Image Encryption Methods Using Intensity Transformations in Visual Cryptography

Masakazu Higuchi, Aya Emori, Shuji Kawasaki, Jonah Gamba, Atsushi Koike and Hitomi Murakami

***Abstract*—In a kind of visual cryptography, a secret image is encoded as other images. Then, we can reconstruct the secret image by using share images produced in secret image encoding process. In the case that share images are binary, the secret image is reconstructed by printing the 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 with high quality by using those share images. The method changes intensities of each pixel in input images as a pre-processing in order to restore a high quality secret image in term of visual effects. By improving the intensity transformation in Myodo's method, authors have proposed a method to generate high quality share images with high speed from which a secret image can be reconstructed with apparently higher quality than myodo's method. In this paper, we review the method and evaluate its performance for any input images objectively and subjectively.**

***Keywords*—Visual cryptography, Halftone image, Superimposing, Intensity transformation, Affine transformation, Histogram equalization.**

I. INTRODUCTION

VISUAL cryptography is a kind of cryptography that can be decoded directly by the human visual system without any special electronic 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 decoding 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 called "secret image." We can consider that secret image is encoded as 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]–[6], [10]–[13]. 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], [10], [11]. 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 the 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. By improving the intensity transformation in Myodo's method, authors have proposed a method to generate high quality share images with high speed from which a secret image can be reconstructed with apparently higher quality than myodo's method [10]–[13].

In this paper, we review the method and evaluate its performance for any input images objectively and subjectively. Also we make mention of qualities of share images obtained by our method.

The organization of this paper is as follows. Section II gives the principle of superimposing of binary pixel domains, which is basis in this kind of visual cryptography. In Section III, we explain Myodo's method which is one of conventional methods generates binary halftone share images. In Section IV, we review our proposed method and evaluate its performance through experimental results. Finally, we conclude this paper in Section V.

II. 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. This section makes consideration on superimposing of two pixels. In general, the intensity of a pixel is from 0 to 1. If the

M. Higuchi is with the Department of Computer and Information Science, the Faculty of Science and Technology, Seikei University, JAPAN (E-mail: m-higuchi@ejs.seikei.ac.jp).

A. Emori is with the Graduate school of Science and Technology, Seikei University, JAPAN.

S. Kawasaki, J. Gamba, A. Koike and H. Murakami are with the Department of Computer and Information Science, the Faculty of Science and Technology, Seikei University, JAPAN.

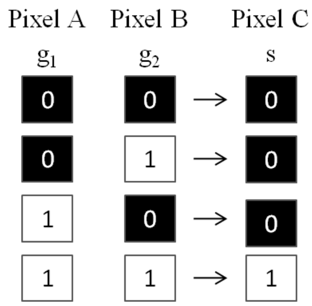

Fig. 1. Superimposing two binary pixels (which is the same as logical product of two pixels in Boolean algebra)

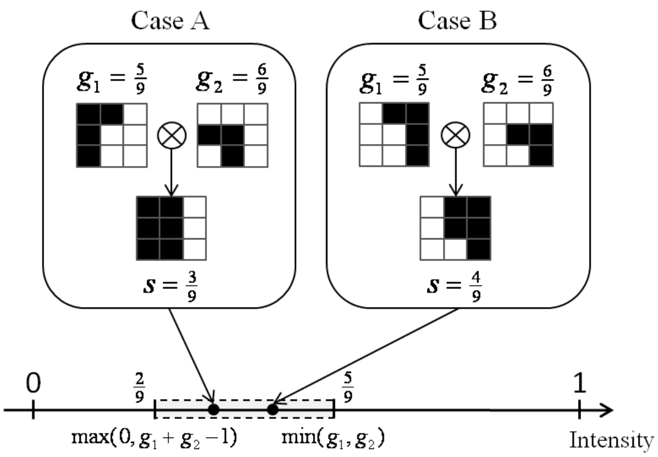

Fig. 2. Superimposing two binary pixel domains and the pseudo-intensities of binary pixel domains

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],

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

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 these pixels in Boolean algebra (see in Fig. 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 Fig. 2. We consider 3×3 square binary pixel domains in Fig. 2. We take a pair of two domains that the one has five white pixels, i.e., the pseudo-intensity of the domain is $5/9 (= g_1)$, and the other has six white pixels, i.e., the pseudo-intensity of the domain is $6/9 (= g_2)$. 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 Cases A and B). In each case, the pseudo-intensity of the binary pixel domain obtained by superimposing those two domains belongs to $[2/9,\ 5/9]$ by the inequality (1). They are $3/9$ and $4/9$ in Case A and B, respectively.

