研究速報
Received May 23, 2012; Revised June 29, 2012; Accepted August 7, 2012
光学 **41**, 10（2012）534–538

2つのキー波長をもつ高次複屈折視覚復号型情報セキュリティーデバイス

高和　宏行*,***,†・手島昂太朗*・岩見健太郎*・高柳　淳夫**・梅田　倫弘*・築地　光雄***

*東京農工大学大学院工学府機械システム工学専攻　〒184–8588 東京都小金井市中町 2–24–16
**東京農工大学機器分析施設　〒184–8588 東京都小金井市中町 2–24–16
***ユニオプト（株）　〒421–1221 静岡市葵区牧ヶ谷 2102

Information Security Device Using Higher-Order Birefringence with Two Decoding Key Wavelengths

Hiroyuki KOWA*,***,†, Kotaro TESHIMA*, Kentaro IWAMI*, Atsuo TAKAYANAGI**, Norihiro UMEDA* and Mitsuo TSUKIJI***

*Graduate School of Engineering, Tokyo University of Agriculture and Technology, 2–24–16, Nakacho, Koganei-shi, Tokyo 184–8588
**Instrumentation Analysis Center, Tokyo University of Agriculture and Technology, 2–24–16, Nakacho, Koganei-shi, Tokyo 184–8588
***Uniopt Co., Ltd., 2102, Makigaya, Aoi-ku, Shizuoka-shi, Shizuoka 421–1221

We propose a new type of visual encryption device composed of higher-order birefringence elements. The encryption device was fabricated by controlling the amount of higher-order birefringence so as to give a high contrast only at a certain wavelength under polarized illumination. In this paper, we describe the encryption device of which decoding operation is performed by plural wavelength keys. We demonstrate that information stored in the device can be decoded only by two key-wavelength illuminations. The decoded result is obtained under simultaneous illumination of two specific wavelengths.

Key words: visual encryption device, retardation, higher-order birefringence, polarized light, wavelength

1. はじめに

現代の情報化社会においては，国家機密や企業秘密情報から個人情報に至るまでほとんどすべての情報がディジタル化され，その情報はコンピューターに接続された記憶装置に記録され保管されている．これらの情報は一般にネットワークに接続され，セキュリティーによって保護されつつも利便性を考慮したサービスが提供されている．このため，情報の漏洩や不正利用などの被害を防止するためのセキュリティー技術の重要性が高まっている．情報セキュリティーにおける一般的な特性として，利便性と安全性はトレードオフの関係にある．Naor らによって提案された視覚復号型秘密分散法（visual secret sharing scheme, 以下VSSS）[1] はこの相反する要求を同時に満たす符号化方式であり，これまで数多くの応用研究が報告されている．

VSSS に用いられる物理キーは，ランダムドット状の透過もしくは遮光画素からなる．復号に必要な物理キーを重ね合わせることで秘匿情報が視認できるようになるが，画質の低下や画像全体のコントラストの低下という問題がある．この問題を解決するために，偏光演算を利用したVSSS（PL-VSSS）が提案されている[2–4]．PL-VSSS で使われる物理キーは，四分の一波長板や二分の一波長板など特定の位相差をもった光学位相フィルムで作製されており，このフィルムを通過する直線偏光の偏光方位を制御することで秘匿画像を表示する．しかし，白色光照射によって復号する際には，位相フィルムの波長分散特性や，多数枚の重ね合わせによる光学軸ずれ誤差などから，コントラストの

†E-mail: kowa@uniopt.co.jp

減少が避けられない．

われわれは，物理キーの光学特性として高次複屈折を利用することで，特定の単波長での照明時にのみ意味のある情報を表示し，それ以外の波長や白色光照明では情報の読み出しができない高次複屈折を利用した視覚復号型情報セキュリティーデバイスを提案した[5]．この手法の特徴は，物理キーだけでなく復号波長をキーとすることで秘匿性が向上し，単色光再生であるため復号画像のコントラストの低下も少ないことである．しかし，再生波長はモノクロメーターなどを用いて照明波長を丹念に走査することで容易に解読できる，構成される複屈折デバイスの次数を適切に設計しないとキー波長以外のところでコントラストが反転し情報が読み出せるポイントが存在する，という問題がある．これに対し，われわれは複数の物理キーを用い，それぞれの物理キーが単独でもつキー波長と，すべての物理キーを重ねて復号する際のキー波長を別に設定することで，秘匿性を高められることを示した[6]．キー波長以外においてコントラストが反転した画像が得られる欠点においては，複屈折次数を適切に選択することで回避できる．しかし，キー波長を複数設定してそれぞれ個別に意味のある情報をもたせようとすると，次数の選択に2波長における明暗制御という別の要因が加わるため，反転像を完全に抑える複屈折次数を決定することが困難となる．

