第 56 卷 第 7 期 2007 年 7 月
1000-3290/2007/56(07)/3924-07

物 理 学 报
ACTA PHYSICA SINICA

Vol.56,No.7,July,2007

基于菲涅耳域的双随机相位编码系统的选择明文攻击*

彭 翔[1)2)†] 位恒政[1)] 张 鹏[3)]

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)

(2006 年 7 月 28 日收到;2006 年 10 月 27 日收到修改稿)

用密码分析学的方法对菲涅耳域双随机相位加密系统进行了安全性分析,并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,成功破解了菲涅耳域的双随机相位加密系统,并给出了密钥的解析式.此方法最大的优点在于解密的无损性,并从理论上加以证明,给出了模拟实验结果.

关键词:信息光学,双随机相位加密,选择明文攻击,菲涅耳变换

PACC:4230,4225K,0650D

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—5].在此领域,Javidi 等人提出的基于标准 4-f 的双随机相位加密系统最为引人瞩目,并在该领域得到了最广泛的研究[1].然而,双随机相位加密系统的安全性始终未得到证明,从密码学分析学的角度对其安全性的分析也鲜有报道.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,这就为其安全性留下了很大的隐患[6—9].2005 年 Carnicer 等人发现,通过选择密文的方法可以得到加密系统的频域会话密钥[6].随后 Peng 等人提出了一种基于 HIO (hybrid input-output algorithm)位相恢复[10,11]的已知明文攻击的方法[7],利用该方法,攻击者可以通过位相恢复的方法获得空域的会话密钥,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.此方法只需一个明文-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.Gopinathan 等人提出了另外一种已知明文攻击方法[8],该方法利用模拟退火(SA)算法估计频域密钥.

Situ 等人通过引入菲涅耳变换[12,13],发展了双随机相位加密方法[13],增加了密钥的维数,在一定程度上提高了密码系统的安全性,但这个系统本质上仍然是一个线性系统,因此其安全性还不是很高.

本文提出了一种菲涅耳域的双随机相位加密系统的选择明文攻击方法[14].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.我们利用多个冲击函数作为选择的明文,得出了该系统的空域密钥,继而得出频域密钥,并给出了密钥解析表达式,通过证明,此解密方法是无损的,模拟实验结果与理论一致.

2. 菲涅耳域的双随机相位加密系统

菲涅耳域的双随机相位加密系统可以看作无透镜的 4-f 系统,利用两块统计无关的随机相位板和两次菲涅耳衍射变换,达到数据加密的目的.其装置如图 1 所示,设两个随机相位函数为 $R_1(x,y)=$

* 国家自然科学基金(批准号:60472107),广东省自然科学基金(批准号:04300862),深圳市科技计划项目(200426),中科院微系统与信息技术研究所资助的课题.

† E-mail:xpeng@szu.edu.cn

$\exp[\mathrm{j}n(x,y)]$ 和 $R_2(x',y')=\exp[\mathrm{j}b(x',y')]$，$n(x,y)$，$b(x',y')$ 分别表示两个分布于 $[0,2\pi]$ 的独立白噪声序列. 加密过程具体描述如下：首先将待加密的图像 $f(x,y)$ 与随机相位函数 $\exp[\mathrm{j}n(x,y)]$ 相乘，得到 $f(x,y)\exp[\mathrm{j}n(x,y)]$，将其作距离为 D_1 的菲涅耳衍射，然后将得到的复振幅与随机相位函数 $\exp[\mathrm{j}b(x',y')]$ 相乘，再作一距离为 D_2 的菲涅耳衍射，得到最后的加密结果.

