文章编号：0253-2239(2008)03-0429-06

约束集投影算法和 4f 相关器的光学密码系统的已知明文攻击

位恒政[1,2] 彭 翔[1,2]

([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光电子器件与系统教育部重点实验室，广东 深圳 518060)

摘要 分析了约束集投影和 4f 相关器的光学加密系统的安全性，并提出一种基于双强度相位恢复的已知明文攻击方法。约束集投影和 4f 相关器的加密系统是典型的光学密码系统，由于其解密系统可以等价于一个标准的 4f 系统，并且加密密钥与解密密钥相同，因此本质上仍是一个线性系统，这就为系统的安全性留下了很大隐患。该攻击方法仅利用一对输入的相位信息和相应输出的强度信息即可成功得到加密系统的密钥，提高了攻击实施的可行性。

关键词 信息光学；光学信息安全；已知明文攻击；相位恢复

中图分类号 TN918 **文献标识码** A

Known-Plaintext Attack on Optical Cryptosystem Based on Projection-Onto-Constraint-Sets Algorithm and a 4f Correlator

Wei Hengzheng[1,2] Peng Xiang[1,2]

([1] *State Key Laboratory of Precision Measurement Technology and Instrumentation, Tianjin University, Tianjin* 300072, *China*
[2] *Institute of Optoelectronics, Key Laboratory of Optoelectronics Devices and Systems of Education Ministry of China, Shenzhen University, Shenzhen, Guangdong* 518060, *China*)

Abstract The security of the cryptosystem based on projection-onto-constraint-sets (POCS) and a 4f correlator is examined. A method of known-plaintext attack based on phase retrieval algorithm from two-intensity information is presented. In the field of information security the cryptosystem based on POCS and the 4f correlator is a typical approach. But its decryption system can be equivalent to the standard 4f system and the encryption and decryption keys are identical. So this linearity characteristic opens avenues of attacks. With the known-plaintext attack method, an attacker is able to break down the cryptosystem by only a pair of input phase data and output intensity data.

Key words information optics; optical-information security; known-plaintext attack; phase retrieval

1 引 言

光学信息安全是近年来国内外研究的一个热点，很多学者对此进行了深入研究[1~8]。从密码学的观点来看，目前多数对光学加密系统的研究主要局限在密码编码学范畴，而对光学加密系统进行密码分析报道很少。2005 年，Carnicer 等[9]通过“选择密文攻击”的方法破解了著名的双随机相位编码系统[1]。随后，Peng 等[10]提出一种基于双强度相位恢复算法的已知明文攻击方法，成功破译了双随机相位编码系统。该方法只需一对明密文，无需大

收稿日期：2007-08-30；**收到修改稿日期**：2007-09-17

基金项目：国家自然科学基金(60472107)、广东省自然科学基金(04300862)、深圳市科技计划项目(200426)和中国科学院微系统与信息技术研究所资助课题。

作者简介：位恒政(1978－)，男，山东德州人，博士研究生，主要从事信息安全、密码学理论、电子商务、电子银行安全、光学信息处理等方面的研究。E-mail：hzhwei@vip.sina.com

导师简介：彭 翔(1955－)，男，天津人，教授，博士生导师，主要从事三维数字成像与造型、光学信息安全、现代光学测试技术等方面的研究。E-mail：xpeng@szu.edu.cn

量精心设计的密文，所需资源大大减少。与此同时，Gopinathan 等[11]提出另外一种已知明文攻击方法，该方法利用模拟退火算法估计出双随机相位编码系统的密钥。最近，Peng 等[12]提出一种唯密文攻击的密码学分析方法，仅利用密文信息就能破解双随机相位编码系统，与其它方法相比，该方法所需资源更少。以上关于光学加密系统的安全性分析主要集中在双随机相位加密系统，而其它光学加密系统的安全性也有待研究。

