. proposed a method that visualizes the confidential information by holding a decoder mask in front of the display [11]. Sugawara et al. proposed a method that embeds encrypted information into a retarder film and decrpyts by sandwiching it with polarized films [12]. Kowa et al. proposed an information hiding method that adopts a polarized illumination condition with a specific wavelength as a key [13]. This study attempts to apply coded aperture imaging to the above mentioned visual cryptograhy.

3 Proposed Information Hiding Method

3.1 Key ideas

The proposed method conceals a hidden image by converting it into a pattern similar to random dots, and decodes the hidden image by capturing the random dot-like pattern with a key aperture at a specific distance outside the focus range. Followings are the key ideas of the proposed method.

Idea 1: Deconvolution-based information hiding. Information hiding using a CA as a key seems to be achieved by a naive method that embeds a watermark as high-frequency components of a cover image like [9]. This is because a certain CA whose frequency response correspond to those of the watermark is essential to decode the hidden image when capturing at the distance outside the focal range. However, if the image is captured at the focal distance, the hidden information could be decrypted without the key aperture.

Therefore, this paper proposes a method to embed a hidden image to a random dot-like pattern image, so that the presense of hidden information is not easily deteted and it cannot be decoded without the key aperture when captured at the focal range. To generate the random dot-like pattern image, the proposed method adds perturbations to the hidden image and applies deconvolution to the perturbed image with the key aperture as a kernel. The hidden image can be decrypted by capturing the random dot-like pattern by a camera including the key aperture at a certain distance outside the focal range.

The above idea of restoring an image by optical convolution is similar to previous work for extending projector depth-of-feld [14], but the task is different.

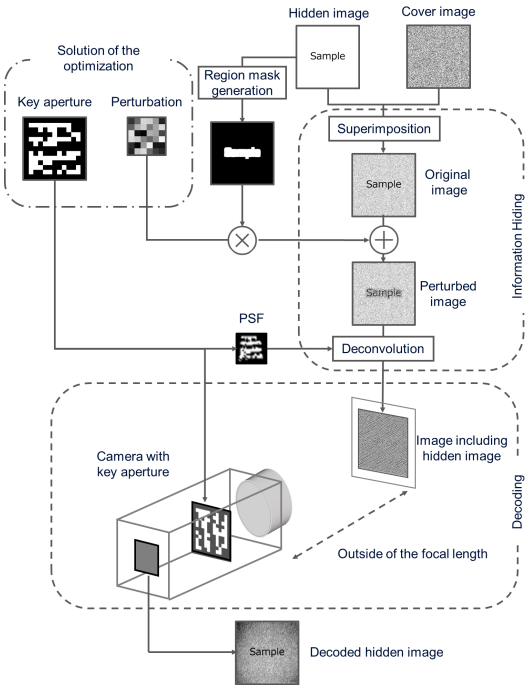


Figure 1. Process flow of the proposed method

Idea 2: Multi-objective optimization for enhancing confidentiality. To generate random dot-like images including hidden information, the proposed method requires a perturbation pattern and a key aperture pattern that are mutually suitable for each other. Therefore, the proposed method designs the perturbation pattern and key aperture pattern by simultaneously maximizing the reconstruction accuracy of the hidden image when captured with the key aperture, while minimizing the accuracy with other apertures and maximizing the likelihood of the image including hidden information as a random dot pattern.

3.2 Outline of the proposed method

Fig. 1 summarizes the detailed outline of the proposed method, which comprises the information hiding phase and decoding phase.

In the information hiding phase, an image involving a hidden image is generated by deconvolution, which is usually applied as post-processing in general computational photography techniques. However, because the deconvolution alone is not sufficient to hide the information, the proposed method superimposes the hidden image and a cover image that contains a random dot pattern and then adds perturbations designed by optimization before deconvolution. This makes the hidden image similar to the random dot pattern. A key aperture whose patten is designed by optimization is used as a kernel when deconvolving the perturbed image. The above process generates the random-dot like im-

age including the hidden information that cannot be decoded without the key aperture even when captured at the focal distance.

In the decoding phase, a camera equipped with the key aperture can decode the hidden image by taking the image at a certain distance outside the focal range. Because no post-processing is required, it is also possible to decrypt the hidden image with instruments that can be looked at directly such as telescopes and kaleidoscopes.

