文章编号：0253-2239(2009)10-2705-04

相位恢复算法用于分区复用多图像加密的研究

史祎诗[1,2] 张静娟[2]

([1] 中国科学院研究生院材料科学与光电技术学院，北京 100049；[2] 中国科学院研究生院物理科学学院，北京 100049)

摘要 衍射投影效应明显降低了基于双相位编码的多图像加密系统的性能。提出分区复用技术来解决这一问题。待加密的多个图像被放置于各个输出平面的不同区域，于是相邻两个输出平面的秘密图像区域将错落开来，因而有效抑制了衍射投影所产生的噪声。在此基础上，重点研究了用于该系统的相位恢复算法。在完整的顺序迭代之后，对解密质量最差的图像进行逐一补偿，从而寻找到了更加符合多幅秘密图像客观特点的子循环次序。根据这一次序，用完整迭代后附加调节性迭代的方法或者完全更换迭代次序的方法，都能够在保留基本算法快速收敛优势的前提下，使多幅解密图像质量以及系统地复用容量得以整体提高。

关键词 傅里叶光学；相位恢复；光学图像加密；信息安全

中图分类号 O438 **文献标识码** A **doi**：10.3788/AOS20092910.2705

Research on the Phase Retrieval Algorithm Used for Multiple-Image Encryption with Region Multiplexing

Shi Yishi[1,2] Zhang Jingjuan[2]

([1] *College of Materials Science and Opt-electronic Technology, Graduate University of Chinese Academy of Sciences, Beijing* 100049, *China*

[2] *College of Physical Sciences, Graduate University of Chinese Academy of Sciences, Beijing* 100049, *China*)

Abstract The effect of diffractive shadow evidently degrades the performance of the multiple-image encryption system based on double phase encoding. The region multiplexing is proposed to solve this problem. Since multiple images to be encrypted are located in different regions of each output plane, the noise arising from the effect of diffractive shadow can be suppressed. The corresponding phase retrieval algorithm is studied through theoretical analysis and computer simulations. After the whole iterations with the normal sequence, the image with the worst decrypted quality is compensated one by one. In this way, we can obtain the sequence of sub-iteration which is objectively suitable for the characters of multiple images to be encrypted. Based on this sequence, either an adjusting iteration after the whole iterations with the original sequence or completely changing the sequence of the whole iterations can be adopted. As a result, maintaining the advantage of the phase retrieval algorithm converging fast, both the quality of all decrypted multiple images and the multiplexing capacity of the system can be improved.

Key words Fourier optics; phase retrieval; optical image encryption; information security

1 引 言

多图像加密和隐藏是光学信息安全领域中的一个热点问题[1,2]。它在多用户认证、内容分发、提高秘密信息传输效率等方面具有很高的应用价值。现有的方法包括 Hadamard 矩阵变换方法[3]、数字全息术主导的方法[4]、波长复用[5]、扩频技术[6]等。然而，现有方法大多包含多幅秘密图像经过编码后实施的迭加操作[2]，其所产生的加性串扰正是造成提

收稿日期：2008-10-12；**收到修改稿日期**：2008-11-30

基金项目：国家自然科学基金（60577039）、中国博士后科学基金、中国科学院研究生院院长基金和王宽诚教育基金会资助项目。

作者简介：史祎诗(1981—)，男，博士后，目前主要从事衍射光学在信息安全中的理论与应用等方面的研究。E-mail：sysopt@126.com

导师简介：张静娟(1942—)，女，教授，主要从事全息和光信息处理、衍射光学的研究。E-mail：jjzhang@gucas.ac.cn.

