Performance Evaluation of Visual Cryptography Schemes with Intensity Transformations for Gray-Scale Images

MASAKAZU HIGUCHI, SHUJI KAWASAKI, JONAH GAMBA,
ATSUSHI KOIKE, HITOMI MURAKAMI
Faculty of Science and Technology
Seikei University
3-3-1 Kichijyoujikitamachi, Musashino, Tokyo, 180-8633
JAPAN
m-higuchi@ejs.seikei.ac.jp

AYA EMORI
Graduate school of Science and Technology
Seikei University
3-3-1 Kichijyoujikitamachi, Musashino, Tokyo, 180-8633
JAPAN
dm096207@cc.seikei.ac.jp

Abstract: In a kind of visual cryptography, a secret image is hidden into other images. Then, we can reconstruct the secret image by using share images produced in secret image hiding scheme. In the case of two binary share images, the secret image is reconstructed by printing the two share images onto transparencies and stacking them together without any special electronic calculation. Myodo's method based on error diffusion can produce two high quality binary halftone share images from three input images, that is, two gray-scale images and a gray-scale secret image, and restore the gray-scale secret image hidden into their share images with high quality. The method changes intensities of each pixel in input images as a pre-processing in order to restore a high quality secret image. In this paper, we investigate intensity transformations to realize higher quality reconstructing of a secret image in myodo's method and we obtain that histogram equalization is effective to reconstruct a secret image with higher quality in term of visual effects.

Key–Words: Visual cryptography, Halftone image, Superimposing, Intensity transformation, Affine transformation, Histogram equalization

1 Introduction

Visual cryptography is a kind of cryptography that can be decoded directly by the human visual system without any special calculation for decryption. The encryption system discussed in this paper takes three images as an input and generates two output images which correspond to two of the three input images. The third image is reconstructed by using the two output images. The two output images are called "share images." When share images are composed of binary pixels, the third image is reconstructed by superimposing one share image on the other. This operation corresponds to logical product in Boolean algebra. Then we can make the reconstruction by printing the two output images onto transparencies and stacking them together. The resulting image reconstructed by using the two share images is called "restored image." In the case of binary share images, it is also a binary image. The input image corresponding to restored image is "secret image." We can consider that secret image is hidden into share images.

The main themes of previous works in this type of visual cryptography are to generate binary share images and to restore secret image with high quality. Noar and Shamir have developed the scheme generates share images with not meaningful random dot pattern [2]. On the other hand, there have been also many reports for productions of meaningful binary halftone share images [3, 4, 5, 6, 7, 8]. Fu and Au have dealt with binary or ternary images like text images as secret image [5], while other many researchers have studied about natural gray-scale images like photographs as secret image [4, 6, 7, 8]. Also, Koga and Yamamoto have challenged to handle color secret images [3]. Conventional methods have many problems about the quality of share and restored images, and the calculation time, and so on. Myodo et al. has applied error diffusion to generating binary halftone share images [6]. Their method can produce high quality share images with high speed from three natural gray-scale images and restore secret image with high quality by superimposing one share image on the other. The error diffusion is one of techniques to generate the halftone image with high quality from a multivalued image [1]. In generating share images, applying error diffusion makes noise less noticeable which arise by embedding information of secret image into share images. Accordingly we obtain natural, i.e., noise is in shade, share images. Myodo's method changes intensities of each pixel of input images as a pre-processing in order to reconstruct a high quality secret image. Emori et al. has obtained higher quality restored images than Myodo's method by improving intensity transformation in Myodo's method [7, 8].

In this paper, we investigate whether the qualities of restored images depend on kinds of share images or not in terms of objective and subjective evaluations in Myodo's and proposed methods in [7, 8]. Also we make mention of qualities of share images obtained by our method.

The organization of this paper is as follows. Section 2 gives the principle of superimposing of binary pixel domains, which is basis in this kind of visual cryptography. In Section 3, we explain Myodo's method which is one of conventional methods generates binary halftone share images. In Section 4, we discusses our proposed method and experimental results. Finally, we conclude this paper in Section 5.

