第 56 卷 第 5 期 2007 年 5 月
1000-3290/2007/56(05)/2629-08

物 理 学 报
ACTA PHYSICA SINICA

Vol.56,No.5,May,2007

双随机相位编码光学加密系统的唯密文攻击*

彭 翔† 汤红乔 田劲东

(深圳大学光电子学研究所,光电子器件与系统教育部重点实验室,深圳 518060)

(2006 年 8 月 14 日收到;2006 年 9 月 3 日收到修改稿)

针对双随机相位编码光学加密系统的安全性分析表明,该系统属于线性对称分组密码系统,其线性性质为安全性留下极大隐患.在唯密文攻击下,仅根据密文估计出物面波函数的‘支撑’(support),然后利用迭代相位恢复算法获得物面波函数(其振幅是明文信息),再根据物面波函数与频域密文的关系可推导出频谱平面的解密密钥.由于估计出来的物面波函数的‘支撑’相对于真实的物面波函数的‘支撑’有一定的平移,使得恢复的物面波函数与真实的物面波函数之间无论在振幅上还是相位上都存在平移,导致用推导出来的解密密钥去解密其他密文时所获得的明文与原始明文之间存在明显平移.然而,可依照这一先验信息,将估计出来的物面波函数的‘支撑’在物面内遍历,从而找到逼近真实解密密钥的解.利用此解密密钥去解密其他密文时获得更好的解密效果.

关键词:光学信息安全,双随机相位编码,唯密文攻击,函数支撑

PACC:4230,0650D

1. 引 言

基于光学理论与方法的数据加密技术是近年来国际上研究的热点.自 Refregier 和 Javidi 提出双随机相位编码光学加密方法以来[1],在此基础上衍生出现各种光学加密方法[2—6].在采用光学加密领域,Javidi 课题组的研究最具代表性[7—12],并获得多项美国专利保护[13—15].尽管双随机相位编码光学加密系统在光学信息安全领域得到广泛应用,但其安全性存在极大隐患:该密码系统把明文置于 4-f 光学系统的输入面,在输出面得到密文,这样使得明文和密文之间满足物像关系,密码系统从本质上说是一种线性系统.

Carnicer 等人通过‘选择密文攻击’的方法可以分析得到双随机相位编码光学加密系统的频谱平面密钥[16].但是,选择密文攻击需要攻击者选择大量精心设计的密文,攻击实施起来难度较大且复杂.Frauel 等人对该加密系统作安全性分析时发现,该加密系统抵抗蛮力攻击很成功,但易被选择明文攻击或已知明文攻击攻破[17].对于选择明文攻击,最少仅需一个选择的明文-密文对即可攻破,恢复出频谱平面的密钥.Peng 等人提出了一种‘已知明文攻击’的方法[18].利用该方法,攻击者可通过迭代相位恢复算法获得 4-f 系统输入平面的波函数,继而可轻易推出频谱平面的密钥,从而攻破此密码系统.与此同时,Gopinathan 等人利用模拟退火算法设计了一种‘已知明文启发式攻击’方法[19].首先,通过一个已知的明文-密文对估计出解密密钥,再利用解密密钥去解密其他密文,得到相应的明文.但是,用模拟退火方法估计出来的解密密钥与理想解密密钥存在不容忽视的误差,利用它去解密其他密文时获得的明文与最初的明文之间的误差进一步扩大,解密得到的明文有可能因噪声太大而不能辨认,使得解密成功率不高.此外,利用解密密钥去解密其他密文时往往选择二值图像,因为二值图像对噪声容忍度好,这就限制了这一攻击方法的应用范围.

总之,无论是选择密文攻击、选择明文攻击还是已知明文攻击,前提是要获得额外的信息资源,例如精心设计的明文-密文对或者已知任意一个明文-密文对.当这样的资源不存在时,选择密文攻击,选择明文攻击,或已知明文攻击很难奏效.本文提出一种“唯密文攻击”的方法,仅根据密文就能推导出频谱平面解密密钥,成功地攻破了双随机相位编码光学

* 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(批准号:200426),中科院上海微系统与信息技术研究所资助的课题.

† E-mail:xpeng@szu.edu.cn

加密系统.与上述密码分析方法相比,唯密文攻击需要的资源最少.

