新しい光学的暗号化技術

的場　修・志村　努・黒田　和男

コピー機やコンピューターとその周辺機器の普及に伴い，紙幣，クレジットカード，パスポート等の偽造が大きな社会問題となっている．また，コンピューターネットワークの発展により，個人情報，インターネット商取引，生活インフラに関する制御信号等のさまざまな情報がネットワークを経由して伝達されることなどから，暗号化技術がますます重要になると考えられる．

現在，主な電子暗号化技術[1]としては，RSA（発明者Rivest，Shamir，Adlemanの頭文字）暗号に代表される公開鍵暗号やDES（data encryption standard）等の秘密鍵暗号がある．RSA暗号の場合には，基本的に素因数分解の計算に要する時間が膨大になることに起因して安全性を保証するものである．しかしながら，量子コンピューターの提案により素因数分解の高速処理が原理的に可能であることが示されている．DES等の秘密鍵暗号では，基本的に鍵のビット長を長くすることや同じ鍵を複数回用いないことで安全性を保証する．解読は，全数検索をすることにより原理的に可能であるが，暗号を解く鍵をもたない場合には，鍵の全数が天文学的数字になり実時間で解読できないように計算量的に安全であることを保証するものである．

一方，偽造防止用にクレジットカードに添付されているホログラムのように，光を用いたセキュリティー技術の開発が行われている．現状では，ホログラム自体を使った認証システムの実用化には至っていないが，光の有する位相，偏光情報は人間の目やCCDカメラでは検出できないため，新しい暗号化技術の開発が期待できる．本稿では，光のもつ物理量（振幅，位相，偏光，波長）を駆使した，より安全性の高い新しい暗号化技術に関する研究を紹介する．特に，ランダム位相コードを用いた光暗号化技術を中心に話を進める．本稿で紹介する光暗号化技術も全数検索により解読可能であるが，鍵の多次元化による計算量的安全性を保証するものである．

東京大学生産技術研究所（〒153-8505 東京都目黒区駒場 4-6-1）
E-mail: matoba@iis.u-tokyo.ac.jp

1. セキュリティー認証システム

セキュリティーシステムへのニーズのひとつに，顔，指紋，光彩等の個人特有の情報を用い個人認証を行うシステムの開発がある．現在までに提案されている光学システムの多くは，相関演算によるパターンマッチングにより識別を試みている．光学的相関演算は光の空間並列性により高速に実行することが可能であり[2]，逐次処理を行う電子計算機よりも有利である．相関演算を行う光学系としては，VanderLugt型相関器や結合変換相関器（joint transform correlator; 以下JTC）が用いられる．認識力向上のために，フィルターの位相化[3]，joint transform power spectrum（JTPS）の非線形化[4]等が提案されている．近年，個人認証の有効な方法として，ランダム位相コードを用いる方法が提案されている[5]．本節ではJTCシステムをもとにその原理を説明する．入力面に入力信号$f(x,y)=o(x,y)\exp\{-\mathrm{j}n(x,y)\}$と参照信号$g(x,y)=\exp\{-\mathrm{j}h(x,y)\}$をそれぞれ，図1のように配置する．入力信号$f(x,y)$はクレジットカード等に添付されているものとする．$o(x,y)$はたとえば，顔，指紋等の振幅変調物体である．$n(x,y)$，$h(x,y)$は，統計的に$[0,\ 2\pi]$の一様分布に従うランダム変数であり，互いに独立である．入力信号に添付されている位相マスク$\exp\{-\mathrm{j}n(x,y)\}$は，人間の目やCCDカメラ等の強度検出デバイスでは検出できない．参照信号用位相マスク$g(x,y)$は，ハードディスクやホログラフィックメモリー等の大容量記録媒体に記録されており，高速読み出し可能であるとする．

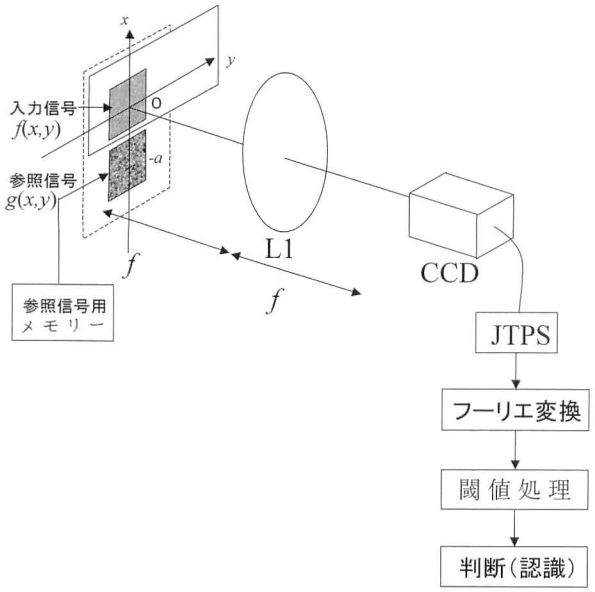

図1　JTC に基づくランダム位相マスクを用いた認識装置.