基于约束集投影（Projection-onto-constraint-sets）和 4f 相关器的加密系统是另一类典型的光学密码系统。该系统由 Rosen 提出[13]，并应用在光学加密、认证[14]以及光学信息隐藏[15]方面。在基于约束集投影算法和 4f 相关器的光学密码系统中，其密文通过反复迭代的约束集投影算法产生，解密结果以强度的形式输出，而不是复振幅的形式。仅由输出的强度信息不能轻易获得该密码系统的密钥。该系统的密文生成过程通过数字方式实现，解密过程既可以通过数字也可通过光学的方式实现[14]。由于其加密系统和解密系统使用同一个密钥，并且其解密系统仍是一个典型的 4f 线性系统，因此基于约束集投影算法和 4f 相关器的安全系统也存在很大的安全隐患。最近，Situ 等人对基于约束集投影算法和 4f 相关器的安全系统进行了密码学分析，利用多对输入及相应输出信息估计出加密系统的密钥[16]。

本文提出一种新的、更为简洁的基于双强度相位恢复算法的已知明文攻击方法，对约束集投影算法和 4f 相关器的密码系统进行了密码学分析。该方法仅仅需要一对输入和相应输出信息，将寻找系统密钥的过程转换为一个双强度的相位恢复问题，从而破译基于约束集投影算法和 4f 相关器的光学密码系统。与 Situ 等的密码分析方法相比，该方法所需资源大大减少，并且具有很好的收敛性能，提高了攻击实施的可行性。

2 约束集投影算法和 4f 相关器的光学密码系统

在约束集投影算法和 4f 相关器的密码系统[14]中，明文信息在密钥 H_2 控制下，通过约束集投影迭代算法编码为纯相位信息 h_1。解密时，如图 1 所示，将加密后的图像（密文）h_1 放在输入平面 P_1，解密密钥 H_2 放置在频谱面 P_2，P_3 平面显示输出图像。h_1 和 H_2 是两个彼此独立、分别经过约束集投影优化迭代算法特殊编码的相位函数。H_2 一经产生，将保持不变，作为密钥使用。h_1 则随待加密图像的不同而发生变化。在解密时，用户只需提交各自的相位函数 h_1 即可进行快速解密。设 $c(x,y)$ 是系统输出的复振幅：

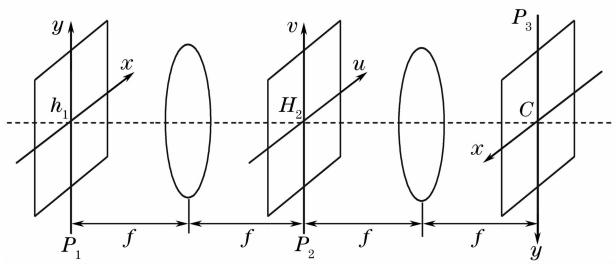

图 1 约束集投影和 4f 相关器的解密系统示意图

Fig. 1 Scheme of decryption system based on projection-onto-constraint-sets and 4f correlator

$$c(x,y)=\mathcal{F}^{-1}\{\mathcal{F}[h_1(x,y)]H_2(u,v)\},\quad(1)$$

其中 $\mathcal{F}$ 表示傅里叶变换，$\mathcal{F}^{-1}$ 表示逆傅里叶变换，$h_1=\exp[\mathrm{j}\phi(x,y)]$ 和 $H_2(u,v)=\exp[\mathrm{j}\psi(u,v)]$ 均是由约束集投影算法得到的特殊编码的相位函数。利用 CCD 等强度探测器即可得到最终的解密结果，所以此系统的实际输出为[14]

$$\left|c(x,y)\right|=\left|\mathcal{F}^{-1}\{\mathcal{F}\{\exp[\mathrm{j}\phi(x,y)]\}\exp[\mathrm{j}\psi(u,v)]\}\right|.\quad(2)$$

3 密码分析和已知明文攻击的概念

密码学分析方法满足“Kerckhoffs”假设[17]，即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。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[17]。