2.双随机相位编码光学加密系统的唯密文攻击分析

2.1. 双随机相位编码光学加密系统

双随机相位编码光学加密系统利用标准 4-f 系统来实现,如图 1 所示.加密时,输入信号 $f(x,y)$(图像)在空域受到随机相位函数 $\exp[i2\pi n(x,y)]$(输入平面密钥)的调制,经过傅里叶变换后,在频域被随机相位函数 $\exp[i2\pi b(u,v)]$(频谱平面密钥)滤波,再经过逆傅里叶变换,在输出面上得到密文,表示为

$$\begin{aligned}\psi(x,y) &= FT^{-1}\{FT(f(x,y)\exp[i2\pi n(x,y)])\\ &\quad\cdot\exp[i2\pi b(u,v)]\}\\ &= FT^{-1}\{\psi(u,v)\}\\ &= \{f(x,y)\exp[i2\pi n(x,y)]\}\\ &\quad * h(x,y),\end{aligned}\tag{1}$$

其中频域密文 $\psi(u,v) = FT\{f(x,y)\exp[i2\pi n(x,y)]\}\cdot\exp[i2\pi b(u,v)]$,$h(x,y)$ 定义为 $h(x,y) = FT^{-1}\{\exp[i2\pi b(u,v)]\}$,$n(x,y)$,$b(u,v)$ 是均匀分布在[0,1]上的两个独立白噪声序列,$FT\{\}$,$FT^{-1}\{\}$ 分别表示傅里叶变换和逆傅里叶变换,$*$ 表示卷积.解密时将密文 $\psi(x,y)$ 置于标准 4-f 系统的输入平面,经傅里叶变换后,在频谱平面上用解密密钥 $\exp[-i2\pi b(u,v)]$ 滤波,再经逆傅里叶变换,即可恢复出 $f(x,y)\exp[i2\pi n(x,y)]$.在输出平面用 CCD 可探测并记录 $f(x,y)$,因为图像 $f(x,y)$ 为正的实函数,CCD 将相位因子 $\exp[i2\pi n(x,y)]$ 滤掉,这说明解密过程中输入平面密钥不起作用.因此在攻击此密码系统时我们只考虑频谱平面密钥.

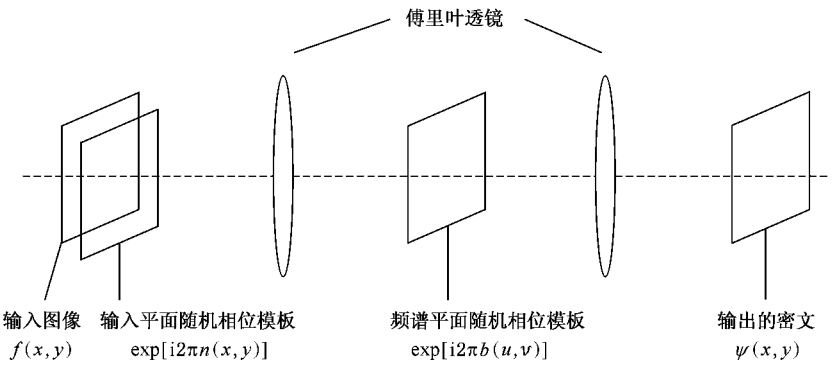

图 1 双随机相位编码光学加密系统

2.2. Kerckhoffs 假设与唯密文攻击(ciphertext-only attack)

1883 年,Kerckhoffs 阐明加密工程中的第一原则,假定密码分析者拥有所使用加密算法的全部知识,密码系统的安全性必须也只能依赖于密钥的选取.因此,在设计和分析一个密码系统时,我们的前提是在 Kerckhoffs 假设下达到安全性.

唯密文攻击 密码分析者仅获得一些消息的密文(加密算法相同),并且试图恢复尽可能多的消息明文,并进一步试图推算出加密消息的密钥(以便通过密钥得出更多的消息明文).从抽象的观点看,若用 E 表示加密算法,用 D 表示解密算法,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,则唯密文攻击的方法即为已知 $c_i = E_k(p_i)$,$1\leqslant i\leqslant l$,推出 $p_1,p_2,\cdots,p_l$,并进一步试图推算出 k,或从 $c_{l+1} = E_k(p_{l+1})$ 求出 p_{l+1} 的算法.

2.3. 双随机相位编码光学加密系统的唯密文攻击

输入平面上的物面波函数 $G(x,y) = f(x,y)\cdot\exp[i2\pi n(x,y)]$,设其傅里叶变换为 $G(u,v)$,于是频域密文

$$\begin{aligned}\psi(u,v) &= FT\{G(x,y)\}\cdot\exp[i2\pi b(u,v)]\\ &= G(u,v)\cdot\exp[i2\pi b(u,v)],\end{aligned}\tag{2}$$

因为输出平面上的密文 $\psi(x,y)$ 已知,$\psi(u,v) = FT\{\psi(x,y)\}$,所以 $\psi(u,v)$ 已知,对(2)式两边取模得

$$|\psi(u,v)| = |G(u,v)|.\tag{3}$$

物面波函数 $G(x,y)$ 的傅里叶变换的模也可知.根

据 $|G(u,v)|$ 来恢复出 $G(x,y)$ 是一个单强度相位恢复问题，可利用迭代相位恢复算法解决.然后根据(2)式物面波函数与频域密文的关系推导出解密密钥

$$\exp[-\mathrm{i}2\pi\hat{b}(u,v)] = \frac{FT\{\hat{G}(x,y)\}}{\psi(u,v)}, \quad (4)$$

其中 $\hat{}$ 表示估计，因为恢复出来的物面波函数是对 $G(x,y)$ 的估计，故推导出来的解密密钥也是对真实解密密钥 $\exp[-\mathrm{i}2\pi b(u,v)]$ 的估计.然而，用迭代相位恢复算法求解时必须知道函数 $G(x,y)$ 的“支撑”(support)，函数“支撑”指的是函数值不为 0 的区域.于是双随机相位编码光学加密系统的唯密文攻击问题转化为仅知物面波函数傅里叶变换的模，如何估计出物面波函数的“支撑”，然后利用迭代相位恢复算法恢复出物面波函数，进而再跟据物面波函数与频域密文的关系推导出解密密钥的问题.

