第 55 卷 第 3 期 2006 年 3 月
1000-3290/2006/55(03)/1130-07

物 理 学 报
ACTA PHYSICA SINICA

Vol.55,No.3,March,2006

双随机相位加密系统的已知明文攻击*

彭 翔[1)2)] 张 鹏[2)†] 位恒政[2)] 于 斌[1)]

1)(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)

2)(天津大学精密测试技术及仪器国家重点实验室,天津 300072)

(2005 年 9 月 1 日收到;2005 年 11 月 11 日收到修改稿)

运用密码分析学的方法对双随机相位加密系统进行了初步的安全性分析.研究结果表明,该系统属于线性的对称分组密码系统,线性性质为其安全性留下隐患.在已知明文攻击下,攻击者可通过常规的相位恢复算法获得 4-f 系统输入平面的随机相位函数密钥,继而可轻易推出频谱平面的随机相位函数密钥,从而攻破此密码系统.

关键词:光学信息安全,双随机相位加密,密码分析学,已知明文攻击

PACC:4230,0650D,9575M

1. 引 言

基于光学理论与方法的数据加密和隐藏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.在采用光学方法对图像进行加密和解密方面,Javidi 的研究成果最具有代表性.自 1995 年提出在标准 4-f 光信号处理器中通过双随机相位编码进行数据加密的光学方法以来[1],不断发表了相关的采用光学方法实现图像加密和隐藏的研究报道[2—8],并获得多项美国专利[9—11].然而,双随机相位加密系统虽然在光学信息安全领域得到了广泛研究,但其安全性始终未得到正式的证明.并且,该密码系统采用 4-f 系统的输出平面(像面)作为密文,这样无疑使得密码系统的明文和密文满足了物像关系,密码系统从本质上来说是一种线性系统.对线性系统而言,其明文、密文、密钥之间的函数依赖关系比较简单,这就为其安全性留下很大的隐患.2005 年 Carnicer 等人通过"选择密文攻击"的办法可以分析得到双随机相位加密系统的会话密钥[12].但是,"选择密文攻击"需要攻击者选择大量的精心设计的密文,攻击实施起来难度较大且复杂.并且,该方法仅能够获得 4-f 系统频谱平面的随机相位函数密钥,而不能获得输入平面的随机相位函数密钥,并且当明文信息为复函数时失效.

本文提出了一种"已知明文攻击"的方法,相对于 Carnicer 等人的"选择密文攻击"来说,攻击实施的难度大大降低,所需要的资源也很少,攻击者只需一个明文-密文对,即可分析获得双随机相位加密系统的会话密钥,从而攻破该密码系统.并且,本方法可同时获得 4-f 系统输入平面的随机相位函数密钥和频谱平面的随机相位函数密钥,因此也适用于明文信息为复函数时的情况.

2. 双随机相位加密系统的已知明文攻击分析

2.1. 双随机相位加密系统

如图 1 所示,双随机相位加密系统采用标准 4-f 系统来实现.用信息光学理论描述:加密时,输入信号(图像)在空间域受到随机相位函数 $\exp[\mathrm{j}n(x,y)]$ 的调制,在频率域被随机相位函数 $\exp[\mathrm{j}b(\alpha,\beta)]$ 滤波,表示为

$$\psi(x,y) = \{f(x,y)\exp[\mathrm{j}n(x,y)]\} * \mu(x,y), \tag{1}$$

其中 $\mu(x,y) = \mathrm{FT}^{-1}\{\exp[\mathrm{j}b(\alpha\beta)]\}$. $n(x,y)$, $b(\alpha,\beta)$ 代表两分布于 $[0,2\pi]$ 独立的白噪声序列,

* 国家自然科学基金(批准号:60472107,60275012)及广东省自然科学基金(批准号:04300862)及深圳市科技计划项目(批准号:200426)资助的课题.

