Journal of the Institute of Industrial Applications Engineers Vol.4, No.1, pp.26–32, (2016.1.25)
DOI: 10.12792/JIIAE.4.26 Online edition: ISSN 2187-8811 Print edition: ISSN 2188-1758

Paper

Visual Cryptography by Speckle Pattern Illumination

Katsuhiro Uno*† Member, Hoan Hoa Tien Dung† Non-member

(Received October 9, 2015, revised December 24, 2015)

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 (visual cryptography), 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 (visual cryptography), 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 share appears meaningless pattern. 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 from 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.

Figure 1: Secret image.

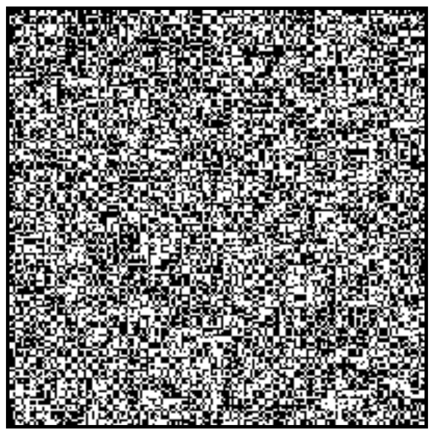


Figure 2: Random pattern (share S1).

2.1.1 Encryption step

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].

* Corresponding: katsuhiro.uno.catsin3@vc.ibaraki.ac.jp
† Ibaraki University
4-12-1 Nakanarusawa, Hitachi, Ibaraki, Japan 316-8511

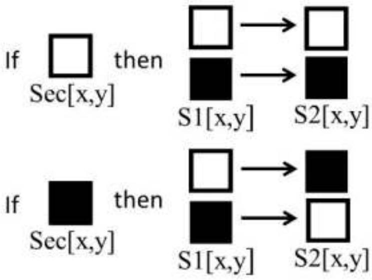


Figure 3: Encryption scheme.

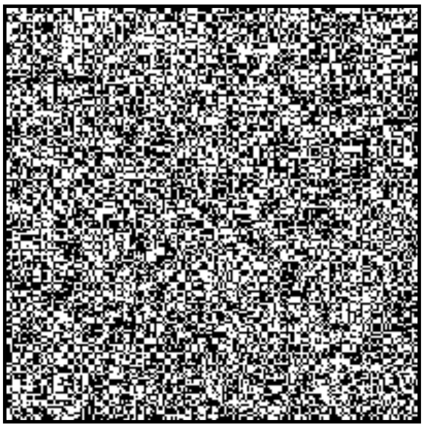


Figure 4: Share S2.

Table 1: Truth table for encryption.

Sec[x,y]	S1[x,y]	S2[x,y]
0	0	1
0	1	0
1	0	0
1	1	1

In the case of black pixels, the pixel of the share S2[x, y] is obtained by reversing the random pattern S1[x, y]. As a result, the share S2 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 as Table 1. From this table, we can see that the scheme is the negation of exclusive OR (XOR) operation of the secret image and a random pattern as,

$$S2 = \overline{Sec \oplus S1} \tag{1}$$

2.1.2 Decryption Superimposing the share S2 (Fig. 4) on the random pattern S1 (Fig. 2), decoding result shown in 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 as Table 2 is obtained. From Table 2, the decoded image is the result of product operation of random patterns and share explained as,

$$\text{decoded image} = S1 \cdot S2 \tag{2}$$

Figure 5: Decoded image.

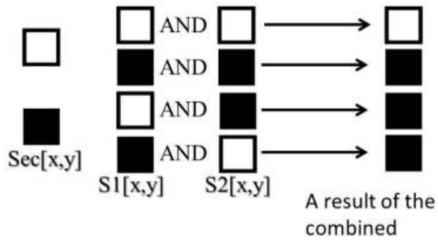


Figure 6: Decryption scheme.