入力面での合成入力信号 $s(x,y)$ は,

$$s(x,y)=f(x,y)+g(x+a,y) \qquad (1)$$

となる. レンズL1によるフーリエ変換のあと CCD で検出される JTPS, $S(\nu,\eta)$ は,

$$\begin{aligned} S(\nu,\eta)&=|F(\nu,\eta)+G(\nu,\eta)\exp(\mathrm{j}a\nu)|^2 \\ &=|F(\nu,\eta)|^2+|G(\nu,\eta)|^2+F^*(\nu,\eta)G(\nu,\eta) \\ &\quad \exp(\mathrm{j}a\nu)+F(\nu,\eta)G^*(\nu,\eta)\exp(-\mathrm{j}a\nu) \end{aligned} \qquad (2)$$

となる. *は複素共役を表し, $F(\nu,\eta)$, $G(\nu,\eta)$ は, それぞれ $f(x,y)$, $g(x,y)$ の光学的フーリエ変換を表す. 右辺第4項をフーリエ変換すると, $f(x,y)\star g(x+a,y)$ が得られる. ★は correlation を表す. つまり, 2つのランダム位相マスクの相関演算が導入されている. 2つのランダム位相マスクが同じ場合には, 鋭い相関ピークが検出されるが, 2つのマスクが異なる場合には無相関となり, 相関信号は白色雑音化されたままで相関ピークは検出されない. 適切な閾値処理をすることで, 本物か偽造かの判断をすることができる.

この方法では, まず添付されている位相マスクのみを取り外して使用することができないことが重要である. マスクの取り外しが, マスク自体に損傷を与えるよう, 接着されている必要がある. また, 干渉計測等により複製されないことも重要なため, 凹凸形状よりは内部に3次元屈折率分布をもたせるなどの工夫が必要である.

ランダム位相マスクの代わりにランダム偏光マスクを利用する方法も提案されている[6]. 偏光情報は, 位相情報同様, 人間の目や CCD カメラでは検出されない. ランダム偏光マスクが一致しない場合には, 可干渉性が劣化し,

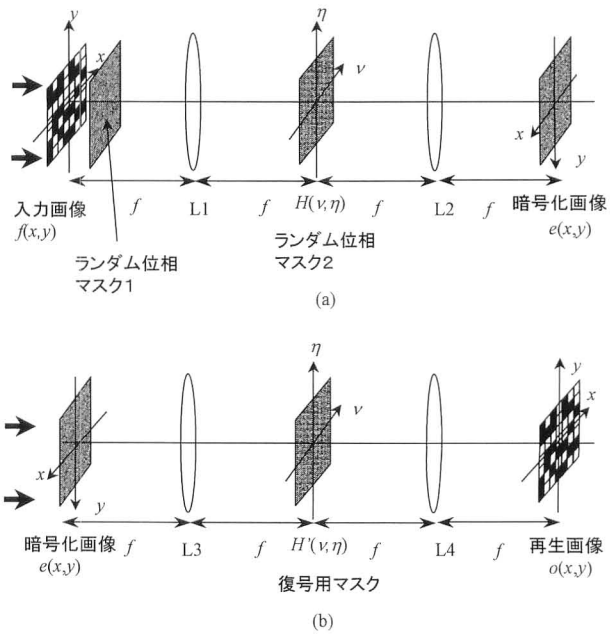

図2　二重ランダム位相符号化法. (a) 暗号化, (b) 復号.

CCD で検出される JTPS の可視度が低下するため, 相関ピーク値が減少する. 適切な閾値処理により, 本物と偽造の区別が可能である.

