Visual Secret Sharing by Speckle Pattern Illumination

Katsuhiro Uno*, Hoang H. T. Dung*

*Graduate School of Science and Engineering, Ibaraki University, Nakanarusawa, Hitachi, Ibaraki 316-8511, Japan

*Corresponding Author: k-uno@mx.ibaraki.ac.jp

Abstract

We used for the first time the speckle pattern created by the scattered laser beam from rough surfaces in order to perform the visual secret sharing, which is alternative material for random grid pattern. Segmentation and binarization of the speckle pattern was performed for making one share embedding secret image. Reconstruction of the secret image was successfully achieved by the product between the share and the original speckle pattern.

Keywords: visual secret sharing, speckle, random grid.

1. Introduction

The visual secret sharing or the visual cryptography was first proposed by Naor and Shamir (1). They divided each pixels of the secret image into k's shares subdivided into subpixels along with the code book. Each shares appear meaningless patterns. The secret image can be seen only in the case of stacking all the shares together without any computation. The pixel size expansion was inevitable for creating the share because of translating one pixel into several subpixel matrices.

In 1987, Kafri and Keren first used the random grid for encryption of the secret (2). They used the random grid that consists of randomly distributed black and white pixels as a first share and generated the second share by calculation between the random grid and the secret image. They needed no pixel expansion in the encryption process. This non-pixel expansion method using the random grid was progressed by Shyu (3,4).

All methods as mentioned above require transparent media for reconstructing the secret image, because stacking shares was necessary. In this paper, we propose to use the speckle pattern that was created by the laser scattering with random media as a random grid. We created the second share by calculation between the secret image and the laser speckle pattern. The proposed method can recover the secret image when illuminating the share by the laser speckle pattern same as the encryption process. It means that the proposed method does not need any transparent object.

2. Theoretical background

2.1 Random grid method

There is a random grid method as one of the technique to create a share in the secret image sharing scheme. This method have treated only black and white binary images as secret images as shown in Fig. 1.

(1) Encryption

First, the random grid method requires a random pattern when you create a share to embed the secret image. The random pattern is a grid of randomly distributed black and white pixels as shown in Fig. 2. This random pattern becomes the first piece of a share S1.

A secondary share S2 is created in accordance with Fig. 3. Reading pixels of the secret image Sec[x, y] one by one, in the case of a white pixel, the share S2[x, y] is set to the same pixel color as the random pattern S1[x, y]. In the case of black pixels, the pixel of the share S2[x, y] is

Fig. 1 Secret image

Fig. 2 Random pattern S1

Fig. 3 Reading pixels of the secret image Sec[x, y] one by one, in the case of a white pixel, the share S2[x, y] is set to the same pixel color as the random pattern S1[x, y]. In the case of black pixels, the pixel of the share S2[x, y] is...
obtained by reversing the random pattern $S_1[x, y]$. As a result, the share $S_2$ was obtained from the random grid as shown in Fig. 4.

Assigning a value "1" to the white pixel and a value "0" to the black pixel, Fig. 3 is translated into the truth table of Table 1. From Table 1, we can see that the scheme is the negation of exclusive OR (XOR) operation of the secret image and a random pattern as,

$$S_2 = \overline{Sec} \oplus S_1. \quad (1)$$

(2) Decryption

Superimposing the share $S_2$ (Fig. 4) on the random pattern $S_1$ (Fig. 2), decoding result (Fig. 5) is obtained. We can recognize the secret image from the decoded image.

Following to Fig. 6, setting the values of the white pixels to “1” and the values of the black pixels to “0”, a truth table Table 2 is obtained. From Table 2, the decoded image is the result of product operation of random patterns and share explained as,

$$\text{decoded image} = S_1 \cdot S_2. \quad (2)$$

(3) Conditions of random pattern

To prevent guessing the secret image from the share, there is a condition in a random pattern that we use. It is that the percentage of white pixels against black pixels is 50%. If the number of white pixels are more (less) than the black pixels as shown in Fig. 7, we can easily guess the secret image from the share.

Following to Fig. 6, setting the values of the white pixels to “1” and the values of the black pixels to “0”, a truth table Table 2 is obtained. From Table 2, the decoded image is the result of product operation of random patterns and share explained as,

$$\text{decoded image} = S_1 \cdot S_2. \quad (2)$$

(3) Conditions of random pattern

To prevent guessing the secret image from the share, there is a condition in a random pattern that we use. It is that the percentage of white pixels against black pixels is 50%. If the number of white pixels are more (less) than the black pixels as shown in Fig. 7, we can easily guess the secret image from the share.