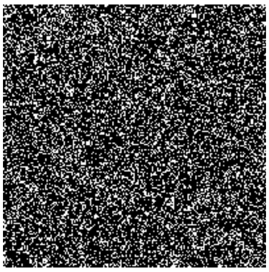
Table 2: Truth table for decryption.

S1[x,y]	S2[x,y]	combined result
0	0	0
0	1	0
1	0	0
1	1	1

2.1.3 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.

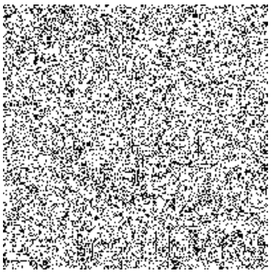
2.2 Speckle pattern When the coherent light such as a laser light irradiates a rough surface such as a paper and a ground glass, we can observe the speckled pattern in the reflected and transmitted light. We call it a "speckle pattern" or simply "speckle". This phenomenon is a random interference at an observation point caused by randomly overlapping scattered waves 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 point at the back focal plane consists of many scattered plane waves emanated from different locations of the rough surface. Since the phases in which



(a) Dark random pattern (white pixel less than black).

(b) Encrypted image from (a)



(c) Bright random pattern (white pixel more than black).

(d) Encrypted image from (c)

Figure 7: Pixel brightness condition for image encryption.

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.

2.2.2 Statistical properties of speckle In Fig. 8, the complex amplitude just reflected from the rough surface is denoted by $\alpha(\xi, \eta)$ and the amplitude in the observation plane is described by $A(x, y)$. The autocorrelation function of the intensity distribution $I(x, y) = |A(x, y)|^2$ at (x, y) plane is,

$$R_I(x_1, y_1; x_2, y_2) = \langle I(x_1, y_1) I(x_2, y_2)\rangle \tag{3}$$

where $\langle ... \rangle$ denotes the ensemble average. To calculate the autocorrelation function, we assume that the coarse rough surface is circular complex Gaussian random variables. The autocorrelation function of the intensity is reduced to a function in terms of the mutual intensity explained as,

$$\begin{aligned} R_I(x_1, y_1; x_2, y_2) = &\langle I(x_1, y_1)\rangle\langle I(x_2, y_2)\rangle \\ &+ |J_A(x_1, y_1; x_2, y_2)|^2 \end{aligned} \tag{4}$$

The mutual intensity is defined as

$$J_A(x_1, y_1; x_2, y_2) = \langle A(x_1, y_1) A^*(x_2, y_2)\rangle \tag{5}$$

From Fig. 8, a basic relationship between the field $\alpha(\xi, \eta)$ 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 [5],

$$A(x, y) = \frac{1}{\lambda f} \iint_{-\infty}^{+\infty} \alpha(\xi, \eta) \exp\left[\frac{i2\pi}{\lambda f}(x\xi + y\eta)\right] d\xi d\eta \tag{6}$$

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

$$\begin{aligned} J_A(x_1, y_1; x_2, y_2) = &\frac{1}{\lambda^2 f^2} \iiiint_{-\infty}^{\infty} J_\alpha(\xi_1, \eta_1; \xi_2, \eta_2) \\ &\times \exp\left[i\frac{2\pi}{\lambda f}(x_1\xi_1 + y_1\eta_1 - x_2\xi_2 - y_2\eta_2)\right] d\xi_1 d\eta_1 d\xi_2 d\eta_2 \end{aligned} \tag{7}$$

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

$$\begin{aligned} J_\alpha(\xi_1, \eta_1; \xi_2, \eta_2) &= \langle \alpha(\xi_1, \eta_1)\alpha^*(\xi_2, \eta_2)\rangle \\ &= \kappa P(\xi_1, \eta_1) P^*(\xi_2, \eta_2) \mu_\alpha(\Delta\xi, \Delta\eta) \end{aligned} \tag{8}$$

where P represents an illuminating function incident on the surface and μ_α 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 coherence factor, the mutual intensity becomes [6],