2.3.1. 估计物面波函数的“支撑”的方法

Crimmins 等人提出一种几何方法[20]，根据信号的自相关函数的“支撑”来估计出信号的“支撑”.利用自相关函数的“支撑”估计信号的“支撑”的几何解释如下：

如果信号的“支撑”为 S，其自相关函数的“支撑”为 A，下面的解释都是基于 $A = S - S = \{x - y, x, y \in S\}$ 这个假设.

设 $u \in R^2$ 是一个单位矢量.两个矢量 $x, y \in R^2$ 的内积定义为 $\langle x, y\rangle$. B 是 R^2 空间里任意一个“紧支集”(compact set)，u 方向最大点(maximal points)的集合表示为 $E(B,u) = \{x \mid \langle x,u\rangle \geqslant \langle y,u\rangle, x \in B, y \in B\}$，注意到 $E(B,u)$ 在几何意义上代表了 B 在 u 方向上最远的点，如图 2 所示. $E(B,u) = \{x_1, x_2\}$, $E(B,-u) = \{x_3\}$，如果把 B 换成某一信号的自相关函数的“支撑”A，根据常用的两点规则(two-point rule)可找出“单边指示器集合”L(single-sided locator set)，即是对这一信号“支撑”S 的估计.

两点规则：设 A 是自相关函数的“支撑”，u 是单位矢量，如果 $E(A,u) = \{a_1, a_2\}$，则 $L = A \cap (A + a_1) \cap (A + a_2)$ 就构成一个“单边指示器集合”.如图 3 所示，更多求“单边指示器集合”的规则和方法参见文献[20].一般地，“单边指示器集合”包含 S 或 $-S$($-S = \{-x : x \in S\}$)的平移，但并不是 S，$-S$ 都包括，而且“单边指示器集合”不唯一，可以有多个.如果求出物面波函数 $G(x,y)$ 的自相关函数的“支撑”，则可根据两点规则找到 $G(x,y)$ 的“支撑”的估计，再利用迭代相位恢复算法恢复出物面波函数，它的振幅即为明文信息.

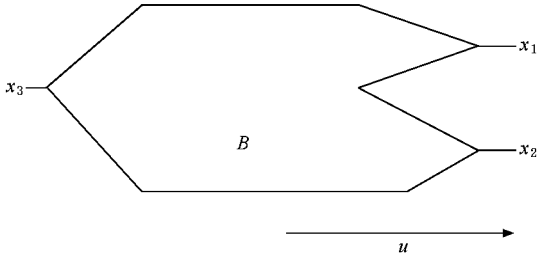

图 2　最大点示例

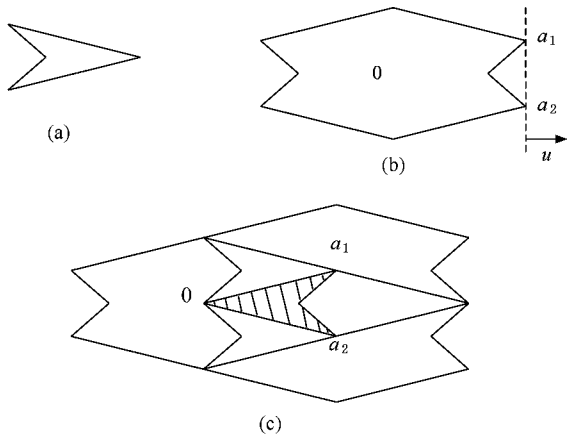

图 3　两点规则示例　(a)信号的“支撑”S；(b)信号的自相关函数的“支撑”$A = S - S$, $E(A,u) = \{a_1, a_2\}$；(c)阴影区域就是“单边指示器集合”，$L = A \cap (A + a_1) \cap (A + a_2)$ 是 $-S$ 的平移

