第 25 卷 第 7 期
2005 年 7 月

光 学 学 报
ACTA OPTICA SINICA

Vol. 25, No. 7
July, 2005

文章编号：0253-2239(2005)07-881-4

基于级联相位恢复算法的光学图像加密*

于 斌[1,2] 彭 翔[1,2]

(1 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
2 天津大学精密测试技术及仪器国家重点实验室，天津 300072)

摘要： 在虚拟光学数据加密理论模型的基础上，提出了一种光学图像加密的可视化密码构造算法。该加密算法基于自由空间传播的光学系统，利用级联迭代角谱相位恢复算法把待加密图像分别编码到两块相位模板之中，从而实现图像的加密。该加密技术不但可通过同时调整两块相位模板的相位分布的搜索策略来扩大搜索空间，提高安全强度，而且扩大了系统密钥空间，使系统获得更高的安全性，且能通过简单的数值运算或光学实验装置得到质量非常高的解密图像，还从理论上分析了该算法的时间复杂度。计算机模拟结果表明，该加密算法的收敛速度快，能迅速找到非常好的近似解，解密图像质量高且系统安全性良好。

关键词： 信息光学；光学加密；信息安全；级联相位恢复算法

中图分类号：O438.2 文献标识码：A

Optical Image Encryption Based on Cascaded Phase Retrieval Algorithm

Yu Bin[1,2] Peng Xiang[1,2]

(1 *Institute of Optoelectronics, Key Laboratory of Optoelectronic Devices and Systems of Ministry of Education, Shenzhen University, Shenzhen* 518060
2 *State Key Laboratory of Precision Measuring Technology and Instruments, Tianjin University, Tianjin* 300072)

Abstract: A new technique of optical image encryption and decryption based on the methodology of virtual optics is proposed. The technique is based on the free space propagation optical system and encodes the target image into two different phase masks (PM) by using cascaded iterative angular spectrum phase retrieval approach (CIASA) and both two phase masks can serve as enciphered texts. The proposed algorithm employs an improved scheme, i.e. modifying the phase distributions of two phase masks synchronously and enlarging the search space, and the time complexity of the algorithm is discussed, too. Computer simulations show that the algorithm generates much faster convergence and better image quality for the decrypted image and key space enlarged. These characters may introduce high security-level that makes the encrypted image much harder to be decrypted by an unauthorized person.

Key words: information optics; optical encryption; information security; cascaded phase retrieval algorithm

1 引 言

近年来，基于光学信息处理的图像加密技术引起人们的广泛关注[1~18]。光学信息处理系统具有高并行性和高加密维度等特点，因而研究和开发光学安全系统对信息安全技术的发展具有重要的学术意义和应用前景。目前用于光学图像加密的算法有多种，但主要可分为两类：一类是基于 Réfrégier 等[1~3]提出的双随机相位编码加密技术，但该方法需要同时记录加密图像的振幅和相位信息，因而在图像解密时光学效率不高；另一类是基于 Wang 等[6,7,9]提出的基于相位恢复算法的光学加密技术，但该方法加密时，其中一块相位板是固定的，限制了搜索空间，必然导致密级降低以及解密图像的质量不高，并且还存在很大的噪声。上述两种纯光学的方法，存在的一个致命缺点就是，4－f 光学系统对元件的空间排列精度要求非常高，尤其是在解密阶段，由于相位的随机性，当全部数据用于解密时，谱平面上的相位板偏离匹配位置哪怕只有一个像素大小的距离，也不能获得解密图像，这成为了光学图像加密走向实用化的一个瓶颈。Peng 等[10~15]提出了

* 国家自然科学基金(60472107)，广东省自然科学基金博士启动基金(04300862)和深圳市科技计划项目(200426)资助课题。
作者简介：于 斌(1976～)，男，博士，主要从事光学信息安全、相位恢复的研究。E-mail：yubin@szu.edu.cn
收稿日期：2004-09-14；收到修改稿日期：2005-03-02

基于虚拟光学框架构造密码算法的思想，并利用并行硬件实现了这一思想，使得光学信息安全技术与业已发展程度非常高的数字技术有机地结合起来，推动了光学信息安全技术的实用化。

本文在虚拟光学框架下的密码算法构造思想的指导下，提出一种新的构造算法，这种把待加密的图像分别编码到两块相位模板(PM)之中的加密算法，既可利用光学的方法，也可利用数字方法来实现。该算法是基于 Mellin 等[19]在设计衍射光学元件时提出的迭代角谱法。本文的方法需要恢复两个级联的相位模板的相位，因此称之为级联迭代角谱法(cascaded iterative angular spectrum approach, CIASA)。文中还对解密图像的均方误差与迭代次数的关系以及算法的收敛速度进行了分析。

