研究論文

Received January 16, 1997; Accepted November 10, 1997

光学 27, 2 (1998) 104-109

# 光学的並列演算を用いたVernam暗号手法

角田　貢・Maria D. MADJAROVA・小尾　高史・山口　雅浩・大山　永昭

東京工業大学像情報工学研究施設　〒226-8503 横浜市緑区長津田町 4259

## Vernam Encryption Using Optical Parallel Processing

Mitsugu KAKUTA, Maria D. MADJAROVA, Takashi OBI, Masahiro YAMAGUCHI and Nagaaki OHYAMA

Imaging Science and Engineering Laboratory, Tokyo Institute of Technology, 4259, Nagatsuta, Midori-ku, Yokohama 226-8503

In the information systems mutually connected through network, the security technology is necessary to protect data from the leakage and the falsification. In this paper, an optical parallel processing method for high speed cryptography is proposed. Pseudo-random sequence is generated by the parallel XOR operations and the rearrangement of bit array, and Vernam cipher is generated by the XOR operation of the generated random bits and the plaintext. Using long array of bit data as a seed for random bit generation, the period of the pseudo-random sequence can be very long so that the security level of the cipher becomes high. The method for the optical implementation of the encryption and the decryption is described, and the experimental results using liquid crystal spatial light modulator are also demonstrated.

## 1. 緒　　言

今後の発展が予想されるオンライン情報ネットワークシステムは，産業・医療・情報通信などのさまざまな分野での利用が期待され，大容量データの高速な通信処理が可能なシステムが求められている．また，ネットワークを介してデータ通信を行う際には，データの安全性を確保することが重要であり，そのためには各種の暗号化技術の利用が有効である．例えば個人の医療や資産等のデータは，プライバシー保護や改竄防止等の観点からも，情報に対する不正な参照や改変等を防止することが必要と考えられている．

情報の安全性を確保するための暗号化方式に関しては，古くは軍事を目的として多くの研究がなされ，これまでに秘密鍵あるいは公開鍵を用いる暗号化方式が開発されてきた．近年では，電子商取引等でも暗号化手法の利用が検討されている．一般的に，暗号化方式の安全性と処理の負荷量はトレードオフの関係にある．例えば，安全性を高めようとすると，暗号化および復号化に要する演算量が増大することを意味している．将来のオンラインネットワークシステムでは，セキュリティーの確保されたリアルタイム処理やオン・デマンド処理が求められると考えられるため，ネットワークを用いて大容量のデータを伝送することが必要になり，暗号化処理の高速化が重要になると予測される．

一方，光のもつ高速性，並列処理性は，画像などの大容量のデータの高速処理に有効な技術と考えられ，これまで種々の光並列処理システムが提案されている[1]．本研究では，高速デジタル通信網を通じて伝送される大容量データの暗号化および復号化を光学的並列演算系を用いて実現することで，安全性と高速処理が両立したシステムの実現を目的としており，本論文では，再現性のある乱数の生成とVernam暗号化を光演算により行うシステムを提案する．

これまでに光学系を用いた暗号化手法[2,3]としては，フーリエ変換光学系を用いた研究が報告されているが[2]，データの再現性や精度の面からデジタルデータへの適用は困難である．また，画像と画像の排他的論理和演算により暗号化を行う手法が提案されているが[3]，データと同数枚の画像を用意する必要があるため，大容量のデータに対しては検討が必要である．本論文では，大容量データを暗号化するために大きな長さをもつ乱数が必要であることから，画像等の大きなビット列をキーとすることで，長周期の乱数を発生し，暗号化を行うシステムを提案する．具体的には，

