Image Size-Preserving Visual Cryptography by Error Diffusion

Ye, Qing
Faculty of Design, Kyushu University

Inoue, Kohei
Faculty of Design, Kyushu University

Hara, Kenji
Faculty of Design, Kyushu University

出版情報：Journal of the Institute of Industrial Applications Engineers. 11 (3), pp.50-54, 2023-07-25. Institute of Industrial Applications engineers(IIAE)
バージョン：

Journal of the Institute of Industrial Applications Engineers Vol.11, No.3, pp.50–54, (2023.7.25)
DOI: 10.12792/JIIAE.11.50 Online edition: ISSN 2187-8811 Print edition: ISSN 2188-1758

Paper

Image Size-Preserving Visual Cryptography by Error Diffusion

Qing Ye* Non-member, Kohei Inoue†* Member
Kenji Hara* Member

(Received January 19, 2023, revised July 11, 2023)

Abstract: We propose a visual cryptography method based on error diffusion for generating share images of the same size as a given secret image. Two share images printed on separate transparencies are stacked to decrypt a secret image, where opaque and transparent pixels correspond to black (0) and white (1), respectively. An opaque pixel on the stacked image can be given by three combinations of pixel values in two share images: '00', '01' and '10'. This arbitrariness in opaque pixels in a secret image is effectively used in the proposed method. Experimental results show that the proposed method conceals a secret image in share images acceptably, and the quality of the reconstructed secret image given by stacking transparencies onto which the share images by the proposed method are printed is better than that of the conventional methods in terms of visual comparison and quantitative evaluation with the peak signal-to-noise ratio (PSNR).

Keywords: Visual cryptography, Error diffusion, Image size-preservation, Visual secret sharing, Halftoning

1. Introduction

Visual cryptography is a visual secret sharing scheme pioneered by Naor and Shamir [1], where a secret image is concealed in a number of share images printed on separate transparencies, and then the transparencies are stacked to decrypt the secret image. There are a large number of publications on related work of visual cryptography. Siva Kumar et al. [2] surveyed the techniques for visual cryptography from 2011 to 2015. Mursi et al. [3] overviewed the basic visual cryptography schemes as well as the new techniques and some applications. Revenkar et al. [4] evaluated the performance of various visual cryptography schemes on some criteria. Solanki and Verma [5] addressed some issues on existing visual cryptographic techniques. Recently, Koga [6] has surveyed recent progress in visual cryptography by the (t, n)-threshold visual secret sharing scheme [7].

The traditional visual cryptography methods replace a pixel in a secret image with blocks in the corresponding share images, that causes a pixel expansion problem, i.e., the share images are larger than the secret image. Rao et al. [8] summarized a number of visual cryptography schemes without pixel expansion. For example, Askari et al. [9] proposed the balanced block replacement (BBR) method for improving the image quality compared with the simple block replacement (SBR) method which divides a halftone secret image into blocks, and then each block is encrypted into the corresponding block of the same size in share images. Menon K and Kuriakose [10] also proposed a modified SBR method which is computationally more efficient than BBR method.

In this paper, we propose an error diffusion-based method for visual cryptography without pixel expansion. Experimental results show that the proposed method can conceal a secret image in two share images successfully, and the visual quality of the reconstructed secret images is better than that of BBR and MSBR methods, which is also quantitatively evaluated by an image quality measure, the peal signal-to-noise ratio (PSNR) [11].

2. Proposed Visual Cryptography Method

Let $f = [f_{ij}]$ be a grayscale image where $f_{ij} \in [0, 1]$ denotes the pixel value at the position (i, j) in $\Omega = \{1, 2, \ldots, m\} \times \{1, 2, \ldots, n\}$, where $\times$ denotes the Cartesian product of two sets, and m and n denote the numbers of rows and columns in f, respectively. Then we first normalize the pixel values in f as follows:

$$\tilde{f}_{ij} = \alpha \frac{f_{ij} - \min\{f_{ij}\}}{\max\{f_{ij}\} - \min\{f_{ij}\}}, \tag{1}$$

where α is a parameter such that $0 < \alpha < 1$, and then obtain the normalized image $\tilde{f} = [\tilde{f}_{ij}]$ whose pixel values are normalized as $\tilde{f}_{ij} \in [0, \alpha]$. We use $\tilde{f}$ as the secret image which will be hidden in two binary share images $S_1 = [s_{1ij}]$ and $S_2 = [s_{2ij}]$, where the pixel values s_{1ij} and s_{2ij} take 0 or 1 corresponding to black (opaque) or white (transparent), respectively.

