Visual Cryptography Using Interference Color of High-Order Retarder Films

Kenji Harada*, Takenobu Yamaguchi, Tomohiro Tsuchida, and Daisuke Sakai

Department of Computer Science, Kitami Institute of Technology, Kitami, Hokkaido 090-8507, Japan

Visual cryptography is known as a method of sharing a secret image through several encrypted images. Conventional visual cryptography can display only monochrome images. We develop a multicolor visual encryption technique using the interference color of high-order retarder films. The encrypted films are composed of a polarizing film and retarder films. Retarder films exhibit an interference color upon sandwiching between two polarizing films. A prototype of a visual cryptography device using interference color is developed. Eight colors are represented by combining an encrypted image and a decoding mask composed of retarder films with various retardations.

*E-mail: haraken@cs.kitami-it.ac.jp

1. Introduction

In recent years, various optical cryptography schemes and devices have been proposed for information security.$^{1\text{-}7)}$ Visual cryptography is known as a method of sharing a secret image through several encrypted images. The basic algorithm of visual cryptography is reported by Naor and Shamir$^{8)}$ and Kafri and Keren.$^{9)}$ This algorithm is considered to be very effective because no information about the secret image leaks from each separated key image. In conventional visual cryptography, each key image (share) is a random distribution of black-and-white subpixels. When shares are copied on transparencies, the secret image can be observed by stacking them.

Many types of visual cryptography have been proposed.$^{8\text{-}19)}$ Conventional visual cryptography reduces the image quality of decoded images because the encryption is based on spatial coding that requires multiple subpixels to modulate light intensity. A polarization encoding technique solves this problem. This encoding technique enables the encryption of each pixel in a secret image into a corresponding single pixel in shares.$^{1\text{-}3,\ 12)}$ A simple polarization encoding technique without optical systems is reported by Imagawa et al.$^{13)}$ A visual encryption device using high-order retarder films is also reported by Kowa et al.$^{14)}$ These techniques enable the display of only a binary image. In conventional visual cryptography, the image is encoded into a black and white binary pattern. The decoded image can only be displayed as a black and white binary image. Improved visual cryptography for gray-level images is reported by Blundo et al.$^{15)}$ Visual cryptography for color images is also reported.$^{16\text{-}19)}$ A color visual cryptography technique is useful for various applications, but multiple color subpixels are needed. For example, to represent color images with two shares, each pixel is composed of at least one red, one green, and one blue subpixel. In order to represent black, the minimum number of subpixels is six, where each pixel is composed of one red, one green, one blue, and three black subpixels.[16)] These color subpixels reduce the image quality of secret images. This is the problem of the traditional color visual cryptography.

To solve the problem, we propose a new type of color visual cryptography. Our system cannot display the gray-level images, but multiple color subpixels are not needed to modulate color. Our encoding technique enables the encryption of each pixel in a secret image into a corresponding single pixel in shares. We can display red, green and blue in only single pixel in shares. So image quality is not reduced by stacking shares. This is the advantage of our proposed system. In contrast with other methods, ours uses no absorption of color ink or color filters. We use the interference color of high-order retarder films. Interference colors are an important source of information for the microscopic observation of birefringent materials.[20)] Interference colors are also used as educational tools.[21-22)] Michel-Levy's color chart describes interference color and has been widely used for determining retardation from an observed interference color.

Our system is composed of transparent retarder films and polarizers. Each color is controlled by the phase retardation of retarder films. We perform polarization decoding using stacked films. Encrypted films are portable, and their manual alignment is easy because the total number of pixels is small. We describe conventional and extended visual cryptography schemes using polarization films in Sect. 2. In Sect. 3, we describe the calculation of interference color. In Sect. 4, we present the design method of visual cryptography using interference color.

2. Principles of Visual Cryptography Using Polarization Films

In this section, principles of visual cryptography using polarization films are described. We consider that a secret image is shared through two key images. Figure 1 shows a conventional polarization-based binary visual cryptography technique. Two key images (key images 1 and 2) are inserted between two crossed polarizers. Each pixel of the key images is composed or not composed of λ/2 retarder films. A λ/2 retarder film rotates to a polarization angle of 90° when the angle between the transmission axis of a polarizer and the retarder axis of a λ/2 retarder film is 45°. Therefore, the overlaid result is bright when one λ/2 retarder film is placed between two polarizers. On the other hand, the overlaid result is dark when two λ/2 retarder films are placed between two polarizers. The result is also the same when no λ/2 retarder film is placed between two polarizers. In this manner, there are four possible combinations, and no decoded result leaks any pixel of one key image.

