# HALFTONE VISUAL CRYPTOGRAPHY EMBEDDING A NATURAL GRAYSCALE IMAGE BASED ON ERROR DIFFUSION TECHNIQUE

*Emi Myodo, Koichi Takagi, Satoshi Miyaji, Yasuhiro Takishima*

KDDI R&D Laboratories Inc.

## ABSTRACT

This paper proposes a novel visual cryptography method that embeds a natural secret image into two natural carrier images with high quality at low computational complexity. The secret image is decoded visually by superposing the two carrier images. For some applications such as entertainment use, all three images should be high quality natural images and low computational complexity is also required. However, in the conventional methods, picture quality and processing speed have been tradeoff relations. To solve this problem, we propose a method which is based on conventional visual cryptography using error diffusion halftoning and introduce an additional feedback mechanism to embed the high quality natural image. Experimental results show that the proposed method can achieve higher quality natural images of a superposed image and carrier images while computational complexity is maintained low when compared with the conventional methods.

## 1. INTRODUCTION

Classical visual cryptography embeds a simple graphic secret image distributed into multiple random-dot carrier images. It visually decodes the secret image by superposing the multiple carrier images without any electronic calculations [1]. As an enhanced scheme of visual cryptography, several methods that embed a secret image into two natural images instead of meaningless random-dots images are studied [2]-[5], where the input natural images are halftoned and they are modulated by the secret image. Moreover, methods [6] and [7] can embed a natural image as a secret image, whereas methods [2]-[5] embed only simple graphics such as a logo image.

If the quality of the carrier and the secret images is improved, the visual cryptography is used not only for security purposes such as secret sharing and authentication, but also entertainment use such as greeting cards and advertisements. For such entertainment use, users may want to use their own photos to embed a secret image. In this case, the following issues must be considered: (i) a secret image should be a natural image, (ii) images that carry a secret image should be high quality natural images and (iii) computational cost should be low.

Methods [6] and [7] can satisfy the requirement of (i). However, since the method [6] does not account for the quality of the pixel pattern arrangement, it may be difficult to satisfy the quality requirement (ii). As for the method [7], it may be difficult to satisfy the requirement of low computational complexity (iii) since the method involves iteration process.

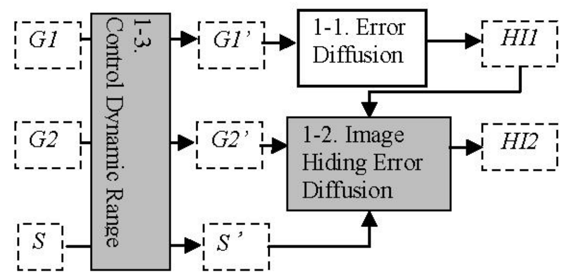



**Fig. 1 Visual cryptography method using error diffusion.**

This paper proposes a method that satisfies all the requirements (i), (ii) and (iii). The proposed method is based on [5] which satisfies both (ii) and (iii), and introduces an additional feedback mechanism into the secret image embedding process in order to improve the quality of the visually decoded secret image (i).

## 2. VISUAL CRYPTOGRAPHY USING ERROR DIFFUSION

### 2.1. Conventional Method

In this subsection we describe the conventional method [5], which uses an error diffusion halftoning technique [8].

Fig. 1 illustrates a typical signal flow of visual cryptography that uses error diffusion. Input images are grayscale natural images $G1$, $G2$ $\{g1, g2 | 0 \leq g1, g2 \leq 1\}$ and a secret image $S\{s | 0 \leq s \leq 1\}$. In the conventional method [5], grayscale $S$ cannot be used as an input image and a ternary image $S''$ is used as an input, which is $S$=$S''\{s'' | s'' \in \{0, 0.5, 1\}\}$. Output images $HI1$ and $HI2$ $\{hi1, hi2 | hi1, hi2 \in \{0, 1\}\}$ that carry the secret image are binary. Symbols in small letters stand for pixel values. 0, 0.5 and 1 are black, gray and white, respectively.