2 级联迭代角谱加密方法

本文提出的级联迭代角谱法加密算法可采用单色平面波照明下的自由空间传播的光学系统来实现，如图 1 所示。在加密过程中，我们希望设计出两块相位模板，把待加密的图像的波函数编码到两块相位模板的相位分布中去。在解密过程中，用平行光照射这两块空间分离的相位模板，在一定的传播距离处获得解密的图像。这种加密的思想相当于已知宿主图像的振幅场分布，反向求解出两块相位模板的相位分布的逆问题。对两块相位模板的求解实际上是两个级联的相位物体的相位恢复问题，即已知两块相位模板和宿主图像的振幅分布，如何确定两块相位模板的相位分布，使之能够调制入射光场，产生期望的光输出。

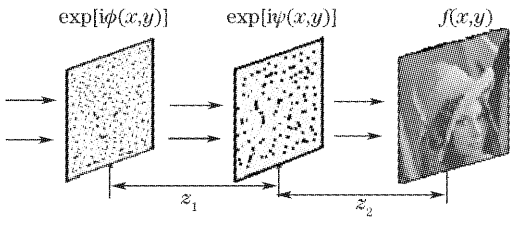


图 1 加密/解密系统的光学实现

Fig. 1 Optical implementation of the encryption and decryption system

根据平面波角谱的传播理论[20]，沿光轴、相互间隔距离为 z 的两平面间的光传播可采用角谱的方法计算，此计算可用快速傅里叶变换(FFT)算法来实现：

$$f_2[m,n]=\mathcal{F}_F^{-1}\{\mathcal{F}_F\{f_1[m,n]\}\cdot H(f_X,f_Y;z)\},\quad(1)$$

其中，

$$H(f_X,f_Y;z)=\exp[\mathrm{j}kz(1-\alpha^2-\beta^2)^{1/2}]=\exp\{\mathrm{j}kz[1-(\lambda f_X)^2-(\lambda f_Y)^2]^{1/2}\}$$

为了书写方便，(1)式简化为

$$f_2[m,n]=L\{f_1[m,n];z\},\quad(2)$$

其中 L 命名为自由空间传播算子，代表(1)式的运算。

级联迭代角谱法就是基于(2)式进行运算的，其运算过程如下：

1) 在[0,2π]之间选择均匀、随机分布的 $M\times N$ 相位阵列，$\phi_1[m,n]$ 和 $\phi_2[m,n]$，即第一块和第二块相位模板的初始相位值，因此，第一块相位模板的初始波前函数为

$$f_1[m,n]=\exp\{\mathrm{j}\phi_1[m,n]\}$$

2) f_1 经自由空间传播距离 z_1 后，到第二块相位模板面前的波前函数：

$$f_2[m,n]=L_1\{f_1[m,n];z_1\}$$

其中 L_1 代表自由空间传播算子；

3) 提取 f_2 的中间相位 θ，并引入振幅限制条件[21]，则在第二块相位模板面后的波前函数为

$$f_3[m,n]=g[m,n]\exp\{\mathrm{j}(\theta[m,n]+\phi_2[m,n])\},$$

其中

$$g[m,n]=\begin{cases}|f_2[m,n]|, & |f_2[m,n]|\leqslant M\\ M, & |f_2[m,n]|\geqslant M\end{cases}$$

式中 M 代表振幅阈值因子。

4) f_3 经自由空间距离传播到像平面，得到像平面的波前函数：

$$f_4[m,n]=L_2\{f_3[m,n];z_2\}$$

其中 L_2 代表自由空间传播算子。

5) 引入 f_4 的振幅限制条件，即相位保持不变，其强度分布变为待加密图像的振幅分布，结果是

$$f_5[m,n]=\sqrt{I[m,n]}\exp\left[\mathrm{j}\arctan\left(\frac{\mathrm{Im}\{f_4[m,n]\}}{\mathrm{Re}\{f_4[m,n]\}}\right)\right],$$

其中 I 代表待加密图像的强度分布。

6) f_5 经反向传播到第二块相位板前的波前函数变为

$$f_6[m,n]=L_2\{f_5[m,n];-z_2\}.$$

7) 提取 f_6 的相位，

$$\phi[m,n]=\arctan\left(\frac{\mathrm{Im}\{f_6[m,n]\}}{\mathrm{Re}\{f_6[m,n]\}}\right),$$

对第二块相位板的相位作修正，作为下一次迭代过程的初始分布：

$$\phi_2[m,n]=\phi[m,n]-\theta[m,n].$$

8) 提取在第三步中获得的相位 θ，附加在波前

函数 f_6 上，获得新的波前函数：

$$f_7[m,n] = |f_6[m,n]|\exp\{j\theta[m,n]\}.$$

9) f_7 反向传播到第一块相位模板，得到新的波前函数：

$$f_8[m,n] = L_1\{f_7[m,n]; -z_1\}.$$

10) 提取 f_8 的相位

$$\phi_1[m,n] = \arctan\left(\frac{\mathrm{Im}\{f_8[m,n]\}}{\mathrm{Re}\{f_8[m,n]\}}\right).$$

