研究論文
Received November 17, 2010; Accepted June 9, 2011
光学 **40**, 9（2011）490–498

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

高和　宏行*,**・岩見健太郎*・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 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

Development of the Information Security Device Using Higher-Order Birefringence

Hiroyuki KOWA*,**, Kentaro IWAMI*, Norihiro UMEDA* and Mitsuo TSUKIJI**

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

We propose a new type of visual information security device (VISD) consists of higher-order birefringence elements. When a higher-order birefringence film which is sandwiched between a pair of polarizer is illuminated by white light from one side, the image with white color is observed. On the other hand, when the film is illuminated by monochromatic light, the brightness of transmitted light depends on its wavelength. The VISD is fabricated by controlling the amount of higher order birefringence which gives a high contrast at the only certain wavelength under polarized illumination. The device can be decoded by the illumination of specific reading wavelength. In this paper, we have simulated and demonstrated observation images of the device under white and monochromatic illuminations. Furthermore, stored information can be easily distributed to multiple physical keys which show arbitrary images. In this case, since the image is decoded by XOR operation of each pixel of physical keys, the decoded result is obtained by superimposing them.

Key words: security, birefringence, higher order, wavelength, polarization, visual cryptography

1. はじめに

近年，インターネットの発達と携帯通信機器の普及により，さまざまな情報共有や商取引などが簡便に行えるようになった．しかし，ネットワークを悪用し個人情報を不正に取得するなど，情報の悪用による被害が増大している．個人情報等の秘匿されるべき情報をいかに保護するかといった情報セキュリティー技術は，情報化社会において必要不可欠となっている．

情報セキュリティーの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．セキュリティー技術を効果的に開発するためには，想定される攻撃を明らかにしたうえで，それに対する対策技術を構築することになる．したがって，複数の種類の攻撃を想定する場合，対策技術は増大し，セキュリティーシステムは複雑になる．

光技術を利用した情報セキュリティー技術は，大きく分けて，情報そのものを隠ぺいする手法と，情報の内容を隠ぺいする手法に大別される[1]．前者の代表技術としてはステガノグラフィーが，後者としては暗号技術があげられ，それぞれ多くの研究が報告されている．一般に，セキュリティーとしての強さを測る尺度として，情報を不正に得ようとする者がその情報を解読するまでに費やされる時間が用いられる．暗号情報を何らかのカバーデータに隠ぺいすれば，解読作業は，暗号が隠されたデバイスを探し，顕在化させ，その後に暗号解読を試みるというように手間が増えることになる．したがって，暗号そのものをステガノグラフィー等の技術によって潜像化させることで，より安全性の高い情報デバイスとなる．

人間の視覚を利用して情報の復号や顕在化を行う技術は，復号に際してコンピューターや特別な機器を必要としない．人間の視覚特性は図形を観察したときに，その図形を細かな要素に分解してとらえる性質をもたず，何らかのまとまり，統一性，経験によって理解される意味に基づい

E-mail: kowa@uniopt.co.jp

て認識する法則性を備えており，この法則によって形状をとらえようとする[2]．

人間の視覚特性を利用した情報セキュリティー技術は，情報デバイスや著作物の正真性を測るためにも利用され，電子透かし技術，電子署名などに応用されている．例えば，低コヒーレンス干渉を利用して散乱媒体の背後にある秘密画像を読み出す技術[3]，光強度の排他的論理和（XOR）を画像間で演算する手法[4]，レンズ系を用いて，そのフーリエ面において画像情報にランダム位相を付加することで情報を秘匿する手法[5]などが提案されている．また，R. A. Lee らは，リソグラフィー技術を使い，暗号化におけるドットサイズを小さくする手法を提案している．この手法では，復号画像の画質を向上させるだけでなく，偽造防止効果も得られる．また，印刷物の表面にシリンドリカルレンズ状のエンボス加工を施すことで，画像の多重記録・表示を実現している[6]．

秘密画像を複数の物理キーに分散して暗号化する方法として，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 とする）[7]がある．この方法は，秘密画像を複数の分散画像に暗号化し，そのうちのいくつかの指定された分散画像を重ねることで秘密画像を視認できるものである．VSSS は多くの応用研究があり，復号画像の最適化[7]やグレースケール画像[8,9]やカラー画像への拡張[9–11]，電子透かしへの応用[12]などが報告されている．さらに，秘匿性を高めるために，空間符号化を利用して秘密画像の復号と視野の制御を同時に実現する方法[13–15]が提案されている．

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．物理キーを重ね合わせるとき，互いが正しい位置関係になった場合にのみ秘匿画像が観察できる．復号時における位置合わせの問題に関しては，F. Liu らの研究報告がある[16]．これに対して，復号時の位置合わせを簡便にするための手法として，チェッカーパターンを用いた暗号技術が提案されている．この方法は，復号マスクにチェッカーパターンを用いることで，位置合わせの困難性を回避している．興味ある応用例として，復号マスクにサンプリング処理を利用し，カメラで暗号画像を撮像するだけで復号画像を再生する例が示されている[17]．