2.　二重ランダム位相コードによる暗号化

Réfrégier と Javidi は, 入力面とフーリエ変換面に2枚のランダム位相コードを用い, 原画像の暗号化と復号を行う方法を提案した[7]. 原画像は2枚のランダム位相コードにより白色雑音化される. その原理図を図2に示す. 暗号化を行う光学系（図2(a) 参照）は, VanderLugt 型相関光学系である. 入力画像は, 2次元ランダム位相コードと積算された後, レンズL1によりフーリエ変換される. フーリエ面には, もう1枚の2次元ランダム位相コードが置かれている. 原画像を $f(x,y)$, 入力面のランダム位相コードを $\exp\{-\mathrm{j}n(x,y)\}$, フーリエ面でのランダム位相コードを $\exp\{-\mathrm{j}H(\nu,\eta)\}$ とすると暗号化された信号 $e(x,y)$ は次式のようになる.

$$e(x,y)=f(x,y)\exp\{-\mathrm{j}n(x,y)\}\otimes F[\exp\{-\mathrm{j}H(\nu,\eta)\}] \qquad (3)$$

式（3）で, (x,y) は入力・出力面の座標軸, (ν,η) はフーリエ面の座標軸, ⊗は convolution, $F[\cdot]$はフーリエ変換を表す. $n(x,y)$, $H(\nu,\eta)$ は統計的に$[0,2\pi]$の一様分布に従うランダム変数であり, 互いに独立である.

復号用光学系（図2(b) 参照）では, 暗号化された信号 $e(x,y)$ を再びフーリエ変換し, フーリエ面において復号用の位相マスク $H'(\nu,\eta)$ と積算させる. レンズL4によるフーリエ変換によって, 復号された画像 $o(x,y)$:

$$o(x,y)=e(x,y)\otimes F[\exp\{-\mathrm{j}H'(\nu,\eta)\}] \quad (4)$$

が再生される．ここで，復号用の位相マスクが暗号用の位相マスクの複素共役，つまり $H'(\nu,\eta)=-H(\nu,\eta)$ のときには，$o(x,y)=f(x,y)\exp\{-\mathrm{j}n(x,y)\}$ となる．出力面でCCDカメラ等の強度検出器を用いると，原画像の強度信号 $|f(x,y)|^2$ が再生される．復号用の位相マスクが暗号用の位相マスクの複素共役でない場合には，フーリエ面での位相がキャンセルされずに残留するため，白色雑音化されたままになる．ランダム位相マスクとして，画素数，位相階調数の多い位相変調型空間光変調器を用いた場合を考えると，2次元ランダム位相マスクの総数は膨大な数になり，暗号時のマスク情報なしで実時間で解読することは非常に困難である．なお，入力面のランダム位相マスクは，入力像が正の実数である場合には，復号時に用いる必要はない．しかしながら，入力面のランダムマスクは，位相回復アルゴリズムによる解読を防ぐ働きをするため，暗号化に必要不可欠である[7]．

VanderLugt型相関光学系の弱点として，フーリエ変換面に位相共役マスクを厳密に置く必要があることが挙げられる．また，復号時にマスクを高速に置き換える必要がある場合には，マスクの更新や位置制御が実用化への大きな課題となる．これを解決する方法として，Nomuraらは，JTCに基づく暗号化・復号システムを提案している[8]．この方法では，フーリエ面に置かれる位相マスクの逆フーリエ変換パターンを入力面に配置する必要がある．位相マスクの逆フーリエ変換パターンは複素分布になり，かつ入力空間に広がる．現在，複素分布を高速かつ精密に表示でき，実用に耐えうるデバイスがないため，Nomuraらはバイナリー計算機ホログラム（CGH）を使った暗号化・復号方法を提案している．バイナリーCGHは，強誘電性液晶デバイスや半導体デバイスを用いると高速表示・書き換えが可能である．

二重ランダム位相コードにより暗号化された信号を用い，光暗号化通信を行う試みがある[9,10]．光暗号化通信を行うひとつの方法としては，超短光パルスを用いた時空間変換系により，暗号化された空間信号を時間信号に変換した後，光ファイバーを通して伝送し，受信側で復号するシステム[9]がある．別の方法としては，ディジタルホログラフィー技術[11]を用いる方法が提案されている[10]．ディジタルホログラフィーは，光学系で得られた干渉像をCCDカメラで取り込み，計算機上で物体を再生する技術である．近年のCCDの大画素化により良好な3次元再生像が得られている．暗号化された信号は複素数のため，暗号化された複素信号を参照光と干渉させ，CCDカメラで強度分布として記録する．記録された干渉強度信号は，暗号化されておりその情報だけでは復号することはできない．ここで，復号用マスクの情報は，あらかじめディジタルホログラフィー技術により記録され，正規の受信者に送られているものとする．