†E-mail:pengzhang@tju.edu.cn

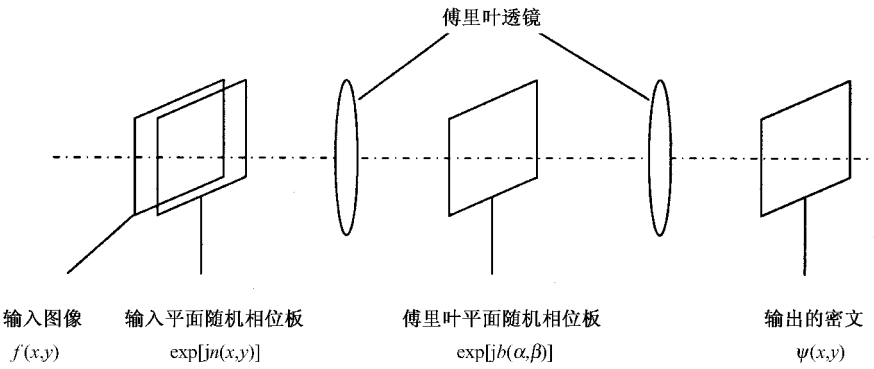

图 1　双随机相位加密系统示意图

$FT^{-1}\{\}$ 代表逆傅里叶变换，$*$ 代表卷积运算.

上述加密过程在频率域中的表示为

$$\psi(\alpha,\beta) = FT\{f(x,y)\exp[jn(x,y)]\} \times \exp[jb(\alpha,\beta)], \quad (2)$$

其中 $FT\{\}$ 代表傅里叶变换.

解密时，将加密后的图像 $\psi(x,y)$ 置于 4-f 系统的输入端，经傅里叶变换后，在频谱平面上用相位函数 $\exp[-jb(\alpha,\beta)]$（解密密钥）滤波，再经逆傅里叶变换，即可恢复出 $f(x,y)\exp[jn(x,y)]$. 因为图像 $f(x,y)$ 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 $f(x,y)$，表示为

$$\begin{aligned} D(x,y) &= FT^{-1}\{\psi(\alpha,\beta)\exp[-jb(\alpha,\beta)]\} \\ &= FT^{-1}\{FT\{f(x,y)\exp[jn(x,y)]\} \\ &\quad \times \exp[jb(\alpha,\beta)]\exp[-jb(\alpha,\beta)]\} \\ &= f(x,y)\exp[jn(x,y)]. \end{aligned} \quad (3)$$

2.2. 密码分析学与已知明文攻击

密码学包括密码编码学和密码分析学两个方面的内容. 在密码分析学中，根据攻击者所掌握的信息，可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、选择密文攻击等[13,14].

本文将着重讨论如何利用已知明文攻击来攻破双随机相位加密系统. 从抽象的观点看，若用 E 表示密码算法，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，则已知明文攻击的办法即为已知 $p_i, c_i = E_k(p_i)$，$1 \leqslant i \leqslant l$，推出 k，或从 $c_{l+1} = E_k(p_{l+1})$ 求出 p_{l+1} 的算法. 因为选择明文攻击和选择密文攻击提供给攻击者可利用的资源更多，故若已知明文攻击能够成功，显然选择明文攻击和选择密文攻击亦有效.

2.3. 双随机相位加密系统的已知明文攻击

在对密码系统进行密码分析时，通常认为攻击者已经知晓密码算法的工作过程，即满足 Kerekboffs 假设[13,14]. 下面利用已知明文攻击的方法来分析双随机相位加密系统，假定攻击者已经掌握若干密文（加密后的图像），并且还知道对应的明文（原始图像）本身. 攻击者取出其中的一个明文-密文对

$$\{f_i(x,y),\psi_i(x,y)\},$$

其中

$$\psi_i(x,y) = \{f_i(x,y)\exp[jn(x,y)]\} * \mu(x,y).$$

攻击的过程分为以下两个步骤.