2 The fundamentals of pixel superimposing

In the case of two binary share images, a restored image is obtained by superimposing one share image on the other. The section makes consideration on superimposing of two pixels. In general, the intensity of a pixel is from 0 to 1. If the intensity of a pixel is 0, the pixel is black pixel. On the other hand, if the intensity of a pixel is 1, the pixel is white pixel. Let g_1 and g_2 be intensities of pixels A and B, respectively. We obtain the pixel C by superimposing pixel A on pixel B. Let s be the intensity of pixel C. s is $g_1 \cdot g_2$ and satisfies the following inequality [4],

$$\max(0,\ g_1 + g_2 - 1) \leq s \leq \min(g_1,\ g_2). \quad (1)$$

In particular, when pixels A and B have binary intensities, i.e., g_1 and g_2 are 0 or 1, superimposing pixels A and B is the same as calculating logical product of their pixels in Boolean algebra (see in Figure 1). When we take some small domains which consist binary pixels and for each domain define pseudo-intensity as the percentage of white pixels in the domain, the pseudo-intensity of the binary pixel domain obtained by superimposing two binary pixel domains satisfies the inequality (1). We illustrate by an example in Figure 2. We consider 3×3 square binary pixel domains in Figure 2. We take a pair of two domains that the one has five white pixels, i.e., the pseudo-intensity of the domain is $\frac{5}{9}(= g_1)$, and the other has six white pixels, i.e., the pseudo-intensity of the domain is $\frac{6}{9}(= g_2)$. We also take another pair that have same pseudo-intensities, i.e., g_1 and g_2, but different arrangement of white and black pixels (see in Case A and B). In each case, the pseudo-intensity of the binary pixel domain obtained by superimposing those two domains belongs to $[\frac{2}{9},\ \frac{5}{9}]$ by the inequality (1). It is $\frac{3}{9}$ and $\frac{4}{9}$ in Case A and B, respectively.

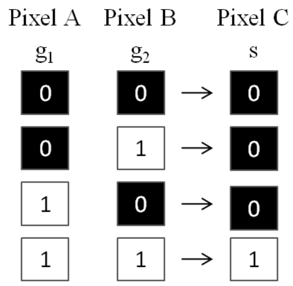

Figure 1: Superimposing two binary pixels

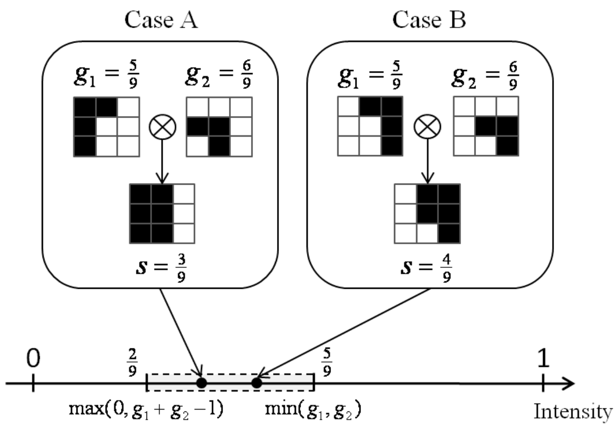

Figure 2: The pseudo-intensities of binary pixel domains

In the case of normal gray-scale pixel, the intensity of the pixel obtained by superimposing two pixels is unique. On the other hand, in the case of binary pixel domain, for the domain generated by superimposing two ones, the pseudo-intensity depends on arrangements of white and black pixels in the parental ones. The principle of image encryption in this paper lie in controlling pseudo-intensities of restored image by changing arrangements of white and black pixels in binary share images.

3 Conventional method

We explain Myodo's method [6], which is one of conventional methods generates binary halftone share images in visual cryptography, in this section.

3.1 The image encryption process

The flowchart of Myodo's method is shown in Figure 3. Myodo's method takes three gray-scale images,

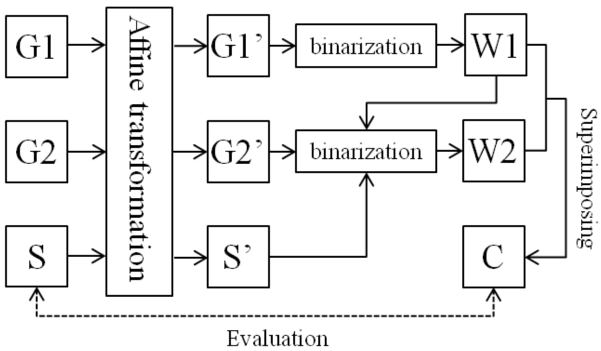

Figure 3: The flowchart of Myodo's method

G1, G2 and S, as input. The image S is a secret image. This method changes intensities of each pixel in input images by affine transformation as a pre-processing in order to reconstruct a high quality secret image. Here G1', G2' and S' denote the images which are transformed intensities of each pixel in G1, G2 and S, respectively. The images W1 and W2 are share images. The image W1 is produced from the image G1' by using error diffusion. Then, with embedding information of images W1 and S in the image G2 and binarizing by using error diffusion, the image W2 is generated. The image C is the restored image obtained by superimposing share images. We evaluate the quality of the image C.