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。密码分析者利用这些已知信息推导出密钥。从抽象的观点来看，已知 p_i，$c_i=E_k(p_i)$，由 p_i 和 c_i 推导出 k，其中 E 表示加密算法，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。

4 约束集投影算法和 4f 相关器的光学密码系统的已知明文攻击

由解密系统图 1 可以看出，此系统在光学上可以等价成一个 4f 系统，与经典双随机相位加密系统

相比，约束集投影算法和 4f 相关器的密码系统只有频域密钥，并且频域密钥是特殊设计的相位函数而不是随机相位函数。此外，应该注意到该系统的密文也并不是随机相位函数，而是经过特殊设计的相位编码函数。由(2)式可知，约束集投影算法和 4f 相关器的密码系统的输出只有强度信息，而无相位信息。如果能够获得输出的相位信息，可以通过输入信息和(1)式很容易推导出系统的密钥。本文提出的已知明文攻击方法仅利用一对已知信息：解密系统输入的纯相位信息及其对应输出的强度信息，将寻找密钥的过程转化为一个双强度相位恢复问题[18]，通过相位恢复算法得到系统输出的相位，进而得到系统密钥。已知明文攻击方法的实施过程描述如下：

设已知的一任意明文-密文对为 $\{\phi(x,y),|c(x,y)|\}$，并设 $c(x,y)$ 的振幅为 $A(x,y)$，相位为 $n(x,y)$，则

$$c(x,y)=A(x,y)\exp[\mathrm{j}n(x,y)], \tag{3}$$

并且 $\phi(x,y)$ 和 $c(x,y)$ 满足(1)式：

$$c(x,y)=\mathscr{F}^{-1}\{\mathscr{F}\{\exp[\mathrm{j}\phi(x,y)]\}H_2(u,v)\}, \tag{4}$$

对等式两边同时做傅里叶变换，得

$$\mathscr{F}[c(x,y)]=\mathscr{F}\{\exp[\mathrm{j}\phi(x,y)]\}H_2(u,v), \tag{5}$$

令

$$\mathscr{F}\{\exp[\mathrm{j}\phi(x,y)]\}=P(u,v)\exp[\mathrm{j}\beta(u,v)], \tag{6}$$

其中 $P(u,v)$ 和 $\beta(u,v)$ 分别是 $\exp[\mathrm{j}\phi(x,y)]$ 傅里叶变换的振幅和相位，由于 $\phi(x,y)$ 是已知信息，因此 $P(u,v)$ 和 $\beta(u,v)$ 也是已知的。将(6)式代入(5)式，得

$$\mathscr{F}[c(x,y)]=P(u,v)\exp[\mathrm{j}\beta(u,v)]H_2(u,v), \tag{7}$$

对(7)式两端取模，得

$$\left|\mathscr{F}[c(x,y)]\right|=P(u,v), \tag{8}$$

由(8)式可以看出，此时攻击者可以通过已知信息 $\phi(x,y)$ 得到 $c(x,y)$ 的傅里叶变换的强度信息，并且 $c(x,y)$ 的强度信息 $|c(x,y)|$ 本来就是已知的，因此可以通过双强度相位恢复算法求解出 $c(x,y)$ 的相位信息。一旦恢复(估计)出 $c(x,y)$ 的相位信息 $\hat{n}(x,y)$，密码分析者可以根据(5)式获得该密码系统的密钥：

$$[\hat{H}_2(u,v)]=\frac{\mathscr{F}\{A(x,y)\exp[\mathrm{j}\hat{n}(x,y)]\}}{\mathscr{F}\{\exp[\mathrm{j}\phi(x,y)]\}}. \tag{9}$$