暗号化される元画像の画素は，それぞれさらに細かな複数のサブピクセルに分割される．このサブピクセルに対して，いくつかの明暗の配列を与えて符号化する．復号時において，複数の物理キーが重ね合わされる際，サブピクセルの遮光画素の密度の違いをもたせることで視覚的に元画像を認識できるように工夫されている．このため，復号される秘密画像はランダムドット状の点群が重畳されることになり，画質の低下，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，Imagawa らは，偏光演算による視覚復号型暗号法を提案している[18]．この手法は，複数の偏光位相子を多重化して重ね，画像を表現するものである．位相差フィルムをモザイク状に貼り合わせたものを積層し，これによって偏光の偏光軸を制御し，分散画像を作成する．このため，サブピクセルが不要になり，1 画素単位での符号化が可能になる．ここでは，Imagawa らによって提案された方法を偏光変調式視覚復号型暗号（以下，PL-VSSS）とよぶことにする．

PL-VSSS は 1 画素単位での符号化が可能なため，復号画像の画質の向上が期待できる．しかし，秘匿性を高めるために物理キーの数を多くすると，フィルムの積層数が多くなり，表面反射による減光，位相フィルムの主軸の重ね合わせ誤差による偏光乱れに起因するコントラストの減少や，位相フィルム自身の複屈折波長依存性に起因するコントラストの減少が避けられず，画質の低下が問題となる．

今回われわれは，視覚復号型情報セキュリティー技術のひとつとして，高次の複屈折による波長分散特性を利用し，ある特定波長の偏光照明だけに意味ある情報を表示させ，その他の波長では表示させないような，読み出し波長をキーとするセキュリティーデバイスを提案する．このデバイスは，非偏光照明や白色光照明では像が形成されず，通常の観察環境では情報画像が潜像化される．本報では，像再生の基本原理，シミュレーション，デバイスの試作結果を示した後，PL-VSSS への応用例を示す．秘匿キーに波長が加わるため，暗号としての強度を高められること，単色光照明を用いることで表示画像のコントラストの向上などが期待できる．

2. 原　　理

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．偏光子を平行ニコル配置とし，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 $(=1/\lambda)$，

δnは試料のもつ単位厚さあたりの複屈折量，dは試料の厚さである．式（1）より，透過光強度I_{out}は波数kに対して余弦波状に変化し，その周波数は試料の複屈折量$\delta n \cdot d$に等しいことがわかる．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比例し，複屈折が大きくなるほど，その周期は短くなる．

次に，偏光子の片側から白色光で照明することを考える．複屈折物質の複屈折量が数千 nm か，あるいはそれ以上の大きな値をもつ場合，透過光強度は可視光の範囲内において，いくつかの極大，極小を繰り返す．可視光波長範囲内で透過光強度のピークが 4 つ以上となる場合に，透過光は白色として観測される．色を感じる錐体視細胞は赤，緑，青の三原色それぞれに感じるような 3 種類が存在し，3 種の視細胞が等強度に刺激を受けたときに，その光を白色として認識するためである．

一方，単色光で照明すると，透過光強度は波長に依存して変化する．したがって，照明波長を選択することにより，試料の透過光強度を変化させることができる．複屈折量を適当に制御し，特定の波長で照明したときにだけ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．

いま，基準波長を 550 nm として，例えば複屈折位相差が 1100 nm になったときの複屈折量は 550 nm の 2 倍と考え，この状態を二次の複屈折量とよぶことにする．この次数を$N(N=0, 1, 2, 3\cdots)$とおき，余弦波の位相をϕとおくと，式（1）は次のように変形できる．

$$I_{\mathrm{out}}=\frac{I_{\mathrm{in}}}{4}\{1+\cos(2\pi N+\phi)\} \qquad (2)$$

したがって，任意の波数kにおける透過光強度I_{out}は次数Nに依存せず，$\phi=0$または2πとなるとき最大となり，$\phi=\pi$のとき最小となる．

ここで，$m\times n$の画素配列を考える．ここに文字などの情報（＝秘匿情報）を表示させるとき，ある波長に対して文字を構成する画素を$\phi=0$，背景になる画素を$\phi=\pi$となるように複屈折位相差を調整すると，その波長で照明したときに，秘匿情報が明瞭に表示される．この波長をキー波長とよぶことにする．ここで，各画素のϕを固定したまま，それぞれの画素の複屈折次数Nをランダムに変化させると，キー波長以外における各画素のϕは0またはπとならず，それぞれがランダムな値をもつ．

したがって，このデバイスは，キー波長でのみ秘匿情報が表示され，白色光を含めてそれ以外の波長で観察したときには，正しい情報が表示されず情報は潜像化される．すなわち，読み出し波長を復号キーとした情報セキュリティーデバイスとなる．秘匿情報の読み出しには，① 読み出し波長がわかっていなければならないこと，② 一対の偏光子が必要であり，通常の観察環境においては，情報は潜像化されている．また，読み出し波長と偏光子の両方がそろわない限り，情報の読み出しができない．

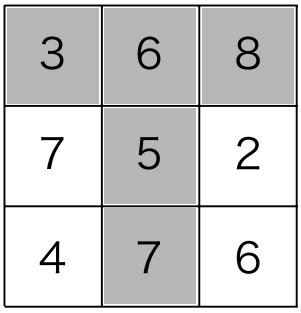


Fig. 1　Design of experimental device. Number and color in each pixel indicate order number and phase of birefringence, respectively. Gray corresponds to π and white corresponds to 0.