Then the pixel value of the reconstructed secret image from S_1 and S_2 is given by $s_1 s_2$, where we omit the subscripts i and j in s_{1ij} and s_{2ij} for the sake of simplicity. All combinations of s_1 and s_2 are shown with the corresponding values of $s_1 s_2$ in Table 1.

If $s_1 s_2 = 1$, then $s_1 = s_2 = 1$ is the unique choice among the combinations, which means that the white pixels in a secret image are also white at the corresponding pixels in the share images. On the other hand, if $s_1 s_2 = 0$, then there

† Corresponding: k-inoue@design.kyushu-u.ac.jp
* Faculty of Design, Kyushu University

Table 1: Pixel values of share images (s_1 and s_2) and their stacked one ($s_1 s_2$).

Image	Values			
s_1	0	1	0	1
s_2	0	0	1	1
$s_1 s_2$	0	0	0	1

Table 2: Error diffusion coefficients by Floyd-Steinberg.

-	#	$w_{0,1} = 7/16$
$w_{1,-1} = 3/16$	$w_{1,0} = 5/16$	$w_{1,1} = 1/16$

are three choices: (i) $s_1 = s_2 = 0$, (ii) $s_1 = 1,\ s_2 = 0$ and (iii) $s_1 = 0,\ s_2 = 1$.

Therefore, for black pixels in the reconstructed secret image, there can be three variations for determining the corresponding pixel values in the share images. We utilize such a variety of binary patterns of s_1 and s_2 on the condition $s_1 s_2 = 0$ for obtaining acceptable share images.

First, we transform the normalized grayscale image $\tilde{f}$ into the binary halftone image by error diffusion. In this paper, we use the coefficients by Floyd-Steinberg [12] as shown in Table 2, where '-' denotes a processed pixel in the raster scan order, and '#' denotes the current pixel from which the error will be diffused to the following unprocessed pixels according to the values of the coefficients in this table.

Let e_{ij} be the quantization error at the pixel (i, j) in $\tilde{f}$, and let it be initialized as $e_{ij} = 0$ for $(i, j) \in \Omega$. At each pixel, $\tilde{f}_{ij}$ is quantized as follows:

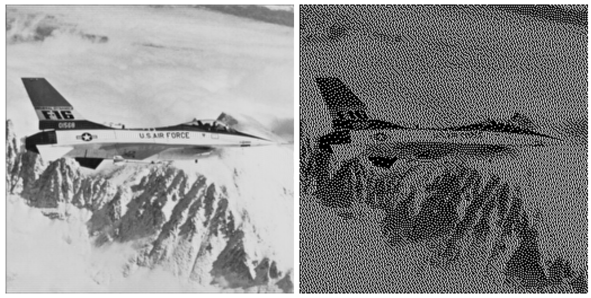
$$b_{ij} = \begin{cases} 0, & \text{if} \quad \tilde{f}_{ij} + e_{ij} < \theta, \\ 1, & \text{otherwise}, \end{cases} \tag{2}$$

where b_{ij} denotes the pixel value of halftoning of $\tilde{f}$, and θ is a threshold value given by $\theta = 0.5$. Then the error subsequent to the current pixel is updated as follows:

$$e_{i+k,j+l} \leftarrow e_{i+k,j+l} + w_{kl}\left(\tilde{f}_{ij} + e_{ij} - b_{ij}\right), \tag{3}$$

where k and l are indices given by $(k, l) \in \{(0, 1),\ (1, -1),\ (1, 0),\ (1, 1)\}$ for indexing the neighboring pixels, and w_{kl} denotes the error diffusion coefficients in Table 2.