二重ランダム位相マスクにより暗号化された信号は，ホログラムの原理のように，原画像の各点の情報が暗号化画像全体に分散されている．そのため，暗号化画像の一部の情報を失った場合にも原画像を再生することが可能になる[12,13]．このことは，二重ランダム位相暗号化がノイズに対して強いことも示している．暗号化画像に原画像と類似したパワースペクトルをもつcolored noiseが加えられた場合を考える．通常の周波数フィルターでは除去するのが困難であるが，再生時にランダム位相マスクによりcolored noiseが白色雑音化され，再生画像全体に広がるため，閾値処理によりノイズを除去することができる．

3. セキュリティーホログラフィック光メモリー

二重ランダム位相コードによる光学的暗号化方法をホログラフィックメモリーに利用することにより，実用的に安全なメモリーシステムを構築することができる[14-18]．ホログラフィックメモリー[19-23]は，近年アメリカを中心に実用化に向け活発に研究されている．ホログラフィックメモリーの特徴としては，高密度大容量記録と2次元画像データに対する高速読み出しが可能であることが挙げられる．暗号化には，原画像を暗号化する方法[7,24]と参照光を暗号化する方法[25]，その両方を用いる方法が考えられる．参照光を暗号化する方法は，体積ホログラムのブラッグ条件を利用して，記録された画像そのものの読み出しを制限するものである．参照光の暗号化は，拡散板等のランダム位相コード[25]やファイバーから射出されたスペックルパターン[26]を利用する方法が考えられる．原画像を暗号化する方法は，メモリーシステムと離れた遠隔地にデータを送信する場合にも利用可能である．

ここでは，著者らが研究を行っている，二重ランダム位相コードによる光暗号化技術を利用したセキュリティーホログラフィック光メモリーシステムについて説明する．原画像の暗号化に用いる情報としては，2枚の2次元ランダム位相マスクとその3次元位置座標，および波長である．光のもつ物理量を鍵として多く用いることにより，鍵の総数が膨大な数になり，より安全なメモリーシステムを構築することができる．

はじめに，2次元ランダム位相マスクのみを用いたセキュリティーメモリーシステム[14]を紹介する．図3に光学

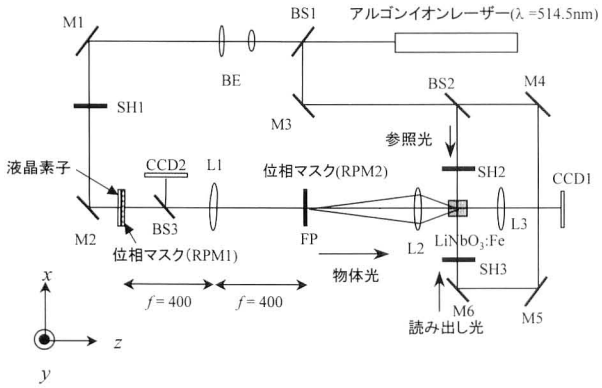

図3　光学系．L's：レンズ；BS's：ビームスプリッター；M's：ミラー；RPM's：ランダム位相マスク；SH's：シャッター；FP：フーリエ面，BE：ビームエキスパンダー；CCD's：CCDカメラ．