2.2 Speckle pattern

When the coherent light such as a laser light irradiates a rough surface such as a paper and a ground glass, we can observe the speckled pattern in the reflected and transmitted light. Such mottled pattern is called speckle pattern or simply speckles. Moreover a phenomenon making such patterns is called a speckle phenomenon. This phenomenon is a random interference phenomenon caused by scattered
waves randomly overlapping at an observation point from each point of the rough object.

2.2.1 Formation of speckle pattern

The geometry of speckle formation is shown in Fig. 8. A sample surface has sufficiently large irregularities in comparison with the wavelength of light. Upon irradiation with laser light to the rough surface located on the front focal plane of the lens, the light field on the observation plane at the back focal plane consists of many scattered plane waves emanated from different locations of the rough surface. Since the phases in which these light waves have are random as reflecting the irregularities of the uneven rough surface, the spatial intensity distribution of light also results in random as a result of interference.

\[ R_f(x_1, y_1; x_2, y_2) = \left\langle I(x_1, y_1)I(x_2, y_2) \right\rangle. \] (4)

The mutual intensity is defined as

\[ J_d(x_1, y_1; x_2, y_2) = \left\langle A(x_1, y_1)A^*(x_2, y_2) \right\rangle. \] (5)

From Fig. 8, a basic relationship between the field \( a(\xi, \eta) \) at the scattering surface and the field \( A(x, y) \) on the observation plane is a principle of Huygens Fresnel, and it is represented by Fraunhofer approximation as

\[ A(x, y) = \frac{1}{i \lambda f} \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} a(\xi, \eta) \exp \left[ \frac{2\pi i}{\lambda f} (x\xi + y\eta) \right] d\xi d\eta. \] (6)

The mutual intensity of the observation plane is related to the mutual intensity on the scattering surface as follows,

\[ J_d(x_1, y_1; x_2, y_2) = \frac{1}{i \lambda f} \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} J_u(\xi_1, \eta_1; \xi_2, \eta_2) \times \exp \left[ \frac{2\pi i}{\lambda f} (x_1\xi_1 + y_1\eta_1 - x_2\xi_2 - y_2\eta_2) \right] d\xi_1 d\eta_1. \] (7)

The mutual intensity just in front of the scattering surface is described by

\[ J_u(\xi_1, \eta_1; \xi_2, \eta_2) = \left\langle a(\xi_1, \eta_1)a^*(\xi_2, \eta_2) \right\rangle \times P(\xi_1, \eta_1)P'(\xi_2, \eta_2)\mu(\Delta\xi, \Delta\eta), \] (8)

where \( P \) represents an illuminating function incident on the surface and \( \mu \) is the complex coherence factor, which only depends on \( \Delta\xi = \xi_1 - \xi_2, \Delta\eta = \eta_1 - \eta_2 \).

When the illuminating function is much broader than the width of the complex coherent factor, the mutual intensity becomes

\[ J_d(x_1, y_1; x_2, y_2) = \frac{k}{\lambda f} \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} \mu(\Delta\xi, \Delta\eta) \exp \left[ \frac{2\pi i}{\lambda f} (x_1\Delta\xi + y_1\Delta\eta) \right] d\Delta\xi d\Delta\eta. \] (9)

Within the small slope condition of the surface, the reflected amplitude in the \((\xi, \eta)\) plane is related to the height function as follows,

\[ a(\xi, \eta) = aP(\xi, \eta) \exp \left[ \frac{2\pi i}{\lambda} (1 + \cos \beta) h(\xi, \eta) \right]. \] (10)

If the assumption is made that the surface height perturbations are Gaussian random variables and also obeys height correlation function of the Gaussian form, the complex coherence factor is derived as

\[ \mu(\Delta\xi, \Delta\eta) = \exp \left[ -\sigma^2 \left[ 1 - \rho(\Delta\xi, \Delta\eta) \right] \right], \] (11)
where $\rho_h$ is the normalized correlation function of the scattering surface and $\sigma_\theta$ represents the standard deviation of the scattering phase, which is related to the standard deviation of the height function $\sigma_h$ as follows:

$$
\sigma_\theta^2 = \left[ \frac{2\pi}{\lambda} (1 + \cos \beta) \right] \sigma_h^2.
$$

(12)

Equation (9) describes that the average speckle size is determined only by the Fourier transform of square modulus of the illuminating function, which is narrow function since the illuminating function is coarse profile. The wider illumination is, the smaller grain size of the speckle is. The complex coherence factor on the scattering surface is short enough, the average intensity of the speckle pattern can be considered to be uniform.