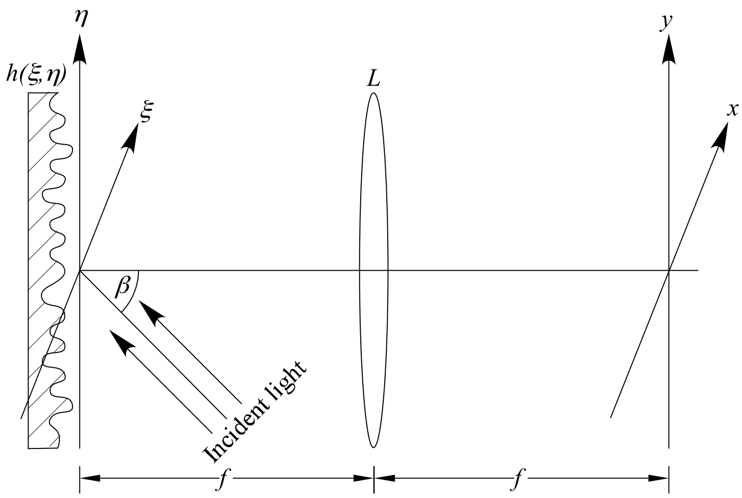


Figure 8: Geometry of speckle formation.

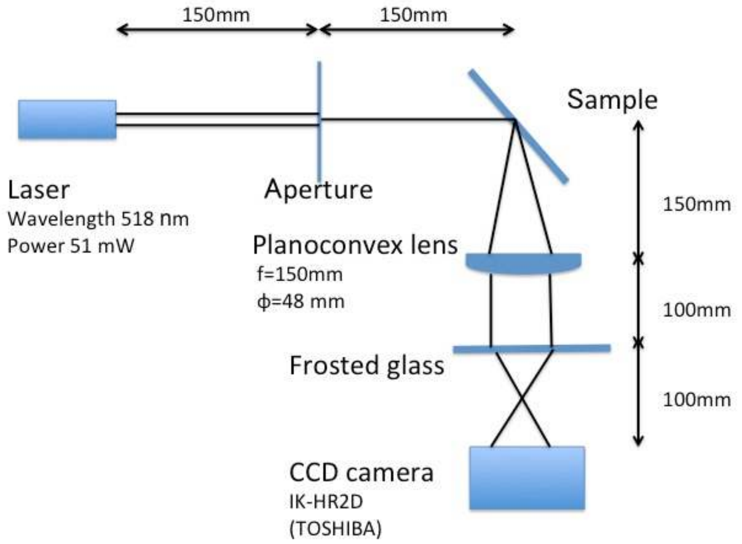


Figure 9: Experimental setup.

$$J_A(x_1, y_1; x_2, y_2) = \frac{\kappa}{\lambda^2 f^2} \iint_{-\infty}^{\infty} |P(\xi_1, \eta_1)|^2 \exp\left[i\frac{2\pi}{\lambda f}(\Delta x\xi_1 + \Delta y\eta)\right] d\xi_1 d\eta_1 \times \iint_{-\infty}^{\infty} \mu_\alpha(\Delta\xi, \Delta\eta) \exp\left[i\frac{2\pi}{\lambda f}(x_2\Delta\xi + y_2\Delta\eta)\right] d\Delta\xi d\Delta\eta \quad (9)$$

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

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

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 coherent factor is derived as [6],

$$\mu_\alpha(\Delta\xi, \Delta\eta) = \exp\{-\sigma_\theta^2[1 - \rho_h(\Delta\xi, \Delta\eta)]\} \quad (11)$$

where ρ_h is the normalized correlation function of the scattering surface and σ_θ represents the standard deviation of the scattering phase, which is related to the standard deviation of the height function σ_h as follows:

$$\sigma_\theta^2 = \left[\frac{2\pi}{\lambda}(1 + \cos\beta)\right]^2 \sigma_h^2 \quad (12)$$

