文章编号：0253-2239(2007)05-0824-6

双随机相位加密系统的选择明文攻击*

位恒政[1] 彭 翔[2] 张 鹏[3] 刘海涛[4] 封松林[4]

(1 天津大学精密测试技术及仪器国家重点实验室，天津 300072
2 深圳大学光电子学研究所教育部光电子器件与系统重点实验室，深圳 518060
3 中国建设银行总行电子银行部，北京 100032
4 中国科学院上海微系统与信息技术研究所，上海 200050)

摘要： 在光学信息安全领域，双随机相位加密方法最引人注目并得到广泛研究，但由于双随机相位加密系统是基于傅里叶变换的系统，其本质上是一种线性变换系统，明文、密文之间的函数依赖关系比较简单，这就为其安全性留下了很大的隐患。双随机相位加密方法可以用光学和数字的方式实现，提出了一种选择明文攻击的方法，利用多个冲击函数作为选择的明文，成功破解了基于数字方法实现的双随机相位加密系统，并给出了恢复密钥的解析式，此方法最大的优点在于解密图像的无损性，并从理论上加以证明，给出了实验结果。

关键词： 信息光学；光信息安全；双随机相位加密；选择明文攻击

中图分类号：TP309.7 文献标识码：A

Chosen-Plaintext Attack on Double Phase Encoding Encryption Technique

Wei Hengzheng[1] Peng Xiang[2] Zhang Peng[3] Liu Haitao[4] Feng Songlin[4]

(1 *National Laboratory of Precision Measurement Technology and Instrumentation, Tianjin University, Tianjin* 300072
2 *Institute of Optoelectronics, Shenzhen University, Key Laboratory of Optoelectronics Devices and Systems, Ministry of Education, Shenzhen* 518060
3 *Electronic Banking Department, China Construction Bank, Beijing* 100032
4 *Shanghai Institute of Microsystem and Information Technology, Shanghai* 200050)

Abstract: In the field of optical information security, the most attractive work is the so-called double random phase encoding encryption scheme. This encryption method is based on the principle of Fourier transform algorithm and its linearity opens avenues of attacks. Double random phase encoding encryption can be implemented optically or digitally. We demonstrate a new approach to chosen-plaintext attack on double-phase encoding encryption system implemented digitally. With this attack an opponent can access both random phase keys with the help of impulse functions. The expressions of retrieved keys are also given. One of the most apparent advantage of proposed approach is that the decryption process is lossless. Numerical simulations show a good agreement with theoretical analysis.

Key words: information optics; optical information security; double random phase encoding encryption; chosen-plaintext attack

1 引 言

光信息安全技术是近年来在国际上开始起步发展的新一代信息安全理论与技术，作为一种“非数学的密码理论和技术”已经显示出极大的发展潜力并成为当前国际上研究的热点[1~8]。在此领域，B. Javidi 等[1]提出的基于标准 4－f 的双随机相位加

* 国家自然科学基金项目(60472107)、广东省自然科学基金(04300862)、深圳市科技计划项目(200426)、深圳大学科研启动基金(200509)和中科院微系统与信息技术研究所资助的课题。

作者简介：位恒政(1978－)，男，山东德州人，博士生，主要从事信息安全、密码学理论、数字水印等方面的研究。E-mail: Hzhwei@vip.sina.com

导师简介：彭 翔(1955－)，男，天津人，教授，博士生导师，主要从事现代光学测试、三维数字成像及造型、光学信息安全等方面的研究。E-mail: xpeng@szu.edu.cn

收稿日期：2006-07-12；收到修改稿日期：2006-09-20

密方法最为引人瞩目并在该领域得到了最广泛的研究。然而，双随机相位加密系统的安全性直到最近才被证明存在安全隐患[9~12]。由于双随机相位加密系统是基于傅里叶变换的系统，其本质上是一种线性变换系统，所以明文、密文之间的函数依赖关系比较简单，这就为其安全性留下了很大的隐患。一些学者已经证明，通过选择密文和明文的方法可以得到该密码系统的频域会话密钥[9,10]。一种已知明文攻击方法最近也被提出，该方法利用模拟退火(SA)算法获得频域密钥，但该方法只能解密明文为实数的信息[11]。

