Journal of Software Engineering and Applications, 2017, 10, 754-763
http://www.scirp.org/journal/jsea
ISSN Online: 1945-3124
ISSN Print: 1945-3116

Dual Visual Cryptography Using the Interference Color of Birefringent Material

Huangyi Qin, Toshiki Matsusaki, Yusuke Momoi, Kenji Harada

Department of Computer Science, Kitami Institute of Technology, Kitami, Japan
Email: 545705507@qq.com

How to cite this paper: Qin, H., Matsusaki, T., Momoi, Y. and Harada, K. (2017) Dual Visual Cryptography Using the Interference Color of Birefringent Material. *Journal of Software Engineering and Applications*, **10**, 754-763.
https://doi.org/10.4236/jsea.2017.108041

Received: May 24, 2017
Accepted: July 16, 2017
Published: July 19, 2017

Abstract

Visual cryptography is a method of encrypting an image into several encrypted images. Conventional visual cryptography can display only monochrome images. We previously proposed a color visual cryptography method that uses the interference color of high-order retarder films and encrypts one secret image into two encrypted images. In other words, this method can only encrypt one image at a time. In this paper, we propose a new method that encrypts two color images using interference color.

Keywords

Visual Cryptography, Polarizer, Interference Color, Birefringent Material

1. Introduction

In recent years, various optical cryptography techniques have been proposed for information security [1]-[7]. Visual cryptography is a method of encrypting an image into several encrypted images. The basic algorithm of visual cryptography was reported by Naor and Shamir [8] and Kafri and Keren [9]. This algorism is very effective because no information about the secret image leaks from each encrypted image. In conventional visual cryptography, each encrypted image is a random distribution of black-and-white subpixels. The secret image is observed by superimposing the encrypted images.

Many types of visual cryptography have been proposed [8]-[19]. Conventional visual cryptography reduces the contrast of the secret image because its encryption is based on a spatial coding that requires multiple subpixels to modulate light intensity. The 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 the encrypted images [1] [2] [3] [12]. A simple polarization encoding technique that does not require optical systems was also reported by Imagawa *et al.* [13]. A visual encryption device using high-order retarder films was also reported by Kowa *et al.* [14]. These methods can only be applied to binary images. The limited ability to display colors is also a problem of visual cryptography. Improved visual cryptography for gray-scale images was reported by Blundo *et al.* [15]. Visual cryptography for color images has also been reported [16] [17] [18] [19]. Color visual cryptography technique is useful for various applications, but color subpixels reduce the image contrast of the secret image. To overcome this problem, we propose using interference color. 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]. We use interference color to display multiple color images. Each color is controlled by the phase of retardation of the retarder films. We calculate the interference color of birefringent materials sandwiched with two polarizers, and polarization decryption is performed using stacked films. Encrypted images are portable, and manual alignment of the films is easy because the total number of pixels is small. Multiple color subpixels are not needed to modulate the color light intensity. We have already reported a color visual cryptography using the interference color of high-order retarder films [23]. In this paper, we propose a new method that encrypts dual color images using interference color.

2. Principles of Dual Visual Cryptography Using Interference Color

This section describes the principles of visual cryptography using interference color. In the conventional method, we share a secret image through two encrypted images. **Figure 1** shows the principle of our proposed polarization-based color visual cryptography. **Table 1** lists the basic information of the retarder films we used in this research. Conventional $\lambda 4$ retarder films are used for the 140 nm retarder films, and conventional λ retarder films are used for the 560 nm

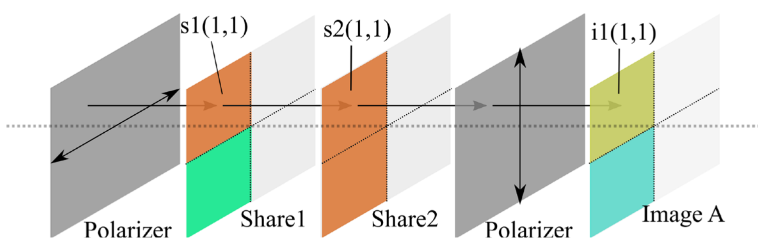


Figure 1. Conventional encryption using interference color.

Table 1. Retardation films used in this research.