3. シミュレーション計算

上記の原理に基づき，像表示の妥当性を検証するため，シミュレーション計算を行った．Fig. 1 に計算に用いたデバイスの複屈折次数Nとϕの配置を示す．図中，次数Nは数字で，ϕは色分けで記してある．灰色画素が$\phi=\pi$，白色画素は$\phi=0$である．このデバイスを平行ニコルに配置した偏光子に挟み単色光で照明したときの，各画素の透過率強度I_{out}を式（2）を用いて計算した．試料の複屈折波長分散の影響は考慮していない．キー波長は 560 nm に設定した．ϕ値は，キー波長においてアルファベットのTの文字が表示されるように配置されている．複屈折次数Nは，2〜8 の間で規則性をもたせないように配置した．

Fig. 2 は，上記のデバイスを波長 400〜700 nm の間で 10 nm きざみで単色光照明したときに観察される透過光強度分布を示している．波長 560 nm において最も高いコントラストで像表示ができていることがわかる．それ以外の波長では，おおむね文字情報としての認識ができない像となっている．しかし，550 nm および 570 nm 近傍では若干のコントラストの低下があるものの，文字Tとして判読できる．これは，複屈折次数が低いため，波長に対する複屈折の変化率が小さくコントラスト変化も緩慢になっていることによると考えられる．そこで，文字のコントラストを求め，複屈折次数と情報画像が認識できる波長範囲との関係を調べた．

画像のコントラスト値Cは，文字を構成する画素の透

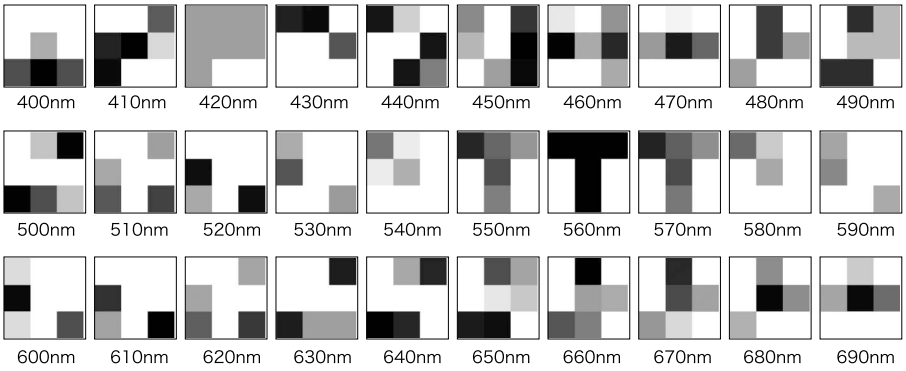


Fig. 2　Simulation results of observed image of information hiding device. The mosaic pattern is changed by illuminated wavelength.

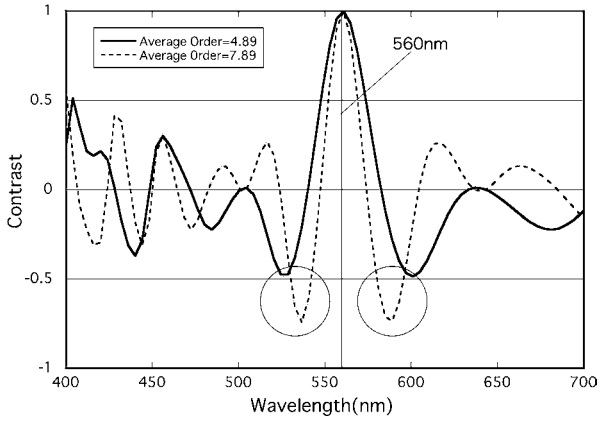


Fig. 3　Simulation result of image contrast.

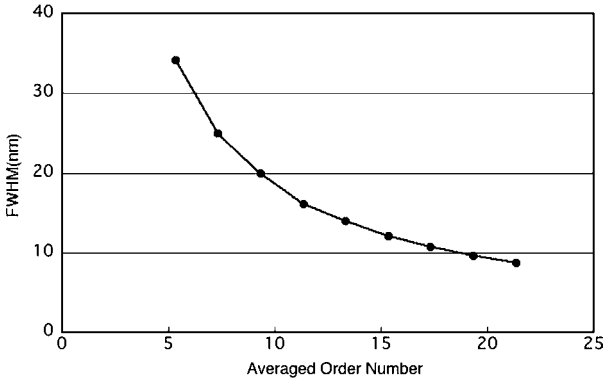


Fig. 4　Variation of full width at half maximum of image contrast as a function of averaged order number.