3.3 Simultaneous design of coded apertures and perturbation patterns

In this study, multi-objective optimization simultaneously designs perturbation pattern $\boldsymbol{\chi}^{(P)}$ for creating random-dot like image including a hidden information and key coded aperture pattern $\boldsymbol{\chi}^{(A)}$. To enhance confidentiality, the multi-objective optimization searches for Pareto-optimal solutions that simultaneously attempt to minimize the visibility of the hidden information, to minimize the decoding error of the hidden information when captured with the key aperture, and to maximize the decoding error with non-key apertures.

Key aperture design is formulated as a combinatorial optimization. Design variables $x_{u,v}^{(A)}$ comprising $\boldsymbol{\chi}^{(A)}$ contain binary value where 0 and 1 correspond to blocking or passing the light at cell (u, v). The search space size is $2^{N_a \times N_a}$, where $N_a \times N_a$ is the number of binary aperture patterns with side length N_a. In accordance with the previous work [1, 9], N_a is set to 11 in this paper.

In the information hiding stage, before the deconvolution, a hidden image is superimposed with a random dot-like cover image and perturbed with pattern $\boldsymbol{\chi}^{(P)}$. Directly designing the perturbation patterns for high-resolution images leads to an increase of the number of variables, making optimization difficult. To reduce the number of dimensions of the optimization, this paper desgins N_{AP} local perturbation patterns for $n \times n$ pixel image block, and designs a pattern map [15].

The candidate solution $\boldsymbol{\chi}$ consisting of $\boldsymbol{\chi}^{(P)}$ and $\boldsymbol{\chi}^{(A)}$ is evaluated by three objective functions f_1, f_2 and f_3. The first objective function f_1 to be minimized is RMSE between the hidden image decoded by the key aperture and its original. The second objective function f_2 to be minimized is the visibility of the hidden information. This study defines f_2 as the likelihood as a random dot image, i.e., the ratio of the area of the remaining text characters after deconvolution against the average blob size of the cover image. The more similar the image including hidden information is to the random dot image, the lower the value of f_2 will be. The third objective function f_3 to be maximized is the difference between the recovery error $f_1(\boldsymbol{\chi})$ when using the key aperture and the minimum recovery error when using non-key apertures.

$$\text{minimize } f_3(\boldsymbol{\chi}) = f_1(\boldsymbol{\chi}) - \min_{r \in \{1,\ldots,N_A\}} f_1(\boldsymbol{\chi}_r^{(A)} \cup \boldsymbol{\chi}^{(P)}) \tag{1}$$

4 Experiments

The effectiveness of the prooposed information hiding method was verified both in simulation and with an actual device. First, the poposed method generated a set of perturbation and key aperture patterns by simultaneous optimization using EMO. Then, the confidentiality of the proposed method using the designed perturbation and key aperture was assessed using randomly-generated coded apertures similar to the generated key aperture. Finally, the result using the actual device was demonstrated.

In this study, the focal length of the camera was set to 50 mm from the camera front, and the target image including hidden information was placed at 80 mm, which is outside the focal range. The hidden and cover images were used shown in Figure 2.

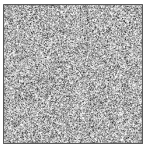
In this experiment, NSGAII [16], an evolutionary multi-objective optimization algorithm, was employed to simultaneously optimize the perturbation and key aperture patterns. Parameters for NSGA-II was configured as follows with reference to [9]; the population size and the generation limit were set to 100 and 2,000, respectively. The number of local perturbation patterns N_{AP} was set to 20.

Figure 3 show the distributions of candidate solutions in the initial and final generations in the objective function space whose axes are the objective functions. At the beginning, the random solutions could not make a difference in the recovery rate of the hidden information between the key and other apertures, i.e., values of f_3 were small. After optimization, some solutions were successfully desigend, which increased the margin between the key and other apertures while reducing the erros with the key aperture.

Figure 4 shows examples of the key aperture, the perturbed image, the image including hidden one, and the decypted hidden image with the key aperture. It can be seen that the visibility of the hidden information in Figure 4(d) was kept low, and that most of the characters in the hidden image were visible as shown in Figure 4(e).

Next, the confidentiality of the designed set of the key aperture and the perturbation patterns shown in Figure 4 was verified in the simulation. In this experiment, the reconstruction error was compared between the key aperture and other apertures similar to the key. For each Hamming distance from the key, 100 apretures were made by randomly modifying the key.