在文献[12]中，我们提出了一种基于相位恢复技术[13]的已知明文攻击方法[14]，攻击者可以通过相位恢复技术获得双随机相位加密系统空域的会话密钥，继而利用空域密钥和频域密钥之间的约束关系获得频域的会话密钥，从而攻破此密码系统。该方法只需一个明文-密文对，无需大量精心设计的密文，攻击实施的难度大大降低，而且此攻击方法对复数的明文信息也适用。但是用该方法解密出来的灰度图像比较模糊，噪声比较大，这是由相位恢复算法本身的性能以及初始相位选择的随机性引入的误差造成的。

本文提出了一种基于数字实现的双随机相位加密系统的选择明文攻击方法。选择明文攻击的破译者除了知道加密算法外，还可以设计一些特殊的明文并知道相应的密文。利用多个冲击函数作为选择的明文，不仅得到了该系统的频域密钥，而且得出了空域密钥，并给出了解析表达式，与已知明文攻击方法[12]相比，其最大的优点在于解密结果是无损的，模拟实验结果与理论证明一致。

2　双随机相位加密系统

双随机相位加密系统采用标准的 $4-f$ 系统来实现，如图 1 所示，利用两块统计无关的随机相位板将输入信息变为平稳白噪声，从而达到加密的目的。用信息光学理论描述上述过程如下：加密时，输入信号 $f(x,y)$ 在空域受到随机相位函数 $N(x,y)=\exp[\mathrm{j}n(x,y)]$ 的调制，在频域被随机函数 $B(\alpha,\beta)=\exp[\mathrm{j}b(\alpha,\beta)]$ 滤波，$n(x,y)$，$b(\alpha,\beta)$ 分别为两个分布于 $[0,2\pi]$ 的独立白噪声序列，加密结果表示如下：

$$\psi(x,y)=\mathscr{F}^{-1}\{\mathscr{F}[f(x,y)\cdot N(x,y)]\cdot B(\alpha,\beta)\},\tag{1}$$

$\mathscr{F}$ 表示傅里叶变换，$\mathscr{F}^{-1}$ 表示傅里叶逆变换。上述加密过程在频域的表示为

$$\psi(\alpha,\beta)=\mathscr{F}[f(x,y)\cdot N(x,y)]\cdot B(\alpha,\beta).\tag{2}$$

解密时，将加密后的数据 $\psi(x,y)$ 置于 $4-f$ 系统的输入端。设 $B(\alpha,\beta)^*$ 为 $B(\alpha,\beta)$ 的复共轭，经傅里叶变换后，在频谱平面上用相位函数 $B(\alpha,\beta)^*$（解密密钥）滤波，再经傅里叶逆变换，即可恢复出 $f(x,y)N(x,y)$。如果 $f(x,y)$ 是正、实函数，故经过 CCD 等强度探测器件即可恢复出明文信息 $f(x,y)$，解密过程表示为下式：

$$\begin{aligned}f_{\mathrm{D}}(x,y)&=\mathscr{F}^{-1}\{\psi(\alpha,\beta)B(\alpha,\beta)^*\}=\\&\mathscr{F}^{-1}\{\mathscr{F}[f(x,y)N(x,y)]B(\alpha,\beta)\cdot B(\alpha,\beta)^*\}=\\&f(x,y)N(x,y),\end{aligned}\tag{3}$$