Next, we explain how to make the share images. For the share images S_1 and S_2, we prepare two grayscale images all of whose pixels have the same value γ, i.e., $C_1 = [c_{1ij}]$ and $C_2 = [c_{2ij}]$ where $c_{1ij} = c_{2ij} = \gamma$ with $0 < \gamma < 1$. Then we compute S_1 and S_2 by error diffusion such that S_1 and S_2 become the binary halftone images of C_1 and C_2, respectively. Let ε_{1ij} and ε_{2ij} be the quantization error at the pixel (i, j) in C_1 and C_2, respectively, and let they be initialized as $\varepsilon_{1ij} = \varepsilon_{2ij} = 0$. If $b_{ij} = 1$, then the corresponding pixel of the reconstructed secret image is white or $s_{1ij} s_{2ij} = 1$, from which the pixel values of share images are uniquely determined as $s_{1ij} = s_{2ij} = 1$. The quantization error is given by



(a) Original image (Airplane) (b) Halftone image ($\alpha = 0.5$)

Figure 1: Secret image.

the following vector notation:

$$\boldsymbol{\delta}_{ij} = \begin{bmatrix} c_{1ij} + \varepsilon_{1ij} \\ c_{2ij} + \varepsilon_{2ij} \end{bmatrix} - \begin{bmatrix} 1 \\ 1 \end{bmatrix}. \tag{4}$$

On the other hand, if $b_{ij} = 0$, then the corresponding pixel of the reconstructed secret image is black or $s_{1ij} s_{2ij} = 0$. In this case, we choose one among three cases (i), (ii) and (iii) described above by minimizing the quantization error as follows:

$$\begin{bmatrix} s_{1ij} \\ s_{2ij} \end{bmatrix} = \boldsymbol{b}_{t^*} \quad \text{for} \quad t^* = \arg \min_{t \in \{0,1,2\}} \left\| \begin{bmatrix} c_{1ij} + \varepsilon_{1ij} \\ c_{2ij} + \varepsilon_{2ij} \end{bmatrix} - \boldsymbol{b}_t \right\|_1, \tag{5}$$

where $\|\cdot\|_1$ denotes l_1 or the Manhattan norm, and

$$\boldsymbol{b}_0 = \begin{bmatrix} 0 \\ 0 \end{bmatrix}, \quad \boldsymbol{b}_1 = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \quad \boldsymbol{b}_2 = \begin{bmatrix} 0 \\ 1 \end{bmatrix}. \tag{6}$$

The quantization error caused by (5) is given by

$$\boldsymbol{\delta}_{ij} = \begin{bmatrix} c_{1ij} + \varepsilon_{1ij} \\ c_{2ij} + \varepsilon_{2ij} \end{bmatrix} - \boldsymbol{b}_{t^*}. \tag{7}$$