At first, $HI1$ is generated from $G1$ by an error diffusion process [8] shown as 1-1 of Fig. 1. Then, $HI2$ is transformed from $G2$ by an image hiding error diffusion process [5] shown as 1-2 in Fig. 1. In the image hiding error diffusion process, pixels of $HI2$ are modulated by corresponding pixels of $HI1$ and a secret image $S$ in order to embed the image $S$ into $HI2$.

1-2 of Fig. 1 includes the error diffusion part and the conventional extension part, both of which are illustrated in Fig. 2. In this scheme, $u2$ is first calculated by the current grayscale pixel $g2'$ plus accumulated error $e2'$ ($u2$=$g2'$+$e2'$). Then, $u2$ is quantized by a threshold $T$ into black or white pixel $t2$ $\{t2 | t2 \in \{0, 1\}\}$ as follows.

**If** ($u2$>T) then $t2$=1(white); **Else** $t2$=0(black); (1)

where $T$=0.5. When the level of $u2$ is very close to the threshold around $\Delta u$ ($T$-$\Delta u$ < $u2$ < $T$+$\Delta u$, $\Delta u \geq 0$), the quality of $HI2$ might not be as deteriorated independently from the $t2$ value being 0 or 1. Therefore, if the condition is satisfied, the pixels of $HI2$ are modulated by $s''$ as follows [5],

**If**($T$-$\Delta u$ < $u2$ < $T$+$\Delta u$) {// condition for embedding
  **If**($s''$==1(white)) then $hi2 = hi1$;
  **Else if** ($s''$==0.5(gray)) then $hi2 = t2$;    (2)
  **Else if** ($s''$ == 0(black)) then $hi2 = \sim hi1$.
}

where $\sim hi1$ stands for inverse value of $hi1$.

Fig. 3 (a) shows the determination process of $hi2$. As shown in Eq. (2), $s''$, $hi1$ and $t2$ determine the value of $hi2$. If black needs to be embedded, $hi2$ should be an inverse value of $hi1$. If white needs to be embedded, $hi2$ should be equal to $hi1$. If gray needs to be embedded, the value of $hi2$ should be equal to the binarized second input image $t2$.

A secret image is optically obtained by superposing the two carrier image $HI1$ and $HI2$. This is also done by mathematical Boolean AND operation of $hi1$ and $hi2$. Fig. 3 (b) shows this process that focuses on a 2 x 2 small block. This example assumes that the density of the block of $HI1$ and $HI2$ is 2/4. When black is embedded into the block, the pixel values of $hi1$ and $hi2$ are inverted to each other. Thus, the superposed (or AND) operation results in four black pixels. When white is embedded into the block, the pixel values of $hi1$ and $hi2$ are exactly the same as each other. In this case, the superposed operation results in two blacks and two whites, which look gray. As for embedding of a gray pixel, no modulation to $hi2$ is applied. Statistically, the average of the pixel value of a natural image is gray level. This means probability of black and white is 50% and 50%. In this case, the result of AND operation of two natural halftoned images would be 25% white and 75% black. Therefore, the block looks like dark gray. This is a basic principle of the halftone visual cryptography [5].

Then, quantization error $e2$ is calculated ($e2$ = $hi2$-$u2$). The error is diffused to the subsequently neighboring pixels by using weighted matrix J [8] as shown in Fig. 4(b). Accumulated error $e2'$ is calculated as follows.

$$e2' = \frac{\sum_{k \in J} J_k \cdot e2_k}{\sum_{k \in J} J_k} \tag{3}$$

This error diffusing mechanism contributes to the quality of $HI1$ and $HI2$ and it also contributes to processing time improvement because it requires no iterative processing to determine the value of pixels.