2.3.1. 利用相位恢复算法获得输入平面的随机相位函数密钥

在已知明文攻击的条件下，攻击者已获知一个明文-密文对 $\{f_i(x,y),\psi_i(x,y)\}$，对 $\psi_i(x,y)$ 取傅里叶变换可得 $\psi_i(\alpha,\beta)$，由密码系统的加密方程（见(2)式）可得

$$\psi_i(\alpha,\beta) = FT\{f_i(x,y)\exp[jn(x,y)]\} \times \exp[jb(\alpha,\beta)], \quad (4)$$

其中，令 $G_i(x,y) = f_i(x,y)\exp[jn(x,y)]$，$G_i(\alpha,\beta) = FT\{G_i(x,y)\}$，可得

$$\begin{aligned} \psi_i(\alpha,\beta) &= FT\{G_i(x,y)\}\exp[jb(\alpha,\beta)] \\ &= G_i(\alpha,\beta)\exp[jb(\alpha,\beta)]. \end{aligned} \quad (5)$$

(5)式两端“取模”得

$$|\psi_i(\alpha,\beta)| = |G_i(\alpha,\beta)|, \quad (6)$$

又因为

$$\begin{aligned} |G_i(x,y)| &= |f_i(x,y)\exp[jn(x,y)]| \\ &= f_i(x,y). \end{aligned} \quad (7)$$

由(6)，(7)式注意到：此时攻击者已知明文（原始图像）$f_i(x,y)$ 和对应的密文（加密后的图像）$\psi_i(x,$

$y)$，寻找输入平面密钥 $\exp[\mathrm{j}n(x,y)]$ 的问题已经转化为已知物平面上的强度信息 $|G_i(x,y)|$（即 $f_i(x,y)$）和傅里叶平面上的强度信息 $|G_i(\alpha,\beta)|$（即 $|\psi_i(\alpha,\beta)|$），如何去恢复物平面上的相位信息 $\exp[\mathrm{j}n(x,y)]$，其中 $G_i(\alpha,\beta)$ 是 $G_i(x,y)$ 的傅里叶变换．这是一个标准的相位恢复问题，可以用多种已知的相位恢复算法[15—18]进行迭代求解．本文采用了 Fienup 提出的迭代的相位恢复算法 HIO（hybrid input-output alnorithm）[16]进行相位恢复，来寻找输入平面的随机相位函数密钥 $\exp[\mathrm{j}n(x,y)]$．该相位恢复算法是对经典 Gerchberg-Saxton（GS）相位恢复算法[15]的一种改进，具有收敛速度快，误差小等特点．我们利用 HIO 相位恢复算法在物平面和傅里叶平面之间反复进行算法迭代来寻找随机相位函数密钥 $\exp[\mathrm{j}n(x,y)]$，直到定义的误差-均方差之和（sum square error，SSE）达到设计精度或者达到设置的最大迭代次数为止．SSE 定义为

$$\mathrm{SSE} = 10\log\frac{\sum[\rho-\rho^{(n)}]^2}{\sum\rho^2}, \tag{8}$$

式中 ρ 代表物平面上的已知振幅分布（即 $f_i(x,y)$），$\rho^{(n)}$ 代表第 n 次迭代结束时，物平面上的振幅分布．

2.3.2. 由输入平面密钥推导出频谱平面密钥

在已知明文攻击的条件下，若攻击者已通过常规的相位恢复算法获得了 4-f 系统输入平面的随机相位函数密钥 $\exp[\mathrm{j}n(x,y)]$，又因为明文 $f_i(x,y)$ 和密文 $\psi_i(x,y)$ 为已知，则由(4)式，可立刻给出其频谱平面的随机相位函数密钥，表示为

$$\exp[-\mathrm{j}b(\alpha,\beta)] = \frac{\mathrm{FT}\{f_i(x,y)\exp[\mathrm{j}n(x,y)]\}}{\psi_i(\alpha,\beta)}. \tag{9}$$