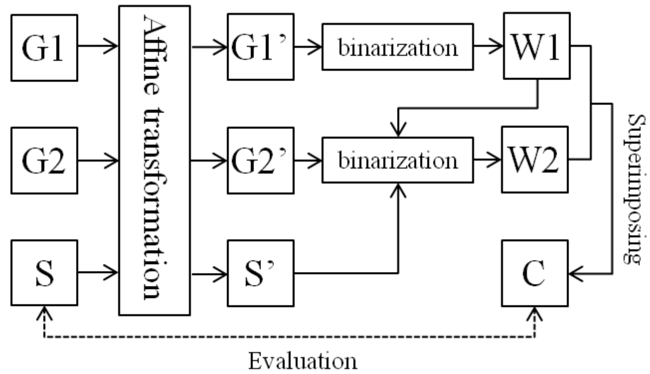

Fig. 3. The flowchart of Myodo's method

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.

III. Conventional method

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

A. The image encryption process

The flowchart of Myodo's method is shown in Fig. 3. Myodo's method takes three gray-scale images, G1, G2 and S, as input. 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. G1, G2 and S are transformed to images G1', G2' and S' by affine intensity transformation, respectively. Images W1 and W2 are share images. W1 is produced from G1' by using error diffusion with high speed and quality. Then, by binarizing G2' according to information of W1 and S' by using error diffusion, W2 is generated with high speed and quality. It means that pixel arrangements of pixel domains in intermediate image of producing W2 change according to information of W1 and S'. The image C is the restored image obtained by superimposing share images. We evaluate the quality of C.

B. Intensity transformation

Myodo's method is based on the principle of superimposing binary pixel domains in Section II. The pseudo-intensities of pixel domains in C approximate to the intensities of corresponding pixels in S' by rearranging white and black pixels

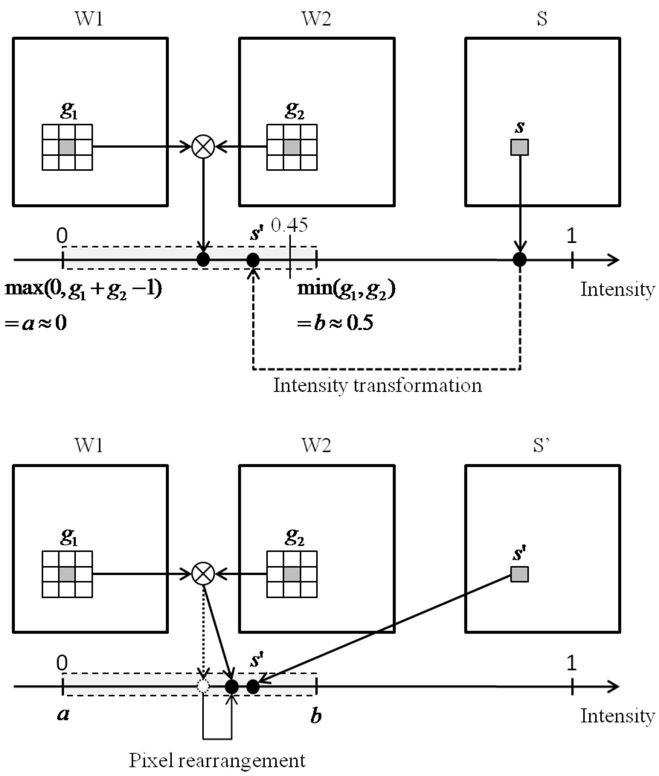

Fig. 4. The mechanism of Myodo's method

in share images. However, it may be error if the inequality (1) is not satisfied. Therefore, Myodo's method requires intensity transformations 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 intensities of each pixel in G1 and G2 to around 0.5, a suitable intensity transformation is applied to G1 and G2, i.e.,

$$g' = 0.45g + 0.275 \tag{2}$$

where g denotes the intensity of a pixel in G1 or G2, and g' denotes the intensity obtained by applying the intensity transformation to the pixel. By this affine transformation, the range of intensities reduce from $[0, 1]$ to $[0.275, 0.725]$. Then, the pseudo-intensities of each pixel domain in images binarized G1 and G2 converge to around 0.5. The intensity of a pixel in S is transformed into below 0.45, i.e.,

$$s' = 0.45s \tag{3}$$

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

We explain the mechanism of Myodo's method in Fig. 4. There is a small gray square in S. Also there are two small gray ones in W1 and W2, respectively. 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,