3.2 Intensity transformation

Myodo's method is based on the principle of superimposing binary pixel domains in the Section 2. The intensity of a pixel in secret image is obtained by rearranging white and black pixels in share images. However, it may be error if the inequality (1) is not satisfied. Therefore, Myodo's method requires intensity transformation for input images as a pre-processing. In the inequality (1), the length of the range is maximum when g_1 and g_2 are 0.5, respectively. Converging the intensity of each pixel in images G1 and G2 to around 0.5, suitable intensity transformation is applied to images G1 and G2, i.e.,

$$g' = 0.45g + 0.275 \quad (2)$$

where g denotes the intensity of a pixel in the image G1 or G2, and g' denotes the intensity obtained by applying intensity transformation to the pixel. This is affine transformation. Then, the pseudo-intensity of each pixel domain in images binarized G1 and G2 converges to around 0.5. The intensity of a pixel in the image S is transformed into below 0.45, i.e.,

$$s' = 0.45s \quad (3)$$

where s denotes the intensity of a pixel in the image S, and s' denotes the intensity obtained by applying intensity transformation to the pixel.

We explain the mechanism of Myodo's method in Figure 4. There is a small gray square in S. Also there

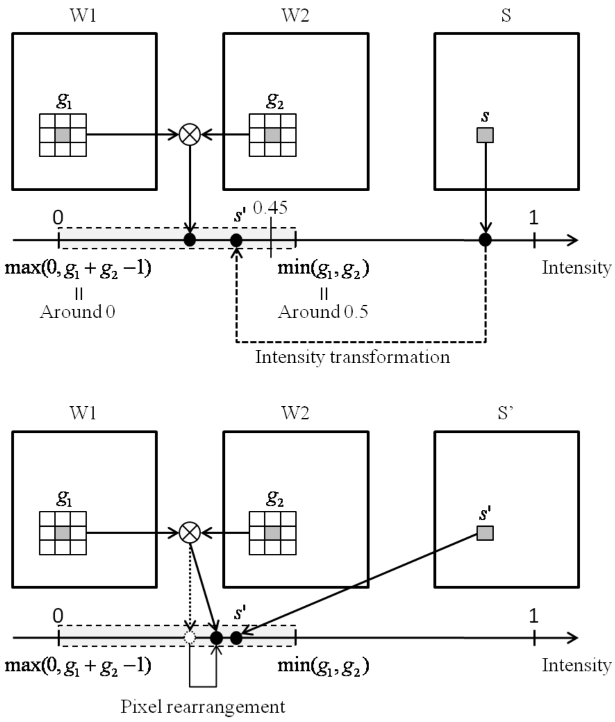

Figure 4: The mechanism of Myodo's method

are two small gray ones in W1 and W2, respectively. Images W1, W2 and S are same size. Each of three small gray boxes means a pixel. Those pixels are locating at same positions, respectively. Now we take a gray pixel of S and consider two tiny pixel domains in W1 and W2 containing two pixels corresponding to the gray one of S with respect to location. Let g_1 and g_2 be pseudo-intensities of the pixel domains in W1 and W2, respectively, and let s be the intensity of the pixel in S. For the g_1 and g_2, the inequality (1) is $[x,\ y]$ where x and y are two numbers close or equal to 0 and 0.5, respectively. Since $s' \in [0,\ 0.45]$, s' almost belongs to $[x,\ y]$ (see the upper part of Figure 4). Hence, rearranging white and black pixels in the domains in W1 and W2, the domain has a pseudo-intensity close to s' is obtained from the domains in W1 and W2 (see the lower part of Figure 4). Therefore, the restored image C is similar to the image S'.

4 proposed method

In this section, we improve intensity transformation in Myodo's method and show that proposed method can reconstructed a secret image with higher quality in term of visual effects than Myodo's method.