可以看出，本文提出的已知明文攻击方法，最终归结为一个双强度的相位恢复问题。而这个问题可以采用 Fienup 提出的“混合输入-输出”(Hybrid input-output，HIO)相位恢复算法来解决[18]。混合输入-输出算法是对经典契伯格-山克斯顿(Gerchberg-Saxton，GS)算法的改进，具有收敛速度快，误差小等特点。混合输入-输出算法具体描述如下：首先随机给定 $c(x,y)$ 的相位 $n(x,y)$ 一个初始值，并设 $c(x,y)$ 的初始值为 $g_1(x,y)$，将其作为混合输入-输出算法的输入。对输入进行傅里叶变换，获得频谱平面上复函数。此时，引入频谱平面上的限制条件，即保持该复函数的相位不变，但振幅变为 $P(u,v)$。然后将新的频谱平面上的复函数进行逆傅里叶变换，获得物平面上的复函数，即混合输入-输出算法的输出。然后由混合输入-输出算法的输入与输出的关系，以及物平面上的限制条件：即保持算法输出的相位不变，振幅变为 $|c(x,y)|$，得到的新复函数作为下一次迭代的输入。这样反复进行，直至满足收敛条件。整个算法可以用四个公式来表示，对于第 n 次迭代：

$$G_n(u,v)=|G_n(u,v)|\exp[\mathrm{j}\delta_n(u,v)]=\mathscr{F}\{g_n(x,y)\}, \tag{10}$$

$$G'_n(u,v)=P(u,v)\exp[\mathrm{j}\delta_n(u,v)], \tag{11}$$

$$g'_n(x,y)=|g'_n(x,y)|\exp[\mathrm{j}\theta_n(x,y)]=\mathscr{F}^{-1}[G'_n(u,v)], \tag{12}$$

$$g'_{n+1}(x,y)=|g'_{n+1}(x,y)|\exp[\mathrm{j}\theta_{n+1}(x,y)]=\begin{cases}g'_n(x,y), & (x,y)\notin\gamma\\ g_n(x,y)-\beta g'_n(x,y), & (x,y)\in\gamma\end{cases}, \tag{13}$$

$$g_{n+1}(x,y)=|c(x,y)|\exp[\mathrm{j}\theta_{n+1}(x,y)], \tag{14}$$

(13)式中，β 为一常数，γ 为定义的数据区域，该区域的元素构成的函数违反了物平面上限制条件[18]。

重复(10)式～(14)式的过程，直至定义的误差-均方差之和(Sum square error，SSE)S_{SSE} 达到设计精度或者设置的最大迭代次数为止。S_{SSE} 定义为

$$S_{\mathrm{SSE}}=10\lg\left\{\sum[c-c^{(n)}]^2\Big/\left(\sum c^2\right)\right\}, \tag{15}$$

式中 c 为已知的系统输出的强度分布(即 $|c(x,y)|$),$c^{(n)}$ 为第 n 次迭代结束时,系统输出的强度分布。

在 Situ 等的攻击方法中,至少需要 $K(K\geqslant 3)$ 对已知的明文-密文对,才能获得系统的密钥,并且其算法的收敛性不能从理论上得到保证,收敛性与迭代算法初始值的选取具有很大的关系[14]。而本文提出的方法只需要一个明文-密文对,即可进行密码分析,所需资源比 Situ 等人的攻击方法明显减少。此外,混合输入-输出相位恢复算法已经被证明具有很好的收敛性,从而大大提高了攻击实施的稳定性。该方法将寻找密钥的过程转化为一个典型的双强度相位恢复的问题,具有清晰的物理意义。

5 仿真实验结果及分析

在 Matlab6.5 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对已知信息:输入的密文 h_1(纯相位函数)和输出的强度信息 $|c(x,y)|$。输入输出平面的维度都是 256 pixel×256 pixel,$|c(x,y)|\in W(W=128\ \text{pixel}\times 128\ \text{pixel})$,如图 2(a)所示。计算输入密文 h_1 的傅里叶变换,得到其强度分布 $P(u,v)$,这等价于 $|\mathscr{F}[c(x,y)]|=P(u,v)$,如图 2(b)所示。于是,问题转化为已知 $|c(x,y)|$ 及 $c(x,y)$ 傅里叶变换的模 $|\mathscr{F}[c(x,y)]|$,求解 $c(x,y)$ 的相位问题,这是典型的双强度相位恢复问题。根据混合输入-输出算法求出 $c(x,y)$ 的相位后,可以利用(9)式得到加密系统的密钥。