The encryption is performed within one pixel. Thus, visual cryptography using a polarization encoding technique does not reduce the image quality of the decoded result. We propose an extended visual cryptography scheme using high-order retarder films. Retarder films exhibit a wavelength dependence of transmission light intensity. The effect of such a dependence can be neglected in low-order retarder films. High-order retarder films exhibit a large wavelength dependence of transmittance, and these films also exhibit interference color. We control the interference color, and apply it to multicolor visual cryptography. The calculation of interference color is shown in the next section.

3. Calculation of Interference Color

Visible color is completely specified by the trichromatic coordinates X, Y, and Z adopted by the Commission Internationale de l'Éclairage (CIE).[23,24] When the birefringence dispersion is negligible, the tristimulus X, Y, and Z values of a specific interference color with crossed polarizers are given by

$$X = K\int_{380}^{780} S(\lambda)\bar{x}(\lambda)\sin^2\left(\frac{\pi R}{\lambda}\right)d\lambda \quad , (1)$$

$$Y = K\int_{380}^{780} S(\lambda)\bar{y}(\lambda)\sin^2\left(\frac{\pi R}{\lambda}\right)d\lambda \quad , (2)$$

$$Z = K\int_{380}^{780} S(\lambda)\bar{z}(\lambda)\sin^2\left(\frac{\pi R}{\lambda}\right)d\lambda \quad , (3)$$

$$K = \frac{100}{\int_{380}^{780} S(\lambda)\bar{y}(\lambda)d\lambda}, \quad (4)$$

where $S(\lambda)$ is the spectral distribution of the illuminant, $\bar{x}$, $\bar{y}$, and $\bar{z}$ are the tristimulus values of the standard observer, R is the retardation, and λ is the wavelength. The XYZ colorimetric system is used to express all visible colors using only positive values, and the Y value means luminance. In the XYZ colorimetric system, it is difficult to determine the relationship between X, Y, and Z values, and color. The xyY colorimetric system is useful for determining the color directly from the x, y, and Y values. The x and y values are defined by

$$x = \frac{X}{X+Y+Z}, \quad (5)$$

$$y = \frac{Y}{X+Y+Z}. \quad (6)$$

Figure 2 shows the calculated chromaticity curves of interference color from the CIE standard illumination D65. The phase retardation of the retarder films is calculated from 0 to 2200 nm. The displayed chroma saturation of the interference color is low, but various colors can be displayed by changing the phase retardation of the retarder films.

This interference color can be converted into the CIE RGB space from the CIE XYZ space using the following relationship:

$$\begin{pmatrix} R \\ G \\ B \end{pmatrix} = \begin{pmatrix} 0.4184 & -0.1586 & -0.0828 \\ -0.0912 & 0.2524 & 0.0157 \\ -0.0009 & -0.0026 & 0.1786 \end{pmatrix} \begin{pmatrix} X \\ Y \\ Z \end{pmatrix}. \qquad (7)$$

The tristimulus R, G, and B values calculated from Eq. (7) can become negative since the gamut of the CIE RGB space does not fully cover the loci of the interference color converted from the CIE XYZ space. The RGB color model cannot display a negative tristimulus value. In our calculation, a negative R, G, or B value is converted to zero. Figure 3 shows the calculated interference color chart using the CIE standard illumination D65. We used approximation in the calculation of the RGB interference color chart, and no dispersion of birefringence was considered. The displayed color also depends on the characteristics of the color monitor. Thus, the color chart is not highly precise, but we can easily determine the approximate interference color from this chart.20)