Retarder film type	Rotate angle	Symbolic	Retardation (nm)
λ	0˚	λ^{0°	560
λ	90˚	λ^{90°	−560
$\lambda/4$	0˚	$\lambda_4^{0^\circ}$	140
$\lambda/4$	90˚	$\lambda_4^{90^\circ}$	−140

retarder films. Two encrypted images (shares 1 and 2) are inserted between two crossed polarizers. Each pixel of the shares is composed of retarder films.

Here, $pixel(1,1)$ of shares 1 and 2 have different phase retardations. Share 1 consists of a λ retarder film rotated by 0˚ and a $\lambda/4$ retarder film rotated by 0˚, in that order. This configuration is expressed as $s1(1,1)=\left[\lambda^{0^\circ},\lambda^{90^\circ}\right]$ in this paper. For share 2, $pixel(1,1)$ is similarly expressed as $s2(1,1)=\left[\lambda^{0^\circ},\lambda^{90^\circ}\right]$. Pixel $s1(1,1)$ has a 420-nm retardation, and the interference color displayed with the crossed polarizer is orange. Moreover, $s2(1,1)$ has the same retardation of 420 nm, and the interference color displayed with the crossed polarizer is orange. The total retardation is 840 nm when we stack $s1(1,1)$ and $s2(1,1)$, and the interference color displayed with the crossed polarizer is yellow. Pixels $s1(1,1)$ and $s2(1,1)$ form one pixel of the shares-dispersed form of $i1(1,1)$ of decoded image 1. These interference color phenomena make our visual cryptography method possible without any loss of contrast.

In this paper, we consider a method to display another image by sliding the share, as shown in Figure 2. For example, $s1(1,2)=\left[\lambda^{40^\circ}\right]$ has a 140-nm retardation, and the interference color displayed with the crossed polarizer is gray. The total retardation is 560 nm when we stack $s1(1,2)$ and $s2(1,1)$, and the interference color displayed with the crossed polarizer is blue. In this way, the output color changes from yellow to blue by sliding share 1. The two combinations of $\{s1(1,1),s2(1,1)\}$, and $\{s1(1,2),s2(1,1)\}$ show two different colors, and this method can be used for dual visual cryptography. This method requires an external pixel column to be added to share 1, and needs to control the interference color used for multicolor visual cryptography exactly. The calculation of these interference color phenomena and the proposed method are presented in the next section.

3. Calculation of Encrypt Images

In this paper, we only use λ or $\lambda/4$ retarder films with rotation angles of 0˚ or 90˚, as shown in Table 1. Calculation of the interference color has been described in the past [23] and this method is based on it. In this method, we can use eight colors for each pixel of the secret image, as shown in Table 2. For example, assume we have image data consisting of sRGB values. The first step is to convert these data into L*a*b color space. The next step is to find the nearest L*a*b value for each image pixel using the squared difference in Table 2 for the eight colors. Finally, the original color is exchanged with the nearest L*a*b value color.

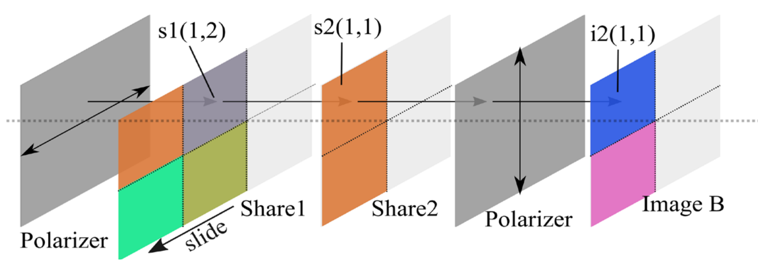


Figure 2. Proposed encryption method using interference color.

After converting the original image into eight colors, we encrypt it. Concretely, suppose we have images A and B of size 2 × 2, as shown in Figure 3. Step 1 is to create a column of pixels (2 × 1) randomly from the eight colors as share 1's first column of pixels. The random retardations have a positive or negative value.

Step 2 is to calculate the first column of share 2. We use values obtained by subtracting the first column of image A from the first column of share 2. Using steps 1 and 2, we hence encrypt the first column of image A. Step 3 is to slide the first column of share 2 onto the second column of share 1. We use the values obtained by subtracting the first column of image B from the first column of share 2 as a second column of share 1. Using step 3, we encrypt the first column of image B. Next, we slide share 1 back and repeat step 2. We use the values obtained

Table 2. Eight colors and their details.