E-mail: kakuta@isl.titech.ac.jp

最大長系列符号を暗号化系列として用いたVernam暗号化を光演算を用いて行う手法について述べる．また，液晶パネルを用いた実験の結果を示す．

## 2. Vernam暗号

Vernam暗号は，暗号化されるデータ系列とランダムな性質をもつ系列との排他的論理和（以下，XOR）による暗号である．ここでそれぞれを$\{d_t\}$と$\{r_t\}$とすると，$t$ビット目のVernam暗号$\{c_t\}$は，

$$c_t = d_t \oplus r_t \qquad (1)$$

により生成される．ここで⊕は，排他的論理和を示す．暗号化されるデータ系列$\{d_t\}$は平文と呼ばれ一般的にランダムな性質をもつ系列$\{r_t\}$は暗号化系列または鍵と呼ばれる．Vernam暗号では，高い乱数性を有する秘密鍵の生成がきわめて重要であり，長大な鍵を用いた場合には安全性の高い暗号化が可能である．そして，Vernam暗号の安全性は，情報理論的見地からShannonによって証明されている．しかし，安全性を確保するためには，平文よりも長い鍵が必要となるため，Vernam暗号は，大容量のデータの暗号化に対して，実用的でないとされてきた．実際には，鍵の管理等の面から，種と呼ばれるある長さの初期値から生成される擬似乱数が鍵として用いられることが多い．このような擬似乱数の周期は種の長さに依存し，一般に種の長さが大きいほどその周期も長くなる．そこで，本研究では，画像などの大きなデータを種から生成した長周期の擬似乱数を用いることで，安全性の高い暗号化を可能にする．そして，鍵としては，良好なランダム性を有する最大長系列符号を用いる．

## 3. 擬似乱数の生成

### 3.1 最大長系列符号

最大長系列符号（以下，M系列）は，Fig. 1に示すような線形フィードバックシフトレジスター回路（以下，LFSR)を用いて生成される系列の中で，周期が$2^n-1$になるものであり，以下のように生成される[4]．$n$次の原始多項式$p(x)$を

$$p(x) = x^n + p_{n-1}x^{n-1} + p_{n-2}x^{n2} + \cdots + p_1 x + p_0 \qquad (2)$$

とおくと，$p(x)$に対するシフトレジスター系列$\{r_t\}$がM系列である．ここで，$p_i \in \{0,1\}$ $(0 \le i \le n-1)$であり，原始多項式は，Watsonらによって報告されているように[5,6]，次数$n$に応じて$p_i$のセットは異なる．このような回路により生成されるM系列は，ある時刻$t$における$n$個のレジスターに保持されている内容を，$s^t_{n-1}$, $s^t_{n-2}$, $s^t_{n-3}$, …, $s^t_2$, $s^t_1$, $s^t_0$とした場合，1クロック後の時刻$(t+1)$に新たに生成される出力$r_{t+1}$は，

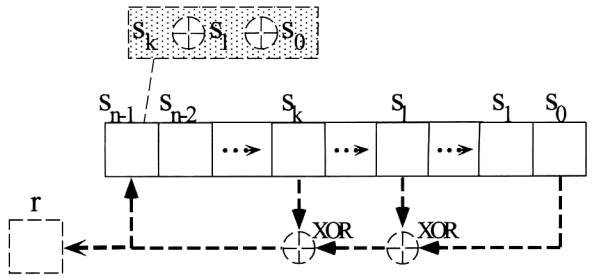



Fig. 1. The diagram of Linear feedback shift register (LFSR). For example, if the LFSR is based on the polynomial $f(x) = x_n + x_k + x_1 + 1$, the content of both register $k$ and $l$ is feedback to generate new bit, and the new bit is generated by calculation of $s_k$ XOR $s_l$ XOR $s_0$.