4.1 The proposed image encryption process

In Myodo's method, the affine transformation, Eq. (3), is applied to the secret image S. Then, the image S' becomes a little bit dark since the intensity of each pixel in the image S is uniformly transformed. Therefore, a low-key image is generated as restored image. So we consider histogram equalization as the way to increase the contrast of an image and add the process to Myodo's method in this paper. The flowchart of the proposed method is shown in Figure 5. In proposed method, we apply histogram equalization and affine transformation to only the secret image S. Parameters in affine transformation are the same as ones in Myodo's method.

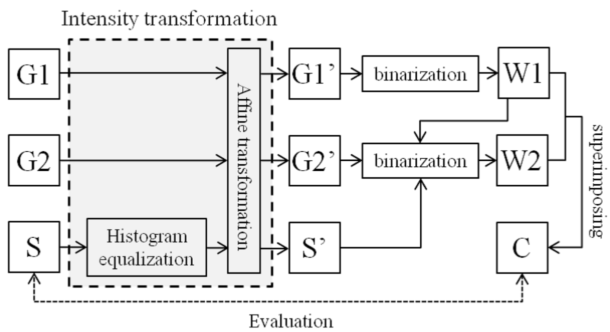

Figure 5: The flowchart of proposed method

4.2 Histogram equalization

In general, it is desirable that the intensity of each pixel in an image is uniformly-distributed between 0 and 1. That is because it makes every intensity used and the contrast of the image becomes clear. We consider histogram equalization as the way to realize it. The histogram equalization is given by the following expression,

$$g' = \frac{\int_0^g p(r)dr - p(0)}{1 - p(0)} \tag{4}$$

where g denotes the intensity of a pixel in an image, g' denotes the intensity obtained by applying intensity transformation to the pixel and p denotes distribution function with respect to the intensity of a pixel in the image. By this intensity transformation, the cumulative distribution function of p is straight.

4.3 Example

We show examples of results obtained by using Myodo's and proposed methods in Figure 6. Images $\mathrm{W1_M}$, $\mathrm{W2_M}$ and $\mathrm{C_M}$ denote two share images generated by Myodo's method and restored image obtained by superimposing $\mathrm{W1_M}$ and $\mathrm{W2_M}$, respectively, and also images $\mathrm{W1_P}$, $\mathrm{W2_P}$ and $\mathrm{C_P}$ denote two share images generated by proposed method and restored image obtained by superimposing $\mathrm{W1_P}$ and $\mathrm{W2_P}$, respectively, in Figure 6. The fact that $\mathrm{W1_M}$ and $\mathrm{W1_P}$ are the same image. By Figure 6, it is difficult to distinguish $\mathrm{W2_M}$ from $\mathrm{W2_P}$. In Myodo's and proposed methods, share images are low-contrast since the intensity of each pixel of G1' and G2' which are materials of share images is around 0.5, that is, G1' and G2' are low-key images. The restored image $\mathrm{C_M}$ is low-key. However, the restored image $\mathrm{C_P}$ is higher-contrast and higher quality than $\mathrm{C_M}$ in term of visual effects.