至此，攻击者已经成功找到了双随机相位加密系统的两个加密密钥 $\exp[\mathrm{j}n(x,y)]$ 和 $\exp[\mathrm{j}b(\alpha,\beta)]$，从而攻破了该密码系统．

3．模拟实验及其结果

我们在 MATLAB6.1 环境下对本文提出的已知明文攻击方法进行了数字仿真实验．假定攻击者已经掌握了一个明文-密文对，明文为灰度图 Pepper（$256\times256\times8$bit），如图 2(a)所示，对应的经过双随机相位加密系统加密后的密文如如图 2(b)所示．

采用 Fienup 的迭代的相位恢复算法 HIO[16] 进行相位恢复，计算迭代 1500 次恢复的相位分布（即恢复的输入平面随机相位函数密钥），如图 3(a)所示．HIO 相位恢复迭代算法中 SSE 和迭代次数 N 的关系如图 3(b)所示，从图中可看出，算法开始收敛速度较快，且迭代次数越高精度越高，但在 1000 至 1500 次左右曲线收敛趋于平缓．也就是说，利用相位恢复算法寻找 4-f 系统输入平面随机相位函数密钥 $\exp[\mathrm{j}n(x,y)]$ 的过程是一个迭代优化的过程，当迭代次数小于 1500 时，输入平面密钥恢复的精度会随着迭代次数的增加而提高；当迭代次数大于 1500 时，密钥恢复的精度没有更多的改善．

密码系统后续传来的密文如图 4(a)所示，相应的原来的明文如图 4(b)所示，是一幅灰度图 Lena（$256\times256\times8$ bit）．利用本文提出的已知明文攻击方法可以找出密码系统的会话密钥 $\exp[\mathrm{j}n(x,y)]$ 和 $\exp[\mathrm{j}b(\alpha,\beta)]$，进而正确解密该密文，如图 4(c)所示．从实验结果可以看出，我们已能够辨认出解密后图像的细节，恢复出明文信息．但是，解密出来的灰度图像比较模糊，噪声比较大．这是因为在采用相位恢复算法 HIO 进行相位恢复（即恢复输入平面随机相位函数密钥）时，由于算法本身的性能以及初始相位选择的随机性引入的误差．应用更为有效的相位恢复算法，如 Yang-Gu[19—21] 算法或迭代角谱算法[22]，有可能进一步改善恢复密钥的质量．