取图像质量明显下降以及复用容量被严重限制的主要原因，并导致现有系统基本上只适用于二值图像的隐藏，从而应用范围也受到较大局限。对此，我们提出频域信息预选系统[7]，从解决信道过载的角度消除了多图像间的串扰，提高了加密性能。并且，我们还提出了双相位编码系统[8]。该系统的核心是用相位恢复算法将多幅秘密图像编码为一对纯相位板(POMs：Phase only masks)。由于采用 Fresnel 域内输出图像的分立构架，避免了多图像之间的加性串扰，较为有效地在保真度和复用容量的矛盾之间取得了平衡。但是，所谓的衍射投影效应[9]明显降低了双相位编码系统用于灰度图像时的性能。

本文提出了分区复用进行多图像加密的概念，并着重研究了相应的相位恢复算法[10~16]以使多图像加密系统获得更高的保真度和复用容量。

2 系统与基本算法

分区复用多图像加密系统如图 1 所示。该图展示了加密 8 幅秘密图像的情形。系统的各个平面均位于 Fresnel 域内。假设待加密的多幅秘密图像集为 $\{g_{oi}\}(i=1,2,\cdots,N)$。当 $N=8$ 时，可用字母“A”至“H”来表示图像集 $\{g_{oi}\}$。如果每幅图像的空间尺寸为 $S\times S$，那么双 POMs 的空间尺寸则为 $2S\times 2S$。因此，图像“A”至“H”在被置于各输出平面时分别只占据各平面的 1/4。需注意，每两个相邻输出平面的兴趣区域，即图 1 中用“A”至“H”标志出的区域必须交错开来。于是，前一个输出平面的兴趣区域向后一个平面兴趣区域的衍射投影所产生的噪声就会被有效地抑制。实际上，由于兴趣区域并不一定要求严格错开，因此对于既定秘密图像集合就存在许多不同的复用方式。本文将这种方式称为分区复用。图 1 给出的是一种严格满足该要求的系统构架。

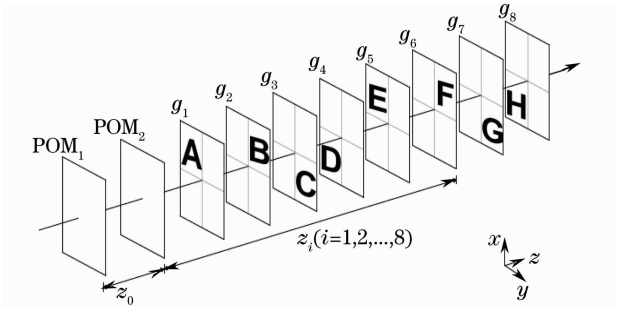

图 1 分区复用多图像加密系统

Fig. 1 The optical setup of the multiple-image encryption with region multiplexing

在加密过程中，用相位恢复算法来产生两个 POMs 的相位分布函数作为所谓的相位密钥。附加密钥包括波长 λ、位置参数 z_0 和 $\{z_i\}$。它们及纯相位板的尺度需要满足 Fresnel 近似。在相应的解密过程中，既定波长的入射平面波被双 POMs 依次调制，在预定义轴向位置的输出平面上产生解密图像，可以用 CCD 等图像传感器在各输出平面相应的兴趣区域获取各解密图像的光强分布。

为了节省篇幅，以框图的形式给出所采用相位算法的基本步骤，如图 2 所示。先将双 POMs 的相位分布函数 Ψ 和 φ 均用随机分布函数初始化。如果总共有 N 幅待加密图像，那么每次迭代中就包含 N 个子循环，各子循环分别针对 $\{g_{oi}\}$ 其中之一。图 2 以 g_{oi} 为例描绘了第 k 次迭代过程中的第 i 个子循环的过程。FrT 表示 Fresnel 变换，IFrT 则代表相应的逆 Fresnel 变换。在每个子循环中，都须顺序进行两次 Fresnel 正变换和两次 Fresnel 逆变换。值得注意的是，得益于分区复用，我们只需约束 g_{oi} 所在平面兴趣区域的振幅。在该循环结束后，g_{oi} 所在平面的相位保留，两个 POMs 的相位分布分别如图 2 中的公式进行替换，随后进入以另一幅相邻图像 $g_{o(i+1)}$ 的子循环之中。当子循环遍历了全部 N 幅秘密图像 $\{g_{oi}\}$ 之后，才完成一次迭代。算法的迭代进程可以由迭代次数或振幅分布之间的相关系数值(C_o)控制：

$$C_o(g,g_o)=\mathrm{cov}(g,g_o)(\sigma_t\cdot\sigma_{t_o})^{-1}, \quad (1)$$

其中 $\mathrm{cov}(g,g_o)$ 表示解密图像 g 和原始秘密图像 g_o 之间的互协方差，σ 为标准偏差。因此，可用 C_o 表示解密图像的质量。C_o 取值范围为[0,1]，其值越接近 1 表明解密像质越高。