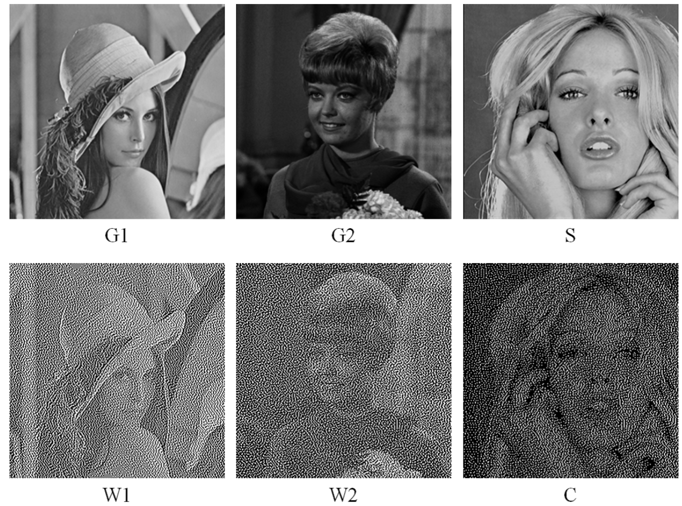

Fig. 5. An example of the results by Myodo's method (Case A)

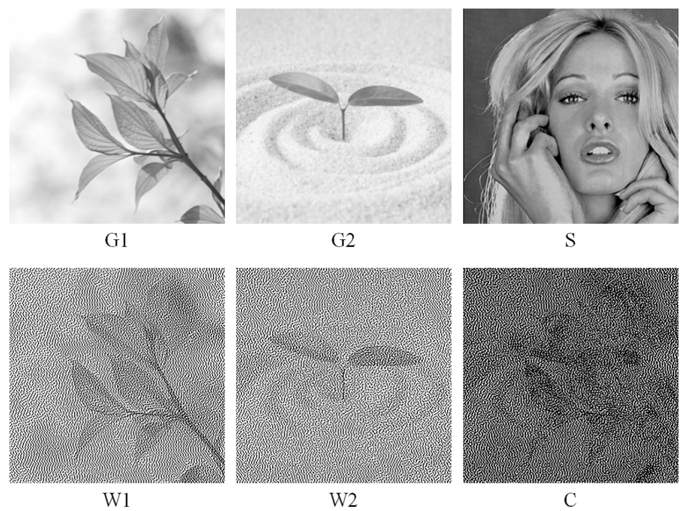

Fig. 6. An example of the results by Myodo's method (Case B)

and let s be the intensity of the pixel in S. For g_1 and g_2, the inequality (1) is $[a,\ b]$ where a and b are two numbers close or equal to 0 and 0.5, respectively, because g_1 and g_2 are around 0.5 by the affine transformation (2) to G1 and G2, respectively. $[a,\ b]$ is a range with almost maximum length. Since $s' \in [0,\ 0.45]$ by the affine transformation (3), s' almost belongs to $[a,\ b]$ (see the upper part of Fig. 4). Moreover, by changing arrangement of white and black pixels in the pixel domain in W2, the pixel domain has a pseudo-intensity close to s' is obtained from the pixel domains in W1 and W2 (see the lower part of Fig. 4). Therefore, C is similar to S'.

C. Example and problem

We show an example of results obtained by using Myodo's method in Fig. 5. W1 and W2 are apparently high quality and also C is reconstructed by superimposing W1 and W2 with apparently high quality in this example.

We show another example in Fig. 6. W1 and W2 are apparently high quality but the quality of C is poor in this

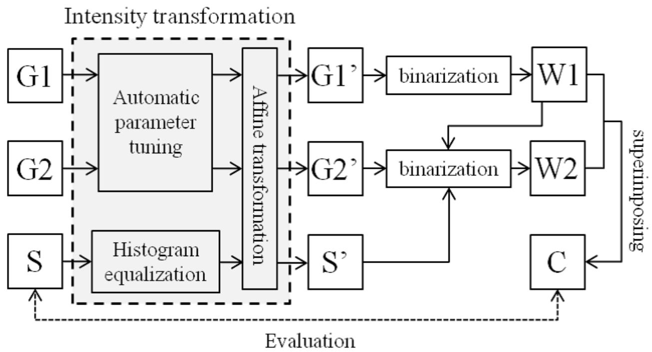

Fig. 7. The flowchart of our method

example. When most of the intensities of pixels in G1 and G2 are high values over 0.5, those in G1' and G2' obtained by applying the affine transformation (2) to G1 and G2 are also high values in the reduced intensity range $[0.275, 0.725]$. Then, the length of the inequality (1) for the pseudo-intensities of pixel domains in W1 and W2 is not enough. Moreover, the left side of the range is around 0.5. On the other hand, the intensities of pixels in S are transformed into below 0.45 by the affine transformation (3). Therefore, the inequality (1) is almost not satisfied in Fig. 4. This reason is the cause of the poor quality of C in Fig. 6.

Hence, Myodo's method is poor performance for a kind of input images.

IV. Proposed method

In this section, we review our method based on improving intensity transformation in Myodo's method [10]–[13] and show that the method can produce share images from which a secret image can be reconstructed with higher quality in term of visual effects than Myodo's method.