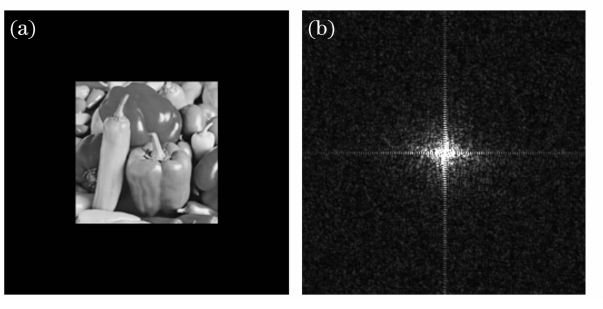

图 2 (a)系统输出的模,(b)系统输出的傅里叶变换的模

Fig. 2 (a) The modulus of the decryption output, (b) the modulus of Fourier transform of decryption output

首先利用上述已知条件和混合输入-输出算法对 $c(x,y)$ 进行双强度条件的相位恢复。计算迭代 1000 次恢复出的 $c(x,y)$ 相位分布如图 3(a)所示。混合输入-输出迭代算法中的 S_{SSE} 与迭代次数 N 的关系如图 3(b)所示,可以看出,算法开始迭代速度较快,在 600 至 1000 次左右曲线收敛趋于平缓,因此,利用混合输入-输出相位恢复算法求解系统输出相位的过程是一个迭代的渐近优化过程,所得结果是一个近似解。求得 $c(x,y)$ 的相位后,由(9)式即可得出系统的密钥。

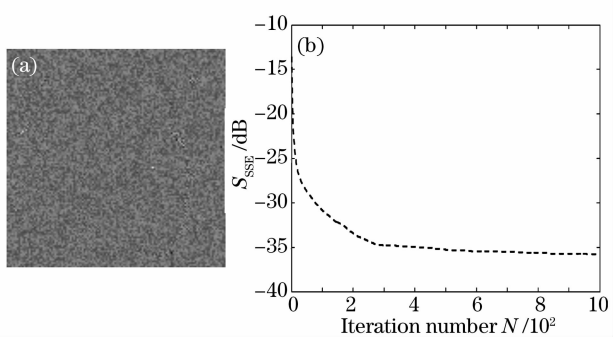

图 3 (a)系统输出的相位恢复结果,(b) S_{SSE} 随迭代次数的收敛情况

Fig. 3 (a) Retrieved phase information of decryption output, (b) S_{SSE} versus the number of iterations

设待加密的图像如图 4(a)所示,通过约束集投影算法,在输入平面和输出平面之间反复迭代,将明文信息编码为纯相位信息,形成密文,如图 4(b)所示。图 5 是约束集投影算法迭代 100 次,均方误差(Mean square error, MSE)E_{MSE} 随迭代次数的收敛曲线。均方误差定义为

$$E_{\text{MSE}}=\frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}[\,|c_n(i,j)|^2-|c(i,j)|^2\,]^2, \tag{16}$$

其中 $|c_n(i,j)|$ 是第 n 次迭代的系统输出的强度分布,$|c(i,j)|$ 表示待加密明文信息的强度分布。从图 5 可以看出,算法开始收敛速度很快,迭代 10 次后基本趋于收敛。由于获得密文的过程也是一个逐渐优化的过程,因此解密结果与输入明文会存在一定的误差。