对第一块相位板的相位进行修正，作为下一次迭代过程的初始分布：

$$f_1[m,n] = \exp\{j\phi_1[m,n]\}.$$

11) 重复步骤 2)～10)，进行新的循环迭代运算，直到定义的均方差(mean square error，MSE)达到设计的精度或者循环次数达到设置的最大迭代次数为止。均方差定义为

$$E_{\mathrm{MSE}}(k) = \frac{1}{M\times N}\sum_{n=1}^{N}\sum_{m=1}^{M}[|f(m,n)|^2 - |f_k(m,n)|^2]^2,$$

其中 $I = |f|^2$ 为被加密图像的强度分布，$I_k = |f_k|^2$ 为经过第 k_{th} 次迭代以后，解密图像的强度分布。

从上面的算法中可看出，单色平面波的波长 λ，传播距离 z_1，z_2 和两块相位板及其排列顺序，都可作为加密的密钥，扩大了密钥空间，而且也增大了算法的搜索空间，因此增加了系统的安全性，提高了解密图像的质量。

从上面的论述可以看出，级联迭代角谱法加密算法是一种虚拟光学的可视化密码技术，把要加密的宿主信息通过该算法隐藏到两个或多个(多次级联)相位模板中，在每一块相位模板中都含有部分信息。如果只持有一块相位模板，则不论用什么方法都无法分析出任何有用信息。只有把所有相位模板按正确位置排列，并且用正确波长照射，才能通过光学方法得到正确解密结果；或者通过简单的计算，通过数字的方法获得加密的明文信息。

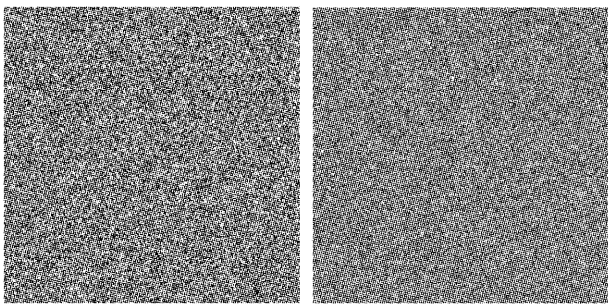
3　计算机模拟结果

为了验证上述算法，我们进行了计算机模拟实验。我们尝试把待加密的图像编码到两块相位板之中去，用 MATLAB 仿真软件进行计算机仿真，待加密的图像为 256 pixel×256 pixel、灰阶数为 256 的莉娜(Lena)像，如图 2 所示。两相位板平面都和图像面采用同样的尺寸，假定系统用一个单位振幅的单色平面波照明，其波长 λ=632.8 nm，第一块相位模板和第二块相位模板面之间的距离 z_1=1 m，第二块相位模板面和待加密图像面之间的距离 z_2=2 m。

图 2　待加密的图像

Fig. 2　The target image to be encrypted

算法开始时，先把两块相位模板均初始化为在 0～2π之间均匀分布的阵列，使它们具有白噪声分布，然后按照算法流程来回迭代，经 20 次迭代后，两块相位板的相位分布的优化值如图 3 所示，此时待加密的图像的波函数已编码到这两块相位板之中，也就是说，这两块相位板就是加密之后的图像的波函数。



(a)　(b)

图 3　图像加密优化后的(a)第一块相位模板 (b)第二块相位模板

Fig. 3　(a) First and (b) second phase masks encrypting the target image after optimization

图 4(a)为正确使用系统参量和相位板时的解

(a)　(b)

图 4　(a)正确解密后的图像，(b)以不正确的相位板顺序得到的解密图像

Fig. 4　The decrypted image with (a) correct phase masks and all parameter keys (b) incorrect order phase masks

密结果，图 4(b)为系统参量正确，只是改变两块相位板的先后位置时的解密结果，从图 4(a)中可看出解密图像的质量非常高，图 4(b)图说明了只要两块相位板不匹配，就得不到正确的解密图像。

图 5 给出了迭代过程中解密图像的均方差函数随迭代次数的变化情况。从图 5 中可以看出，经过 20 次迭代，均方差函数已接近 10^{-7}，这表明级联迭代角谱加密算法的收敛速度特别快。