Figure 5 shows the averaged reconstruction errors for each Hamming distance. The horizontal and vertical axes indicate the distance from the key aperture



i) Cover image

ii) Hidden image

Figure 2. Cover and hidden images.

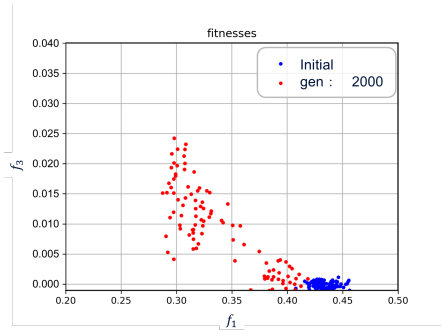
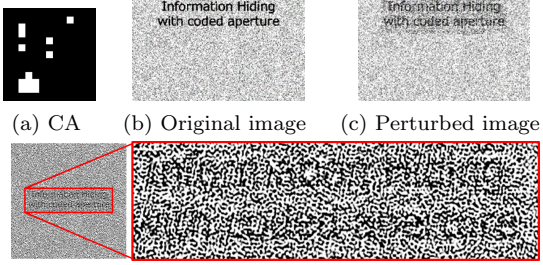


Figure 3. Distributions of soltuion candidates in the objective space (f_1-f_3).



(a) CA (b) Original image (c) Perturbed image

(d) Image including hidden image

(e) Decoded hidden image with the key aperture

Figure 4. Best solution designed in simulation.

and the reconstruction error, respectively. The error at the distance zero denotes the error with the key aperture. The averaged error shown as the orange-colored curve demonstrates that the decryption error increased as the Hamming distance from the key increased.

Figure 6 shows examples of apertures and recovered hidden images. It can be seen that when the Hamming distance exceeds 20, it becomes difficult to distinguish the characters in the image. Here, we assume that the characters in the hidden image cannot be read if the distance is greater than 20. Inhat case, the total number of the aperture patterns is $\sum_{d=0}^{20} {}_{121}C_d \simeq 4.4 \times 10^{22}$, which is $\frac{1}{6.1 \times 10^{13}}$ of all aperture patterns that can be represented in 11×11 cell. Therefore, the proposed information hiding method can be regarded as more secure than a password consisting of eight case-insensitive alphanumeric characters (2.9×10^{12} patterns).

Finally, the designed set of the key aperture and the

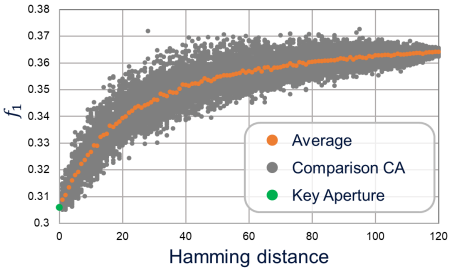
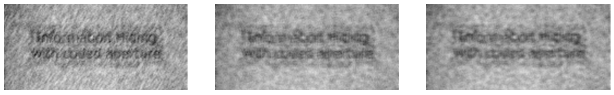
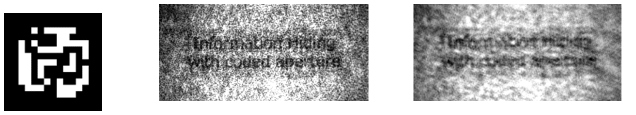


Figure 5. Confidentiality of the designed image and the key aperture.



(a) Distance: 10 (b) Distance: 20 (c) Distance: 40

Figure 6. Examples of decrypted hidden images.



(a) CA for deblurring [1] (b) Decrypted result using the key (c) Decrypted result using (a)

Figure 7. Results with the actual device.

perturbation patterns shown in Figure 4 was tested in the actual enviromnent including a programmable-aperture camera [17]. An aperture for deblurring [1] shown in 7(a) was also tested.

Figure 7(b) and (c) show the decrypted hidden images with the key aperture and the one for deblurring. The brightness of the result images were adjusted. From the figure, the decrypted hidden image using the key was closer to the original hidden image than the one using [1], though it is necessary to improve the proposed method such as introducing the refinement process in the actual environment in order to obtain an image that is clear enough to read the characters.

5 Conclusions

This paper proposes a simple information hiding method that employs a coded aperture as a key. The proposed method embeds hidden information into random dot-like images by deconvolution. Experimental results showed that simultaneous optimization of key aperture and perturbation design achieved the confidentiality more secure than a password consisting of eight case-insensitive alphanumeric characters. In future, we plan to introduce refinement process with actual devices.