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 determines the average intensity over the whole speckle pattern. When the correlation length of 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, μ_α becomes,

$$\mu_\alpha'(r) = \frac{\exp\{-\sigma_\theta^2|1 - e^{-(r/r_c)^2}|\} - \exp(-\sigma_\theta^2)}{1 - \exp(-\sigma_\theta^2)} \quad (13)$$

after subtracting the specular component and renormalization at the origin, where $r = \sqrt{\Delta\xi^2 + \Delta\eta^2}$. The coherence area defined by $A_\alpha = 2\pi \int_0^\infty r\mu_\alpha'(r)dr$ becomes [7],

$$A_\alpha = \frac{\pi r_c^2 e^{-\sigma_\theta^2}}{1 - e^{-\sigma_\theta^2}}\left[\mathrm{Ei}(\sigma_\theta^2) - E - \ln(\sigma_\theta^2)\right] \quad (14)$$

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

$$A_p = \frac{\iint P(\xi, \eta)d\xi d\eta}{P(0, 0)} \quad (15)$$

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

$$N = \frac{A_p}{A_\alpha} = \frac{N_0(e^{\sigma_\theta^2} - 1)}{\mathrm{Ei}(\sigma_\theta^2) - E - \ln(\sigma_\theta^2)} \quad (16)$$

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

$$C = \frac{\sigma_I}{\bar{I}} = \sqrt{\frac{8(N-1)[N - 1 + \cosh(\sigma_\theta^2)]\sinh^2(\sigma_\theta^2/2)}{N(N - 1 + e^{\sigma_\theta^2})^2}} \quad (17)$$

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.

Figure 10: Speckle pattern.

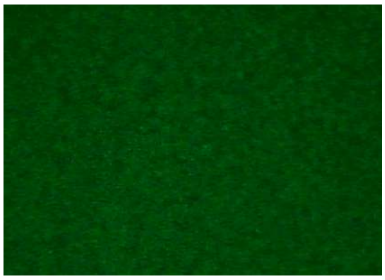
3. Experiments

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.

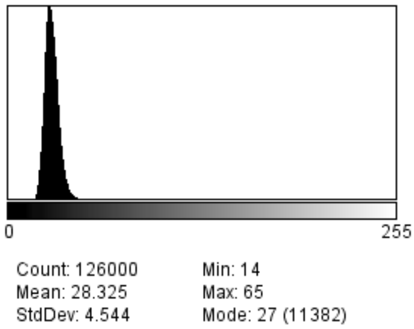
3.1 Unadjusted share We first made a confidential binary image same as Fig. 1. Negation of exclusive OR (XOR) operation between the binary secret image and the binary random pattern (Fig. 12(a)) that was made by binarizing the random pattern with unadjusted threshold was performed to create a share shown in Fig. 12(b). In this share, we can see a part of the secret image. The reason is that the percentage of white pixels against black pixels is not 50%.

3.2 Adjusted share We used fifty percent threshold to make binary random pattern, which was necessary condition for confidential image invisible. Using each threshold values, we assigned "white" to pixels brighter than the thresholds and set "black" to pixels lower than the thresholds (Fig. 13(a)). Negation of exclusive OR (XOR) operation between the binary secret image and the binary random pattern that was made by binarizing the random pattern with adjusted threshold was performed to create a share shown in Fig. 13(b).

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

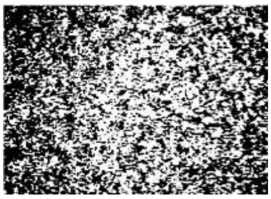


(a) Random pattern truncated from Fig. 10.

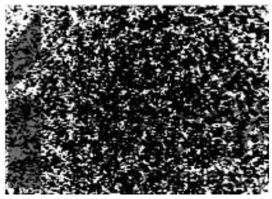


(b) The histogram of the random pattern.

Figure 11: Random pattern created from the speckle pattern.