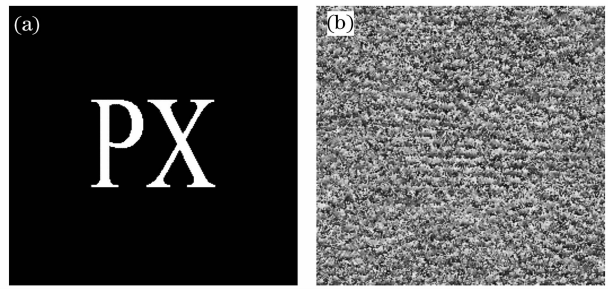

图 4 (a)待加密的明文,(b)通过约束集投影算法生成的密文

Fig. 4 (a) Plaintext, (b) ciphertext encrypted with POCS algorithm

现用原密钥与恢复的密钥来解密图 4(b)的密

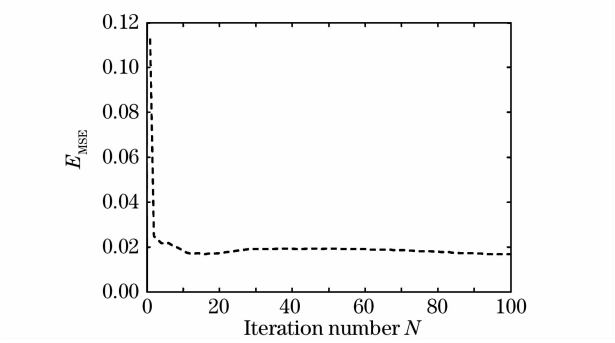

图 5　均方误差随迭代次数的收敛情况

Fig. 5　Mean square error versus the number of iterations

文，解密结果分别如图 6(a)和图 6(b)所示，均方误差数值分别为 0.016778 和 0.020639。从仿真结果可以看出，本文提出的已知明文攻击方法是十分有效的。由于相位恢复算法恢复出的密钥是一个近似解，因此所得的破译结果与原密钥解密解密结果存在一定的误差。

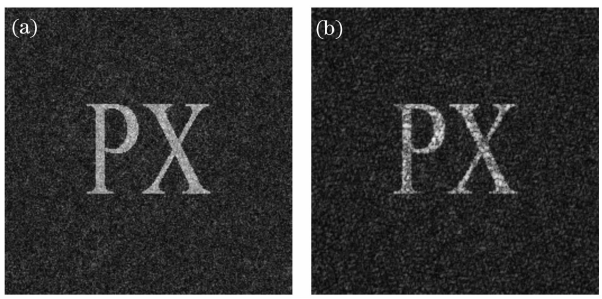

图 6　(a)利用原密钥的解密结果，(b)利用恢复密钥的解密结果

Fig. 6　(a) Decryption result from original key, (b) decryption result from retrieved key

6　结　　论

1) 在约束集投影算法和 4f 相关器的光学密码系统中，傅里叶平面上的加密密钥始终保持不变，并且与解密密钥相同，这就意味着基于约束集投影算法和 4f 相关器的密码系统仍然属于对称密码系统。此外，尽管这种光学密码系统在密钥产生以及密文的产生过程中引进了一些非线性的运算的机制，例如用限幅运算和提取相位的运算，但该密码系统的加密和解密过程仍然是基于线性系统实现的，这就为密码系统留下了很大的安全隐患。

2) 通过对约束集投影算法和 4f 相关器的密码系统的解密系统方程分析，可以将该密码系统密钥的求解过程转化为一个双强度相位恢复的问题。本文给出一种已知明文攻击方法，仅利用一任意明文-密文对即可获得加密系统的密钥。计算机仿真结果验证了本文提出的密码分析理论的正确性。

3) 与 Situ 等的方法相比，本文提出的方法仅需一对明文-密文即可破译约束集投影算法和 4f 相关器的光学密码系统，所需资源比 Situ 等人的方法大大减少，从而提高了密码攻击实施的可行性。而且该算法不依赖于迭代算法初始值的选择，具有很好的收敛性和稳定性。