$$r_{t+1} = \sum_{i=0}^{n-1} p_i s_i^t \pmod 2 \qquad (3)$$

である．ここで，(mod 2)は，2を法とする演算を意味し，加法の結果，偶数の時は0，奇数の時は1となる．また同時に，最上位のレジスターの内容は，この値によって更新されるために，

$$s^{t+1}_{n-1} = r_{t+1} \qquad (4)$$

となる．また，$0 \le j \le n-2$では，

$$s^{t+1}_j = s^t_{j+1} \qquad (5)$$

となる．M系列は，式(2)～(4)で与えられるプロセスを繰り返すことで，1クロックにつき1ビットずつ生成される擬似的にランダムな系列である．M系列を生成させるためには，すべてが0以外の任意の値を初期値(時刻$t=0$)としてレジスター$s^0_{n-1}$, $s^0_{n-2}$, …, $s^0_2$, $s^0_1$, $s^0_0$にセットすればよい．つまりFig. 1において，時刻$(t+1)$でのレジスターの内容$s^{t+1}_{n-1}$は，式(3)および(4)から$s^t_k \oplus s^t_l \oplus s^t_0$である．同時に，これは生成されたM系列となるため，暗号化は，式(1)に示すように1クロックにつき1ビット行われる．次節では，時刻$t$から$(t+n)$までのビット列を暗号化するために，$n$ビットを並列生成する手法について述べる．

### 3.2 並 列 化

3.1節では，式(2)に基づく$n$次の原始多項式によってM系列が生成されることについて述べた．本節では，M系列はある時刻において各レジスターに保持されている内容と等しいということを基に，並列処理の検討を行う．

時刻$t=t_0$のおけるレジスターの状態を$s^{t_0}_{n-1}$, $s^{t_0}_{n-2}$, …, $s^{t_0}_2$, $s^{t_0}_1$, $s^{t_0}_0$とし，出力系列$\{r_t\}$は

$$r_t = s^t_{n-1} \qquad (6)$$

と定義すると，M系列は，時刻$t=t_0+n$におけるレジスターの状態$s^{t+n}_{n-1}$, $s^{t+n}_{n-2}$, …, $s^{t+n}_2$, $s^{t+n}_1$, $s^{t+n}_0$であると解釈できる．つまりM系列は，$n$次の原始多項式を用いて，ある状

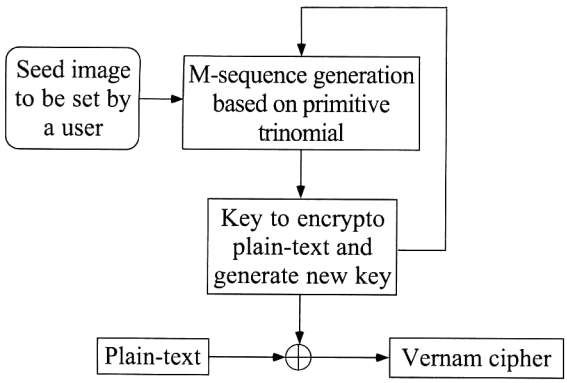



Fig. 2. The block diagram of Vernam cipher using random number.

態から $n$ クロックシフト後の状態への変換を用いることにより，$n$ 個の初期入力に対して一度に $n$ 個の系列を生成することができる．しかし，一般的に，$n$ 次の原始多項式を用いて並列に $n$ ビットを生成する際には，最大 $n$ 個の XOR 演算によって 1 ビットが生成されるために，最大 $(n-1)$段の XOR 演算のゲートが必要である．次節ではこれを 2 段のゲートによって生成する手法について述べる．

### 3.3 原始 3 項式

さらに，M 系列は，その次数 $n$ を適当に選択することで，

$$p(x)=x^n+x^i+1 \qquad (7)$$

に基づいて生成される[5,6]．これは，$n$ 次の原始 3 項式と呼ばれる．ただし，$(1<i<n)$ である．さらに，

$$i<\frac{n}{2} \qquad (8)$$

に着目すると，ビットの入れ換えと最大 2 段の XOR ゲートを組み合わせることによって，$n$ 個の系列の生成が可能となる．なお，式(7)に対して，

$$\tilde{p}(x)=x^n\cdot p(x^{-1})=x^n+x^{n-i}+1 \qquad (9)$$

は相反多項式と呼ばれ，これもまた $n$ 次原始 3 項式となる．このことから，式(7)が存在するならば，一般性を失うことなく，条件(8)を仮定することができる．