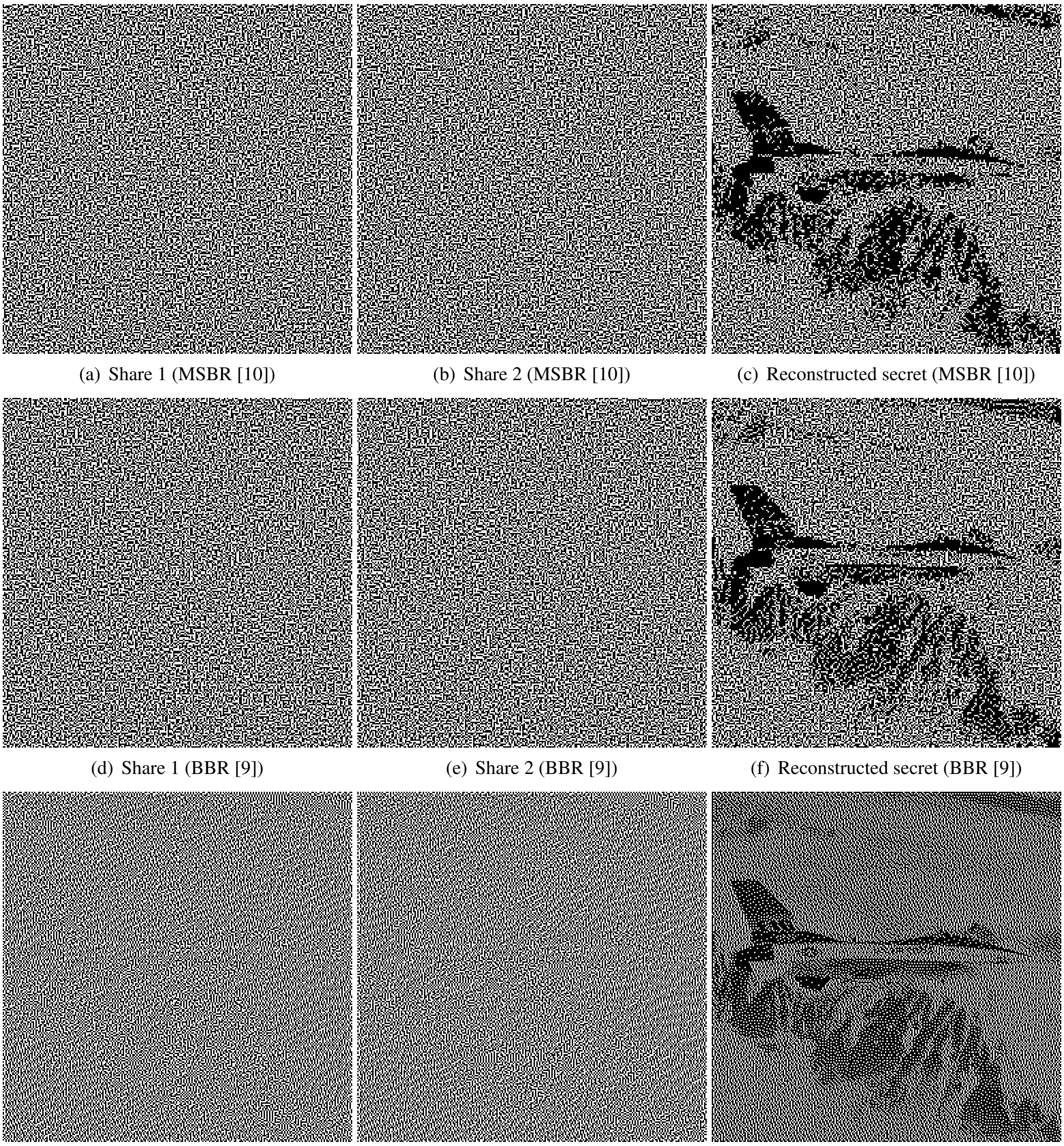
The quantization error $\boldsymbol{\delta}_{ij}$ in (4) or (7) is diffused to the subsequent pixels as follows:

$$\begin{bmatrix} \varepsilon_{1,i+k,j+l} \\ \varepsilon_{2,i+k,j+l} \end{bmatrix} \leftarrow \begin{bmatrix} \varepsilon_{1,i+k,j+l} \\ \varepsilon_{2,i+k,j+l} \end{bmatrix} + w_{kl} \boldsymbol{\delta}_{ij}. \tag{8}$$

The error diffusion process described above is executed for all pixels in the raster scan order. This procedure is summarized in Algorithm 1.

3. Experimental Results

In this section, we show the results of the proposed visual cryptography on the SIDBA standard image database [13] (this dataset can be downloaded from `http://www.ess.ic.kanagawa-it.ac.jp/app_images_j.html`). For example, Fig. 1(a) shows a grayscale image in the SIDBA database, the size of which is 256×256 pixels. In our experiments, these grayscale images in the SIDBA database are used as secret images concealed in their share images of the same size. Figure 1(b) shows the halftone image of the normalized version of Fig. 1(a) with $\alpha = 0.5$ in (1), and is identical to the reconstructed secret image given by the proposed method.



(a) Share 1 (MSBR [10]) (b) Share 2 (MSBR [10]) (c) Reconstructed secret (MSBR [10])

(d) Share 1 (BBR [9]) (e) Share 2 (BBR [9]) (f) Reconstructed secret (BBR [9])

(g) Share 1 (Proposed) (h) Share 2 (Proposed) (i) Reconstructed secret (Proposed)

Figure 2: Share and reconstructed secret images by MSBR [10] (top), BBR [9] (middle) and the proposed (bottom) methods.