4. Design of Visual Cryptography Using Interference Color

Various colors can be displayed by changing the phase retardation of the retarder films, and the colors can be changed by adding or subtracting the phase retardations. In this section, we show the design method of visual cryptography using interference color. Figure 4 shows a simple example of a design algorithm of visual cryptography using interference color. We consider that each pixel of the secret image is composed or not composed of 840 nm retarder films, and that the angle between the transmission axis of a polarizer and the retarder axis of a retarder film is ±45°, as shown in Fig. 4(a). The color of the overlaid result is yellow or black. The color can be determined using the interference color chart shown in Fig. 3. The same interference color is obtained when the angle between the transmission axis of a polarizer and the retarder axis of a retarder film is +45° or -45°. The secret image is shared through two key images (key images 1 and 2). There are various combinations used to design key images. Phase retardation is calculated by adding the phase retardation values of each pixel. Figure 4(b) shows one possible combination of key images. The phase retardations of the upper left pixels of two key images are 420 nm, and the total phase retardation is 840 nm. The phase retardations of the upper right pixels of two key images are also 420 nm, but the retarder axes are in the orthogonal direction. In this case, phase retardation is canceled, and the total phase retardation becomes 0 nm. In the same manner, the total phase retardation of the lower left pixels is 0 nm.

The lower right pixels of key images show 280 and 1120 nm phase retardations, and the retarder axes are in the orthogonal direction. The total phase retardation is calculated to be 840 nm by subtracting the phase retardations. The secret image cannot be decoded with only one key image. To confirm the color variation of this technique, we designed a model of multicolor visual cryptography, which is shown in Fig. 5. We used two types of retarder film with retardations of 140 and 570 nm. Conventional λ/4 retarder films are used as 140 nm retarder films, and conventional λ retarder films are used as 570 nm retarder films. The wavelength dispersion of the λ/4 retarder films and the λ retarder films is the same; otherwise the difference in wavelength dispersion between these retarder films worsens the accuracy of the displayed color. The image is composed of 8 x 8 pixels, and the pixel size is 12 x 12 mm^2. Retarder films are pasted directly onto a polarizing film. White backlight KLV-7000 (Hakuba) is used to view the image. Figure

5(a) shows the interference color of key image 1 with crossed polarizers. We designed key image 1 such that eight colors (black, white, cyan, red, magenta, green, yellow, and blue) are displayed in the horizontal direction. The phase retardation of each pixel is shown in Fig. 5(b). The phase retardations of the eight colors are 0, 280, 710, 430, 1000, 1280, 850, and 570 nm, respectively. These phase retardations are obtained by stacking two types of retarder film with phase retardations of 140 and 570 nm. For example, the phase retardation of the green pixel is 1280 nm, and the pixel is composed of one 140 nm retarder film and two 570 nm retarder films that are parallel to the retarder axes in phase. Figure 5(c) shows the interference color of key image 2 with crossed polarizers. The phase retardation of each pixel is shown in Fig. 5(d). Key image 2 is designed such that the overlaid image of eight colors is displayed in the vertical direction. The negative retardation value shows that the retarder films of key images 1 and 2 are in the orthogonal direction of the retarder axis in phase. Figure 5(e) shows the overlaid image of key images 1and 2 with crossed polarizers, and Fig. 5(f) shows the total phase retardation of each pixel. All eight color combinations (8 x 8) are demonstrated using interference color without color filters.

Next, we designed a prototype of a multicolor visual cryptography device using interference color. A secret image is composed of 10 x 10 pixels, and the pixel size is 12 x 12 mm^2. The secret image is shared through two key images (key images 1 and 2). Retarder films are pasted directly onto a polarizing film. White backlight, KLV-7000, is used to view the image. Figures 6(a) and 6(b) show the interference colors of key images 1 and 2 with crossed polarizers. A random color dot pattern is observed. The phase retardation of each pixel is designed to be in the range from 0 to 1280 nm. There are various code set combinations with key images 1 and 2. No information is leaked from either key image. Figure 6(c) shows the result of incorrectly overlaying key images 1 and 2 with crossed polarizers. In this case, the direction of the key image is opposite, and no correct image is observed. When a slight shift of the two images exists, we observe the same kind of scrambled color image. Figure 6(d) shows the result of correctly overlaying key images 1 and 2 with crossed polarizers. Multicolor visual cryptography is successfully demonstrated using interference color. The pixel size of the prototype device is large, because we made the device by stacking the films manually. To realize our cryptography system, we can use a cutting plotter to cut the retarder films. There is a trade-off relationship between difficulty of alignment and pixel size. The stacking process is necessary, but manual alignment becomes difficult with small-pixel devices. The most suitable pixel size of our device is about 2 × 2 mm^2.