## 4. 並列処理による Vernam 暗号化システム

### 4.1 並 列 処 理

M 系列を用いた Vernam 暗号化処理について，Fig. 2 に示すブロック図を用いて説明する．まず，最初に，ユーザーごとにセットされた種画像が M 系列の生成のために与えられる．M 系列生成のブロックでは，設定された原始 3 項式に基づいて一度に $n$ ビットのランダムな系列が生成される．この系列を鍵として，$n$ ビットの平文との排他的論理和演算を行うことにより，$n$ ビットごとに Vernam 暗号が生成される．また，この時生成された $n$ ビットのランダムな系列は，次の $n$ ビットの系列生成のために擬似乱数処理部へフィードバックされる．これを繰り返すことで，同時に $n$ ビットの鍵の生成と暗号化が並列処理により高速に行われる．

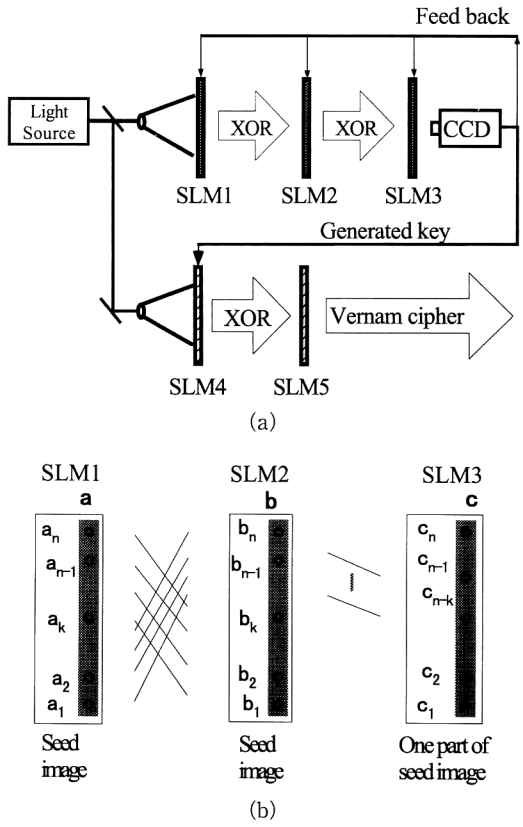


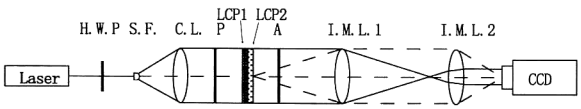

Fig. 3. (a) The optical system for generating Vernam cipher, (b) the interconnection between SLMs.

なお，Vernam 暗号では，同じ鍵を繰り返して用いると安全性が極端に損なわれる．M 系列では，$n$ を大きくすることによって指数関数的に周期が増大する．例えば，4,000 ビットの画像を初期値として用いると，擬似乱数の周期は，約 $10^{1,200}$ ビットとなる．この場合，ユーザーが 1 テラ $(10^{12})$ ビット/秒の通信回線を用いて常時暗号化を行ったとしても，約 $10^{1,000}$ 年分の乱数の生成が可能である．

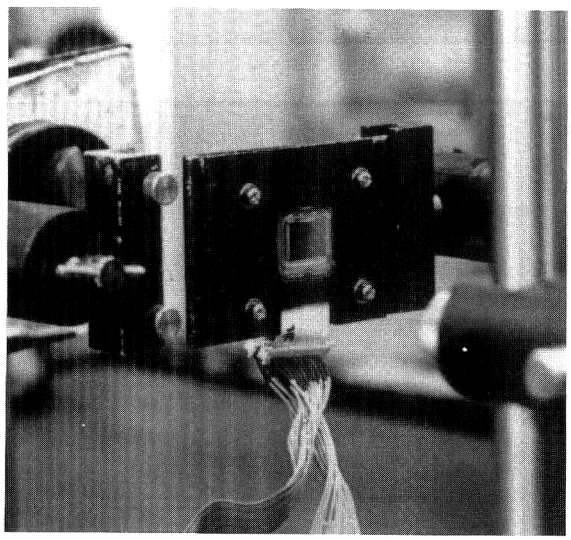
このように十分大きな周期をもつ場合には，初期値の推定のために膨大な計算時間を必要とする．初期値のビット数を増やすことは，長周期の乱数が生成されることから安全性の確保につながるばかりでなく，並列的に一括処理されるビット数が増えることにより処理速度の向上につながる．例えば，大容量データの暗号化を考えた場合，十分大きな次数をもつ原始多項式を設定することによって，同じ鍵を 2 度と用いることがないため，安全性の高い Vernam 暗号化が行えるのみならず，一度に処理されるビット数が増えることで，処理の高速化が可能となる．