A. The proposed image encryption process

The flowchart of our method is shown in Fig. 7. We improve the intensity part in Myodo's method. The affine transformation tuned its parameters according to input images is applied to G1 and G2. Also we apply the histogram equalization to S before affine transformation with the same parameters in Myodo's method. The other parts except intensity part are the same as Myodo's method.

B. Automatic tuning of parameters in affine transformation

In Section III, Myodo's method is poor performance for input images G1 and G2 like whitish. In order to solve the problem, we make an affine transformation that transform the average of intensities of pixels in input images into 0.5 and reduce the intensity range. We determine the parameters of the affine transformation as follows:

1) For each G1 and G2, calculating the average intensity m of the input image.
2) Getting the minimum intensity g_{min} and the maximum intensity g_{max} of the input image.
3) If $|m - g_{min}| \leq |m - g_{max}|$,
$$p_1 = \frac{U - 0.5}{g_{max} - m}, \quad p_2 = 0.5 - p_1 m,$$
otherwise
$$p_1 = \frac{0.5 - L}{m - g_{min}}, \quad p_2 = 0.5 - p_1 m,$$
where L and U denote the minimum and maximum intensities of the image obtained by applying the affine transformation to the input image, respectively.
4) Making the affine transformation by
$$g' = p_1 g + p_2 \tag{4}$$
where g denotes the intensity of a pixel in the input image, and g' denotes the intensity obtained by applying the intensity transformation to the pixel.

By applying the affine transformation (4) to G1 and G2, the intensities of pixels in G1' and G2' converge around 0.5 even if G1 and G2 are whitish. Hence, for those input images, the inequality (1) is satisfied in Fig. 4 and C is reconstructed with high quality.

C. Histogram equalization

In Myodo's method, the affine transformation (3) is applied to S. Then, S' becomes a little bit dark since the intensity of each pixel in S is uniformly transformed. Therefore, a low-key image is generated as restored image by superimposing share images. So we consider histogram equalization as the way to increase the contrast of an image and apply it to S before affine transformation in order to obtain restored images with apparently higher quality.

The histogram equalization is given by the following expression,
$$g' = \frac{\int_0^g p(r)dr - p(0)}{1 - p(0)} \tag{5}$$
where g denotes the intensity of a pixel in an image, g' denotes the intensity obtained by applying the histogram equalization to the pixel and p denotes distribution function with respect to the intensity of a pixel in the image. 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. The histogram equalization is one of ways to realize the thing. By the histogram equalization, the cumulative distribution function of p is straight.

D. Examples of comparison of results by Myodo's and proposed methods

We show examples of results obtained by using Myodo's and proposed methods in Fig. 8 and Fig. 9. We set $L = 0.25$ and $U = 0.75$ when calculating the parameters in the affine transformation (4). 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

Fig. 8. An example of results by Myodo's and proposed methods (Case A)

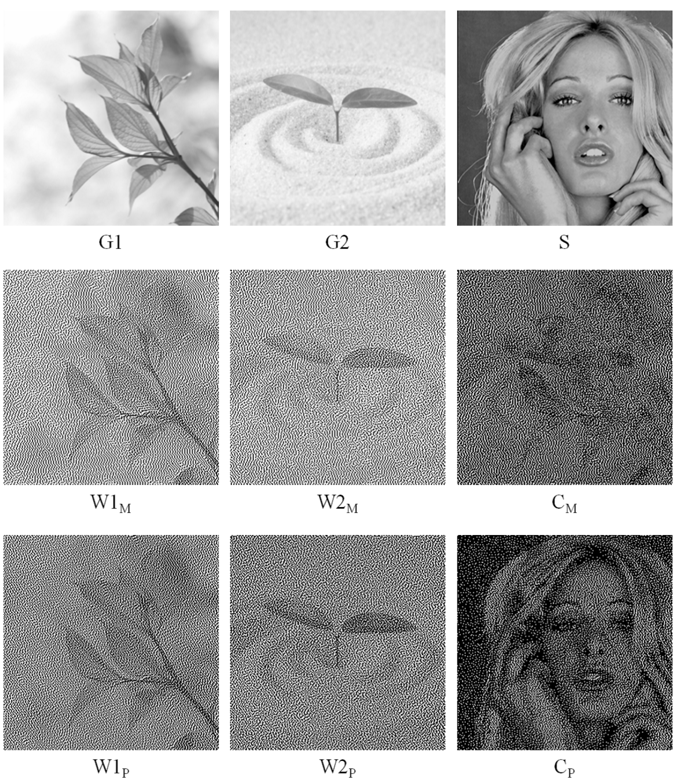

Fig. 9. An example of results by Myodo's and proposed methods (Case B)

generated by our method and restored image obtained by superimposing $\mathrm{W1_P}$ and $\mathrm{W2_P}$, respectively, in Fig. 8 and Fig. 9. It is difficult to distinguish $\mathrm{W1_M}$ from $\mathrm{W1_P}$ and