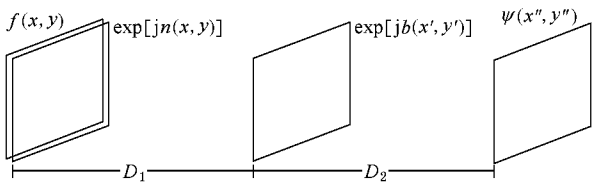

图 1　菲涅耳域的双随机相位加密系统

由于在此系统中，用到了菲涅耳衍射，因此我们首先对菲涅耳衍射公式进行了简化. 设 λ 为入射波长，$u(x_0,y_0)$ 是信息平面，衍射距离为 D，对 $u(x_0,y_0)$ 作衍射距离为 D 的菲涅耳衍射得到 $U_D(x,y)$，则此过程可以表示为

$$U_D(x,y)=\frac{\exp(\mathrm{j}kD)}{\mathrm{j}\lambda D}\int_{-\infty}^{\infty}\int_{-\infty}^{\infty}u(x_0,y_0)\times\exp\left[\mathrm{j}k\frac{(x-x_0)^2+(y-y_0)^2}{2D}\right]\mathrm{d}x_0\mathrm{d}y_0,\quad(1)$$

其中 $k=\frac{2\pi}{\lambda}$，将上式积分中二次相位因子展开，可以得到

$$\begin{aligned}U_D(x,y)&=\frac{\exp(\mathrm{j}kD)}{\mathrm{j}\lambda D}\int_{-\infty}^{\infty}\int_{-\infty}^{\infty}u(x_0,y_0)\times\exp\left[\mathrm{j}k\frac{(x-x_0)^2+(y-y_0)^2}{2D}\right]\mathrm{d}x_0\mathrm{d}y_0\\&=\frac{\exp(\mathrm{j}kD)}{\mathrm{j}\lambda D}\exp\left[\frac{\mathrm{j}\pi}{\lambda D}(x^2+y^2)\right]\times\mathrm{FT}\left\{u(x_0,y_0)\exp\left[\frac{\mathrm{j}\pi}{\lambda D}(x_0^2+y_0^2)\right]\right\},\quad(2)\end{aligned}$$

其中 FT 表示傅里叶变换，设

$$q(x_0,y_0)=\exp\left[\frac{\mathrm{j}\pi}{\lambda D}(x_0^2+y_0^2)\right],$$

在波长和衍射距离已知的情况下，忽略常数位相因子，可以得到简化的菲涅耳衍射的傅里叶变换表达式

$$U_D(x,y)=\mathrm{FT}[u(x_0,y_0)\cdot q(x_0,y_0)].\quad(3)$$

设待加密图像为 $f(x,y)$，则图 1 的菲涅耳域双随机相位加密的过程可以描述为

$$\psi(x'',y'')=\mathrm{FT}\{\mathrm{FT}[f(x,y)R_1(x,y)q_1(x,y)]\times R_2(x',y')q_2(x',y')\},\quad(4)$$

其中 $q_1(x,y)=\exp\left[\frac{\mathrm{j}\pi}{\lambda D_1}(x^2+y^2)\right]$，$q_2(x',y')=\exp\left[\frac{\mathrm{j}\pi}{\lambda D_2}\right](x'^2+y'^2)$，$R_1(x,y)$，$R_2(x',y')$ 为两个随机位相函数.

为方便起见，将加密结果 $\psi(x'',y'')$ 的逆傅里叶变换记作 $K(x',y')$，则

$$K(x',y')=\mathrm{FT}[f(x,y)R_1(x,y)q_1(x,y)]\times R_2(x',y')q_2(x',y').\quad(5)$$

记 $A(x,y)=R_1(x,y)q_1(x,y)$，$B(x',y')=R_2(x',y')q_2(x',y')$，将 $A(x,y)$ 和 $B(x',y')$ 看作加密系统的密钥，则菲涅耳域的双随机相位加密过程可以描述为

$$K(x',y')=\mathrm{FT}[f(x,y)A(x,y)]B(x',y').\quad(6)$$

由系统的加密方程(6)可以看出，其与标准的 4-f 双随机相位加密系统的加密方程是一致的，$A(x,y)$ 相当于系统的空域密钥，$B'(x',y')$ 相当于频域密钥，不同的是密钥构成中多了一个二次位相因子，当衍射距离和入射波长一定时，这个二次位相因子是确定的，与随机相位函数相乘构成一个新的密钥.