当 $f(x,y)$ 为复函数时，还必须知道空域解密密钥，才能正确解密 $f(x,y)$。

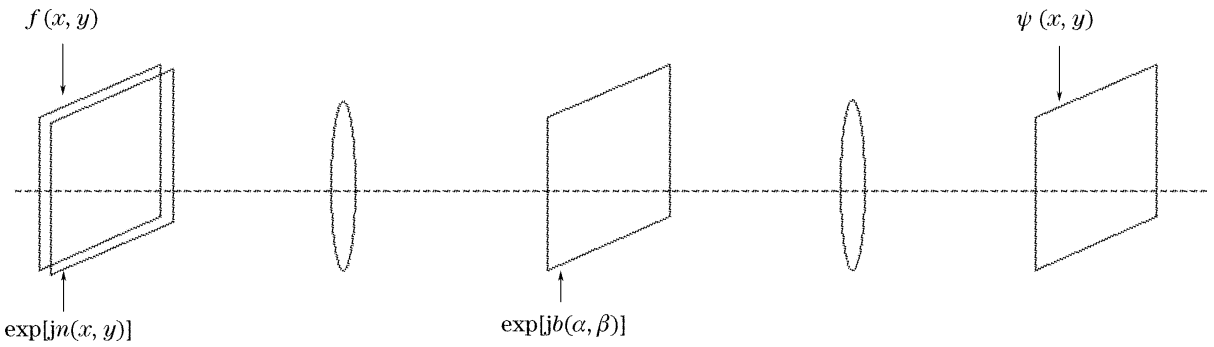

图 1　双随机相位加密系统示意图

Fig. 1　Double random phase encoding encryption scheme

3　典型的密码学分析方法

在对密码系统进行密码分析时，通常认为攻击者已经拥有所使用加密算法的全部知识，密码系统的安全性完全寓于密钥之中，即满足“Kerckhoffs 假

设”[14]。根据攻击者所掌握的信息，可将密码的攻击分为以下几类：唯密文攻击，已知明文攻击，选择明文攻击等。

我们将加密输入的原始信息称为明文，将加密变换后的结果称为密文，用 E 表示加密算法，用 k 表示密钥，$p(p_1,p_2,\cdots,p_n)$ 表示明文，$c(c_1,c_2,\cdots,c_n)$ 表示密文。下面简要介绍一下这几种密码分析方法。

3.1 唯密文攻击

对于这种攻击方法，攻击者掌握的信息只有加密算法和一些待破译的密文，利用这些信息来推导系统的密钥。从抽象的观点看，唯密文攻击的方法可以表示为：已知 $c_i=E_k(p_i)$，$1\leqslant i\leqslant l$，推出 $p_1,p_2,\cdots,p_l$ 或 k。

3.2 已知明文攻击

在已知明文攻击中，攻击者已获得的信息包括：加密算法和经密钥加密形成的一个或多个明文-密文对，即知道一定数量的任意密文和相应的明文。密码分析者利用它们来推出密钥。从抽象的观点来看，即已知 $p_i,c_i=E_k(p_i)$，推出 k。

3.3 选择明文攻击

与已知明文相比，选择明文的攻击者还可以选定特殊的明文信息，并可以知道对应的密文，从而推导出加密密钥。这种特殊的选择可能导致产生更多关于密钥的信息，从而更容易获得所需要的密钥。从抽象的观点来看，即攻击者选择 $p_1,p_2,\cdots,p_l$，并知道 $c_i=E_k(p_i)$，$1\leqslant i\leqslant l$，推出密钥 k。

以上三种攻击方法对密码分析者来说，所具有的条件是不同的，进行密码分析的难度也是不同的。攻击者掌握的信息越多，密码分析也就越容易。

4 双随机相位加密系统的选择明文攻击

双随机相位加密系统可以用光学和数字的方法来实现[1]，在实际应用中，双随机相位加密系统的数字实现是普遍应用的方法，本文提出的攻击方法是针对双随机相位加密系统的数字实现方法。为了分析的需要，$f(x,y)$，$N(x,y)$，$B(\alpha,\beta)$，$\psi(\alpha,\beta)$ 均已离散化，其维数均为 $N\times N$，矩阵之间的运算为对应像素的点乘运算。

下面利用选择明文攻击的方法来分析双随机相位加密系统。假设攻击者将冲击函数作为选择的特殊明文，并且还知道相应的密文。攻击的具体过程分两步进行：首先加密若干个冲击函数，应用冲击函数的运算性质得到若干个对应的密文，利用这些明文-密文对推导空域密钥；然后加密其它任意一个明文，得到相应的密文，利用已经恢复的空域密钥和加密系统的加密方程，得出双随机相位加密系统的频域密钥。最后利用正确获得的空域密钥和频域密钥解密后续传来的其它密文。