Table 1. Interconnection for parallel bit generation using primitive trinominal $x^{10}+x^3+1$.

| Connection state | $i$ | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 |
| $a_i$ (Initial state) | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 |
| $b_i$ (Cycle of $a_i$) | 2 | 1 | 0 | 9 | 8 | 7 | 6 | 5 | 4 | 3 |
| $c_i$ (Shift of $b_i$) | 5 | 4 | 3 | $x$ | $x$ | $x$ | $x$ | $x$ | $x$ | $x$ |
| State after 10 clocks | 9^5^2 | 8^4^1 | 7^3^0 | 9^6 | 8^5 | 7^4 | 6^3 | 5^2 | 4^1 | 3^0 |




(a)



(b)

Fig. 4. (a) The optical setup used in the experiment, (b) homogeneous liquid crystal spatial light modulators used in the experiment.

### 4.2 光学系

これまでに述べたように，Vernam 暗号化を行うためには，XOR 演算が必要である．光学的に XOR 演算を行う手法として，これまでに種々の方法が提案されている[7]．ここでは，光システムの一例として，液晶パネルを用いた光システムを Fig. 3(a) に示す．乱数の種は画像として SLM 1～3 に表示され，鍵および平文は，それぞれ SLM 4 と SLM 5 に表示される．

まず，最初に種となる画像を表示する SLM 1～SLM 3 では，前節で述べたルールに基づいた光接続が行われると，CCD 面上に $n$ 個の乱数列が得られる．それぞれの接続は，初期値に対して，位置の巡回およびシフトの関係となっており，Fig. 3(b) に示すように，各 $a, b, c$ 間の関係を示すと以下のようになる．

$$b_i=a_{i+k-n}\ [i\geq n-k] \tag{10}$$

$$b_i=a_{i+k}\ [i<n-k] \tag{11}$$

$$c_i=a_{i-n+2k}\ [i\geq n-k] \tag{12}$$

$$c_i=0\ [i<n-k] \tag{13}$$

本手法の具体例として，原始 3 項式 $x^{10}+x^3+1$ の場合について Table 1 に示す．10 クロック後の状態に着目すると，1 ビットを生成するのに，最大 2 個の排他的論理和演算が必要であることがわかる．また，$b_i$ は，$a_i$ に対して 7 ビット巡回したパターンであり，さらに，$c_i$ は，$b_i$ に対して 7 ビットシフトしたパターンであることがわかる．つまり，$a_i$, $b_i$, $c_i$ の間を 2 段の XOR ゲートで組み合わせることによって，一度に 10 ビットの系列の生成が可能である．また，原始 3 項式の一般形が式(7)であたえられるとき，$(n-i)$ ビットの巡回とシフトが行われる．なお，Table 1 における $x$ は，0 と排他的論理和を行うことを意味する．

CCD に得られた系列を SLM 1～3 へ表示すると，次の系列が生成でき，この繰り返しによって，一度に $n$ ビットの乱数が生成される．この乱数列を鍵として，平文との XOR を計算することで，平文ごとに異なった鍵を用いた XOR 演算が行われる．それぞれの SLM は，同期信号によってすべて同時に制御される．また，平文の前に新たに別のキーを表示するための液晶パネルを挿入することで，複数のキーによる暗号化を行うことも可能である．