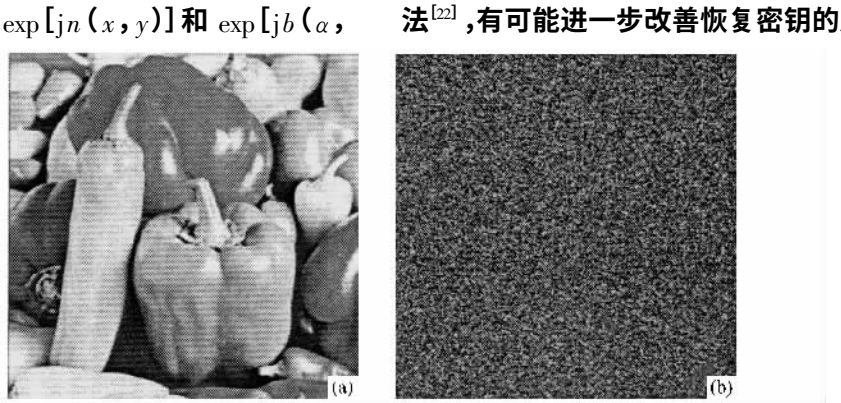

图 2 攻击者已知的一个明文-密文对 (a)明文；(b)相应的密文

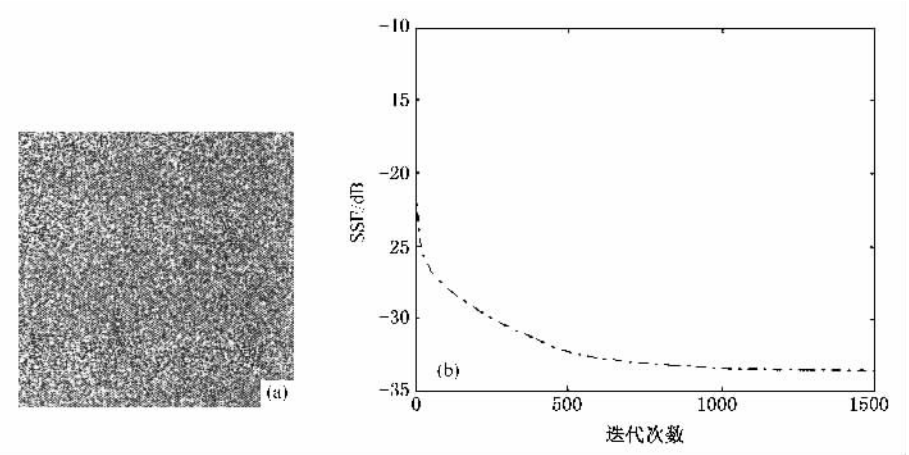

图 3　输入平面随机相位函数密钥的恢复结果　(a)恢复的输入平面密钥；(b)SSE 随迭代次数的收敛情况

图 4　灰度图像的模拟实验结果　(a)后续传来的密文；(b)相应的原来的明文；(c)运用攻击所得的会话密钥解密出来的结果

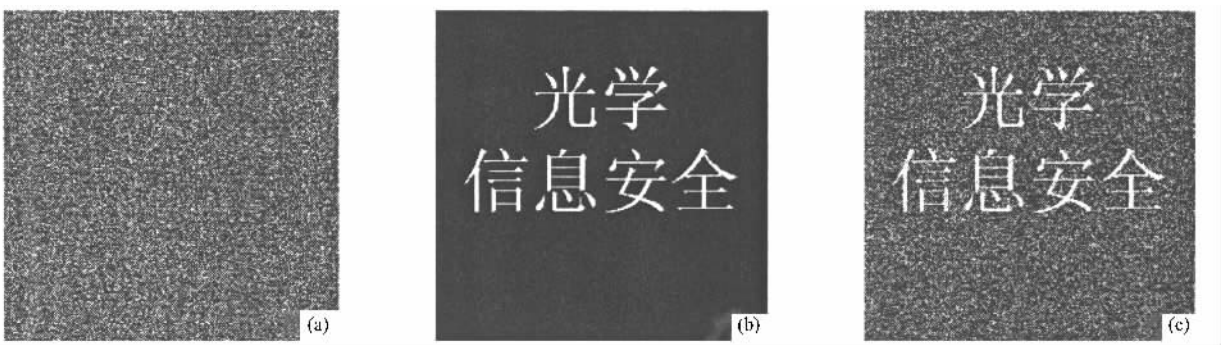

图 5　二值图像的模拟实验结果　(a)后续传来的密文；(b)相应的原来的明文；(c)运用攻击所得的会话密钥解密出来的结果

图 5(a)—(c)所示是对二值图像的模拟实验结果.在运用相位恢复迭代算法寻找输入平面密钥的过程中,灰度图像和二值图像的 SSE 收敛曲线的比较,如图 6 所示.对于二值图像,由于只涉及 0 和 1 两种灰度值,且相比灰度图像具有最大的对比度,故解密图像的信噪比要好得多.

4. 几点讨论

4.1. 明文为复函数时的情况

前面的讨论假定明文 $f(x,y)$ 为正、实函数(图像信息),已经证明本文所述攻击方法适用.此时解密过程只需频谱平面密钥 $\exp[-jb(\alpha,\beta)]$,乘积 $f(x,y)\exp[jn(x,y)]$ 只需经过 CCD 等强度探测器件即可恢复出明文信息 $f(x,y)$.