We compared the proposed method with the balanced block replacement (BBR) method by Askari et al. [9] and the modified simple block replacement (MSBR) by Menon K and Kuriakose [10]. Figure 2 shows the share images and the reconstructed secret images by the compared methods. The top row in Fig. 2 shows two share images ((a) and (b)) and the reconstructed secret image (c) by MSBR method [10], and the middle and bottom rows similarly show the results by BBR [9] and the proposed methods, respectively. The three methods successfully conceal the secret image in their share images as shown in the left and middle columns in Fig. 2. The reconstructed secret image by MSBR method in Fig. 2(c) reveals the image of an airplane; however, the grayish tone on the face of the mountain becomes blackish. The BBR method improves the quality of the reconstructed secret image as shown in Fig. 2(f), where the grayish regions are recovered better than Fig. 2(c). Figure 2(i) shows the reconstructed secret image by the proposed method with $\gamma = 0.5$, which achieves visually better quality than both MSBR and BBR methods.

Next, we show the results of quantitative evaluation of the reconstructed secret images. The original secret images to be concealed are grayscale or continuous-tone images. On the other hand, their reconstructed images are binary halftone ones. To compare binary halftone images with grayscale images, we first transform the reconstructed

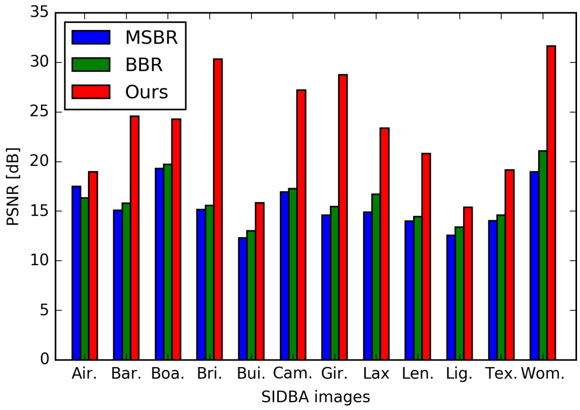


Figure 3: PSNR of inverse-halftoned images.

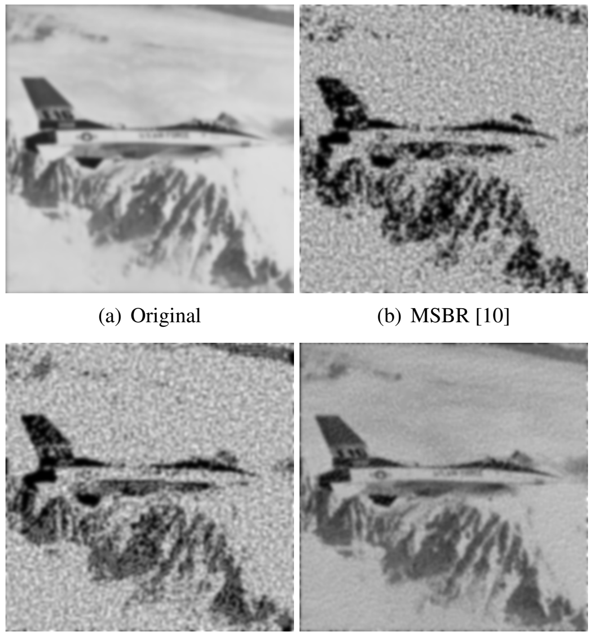
halftone images into the grayscale images by an inverse halftoning technique as follows: First, we use the Gaussian filter for smoothing the halftone images, and then, normalize the maximal pixel value to 1 by dividing all pixel values in the smoothed image by the largest pixel value so as to recover the contrast. We also smooth the original grayscale images by the Gaussian filter with the same standard deviation $\sigma = 1.5$ as the above filter for smoothing the halftone images. Then we compute the peak signal-to-noise ratio (PSNR) [11] between the smoothed images. Figure 3 shows PSNR for twelve images in the SIDBA database [13], where the vertical axis denotes the PSNR value, and the horizontal axis denotes the abbreviated names of the images. The blue, green and red bars in Fig. 3 denote MSBR [10], BBR [9] and the proposed methods, respectively. The proposed method achieved the highest PSNR values among the compared methods. The different values of σ such as $1, 2, 3$ also gave the similar results to Fig. 3.

Figure 4 shows an example of the smoothed images used for computing the PSNR values, where Fig. 4(a) shows the result of the Gaussian filtering for the original grayscale image in Fig. 1(a) with $\sigma = 1.5$, Figs. 4(b)-(d) show the results of inverse halftoning applied to Figs. 2(c), (f) and (i), respectively. Figure 4(d) by the proposed method is visually more similar to Fig. 4(a) than Figs. 4(b) and (c) by the compared methods.