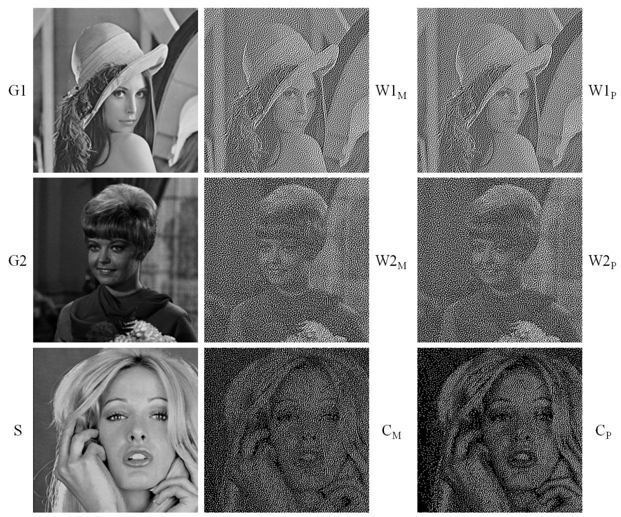

Figure 6: An example of the results by Myodo's and proposed methods

4.4 Experimental results

We investigate whether the qualities of restored images depend on kinds of share images or not in terms of objective and subjective evaluations in Myodo's and proposed methods. Also we make mention of qualities of share images obtained by our method. There are 20 images. We choose an original image as secret image S. Then we also choose two images from the rest 19 images in random order as images G1 and G2. By using both of Myodo's and our methods, we generate two pairs of two share images, i.e., $(\mathrm{W1_M}, \mathrm{W2_M})$ and $(\mathrm{W1_P}, \mathrm{W2_P})$, from images G1, G2 and S. Now we consider how to be reconstructed secret image S from two pairs $(\mathrm{W1_M}, \mathrm{W2_M})$ and $(\mathrm{W1_P}, \mathrm{W2_P})$. We ditto swapping images G1 and G2 and estimate how the qualities of restored images by the way we look and objectify resulting images. Those procedure are one set. Here we have 20 images. We take another original image and start the procedure again. For each set, Pairs of images G1 and G2 amount to 342, note that we distinguish between (G1,G2) $= (a, b)$ and (G1,G2) $= (b, a)$. We show sample images used in this experiment in Figure 7.

We use a block PSNR as objective evaluation. Now we take images G and W which are the same in size $N \times M$, where N and M denote the width and height, respectively. The block PSNR of images G and W is given by the following expression,

$$\begin{aligned} \mathrm{bPSNR} &= 10 \log_{10}(1 \cdot 1/\mathrm{ER}) \\ \mathrm{ER} &= \frac{m^2}{NM} \sum_{k=1}^{\lceil NM/m^2 \rceil} (\hat{g}_k - \hat{w}_k)^2 \\ \hat{g}_k &= \frac{\sum_{i \in R_k^{\mathrm{G}}} g_i}{\sum_{i \in R_k^{\mathrm{G}}} 1}, \quad \hat{w}_k = \frac{\sum_{i \in R_k^{\mathrm{W}}} w_i}{\sum_{i \in R_k^{\mathrm{W}}} 1} \end{aligned} \tag{5}$$

where g_i and w_i denote intensities of each pixel in images G and W, respectively, R_k^{G} and R_k^{W} denote $m \times m$ pixels square which are locating at same positions in images G and W, respectively.

Let S be fixed in sample images. Then we can take 342 patterns of the pair G1 and G2 from the rest 19 images. For each pair of G1 and G2, we compute block PSNRs corresponding to Myodo's and proposed methods, respectively, as the following way: First, we take G1 and G2. Second, we apply both of Myodo's and proposed methods to G1, G2 and S. So, we obtain two pairs of two share images $(\mathrm{W1_M}, \mathrm{W2_M})$ and $(\mathrm{W1_P}, \mathrm{W2_P})$, where $(\mathrm{W1_M}, \mathrm{W2_M})$ and $(\mathrm{W1_P}, \mathrm{W2_P})$ are corresponding to Myodo's and proposed methods, respectively. Then, we produce two restored images $\mathrm{C_M}$ and $\mathrm{C_P}$ from $(\mathrm{W1_M}, \mathrm{W2_M})$ and $(\mathrm{W1_P}, \mathrm{W2_P})$, respectively. Finally, we compute block PSNRs of two pairs ($\mathrm{C_M}$, S) and ($\mathrm{C_P}$, S). After that we calculate the average block PSNRs of ($\mathrm{C_M}$, S), which we name "$\mathrm{bPSNR}_{\mathrm{M}}^{ave}$." Similarly we calculate the average block PSNRs of ($\mathrm{C_P}$, S), which we name "$\mathrm{bPSNR}_{\mathrm{P}}^{ave}$." For All of patterns of the pair G1 and G2, it is difficult to distinguish $\mathrm{W2_M}$ from $\mathrm{W2_P}$ for any S in sample images. Therefore, we obtain the average of absolute values of differences between block PSNRs of two pairs ($\mathrm{W2_M}$, G2) and ($\mathrm{W2_P}$, G2), which we name "$\mathrm{bPSNR}_{diff}^{ave}$." The results are shown in Table 1. Also, for each S in sample images, we investigate proportions of the pair (G1, G2) as $\mathrm{C_P}$ is apparently better than $\mathrm{C_M}$, the block PSNR of ($\mathrm{C_P}$, S) is higher than it of ($\mathrm{C_M}$, S) and subjective evaluation of the pair ($\mathrm{C_M}$, $\mathrm{C_P}$) corresponds with objective one to total patterns, respectively. The results are shown in Table 2.