2.3.2. 推导频谱平面解密密钥

本文采用 Fienup 提出的“混合输入输出”算法(hybrid input-output algorithm，HIO)[21] 作单强度相位恢复.HIO 算法是对经典 Gerchberg-Saxton 算法[22] 的一种改进，具有收敛速度快、稳定、能迅速逼近真实解等特点.在作单强度相位恢复时，由 Fienup 提出[21]，经 Bauschke 等人[23] 改进建立的误差度量是

$$E_S(x_n) = \frac{\| P_S P_M(x_n) - P_M(x_n) \|^2}{\| m \|^2}, \quad (5)$$

它度量信号 $P_M(x_n)$ 到 S 归一化的平方距离.其中 x_n 是第 n 次迭代时对物面波函数的估计，S 和 M 分别是支撑限制集合和傅里叶模限制集合，m 表示物面波函数的傅里叶变换的模，投影算子 P_S 和 P_M 各自把信号投影到 S 和 M 上.如果迭代一定次数后 $E_S(x_n)$ 足够小(例如小于设定的误差值)，那么此时的 x_n 同时满足物平面的支撑限制集 S 和傅里叶平面的模限制集 M 的条件，并且 x_n 就是相位恢复问题的一个解.

恢复出物面波函数后,根据(4)式推导出解密密钥 $\exp[-\mathrm{i}2\pi\hat{b}(u,v)]$.由于估计出来的物面波函数的‘支撑’相对于真实的‘支撑’有一定的平移,而傅里叶变换具有平移不变性和对称性,使得恢复的物面波函数与真实的物面波函数之间无论在振幅上还是相位上都存在平移,导致用估计出来的解密密钥去解密其他密文(均在相同密钥下加密)时获得的明文与原始明文之间存在明显平移.根据这一先验信息,为了消除平移的影响,获得更好的解密效果,我们将估计的物面波函数的‘支撑’在物面上进行遍历,使它的中心逼近真实的物面波函数的‘支撑’中心,促使估计的物面波函数的‘支撑’在位置上尽可能多的与真实的物面波函数的‘支撑’相重合,从而获得比较好的相位恢复解和解密密钥.定义解密的明文 B 与原始明文 A 之间的相关性系数为

$$r=\frac{\sum_m\sum_n(A_{mn}-\bar{A})(B_{mn}-\bar{B})}{\sqrt{(\sum_m\sum_n(A_{mn}-\bar{A})^2)(\sum_m\sum_n(B_{mn}-\bar{B})^2)}},\tag{6}$$

$\bar{A},\bar{B}$ 分别表示 A 中元素的平均值和 B 中元素的平均值,估计的解密密钥愈逼近真实解密密钥,解密的明文与原始明文之间的相关性系数就越大,解密效果越好.