4.1 空域密钥的恢复

设选择的明文为冲击函数 $\delta(x-i,y-j)$，冲击函数在 (i,j) 处为 1，其余处为 0。当 $i=0,j=0$ 时，由加密方程(2)式可以得到

$$\begin{aligned}\psi(\alpha,\beta)&=\mathscr{F}[f(x,y)\cdot N(x,y)]\cdot B(\alpha,\beta)=\\&\mathscr{F}[\delta(x,y)\cdot N(x,y)]\cdot B(\alpha,\beta)=\\&\mathscr{F}[\delta(x,y)\cdot N(0,0)]\cdot B(\alpha,\beta)=\\&\mathscr{F}[\delta(x,y)]\cdot N(0,0)\cdot B(\alpha,\beta)=\\&N(0,0)\cdot B(\alpha,\beta),\end{aligned}\tag{4}$$

同理，当 $i\neq 0,j\neq 0$，可以得到

$$\psi'(\alpha,\beta)=N(i,j)\cdot B(\alpha,\beta),\tag{5}$$

联立(4)式、(5)式，可以得到

$$\frac{\psi'(\alpha,\beta)}{\psi(\alpha,\beta)}=\frac{1}{N(0,0)}N(i,j)\cdot\boldsymbol{I},\tag{6}$$

I 为全 1 的矩阵，$\psi'(\alpha,\beta)$，$\psi(\alpha,\beta)$ 都是已知量，设 $N(0,0)$ 为参考点，其值可以为任意非零值，从而可得到 $N(i,j)$ 的值。对一幅 $N\times N$ 的图像而言，需要 $N\times N$ 个这样的冲击函数，就可以得出空域的密钥，这些值都是相对参考点 $N(0,0)$ 的值。

设 $N'(x,y)=\dfrac{\psi'(\alpha,\beta)}{\psi(\alpha,\beta)}$ 为恢复的空域密钥，则其与真实密钥 $N(x,y)$ 的关系可以表示为

$$N'(x,y)=\frac{1}{N(0,0)}N(x,y),\tag{7}$$

恢复的空域密钥与真实空域密钥之间只差一个常数因子 $1/N(0,0)$，但这不会影响解密结果，随后的数值仿真实验证明了这一点。

4.2 利用恢复的空域密钥推导频域密钥

首先加密一个任意明文 $f_2(x,y)$，由加密方程(2)式可以得到：

$$\psi_2(\alpha,\beta)=\mathscr{F}[f_2(x,y)\cdot N(x,y)]\cdot B(\alpha,\beta),\tag{8}$$

将恢复得到的空域密钥 $N'(x,y)$ 代入上式，并设待恢复的频域密钥为 $B'(\alpha,\beta)$，则

$$\psi_2(\alpha,\beta)=\mathscr{F}[f_2(x,y)\cdot N'(x,y)]\cdot B'(\alpha,\beta),\tag{9}$$

所以可以得出频域密钥：

$$B'(\alpha,\beta)=\frac{\psi_2(\alpha,\beta)}{\mathscr{F}[f_2(x,y)\cdot N'(x,y)]},\tag{10}$$

将(8)式代入(10)式，简化(10)式，可以得到

$$B'(\alpha,\beta)=\frac{\psi_2(\alpha,\beta)}{\mathscr{F}[f_2(x,y)\cdot N'(x,y)]}=\frac{\mathscr{F}[f_2(x,y)\cdot N(x,y)]\cdot B(\alpha,\beta)}{\mathscr{F}[f_2(x,y)\cdot N'(x,y)]}=$$

$$\frac{\mathscr{F}[f_2(x,y)\cdot N(x,y)]}{\mathscr{F}[f_2(x,y)\cdot N(x,y)]}\cdot B(\alpha,\beta)\cdot N(0,0)=B(\alpha,\beta)\cdot N(0,0),\tag{11}$$

可以得到恢复的频域密钥与真实频域密钥之间的关系为

$$B'(\alpha,\beta)=B(\alpha,\beta)\cdot N(0,0),\tag{12}$$

恢复的频域密钥与真实的频域密钥之间也只相差一个因子，但这同样不会影响解密结果，随后的数值仿真实验也证明了这一点。

4.3　利用恢复的空域密钥和频域密钥解密后续传来的密文

假设截获一密文 $\psi_i(\alpha,\beta)$，其相应的明文为 $f_i(x,y)$，并满足加密方程

$$\psi_i(\alpha,\beta)=\mathscr{F}[f_i(x,y)\cdot N(x,y)]\cdot B(\alpha,\beta),\tag{13}$$