3. 典型的密码学分析方法

在密码分析学中，有一个基本的假设称为“Kerchhoffs 假设”，该假设假定攻击者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. 根据攻击者所掌握的信息，可以将分组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,攻击者已知的东西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,即知道一定数量的密文和相应的明文.密码分析者利用它来推出加密用的密钥.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. 菲涅耳域双随机相位加密系统的选择明文攻击

下面利用选择明文攻击的方法来分析菲涅耳域的双随机相位加密系统.假设攻击者将冲击函数 $\delta(x,y)$ 作为选择的特殊明文,并且还知道对应的密文.攻击的具体过程如下所述.

4.1. 恢复密钥 $A(x,y)$

设输入的明文为冲击函数 $\delta(x,y)$,此冲击函数在(0,0)处为 1,其余为 0.由加密方程(6)式得到其密文为

$$\begin{aligned} K(x',y') &= \mathrm{FT}[f(x,y)\cdot A(x,y)]\cdot B(x',y') \\ &= \mathrm{FT}[\delta(x,y)\cdot A(x,y)]\cdot B(x',y') \\ &= \mathrm{FT}[\delta(x,y)\cdot A(0,0)]\cdot B(x',y') \\ &= \mathrm{FT}[\delta(x,y)\cdot A(0,0)]\cdot B(x',y') \\ &= A(0,0)\cdot B(x',y'). \end{aligned} \tag{7}$$

同理,当冲击函数 $\delta(x,y)$ 在 (i,j) 处为 1,其余为 0 时,我们可以得到

$$K'(x',y') = A(i,j)\cdot B(x',y'). \tag{8}$$

联立(7),(8)式,我们可以得到

$$\frac{K'(x',y')}{K(x,y)} = \frac{1}{A(0,0)}A(i,j)\cdot I, \tag{9}$$

I 为全 1 的矩阵,$K(x',y')$,$K'(x',y')$ 都是已知量,设 $A(0,0)$ 为参考点,其值可以为任意非零值,从而得到 $A(i,j)$ 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,我们就可以得到密钥 $A(x,y)$ 的值,这些值都是相对参考点的值.

设 $A'(x,y) = \dfrac{K'(x',y')}{K(x,y)}$ 为恢复的密钥,则其与真实密钥 $A(x,y)$ 的关系可以表示为

$$A'(x,y) = \frac{1}{A(0,0)}A(x,y). \tag{10}$$

恢复的密钥与真实密钥只差一个常数因子,但不会影响解密结果,在后面的证明中可以看到.

4.2. 利用恢复的密钥 $A'(x,y)$ 求解密钥 $B(x',y')$

首先加密另外一个任意明文 $f_2(x,y)$,由加密方程(6)式得到其密文为

$$\begin{aligned} K_2(x',y') &= \mathrm{FT}[f_2(x,y)A(x,y)] \\ &\quad \times B(x',y'). \end{aligned} \tag{11}$$

将恢复得到的密钥 $A'(x,y)$ 代入上式,并设待恢复的密钥为 $B(x',y')$,则

$$\begin{aligned} K_2(x',y') &= \mathrm{FT}[f_2(x,y)A'(x,y)] \\ &\quad \times B'(x',y'), \end{aligned} \tag{12}$$

所以可以得出密钥

$$B'(x',y') = \frac{K_2(x',y')}{\mathrm{FT}[f_2(x,y)\cdot A'(x,y)]}. \tag{13}$$

将(11)式代入(13)式,简化(13)式,可以得到

$$\begin{aligned} B'(x',y') &= \frac{K_2(x',y')}{\mathrm{FT}[f_2(x,y)\cdot A'(x,y)]} \\ &= \frac{\mathrm{FT}[f_2(x,y)\cdot A(x,y)]\cdot B(x',y')}{\mathrm{FT}[f_2(x,y)\cdot A'(x,y)]} \\ &= \frac{\mathrm{FT}[f_2(x,y)\cdot A(x,y)]}{\mathrm{FT}[f_2(x,y)\cdot A(x,y)]} \\ &\quad \times B(x',y')\cdot A(0,0) \\ &= B(x',y')\cdot A(0,0). \end{aligned} \tag{14}$$

可以得到恢复的密钥与真实密钥之间的关系为

$$B'(x',y') = B(x',y')\cdot A(0,0). \tag{15}$$

恢复的密钥与真实密钥也只差一个常数因子,但不会影响解密结果,随后的数值仿真实验也证明了这一点.