### 2.2. Proposed Method

#### *2.2.1. Preprocess of dynamic range control*

As one of the requirements mentioned in Section 1, grayscale natural image embedding is required. The fidelity of a superposed image highly depends on its dynamic range. Possible pixel density of the superposed image is given by the following equation (4):

$$\max(0, g1'+g2'-1) < ds < \min(g1', g2') \tag{4}$$

where $g1'$ and $g2'$ are pixel values of dynamic-range-controlled input images and $ds$ is pixel density of the superposed image that is estimated with the surrounding pixels.

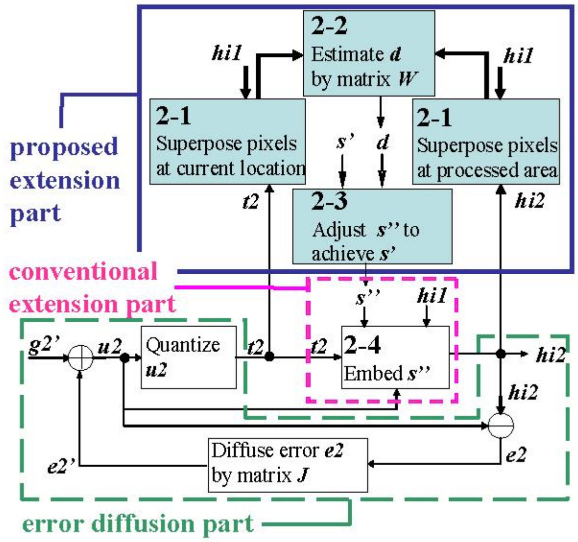



**Fig. 2 Block diagram of embedding process ($HI2$) corresponding to 1-2 of Fig. 1.**

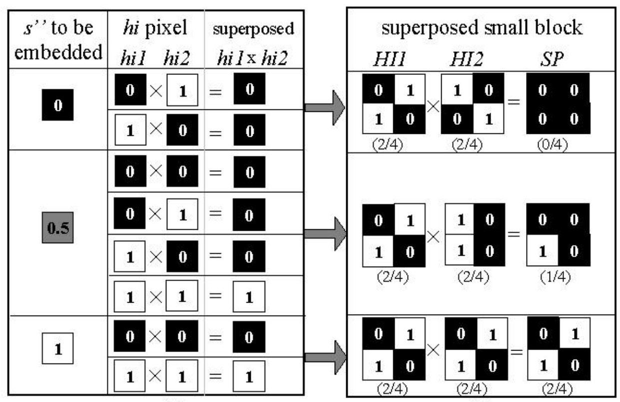



**Fig. 3 Superposed pixel value determination process.**

| | | | | |
|---|---|---|---|---|
| 1 | 2 | 2 | 2 | 1 |
| 2 | 4 | 5 | 4 | 2 |
| 2 | 5 | **6** | - | - |

**current pixel**

(a) Weighting Matrix $W$ for superposed image

| | | | | |
|---|---|---|---|---|
| 1 | 3 | 5 | 3 | 1 |
| 3 | 5 | 7 | 5 | 3 |
| 5 | 7 | ***** | - | - |

**current pixel**

(b)Weighting Matrix $J$ for $HI1$ and $HI2$

**Fig. 4 Weighting matrices.**

This equation indicates that $g1'$=$g2'$=0.5 gives the widest dynamic range of the superposed image. Therefore, pixel values of input images should be modified around 0.5 by reducing their dynamic range. Accordingly, each pixel value of a secret image $S$ should be restricted between 0 and 0.5. In this paper, $S'$ indicates the secret images $S$ with a dynamic range restriction. This operation allows to use any grayscale natural images as inputs $G1$, $G2$ and $S$.

#### *2.2.2. Embed Grayscale Secret Image*

The conventional method [5] has a feedback mechanism to $G1'$ and $G2'$ to enhance the image quality of $HI1$ and $HI2$. In addition to this, the proposed method introduces another feedback mechanism to the secret image embedding process to enhance the quality of the superposed image. The following explains details of the proposed method.