過光強度の平均値を I_C，背景となる画素の透過光強度の平均値を I_B とし，次式により求めた．

$$C=\frac{I_C-I_B}{I_C+I_B} \qquad (3)$$

Fig. 2 におけるそれぞれの表示画像のコントラストを波長に対してプロットした結果が Fig. 3 の実線である．コントラスト値が負を示すとき，像の明暗が反転する．550 nm および 570 nm のコントラストは，それぞれ 0.64, 0.71 であった．また，文字として認識できない 540 nm および 580 nm のコントラストは，それぞれ−0.02, 0.13 である．キー波長から離れるに従って，コントラスト値は増減を繰り返す．520 nm および 610 nm においてコントラスト値は −0.38 となっているが，Fig. 2 における当該波長の像は，明暗が反転した文字として認識できる限界にみえる．それ以外の波長においては，文字としての認識ができない．

Fig. 3 には，Fig. 1 に示した配列のそれぞれの画素の複屈折次数をすべて三次分だけ加算したグラフを破線で示している．複屈折次数が高くなると，コントラストのピークを示す幅が鋭敏になる一方，図中円で示したようにキー波長の両側にコントラスト値が負側に大きくなる領域がみられるようになる．平均次数が高くなると，余弦波状に変化する光強度の周期が短くなり，それぞれの画素の透過光強度の変化の差が相対的に小さくなるため，反転画像のコントラストが高くなる．

いま，$C=0.5$ を画像認識の閾値として設定することとし，$C>0.5$ となる波長幅，すなわちコントラスト値の半値全幅 C_{FWHM} が複屈折次数に対し，どのように変化するかを調べた．半値全幅 C_{FWHM} は，コントラストのピーク位置を中心にして，その両側のコントラスト値が 0.5 を示す波長間隔として定義する．複屈折次数は，Fig. 1 で示した複屈折配列における 9 画素の平均値を用いた．次数の変化は，同図のすべての画素に対して同量の次数を加えている．その結果を Fig. 4 に示す．コントラストの半値全幅は，複屈折次数に反比例することがわかる．情報の秘匿性を高めるためには，像再生できる波長範囲を狭くすることが望ましいので，複屈折次数を高くすればよいことがわかるが，一方で前述のように反転コントラストを示す領域が出現する．このため，複屈折次数の配置に関して設計指針

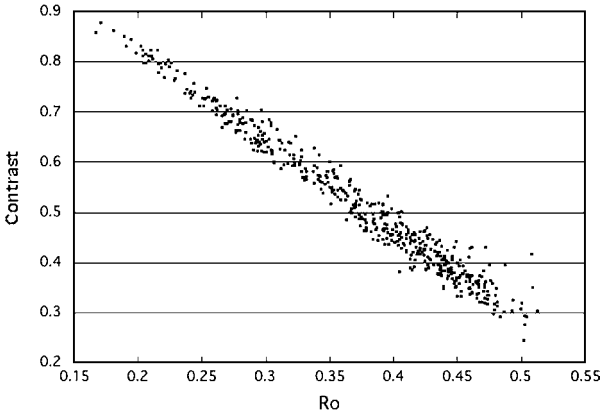


Fig. 5　Relation between contrast and R_o value.

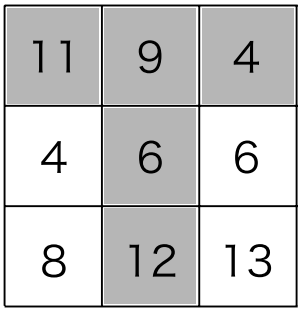


Fig. 6　Design of experimental device. Number and color in each pixel indicate order number and phase of birefringence, respectively. Gray corresponds to π and white corresponds to 0.

が必要となる．そこで，反転コントラストを抑える複屈折配列の指針を得ることを目的としたシミュレーションを行った．

反転コントラストを低く抑えるためには，低い次数の画素と高い次数の画素を適度に混在させる必要がある．また，白色光照明下においては，デバイスが白色で観察されることが情報の潜像化に対して必要となる．そこで，デバイスの設計指針を得るために，配置する複屈折次数すべての平均値と，標準偏差との比を R_o 値とし，これを用いる．R_o 値を，式（4）で定義する．

$$R_o = \frac{S_o}{A_o} \qquad (4)$$

ここで，S_o は画素の複屈折次数の標本標準偏差，A_o は平均値を表す．

シミュレーションは，次のように行った．10×10 画素の配列のデバイスを設定し，個々の画素に 4 から 30 次の間でランダムに複屈折次数を割り当て，500 個のデバイスを作成した．複屈折次数の割り当ては，コンピュータープログラム Mathematica ver. 8 のランダム関数を用いた．100 画素の半数を文字部，半数を背景部画素に設定し，コントラストと R_o 値を計算した．その結果を Fig. 5 に示す．R_o 値とコントラストには強い負の相関があることがわかる．これより，コントラストを 0.5 以下にするためには R_o 値を 0.38 以上にすればよいことが示された．