5. Conclusions

We have produced a multicolor visual encryption technique using the interference color of high-order retarder films. We calculated the interference color and designed a multicolor encryption code set. A prototype of a visual cryptography device using interference color was developed. We need no special optical systems to observe portable encrypted images. Color filters and color subpixels are also not needed; thus the encoding technique proposed in this study enables the encryption of each pixel in a secret image into a corresponding single pixel in shares. This technique is very simple and can be applied in, for example, security, entertainment, and educational use.

References

1) S. Fukushima, T. Kurokawa, and Y. Sakai: IEEE Trans. Photonics Technol. Lett. **3** (1991) 1133.

2) B. Javidi and J. L. Horner: Opt. Eng. **33** (1994) 1752.

3) P. Refregier and B. Javidi: Opt. Lett. **20** (1995) 767.

4) Y. Hayasaki, Y. Matsuba, A. Nagaoka, H. Yamamoto, and N. Nishida: Appl. Opt. **43** (2004) 1552.

5) Y. Sheng, Z. Xin, M. S. Alam, L. Xi, and L. Xiao-feng: Opt. Express **17** (2009) 3270.

6) B. Javidi and T. Nomura: Opt. Lett. **25** (2000) 28.

7) O. Matoba and B. Javidi: Opt. Lett. **27** (2002) 321.

8) M. Naor and A. Shamir: *Lecture Notes in Computer Science* (Springer, Heidelberg, 1994) Vol. 950, p. 1.

9) O. Kafri and E. Keren: Opt. Lett. **12** (1987) 377.

10) R. Shogenji and J. Ohtsubo: Opt. Rev. **16** (2009) 517.

11) J. Machizaud, P. Chavel, and T. Fournel: Opt. Express **19** (2011) 22709.

12) H. Yamamoto, Y. Hayasaki, and N. Nishida: Opt. Lett. **28** (2003) 1564.

13) T. Imagawa, S. Suyama, and H. Yamamoto: Jpn. J. Appl. Phys. **48** (2009) 09LC02.

14) H. Kowa, T. Murana, K. Iwami, N. Umeda, M. Tsukiji, and A. Takayanagi: Proc. SPIE 8134, Optics and Photonics for Information Processing V, 2011, 81340V.

15) C. Blundo, A. De Santis, and M. Naor: Information Process. Lett. **75** (2000) 255.

16) H. Yamamoto, Y. Hayasaki, and N. Nishida: Opt. Express **12** (2004) 1258.

17) H. Koga, M. Iwamoto, and H. Yamamoto: IEICE Trans. Fundam. Electron. Commun. Comput. Sci. **E84-A** (2001) 262.

18) Y. C. Hou: Pattern Recognition **36** (2003) 1619.

19) S. Cimato, R. De Prisco, and A. De Santis: Theor. Comput. Sci. **374** (2007) 261.

20) T. Kato: J. Geol. Soc. Jpn. **107** (2001) 64.

21) K. Harada, D, Sakai, and S. Kamemaru: Oyobuturikyoiku **30** (2006) 25 [in Japanese].

22) K. Harada, D, Sakai, Y. Sone, H. Harada, and S. Kamemaru: Oyobuturikyoiku **34** (2010) 35 [in Japanese].

23) Commission Internationale de l'Éclairage: Proc. 8th Session, Cambridge, 1931, p. 19.

24) JIS Z 8701 (1999).

Figure Captions

Fig. 1. Combination of rotations of polarization using two key images and decoded results.

Fig. 2. Calculated chromaticity curves of interference color from CIE standard illumination D65.

Fig. 3. (Color online) Calculated interference color chart from CIE standard illumination D65.

Fig. 4. (Color online) Design algorithm of visual cryptography using interference color. Designs of (a) secret image and (b) key images.

Fig. 5. (Color online) Model of multicolor visual cryptography. (a) Key image 1, (b) phase retardation of key image 1, (c) key image 2, (d) phase retardation of key image 2, (e) overlaid result, and (f) total phase retardation of key images 1 and 2.