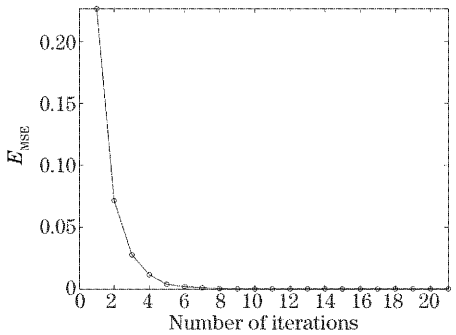


图 5 均方差与迭代次数的关系

Fig. 5 Relationship between the mean square error and the number of iterations

4 算法复杂度分析

算法的复杂度决定了该算法所占用的工作时间和计算工作量。级联迭代角谱法加密算法的核心运算是快速傅里叶变换，从第二节的公式中可以看出，在一次迭代过程中要进行八次快速傅里叶变换运算和四次复振幅修正运算，快速傅里叶变换的复杂度为 $O(n\mathrm{lb}n)$，因此，级联迭代角谱法算法的复杂度为 $O[m\cdot(8n\mathrm{lb}n+4)]$，$m$ 为迭代次数，n 为像元数。可以看出，该算法运算工作量不大。

5 结 论

本文提出了一种新的级联迭代角谱相位恢复的加密算法，成功地把一幅图像加密到两块相位板之中，该算法扩大了密钥空间，且可同时调整两块相位板的相位分布，即也扩大了搜索空间，因此，能得到高质量，高安全性的解密图像。计算机模拟表明，该算法收敛速度也非常快。我们还发现该算法具有较强的稳健性和抗噪性能，具体分析将另文讨论。

参 考 文 献

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

2 E. Tajahuerce, O. Matoba, S. C. Verrall *et al.*. Optoelectronic information encryption with phase-shifting interferometry[J]. *Appl. Opt.*, 2000, **39**(14): 2313～2320

3 G. Unnikrishnan, J. Joseph, K. Singh. Optical encryption by double-random phase encoding in the fractional Fourier domain [J]. *Opt. Lett.*, 2000, **25**(12): 887～889

4 Shutian Liu, Li Yu, Banghe Zhu. Optical image encryption by cascaded fractional Fourier transforms with random phase filtering[J]. *Opt. Commun.*, 2001, **187**(1～3): 57～63

5 D. Weber, J. Trolinger. Novel implementation of nonlinear joint transform correlators in optical security and validation[J]. *Opt. Engng.*, 1999, **38**(1): 62～68

6 R. K. Wang, lan A. Watson, C. Chatwin. Random phase encoding for optical security[J]. *Opt. Engng.*, 1996, **35**(9): 2464～2469

7 Y. Li, K. Kreske, J. Rosen. Security and encryption optical systems based on a correlator with significant output image[J]. *Appl. Opt.*, 2000, **39**(29): 5295～5301

8 D. Abookasis, O. Arazi, J. Rosen *et al.*. Security optical systems based on a joint transform correlator with significant output images[J]. *Opt. Engng.*, 2001, **40**(8): 1584～1589

9 H. T. Chang, W. C. Lu, C. J. Kuo. Multiple-phase retrieval for optical security systems by use of random-phase encoding[J]. *Appl. Opt.*, 2002, **41**(23): 4825～4834

10 Xiang Peng, Lingfeng Yu, Lilong Cai. Double-lock for image encryption with virtual opitcal wavelength[J]. *Opt. Express*, 2001, **10**(1): 41～45

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

12 Xiang Peng, Zhiyong Cui, Tieniu Tan. Image encryption with virtual-optics[C]. *Proc. SPIE*, 2002, **4929**: 96～104

13 Xiang Peng, Peng Zhang, Hanben Niu. Architecture design of virtual-optics data security using parallel hardware and software [J]. *Optik*, 2004, **115**(1): 15～22

14 Peng Xiang, Zhang Peng, Niu Hanben. Information hiding theory based on virtual optics and its implementation with parallel hard ware[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

15 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

16 G. Situ, J. Zhang. A cascaded iterative Fourier transform algorithm for optical security applications [J]. *Optik*, 2003, **114**(10): 473～477

17 E. G. Johnson, J. D. Brasher. Phase encryption of biometrics in diffractive optical elements [J]. *Opt. Lett.*, 1996, **21**(16): 1271～1273

18 G. Situ, J. Zhang. A lensless optical security system based on computer-generated phase only masks[J]. *Opt. Commun.*, 2004, **232**(1～6): 115～122

19 Stephen D. Mellin, Gregory P. Nordin. Limits of scalar diffraction theory and an iterative angular spectrum algorithm for finite aperture diffractive optical element design [J]. *Opt. Express*, 2001, **8**(13): 706～722

20 J. Goodman. *Introduction to Fourier Optics* [M]. New York: McGraw-Hill, 1968

21 Henry Stark. *Image recovery: Theory and Application* [M]. Academic: Orlando, Fla., 1987. Chap. 8, 277