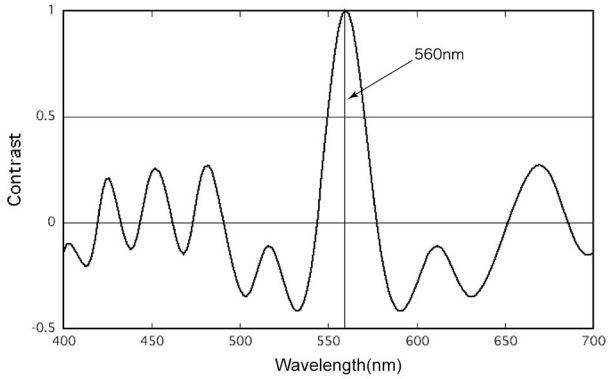
この結果をふまえ，新たに 3×3 画素のデバイスの配列を決めた．上記と同様にランダム関数を用いて複屈折次数の割り当てを 300 個のデバイスに対して行い，それぞれの R_o 値を求めた．ただし，ここでは実際にデバイスを試作するときの作製難易性を考慮し，複屈折次数を 4 から 14 次の範囲に限定した．その中で，最も大きな R_o 値を示した配列を Fig. 6 に示す．この配列の R_o 値は 0.406 である．キー波長は 560 nm である．

Fig. 6 に示したデバイスを単色光で照明したときの，波長に対する表示画像コントラストの関係を Fig. 7（a）に示す．キー波長を除くすべての可視光領域において，コントラスト値の絶対値は 0.42 以下となった．Fig. 6 の配列では，複屈折の最低次数が 4 次となっており，白色光観察においても潜像化ができている．この結果から，デバイスの複屈折次数の配列の設計に際して R_o 値を用いることが，有効であることが示された．Fig. 7（b）に，400〜700 nm における単色光照明における観察画像の様子を示す．Fig. 2 と同様に，キー波長以外ではアルファベットの文字が読めない．

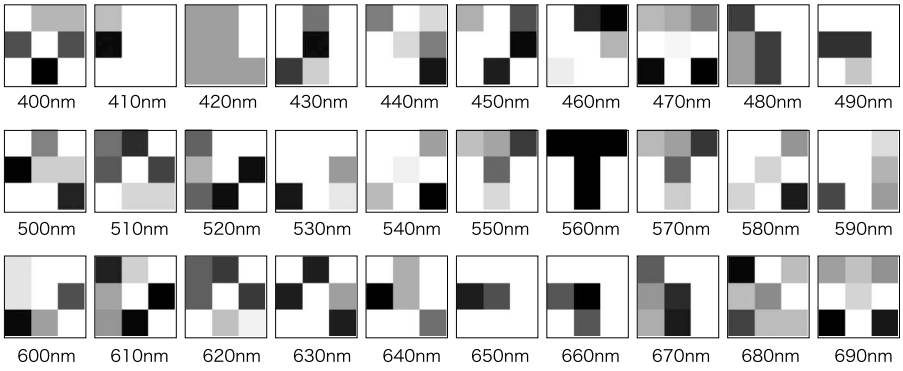
4.　試作したデバイスと観察結果

原理の有効性を確認するために，複屈折量 560 nm と 140 nm のポリカーボネート製光学用位相差フィルムを積層し，3×3 画素のデバイスを作製した．以下，560 nm フィルム（全波長フィルム）を N 枚重ねた状態を N 次の複屈折とよび，140 nm フィルム（4 分の 1 波長フィルム）を 2 枚用いたときを $\phi = \pi$，用いないときを $\phi = 0$ とする．デバイスの複屈折の画素配列は，Fig. 6 で示したものとした．ϕ 値の配列から，このデバイスを偏光子で挟み，波長 560 nm の単色光で照明すると，アルファベットの T が観察できると予想される．

このデバイスを平行ニコル間に挟み，白色光で照明したときの各画素における分光透過率を Fig. 8 に示す．光源は 6.5 W タングステンハロゲンランプ（OceanOptics 社，LS-1）を用い，分光器には OceanOptics 社製 QE65000 を用いた．偏光子には，フィルム製を用いた．太線は文字部，細線は背景部の透過率曲線である．太線は，波長 560 nm の位置で文字部を構成するすべての画素の透過率が極小値を示している．細線は逆に，背景部を構成するすべての画素の透



(a)



(b)

Fig. 7　Simulation results of optimized device; (a) image contrast and (b) observed image.