现利用恢复的空域密钥 $N'(x,y)$ 和频域密钥 $B'(\alpha,\beta)$ 进行解密，设待恢复的明文为 $f'_i(x,y)$，$N'(x,y)^*$，$B'(\alpha,\beta)^*$ 分别为 $N'(x,y)$，$B'(\alpha,\beta)$ 的复共轭，$|B(\alpha,\beta)|=1$，$|N(x,y)|=1$，则

$$\begin{aligned}
f'_i(x,y)=&\mathscr{F}^{-1}[\psi_i(\alpha,\beta)\cdot B'(\alpha,\beta)^*]\cdot N'(x,y)^*=\\
&\mathscr{F}^{-1}\{\mathscr{F}[f_i(x,y)\cdot N(x,y)]\cdot B(\alpha,\beta)\cdot B'(\alpha,\beta)^*\}\cdot N'(x,y)^*=\\
&\mathscr{F}^{-1}\{\mathscr{F}[f_i(x,y)\cdot N(x,y)]\cdot B(\alpha,\beta)\cdot B(\alpha,\beta)^*\cdot N(0,0)^*\}\cdot N'(0,0)^*=\\
&\mathscr{F}^{-1}\{\mathscr{F}[f_i(x,y)\cdot N(x,y)]\cdot |B(\alpha,\beta)|^2\cdot N(0,0)^*\}\cdot N'(x,y)^*=\\
&N(0,0)^*\cdot\mathscr{F}^{-1}\{\mathscr{F}[f_i(x,y)\cdot N(x,y)]\}\cdot N'(x,y)^*=\\
&N(0,0)^*\cdot f_i(x,y)\cdot N(x,y)\cdot N'(x,y)^*=\\
&N(0,0)^*\cdot f_i(x,y)\cdot N(x,y)\cdot N(x,y)^*\cdot\frac{1}{N(0,0)^*}=\\
&f_i(x,y)\cdot|N(x,y)|^2=f_i(x,y),
\end{aligned}\tag{14}$$

所以 $f'_i(x,y)=f_i(x,y)$，可以看出，此解密结果是无损的。

5　模拟实验及其结果分析

在 Matlab6.5 环境下对本文提出的选择明文攻击方法进行了数值仿真实验。首先加密若干个冲击函数，应用冲击函数的运算性质得到若干个对应的密文，利用这些明文-密文对推导空域密钥；然后加密其它任意一个明文，得到相应的密文，利用已经恢复的空域密钥和加密系统的加密方程，得出双随机相位加密系统的频域密钥。在仿真实验中，我们分别运用文献[12]提出的已知明文攻击方法和本文提出的选择明文攻击方法，对双随机相位加密系统进行了密码学攻击实验，并进行了对比分析。图 2(a)是一幅灰度图 Lena(256 pixel×256 pixel×8 bits)，图 2(b)是灰度图像加密后的密文，图 3(a) 是用文献[12]提出的已知明文攻击方法所得密钥解密的结果，图 3(b)是用本文提出的选择明文攻击方法所得密钥解密的结果。图 4(a)是一幅二值图(256 pixel×256 pixel×8 bits)，图 4(b)是二值图加密后的密文，图 5(a)是用文献[12]提出的已知明文攻击方法所得密钥解密的结果，图 5(b)是用本文提出的选择明文攻击方法所得密钥解密的结果。