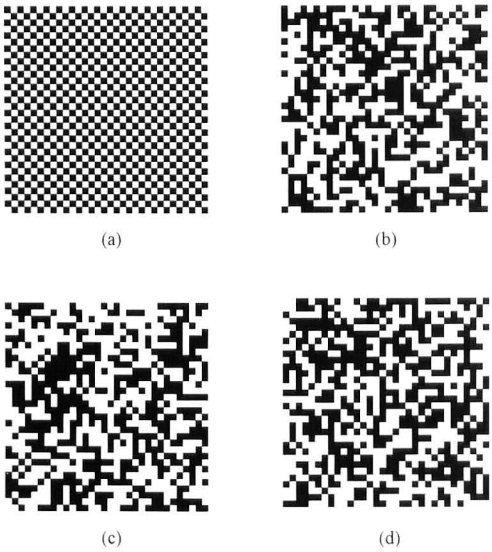

図4　原画像．

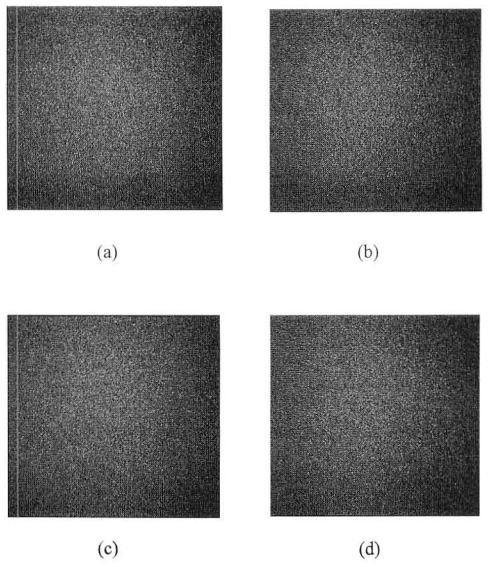

図5　暗号化画像．

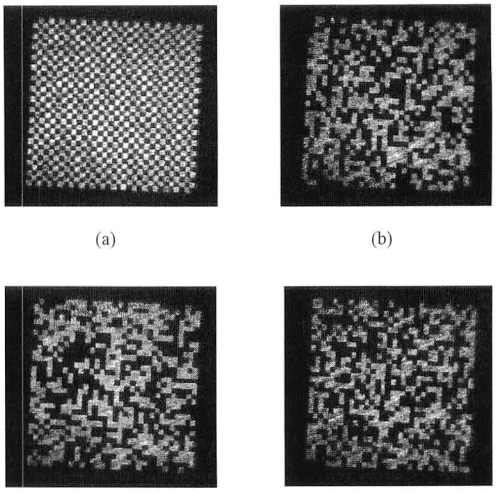

図6　正しいマスクにより再生された画像．

系を示す．入力画像は振幅変調物体であり，2枚の偏光板に挟まれた液晶表示素子に表示される．1枚目のランダム位相マスク（RPM1）は，入力画像に密着されている．ランダム位相マスクと積算された入力画像は，レンズL1により光学的フーリエ変換された後，フーリエ面（FP）に置かれたもう1枚のランダム位相マスク（RPM2）と積算される．この2枚のランダム位相マスクにより，原画像は白色雑音化される．暗号化された信号は式（3）で与えられ，CCD1で記録される．このシステムでは，暗号化された画像のフーリエ変換像を平面波の参照波とともにホログラフィックに記録する．再生時には，読み出し光として参照光の位相共役光（この場合，対向する平面波）を用いる．位相共役再生光が，記録時に用いたランダム位相マスクを再び通過することによって，暗号時に与えられた位相がキャンセルされ，原画像がCCD2に再生される．記録時と異なるランダム位相マスクを用いた場合には，位相が補償されずに，再生像は白色雑音化されたままである．位相共役光再生により暗号化・復号共通のランダム位相マスクを用いることができる．

原理確認実験としてフォトリフラクティブ$Fe:LiNbO_3$結晶中に角度多重記録により4枚の画像を記録した．角度多重は結晶を回転させることにより実行される．図4，5に入力画像と暗号化画像を示す．2枚のランダム位相マスクにより，原画像は白色雑音化されていることがわかる．図6に，記録時と同じランダム位相マスクによる再生像を示す．図4，6より原画像が正しく再生されていることがわかる．閾値処理をすることにより，4枚の画像に対してビット誤り率ゼロで再生することができた．記録時と異なる位相マスクを用いた場合には，図5と同様の白色雑音化

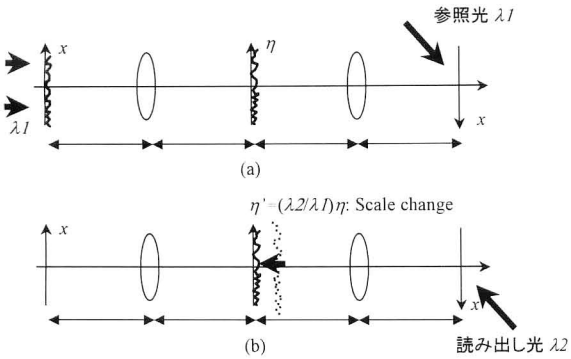

図7　2次元ランダム位相コードと波長コードを組み合わせたセキュリティー光メモリーシステムの原理図．(a) 記録系，(b) 再生系．

された画像が再生され，原画像を知ることはできない．

上述のシステムでは2つのランダム位相マスクは入力面・フーリエ面に置かれていたが，これをフレネル領域に置くことによりマスクの3次元位置情報を新しい鍵として利用することができる[15]．この場合，仮に復号用鍵のランダム位相マスクが盗まれた場合でもマスクの3次元位置情報を知らなければ原画像を再生することができない．さらに，位相マスクを光軸に垂直に置かない場合には，角度情報も鍵として用いることができる．