Figure 7: Sample images

4.5 Discussion

By Table 1 and the third row in Table 2, we see that for 10 kinds of S in 20 sample images, $\mathrm{bPSNR}_{\mathrm{P}}^{ave}$ is higher than $\mathrm{bPSNR}_{\mathrm{M}}^{ave}$ and for each of the 10 images, the block PSNR of the pair ($\mathrm{C_P}$, S) is higher than it of the pair ($\mathrm{C_M}$, S) over 78 percent of all the pairs (G1, G2), respectively. For all cases, $\mathrm{W2_M}$ is the same as $\mathrm{W2_P}$ with respect to appearance. Therefore, block PSNRs of two pairs ($\mathrm{W2_M}$, G2) and ($\mathrm{W2_P}$, G2) are almost the same values (see in the fourth row in Table 1). For each ($\mathrm{W2_M}$, $\mathrm{W2_P}$) which are obtained from G2 in the sample images, $\mathrm{W2_M}$ and $\mathrm{W2_P}$ have equally high qualities in term of visual effects, except that W2s obtained from two sample images, "Couple" and "Cups," are low-contrast, i.e., those images are darkish and whitish, respectively.

ISSN: 1792-6130

ISBN: 978-960-474-246-2

Table 1: Objective evaluations of the qualities of restored and share images in Myodo's and proposed methods (unit dB)

S	$\mathrm{bPSNR}^{ave}_{\mathrm{M}}$ ($\mathrm{C_M}$ v.s. S)	$\mathrm{bPSNR}^{ave}_{\mathrm{P}}$ ($\mathrm{C_P}$ v.s. S)	$\mathrm{bPSNR}^{ave}_{diff}$ (W2 v.s. G2)
Lenna	10.79963	11.21899	0.02187
Girl	16.01620	19.05140	0.02691
Woman	10.24730	10.21722	0.02241
Airplane	7.45651	6.42877	0.02606
Couple	17.97330	16.81760	0.03161
Mandrill	10.82064	11.06351	0.02152
Milk-drop	11.96263	13.04227	0.02450
Parrots	11.07673	11.64873	0.02188
Leaf	5.96887	4.72352	0.03094
Sprout	5.49871	4.02694	0.03030
Tomato	9.53941	9.61934	0.02188
Mt. Fuji	10.49712	10.81568	0.02293
Bridge	14.21263	16.09438	0.02599
Horse	10.95558	11.47239	0.02269
Indicator	13.38746	14.75369	0.02703
Cups	4.69216	3.16564	0.03146
Text1	4.76762	4.74242	0.01631
Text2	13.96282	13.77411	0.01524
Tile	10.32030	10.24768	0.02249
Tiger	4.61120	3.99235	0.02311

Table 2: Subjective evaluation of the qualities of restored images in Myodo's and proposed methods and relationships with objective one (unit percent)

S	subjectively ($\mathrm{C_M} < \mathrm{C_P}$)	objectively ($\mathrm{C_M} < \mathrm{C_P}$)	subject = object
Lenna	83.63	97.66	82.16
Girl	90.64	100	90.64
Woman	95.03	40.35	35.38
Airplane	89.77	0	0
Couple	88.89	6.73	6.73
Mandrill	91.23	78.95	70.18
Milk-drop	0	100	0
Parrots	83.04	100	83.04
Leaf	76.90	0	0
Sprout	95.91	0	0
Tomato	0	92.69	0
Mt. Fuji	0	89.47	0
Bridge	0.88	100	0.88
Horse	8.48	100	8.48
Indicator	0	100	0
Cups	88.30	0	0
Text1	0	2.05	0
Text2	0	0	0
Tile	89.77	35.96	26.32
Tiger	98.54	0	0