SLM 間の光接続については，CCD から得られたデータを SLM に書き込む際に，データをシフトまたは巡回した位置に書き込むことで実現できる．また，フィードバック毎に接続を再構築する必要がないため，この接続を光ファイバーや回折格子等をもちいることが可能である．更に，並列にデータの書き込みと読み出しが可能な光アドレス型の空間光変調器[8]を用いれば，CCD 等によるボトルネックを解消することが可能である．

## 5. 実験

### 5.1 擬似乱数の生成

実験では，ホモジニアス配向の液晶パネルを用い[9,10]，直線偏光の入射光の偏光方向と，液晶パネルの各画素にかける電圧の on/off によりビットの on/off を表すことで，偏光を利用して排他的論理和演算を行った．

実験に用いた光学系を Fig. 4(a) に示し，また実験に用

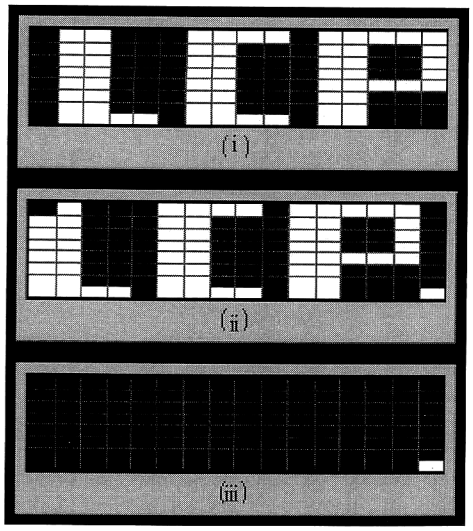



Fig. 5. Seed image used in the experiment.

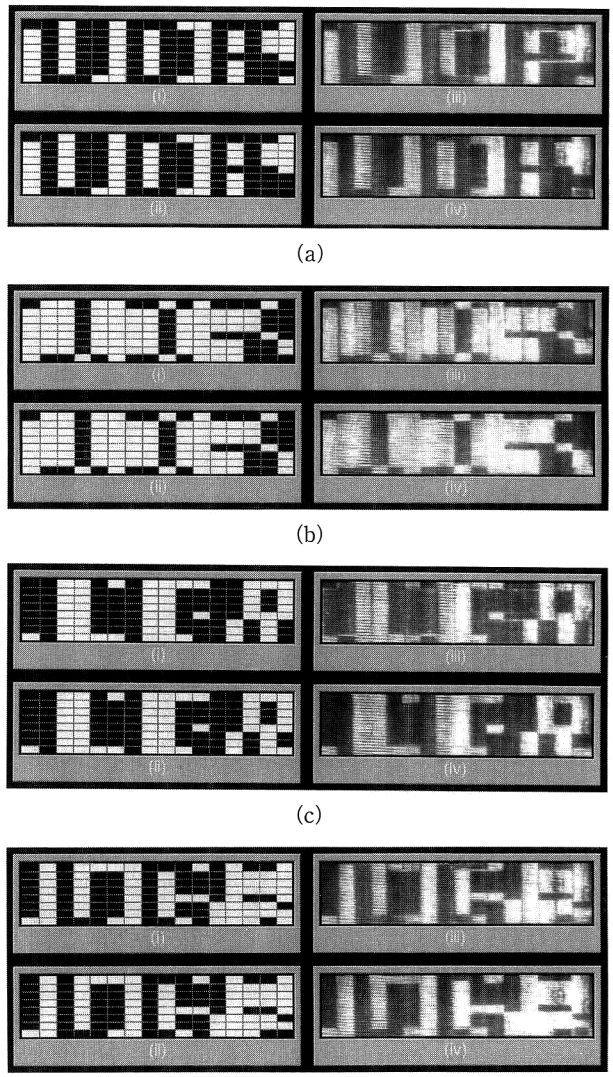
いた液晶パネルを同図(b)に示す．実験では，光源に He-Ne レーザーを用いて，2枚のホモジニアス配向の液晶パネルを組み合わせることで，1段のゲートを構築して XOR 演算を行った．液晶パネルの液晶のディレクターに対する入射光の偏光面は，偏光子 (P) によって 45° とした．また，検光子 (A) は偏光子に対してクロスニコルとし，明が on，暗が off である明論理とした．種画像として，Fig. 5(i) を用いた．