ここで，マスクの3次元位置の総数を簡単に求めてみる．位相マスクの大きさ $L_x \times L_y$，画素サイズ $\Delta x \times \Delta y$，光軸方向のマスク位置の取りうる数 N_z とすると，2枚のランダム位相マスクによる3次元位置の総数 N は，

$$N = \{(L_x/\Delta x)(L_y/\Delta y) N_z\}^2 \qquad (5)$$

となる．図3の実験システムでは，$L_x = L_y = 25$ mm，$\Delta x = \Delta y = 6\ \mu$m，$N_z = 100$ であり，3次元位置の総数は 3×10^{18} になる．これは，1秒間に 10^9 点検索した場合でも，全数検索が終了するのに約95年要することになり実用上安全であるといえる．図3の実験システムを用い，原理確認を行った．その結果，正しいマスクを正しい位置で用いた場合は，ほぼ完全な再生像が得られたが，間違った位置で再生した場合は原画像が再生されず，白色雑音化されたままであった[15]．

さらに波長情報を新しい鍵として用いる方法も提案されている[16]．このシステムでは，暗号化した画像をフーリエ面ではなく結像面でホログラフィックに記録する．図7に原理図を示す．記録時の波長を λ1，再生時の読み出し光の波長を λ2 とする．$\lambda 2 \neq \lambda 1$ でかつブラッグ条件を満たす読み出し光を用いた場合を考える．波長の変化によりフーリエ面に再生される光電場分布のスケールが（λ2/λ1）に比例して変化する．ランダム位相マスクの各画素の大きさが無限小のときには，このスケール変化により光

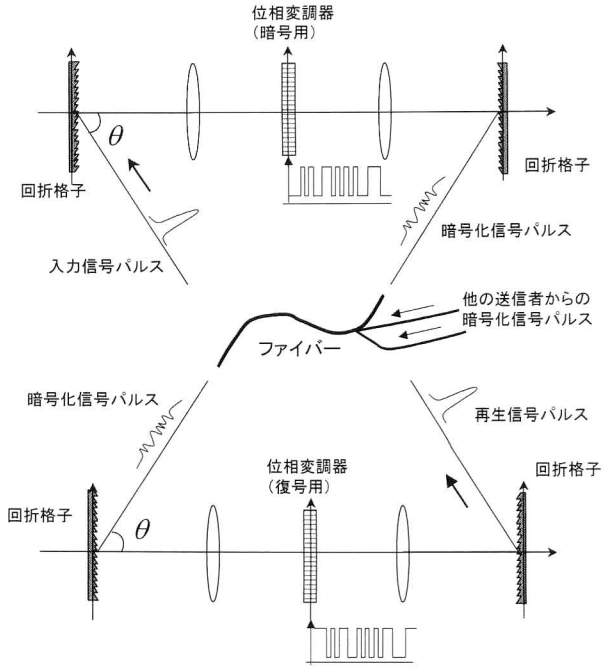

図8　パルス整形による光暗号化通信の原理図．

軸上のみ位相補償が行われるが，その他の部分では位相補償が行われない．したがって再生信号はランダム信号のままである．原理確認実験として，フーリエ面にのみランダム位相マスクを用い，波長 514.5 nm でホログラムを記録した．記録時と同じ波長，同じランダム位相マスクで再生した場合には，ほぼ完全な原画像が再生されたが，波長 632.8 nm で再生した場合には，白色ノイズのままであった．実験では記録時と再生時の波長差が 118 nm と大きいが，ランダム位相マスクの画素サイズを小さくすることにより，波長コードの間隔を小さくすることができる．1次元二値信号を用いた数値計算では，位相マスクの画素サイズ 320 μm のときに再生像が暗号化画像とほぼ同じになる波長差は 40 nm になる．今後，記録光と読み出し光の波長差による再生像の詳細な評価を行う必要がある．

上述のように，2次元ランダム位相マスクと3次元位置情報および波長を組み合わせることにより，実用的に安全なホログラフィック光メモリーシステムを構築することができる．また，入力信号を位相情報または，偏光情報として表示することにより，さらに安全なメモリーシステムの開発が期待できる．