Color	Components	Retardation(nm)	L*a*b
	No film	±0	(0, 0, 0)
	$\left[\lambda_4^{0^\circ},\lambda_4^{0^\circ}\right]$	±280	(99, −8, 17)
	$\left[\lambda^{0^\circ},\lambda_4^{0^\circ}\right]$	±700	(79, −57, −11)
	$\left[\lambda^{0^\circ},\lambda_4^{90^\circ}\right]$	±420	(72, 20, 79)
	$\left[\lambda^{0^\circ},\lambda^{0^\circ},\lambda_4^{90^\circ}\right]$	±980	(73, 70, −23)
	$\left[\lambda^{0^\circ},\lambda^{0^\circ},\lambda_4^{0^\circ}\right]$	±1120	(78, −90, 29)
	$\left[\lambda^{0^\circ},\lambda_4^{0^\circ},\lambda_4^{0^\circ}\right]$	±840	(93, −23, 78)
	$\left[\lambda^{0^\circ}\right]$	±560	(37, 70, −89)

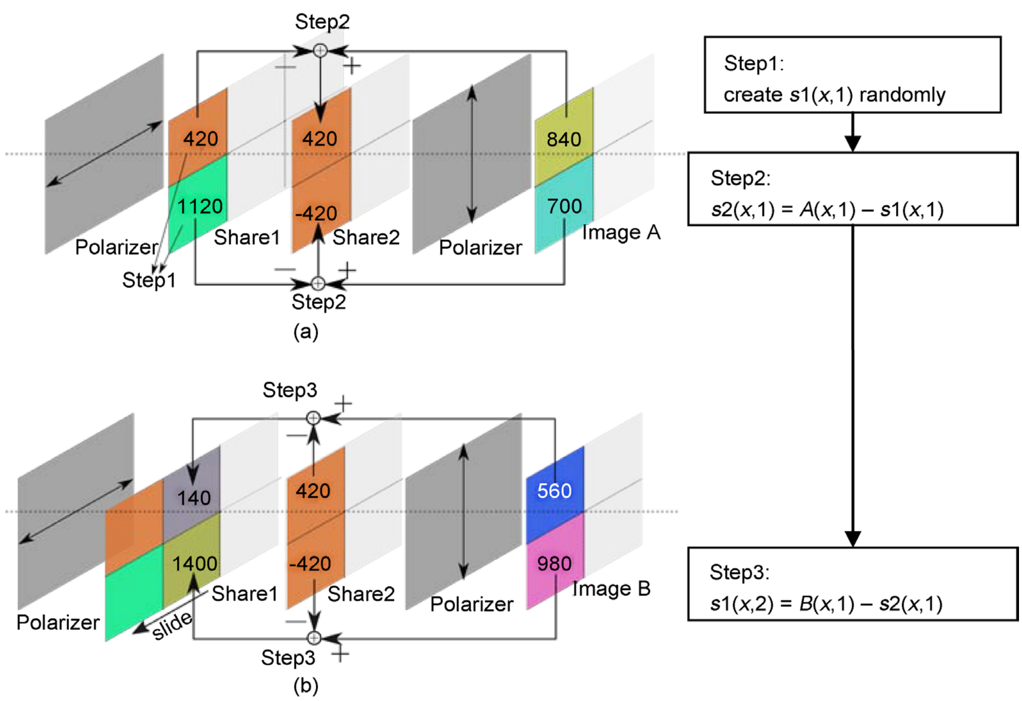


Figure 3. Proposed encryption method. (a) Steps 1 and 2; (b) step 3.

by subtracting the second column of image A from the second column of share 1 as the second column of share 2. Then, we encrypt the second column of image A. In this way, we repeat these steps until there are no more pixels of the image to encrypt.