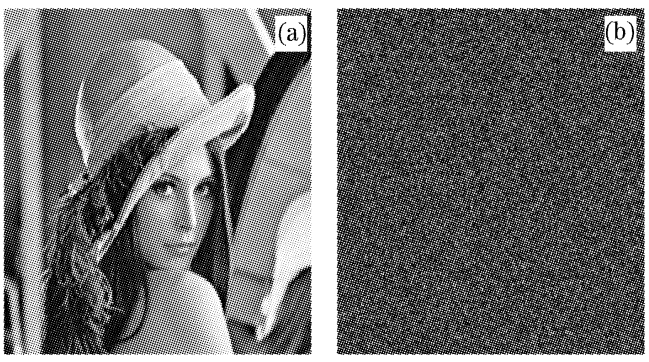

图 2　(a)灰度图像(明文)，(b) 相应的密文

Fig. 2　(a) Gray-scale image (plain text), (b) corresponding cipher text

为了客观地评价图像解密效果，引入峰值信噪比(PSNR)来评价解密结果的质量(用 R 表示，单位为 dB)，定义如下：

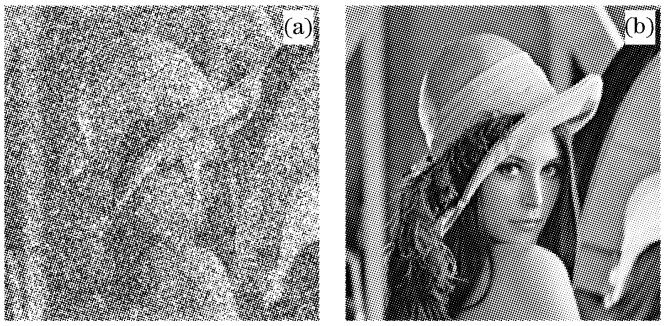

图 3 (a)用已知明文攻击所得密钥解密的结果，(b)用选择明文攻击所得密钥解密的结果

Fig. 3 (a) The retrieved results of gray-scale image with known-plain text attack, (b) the retrieved results of gray-scale image with chosen-plain text attack

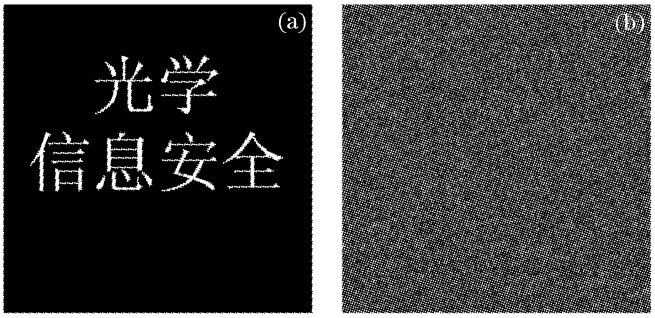

图 4 (a)二值图像(明文)，(b) 相应的密文

Fig. 4 (a) Binary image (plain text), (b) corresponding cipher text

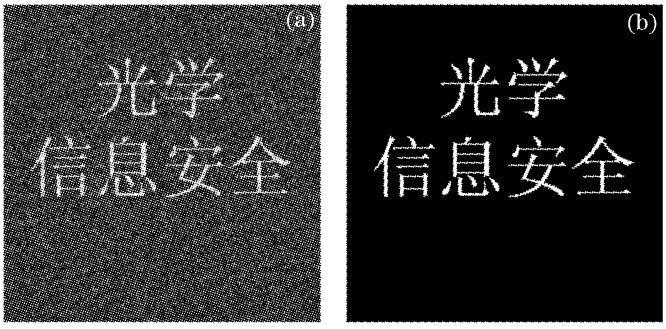

图 5 (a)用已知明文攻击所得密钥解密的结果，(b)用选择明文攻击所得密钥解密的结果

Fig. 5 (a) Retrieved results of binary image with known-plain text attack, (b) retrieved results of binary image with chosen-plain text attack

$$R_{\mathrm{P}}=10\lg\frac{P^2MN}{\sum_{i=1}^{M}\sum_{j=1}^{N}[f(i,j)-f_{\mathrm{D}}(i,j)]^2},\quad(15)$$

其中 P 表示原图像的最大幅值，$f(i,j)$ 为原图像的幅值分布，$f_{\mathrm{D}}(i,j)$ 为解密图像的幅值分布，M,N 表示图像的维数，由(15)式可知，R 值越大，就代表失真越小。表 1 给出了灰度图和二值图分别用两种攻击方法所得到的 R_{P} 的数值。