4.　その他の光暗号化・復号技術

4.1　超短光パルスを用いた光暗号化通信

1次元ランダム位相マスクによる超短光パルスの暗号化および光通信への応用が Weiner らにより提案されている[27,28]．Weiner らの方法では，超短光パルスを用いた波

形整形システム（図8）において，各スペクトルに対してバイナリーランダム位相コードによる変調を行い，暗号化する．この暗号化によりパルス幅が広がり，その包絡線はランダムノイズ化される．そのため，ピーク強度は十分小さくなる．暗号化されたパルスは，光ファイバーを通して，受信者へと配布される．このとき，他の送信者からの暗号化されたパルスと重ね合わされた後に配布される．各受信者は，暗号化時に用いたランダム位相コードの複素共役分布を用いて再びパルス整形（復号）し，オリジナル信号を得る．他の受信者用の信号は，復号コードが異なるため白色雑音化されたままとなり，閾値処理により除去することが可能である．近年のフェムト秒レーザー開発の急速な進展により，時空間変換系を用いた毎秒テラビットを超えるデータの送信が可能なため，次世代の暗号化通信システムへの応用が期待できる．また，超短光パルスを用いた2次元画像の送信方法も提案されており[29]，ランダム位相マスクと組み合わせることで，光暗号化された2次元，3次元ディスプレイ等の応用も期待される．

4.2 排他的論理和演算による暗号化

排他的論理和（XOR）演算による暗号は広く知られている暗号化方法のひとつである．原信号をI，暗号化鍵をK，暗号化された信号をE，復号鍵をK，復号信号をDとすると，暗号化，復号はそれぞれ，

$$E=I*K \qquad (5)$$

$$D=E*K=I*K*K=I \qquad (6)$$

となる．ここで，＊はXOR演算を表す．光を用いると2次元画像データに対して，並列にXOR演算を実行できるため，高速処理が可能である[30,31]．Hangらは，光学的XOR演算に2つの液晶を用いた偏光コード化を利用している[31]．鍵となる2次元ランダム信号の発生には，線形フィードバックシフトレジスターを用いている．また，2次元ランダム信号の光学的生成方法も提案されている[32,33]．

光のもつ物理量（振幅，位相，偏光，波長）を制御することによる光暗号化技術を紹介し，それに基づくセキュリティー光情報処理システムについて述べた．特にランダム位相マスクを用いた暗号化・復号方法，セキュリティー認証システム，ホログラフィックメモリーシステム，光通信システムを紹介した．ランダム位相マスクによる暗号化方法では，解読は全数検索をすることにより原理的に可能である．暗号を解く鍵をもたない場合には，鍵の全数が天文学的数字になり実時間で解読できないように計算量的に安全であることを保証する．光暗号化技術は，次世代メモリーとして期待されているホログラフィック光メモリーやフェムト秒パルスレーザーを用いた超高速光通信に組み込むことが可能であり，今後の研究の進展が期待される．また，光による公開鍵暗号方法の開発も望まれる．