然而,当明文 $f(x,y)$ 为复函数时,必须同时获取输入平面的解密密钥 $\exp[-jn(x,y)]$ 和频谱平面的解密密钥 $\exp[-jb(\alpha,\beta)]$ 才可解密出正确的明文信息[2].设已知的明文-密文对为 $\{f_i(x,y),\psi_i(x,y)\}$,其中 $f_i(x,y)=|f_i(x,y)|,\exp[jp(x,y)]$,由密码系统的加密方程(见(2)式)可得

$$\psi_i(\alpha,\beta)=\mathrm{FT}\{f_i(x,y)\exp[jn(x,y)]\}\exp[jb(\alpha,\beta)]$$

$$= \mathrm{FT}\{f_i(x,y) \cdot \exp[\mathrm{j}p(x,y) + n(x,y))]\}\exp[\mathrm{j}b(\alpha,\beta)]. \quad (10)$$

令 $M_i(x,y) = |f_i(x,y)|\exp[\mathrm{j}p(x,y) + n(x,y))]$，$M_i(\alpha,\beta) = \mathrm{FT}\{M_i(x,y)\}$ 可得

$$\psi_i(\alpha,\beta) = M_i(\alpha,\beta)\exp[\mathrm{j}b(\alpha,\beta)]. \quad (11)$$

(11)式两端‘取模’得

$$|\psi_i(\alpha,\beta)| = |M_i(\alpha,\beta)|, \quad (12)$$

又因为

$$|M_i(x,y)| = |f_i(x,y)|. \quad (13)$$

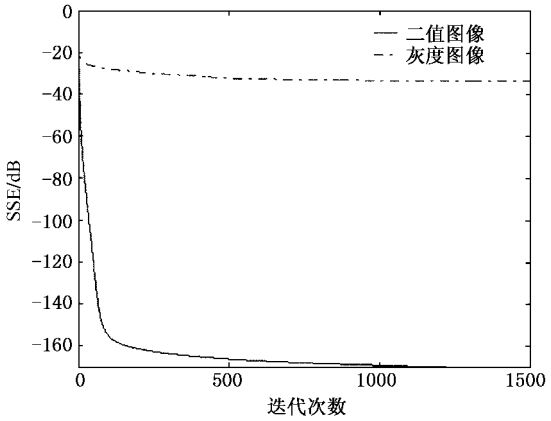

图 6 在运用相位恢复算法寻找输入平面密钥的过程中，灰度图像和二值图像的 *SSE* 随迭代次数的收敛情况比较

由(12)，(13)式注意到：此时，攻击者仍可从物平面上的强度信息 $|M_i(x,y)|$（即 $|f_i(x,y)|$）和傅里叶平面上的强度信息 $|M_i(\alpha,\beta)|$（即 $|\psi_i(\alpha,\beta)|$），通过常规的相位恢复算法进行迭代求解，恢复出物平面上的相位信息 $\exp[\mathrm{j}(p(x,y) + n(x,y))]$，又因为 $f_i(x,y)$ 的相位信息 $\exp[\mathrm{j}p(x,y)]$ 为已知条件，显然可立刻求出 4-f 系统输入平面密钥 $\exp[\mathrm{j}n(x,y)]$. 同上，由输入平面密钥可立刻推出频谱平面密钥 $\exp[\mathrm{j}b(\alpha,\beta)]$（见(9)式）. 因此，本文所提出的攻击方法同样适用于明文信息为复函数时的情况.

4.2. 攻击的光学实现

下面给出一种可能的已知明文攻击的光学实现方式. 设已知的明文-密文对为 $\{f_i(x,y),\psi_i(x,y)\}$，首先攻击者利用这个明文-密文对，通过常规的相位恢复算法获得 4-f 系统输入平面的随机相位函数密钥 $\exp[\mathrm{j}n(x,y)]$. 其次，将 $f_i(x,y)$ 与获得的输入平面密钥 $\exp[\mathrm{j}n(x,y)]$ 相乘，对乘积 $f_i(x,y)\exp[\mathrm{j}n(x,y)]$ 做傅里叶变换并取共轭后置于标准 4-f 系统的频谱平面，然后将密文 $\psi_i(x,y)$ 置于 4-f 系统的输入平面. 这样，4-f 系统输出平面的傅里叶变换即为 $A\exp[\mathrm{j}b(\alpha,\beta)]$，其中 A 为振幅. 即攻击者成功找到了双随机相位加密系统的两个加密密钥 $\exp[\mathrm{j}n(x,y)]$ 和 $\exp[\mathrm{j}b(\alpha,\beta)]$，从而可以攻破该密码系统. 用公式表示为