Fig. 6. (Color online) Prototype of multicolor visual cryptography using interference color. (a) Key image 1, (b) key image 2, (c) incorrect decoded image, and (d) correct decoded image.

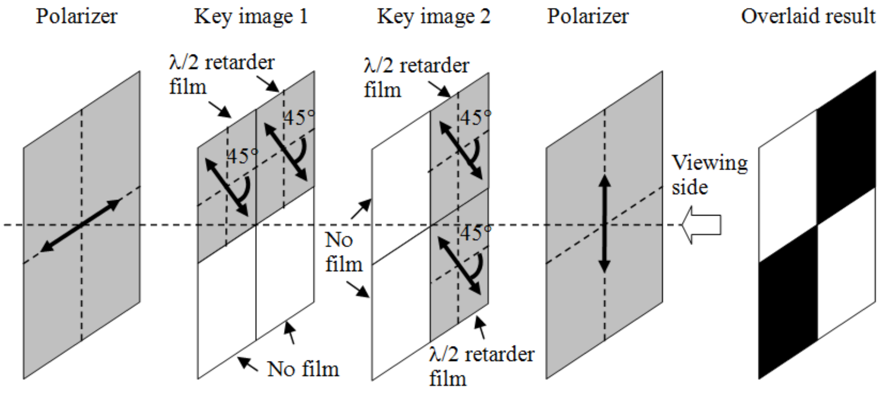

Polarizer
Key image 1
Key image 2
Polarizer
Overlaid result
λ/2 retarder film
λ/2 retarder film
45°
45°
45°
45°
No film
No film
λ/2 retarder film
Viewing side