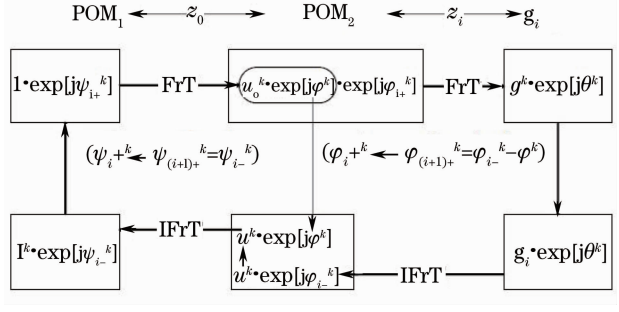

图 2 所采用的相位恢复算法框图

Fig. 2 The flow chart of the phase retrieval algorithm employed

3 模拟分析与算法研究

在每次迭代中，我们均依照从 g_{o1} 至 g_{oN} 的顺序来进行子循环以完成对秘密图像集 $\{g_{oi}\}$ 中 N 幅图

像的遍历。由于在算法中只对占各平面一部分的兴趣区域进行约束，因而可以取得比未引入分区复用的系统[7]要好得多的效果。将灰度图像的复用容量从少量的几幅提高到十幅以上，且保真度也同时大为改善。这些将从稍后的模拟结果中得到证实。另外，尽管在图 1 所示的系统中 POMs 的空间尺寸为单幅加密图像时的四倍，但算法的时间开销并不随之而线性递增。模拟结果显示，所增时间开销不超过 10%。同时因为原算法时间开销本身就很小[8]，所以仍能确保算法的高效率。

然而，有一个问题不得不引起注意：一些解密图像质量很高，而另外一些则差强人意。尤其对于灰度图而言，C_o 值如能高于 0.9 才比较理想。原因在于，本算法的子循环收敛速度非常快[11]。于是，在经过有限次数的迭代之后，双 POMs 的相位分布函数就会接近于对其中几幅秘密图像的恢复准确的解，而远离对另外几幅秘密图像的解。更重要的是，随着待加密图像的幅数增加，多幅解密图像之间质量的悬殊就更加明显了。

我们提出了两种方法解决这一问题：方法一(Method 1)是在完整迭代进程结束之后，增加一个调节性的迭代来补偿解密质量下降的图像。方法二(Method 2)则彻底改变迭代中 N 个子循环的次序。事实上，上述两种方法均基于以下观点，即尊重所有待加密的 N 幅图像各自的客观特点。因此，有必要寻找一种更切合于 N 幅秘密图像的子循环次序，来替代简单的按照从 1 至 N 的子循环次序，从而最终寻求 N 幅图像解密质量的整体改善。

解密质量的补偿是寻找子循环顺序的重要线索。当按照常规顺序完成既定迭代之后，利用所得到的双 POMs 相位密钥就可以获取所有 N 幅解密图像与原始秘密图像之间的相关系数值。假设其中最小的 C_o 值所对应的图像为 g_{op}，则对其进行一次额外的子循环作为补偿。再重复上述步骤，在新得到的一组 C_o 中找出并补偿另外一幅图像 g_{oq}。依靠这一途径，就相当于用 C_o 值及子循环补偿机制标记了多幅秘密图像。当补偿了(N-1) 幅图像时，我们假设所得到的补偿次序为$\{p \to q \to \cdots \to v\}$。由此，也得到了适用于方法一的调节性迭代次序，即其逆序：$\{v \to \cdots \to p \to q\}$。对于方法二，完整的子循环次序应为$\{N \to v \to \cdots \to p \to q\}$，其中加上了待加密图像 g_{oN}，这是因为若迭代中之于 g_{oN}，则其解密质量往往最好。以上所研究的子循环次序，均是针对 N 幅图像在系统中既定的排列顺序而论的。