原始3項式 $x^{127}+x+1$ に基づいて発生した擬似乱数を Fig. 6 に示す．同図において，左には1クロックに1ビットずつ生成する方法に基づいた計算機シミュレーションによって得られた系列を，右には光学系を用いて得られた系列を示す．M 系列を生成するために XOR 演算を2回繰り返すことで，1段の XOR ゲートによって演算を行った．また，ビットの入れ換えは電気的に行った．Fig. 6(a)～(d) の中で (iv) が実験により得られた M 系列である．光学系を用いて生成されたデータに対して閾値処理を行い，計算機を用いて発生した結果と比較した結果，擬似乱数系列が一致した．なお，一番左上のビットは，don't care のビットであり，常に0としている．

### 5.2 暗号化および復号化

前節で生成した擬似乱数を用いて Vernam 暗号化を行い，そして，同じ鍵を用いて復号化を行った．実験光学系は 5.1 節と同様である．1枚目の液晶に Fig. 7 に示す平文を入力し，2枚目の液晶パネルには，Fig. 6 の (iv) を暗号化鍵として用いた．

得られた Vernam 暗号を Fig. 8 に示す．さらに，同じ鍵を用いて復号化を行った結果を Fig. 9 に示す．5.1 節と同様の閾値処理を行い，比較した結果，系列が一致していることを確認できた．




(a) (b) (c) (d)

Fig. 6. (a) Random pattern generated by experiment [1-127 bits], (b) random pattern generated by experiment [128-254 bits], (c) random pattern generated by experiment [255-381 bits], (d) random pattern generated by experiment [382-508 bits].

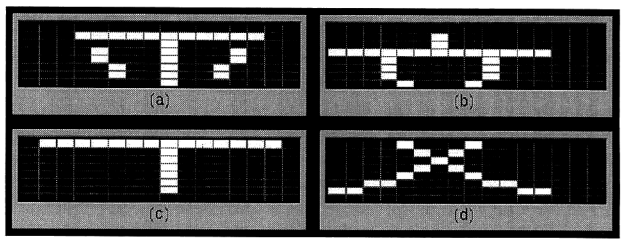



Fig. 7. Input data as plaintext image.

## 6. 考　　察

Vernam 暗号では，平文と同じ長さの鍵を用意する必要

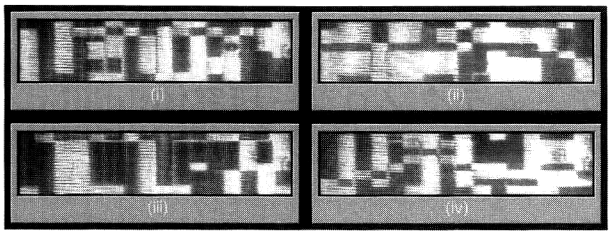


Fig. 8. Cipher patterns generated by experiment.

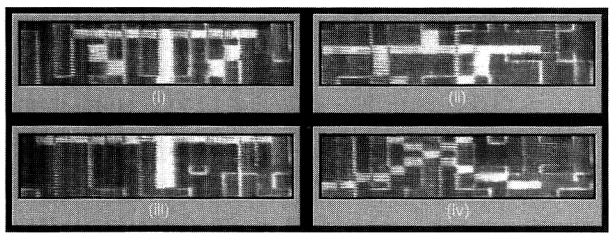


Fig. 9. Deciphered patterns generated by experiment without thresholding.