Figure 1

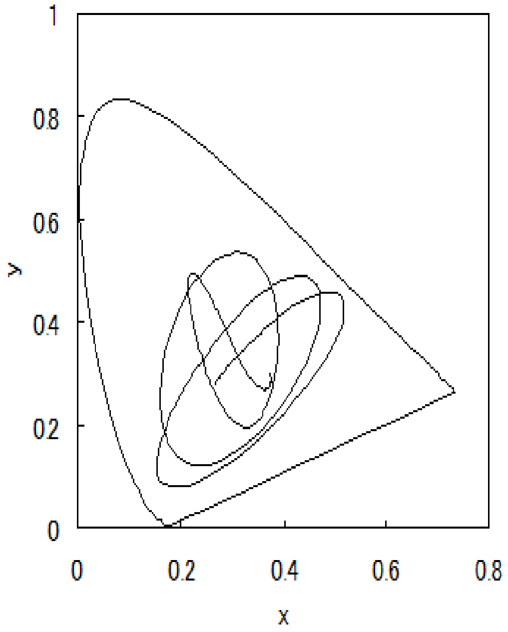


Figure 2

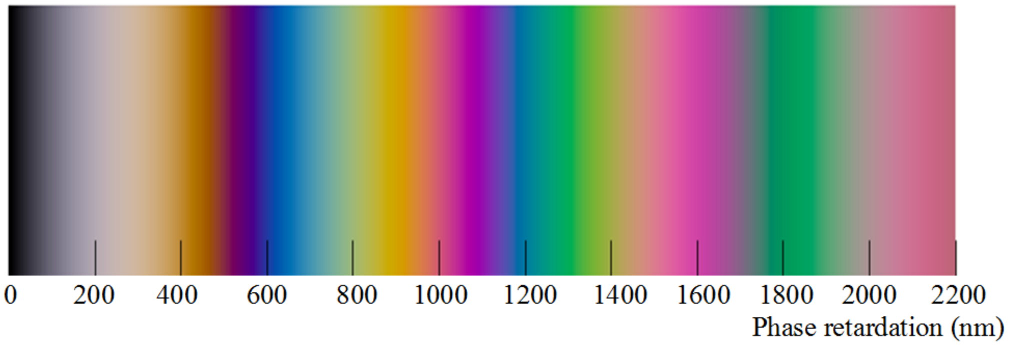
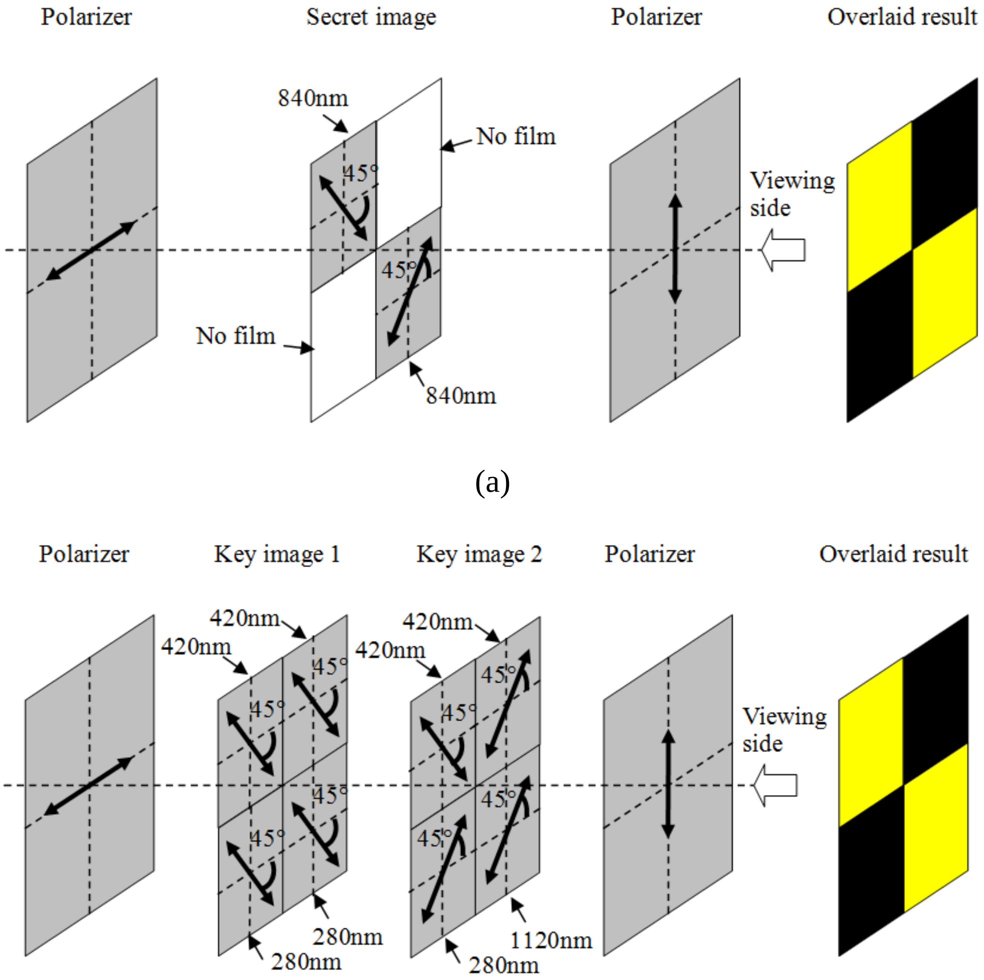

0
200
400
600
800
1000
1200
1400
1600
1800
2000
2200
Phase retardation (nm)

Figure 3


Polarizer
Secret image
Polarizer
Overlaid result
840nm
No film
45°
45°
No film
840nm
Viewing side
Polarizer
Key image 1
Key image 2
Polarizer
Overlaid result
420nm
420nm
45°
45°
45°
45°
280nm
280nm
420nm
420nm
45°
45°
45°
45°
1120nm
280nm
Viewing side

(a)

(b)

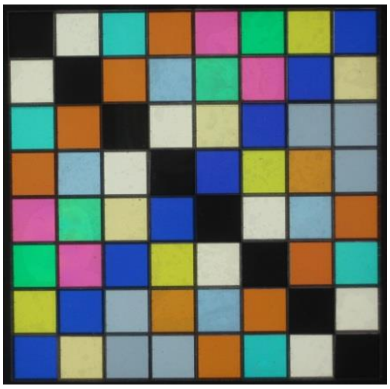
Figure 4

(a)