$$\begin{aligned} K(\alpha,\beta) &= \mathrm{FT}\{\psi_i(x,y)\}\mathrm{FT}^*\{f_i(x,y)\exp[\mathrm{j}n(x,y)]\} \\ &= \mathrm{FT}\{f_i(x,y)\exp[\mathrm{j}n(x,y)]\}\exp[\mathrm{j}b(\alpha,\beta)] \\ &\quad \times \mathrm{FT}^*\{f_i(x,y)\exp[\mathrm{j}n(x,y)]\} \\ &= |\mathrm{FT}\{f_i(x,y)\exp(\mathrm{j}n(x,y)]\}|^2 \\ &\quad \times \exp[\mathrm{j}b(\alpha,\beta)], \end{aligned} \quad (14)$$

其中 $K(\alpha,\beta)$ 是 4-f 系统输出平面的傅里叶变换.

注意到

$$\begin{aligned} |\psi_i(\alpha,\beta)| &= |\mathrm{FT}\{f_i(x,y)\exp[\mathrm{j}n(x,y)]\} \\ &\quad \times \exp[\mathrm{j}b(\alpha,\beta)]| \\ &= |\mathrm{FT}\{f_i(x,y)\exp[\mathrm{j}n(x,y)]\}|. \end{aligned} \quad (15)$$

将(15)式代入(14)式可得

$$K(\alpha,\beta) = |\psi_i(\alpha,\beta)|^2\exp[\mathrm{j}b(\alpha,\beta)]. \quad (16)$$

令 $A = |\psi_i(\alpha,\beta)|^2$，得

$$K(\alpha,\beta) = A\exp[\mathrm{j}b(\alpha,\beta)]. \quad (17)$$

$K(\alpha,\beta)$ 的相位部分即为双随机相位加密系统频谱平面密钥. 图 7 为攻击方法的光学实现原理图.

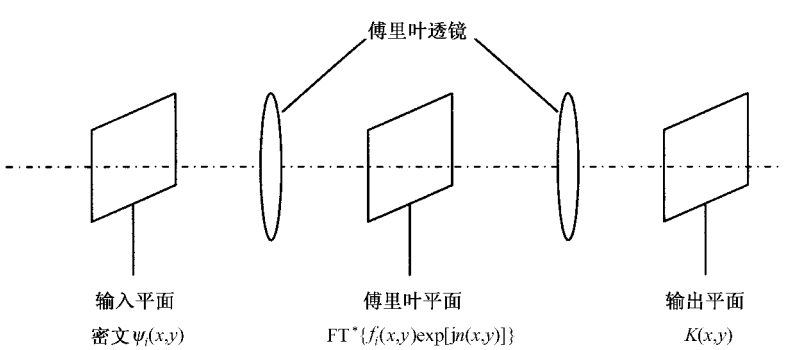

图 7 一种已知明文攻击的光学实现示意图. 其中，$K(x,y)$ 是 $K(\alpha,\beta)$ 的逆傅里叶变换

5. 结　论

本文提出了一种双随机相位加密系统的已知明文攻击方法，该方法使得攻击者只需通过一个明文-密文对，即可获得 4-f 系统输入平面的随机相位函数密钥和频谱平面的随机相位函数密钥. 与 Carnicer 等人的工作相比，本文提出的方法只需一个明文-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，所需的资源也很少. 同时，Carnicer 等人的攻击方法只适用于明文信息为实函数时的情况，而本文方法对于明文信息为复函数时的情况亦适用. 此外，本文还给出了一种可能的已知明文攻击的光学实现方式.