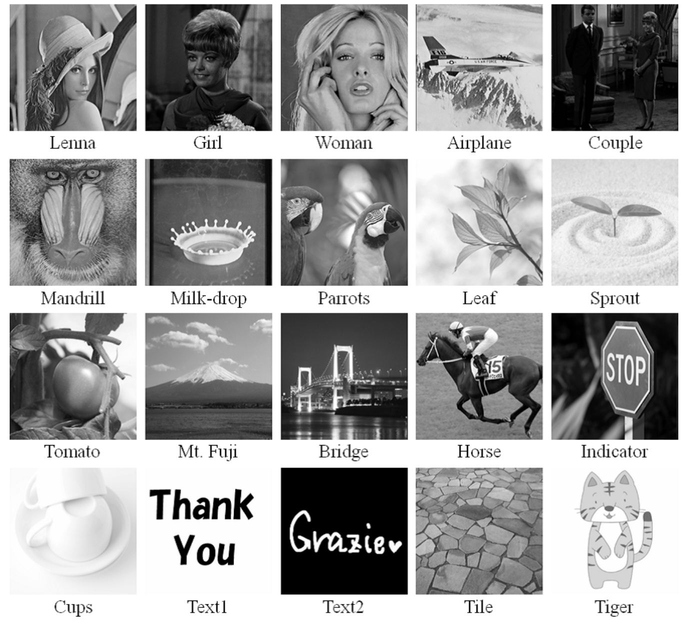

Fig. 10. Sample images used in our experiment

$\mathrm{W2_M}$ from $\mathrm{W2_P}$, respectively, in both of Fig. 8 and Fig. 9. In Myodo's and our methods, share images are low-contrast since the intensity ranges of G1 and G2 which are materials of share images are reduced by affine transformations. $\mathrm{W1_P}$s and $\mathrm{W2_P}$s are gray-like in Fig. 8 and Fig. 9 since the intensities of pixels in G1 and G2 are transformed into around 0.5 by the affine transformation (4). $\mathrm{C_M}$ and $\mathrm{C_P}$ are low-key but $\mathrm{C_P}$ is higher-contrast and apparently higher quality than $\mathrm{C_M}$ in Fig. 8. Also, $\mathrm{C_P}$ is reconstructed with apparently higher quality than $\mathrm{C_M}$ in Fig. 9.

E. Experimental results

We evaluate the performance of Myodo's and our method for any input images objectively and subjectively. We show sample images used in this experiment in Fig. 10. The experiment procedure is as follow:

1) We choose three images from 20 sample images as G1, G2 and S. The triplets of (G1, G2, S) amount to 6840, note that we distinguish between (G1,G2, S) $= (a, b, c)$ and (G1, G2, S) $= (b, a, c)$.
2) From each triplet, we generate two pairs of $(\mathrm{W1_M}, \mathrm{W2_M})$ and $(\mathrm{W1_P}, \mathrm{W2_P})$ by using both of Myodo's and our methods.
3) We produce $\mathrm{C_M}$ and $\mathrm{C_P}$ from each pair of share images, respectively.
4) We evaluate how the qualities of two restored images by the way we objectify and look resulting images.
5) We also evaluate how the qualities of share images objectively and subjectively.

As an objective evaluation, we use a block PSNR. 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 G and W is given by the following expression,

$$\begin{aligned} &\mathrm{bPSNR} = 10\log_{10}(1 \cdot 1/\mathrm{ER}), \\ &\mathrm{ER} = \frac{m^2}{NM} \sum_{k=1}^{\lceil NM/m^2 \rceil} (\hat{g}_k - \hat{w}_k)^2, \\ &\hat{g}_k = \frac{\sum_{i \in R_k^{\mathrm{G}}} g_i}{\sum_{i \in R_k^{\mathrm{G}}} 1}, \quad \hat{w}_k = \frac{\sum_{i \in R_k^{\mathrm{W}}} w_i}{\sum_{i \in R_k^{\mathrm{W}}} 1} \end{aligned} \tag{6}$$