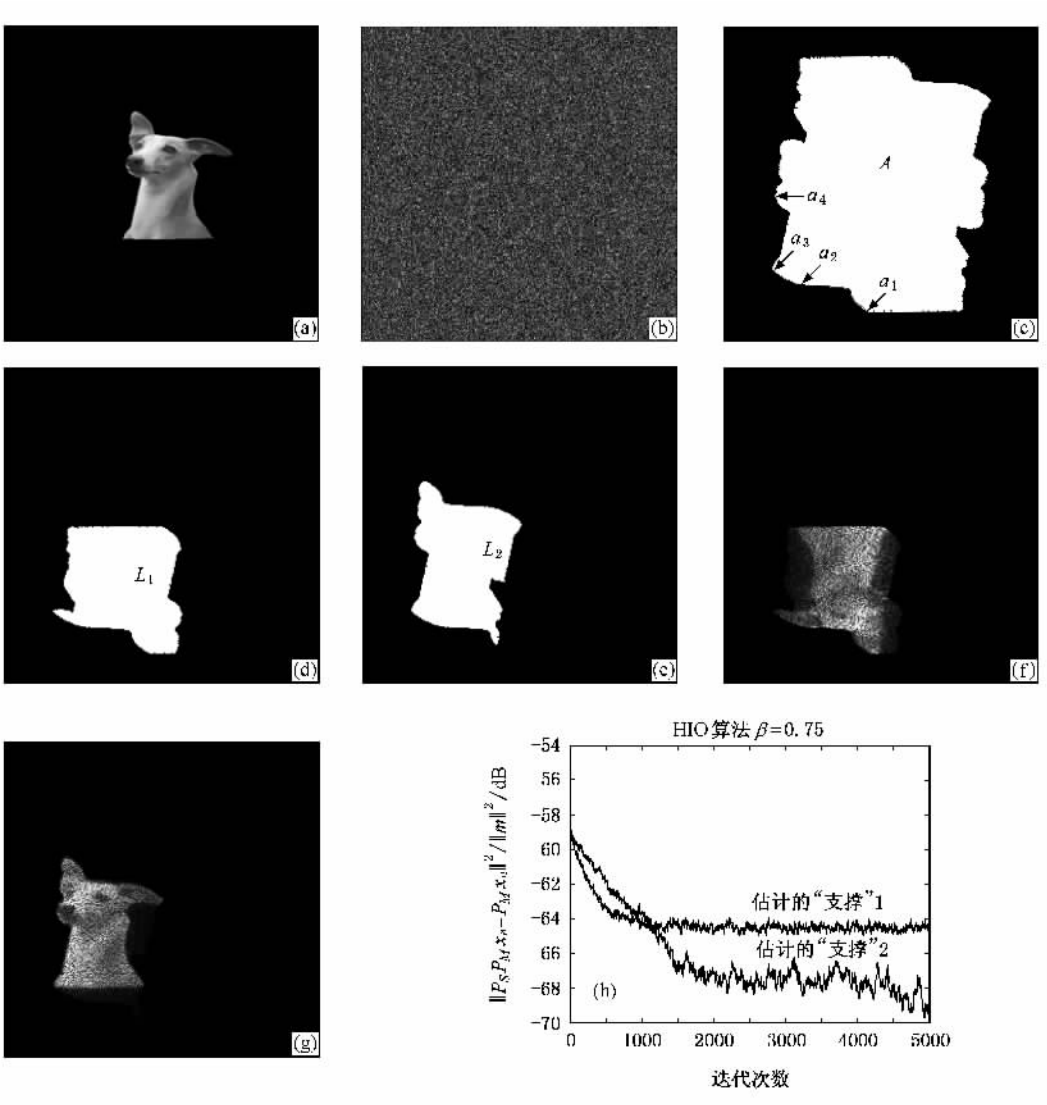

图 4 利用估计的‘支撑’作相位恢复示例 (a)明文 dog;(b)加密的密文;(c)物面波函数的自相关函数的‘支撑’;(d)表示根据(c)利用两点规则估计出来的物面波函数的‘支撑’1;(e)表示根据(c)利用两点规则估计出来的物面波函数的‘支撑’2;(f)表示将(d)作为物面‘支撑’时恢复出来的明文信息;(g)表示将(e)作为物面‘支撑’时恢复出来的明文信息;(h)表示利用 HIO 算法经过两次相位恢复的误差曲线,其中参数 β 取 0.75

3. 模拟实验及其结果

我们利用 Matlab6.5 对本文提出的唯密文攻击方法进行了数字仿真实验. 明文为灰度图 dog(256x256x8bit)，如图 4(a)所示. 加密后的密文示于图 4(b)，它是攻击者唯一知道的信息. 此时待恢复的物面波函数 $G(x,y)$是明文与输入平面密钥的乘积函数. 根据密文可计算出 $G(x,y)$傅里叶变换的模，因此 $G(x,y)$的自相关函数可由 $FT^{-1}\{|G(u,v)|^2\}$求出. 图 4(c)是经过阈值化处理的自相关函数的“支撑”A，阈值取自相关函数模最大值的 0.00002 倍，箭头指向的自相关“支撑”边界上的四个点 a_1, a_2, a_3, a_4 是根据两点规则找到的两组最大点集合 $\{a_1, a_2\}$和 $\{a_3, a_4\}$，因此可得到两个“单边指示器集合”，$L_1 = A \cap (A + a_1) \cap (A + a_2)$，$L_2 = A \cap (A + a_3) \cap (A + a_4)$，即估计出来的物面波函数的“支撑”1 和“支撑”2，如图 4(d)，图 4(e)所示. 图 4(f)，(g)分别是以 L_1, L_2 作为物面“支撑”，利用 HIO 算法迭代 5000 次恢复出来的物面波函数 $G(x,y)$的振幅，即明文信息. 比较图 4(d)，(e)，(f)，(g)，L_2 包含真实的 $G(x,y)$“支撑”S 的平移，L_1 包含 $-S$ 的平移，傅里叶变换具有平移不变性和对称性，因此图 4(g)相对于原始明文图 4(a)平移了一段距离，而图 4(f)不仅平移了一段距离，还反转了 180°. 图 4(h)描述了两次相位恢复实验的误差曲线，由图可见，以估计的“支撑”2 作为物面“支撑”时收敛效果更好，能获得更好的相位恢复解.

记录下以估计的“支撑”2 作为物面“支撑”时恢复出来的物面波函数 $\hat{G}(x,y)$，再根据(4)式推导出解密密钥 $\exp[-i2\pi\hat{b}(u,v)]$，然后用它去解密其他密文(均在相同密钥下加密). 图 5(a)为灰度图 Lena (256x256x8bit)，对应的加密图像如图 5(b)所示，图 5(c)表示用解密密钥解密的明文. 解密出来的 Lena 图像相对于原始 Lena 图像存在明显的平移，这正是因为估计的“支撑”2 偏离了真实的物面波函数“支撑”而造成的.