文　献

1) 池野信一，小山謙二：現代暗号(電子情報通信学会，1986).
2) J. W. Goodman: *Introduction to Fourier Optics*, 2 nd ed. (McGraw-Hill Companies, New York, 1996).
3) J. L. Horner and P. D. Gianino: "Phase-only matched filtering," Appl. Opt., **23** (1984)812-816.
4) B. Javidi: "Nonlinear joint transform correlators," *Real-time Optical Information Processing*, eds. B. Javidi and J. L. Horner(Academic Press, Boston, 1994) pp. 115-183.
5) B. Javidi and J. L. Horner: "Optical pattern recognition for validation and security verification," Opt. Eng., **33** (1994) 1752-1756.
6) T. Nomura and B. Javidi: "Polarization encoding for optical security systems," Proc. SPIE, **3804** (1999)196-203.
7) P. Réfrégier and B. Javidi: "Optical image encryption based on input plane and Fourier plane random encoding," Opt. Lett., **20** (1995) 767-769.
8) T. Nomura and B. Javidi: "Optical encryption using joint transform correlator architecture for robust alignment," Proc. SPIE, **3804** (1999) 180-187.
9) O. Matoba and B. Javidi: "Secure ultrafast communication using time-to-space converters," Appl. Opt., **39** (2000) 2975-2981.
10) B. Javidi and T. Nomura: "Securing information by use of digital holography," Opt. Lett., **25** (2000) 28-30.
11) I. Yamaguchi and T. Zhang: "Phase-shifting digital holography," Opt. Lett., **22** (1997) 1268-1270.
12) B. Javidi, A. Sergent, G. Zhang and L. Guibert: "Fault tolerance properties of a double phase encoding encryption technique," Opt. Eng., **36** (1997) 992-998.
13) F. Goudail, F. Bollaro, B. Javidi and P. Réfrégier: "Influence of a perturbation in a double phase-encoding system," J. Opt. Soc. Am. A, **15** (1998) 2629-2638.
14) O. Matoba and B. Javidi: "Encrypted optical storage with angular multiplexing," Appl. Opt., **38** (1999) 7288-7293.
15) O. Matoba and B. Javidi: "Encrypted optical memory system using three-dimensional keys in the Fresnel domain," Opt. Lett., **24** (1999) 762-764.
16) O. Matoba and B. Javidi: "Encrypted optical storage with wavelength-key and random phase codes," Appl. Opt., **38** (1999) 6785-6790.
17) B. Javidi, G. Zhang and J. Li: "Encrypted optical memory using double-random phase encoding," Appl. Opt., **36** (1997) 1054-1058.
18) G. Unnikrishnan, J. Joseph and K. Singh: "Optical encryption system that uses phase conjugation in a photorefractive crystal," Appl. Opt., **37** (1998) 8181-8186.
19) J. F. Heanue, M. C. Bashaw and L. Hesselink: "Volume holographic storage and retrieval of digital data," Science, **265** (1994) 749-752.
20) F. H. Mok: "Angle-multiplexed storage of 5000 holograms in lithium niobate," Opt. Lett., **11**, (1993) 915-917.
21) J.-J. R. Drolet, E. Chuang, G. Barbastathis and D. Psaltis: "Compact, integrated dynamic memory with refreshed

holograms," Opt. Lett., **22** (1997) 552-554.
22) C. Denz, G. Pauliat, G. Roosen and T. Tschudi: "Volume hologram multiplexing using a deterministic phase encoding method," Opt. Commun., **85** (1991) 171-176.
23) G. A. Rakuljic, V. Leyva and A. Yariv: "Optical data storage by using orthogonal wavelength-multiplexed volume holograms," Opt. Lett., **17** (1992) 1471-1473.
24) H. Kogelnik: "Holographic image projection through inhomogeneous media," Bell Syst. Tech. J., **44** (1965) 2451-2455.
25) H. F. Heanue, M. C. Bashaw and L. Hesselink, "Encrypted holographic data storage based on orthogonal-phase-code multiplexing," Appl. Opt., **34** (1995) 6012-6015.
26) Y. H. Kang, K. H. Kim and B. Lee: "Volume hologram scheme using optical fiber for spatial multiplexing," Opt. Lett., **22** (1997) 739-741.
27) A. M. Weiner, D. E. Leaird, D. H. Reitze and E. G. Paek: "Femtosecond spectral holography," IEEE J. Quantum Electron., **28** (1992) 2251-2261.
28) A. M. Weiner, J. P. Heritage and J. A. Salehi: "Encoding and decoding of femtosecond pulses," Opt. Lett., **13** (1988) 300-302.
29) T. Konishi and Y. Ichioka: "Ultrafast image transmission by optical time-to-two-dimensional-space-time-to-two-dimensional-space conversion," J. Opt. Soc. Am. A, **16** (1999) 1076-1088.
30) S. Fukushima, T. Kurokawa and Y. Sakai: "Image encipherment based on optical parallel processing using spatial light modulator," IEEE Trans. Photonics Technol. Lett., **3** (1991) 1133-1135.
31) J.-W. Hang, C.-S. Park, D.-H. Ryu and E.-S. Kim: "Optical image encryption based on XOR operations," Opt. Eng., **38** (1999) 47-54.
32) M. Madjarova, M. Kakuta, M. Yamaguchi and N. Ohyama: "Optical implementation of the stream cipher based on the irreversible cellular automata algorithm," Opt. Lett., **22** (1997) 1624-1626.
33) 角田　貢, M. D. Madjarova, 小尾高史, 山口雅浩, 大山永昭："光学的並列演算を用いたVernam暗号手法", 光学, **27** (1997) 104-109.

(2000年2月14日受理)