where g_i and w_i denote the intensities of each pixel in G and W, respectively, R_k^{G} and R_k^{W} denote $m \times m$ pixels square which are locating at same positions in G and W, respectively. In the case that G is a gray-scale image and W is a binary image, $\hat{g}_k$ and $\hat{w}_k$ are the average of intensities of pixels in R_k^{G} and the pseudo-intensity of R_k^{W}, respectively. We set $m = 4$ in our experiment. For all of triplets of (G1, G2, S), we compute two block PSNRs corresponding to two pairs ($\mathrm{C_M}$, S) and ($\mathrm{C_P}$, S), respectively. After that we average each of those block PSNRs with respect to S, which we name "$\mathrm{bPSNR}^{ave}_{\mathrm{C_M}}$" and "$\mathrm{bPSNR}^{ave}_{\mathrm{C_P}}$," respectively. Moreover, we investigate the proportion of triplets as the block PSNR of ($\mathrm{C_P}$, S) is higher than it of ($\mathrm{C_M}$, S). Also, we get two block PSNRs corresponding to two pairs ($\mathrm{W1_M}$, G1) and ($\mathrm{W1_P}$, G1), which we name "$\mathrm{bPSNR}_{\mathrm{W1_M}}$" and "$\mathrm{bPSNR}_{\mathrm{W1_P}}$," respectively. Similarly we obtain two block PSNRs corresponding to two pairs ($\mathrm{W2_M}$, G2) and ($\mathrm{W2_P}$, G2), respectively, and average each of those block PSNRs with respect to G2, which we name "$\mathrm{bPSNR}^{ave}_{\mathrm{W2_M}}$" and "$\mathrm{bPSNR}^{ave}_{\mathrm{W2_P}}$," respectively. The encryption of secret images does not affect the quality of W1. It depends on affine transformations and the performance of error diffusion. Therefore, we use block PSNRs of (W1, G1) as quality indicators of W2. The results are shown in Table I and Table II.

As a subjective evaluation, we consider the following four terms of visual effects for restored images:

- Case A that $\mathrm{C_P}$ is apparently better than $\mathrm{C_M}$.
- Case B that $\mathrm{C_M}$ is apparently better than $\mathrm{C_P}$.
- Case C that both of $\mathrm{C_M}$ and $\mathrm{C_P}$ are poor qualities.
- Case D that both of $\mathrm{C_M}$ and $\mathrm{C_P}$ are high qualities and indistinguishable.

We investigate the proportion of triplets such as Case A or D. For share images, it is difficult to distinguish them in most of resulting images. So, we consider the following three terms of visual effects:

- Indistinguishable.
- Darkish.
- Whitish.

Also, we investigate the proportion of triplets as the subjective evaluation of ($\mathrm{C_M}$, $\mathrm{C_P}$) corresponds with the objective one. For Case C, it does not always result in the block PSNR of ($\mathrm{C_M}$, S) being near to it of ($\mathrm{C_P}$, S) since the restored images are not necessarily similar in this case. So, we except the proportion of triplets as (objective evaluation = Case C) from this investigation. The results are shown in Table III and Table IV.

TABLE I
OBJECTIVE EVALUATIONS OF THE QUALITIES OF RESTORED IMAGES IN MYODO'S AND OUR METHODS

S	$\mathrm{bPSNR}^{ave}_{\mathrm{C_M}}$	$\mathrm{bPSNR}^{ave}_{\mathrm{C_P}}$	Objectively ($\mathrm{C_M} < \mathrm{C_P}$)
Lenna	10.7996 dB	11.1173 dB	71.05 %
Girl	16.0162 dB	20.5998 dB	100.00 %
Woman	10.2473 dB	10.0397 dB	50.88 %
Airplane	7.4565 dB	6.3010 dB	0.00 %
Couple	17.9733 dB	17.8251 dB	37.43 %
Mandrill	10.8206 dB	10.8654 dB	62.28 %
Milk-drop	11.9626 dB	13.1704 dB	94.44 %
Parrots	11.0767 dB	11.5528 dB	75.15 %
Leaf	5.9689 dB	4.6338 dB	0.00 %
Sprout	5.4987 dB	3.9277 dB	0.00 %
Tomato	9.5394 dB	9.6840 dB	61.99 %
Mt. Fuji	10.4971 dB	10.7505 dB	69.30 %
Bridge	14.2126 dB	16.6565 dB	100.00 %
Horse	10.9556 dB	11.4167 dB	80.70 %
Indicator	13.3875 dB	15.5784 dB	100.00 %
Cups	4.6922 dB	3.0951 dB	0.00 %
Text1	4.7676 dB	5.0835 dB	53.22 %
Text2	13.9628 dB	15.1747 dB	58.19 %
Tile	10.3203 dB	9.9868 dB	42.40 %
Tiger	4.6112 dB	4.1711 dB	27.78 %
For the total of 6840 patterns			54.24 %