The error diffusion data hiding process (1-2 of Fig. 1) of the proposed method consists of the proposed extension part, the error diffusion part and the conventional extension part, all of which are shown in Fig. 2.

First of all, *G2'* is quantized into a binary image with the error diffusion process and each pixel value *t2* is provided to the proposed extension part and the conventional extension part.

Next, the temporary internal superposed image is calculated by AND operation of *HI1* and *HI2* in the proposed extension part. It should be noted that each pixel value of *HI2* is determined one by one in the embedding process (2-4 of Fig. 2). Therefore, this superposing operation can be performed only on the processed area of *HI2*. Regarding the pixel value of the current position, *t2* is used instead of a pixel of *HI2*. This operation is indicated as 2-1 in Fig. 2.

Then, the proposed method estimates density *d* of the temporary superposed image with the equation (5). This is processed in 2-2 of Fig. 2.

$$d = \frac{\sum_{k \in W} W_k \cdot \{(hi1_k) AND (hi2_k)\}}{\sum_{k \in W} W_k} \quad (5)$$

where *W* is a part of a low-pass filter such as a Gaussian filter as shown in Fig. 4(a) and the AND operation means generating of the temporary internal superposed image.

In order to make the superposed result closer to the secret image *s'*, a new component is introduced in the proposed extension part, which is indicated as 2-3 in Fig. 2. In this component (2-3), the value *s''* is determined according to the direction to be taken by the current density, which is toward darker or toward brighter. The value *s''* is used for the modulation process of *HI2* in the component 2-4 in Fig. 2, where *s''*=0 changes density of the superposed image into darker direction, *s''*=1 changes it into brighter and *s''*=0.5 doesn't change density at all.

The direction is controlled by the distance between *s'* and *d* as follows. If *d* is much smaller than *s'*, the current density should be brighter to achieve the desired embedding of *s'*. Therefore, 1 (white pixel) is chosen for *s''*. If *d* is much larger than *s'*, 0 (black pixel) is chosen for *s''*. Otherwise, *s''* is equal to 0.5 because the current density is already close enough to that of the desired one in this case. The following is pseudo code of this process:

**If** (*s'-d* > Tb) then {*s''*=1;}
**Else if** (*d-s'* > Tw) then {*s''*=0;} (6)
**Else** {*s''*=0.5;}

where Tb and Tw are thresholds to decide the embedded value *s''* to be brightened and darkened, respectively.

Finally, *hi2* is determined according to *t2*, *hi1* and *s''* in the conventional extension part (2-4 of Fig. 2). A graphical explanation is shown in Fig. 3.

Thus, in the proposed method, the additional feedback mechanism from the temporary superposed image improves the fidelity of the grayscale original secret image. Moreover, no iteration procedure is required in the same way as the method [5].

## 3. SIMULATION RESULTS AND DISCUSSION

To verify the performance of the proposed method described in the above section, objective and subjective quality evaluation was carried out and the processing cost was also evaluated.

**Table 1 Comparison of image quality and processing cost.**

| Method | Image Quality (MAE[9]) | | | Cost |
|---|---|---|---|---|
| | *HI1* | *HI2* | *SP* | |
| | Req=(ii) | | Req=(i) | Req=(iii) |
| CM1[5] | 4.50 | 4.56 | 20.52 | 1 |
| CM2[6] | 15.59 | 14.81 | 15.70 | –*[1] |
| CM3[7] | 11.46 | 8.75 | 10.83 | 15 |
| PM | 4.50 | 4.99 | 11.51 | 1.5 |