参　考　文　献

1 Philippe Refregier, Bahram 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. Exp.*, 2001, **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
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
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
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 Yuchi Liang, 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
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, **27**(3): 224～228
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，**27**(3)：224～228

9 Arturo Carnicer, Mario Montes-Usategui, Sergio 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

10 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

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

12 Peng xiang, Tang Hongqiao, Tian jindong. Ciphertext-only attack on double random phase encoding optical encryption system[J]. *Acta Physica Sinica*, 2007, **56**(5): 2639～2636
彭　翔，汤红乔，田劲东. 双随机相位编码光学加密系统的唯密文攻击[J]. 物理学报，2007，**56**(5)：2629～2636

13 Joseph Rosen. Learning in correlators based on projections onto constraint sets[J]. *Opt. Lett.*, 1993, **18**(14): 1183～1185
14 Youzhi Li, Kathi Kreske, Joseph Rosen. Security and encryption optical systems based on a correlator with significant output images[J]. *Appl. Opt.*, 2000, **39**(29): 5295～5301
15 Joseph Rosen, Bahram Javidi. Hidden images in halftone pictures [J]. *Appl. Opt.*, 2001, **40**(20): 3346～3353
16 Guohai Situ, Unnikrishnan Gopinathan, David Monaghan *et al*.. Cryptanalysis of optical security systems with significant output images[J]. *Appl. Opt.*, 2007, **46**(22): 5275～5262
17 Bruce Schneier. *Applied Cryptography and Network Security: Principle, Algorithms, and Source Code in C* [M]. New York: John Wiley & Sons Inc., 1996. 5～7
18 J. R. Fienup. Phase retrieval algorithms: a comparison [J]. *Appl. Opt.*, 1982, **21**(15): 2758～2769

欢迎成为《中国光学期刊网》企业会员

中国光学期刊网(http://www.opticsjournal.net)是由中科院上海光学精密机械研究所主办、国内光学期刊界共同参与建设的光学期刊网络信息发布平台。自 2004 年 5 月开通以来,得到了广大科研工作者、企事业单位人士的好评。

为进一步提高服务水平,中国光学期刊网从 2006 年起在信息服务上实行会员制度,凡光电子、激光、光通信等相关的企业均可申请成为中国光学期刊网的企业会员,中国光学期刊网将为企业会员提供优质超值的专业服务。

一、会员企业享受的服务包括:

1) 企业名称在中国光学期刊网首页的会员企业栏目中出现,并链接到企业自己的网址。

2) 会员企业可获赠光学类期刊一份,全年 12 册,在《中国激光》《光学学报》《激光与光电子学进展》《Chinese Optics Letters》中任选一种。

3) 可免费在本站"特别推荐"栏目发布文字信息(含广告)10 条,每篇不过 2000 字。

4) 如在中国光学期刊网发布广告,可享受广告报价的 80%优惠。

5) 优先或免费参加光学期刊网组织的各类学术和业务活动。

6) 可免费阅读本网站期刊全文 300 篇次。

二、会员义务:

1) 注册时向中国光学期刊网递交企业真实信息。

2) 每年交纳会员费 2800 元,会员资格从交费之日起计算,一年有效。

3) 不得将中国光学期刊网提供给会员的信息转给第三方使用。

4) 尊重并保护本网及论文作者的知识产权。

5) 在本网发布信息必须遵守中华人民共和国相关法律法规。

三、成为企业会员的步骤:

1) 注册成为中国光学期刊网的一般用户,也可以直接填写广告投放申请表单,说明您的意向。

2) 来信 mail@opticsjournal.net 告知您已经注册成功。并请告知选择何种期刊及收刊地址、联系人。

3) 银行汇款 2800 元至下列帐户:

开户行:工商银行上海嘉定支行营业部　户　名:中国科学院上海光学精密机械研究所

帐　号:1001700809026400195

4) 联系人:郑继承;电话:021-69918253;Email:expert@mail.siom.ac.cn