本報では，2つのキー波長による同時照明下での復号により秘匿情報が表示される情報セキュリティーデバイスについて報告する．秘匿情報を複数のキー波長に分散することで，単一波長による照明だけでは意味のある情報が得られないことに加えて，反転コントラスト像が生じたとしても，それ自身で秘匿情報が漏洩することがなくなり，情報漏洩に対しての安全性を高められる．従来型の視覚復号型暗号は秘密情報を分散した物理キーを重ね合わせることに対し，本報はキーとなる複数波長の照明光を重ねることで秘密情報が視認できるようになる．いいかえると，秘密情報を複数の照明波長に分散記録している．復号に際しては人間の目視により復号することを前提としているため，視覚復号型暗号の応用形態であると考える．

2. 情報セキュリティーデバイスの原理および製作

一対の偏光子の間に複屈折物質を挟んで片側から単色光で照明すると，透過光強度は複屈折物質のもつ複屈折量に依存して変化する．偏光子を直交ニコル配置とし，透過光強度を考える．試料の複屈折位相差を Δ，主軸方位を偏光子方位に対して45度に設置すると，透過光強度 I_{out} は式（1）で表される．

$$I_{\mathrm{out}}=\frac{I_{\mathrm{in}}}{4}(1-\cos\Delta)=\frac{I_{\mathrm{in}}}{4}\left\{1-\cos\left(\frac{2\pi}{\lambda}\cdot\delta n\cdot d\right)\right\}$$
$$=\frac{I_{\mathrm{in}}}{4}\{1-\cos(2\pi\cdot\delta n\cdot d\cdot k)\} \qquad (1)$$

ただし，I_{in} は入射光強度，λ は波長，k は波数（$=1/\lambda$），d は試料の厚さである．

δn は試料のもつ単位厚さあたりの複屈折量なので，波長分散性をもっている．複屈折は常光線，異常光線に対する屈折率の差で定義されるため，コーシーの屈折率分散の式を用いて式（2）で表わされる．

$$\delta n=n_{\mathrm{e}}-n_{\mathrm{o}}=A_{\mathrm{e}}\left(1-\frac{B_{\mathrm{e}}}{\lambda^2}\right)-A_{\mathrm{o}}\left(1-\frac{B_{\mathrm{o}}}{\lambda^2}\right)=\Delta A\left(1-\frac{B'}{\lambda^2}\right) \qquad (2)$$

ただし，n_{e}, n_{o} はそれぞれ異常光線，常光線に対する屈折率，A および B はコーシーの屈折率分散式における係数であり，添字のeとoはそれぞれ異常光線，常光線に対することを表す．また，ΔA，B' は式（3）で表される．

$$\Delta A=A_{\mathrm{e}}-A_{\mathrm{o}}$$
$$B'=\frac{A_{\mathrm{e}}B_{\mathrm{e}}-A_{\mathrm{o}}B_{\mathrm{o}}}{A_{\mathrm{e}}-A_{\mathrm{o}}} \qquad (3)$$

これらは材料固有の定数である．式（2）を式（1）に代入することで，複屈折の波長分散性を考慮した透過光強度 I_λ が求められる．

$$I_\lambda=\frac{I_{\mathrm{in}}}{4}\left\{1-\cos\left(\frac{2\pi}{\lambda}\cdot\delta n\cdot d\right)\right\}$$
$$=\frac{I_{\mathrm{in}}}{4}(1-\cos[2\pi\cdot\{\Delta A(1-B'k^2)\}\cdot d\cdot k]) \qquad (4)$$

式（4）より，透過光強度 I_λ は波数 k に対して，おおまかには余弦波状に変化し，その周波数は試料の複屈折量 $\delta n\cdot d$ に依存することがわかる．つまり，任意の波長範囲に対して，その中に含まれる正弦波の繰り返し数は試料の複屈折の大きさに依存し，複屈折が大きくなるほど，その周期は短くなる．したがって，照明波長を選択することによって，試料の透過光強度を変化させることができる．複屈折量を適切に制御し，特定の波長で照明したときだけに意味のある画像が表示されるように画素を配列することによって，読み出し波長がキーになった暗号デバイスができる．