Assuming the Gaussian form of the normalized correlation function of the surface height, $\mu_h$ becomes,

$$
\mu_h'(r) = \exp \left[ \frac{1}{2} \sigma_h^2 \left( 1 - e^{-r^2/\sigma_h^2} \right) \right] \frac{1 - \exp(-\sigma_h^2)}{1 - \exp(-2\sigma_h^2)},
$$

(13)

after subtracting the specular component and renormalizing at the origin, where $r = \sqrt{A^2 + \eta^2}$. The coherence area defined by $A_c = 2\pi \int_0^\infty r \mu_h'(r) dr$ becomes(7),

$$
A_c = \frac{\pi \sigma_h^2}{1 - e^{-\sigma_h^2}} \left[ E\left( \sigma_h^2 \right) - E - \ln(\sigma_h^2) \right],
$$

(14)

where $E(x)$ represents the exponential integral and $E$ is Euler’s constant. The illuminating area is defined by

$$
A_i = \sum_{\xi,\eta} P(\xi,\eta) d\xi d\eta
$$

(15)

under the assumption of real valued illuminating function. The ratio of $A_i$ to $A_c$ describes the number of independent scattering waves within the illuminating portion, which is represented by

$$
N = \frac{A_i}{A_c} = \frac{N_0(e^{\alpha^2} - 1)}{E\left( \sigma_h^2 \right) - E - \ln(\sigma_h^2)},
$$

(16)

where the number of independent scatterers within the illuminating portion is described as $N_0 = A_i/(\sigma_h^2)$. After some cumbersome calculations, the speckle contrast defined as the ratio of the standard deviation to the average intensity is given by(7)

$$
C = \frac{\sigma_c}{T} = \frac{\sqrt{8(N-1)N-1 + \cosh(\sigma_h^2) \sinh(\sigma_h^2/2)}}{N(N-1+e^{\sigma_h^2})},
$$

(17)

where we assume that the all scattering waves within the illuminating portion have unity amplitude and their phases are Gaussian random variables with zero mean.

### 3. Experimental

An experimental setup is shown in Fig. 9. The laser beam was passed through an aperture with 6 mm diameter and irradiated on the sample. The scattered beam was collected at the plano-convex lens, which was on the front focal plane away from the sample. The speckle observed in the ground glass was acquired by a CCD camera (IK-HR2D, TOSHIBA), which focused on the frosted glass by a camera lens (JK L09 HF, TOSHIBA). A copy paper (64846-B, MITSUBISHI) was used as the sample. The captured speckle pattern is shown in Fig. 10. Trimming away peripheral image with low brightness, a random pattern which was the same size with confidential image was obtained shown in Fig. 11 (a). The brightness histogram of the random pattern is shown in Fig. 11 (b). The average intensity and the standard deviation of the random pattern was $\bar{I} = 28.9$ and $\sigma_i = 4.5$, so that the contrast was $C=0.16$. The reason for such a small contrast value may come from the resolution limit of CCD camera.

We first made a confidential image binary same as Fig. 1. Then, we used fifty percent threshold to make random pattern binary, which was necessary condition for confidential image invisible. Unfortunately, the average brightness of the speckle was not uniform over the entire image. The central portion was brighter than the peripheral image. Therefore, using only one threshold value caused violation of the fifty percent condition locally. To avoid this problem, we divided the random pattern into six parts as shown in Fig. 12 and set the fifty percent threshold individually. Using each threshold values, we assigned "white" to pixels brighter than the thresholds and set "black" to pixels lower than the thresholds. After the individual thresholding, the binarized image parts were joined together to prepare a synthetic random pattern shown in Fig. 13. Negation of exclusive OR (XOR) operation between the binary secret image and the synthetic random
pattern was performed to create a share shown in Fig. 14.

Fig. 9 Experimental setup

Fig. 10 Speckle pattern

(a) Random pattern truncated from the speckle pattern
(b) The histogram of the random pattern

Fig. 11 Random pattern creation form the speckle pattern

Fig. 12 Six segments of random pattern

Fig. 13 Synthetic random pattern

Fig. 14 Share created from Fig. 13

4. Results

From eq. (2), decryption was performed by the product operation between the original random pattern in Fig. 11(a) and the share in Fig. 14. The results are shown in Fig. 15(a). The image which contrast and brightness were adjusted is also shown in Fig. 15(b) for clarity.
5. Conclusion

In this paper, we used a speckle pattern to make the visual secret sharing and carried out the image decoding by using the speckle pattern. The share can be made by the binary speckle pattern, and it was able to decode. Even in the luminance non-uniformity in the speckle pattern, by adjusting the binary level where the image was divided into small image area, it was possible to create a share that cannot infer the secret image. In spite of binary image of the share made from a binarized random pattern, it was able to be decrypted by the original random pattern (not binarized). Thereby, we consider that the secret image is decodable by irradiating directly the speckle pattern into the share. We have now been performing an experiment to decode the confidential image by irradiating the speckle pattern directly to the share.

Acknowledgment

This study has been financially supported by the grants-in-aid for scientific research of Japan society for the promotion of science.

References