References

[1] Changyin Zhou and Shree Nayar. What are good apertures for defocus deblurring? In *Computational Photography (ICCP), 2009 IEEE International Conference on*, pp. 1–8. IEEE, 2009.

[2] Anat Levin, Rob Fergus, Frédo Durand, and William T Freeman. Image and depth from a conventional camera with a coded aperture. *ACM Transactions on Graphics (TOG)*, Vol. 26, No. 3, p. 70, 2007.

[3] Changyin Zhou, Stephen Lin, and Shree Nayar. Coded aperture pairs for depth from defocus. In *IEEE 12th International Conference on Computer Vision*, pp. 325–332, 2009.

[4] Ashok Veeraraghavan, Ramesh Raskar, Amit Agrawal, Ankit Mohan, and Jack Tumblin. Dappled photography: Mask enhanced cameras for heterodyned light fields and coded aperture refocusing. *ACM Trans. Graph.*, Vol. 26, No. 3, p. 69, 2007.

[5] Stephen R Gottesman and EE Fenimore. New family of binary arrays for coded aperture imaging. *Applied optics*, Vol. 28, No. 20, pp. 4344–4352, 1989.

[6] Yasutaka Inagaki, Yuto Kobayashi, Keita Takahashi, Toshiaki Fujii, and Hajime Nagahara. Learning to capture light fields through a coded aperture camera. In *Proceedings of the European Conference on Computer Vision (ECCV)*, pp. 418–434, 2018.

[7] Zihao W Wang, Vibhav Vineet, Francesco Pittaluga, Sudipta N Sinha, Oliver Cossairt, and Sing Bing Kang. Privacy-preserving action recognition using coded aperture videos. In *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops*, pp. 0–0, 2019.

[8] Anu Pramila, Anja Keskinarkaus, and Tapio Seppänen. Increasing the capturing angle in print-cam robust watermarking. *Journal of Systems and Software*, Vol. 135, pp. 205–215, 2018.

[9] Hamasaki Hiroki, Takeshita Shingo, Nakai Kentaro, Sonoda Toshiki, Kawasaki Hiroshi, Nagahara Hajime, and Satoshi Ono. A coded aperture for watermark extraction from defocused images. In *Proceedings of the Asian Conference on Computer Vision (ACCV)*, 2018.

[10] Eric Wengrowski and Kristin Dana. Light field messaging with deep photographic steganography. In *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, pp. 1515–1524, 2019.

[11] Hirotsugu Yamamoto, Yoshio Hayasaki, and Nobuo Nishida. Secure information display with limited viewing zone by use of multi-color visual cryptography. *Optics express*, Vol. 12, No. 7, pp. 1258–1270, 2004.

[12] Kenji Harada, Takenobu Yamaguchi, Tomohiro Tsuchida, and Daisuke Sakai. Visual cryptography using interference color of high-order retarder films. *Japanese Journal of Applied Physics*, Vol. 52, No. 6R, p. 062501, jun 2013.

[13] Hiroyuki KOWA, Kentaro IWAMI, Norihiro UMEDA, and Mitsuo TSUKIJI. Development of the information security device using higher-order birefringence (in japanese). *Japanese journal of optics*, Vol. 40, No. 9, pp. 490–498, sep 2011.

[14] Max Grosse, Gordon Wetzstein, Anselm Grundhöfer, and Oliver Bimber. Coded aperture projection. *ACM Transactions on Graphics (TOG)*, Vol. 29, No. 3, pp. 1–12, 2010.

[15] Takahiro Suzuki, Shingo Takeshita, and Satoshi Ono. Adversarial example generation using evolutionary multiobjective optimization. In *2019 IEEE Congress on evolutionary computation (CEC)*, pp. 2136–2144. IEEE, 2019.

[16] Kalyanmoy Deb, Amrit Pratap, Sameer Agarwal, and TAMT Meyarivan. A fast and elitist multiobjective genetic algorithm: Nsga-ii. *IEEE transactions on evolutionary computation*, Vol. 6, No. 2, pp. 182–197, 2002.

[17] Hajime Nagahara, Changyin Zhou, Takuya Watanabe, Hiroshi Ishiguro, and Shree K Nayar. Programmable aperture camera using lcos. In *Computer Vision–ECCV 2010*, pp. 337–350. Springer, 2010.