0	0	0	0	0	0	0	0
280	280	280	280	280	280	280	280
710	710	710	710	710	710	710	710
430	430	430	430	430	430	430	430
1000	1000	1000	1000	1000	1000	1000	1000
1280	1280	1280	1280	1280	1280	1280	1280
850	850	850	850	850	850	850	850
570	570	570	570	570	570	570	570

(nm)

(b)

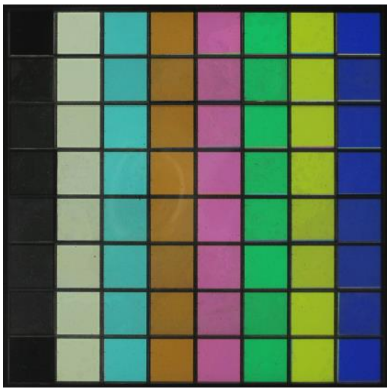


(c)

0	280	710	430	1000	1280	850	570
-280	0	430	150	720	1000	570	290
-710	-430	0	-280	290	570	140	-140
-430	-150	280	0	570	850	420	140
-1000	-720	-290	-570	0	280	-150	-430
-1280	-1000	-570	-850	-280	0	-430	-710
-850	-570	-140	-420	150	430	0	-280
-570	-290	140	-140	430	710	280	0

(nm)

(d)



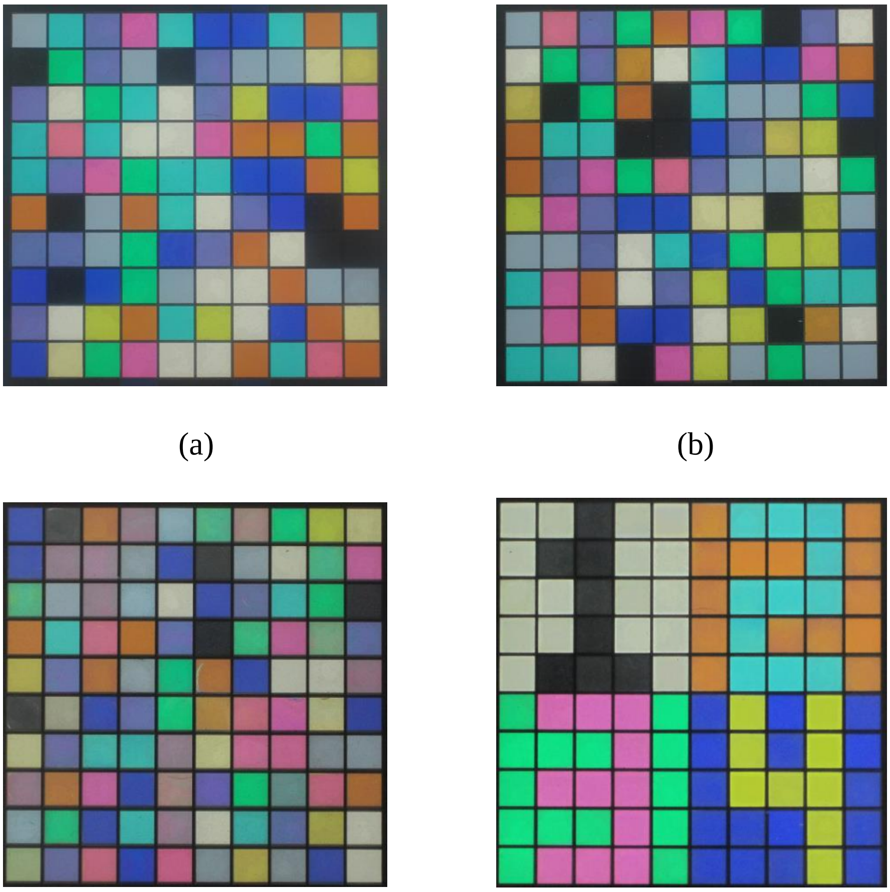
(e)

0	280	710	430	1000	1280	850	570
0	280	710	430	1000	1280	850	570
0	280	710	430	1000	1280	850	570
0	280	710	430	1000	1280	850	570
0	280	710	430	1000	1280	850	570
0	280	710	430	1000	1280	850	570
0	280	710	430	1000	1280	850	570
0	280	710	430	1000	1280	850	570

(nm)

(f)

Figure 5



(a) (b)

(c) (d)

Figure 6