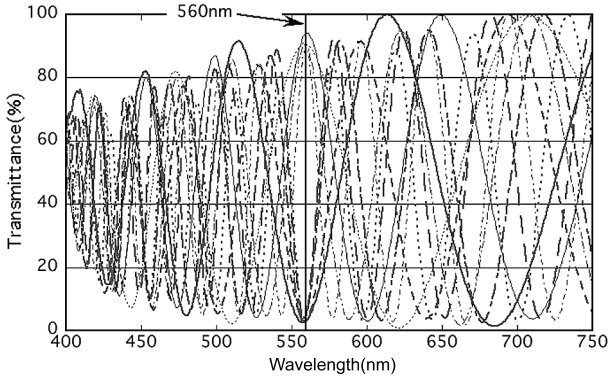


Fig. 8　Spectral transmittance of each pixels of the device. Bold and thin lines indicate text and background pixels, respectively.

Table 1　Optical characteristics of band-pass-filters for illumination.

Filter No.	Peak wavelength (nm)	FWHM (nm)
#1	497	14.0
#2	513	10.4
#3	534	9.3
#4	556	13.4
#5	599	12.5
#6	635	10.3
#7	643	17.0
#8	670	14.5

過率がすべて極大値となっている．したがって，このデバイスを 560 nm の単色光で照明すれば，文字を明瞭に観察できることが期待される．また，500 nm や 670 nm などキー波長以外では，文字部，背景部ともに透過率に規則性はみられないため，画像はスクランブルがかかった状態となり，文字は認識できないことが予想される．

画像の観察に用いた光源は，497 nm, 513 nm, 534 nm, 556 nm, 584 nm, 599 nm, 635 nm, 643 nm, 670 nm の単色光と白色光である．光源は 100 W ハロゲンランプ（ショット日本社，MegaLight100）を用い，アクリル性の拡散板を用いて均一照明とした．この白色光と試料デバイスの間に狭帯域バンドパスフィルターを取り付けて，単色光照明とした．バンドパスフィルターの光学特性を Table 1 に示す．

Fig. 9 に，それぞれの光源によるデバイスの再生結果を示す．キー波長に最も近い 556 nm 単色光での再生像において，アルファベットの T の文字が明瞭に観察できる．そ

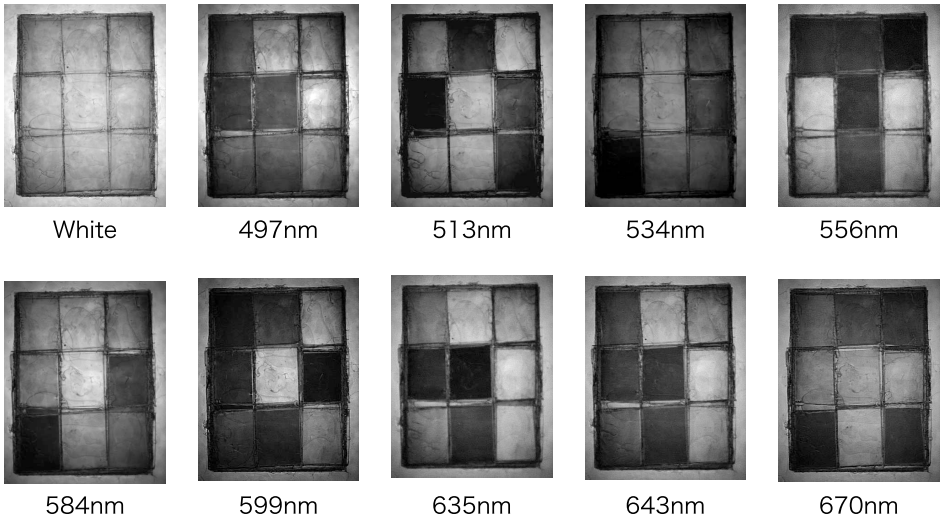


Fig. 9　Observation results of the information hiding device for changing the wavelength of illumination.

れ以外の波長では，規則性のみられない透過光強度分布となっており，文字は認識できない．前章で述べたシミュレーションで得られたパターンとは異なる透過光強度分布となっているが，これは，シミュレーションではフィルム材料の複屈折の波長分散特性を考慮していないためと考えられる．

白色光照明下での像再生においては，すべての画素が白色で観察されることが望ましい．潜像を予想させることは，暗号解読の引き金となりうるからである．Fig. 9 に示した白色光照明では，デバイス全体が一様に白色として観察された．すなわち，このデバイスの情報は白色光照明下では潜像化ができているといえる．

以上により，提案した情報セキュリティーデバイスの基本特性が確認できた．

5.　偏光変調式視覚復号型暗号への応用

前述のように，PL-VSSS は，単一画素による情報の符号化が可能なため，秘匿画像の画質を落とさない利点がある．高次複屈折デバイスを用いても，この原理をそのまま応用することが可能である．つまり，式（2）における ϕ を四分の一波長板の主軸方位によって変調される光強度の変調量に置き換えればよい．

複屈折量 Δ，主軸方位 θ の複屈折試料が平行ニコル間に置かれたときの光透過率 $I_{\Delta,\theta}$ は，入射光量を I_{in} として次式で表される．

$$I_{\Delta,\theta}=\frac{I_{\mathrm{in}}}{8}(3+\cos\Delta+\cos 4\theta-\cos\Delta\cdot\cos 4\theta) \qquad (5)$$