比较图5中的明文与解密的明文，发现解密得到的图像相对于原始图像向左下方平移了一段距离. 根据这一先验信息，可尝试将估计的“支撑”2 的中心先竖直向上平移，每次平移时都以当前平移的“支撑”作为物面“支撑”，利用 HIO 算法作 5000 次迭代，恢复出物面波函数，即可获得明文信息，然后根据物面波函数与频域密文的关系，估计出解密密钥，再利用估计的解密密钥去解密 Lena 的密文，如解密得到的 Lena 图像在竖直方向无明显平移，则停止向上平移，转而水平向右平移估计的“支撑”2 的中心，直至解密的 Lena 图像与明文 Lena 图像之间在水平方向无明显平移. 此时可认为估计的“支撑”2 逼近真实的“支撑”，记录下当前估计的解密密钥，再用它去解密其他密文. 为减少计算时间，解密图像相对于原始图像的微小平移是能够容忍的，因为攻击者通常能够从一幅有些许错误的解密图像里获得足够的信息. 图 6(a)—(e)显示了估计的“支撑”2 在平移过程中依次经过的五个位置，每个“支撑”的中心像素坐标分别是 1(135,81)，2(130,81)，3(130,124)，4(130,132)，5(130,136)，图 6(f)—(j)是在每个位置时对应恢复的振幅信息，图 6(k)—(o)表示在各个位置时用当前估计的解密密钥恢复的 Lena 图像.

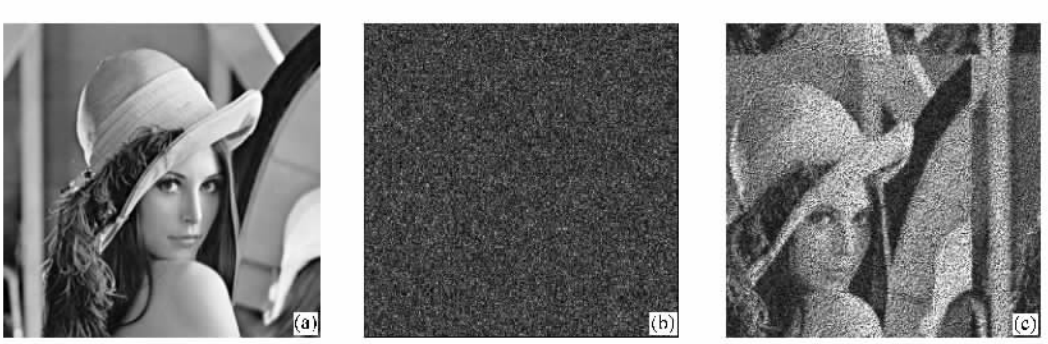

图 5　用估计的解密密钥去解密其他密文　(a)明文 lena；(b)加密的图像；(c)解密的图像

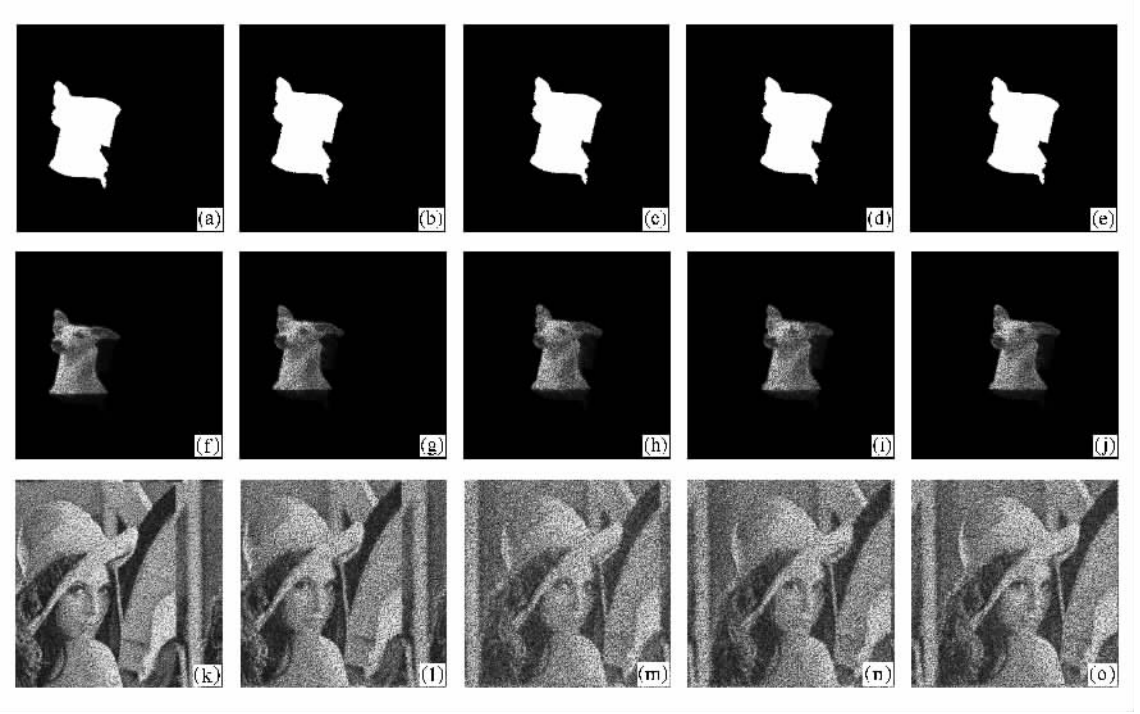

图 6 平移估计的‘支撑’2 及用每次估计的解密密钥去解密 Lena 密文的结果 (a)—(e)是平移过程中依次经过的五个位置;(f)—(j)是对应每个支撑恢复的振幅信息;(k)—(o)是对应每个支撑所获得的 Lena 解密图像