今回用いたフィルム材料は，市販のポリカーボネート製光学位相フィルムである．厚さ56.7 μm で，波長560 nmに対して1波長の位相差が生じるフィルム（以下，全波長フィルム），そして，厚さ65.6 μm で，波長560 nmに対して1/4波長の位相差が生じるフィルム（以下，四分の一波長フィルム）の2種類である．$\Delta A, B'$ の定数は，文献等に

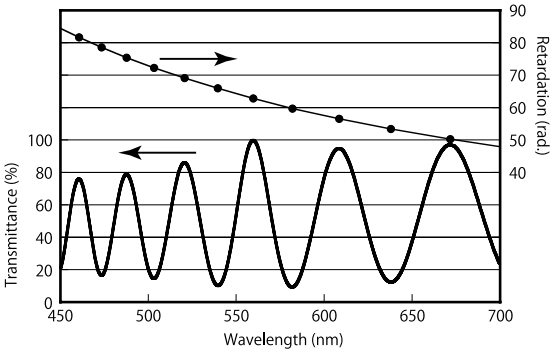


Fig. 1 Channeled spectrum and retardation for ten sheets of commercial retardation film.

掲載されている例は多くないため，実験的に求めなければならない．

全波長フィルムの主軸を一致させて 10 枚重ね，平行ニコル間にはさみ，白色光を照射したときの分光透過率曲線を Fig. 1 の太線に示す．透過率の極小値，極大値はそれぞれ複屈折位相差における $0, \pi$ に相当する波長である．したがって，これらの極値における波長と位相差を使い，式（4）を使って最小 2 乗法により $\Delta A, B'$ を求め，それぞれ，

$$\Delta A = 8.41\times10^{-3},\quad B' = 5.51\times10^{-14} \qquad (5)$$

を得た[6]．Fig. 1 の細線で，式（2）に式（5）を代入したときの，波長に対する δn のフィッティング曲線を示した．ここでは，偏光子を平行ニコル配置としたが，これは分光透過率測定において，光源の光強度分布と偏光子の透過率分布を校正する際に都合がよいためである．得られる結果は，光強度の明暗がちょうど反転することになり，位相差の極値を求めたときの $0, \pi$ を入れ替えて考えればよい．

いま，全波長フィルム N 枚を，波長 560 nm に対して複屈折次数 N 次に対応させて考える．ここで四分の一波長フィルムと全波長フィルムは同一材料であることから，簡単のため，両者の複屈折分散特性は等しいものとする．透過率 T_λ は，式（4）に式（5）を代入し，複屈折次数を使った表現に置き換えて，式（6）のように表される．

$$T_\lambda = \frac{I_{\mathrm{out}}}{I_{\mathrm{in}}} = \frac{1}{4}\left(1-\cos\left[\frac{2\pi}{\lambda}\cdot\left\{8.41\times10^{-3}\cdot\left(1-\frac{5.50\times10^{-14}}{\lambda^2}\right)\cdot N\cdot d_0\right\}\right]\right) \qquad (6)$$

ここで，d_0 はフィルム 1 枚あたりの厚さを表す．本報では，キー波長を 2 つ設定する場合について述べる．それぞれの波長に対する次数を求めるためには，式（6）を連立させる方法や表計算を用いる方法が考えられるが，ここでは図式解で求める方法によって説明する．式（6）を用いて縦軸に次数 N，横軸に波長 λ をとり，透過率をグレースケールで表した図を Fig. 2 に示す．基準とするキー波長は任意で構わないが，ここでは所有している単色フィルターの基準波長の中で，入手が容易な高輝度 LED の波長を考慮して，それぞれ 535 nm, 635 nm と決めた．その波長を灰色の線で示した．デバイス作成に使用する位相フィルムは波長 560 nm に対する全波長フィルムと四分の一波長フィルムであるから，複屈折次数は 0.25 次ステップとなる．これを破線で示した．この破線とキー波長との交点における明暗を調べることで，条件に合う複屈折次数を検索できる．