4. Conclusion

In this paper, we proposed a visual cryptography method based on error diffusion. The proposed method can avoid the pixel expansion problem which occurs in conventional visual cryptography schemes by replacing pixels with blocks. We compared the proposed method with two pixel expansion-free methods experimentally, and demonstrated the effectiveness of the proposed method visually and quantitatively.

For future work we would like to develop a method for setting parameters adaptively to a given secret image. We are also planning to develop an improved method for generating meaningful share images by using error diffusion.



(a) Original (b) MSBR [10]

(c) BBR [9] (d) Proposed

Figure 4: Inverse halftoning for quantitative evaluation.

Acknowledgment

This work was supported by JSPS KAKENHI Grant Number JP21K11964.

References

[1] M. Naor, A. Shamir, "Visual cryptography", In: De Santis A. (eds) Advances in Cryptology — EUROCRYPT'94. EUROCRYPT 1994. *Lecture Notes in Computer Science*, vol. 950. Springer, Berlin, Heidelberg, 1995. https://doi.org/10.1007/BFb0053419

[2] M. Siva Kumar, A. Shilpa, J. R. Vijayalakshmi, "A Survey on Visual Cryptography Techniques", *Int. J. Application or Innovation in Engineering & Management (IJAIEM)*, vol. 5, no. 2, pp. 100–112, 2016. https://ijaiem.org/pabstract_Share.php?pid=IJAIEM-2016-02-26-24

[3] M. F. M. Mursi, M. Salama, M. Mansour, "Visual Cryptography Schemes: A Comprehensive Survey", *Int. J Emerging Research in Management &Technology*, vol. 3, no. 11, pp. 142–154, 2014.

[4] P. S. Revenkar, A. Anjum, W. Z. Gandhare, "Survey of Visual Cryptography Schemes", *Int. J. Security and Its Applications*, vol. 4, no. 2, pp. 49–56, 2010. http://article.nadiapub.com/IJSIA/vol4_no2/5.pdf

[5] J. Solanki, M. K. Verma, "A Brief Survey on Visual Cryptographic Approaches", *Int. J. Advanced Research in Computer Engineering & Technology (IJARCET)*, vol. 5, no. 5, pp. 1483–1486, 2016.

[6] H. Koga, "Recent Progress in Visual Cryptography", *The Journal of Institute of Electronics, Information and Com-*

Algorithm 1 Visual cryptography by error diffusion

Require: a grayscale image f, parameters α and γ

Ensure: share images $S_1 = [s_{1ij}]$ and $S_2 = [s_{2ij}]$

Compute the normalized image $\tilde{f} = [\tilde{f}_{ij}]$ by (1);
Initialize arrays as $e_{ij} = \varepsilon_{1ij} = \varepsilon_{2ij} := 0$;
Initialize arrays as $c_{1ij} = c_{2ij} := \gamma$;
Initialize vectors as $\boldsymbol{b}_0 := \begin{bmatrix} 0 \\ 0 \end{bmatrix}$, $\boldsymbol{b}_1 := \begin{bmatrix} 1 \\ 0 \end{bmatrix}$, $\boldsymbol{b}_2 := \begin{bmatrix} 0 \\ 1 \end{bmatrix}$;
for $i = 0$ to m **do**
  for $j = 0$ to n **do**
    if $\tilde{f}_{ij} + e_{ij} \geq \theta$ **then**
      $b_{ij} := 1$;
      $d_{ij} := \tilde{f}_{ij} + e_{ij} - b_{ij}$;
      $s_{1ij} = s_{2ij} := 1$;
      $\boldsymbol{\delta}_{ij} = \begin{bmatrix} c_{1ij} + \varepsilon_{1ij} \\ c_{2ij} + \varepsilon_{2ij} \end{bmatrix} - \begin{bmatrix} 1 \\ 1 \end{bmatrix}$;
    else
      $b_{ij} := 0$;
      $d_{ij} := \tilde{f}_{ij} + e_{ij} - b_{ij}$;
      Compute

$$t^* = \arg \min_{t \in \{0,1,2\}} \left\| \begin{bmatrix} c_{1ij} + \varepsilon_{1ij} \\ c_{2ij} + \varepsilon_{2ij} \end{bmatrix} - \boldsymbol{b}_t \right\|_1 ;$$