表 1 给出了三组计算机模拟结果的对比。模拟所用的波长参量 λ 为 632 nm，z_0 为 30 mm，z_1 为 20 mm，各输出平面的轴向距离为 10 mm。双 POMs 为每个采样点 512 pixel×512 pixel，各幅图像均为 256 灰阶、每个采样点 256 pixel×256 pixel，采样点间距6.25 μm。$\{C_{o14}\}$是用按照常规的 1 至 N 的子循环次序进行了 14 次完整迭代后，得到的双 POMs 所获得的 8 幅解密图像对应的结果。对比我们以前仅能加密 3 幅平均 C_o 值低于 0.8 的灰度图像的系统而言[7]，本系统与算法已经有了显著提高。方法一和方法二则进一步改善了基本算法的总体效果。其对应的 $\{C_{oM1}\}$ 和 $\{C_{oM2}\}$ 结果显示，平均相关系数增大，尤其在 $\{C_{oM1}\}$ 中所有的相关系数值均大于0.92，而 $\{C_{o14}\}$ 中却有三个值低于0.90。更重要的是，如前述分析所料，两法将最大、最小 C_o 的差值 ΔC_o 从 0.1477 分别减小到 0.0619 和 0.0708。C_o 值的趋同性更加表明这两种算法策略对于多幅解密图像恢复质量的补偿是较成功的。

表 1　加密 8 幅图像时不同算法策略的效果对比

Tab 1　Comparison on the results of different strategies of the algorithms when eight images are encrypted

C_o	Average	g_1	g_2	g_3	g_4	g_5	g_6	g_7	g_8
$\{C_{o14}\}$	0.9285	0.8470	0.8731	0.8838	0.9396	0.9514	0.9654	0.9730	0.9947
$\{C_{oM1}\}$	0.9436	0.9839	0.9693	0.9566	0.9352	0.9314	0.9246	0.9220	0.9256
$\{C_{oM2}\}$	0.9415	0.9881	0.9735	0.9602	0.9243	0.9255	0.9173	0.9151	0.9280

为直观起见，同时给出与表 1 相应的灰度图像，如图 3 所示。图 3(a1)，(a2)分别为原始秘密图像 g_1 和 g_8。图 3(b)～(e)分别是在三种算法策略下求解出的双 POMs 相位密钥所得到相应的解密图像。这里，图 3 和表 1 数据充分地证明了基本算法的有效性以及两种改进算法对多幅解密图像质量的整体均衡效用。

此外，以灰度图像为对象进行了大量模拟，发现在上述参量所限定的系统中，用上述算法经过几十次迭代后产生的双 POMs 相位密钥，可获得平均 C_o 值为 0.9 以上的 12 幅解密图像。并且发现，通过参量选取，能够使系统达到更高的复用容量和保真度。

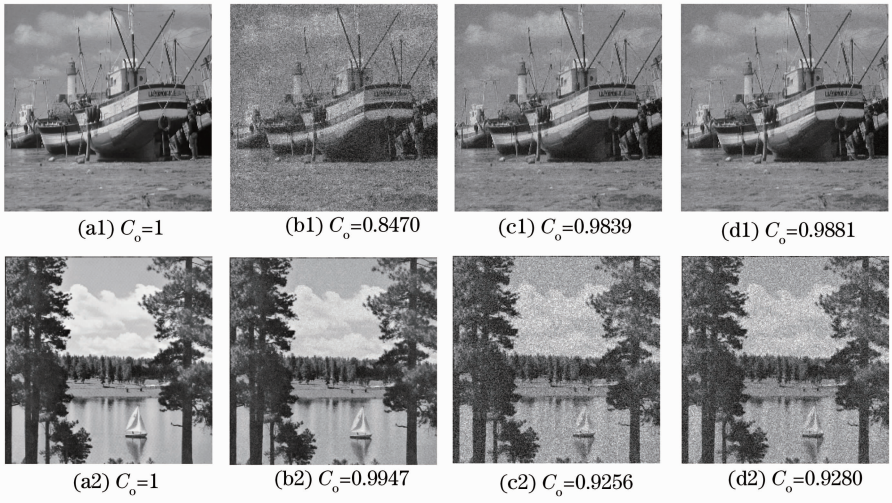

图 3 原始秘密图像与解密图像对比

Fig. 3 Comparison between chosen original secret images and corresponding decrypted images by different algorithms