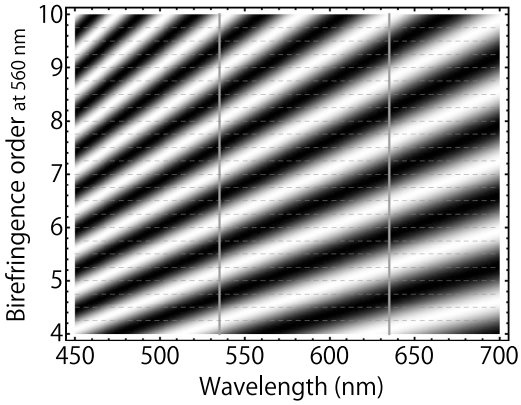


Fig. 2 Transmittance characteristics as function of the amount of high-order retardation and wavelength. Solid lines and dotted lines show decoding wavelength and nominal retardation value of retardation film, respectively.

Table 1 Encoding value of birefringence order used in pixels of the experimental device.

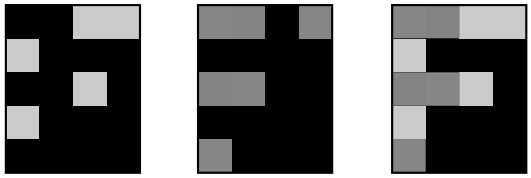
535 nm	635 nm	Order of birefringence at 560 nm
Dark	Dark	4.75, 5.75, 9.5
Bright	Dark	7.0
Dark	Bright	6.5, 7.5
Bright	Bright	5.25

図から，2 つの波長で二値の画像を表示する場合，両者の波長における明暗を表現する 4 つの組み合わせを満足する次数を決定する．試作するデバイスの作製難易性を考慮し，対象とする複屈折次数を 4〜10 とした．この条件におけるデバイスとして有効に使える次数の組み合わせを Table 1 に示す．これらを組み合わせることで，キー波長以外の照明における像にスクランブルをかけることができる．

Table 1 で得られた次数にもとづいて，画素サイズ 5×5 mm，4×5 画素の情報セキュリティーデバイスを試作した．デバイスの複屈折次数配列と，それをキー波長で照明したときに得られる表示像のシミュレーション結果を Fig. 3 に示す．(a) が複屈折次数配列，(b)，(c) はそれぞ

6.5	7.5	7.0	5.25
7.0	9.5	4.75	5.75
7.5	6.5	7.0	9.5
7.0	4.75	4.75	5.75
6.5	9.5	5.75	9.5

(a)



(b) (c) (d)

Fig. 3 Design of experimental device; (a) retardation order, (b) simulated image illuminated by the wavelength of 535 nm, (c) simulated image illuminated by the wavelength of 635 nm, (d) simulated image under illumination of wavelength of 535 nm and 635 nm.

れ 535 nm，635 nm で照明したときの表示像，(d) は 2 つのキー波長を同時に照射したときの表示像の計算結果である．単独のキー波長では文字の認識ができないが，両者を同時に照射することで文字 F が表示されることが期待できる．

3. 観 察 結 果

試作したデバイスを直交ニコル間に挟み，単色光で照明したときの観察結果を Fig. 4 に示す．光源は 100 W ハロゲンランプ（ショット日本社，MegaLight100）を用い，単色光の取り出しにはモノクロメーター（OEL システムズ社，OMS-100：波長分解能 5 nm）を用いた．波長は 485 から 655 nm まで 10 nm ステップとした．キー波長は 535 nm と 635 nm である．535 nm では，シミュレーションとほぼ同じ観察像が得られている．しかし，635 nm ではややコントラストが悪く，期待通りの表示像が得られていない．シミュレーション像に相当する観察像は 645 nm が近く，やや長波長側にシフトした結果となっている．キー波長のずれの原因は，波長フィルムの重ね合わせ誤差や光軸に対するデバイスの設定角度のずれなどが起因しているものと考える．460 nm より短波長側は，光源の光強度が弱いことと，使用した偏光子の光吸収の影響で十分な観察感度が得られなかった．

Fig. 4 に示した波長全域で，秘匿情報―文字 F ―は観察

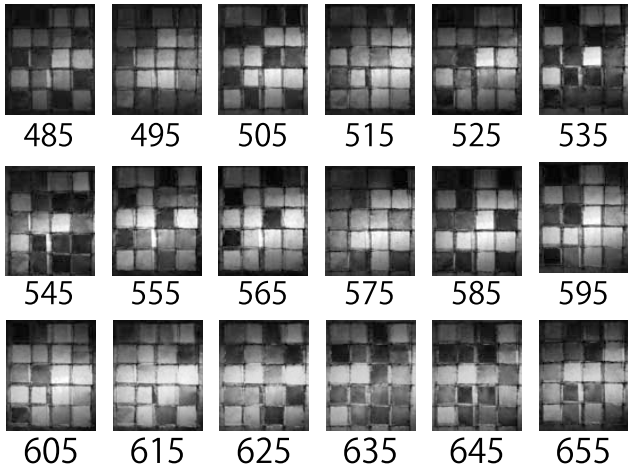


Fig. 4 Observation results of the information hiding device for changing the wavelength of illumination.