Figure 4 shows examples of the calculated combinations of retardations and

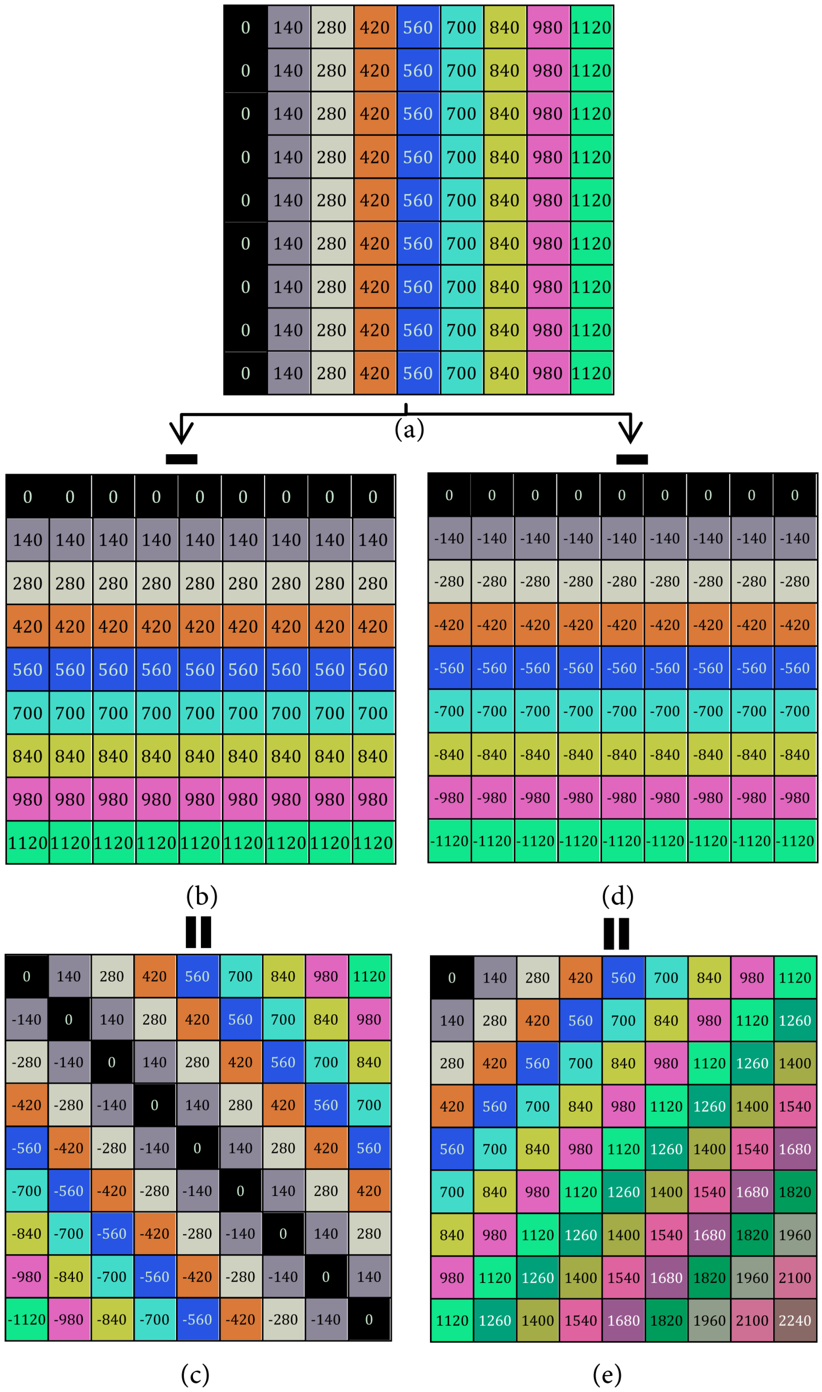


Figure 4. Calculated combinations of retardations and colors. (a) Combinations of images A and B; (b) shares 1 or 2 when the retardation values are positive; (c) result when Figure 4(b) is subtracted from Figure 4(a); (d) shares 1 or 2 when the retardation values are negative; (e) result when Figure 4(d) is subtracted from Figure 4(a).

colors. Figure 4(a) shows the combinations of image A and B when all the retardation values are positive. Figure 4(b) shows the retardations and colors of shares 1 or 2 when the retardation values are positive, and Figure 4(c) shows results of subtracting the value of Figure 4(b) from the value of Figure 4(a). Figure 4(d) shows the retardations and colors of shares 1 or 2 when the retardation values are negative, and Figure 4(e) shows results of subtracting the value of Figure 4(d) from the value of Figure 4(a).

The pseudo code for our proposed encryption method is listed in Table 3.

We need to design the value of $s1$ so that it does not exceed the range −2240 to 2240 nm. Line 17 in Table 3 can be written as

$$s1_{i,j+1} = B_{i,j} - s2_{i,j} = B_{i,j} - \left(A_{i,j} - s1_{i,j}\right) = s1_{i,j} + \left(B_{i,j} - A_{i,j}\right) \tag{1}$$

using the equation written in line 16. Equation (1) is an arithmetic sequence, and can be rewritten as

$$s1_{i,n} = s1_{i,1} + \sum_{k=1}^{k\le n-1}\left(B_{i,k} - A_{i,k}\right) \tag{2}$$

Here, $s1_{i,1}$ is defined within the range −1120 to 1120 nm. To ensure all the values of $s1$ do not exceed the range −2240 to 2240 nm, the value of $\sum_{k=1}^{k\le n-1}\left(B_{i,k} - A_{i,k}\right)$ must not exceed the range −1120 to 1120 nm. Lines 6 - 11 in Table 3 are designed to satisfy this condition.