4.3. 利用恢复的密钥解密其他密文

假设攻击者截获一任意密文 $K_i(x',y')$,其对应的明文为 $f_i(x,y)$,二者满足加密方程(6)式,即

$$K_i(x',y') = \mathrm{FT}[f_i(x,y)A(x,y)]B(x',y'). \tag{16}$$

现利用恢复的密钥 $A'(x,y)$ 和 $B'(x',y')$ 解密

$K_i(x',y')$，设待恢复的明文为 $f_i'(x,y)$，$A(x,y)^*$，$A'(x,y)^*$，$B(x',y')^*$，$B'(x',y')^*$ 分别为 $A(x,y)$，$A'(x,y)$，$B(x',y')$，$B'(x',y')$ 的复共轭，$|B(x',y')|=1$，$|A(x,y)|=1$，则

$$\begin{aligned}
f_i'(x,y) &= \mathrm{FT}^{-1}[K_i(x',y')\cdot B'(x',y')^*]\cdot A'(x,y)^* \\
&= \mathrm{FT}^{-1}[K_i(x',y')\cdot B'(x',y')^*]\cdot A'(x,y)^* \\
&= \mathrm{FT}^{-1}\left\{\mathrm{FT}[f_i(x,y)\cdot A(x,y)]\cdot B(x',y')\cdot B'(x',y')^*\right\}\cdot A'(x,y)^* \\
&= \mathrm{FT}^{-1}\left\{\mathrm{FT}[f_i(x,y)\cdot A(x,y)]\cdot B(x',y')\cdot B(x',y')^*\cdot A(0,0)^*\right\}\cdot A'(x,y)^* \\
&= \mathrm{FT}^{-1}\left\{\mathrm{FT}[f_i(x,y)\cdot A(x,y)]\cdot |B(x',y')|^2\cdot A(0,0)^*\right\}\cdot A'(x,y)^* \\
&= A(0,0)^*\cdot \mathrm{FT}^{-1}\left\{\mathrm{FT}[f_i(x,y)\cdot A(x,y)]\right\}\cdot A'(x,y)^* \\
&= A(0,0)^*\cdot f_i(x,y)\cdot A(x,y)\cdot A'(x,y)^* \\
&= A(0,0)^*\cdot f_i(x,y)\cdot A(x,y)\cdot A(x,y)^*\cdot \frac{1}{A(0,0)^*} \\
&= f_i(x,y)\cdot |A(x,y)|^2 \\
&= f_i(x,y).
\end{aligned} \tag{17}$$

所以 $f_i'(x,y)=f_i(x,y)$，此解密结果是无损的.

5. 模拟实验及结果分析

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. 设入射波长 $\lambda=633$ nm，$D_1=1$ m，$D_2=2$ m，两个随机相位函数 $R_1(x,y)$ 和 $R_2(x',y')$ 如图 2 所示. 首先利用这些加密参数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 $A(x,y)$. 然后加密其他任意一个明文，得到相应的密文，利用已经恢复的密钥 $A'(x,y)$ 和加密系统的加密方程，得出双随机相位加密系统的密钥 $B'(x',y')$. 图 3(a) 是一幅灰度图 Pepper($256\times256\times8$ bit)，图 3(b) 是灰度图像加密后的密文，图 3(c) 用选择明文攻击方法恢复的密钥进行解密的结果. 图 4(a) 是一幅二值图($256\times256\times8$ bit)，图 4(b) 是二值图加密后的密文，图 4(c) 是用选择明文攻击方法恢复的密钥进行解密的结果.