***[1] no filtering**

### 3.1. Experimental Conditions

We used a set of the three images (*G1*, *G2*, *S*) =(Lenna, Girl, Woman) for the experiment. For the proposed method (**PM**), the conventional method [5] (**CM1**) and [7] (**CM3**), the size of the input images and the output images were 256 x 256 pixels and they have 256 gray levels. For the conventional method [6] (**CM2**), the size of the input images was 64 x 64 and the output images were 256 x 256 pixels because the method [6] cannot generate an output image of which the size is the same as the input image. Dynamic range transformation is *g'*=0.45*g*+0.275 for *G1* and *G2* and *s'*=0.45*s* for *S*. The threshold for quantization *T* is set to 0.5. These parameters are determined by the preliminary experiments. A threshold for ternary conversion is *Tw=Tb=w*/(2 $\Sigma$ *W*), where *w* is the weighting value of *W* of the position corresponding to the current pixel. Refering to each value of W shown in Fig.4 (a), Tw=Tb=6/(2 x 38)=0.0789.

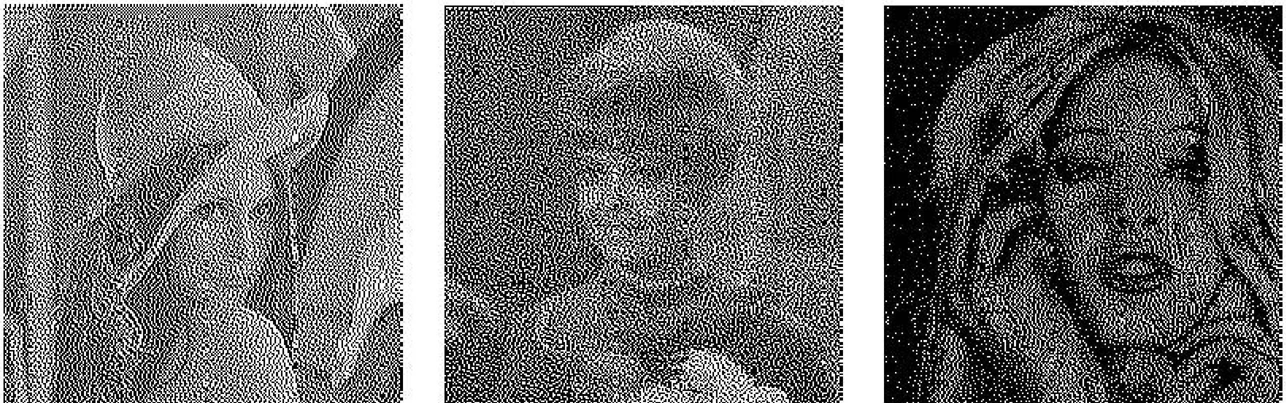
A Gaussian matrix (Fig. 4(a)) is used for density calculation of the superposed image and a *Jarvis, Judice & Ninke* weighted matrix (Fig. 4(b)) is used for *HI1* and *HI2* generation [8]. Embedding condition parameter $\Delta u$ (2) is 0.067. It should be noted that an only simple ternary image can be used for the secret image in **CM1**, therefore *s* must be reduced to 3 levels in advance in this case. If *s*>0.75, *s''*=1, if *s*<0.25, *s''*=0, if $0.25 \leq s \leq 0.75$, *s''*=0.5 for input *S*(=*S''*).

### 3.2. Image Quality of Carrier Image *HI1*, *HI2* and Superposed Image *SP*

Objective quality is evaluated by Mean Absolute Error (MAE) between *HI1* and *G1'*, *HI2* and *G2'*, a superposed image *SP* and *S'* as shown in Table 1 [9]. Since *HI1*, *HI2* and *SP* are binary images, density is used to calculate MAE, where a 5 x 5 Gaussian filter *W* ($\sigma = 1.5$) applies to emulate human visual system against binary images. Processing cost is also shown in the table and it is calculated in proportion to the cost of filter convolution when the cost of the conventional method [5] (**CM1**) is set to 1 except for the conventional method [6] (**CM2**) which doesn't require a filter.