4. Experiment

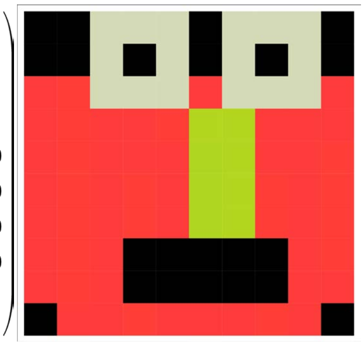
We designed and simulated two secret images using the algorithm shown in Table 3. The two secret images used in this experiment are shown in Figure 5(a)

Table 3. Algorithm to compute two shares from two images.

Input: secret image A of size (n, m) and secret image B of size (n, m)
Output: share s1 of size (n, m + 1), share s2 of size (n, m)
1. Define zero matrix S of size (n, 1)
2. For j = 1 to m do
3. For i = 1 to n do
4. a = nearest retardation to Ai,j of the eight retardations in Lab color space
5. b = nearest retardation to Bi,j of the eight retardations in Lab color space
6. While $\left(S_i + B_{i,j} - A_{i,j}\right)$ not in [−1120, 1120]
7. $a = a^{*}\left(\text{randomly set } -1 \text{ or } 1\right)$
8. $b = b^{*}\left(\text{randomly set } -1 \text{ or } 1\right)$
9. $A_{i,j} = a$
10. $B_{i,j} = b$
11. $S_i = S_i + B_{i,j} - A_{i,j}$
12. For i = 1 to n do
13. Randomly set pixel $S1_{i,1}$ to one of the eight retardations with a positive or negative sign.
14. For j = 1 to m do
15. For i = 1 to n do
16. $s2_{i,j} = A_{i,j} - s1_{i,j}$
17. $s1_{i,j+1} = B_{i,j} - s2_{i,j}$

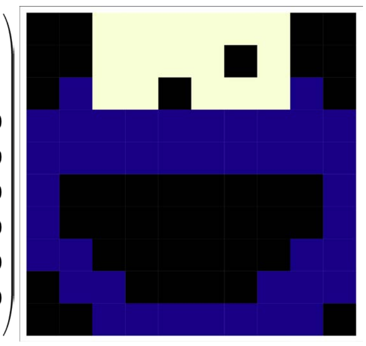
and Figure 5(b). These figures show the retardation value of each pixel (nm) and the calculated color of the pixels. First, we set pixel $s1_{i,1}$ randomly from the eight retardations using the algorithm in Table 3. Next, we calculated shares 1

$$\begin{pmatrix} 0 & 0 & 280 & 280 & 280 & 0 & 280 & 280 & 280 & 0 \\ 0 & 0 & 280 & 0 & 280 & 0 & 280 & 0 & 280 & 0 \\ 980 & -980 & 280 & 280 & 280 & 980 & 280 & 280 & 280 & 980 \\ 980 & -980 & 980 & 980 & -980 & 840 & 840 & 980 & 980 & 980 \\ 980 & -980 & 980 & 980 & 980 & -840 & 840 & 980 & 980 & -980 \\ 980 & -980 & 980 & -980 & 980 & -840 & 840 & -980 & 980 & -980 \\ 980 & -980 & 980 & -980 & 980 & -840 & 840 & -980 & 980 & -980 \\ 980 & -980 & 980 & 0 & 0 & 0 & 0 & 0 & 980 & -980 \\ 980 & -980 & 980 & 0 & 0 & 0 & 0 & 0 & 980 & 980 \\ 0 & 980 & 980 & -980 & 980 & 980 & 980 & -980 & 980 & 0 \end{pmatrix}$$