为了客观评价解密效果，我们引入几个标准来评价解密结果的质量，它们分别是归一化均方误差(NMSE)、归一化信噪比(NSNR)、图像逼真度(IF)，定义如下：

$$\mathrm{NMSE}=\frac{\sum_i\sum_j[f(i,j)-f_D(i,j)]^2}{\sum_i\sum_j[f(i,j)]^2}, \tag{18}$$

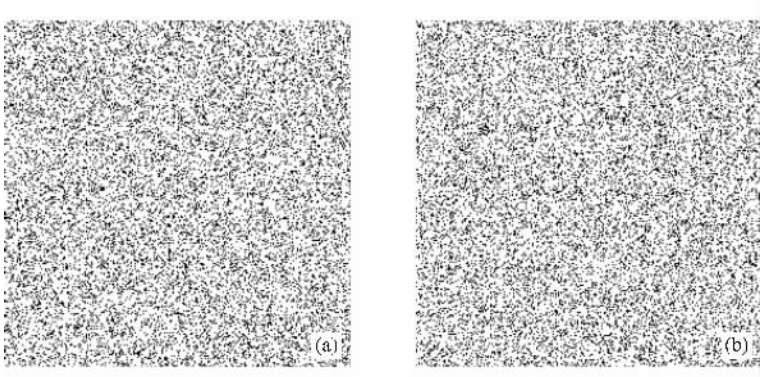

图 2　菲涅耳域双随机相位加密系统中的随机相位函数　(a) 随机相位函数 $R_1(x,y)$；(b) 随机相位函数 $R_2(x',y')$

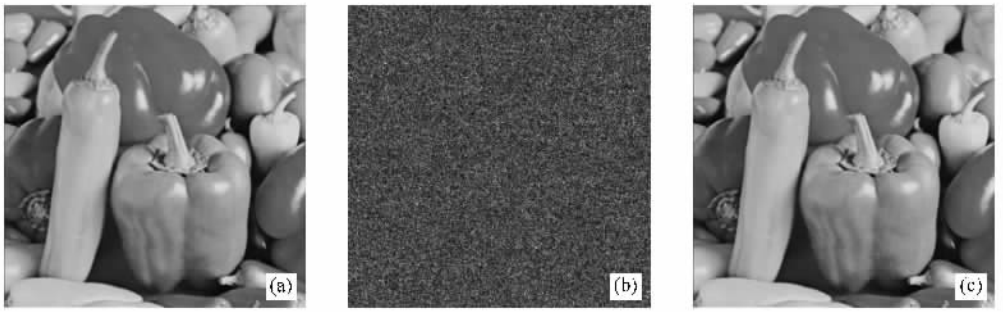

图 3 灰度图像的模拟实验结果 (a)灰度图(明文);(b)相应的密文;(c)用攻击所得密钥进行解密的结果

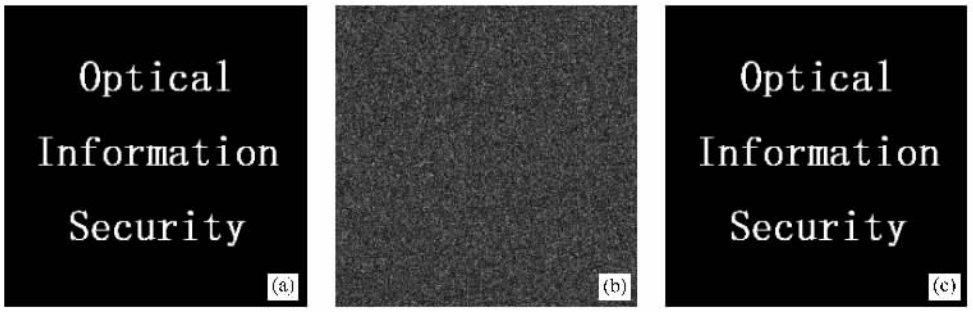

图 4 二值图像的模拟实验结果 (a)二值图(明文);(b)相应的密文;(c)用攻击所得密钥进行解密的结果

$$\mathrm{NSNR} = -10\log_{10}(\mathrm{NMSE}), \tag{19}$$

$$\mathrm{IF} = 1 - \mathrm{NMSE}, \tag{20}$$

其中 $f(i,j)$ 为经采样后原图像幅值分布,$f_D(i,j)$ 为解密的图像幅值分布,由(18)—(20)式可知,归一化均方误差表示解密图像与原图像之间相应像素幅值误差的统计关系,显然,值越小,从统计意义上的解密图像与原图像的差异越小,信噪比越高,逼真度越高.根据以上三式对灰度图和二值图的解密结果进行相应计算,结果见表 1.