当估计的‘支撑’2 的中心平移到(130,136)时,利用此时估计的解密密钥去解密 Lena 的密文获得的 Lena 图像与明文 Lena 图像之间无明显平移,记录下此时的解密密钥,它最逼近真实解密密钥,因此是最优解密密钥.计算估计的‘支撑’2 的中心在上述五个位置时解密的 Lena 图像与明文 Lena 图像的相关性系数,并绘制成坐标曲线,如图 7 所示.

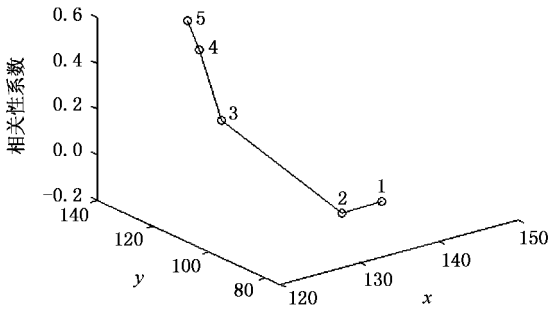

图 7 估计的‘支撑’2 的中心在五个位置时解密的 Lena 图像与明文 Lena 图像的相关性系数

当估计的‘支撑’2的中心平移到位置1,2点时,相关性系数是负的,这是因为解密的 Lena 图像与明文 Lena 图像之间存在较大的平移.随后平移到位置 3,4,5 点后,解密的 Lena 图像中存在的平移逐渐消除,因而与明文 Lena 图像的相关性系数逐渐增大,在位置 5 点时达到最大,为 0.51423,此时解密的 Lena 图像质量无论在主观上(参看图 6)还是客观上(相关性系数)都能满足密码攻击的要求.再利用当前获得的最优解密密钥去解密其他密文,能得到满意的结果,如图 8 所示.图 8(a)与图 8(d)分别表示灰度图 Pepper($256 \times 256 \times 8$ bit)和二值图($256 \times 256 \times 1$ bit),图 8(b)与图 8(e)是各自对应的加密图像,解密图像分别示于图 8(c)与图 8(f),图 8(a)与图 8(c)的相关性系数是 0.47296,图 8(d)与图 8(f)的相关性系数是 0.33672.这说明利用估计的最优解密密钥去解密其他密文时在主观上可以获得比较好的结果,客观上的评价是解密明文与原始明文之间的相关性系数,这里相关性系数不太高的原因是获得的解密密钥只是逼近真实解密密钥的解,毕竟还存在一些差异;另外,解密的明文相对于原始明文还有微小的平移,导致相关性降低.

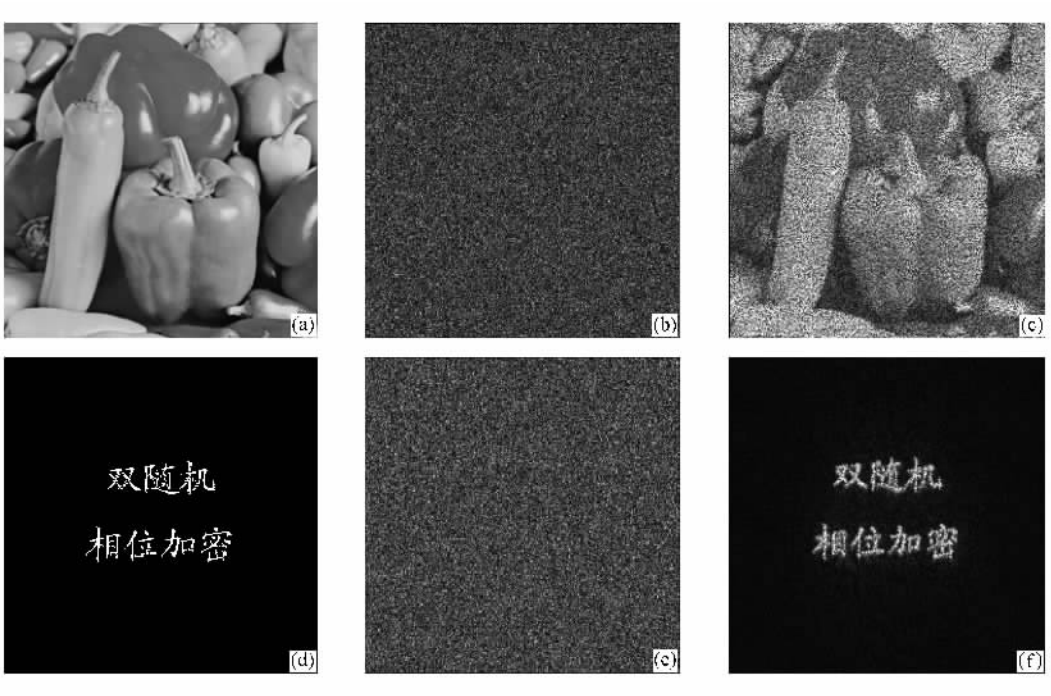

图 8　用记录的最优解密密钥解密其他密文时的结果　(a)灰度图 pepper(256 × 256 × 8 bit)；(b)pepper 的加密图像；(c)解密的 pepper 图像；(d)二值图(256 × 256 × 1 bit)；(e)二值图加密图像；(f)解密的二值图