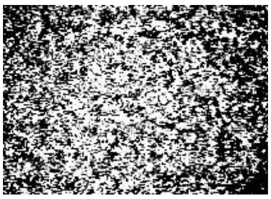


(a) Unadjusted binary random pattern.

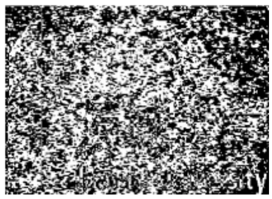


(b) Share made from Fig. 12(a).

Figure 12: Share made from the unadjusted binary random pattern.



(a) Adjusted binary random pattern.



(b) Share made from Fig. 13(a).

Figure 13: Share made from the adjusted binary random pattern.

value caused violation of the fifty percent condition locally, so that we can guess information from the share.

3.3 Synthetic random pattern To overcome the previous problem, we divided the random pattern into six parts as shown in Fig. 14 and set the fifty percent threshold individually. After the individual thresholding, the binarized image parts were joined together to prepare a synthetic random pattern shown in Fig. 15. Negation of exclusive OR

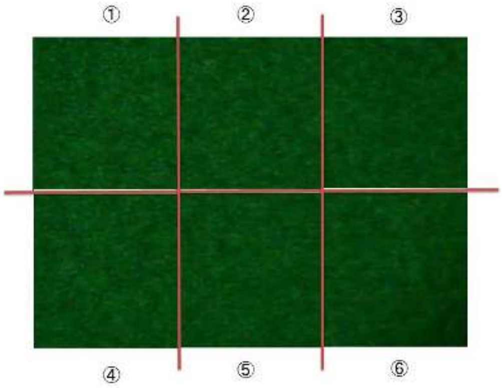


Figure 14: Random pattern divided into six segments.

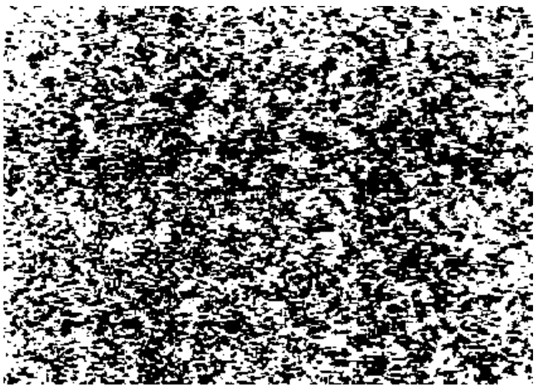


Figure 15: Synthetic random pattern.

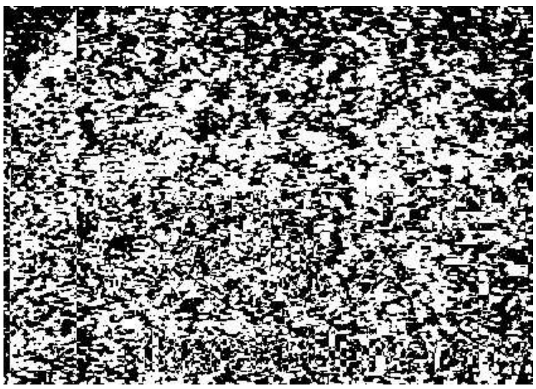


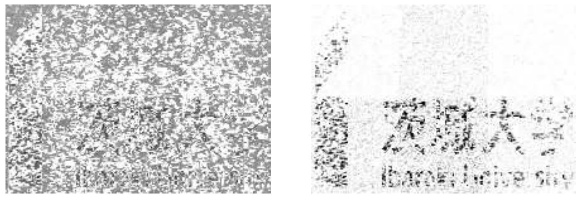
Figure 16: Share from the synthetic random pattern.

(XOR) operation between the binary secret image and the synthetic random pattern was performed to create a share shown in Fig. 16.