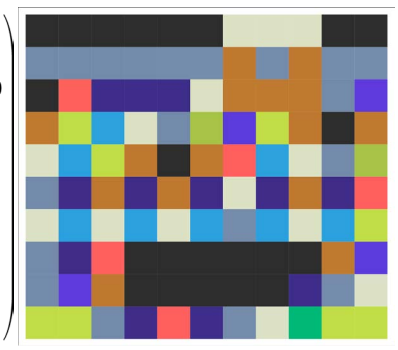
(a)

$$\begin{pmatrix} 0 & 0 & 280 & 280 & 280 & 280 & 280 & 280 & 0 & 0 \\ 0 & 0 & 280 & 280 & 280 & 280 & 0 & 280 & 0 & 0 \\ 0 & 560 & 280 & 280 & 0 & 280 & 280 & 280 & 560 & 0 \\ 560 & 560 & 560 & 560 & 560 & 560 & 560 & 560 & 560 & 560 \\ 560 & 560 & 560 & 560 & 560 & 560 & 560 & 560 & 560 & 560 \\ 560 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 560 \\ 560 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 560 \\ 560 & 560 & 0 & 0 & 0 & 0 & 0 & 0 & 560 & 560 \\ 0 & 560 & 560 & 0 & 0 & 0 & 0 & 560 & 560 & 560 \\ 0 & 0 & 560 & 560 & 560 & 560 & 560 & 560 & 560 & 0 \end{pmatrix}$$



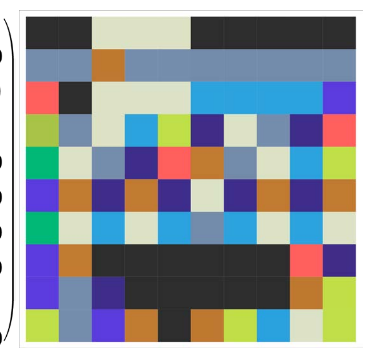
(b)

$$\begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 280 & 280 & 280 & 0 & 0 \\ -140 & -140 & -140 & -140 & 140 & 140 & 420 & 140 & 420 & 140 & 140 \\ 0 & -980 & 560 & 560 & 560 & 280 & -420 & -420 & -420 & -140 & -1120 \\ -420 & -840 & 700 & 280 & -140 & 1400 & 1120 & 840 & 420 & 0 & -420 \\ -280 & -700 & 840 & 420 & 0 & -420 & 980 & 700 & 280 & -140 & 1400 \\ -140 & -560 & 420 & -560 & 420 & -560 & 280 & -560 & 420 & -560 & 980 \\ -280 & -700 & 280 & -700 & 280 & -700 & 140 & -700 & 280 & -700 & 840 \\ -140 & -560 & 980 & 0 & 0 & 0 & 0 & 0 & 0 & -420 & 1120 \\ -140 & -1120 & 420 & 0 & 0 & 0 & 0 & 0 & 560 & 140 & -280 \\ 840 & 840 & -140 & -560 & 980 & 560 & 140 & -280 & 1260 & 840 & 840 \end{pmatrix}$$



(c)

$$\begin{pmatrix} 0 & 0 & 280 & 280 & 280 & 0 & 0 & 0 & 0 & 0 \\ 140 & 140 & 420 & 140 & 140 & -140 & -140 & -140 & -140 & -140 \\ 980 & 0 & -280 & -280 & -280 & 700 & 700 & 700 & 700 & 1120 \\ 1400 & -140 & 280 & 700 & -840 & -560 & -280 & 140 & 560 & 980 \\ 1260 & -280 & 140 & 560 & 980 & -420 & -140 & 280 & 700 & -840 \\ 1120 & -420 & 560 & -420 & 560 & -280 & 560 & -420 & 560 & -420 \\ 1260 & -280 & 700 & -280 & 700 & -140 & 700 & -280 & 700 & -280 \\ 1120 & -420 & 0 & 0 & 0 & 0 & 0 & 0 & 980 & -560 \\ 1120 & 140 & 560 & 0 & 0 & 0 & 0 & 0 & 420 & 840 \\ -840 & 140 & 1120 & -420 & 0 & 420 & 840 & -700 & -280 & -840 \end{pmatrix}$$



(d)

Figure 5. Simulation of dual visual cryptography. (a) secret image A; (b) secret image B; (c) share1; (d) share 2.