Regarding the proposed method (**PM**) and the conventional method [5] (**CM1**), MAE of *HI1* and *HI2* is almost the same, but the MAE of superposed image *SP* of **PM** is remarkably decreased to 1/2 compared with **CM1**. This indicates that **PM** improves the quality of *SP* while minimizing the quality degradation of *HI1* and *HI2*. This is because **PM** introduced the feedback mechanism to a secret image embedding process that is not included in **CM1**.

As for the conventional method [6] (**CM2**), very large degradation has been observed. This is because the fidelity to the input images is not taken into account in terms of density perceived by human visual system.



(a) *HI1* (b) *HI2* (c) *SP* of (a) AND (b)

**Fig. 5 Generated images of *HI1*, *HI2* and superposed image *SP* of the proposed method PM.**

The conventional method [7] (**CM3**) uses an iteration procedure. If the number of iterations is increased, the image quality of *SP* improves, whereas *HI1* and *HI2* gets worse compared to the initial images that are produced just by the error diffusion process onto the input images. In addition, the iteration process might cause an increase of computational complexity. The MAE of **CM3** saturates when the number of iterations reaches approximately 3, where processing cost is 10 times higher than that of the proposed method which requires no iteration procedure while MAE of **CM3** is still higher than that of **PM**.

Fig. 5 shows *HI1*, *HI2* and *SP* generated by **PM**. The natural image is visually decoded clearly as shown in Fig.5(c) by superposing carrier images (Fig. 5(a)(b)). Fig. 6 shows the superposed image generated by **CM1**. The superposed image of Fig. 6 looks noisy and the fidelity to the original secret image is low because **CM1** doesn't account for the quality of the superposed image.

Since **PM** achieves the above mentioned high quality results without using any iteration processes, **PM** outperformed among all the methods in terms of processing speed and quality. We consider that high quality secret and carrier images will contribute to various entertainment applications such as lottery, secret greeting cards, advertisements and so on. Low computational complexity will contribute to future enhancements such as the enlargement of image size, server applications that requires 10 times simultaneous processing capacity and so on.

**Fig. 6 Superposed image *SP* of the conventional method CM1.**

## 4. CONCLUSIONS

This paper proposed a visual cryptography method for embedding a natural image based on error diffusion halftoning. To improve the quality of a secret image, a density feedback mechanism is introduced in the process of the carrier image generation. As a result, we verified that the proposed method can embed a secret image with the least impact to quality of the carrier images while keeping low computational complexity. In addition, quality of the visually decoded secret image is also improved compared to the conventional method.

## 5. ACKNOWLEDGMENTS

The authors would like to thank Dr. Shigeyuki Akiba, Dr. Shuichi Matsumoto and Dr. Yasuyuki Nakajima for their continuous support and encouragement.

## 6. REFERENCES

[1] M. Noar and A. Shamir, "Visual Cryptography," *Proc. Eurocrypt '94*, pp.1-12, 1994.

[2] K. Oka, Y. Nakamura and K. Matsui, "Embedding Signature into a Hardcopy Image Using a Micro-Patterns," *IEICE Trans.*, Vol. J79-D-II, No. 9, pp. 1624-1626, 1996 (in Japanese).

[3] K. Oka, Y. Nakamura and K. Matsui, "Embedding Signature into a Hardcopy of Ordered Dithered Image," *IEICE Trans.*, Vol. J80-D-II, No. 3, pp. 820-823, 1997 (in Japanese).

[4] E. Myodo, S. Sakazawa and Y. Takishima "Visual Cryptography Based on Void-and-cluster Halftoning Technique," *Proc. IEEE ICIP*, pp. 97-100, 2006

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

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

[7] C. W. Wu and G. R. Thompson, "Digital watermarking and steganography via overlays of halftone images," *Proc. SPIE* , Vol. 5561, pp. 152-163, 2004.

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

[9] K. Yamada, M. Minoh and T. Sakai, "Evaluation method of the quality of pseudo continuous tone images," *Journal of IIEEJ*, pp. 72-82, 1987 (in Japanese).