从表 1 可以看出,用选择明文攻击方法得到的解密结果的均方误差为 0,逼真度为 1,这说明解密结果是无损的,实验结果与理论推导一致.

表 1 灰度图和二值图的解密结果的客观评价

	归一化均方误差	归一化信噪比	图像逼真度
灰度图像	0	∞	1
二值图像	0	∞	1

我们从恢复的密钥 $B'(x',y')$ 的内中心取出 $n \times n$ ($n \leqslant 256$) 的像素作为解密密钥,来观察解密结果,n 称为窗口矩阵的尺寸.以二值图为例,图 5(a)是用 64×64 的密钥恢复的结果,图 5(b)是用 96×96 的密钥恢复的结果,图 5(c)是用 128×128 的密钥恢复的结果.从解密结果可以看出,我们可以使用

图 5 用恢复的部分密钥解密的结果 (a)用 64×64 的密钥恢复的结果;(b)用 96×96 的密钥恢复的结果;(c)用 128×128 的密钥恢复的结果

其中的部分密钥进行解密.表 2 给出了用不同部分密钥解密的结果评价.

表 2　用不同部分密钥的解密结果的评价

解密秘密的数目	归一化均方误差	归一化信噪比	图像逼真度
64 × 64	0.7532	1.2307	0.2468
96 × 96	0.5613	2.5080	0.4387
128 × 128	0.4568	3.4027	0.5432

从表 2 中数据可以看出,使用部分密钥解密的图像与原图像均方误差很大,即与原图像差异大,信噪比很小,与原图像的逼真度小,解密密钥越多,解密效果越好.由系统的加密方程(6)式可以看出,其与标准的 4f 双随机相位加密系统的加密方程是一致的,明文信息经过傅里叶变换加密,其信息已全部分布在整个密文中,密文的每一点都包含了明文的全部信息,所以用部分密文来恢复明文也是可行的,

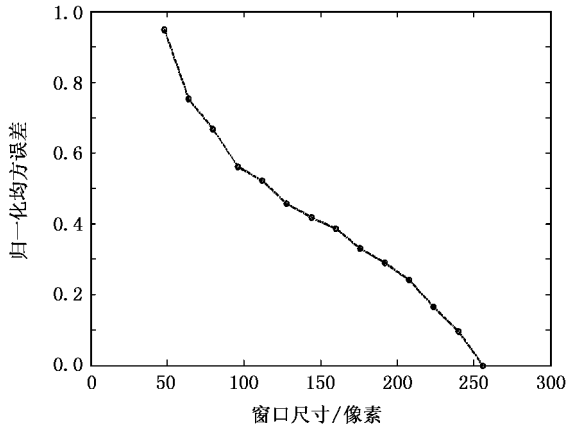

图 6　归一化均方误差随选取密钥窗口尺寸的变化情况

而使用部分密文来恢复明文等价于使用部分密钥 $B'(x',y')$ 来恢复明文,这由下式可以看出:

$$P \cdot K(x',y') = \mathrm{FT}[f(x,y)A(x,y)] \times B(x',y') \cdot P, \qquad (21)$$

P 表示密钥选取 $n \times n$ ($n \leqslant 256$) 的窗口矩阵,中间部分为 1,其余部分为 0.归一化均方误差 NMSE 随密钥选取矩阵窗口尺寸的变化如图(6)所示,从图中可以看出,NMSE 随密钥选取窗口尺寸的增大而逐渐变小.

6. 结　论

1. 我们从理论上推导了菲涅耳域双随机相位加密系统的选择明文攻击的过程,虽然推导出的密钥与真实密钥相差一个常数因子,但解密结果却是无损的,其根本原因在于菲涅耳域双随机相位加密系统是一个线性系统.