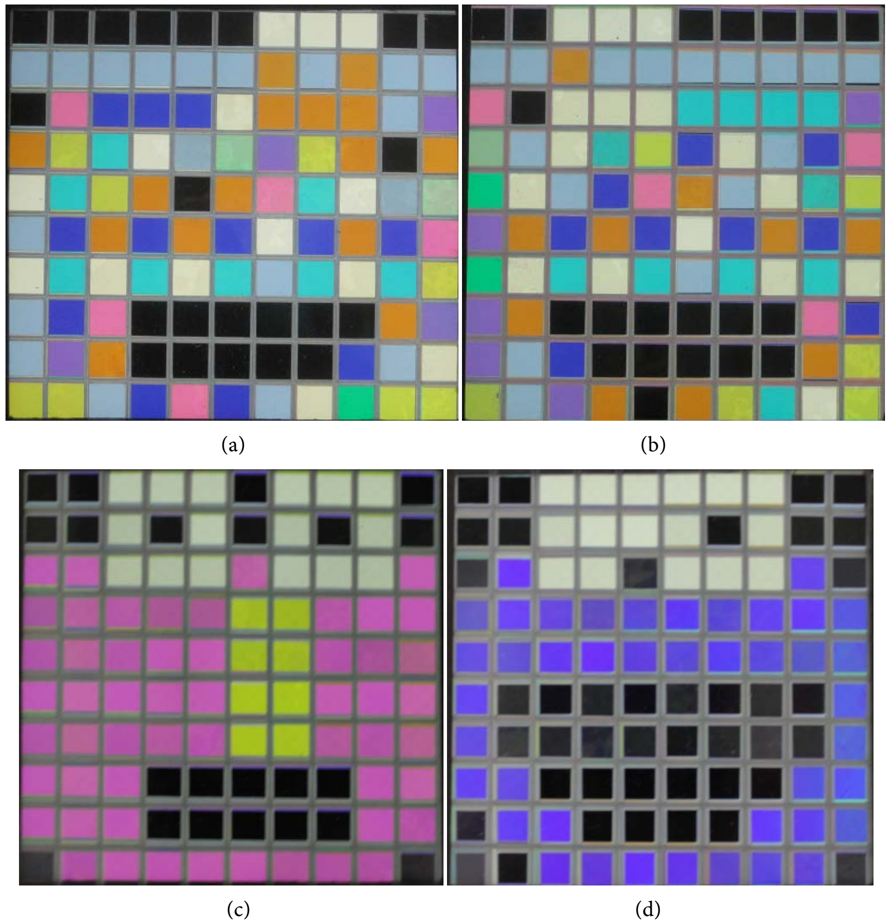


Figure 6. Experimental results of dual visual cryptography. (a) Share 1; (b) share 2; (c) secret image A; (d) secret image B.

and 2 accordingly. Figure 5(c) and Figure 5(d) show the calculated share 1 and share 2 images.

We also made a prototype of the dual visual cryptography using polarizers and retarder films. Figure 6(a) and Figure 6(b) show shares 1 and 2. Share 1 is composed of 10 × 11 pixels, and share 2 is composed of 10 × 10 pixels. The pixel size is 12 × 12 mm^2. By stacking shares 1 and 2, secret image A and secret image B are decoded by sliding share 1, as shown in Figure 6(c) and Figure 6(d).

5. Conclusion

In this paper, we proposed a new method of dual visual cryptography using the interference color of a birefringent material. The resolution and contrast problems in conventional visual cryptography were overcome by polarization processing. We calculated the combinations of interference colors for dual visual cryptography, and a prototype of a dual color visual cryptography device using interference color was developed. Two secret images are decoded by sliding the share. This method solves the resolution and contrast problems of visual cryptography and demonstrates the potential of interference color in visual cryptography.

References

[1] Fukushima, S., Kurokawa, T. and Sakai, Y. (1991) Image Encipherment Based on Optical Parallel Processing Using Spatial Light Modulators. *IEEE Photonics Technology Letters*, **3**, 1133-1135. https://doi.org/10.1109/68.118031

[2] Javidi, B. and Horner, J.L. (1994) Optical Pattern Recognition for Validation and Security Verification. *Optical Engineering*, **33**, 1752-1756. https://doi.org/10.1117/12.170736

[3] Refregier, P. and Javidi, B. (1995) Optical Image Encryption Based on Input Plane and Fourier Plane Random Encoding. *Optics Letters*, **20**, 767-769. https://doi.org/10.1364/OL.20.000767

[4] Hayasaki, Y., Matsuba, Y., Nagaoka, A., Yamamoto, H. and Nishida, N. (2004) Hiding an Image with a Light-Scattering Medium and Use of a Contrast-Discrimination Method for Readout. *Applied Optics*, **43**, 1552-1558. https://doi.org/10.1364/AO.43.001552