从表 1 的数据可以看出，用已知明文攻击所得密钥解密的结果与原图像之间的峰值信噪比相对较小，失真比较大；而用选择明文攻击所得密钥解密的结果解密后图像与原图像的峰值信噪比为无穷大，由此可见，用选择明文攻击得到的密钥进行解密的结果是无损的。

表 1 灰度图和二值图分别用两种攻击方法所得到的 R_{P} 的数值

Table 1 Peak signal-noise ratio of the retrieved image with the known-plain text and chosen-plain text attack

	Gray-scale image	Binary image
Known-plain text attack [R_{P}/dB]	10.319	13.37
Chosen-plain text attack [R_{P}/dB]	∞	∞

在已知明文攻击[12]中，空域密钥的恢复基于相位恢复技术，在物平面和傅里叶平面之间反复迭代来寻找空域密钥，这是一个逐渐逼近的过程。误差平方和 SSE(用 E 表示)定义为

$$E=10\lg\frac{\sum[\rho-\rho^{(n)}]^2}{\sum\rho^2},\quad(16)$$

式中 ρ 代表物平面上的已知振幅分布，$\rho^{(n)}$ 代表第 n 次迭代结束时物平面上的振幅分布。E 随迭代次数的收敛情况如图 6 所示。

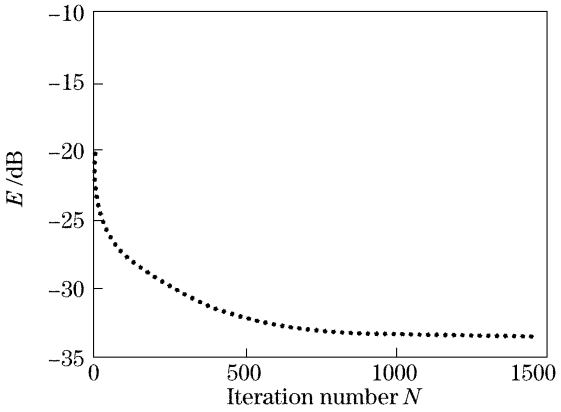

图 6 E 随迭代次数的收敛情况

Fig. 6 E versus the number of iterations

从图中可看出，算法开始收敛速度较快，且迭代次数 n 越高精度越高，因此用此方法得到的密钥是一个近似的空域密钥。在通过空域密钥求解频域密钥的过程中，误差会进一步传播，因此用此方法恢复的密钥解密其它密文时，解密结果就比较差。

而本文提出的选择明文攻击方法给出的密钥是解析式，如(17)式、(18)式所示，$N'(x,y)$，$B'(\alpha,\beta)$ 分别表示恢复的空域和频域密钥，$N(x,y)$，$B(\alpha,\beta)$ 表示相应的真实密钥，$N(0,0)$为一非零常数因子，

$$N'(x,y) = \frac{1}{N(0,0)}N(x,y), \quad (17)$$

$$B'(\alpha,\beta) = B(\alpha,\beta) \cdot N(0,0). \quad (18)$$

虽然恢复出的空域密钥与频域密钥与真实密钥都差一个因子，但由于双随机相位系统是一个线性系统，所以常数因子并不影响解密结果。实验结果也验证了该理论的正确性。

6 结　论

1）从理论上推导了利用选择明文攻击方法求解密钥的过程，并从实验加以验证，虽然推导出的密钥与真实密钥相差一个因子，但解密结果却是无损的，其根本原因就是双随机相位加密系统是一个线性系统。

2）当推导出空域密钥后，很容易就得到了频域密钥，这证明了双随机相位加密系统不满足密码系统的一个基本要求“稳定的安全性”。“稳定的安全性”要求：当部分密钥被破译后，密码系统仍具有一定的抗攻击能力，整个密码系统不至于立刻崩溃。可见双随机相位加密系统的安全性仅仅依赖于其中的部分密钥。

3）双随机相位加密系统拥有巨大的密钥数，可以抵抗穷举法的攻击，但一个系统的安全性不能仅仅依赖于密钥的数量，更重要的是密码系统的结构是否满足密码学中的混乱和扩散的原则，也即是否存在非线性变换。双随机相位加密系统是一个典型的线性系统，所以其安全性是比较弱的。