TABLE II
OBJECTIVE EVALUATIONS OF THE QUALITIES OF SHARE IMAGES IN MYODO'S AND OUR METHODS

S	Quality indicators		$\mathrm{bPSNR}^{ave}_{\mathrm{W2_M}}$	$\mathrm{bPSNR}^{ave}_{\mathrm{W2_P}}$
	$\mathrm{bPSNR}_{\mathrm{W1_M}}$	$\mathrm{bPSNR}_{\mathrm{W1_P}}$		
Lenna	19.1535 dB	19.6590 dB	19.0594 dB	19.6432 dB
Girl	14.9969 dB	10.7336 dB	14.9754 dB	10.7240 dB
Woman	19.9717 dB	19.9387 dB	19.8624 dB	19.9144 dB
Airplane	16.3673 dB	12.7882 dB	16.3865 dB	12.7768 dB
Couple	13.1576 dB	8.3284 dB	13.1281 dB	8.3198 dB
Mandrill	20.9988 dB	21.4884 dB	20.8519 dB	21.4025 dB
Milk-drop	17.8038 dB	16.2585 dB	17.6381 dB	16.1945 dB
Parrots	18.8770 dB	18.8974 dB	18.7999 dB	18.8150 dB
Leaf	14.1199 dB	9.7251 dB	14.1371 dB	9.7230 dB
Sprout	13.5114 dB	8.6678 dB	13.5349 dB	8.6573 dB
Tomato	16.1728 dB	16.9401 dB	16.1099 dB	16.8971 dB
Mt. Fuji	18.1699 dB	19.0304 dB	18.1216 dB	19.0041 dB
Bridge	16.1355 dB	12.5485 dB	16.1111 dB	12.5428 dB
Horse	18.2099 dB	18.1497 dB	18.1734 dB	18.1066 dB
Indicator	14.2337 dB	10.7127 dB	14.2456 dB	10.6990 dB
Cups	12.2412 dB	7.2521 dB	12.2379 dB	7.2487 dB
Text1	11.5065 dB	7.3932 dB	11.4832 dB	7.3980 dB
Text2	11.3465 dB	6.6463 dB	11.3135 dB	6.6381 dB
Tile	21.8169 dB	21.8167 dB	21.6343 dB	21.8030 dB
Tiger	12.0227 dB	7.1145 dB	12.0160 dB	7.1133 dB

F. Discussion

By Table I, patterns that the block PSNR of ($\mathrm{C_P}$, S) is higher than it of ($\mathrm{C_M}$, S) are about 54 percent in 6840 triplets of (G1, G2, S) and we see that for 12 kinds of S in 20 sample images, $\mathrm{bPSNR}^{ave}_{\mathrm{C_P}}$ is higher than $\mathrm{bPSNR}^{ave}_{\mathrm{C_M}}$ and for each of the 12 images, the block PSNR of ($\mathrm{C_P}$, S) is higher than it of ($\mathrm{C_M}$, S) over 58 percent in 342 pairs of (G1, G2). By Table III, patterns that the subjective quality of ($\mathrm{C_M}$, $\mathrm{C_P}$)

TABLE III
SUBJECTIVE EVALUATION OF THE QUALITIES OF RESTORED IMAGES IN MYODO'S AND OUR METHODS AND RELATIONSHIPS WITH OBJECTIVE ONE

S	subjectively ($\mathrm{C_M} \leq \mathrm{C_P}$)	Objective eval. corresponds with		
		Case A	Case B	Case D
Lenna	100.00 %	71.05 %	0.00 %	0.00 %
Girl	100.00 %	100.00 %	0.00 %	0.00 %
Woman	100.00 %	50.88 %	0.00 %	0.00 %
Airplane	100.00 %	0.00 %	0.00 %	0.00 %
Couple	100.00 %	37.43 %	0.00 %	0.00 %
Mandrill	100.00 %	62.28 %	0.00 %	0.00 %
Milk-drop	0.00 %	0.00 %	0.00 %	0.00 %
Parrots	100.00 %	75.15 %	0.00 %	0.00 %
Leaf	89.47 %	0.00 %	0.00 %	0.00 %
Sprout	100.00 %	0.00 %	0.00 %	0.00 %
Tomato	98.25 %	9.06 %	0.00 %	5.56 %
Mt. Fuji	0.00 %	0.00 %	0.00 %	0.00 %
Bridge	0.00 %	0.00 %	0.00 %	0.00 %
Horse	97.37 %	35.96 %	0.00 %	0.00 %
Indicator	0.00 %	0.00 %	0.00 %	0.00 %
Cups	98.25 %	0.00 %	0.00 %	0.00 %
Text1	100.00 %	14.33 %	0.00 %	6.14 %
Text2	38.89 %	26.61 %	6.43 %	0.29 %
Tile	100.00 %	42.40 %	0.00 %	0.00 %
Tiger	100.00 %	27.78 %	0.00 %	0.00 %
For 6840 pat.	76.11 %	27.65 %	0.32 %	0.60 %