[5] Sheng, Y., Xin, Z., Alam, M.S., Xi, L. and Xiao-Feng, L. (2009) Information Hiding Based on Double Random-Phase Encoding and Public-Key Cryptography. *Optics Express*, **17**, 3270-3284. https://doi.org/10.1364/OE.17.003270

[6] Javidi, B. and Nomura, T. (2000) Securing Information by Use of Digital Holography. *Optics Letters*, **25**, 28-30. https://doi.org/10.1364/OL.25.000028

[7] Matoba, O. and Javidi, B. (2002) Optical Retrieval of Encrypted Digital Holograms for Secure Real-Time Display. *Optics Letters*, **27**, 321-323. https://doi.org/10.1364/OL.27.000321

[8] Naor, M. and Shamir, A. (1994) Visual Cryptography. *Lecture Notes in Computer Science*, **950**, 1-12.

[9] Kafri, O. and Keren, E. (1987) Encryption of Pictures and Shapes by Random Grids. *Optics Letters*, **12**, 377-379. https://doi.org/10.1364/OL.12.000377

[10] Shogenji, R. and Ohtsubo, J. (2009) Hiding Information Using a Checkered Pattern. *Optical Review*, **16**, 517-520. https://doi.org/10.1007/s10043-009-0101-9

[11] Machizaud, J., Chavel, P. and Fournel, T. (2011) Fourier-Based Automatic Alignment for Improved Visual Cryptography Schemes. *Optics Express*, **19**, 22709-22722. https://doi.org/10.1364/OE.19.022709

[12] Yamamoto, H., Hayasaki, Y. and Nishida, N. (2003) Securing Information Display by Use of Visual Cryptography. *Optics Letters*, **28**, 1564-1566. https://doi.org/10.1364/OL.28.001564

[13] Imagawa, T., Suyama, S. and Yamamoto, H. (2009) Construction of Visual Cryptography by Use of Polarization-Modulation Films. *Japanese Journal of Applied Physics*, **48**, 09LC02. https://doi.org/10.1143/JJAP.48.09LC02

[14] Kowa, H., Murana, T., Iwami, K., Umeda, N., Tsukiji, M. and Takayanagi, A. (2011) Development of a Visual Encryption Device Using Higher-Order Birefringence. *Proceedings of SPIE*, **8134**, 81340V. https://doi.org/10.1117/12.892969

[15] Blundo, C., De Santis, A. and Naor, M. (2000) Visual Cryptography for Grey Level Images. *Information Processing Letters*, **75**, 255-259.

[16] Yamamoto, H., Hayasaki, Y. and Nishida, N. (2004) Secure Information Display with Limited Viewing Zone by Use of Multi-Color Visual Cryptography. *Optics Express*, **12**, 1258-1270. https://doi.org/10.1364/OPEX.12.001258

[17] Koga, H., Iwamoto, M. and Yamamoto, H. (2001) An Analytic Construction of the Visual Secret Sharing Scheme for Color Images. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, **E84-A**, 262-272.

Scientific Research Publishing

[18] Hou, Y.C. (2003) Visual Cryptography for Color Images. *Pattern Recognition*, **36**, 1619-1629.

[19] Cimato, S., De Prisco, R. and De Santis, A. (2007) Colored Visual Cryptography without Color Darkening. *Theoretical Computer Science*, **374**, 261-276.

[20] Kato, T. (2001) A Method to Synthesize Interference Color Chart with Personal Computer. *The Journal of the Geological Society of Japan*, **107**, 64-67. https://doi.org/10.5575/geosoc.107.64

[21] Harada, K., Sakai, D. and Kamemaru, S. (2006) A New Teaching Material of Polarization Color. *Japanese Journal of Applied Physics Education*, **30**, 25-28. (In Japanese) https://annex.jsap.or.jp/edu/dape/english/e_journal.html

[22] Harada, K., Sakai, D., Sone, Y., Harada, H. and Kamemaru, S. (2010) A New Teaching Material of Interference Color. *Japanese Journal of Applied Physics Education*, **34**, 35-40. (In Japanese) https://annex.jsap.or.jp/edu/dape/english/e_journal.html

[23] Harada, K., Yamaguchi, T., Tsuchida, T. and Sakai, D. (2013) Visual Cryptography Using Interference Color of High-Order Retarder Films. *Japanese Journal of Applied Physics*, **52**, Article ID: 062501. https://doi.org/10.7567/jjap.52.062501