      $\begin{bmatrix} s_{1ij} \\ s_{2ij} \end{bmatrix} := \boldsymbol{b}_{t^*}$;
      $\boldsymbol{\delta}_{ij} = \begin{bmatrix} c_{1ij} + \varepsilon_{1ij} \\ c_{2ij} + \varepsilon_{2ij} \end{bmatrix} - \boldsymbol{b}_{t^*}$;
    end if
    for (k, l) in $\{(0, 1),\ (1, -1),\ (1, 0),\ (1, 1)\}$ **do**
      if $(i + k, j + l) \in \Omega$ **then**
        $e_{i+k,j+l} := e_{i+k,j+l} + w_{kl} d_{ij}$;
        $\begin{bmatrix} \varepsilon_{1,i+k,j+l} \\ \varepsilon_{2,i+k,j+l} \end{bmatrix} := \begin{bmatrix} \varepsilon_{1,i+k,j+l} \\ \varepsilon_{2,i+k,j+l} \end{bmatrix} + w_{kl} \boldsymbol{\delta}_{ij}$;
      end if
    end for
  end for
end for

munication Engineers, vol. 106, no. 1, pp. 39–46, 2023. (in Japanese)

[7] H. Koga, "A General Formula of the (t, n)-Threshold Visual Secret Sharing Scheme", In: Zheng, Y. (eds) *Advances in Cryptology — ASIACRYPT 2002*, ASIACRYPT 2002, Lecture Notes in Computer Science, vol. 2501, Springer, Berlin, Heidelberg, 2002. `https://doi.org/10.1007/3-540-36178-2_21`

[8] J. Rao, V. Patil, S. Patil, "Survey of Visual Cryptography Schemes without Pixel Expansion", *Int. J. Engineering And Computer Science*, vol. 3, no. 9, pp. 8372–8376, 2014. `http://www.ijecs.in/index.php/ijecs/article/view/1574`

[9] N. Askari, H. M. Heys, C. R. Moloney, "An extended visual cryptography scheme without pixel expansion for halftone images", *Proc. Electrical and Computer Engineering (CCECE)*, 2013. `https://www.engr.mun.ca/~howard/PAPERS/ccece2013_evcs.pdf`

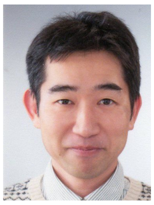
[10] N. Menon K, M. Kuriakose, "A Novel Visual Cryptographic Scheme Using Floyd Steinberg Halftoning and Block Replacement Algorithms", *Int. J. Advanced Research in Basic Engineering Sciences and Technology (IJARBEST)*, vol. 1, no. 1, pp. 47–51, 2015. `https://www.ijarbest.com/journal/issue1/11`

[11] K. -H. Thung and P. Raveendran, "A survey of image quality measures", *2009 International Conference for Technical Postgraduates (TECHPOS)*, Kuala Lumpur, Malaysia, pp. 1-4, 2009. `https://doi.org/10.1109/TECHPOS.2009.5412098`

[12] R. W. Floyd, L. Steinberg, "An adaptive algorithm for spatial grey scale", *Proc. the Society for Information Display*, vol. 17, no. 2, pp. 75–77, 1976.

[13] M. Sakauchi, Y. Ohsawa, M. Sone, M. Onoe, "Management of the Standard Image Database for Image Processing Researches", *ITEJ Technical Report*, vol. 8, no. 38, pp. 7–12, 1984. (in Japanese)

Qing Ye (Non-member) He received B.Sc. degree from Jinggangshan University in 2021. He is currently a Master's student at Kyushu University. His research interests include pattern recognition and image processing.



Kohei Inoue (Member) He received B.Des., M.Des. and D.Eng. degrees from Kyushu Institute of Design in 1996, 1998 and 2000, respectively. He is currently an Associate Professor in Kyushu University. His research interests include pattern recognition and image processing.

Kenji Hara (Member) He received the BE and ME degrees from Kyoto University in 1987 and 1989, respectively, and the PhD degree from Kyushu University in 1999. He is currently a Professor in Kyushu University. His research interests include physics-based vision and geometric modeling.