があり，光演算が画像などの並列処理に適していることから，画像などの大きなビット列を種として用いて生成した長周期の鍵を用いた暗号化が可能である．光演算を用いてこのような長周期の鍵の生成が可能であることから，安全性と高速処理の両立が可能であることが特徴として挙げられる．

さらに高速化するためには，高次の原始3項式[6]を用いると一度に生成される鍵の量を増やすことが可能であることから，システム処理量の向上や，光アドレス型のデバイスを用いた高速処理可能なシステムの検討等が今後の課題として考えられる．

また，Vernam暗号の場合は鍵の生成が重要であり，本論文で述べたように光演算を用いれば大きな鍵の生成が可能であるが，アルゴリズム的には鍵の推定が可能である．さらに安全性の高いシステムを構築するためには，このような光演算のメリットを生かし，かつ擬似乱数の生成手法に検討を行うことが必要である．具体的な例としては，非線形アルゴリズムを用いることが考えられる．

光学的並列処理は画像などを2次元データの並列処理に適していることから，大きな原始多項式を用いることによって，画像等の長いビット列を種として利用することも可能である．例えば，ユーザーごとに画像を鍵として設定できることから，本人固有の情報である指紋，印影，本人の顔画像等を用いることで，鍵の設定が容易であること，また，ユーザーにとってわかりやすい暗号化が行えると考えられる．

## 7. 結　　言

本論文では，今後の情報化社会において重要であると考えられる暗号化技術として，大きな種から生成したM系列を鍵として用いたVernam暗号を，光学的並列演算により行う手法について述べた．

まず，原始3項式を用いた2段のXOR演算によって，一度に多数の擬似乱数を生成できることを示した．

実験では，Watsonの報告の中で最高次数の原始多項式である127次の原始3項式に基づいて鍵の生成を行った．次に，生成された系列を用いて127ビットごとにデータのVernam暗号化および復号化を行った．そして，これらの実験データに対して閾値処理を行い，比較した結果，系列が一致していることを確認できた．

以上のことから光学系を用いたVernam暗号化の実現可能性を示した．

本研究を進めるにあたり，暗号学的側面から御助言をいただきました，東京工業大学伊東利哉助教授に感謝いたします．また，実験を行うにあたり，液晶パネルについて御協力および御助言をいただきました，エプソン株式会社の曽根原富雄氏，尼子淳氏に感謝いたします．

## 文　　献

1) 辻内順平，一岡芳樹，峯本　工：光情報処理（オーム社，東京，1989）．
2) P. Hilippe and B. Javidi: "Optical image encryption based on input and Fourier plane random encoding," Opt. Lett., **20** (1995) 767-769.
3) S. Fukushima, T. Kurokawa and Y. Sakai: "Image encipherment based on optical parallel processing using spatial light modulators," IEEE Trans. Photonics Technol. Lett., **3** (1991) 1133-1135.
4) S. W. Golomb: *Shift Register Sequences* (Holden-Day, Inc., San Francisco, 1967).
5) E. J. Watson: "Primitive polynomials (mod 2)," Math. Comput. **16** (1961) 368.
6) N. Zierler: "Primitive trinomials whose degree is a Mersenne exponet," Inf. Control, **15** (1969) 67-69.
7) F.T.S. Yu and S. Jutamulia: *Optical Signal Processing, Computing, and Neural Networks* (John Wiley & Sons, New York, 1992) pp. 287-338.
8) 例えば，N. Mukohzaka, N. Yoshida, H. Toyoda, Y. Kobayashi and T. Hara: "Diffraction efficiency analysis of a parallel-aligned nematic-liquid-crystal spatial light modulator," Appl. Opt., **33** (1994) 2804-2811.
9) T. Sonehara, H. Miura and J. Amako: "Moving 3D-CGH reconstruction using a liquid crystal spatial wavefront modulator," *Proc. Jpn. Disp. S9-6* (1992) pp. 315-318.
10) J. Amako, H. Miura and T. Sonehara: "Wave-front control using liquid-crystal devices," Appl. Opt., **32** (1993) 4323-4329.