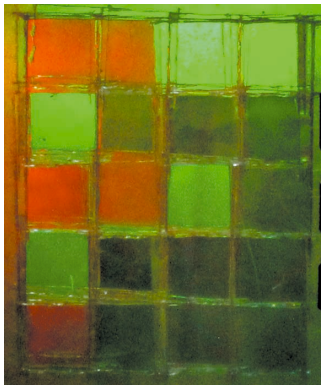


Fig. 5 Observation result of the information hiding device under two key wavelengths of illumination.

されない．また，キー波長を想像させるポイントも見当たらない．したがって，このデバイスに対して単色光の波長を変えながら丁寧に探索を試みても，ただちに秘匿情報が漏洩することはないものと考えられる．

次に，2 つのキー波長を同時に照明したときの観察を試みた．光源には，中心波長が 535 nm, 635 nm の高輝度 LED を用いた．LED の発光波長の半値幅は 10〜15 nm であるため，そのまま照射すると複屈折の波長分散特性の影響を受け，十分な画像コントラストが得られない．したがって，中心波長が LED と同じ狭帯域バンドパスフィルターを挿入し，波長純度を高めた．Fig. 3 で示したように，長波長側のキー波長は 635 nm ではなく 645 nm 近辺にシフトしている．したがって，バンドパスフィルターを傾斜させて配置し，透過率の中心波長をシフトさせた．

Fig. 5 に観察結果を示す．緑と赤のピクセルによって文字 F が表示されている．Fig. 3 (d) で示したシミュレーション結果とほぼ同じ表示画像が得られており，本手法の有効性を示している．

4. ま と め

高次複屈折を利用した視覚復号型情報セキュリティーデバイスの応用例として，秘匿情報をひとつのデバイス内において複数のキー波長に分散記録させる方法を提案し，その有効性を示した．復号はキー波長を同時に照明することで容易に観察することができる．一方，キー波長が知られない場合においては，たとえ単一波長を走査し解読を試みても，容易に情報を読み出すことができない．復号に際しては，キー波長を同時に照明することだけでなく，それぞれ個別に照明した画像を撮影記録し，コンピューターによって画像合成することでも可能である．また，単一キー波長の場合には，文献 5）で示されたように，キー波長近傍に秘匿画像の反転像が現れる場合があり，キー波長に限らず近傍の単色光で秘匿画像が読み出される危険性があった．キー波長を複数とし，それぞれが単独で意味のない像とすることで，反転像が現れたとしても，それが秘匿情報であることを察知されることはない．

本研究は，科学研究費挑戦的萌芽研究（課題番号 23656250）の助成を受けたものである．

文 献

1）M. Naor and A. Shamir: “Visual cryptography,” *Lecture Notes in Computer Science*, **950**（1994）1–12.
2）T. Imagawa, S. Suyama and H. Yamamoto: “Visual cryptography using polarization-modulation films,” *Jpn. J. Appl. Phys.,* **48**（2009）09LC02.
3）原田建治：“複屈折性材料の干渉色を用いた偏光暗号”，第 58 回応用物理学関係連合講演会，25a-KL-7（2011）.
4）山本裕紹，今川貴紀，陶山史朗：“多層の位相差フィルムを用いた偏光式視覚復号型暗号”，応用物理学関係連合講演会講演予稿集，17p-J-3（2010）.
5）高和宏行，岩見健太郎，梅田倫弘，築地光雄：“高次複屈折を用いた情報セキュリティーデバイスの開発”，光学，**40**（2011）490–498.
6）H. Kowa, T. Murana, K. Iwami, N. Umeda, M. Tsukiji and A. Takayanagi: “Development of a visual encryption device using higher-order birefringence,” Proc. SPIE, **8134**（2011）81340V.