式（5）は，光透過率に対して複屈折量 Δ と主軸方位 4θ とは同等に寄与することを示している．したがって，PL-VSSS において，波長板の主軸方位 θ を変化させるかわりに複屈折量 Δ を変化させても，同じ特性が得られる．

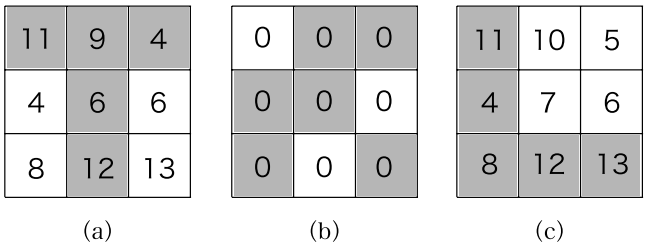


Fig. 10　Design of experimental device for application of visual cryptography. Number and color in each pixel indicate order number and phase of birefringence, respectively. Gray corresponds to π and white corresponds to 0. (a) Secret key, (b) decode mask and (c) decoded image.

本報では，二値化画像の重ね合わせによる応用を例示する．光透過率が最大のときを 1，最小のときを 0 とすると，式（2）において $\phi=0$ または 2π のときを 1，$\phi=\pi$ のときを 0 として符号化できる．いま，暗号情報を 2 つの物理キーに分けることを考える．複屈折量と光透過率との関係は $\Delta=2\pi$ の周期性があるため，復号される画素の符号は排他的論理和演算（XOR）で記述できる．

Fig. 10 (a)，(b) に 2 つの物理キーの複屈折配列を示す．(a) は，Fig. 6 と同じものである．両者を重ね合わせたときの複屈折配列は，同図 (c) のようになる．したがって，復号画像はアルファベットの文字 L が表示されることが予想される．この例では，(a) のみの観察で表示されるアルファベットの T はダミーとなり，復号画像として得られる L が暗号となる．

2 つの物理キーと復号画像の観察結果を Fig. 11 に示す．照明光は前章と同じである．上段が復号画像，中段がマス

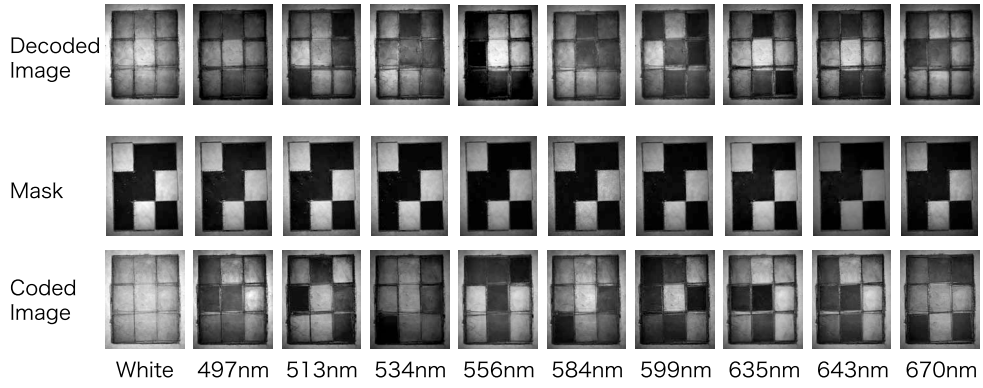


Fig. 11　Experimental results of viewing image in visual cryptography.

ク，下段が情報記録鍵の画像である．キー波長に近い 556 nm 照明の画像をみると，2 つの物理キーの XOR 演算結果が復号画像に等しくなっていることがわかる．そして，復号画像はアルファベットの文字 L が表示されている．それ以外の波長については，画像にスクランブルがかかった状態となっていて，正しい波長で観察しない限り秘匿情報が表示されないことがわかる．これは，前章で示した単板での観察結果と同様である．

中段の画像は，白色光を含めたすべての波長において同じパターンを示している．これは，複屈折次数を $N=0$ としたためである．すなわち，$\phi=\pi$ はゼロ次の半波長板となっていて，この場合には ϕ の波長誤差が小さくなるため，波長によらず同じパターンが表示される．Imagawa らによって提案された PL-VSSS は $N=0$ であるため，白色光を含めたすべての波長で XOR 演算が成り立つ構成となっている．これに対して，本報で提案する高次複屈折デバイスを用いた場合には，波長によって表示されるパターンが異なる．

秘匿キーとして波長が追加されると，暗号に対する攻撃者は物理キーの重ね合わせ位置を調整することに加えて，波長を走査して表示画像を探すことになる．したがって，暗号解読に長時間を要することになるため，攻撃に対して強い暗号となっているといえる．ここで示した例では，キー波長でダミー情報が表示される構成をとった．しかし，いったんダミー情報が表示されキー波長が明らかになると，復号に際しての暗号解読のリスクが高くなる．ダミー情報を表示する波長とキー波長とを別に設定することで，この問題は解決できると考えられる．