2. 通过模拟实验证明,可以通过其中的部分密钥来恢复明文.由于明文信息经过傅里叶变换加密,其信息已全部分布在整个密文中,密文的每一点都包含了明文的全部信息,所以用部分密文来恢复明文也是可行的.

3. 菲涅耳域双随机相位加密系统相对于标准的 4f 双随机相位加密来说,增加了密钥的维数,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淆和扩散的原则,也就是是否存在非线性变换.菲涅耳双随机相位加密系统仍是一个典型的线性系统,所以其安全性并没有提高.

[1] Refregier P, Javidi B 1995 *Opt. Lett.* **20** 767

[2] Peng X, Yu L F, Cai L L 2001 *Opt. Express* **10** 41

[3] Peng X, Cui Z Y, Tan T N 2002 *Opt. Commun.* **212** 235

[4] Peng X, Zhang P, Niu H B 2004 *Acta Opt. Sin.* **24** 623 (in Chinese) [彭　翔、张　鹏、牛憨笨 2004 光学学报 **24** 623]

[5] Yang X P, Zhai H C 2005 *Acta Phys. Sin.* **54** 1578 (in Chinese) [杨晓苹、翟宏琛 2005 物理学报 **54** 1578]

[6] Carnicer A, Usategui M M, Arcos S, Juvells I 2005 *Opt. Lett.* **30** 1644

[7] Peng X, Zhang P, Wei H Z, Yu B 2006 *Acta Phys. Sin.* **55** 1130 (in Chinese) [彭　翔、张　鹏、位恒政、于　斌 2006 物理学报 **55** 1130]

[8] Gopinathan U, Monaghan D S, Naughton T J, Sheridan J T 2006 *Opt. Express* **14** 3181

[9] Frauel Y, Castro A, Naughton T J, Javidid B 2005 *Proc. SPIE* **5986** 25

[10] Fienup J 1982 *Appl. Opt.* **21** 2758

[11] Yu B, Peng X, Tian J D, Niu H B 2005 *Acta Phys. Sin.* **54** 2034 (in Chinese) [于　斌、彭　翔、田劲东、牛憨笨 2005 物理学报 **54** 2034]

[12] Situ G H, Zhang J J 2004 *Opt. Lett.* **29** 1584

[13] Teng S Y, Cheng C F, Liu M, Liu L R, Xu Z Z 2003 *Acta Phys. Sin.* **52** 316 (in Chinese) [滕树云、程传福、刘　曼、刘立人、徐至展 2003 物理学报 **52** 316]

[14] Stallings W 1999 *Cryptography and Network Security : Principles and Practice* 2nd Ed. (New Jersey : Prentice Hall) p24

Chosen plaintext attack on double random-phase encoding in the Fresnel domain *

Peng Xiang[1)2)†] Wei Heng-Zheng[1)] Zhang Peng[3)]

1) (*National Laboratory of Precision Measurement Technology and Instrumentation, Tianjin University, Tianjin* 300072, *China*)

2) (*Institute of Optoelectronics, Shenzhen University, Key Laboratory of Optoelectronics Devices and Systems of Education Ministry, Shenzhen* 518060, *China*)

3) (*Electronic Banking Department, China Construction Bank, Beijing* 100032, *China*)

(Received 28 July 2006; revised manuscript received 27 October 2006)

Abstract

This paper analyzes the security of double random phase encoding in fresnel domain from the viewpoint of cryptoanalysis. We demonstrate the encryption system is vulnerable to chosen-plaintext attack with a prior knowledge of diffraction distance and wavelength. With this attack an opponent can access double random phase keys with the help of the impulse functions as chosen plaintext. The significant feature of proposed attack is that the decryption process is lossless. Numerical simulations show good agreement with theoretical analysis.

Keywords: information optics, double random phase encoding, chosen-plaintext attack, Fresnel transform

PACC: 4230, 4225K, 0650D

* Project supported by the National Natural Science Foundation of China (Grant No. 60472107), the Natural Science Foundation of Guangdong Province (Grant No. 04300862), the Science and Technology Bureau of Shenzhen (Grant No. 200426), and Shanghai Institute of Microsystem and Information Technology.

† E-mail: xpeng@szu.edu.cn