There are the following four cases in term of visual effects: $\mathrm{C_P}$ is better than $\mathrm{C_M}$ (Case A), $\mathrm{C_M}$ is better than $\mathrm{C_P}$ (Case B), both of them are poor qualities (Case C) and both of them are high qualities but are indistinguishable (Case D). By the second row in Table 2, for 12 kinds of S in 20 sample images, Case A is over 76 percent of all the pairs (G1, G2) and most of the rest pairs are Case C. For "Tomato," "Mt. Fuji," "Horse," "Text1" and "Text2" in the sample images, the subjective quality of ($\mathrm{C_M}$, $\mathrm{C_P}$) is almost Case D. However, for "Text2," a part of G1 or G2 sometimes appears in $\mathrm{C_M}$ and $\mathrm{C_P}$. For "Milk-drop," "Bridge" and "Indicator," in the sample images, the subjective quality of ($\mathrm{C_M}$, $\mathrm{C_P}$) is almost Case B. Also the subjective quality of ($\mathrm{C_M}$, $\mathrm{C_P}$) tends to belong to Case B or C when at least one of G1 and G2 contains whitish images, e.g., "Leaf," "Sprout," "Cups," "Text1" and "Tiger" in the sample images. By the fourth row in Table 2, subjective evaluation does not necessarily correspond with objective one in Myodo's and proposed methods. It means that $\mathrm{C_P}$ is apparently better than $\mathrm{C_M}$ but the block PSNR of ($\mathrm{C_M}$, S) is higher than it of ($\mathrm{C_P}$, S), and vice versa.

From these results, the quality of restored image by subjective and objective evaluations almost depends on the property of secret image. Moreover, reconstructing secret image tends to fail when at least one of G1 and G2 is a whitish image.

5 Conclusion

In this paper, we investigated whether the qualities of restored images depend on kinds of share images or not in terms of objective and subjective evaluations in Myodo's and proposed methods. Also we checked qualities of share images in Myodo's and proposed methods. As a result, we obtained the following six remarks:

- proposed method is better than Myodo's one with respect to subjective evaluation.
- Myodo's and proposed methods have same efficiency with respect to objective evaluation.
- Subjective evaluation does not necessarily correspond with objective one in Myodo's and proposed methods.
- The quality of restored image by subjective and objective evaluations almost depends on the property of secret image.
- Reconstructing secret image tends to fail when at least one of input images except secret one is a whitish image.

- ◦ Share images are rather high qualities in both Myodo's and proposed methods. These are indistinguishable.

The key point is a intensity transformation for input images in this kind of visual cryptography. In the future works, we need to study adjusting parameters of affine transformation to an input secret image according to the property of the image in order to make a restored image with higher quality for any secret image. Also we must give optimal parameters of affine transformation to the other two input images in order to accommodate to the case that at least one of these images is a whitish image. Moreover, the objective evaluation by block PSNR proposed in this paper does not corresponds with subjective one, so we need to invent a new quantitative measurement including a subjective term.

Acknowledgements: A part of this study was supported by MEXT Grant-in-Aid for Building Strategic Research Infrastructures.

References:

[1] R. A. Ulichney, *Digital halftoning*, MIT Press, Cambridge, 1987.

[2] M. Noar, A. Shamir, Visual Cryptography, *Proc. Eurocrypt'94*, 1994, pp. 1–12.

[3] H. Koga and H. Yamamoto, Proposal of a lattice-based visual secret sharing scheme for color and gray-scale images, *IEICE Transaction on Fundamentals* E81-A, No. 6, 1998, pp. 1262–1269.

[4] M. Nakajima and Y. Yamaguchi, Extended visual cryptography for natural images, *Journal of WSCG* 2, 2002, pp. 303–310.

[5] M. S. Fu, O. C. Au, A novel method to embed watermark in different halftone images: data hiding by conjugate error diffusion (OHCED), *Proc. IEEE Int. Conf. on Multimedia and Expo* 1, 2003, pp. 609–612.

[6] E. Myodo, K. Takagi, S. Sakazawa and Y. Takishima, Gray-scale Image Hiding Method for Plural Halftone Images Based on Error Diffusion Technique, *IEICE Technical Report* 106, No. 22, IE2006-2, 2006, pp. 7–12.

[7] A. Emori, M. Higuchi, E. Myodo, S. Kawasaki, A. Koike, H. Murakami, A study on intensity transformations for high-quality decoding of a hidden image in visual cryptography, *Journal of the Faculty of Science and Technology, Seikei University* 47, No. 1, 2010, pp. 67–73.

[8] A. Emori, M. Higuchi, S. Kawasaki, A. Koike and H. Murakami, A study on intensity transformations to generate a high-quality decoding image in visual cryptography, *ITE Technical Report* 34, No. 31, AIT2010-106, 2010, pp. 53–56.