以上のように，提案したデバイスは，PL-VSSS に適用できることが示された．

6. ま　と　め

光の波長を暗号キーとした視覚復号型情報セキュリティーデバイスを提案し，その基本特性を示した．このデバイスは，高次複屈折の複屈折位相を配列することで文字等の情報を表し，複屈折次数を配列に対してランダムに配置することにより，情報を秘匿することが特徴である．本報では，シミュレーション計算において情報の秘匿性を高めるための設計指針として，R_0 値が有効であることを示した．また，位相差フィルムを積層したデバイスを試作し，白色光と単色光照明のもとでの観察実験を行った．その結果，キー波長で照明したときだけ意味のある情報画像が得られ，それ以外の条件では画像にスクランブルがかけられた状態になり，情報が秘匿されることが示された．

この方法は，偏光子と，単色光源だけで像再生が可能であるため，特別な再生機器が不要であることから，デバイスを手で持った状態でも容易に観察ができる．単色光源としては，光学フィルターや LED，レーザーなどを使うことができる．これに対して，キー波長がわからないときには，例えばモノクロメーターなどの特殊な分光器機に偏光光学系を組み合わせて，逐一波長を走査する必要がある．

最後に，このデバイスを用いて，PL-VSSS への応用を示した．秘匿キーとして波長が追加されると，暗号に対する攻撃者は，物理キーの重ね合わせ位置を調整することに加えて波長を走査して表示画像を探すことになるため，暗号解読に長時間を要することになる．したがって，本手法は，攻撃に対してより強い暗号となっているといえる．

文　　献

1）結城　浩：新版　暗号技術入門（ソフトバンククリエイティブ（株），2010）pp. 13–17.
2）渡部　叡：“第 9 章　形の知覚”，視覚の科学（写真工業出版，1981）pp. 134–146.
3）Y. Hayasaki, Y. Matsuba, A. Nagaoka, H. Yamamoto and N.

Nishida: “Hiding an image with a light-scattering medium and use of a contrast-discrimination method for readout,” Appl. Opt., **43** (2004) 1552–1558.
4) S. Fukushima, T. Kurokawa and Y. Sakai: “Image encipherment based on optical parallel processing using spatial light modulators,” IEEE Trans. Photon. Technol. Lett., **3** (1991) 1133–1135.
5) P. Refregier and B. Javidi: “Optical image encryption based on input plane and Fourier plane random encoding,” Opt. Lett., **20** (1995) 767–769.
6) R. A. Lee, P. W. Leech, L. D. McCarthy and G. F. Swiegers: “New applications of modulated digital images in document security,” Proc. IEEE, **6075** (2006) 60750c.
7) M. Naor and A. Shamir: “Visual cryptography,” Lect. Notes Comput. Sci., **950** (1994) 1–12.
8) M. Iwamoto and H. Yamamoto: “The optimal n-out-of-n visual secret sharing scheme for gray-scale images,” IEICE Trans. Fundam., **E85-A** (2002) 2238–2247.
9) H. Koga and H. Yamamoto: “Proposal of a lattice-based visual secret sharing scheme for color and gray-scale images,” IEICE Trans. Fundam., **E81-A** (1998) 1262–1269.
10) H. Koga, M. Iwamoto and H. Yamamoto: “An analytic construction of the visual secret sharing scheme for color images,” IEICE Trans. Fundam., **E84-A** (2001) 262–272.
11) Y.-C. Hou and S.-F. Tu: “A visual cryptographic technique for cromatic images using multi-pixel encoding method,” J. Res. Pract. Inform. Technol., **37** (2005) 179–191.
12) S.-C. Tai, C.-C. Wang and C.-S. Yu: “Visual secret sharing watermarking for digital image,” Informatica, **26** (2002) 381–388.
13) H. Yamamoto, Y. Hayasaki and N. Nishida: “Securing information display by use of visual cryptography,” Opt. Lett., **28** (2003) 1564–1566.
14) H. Yamamoto, Y. Hayasaki and N. Nishida: “Secure information display with limited viewing zone by use of multi-color visual cryptography,” Opt. Express, **12** (2004) 1258–1270.
15) H. Yamamoto, Y. Hayasaki and N. Nishida: “Secure information display with two limited viewing zones using two decoding masks based on visual secret sharing scheme,” Jpn. J. Appl. Phys., **44** (2005) 1803–1807.
16) F. Liu, C. K. Wu and X. J. Lin: “The allignment problem of visual cryptography schemes,” Des. Codes Cryptogr., **50** (2009) 215–227.
17) R. Shogenji and J. Ohtsubo: “Hiding information using a checkered pattern,” Opt. Rev., **16** (2009) 517–520.
18) T. Imagawa, S. Suyama and H. Yamamoto: “Visual cryptography using polarization-modulation films,” Jpn. J. Appl. Phys., **48** (2009) 09LC02.