4）与基于相位恢复算法的已知明文攻击方法相比，选择明文攻击方法的解密结果是无损的，这是选择明文攻击的优势，但选择明文需要特殊设计的明文，也就是说选择明文攻击需要掌握更多的信息，增加了攻击实施的难度。已知明文不需要特殊设计的明文，因此其攻击所需的信息量小，攻击实施的难度较低，但由于其恢复的密钥不够精确，其解密结果是比较差的，这是由相位恢复算法本身的性能以及初始相位选择的随机性引入的误差造成的。

参 考 文 献

1 P. Refregier, B. Javidi. Optical image encryption based on input plane and Fourier plane random encoding[J]. *Opt. Lett.*, 1995, **20**(7): 767～769

2 Xiang Peng, Lingfeng Yu, Lilong Cai. Double-lock for image encryption with virtual optical wavelength[J]. *Opt. Express*, 2002, **10**(1): 41～45

3 Xiang Peng, Zhiyong Cui, Tieniu Tan. Information encryption with virtual-optics imaging system[J]. *Opt. Commun.*, 2002, **212**(4～6): 235～245

4 Peng Xiang, Zhang Peng, Niu Hanben. Information hiding theory based on virtual optics and its implementation with parallel hardware[J]. *Acta Optica Sinica*, 2004, **24**(5): 623～627 (in Chinese)
彭　翔，张　鹏，牛憨笨. 虚拟光学信息隐藏理论及并行硬件实现[J]. 光学学报，2004，**24**(5)：623～627

5 Peng Xiang, Zhang Peng, Niu Hanben. 3-D spatial digital watermarking system based on virtual optics[J]. *Acta Optica Sinica*, 2004, **24**(11): 1507～1510 (in Chinese)
彭　翔，张　鹏，牛憨笨. 基于虚拟光学的三维空间数字水印系统[J]. 光学学报，2004，**24**(11)：1507～1510

6 Yu Bin, Peng Xiang. Optical image encryption based on cascaded phase retrieval algorithm[J]. *Acta Optica Sinica*, 2005, **25**(7): 881～884 (in Chinese)
于　斌，彭　翔. 基于级联相位恢复算法的光学图像加密[J]. 光学学报，2005，**25**(7)：881～884

7 Yu Chiliang, Gu Jihua, Liu Wei *et al.*. An image digital watermark technique based on digital holography and discrete cosine transform[J]. *Acta Optica Sinica*, 2006, **26**(3): 355～361 (in Chinese)
尉迟亮，顾济华，刘　薇 等. 基于数字全息及离散余弦变换的图像数字水印技术[J]. 光学学报，2006，**26**(3)：355～361

8 Zhang Peikun, Li Yulin, Liu Jiaying *et al.*. Study on the rotative invariance in the phase encrypted image and the phase-ring decryption[J]. *Chin. J. Lasers*, 2000, **A27**(3): 224～228 (in Chinese)
张培琨，李育林，刘家英 等. 光学图像相位加密中旋转不变性的实现及环形相位解密[J]. 中国激光，2000，**A27**(3)：224～228

9 Y. Frauel, A. Castro, T. J. Naughton *et al.*. Security analysis of optical encryption[C]. *Proc. SPIE*, 2005, **5986**: 25～34

10 A. Carnicer, M. Montes-Usategui, S. Arcos *et al.*. Vulnerability to chosen-cyphertext attacks of optical encryption schemes based on double random phase keys[J]. *Opt. Lett.*, 2005, **30**(13): 1644～1646

11 U. Gopinathan, D. S. Monaghan, T. J. Naughton *et al.*. A known-plaintext heuristic attack on the Fourier plane encryption algorithm[J]. *Opt. Express*, 2006, **14**(8): 3181～3186

12 Xiang Peng, Peng Zhang, Hengzheng Wei *et al.*. Known-plaintext attack on optical encryption based on double random phase keys[J]. *Opt. Lett.*, 2006, **31**(8): 1044～1046

13 J. R. Fienup. Phase retrieval algorithms: a comparison[J]. *Appl. Opt.*, 1982, **21**(15): 2758～2769

14 W. Stallings. *Cryptography and Network Security: Principles and Practice* [M]. 2nd edition, New Jersey: Prentice Hall, 1999. 24～26