4. Results

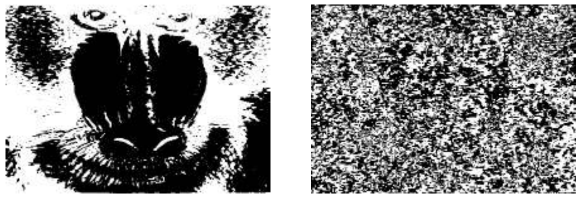
From eq. 2, decryption was performed by the product operation between the original random pattern in Fig. 11(a) and the share in Fig 16. The results are shown in Fig. 17(a). The image which contrast and brightness were adjusted is also shown in Fig. 17(b) for clarity.

We also tried to make a share of another image (baboon) by using the synthetic random pattern. The original image was expanded to fit the random pattern and was binarized

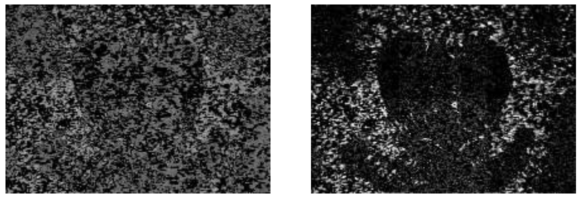


(a) Decoded image(raw data). (b) Decoded image (Contrast enhancement)

Figure 17: Decoding result of the secret image.



(a) Binary baboon image). (b) Share from pattern random synthetic



(c) Decoded image (raw data). (d) Decoded image (Contrast enhancement)

Figure 18: Share and decrypted result of baboon image.

(Fig. 18(a)). We narrowly could hide the secret image in the share (Fig. 18(b)). However, there is something non-uniform texture in the pattern. The share was multiplied by the synthetic random pattern and the original speckle pattern for decoding. We can guess the secret image from decoded image, but not clearly (Fig. 18(c)). We also show the same image of which contrast was enhanced as shown in Fig. 18(d).

Comparing the decoded logo image (Fig. 17(b)) with that of the baboon image (Fig. 18(d)), the decoded logo image looks clearer than the baboon image. Because the baboon image has finer structure than the logo image, the decoding error noise conceals the fine structure of decrypted image.

5. Conclusions

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 also made a secret share of the image having finer structure. Unfortunately, the fine structure was not clearly decrypted due to decrypting error noise. 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

[1] M. Naor, and A. Shamir, "Visual cryptography", *Advances in Cryptology - EUROCRYPT'94, Lecture Notes in Computer Science*, Vol.950, pp.1-12, 1995.

[2] O. Kafri, and E. Keren, "Encryption of pictures and shapes by random grids", *Optics Letters*, Vol.12, No.6, pp.377-379, 1987.

[3] S. J. Shyu, "Image encryption by random grids", *Pattern Recognition*, Vol.40, No.3, pp.1014-1031, 2007.

[4] S. J. Shyu, "Image encryption by multiple random grids", *Pattern Recognition*, Vol.42, No.7, pp.1582-1596, 2009.

[5] J. W. Goodman, "Introduction to Fourier Optics", *Mc-Grawhill, 2nd. ed.*, Chap.5, pp.96-120, 1996.

[6] J. W. Goodman, "Statistical properties of laser speckle patterns in Laser speckle and related phenomena 2nd enlarged ed.", *Springer-Verlag*, pp.9-75, 1984.

[7] J. W. Goodman "Speckle Phenomena in Optics : Theory and Applications", *Roberts & Company*, Chap.4, pp.59-139, 2007.

Katsuhiro Uno (Member) was born in Hokkaido, Japan, on August 19, 1967. He received a Ph.D. degree in engineers from Hokkaido University in 1995, and is presently an assistant professor at Ibaraki University. He has worked on image processing. He is member of IIAE.

Hoan Hoa Tien Dung (Non-member) was born in Hanoi, Vietnam, on February 11, 1991. She is a student of graduate school of Science and Engineering of Ibaraki University. She is now studying the visual secret sharing and holography.