4. 结　论

本文提出了一种双随机相位编码光学加密系统的唯密文攻击方法，该系统利用标准 4-f 光学系统来实现加密和解密. 唯密文攻击方法仅依靠密文即可估计出物面波函数的‘支撑’，从而恢复出输入平面上的物面波函数，然后根据物面波函数与频域密文的关系推导出频谱平面解密密钥，利用估计的解密密钥去解密其他密文时，由于估计的物面波函数的‘支撑’相对于它的真实‘支撑’有一定的平移，使得解密的明文相对于原始明文也存在平移. 根据这一先验信息，把估计的‘支撑’在物面范围内遍历，找到最优解密密钥，彻底攻破了这一加密系统. 与选择密文攻击，选择明文攻击，已知明文攻击相比，本文提出的唯密文攻击方法无需额外的资源，所需资源最少，因此更具实际意义.

[1] Refregier P, Javidi B 1995 *Opt. Lett.* **20** 767
[2] Mogensen C P, Gluckstad J 2000 *Opt. Lett.* **25** 566
[3] Unnikrishnan G, Joseph J, Singh K 2000 *Opt. Lett.* **25** 887
[4] Liu F M, Zhai H C, Yang X P 2003 *Acta Phys. Sin.* **52** 2462(in Chinese) [刘福民、翟宏琛、杨晓萍 2003 物理学报 **52** 2462]
[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] Niu C H, Zhang Y, Gu B Y 2005 *Chin. Phys.* **14** 1996
[7] Javidi B, Zhang G S, Li J 1997 *Appl. Opt.* **36** 1054
[8] Matoba O, Javidi B 1999 *Opt. Lett.* **24** 762
[9] Matoba O, Javidi B 1999 *Appl. Opt.* **38** 6785
[10] Nomura T, Javidi B 2000 *Appl. Opt.* **39** 4783
[11] Matoba O, Javidi B 2002 *Opt. Lett.* **27** 321
[12] Matoba O, Javidi B 2004 *Appl. Opt.* **43** 2915
[13] Javidi B 1999 *U. S. Patent* 6, 002, 773
[14] Javidi B 1999 *U. S. Patent* 5, 903, 648
[15] Javidi B 2003 *U. S. Patent* 6, 519, 340
[16] Carnicer A, Usategui M M, Arcos S *et al* 2005 *Opt. Lett.* **30** 1644
[17] Frauel Y, Castro A, Naughton J T *et al* 2005 *Proc. of SPIE* **5986** 598603
[18] Peng X, Zhang P, Wei H Z *et al* 2006 *Opt. Lett.* **31** 1044
[19] Gopinathan U, Monaghan S D, Naughton J T *et al* 2006 *Opt. Exp.* **14** 3181
[20] Crimmins R T, Fienup R J, Thelen J B 1990 *J. Opt. Soc. Am.* A **7** 3
[21] Fienup R J 1982 *Appl. Opt.* **21** 2758
[22] Gerchberg R W, Saxton W O 1972 *Optik* **35** 237
[23] Bauschke H H, Combettes L P, Luke R D 2003 *J. Opt. Soc. Am.* A **20** 1025

Ciphertext-only attack on double random phase encoding optical encryption system*

Peng Xiang Tang Hong-Qiao Tian Jin-Dong

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

(Received 14 August 2006; revised manuscript received 3 September 2006)

Abstract

Security analysis of optical encryption system based on double random phase encoding indicates that the system can be classified as a linear symmetric block-cipher cryptosystem, which may lead to a great vulnerability. Under the ciphertext-only attack (COA), an opponent can attack such a cryptosystem only on the basis of estimated support of wave function in the object plane with iterative phase retrieval methods, and subsequently deduce the phase keys in the Fourier plane easily. The ciphertext-only attack (COA) requires much less resources than other types of attacks. Estimated support of wave function in the object plane could have some translations relative to the true support, so retrieved wave function could also have translations in both the amplitude and the phase, leading to a translation of retrieved plaintext relative to original plaintext. However, attackers can take this translation as *a priori* knowledge to traverse estimated support in the object plane until finding the best estimated keys, which bring about the best decryption quality.

Keywords: optical information security, double random phase encoding, ciphertext-only attack, function support

PACC: 4230, 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 Microsystems and Information Technology, CAS.