TABLE IV
SUBJECTIVE EVALUATION OF THE QUALITIES OF SHARE IMAGES IN MYODO'S AND OUR METHODS

S	Myodo's method	Our method
Lenna	Indistinguishable	
Girl	Darkish	Whitish
Woman	Indistinguishable	
Airplane	Whitish	Darkish
Couple	Darkish	Whitish
Mandrill	Indistinguishable	
Milk-drop	Indistinguishable	
Parrots	Indistinguishable	
Leaf	Whitish	Darkish
Sprout	Whitish	Darkish
Tomato	Indistinguishable	
Mt. Fuji	Indistinguishable	
Bridge	Darkish	Whitish
Horse	Indistinguishable	
Indicator	Darkish	Whitish
Cups	Whitish	Darkish
Text1	Whitish	Darkish
Text2	Darkish	Whitish
Tile	Indistinguishable	
Tiger	Whitish	Darkish

become Case A or D are about 76 percent in 6840 triplets of (G1, G2, S) and we see that for 15 kinds of S in 20 sample images, Case A or D is over about 90 percent in 342 pairs of (G1, G2). For "Milk-drop," "Mt. Fuji," "Bridge," "Indicator" and "Text2," in the sample images, the subjective quality is almost Case B or C. When at least one of G1 and G2 contains those images or "Text1," a part of G1 or G2 tends to appear in restored images. From this result, the qualities of restored images by subjective evaluation almost depend on the properties of secret images. Also, subjective evaluation does not necessarily correspond with objective one. For example, 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.

By Table II, for 15 kinds of S in 20 sample images, both of $\mathrm{bPSNR}^{ave}_{\mathrm{W2_M}}$ and $\mathrm{bPSNR}^{ave}_{\mathrm{W2_P}}$ are slightly lower than their quality indicators, respectively, since W2s contain the information of W1 and S, i.e., the qualities of them may be worse than W2s obtained by binarizing G2 normally. The effect by changing affine transformation in Myodo's and our methods is that for "Girl," "Airplane," "Couple," "Leaf," "Sprout," "Bridge," "Indicator," "Cups," "Text1," "Text2" and "Tiger," the objective qualities of the share images by our method are very lower than them by Myodo's method, and appears in the subjective qualities of share images too (see in Table IV), note that "Indistinguishable" in Table IV means that share images are the same and rather high qualities with respect to appearance in both of Myodo's and our methods. For most of triplets of (G1, G2, S), share images have rather high qualities in term of visual effects in both of Myodo's and our methods, except two sample images, "Couple" and "Cups." The share images obtained from "Couple" and "Cups" are poor quality in our and Myodo's method, respectively.

V. CONCLUSION

In this paper, we reviewed the method developed by us previously and evaluated its performance for any input images objectively and subjectively. As a result, we obtained the following five remarks:

- Myodo's and our methods have almost the same efficiency with respect to objective evaluation.
- Our method is better than Myodo's one with respect to subjective evaluation.
- The qualities of restored images by subjective evaluation almost depend on the properties of secret images.
- Subjective evaluation does not necessarily correspond with objective one.
- Share images are rather high qualities in term of visual effects in both of Myodo's and our methods. They 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 input secret images according to the properties of those images in order to generate higher quality share images with higher speed from which a secret image can be reconstructed with higher quality than our method in this paper. 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.

ACKNOWLEDGMENT

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*, vol. E81-A, No. 6, 1998, pp. 1262–1269.

[4] M. Nakajima and Y. Yamaguchi, "Extended visual cryptography for natural images," *Journal of WSCG*, vol. 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*, vol. 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*, vol. 106, No. 22, IE2006-2, 2006, pp. 7–12.

[7] M. Nakamura, Y. Omiya, K. Katagishi, Y. Morooka, K. Toraichi, H. Murakami, "A Secure Coding for Function-Approximated Images," *Proceedings of the 12th WSEAS International Conference on COMMUNICATIONS*, 2008, pp. 416–420.

[8] Y. Omiya, M. Nakamura, K. Katagishi, Y. Morooka, K. Toraichi, H. Murakami, "Scalable and High-Precision Function-Approximated Images and Its Secure Coding," *WSEAS TRANSACTIONS on COMMUNICATIONS*, Issue 9, vol. 7, 2008, pp. 954–963.

[9] Dusmanescu Dorel, "Encrypting messages with visual key," *WSEAS TRANSACTIONS on COMPUTERS*, Issue 5, vol. 8, 2009, pp. 757–766.

[10] 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*, vol. 47, No. 1, 2010, pp. 67–73.

[11] 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*, vol. 34, No. 31, AIT2010-106, 2010, pp. 53–56.

[12] M. Higuchi, A. Emori, S. Kawasaki, J. Gamba, A. Koike, H. Murakami, "High-Quality Reconstruction of Secret Images by Tuning Parameters of Intensity Transformations in Visual Cryptography," *Journal of the Faculty of Science and Technology, Seikei University*, 2010, accepted.

[13] M. Higuchi, A. Emori, S. Kawasaki, J. Gamba, A. Koike, H. Murakami, "Performance Evaluation of Visual Cryptography Schemes with Intensity Transformations for Gray-Scale Images," *Proceedings of the 3rd WSEAS International Conference on VISUALIZATION, IMAGING and SIMULATION*, 2010, pp. 111–117.