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

[2] Javidi B 1997 *Physics Today* **50** 27

[3] Javidi B, Sergent A, Zhang G *et al* 1997 *Opt. Eng.* **36** 992

[4] Javidi B, Zhang G, Li J 1997 *Appl. Opt.* **36** 1054

[5] Goudail F, Bollaro F, Javidi B *et al* 1998 *J. Opt. Soc. Am.* A **15** 2629

[6] Javidi B, Bemard L, Towghi N 1999 *Opt. Eng.* **38** 9

[7] Kishk S, Javidi B 2003 *Opt. Lett.* **28** 167

[8] Kishk S, Javidi B 2003 *Opt. Exp.* **11** 874

[9] Javidi B 1999 *U.S. patent* 6,002,773

[10] Javidi B 1999 *U.S. patent* 5,903,648

[11] Javidi B 2003 *U.S. patent* 6,519,340

[12] Camicer A, Usategui M M, Arcos S *et al* 2005 *Opt. Lett.* **30** 1644

[13] Feng D G 2000 Cryptography analysis (Beijing: Tsinghua University Press) p50 (in Chinese) [冯登国 2000 密码分析学(北京 清华大学出版社)第 50 页]

[14] Stallings W 1999 *Cryptography and Network Security: Principles and Practice*. 2nd Ed. (Upper Saddle River, NJ: Prentice Hall) p24

[15] Gerchberg R W, Saxton W O 1972 *Optik* **35** 237

[16] Fienup J R 1982 *Appl. Opt.* **21** 2758

[17] Bauschke H H, Combettes P L, Luke D R 2003 *J. Opt. Soc. Am.* A **20** 1025

[18] Bauschke H H, Combettes P L, Luke D R 2002 *J. Opt. Soc. Am.* A **19** 1334

[19] Yang G Z, Gu B Y 1981 *Acta Phys. Sin.* **30** 410 (in Chinese) [杨国桢、顾本源 1981 物理学报 **30** 410]

[20] Yang G Z, Gu B Y 1981 *Acta Phys. Sin.* **30** 414 (in Chinese) [杨国桢、顾本源 1981 物理学报 **30** 414]

[21] Yang G Z, Dong B Z, Gu B Y *et al* 1994 *Appl. Opt.* **33** 209

[22] Yu B, Peng X, Tian J D *et al* 2005 *Acta Phys. Sin.* **54** 2034 (in Chinese) [于　斌、彭　翔、田劲东等 2005 物理学报 **54** 2034]

Known-plaintext attack on double phase encoding encryption technique*

Peng Xiang[1)2)] Zhang Peng[2)] Wei Heng-Zheng[2)] Yu Bin[1)]

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

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

(Received 1 September 2005; revised manuscript received 11 November 2005)

Abstract

In the field of optical information security, the most attractive work is the so-called double-random-phase encoding encryption scheme proposed by Javidi. However, the security of this cryptosystem has not been analyzed thoroughly from the point of view of cryptoanalysis. In this article, the weakness of Javidi's optical security system is carefully analyzed with a known-plain text attack. It is shown that the double-random-phase encoding encryption scheme is a linear symmetric block cipher cryptosystem and its linearity opens avenues of attacks. Under the known-plaintext attack, attacker can obtain the phase key(s) in the input plane using the typical phase retrieval algorithms and subsequently deduce the phase key(s) in the Fourier domain easily. In addition, an optical implementation of known-plain text attack is also proposed.

Keywords: optical information security, double random phase encryption, cryptanalysis, known-plaintext attack

PACC: 4230, 0650D, 9575M

* Project supported by the National Natural Science Foundation of China (Grant Nos. 60472107, 60275012), the Natural Science Foundation of Guangdong Province (Grant No. 04300862), and the Science and Technology Bureau of Shenzhen (Grant No. 200426).