4 结 论

在引入分区复用技术之后，基于双相位调制的多图像加密系统的性能得以显著提高。这归因于分区复用的方式抑制了衍射投影效应的噪声影响。研究了用于该系统的相位恢复算法后发现：用逐一补偿解密图像质量的方法，可以寻找到客观上更加符合多幅秘密图像集自身特点的子循环次序；以该次序完成迭代，就能够在保留基本算法快速收敛优势的同时，从整体上提高多图像的解密质量。

参 考 文 献

1 I. J. Cox, M. L. Miller, J. A. Bloom. *Digital Watermarking* [M]. San Francisco, CA: Morgan Kaufmann, 2002

2 Zhang Jingjuan, Shi Yishi, Situ Guohai. A Survey on Optical information hiding[J]. *Journal of the Graduate School of the Chinese Academy of Sciences*, 2006, **23**(3): 289～296
张静娟，史祎诗，司徒国海. 光学信息隐藏综述[J]. 中国科学院研究生院学报, 2006, **23**(3): 289～296

3 J. Kim, J. Choi, E. Kim. Optodigital implementation of multiple information hiding and extraction system [J]. *Opt. Eng.*, 2004, **43**(1): 113～125

4 M. He, L. Cai, Q. Liu *et al*.. Multiple image encryption and watermarking by random phase matching[J]. *Opt. Commun.*, **247**(1): 29～37

5 Guohai Situ, Jingjuan Zhang. Multiple-image encryption by wavelength multiplexing [J]. *Opt. Lett.*, 2005, **30** (11): 1306～1308

6 B. M. Hennelly, T. J. Naughton, J. Mcdonald *et al*.. Spread-space spread-specrum technique for secure multiplexing[J]. *Opt. Lett.*, 2007, **32**(9): 1060～1062

7 Yishi Shi, Guohai Situ, Jingjuan Zhang. Multiple-image hiding by information prechoosing [J]. *Opt. Lett.*, 2008, **32** (13): 1914～1916

8 Yishi Shi, Guohai Situ, Jingjuan Zhang. Multiple-image hiding in the Fresnel domain[J]. *Opt. Lett.*, 2007, **33**(6): 542～544

9 M. Makowski, M. Sypek, A. Kolodziejczyk *et al*.. Three-plane phase-only computer hologram generated with iterative Fresnel algorithm[J]. *Opt. Eng.*, 2005, **44**(12): 125805

10 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

11 Yishi Shi, Guohai Situ, Jingjuan Zhang. Optical image hiding in the Fresnel domain[J]. *J. Opt. A: Pure. Appl. Opt.*, 2006, **8**(6): 569～577

12 Ji jin, Huang Fei, Wang liang *et al*.. Information encryption based on digital holography and phase retrieve algorithm [J]. *Chinese J. Lasers*, 2007, **34**(10): 1408～1412
季 瑾，黄 飞，王 亮 等. 利用数字全息和相位恢复算法实现信息加密[J]. 中国激光, 2007, **34**(10): 1408～1412

13 Zhang Haiying, Ran Qiwen, Zhang Jin. Optical image encryption and multiple parameter weighted fractional fourier transform[J]. *Acta Optica Sinica*, 2008, **28**(s2): 117～120
张海莹，冉启文，张 晋. 光学图像加密与多参数加权类分数傅里叶变换[J]. 光学学报, 2008, **28**(s2): 117～120

14 Wang Xiao, Mao Heng, Zhao Dazun. Experimental verification of phase retrieval based on intensity transport equation[J]. *Acta Optica Sinica*, 2008, **28**(s2): 87～90
王 潇，毛 珩，赵达尊. 光强传播方程相位恢复的实验验证[J]. 光学学报, 2008, **28**(s2): 87～90

15 Wei Hengzheng, Peng Xiang, Zhang Peng *et al*.. Chosen-plaintext attack on double phase encoding encryption technique [J]. *Acta Optica Sinica*, 2007, **27**(5): 824～829
位恒政，彭 翔，张 鹏 等. 双随机相位加密系统的选择明文攻击[J]. 光学学报, 2007, **27**(5): 824～829

16 Wu Kenan, Hu Jiasheng, Wu Xu. Optical Encryption for Information Security [J]. *Laser & Optoelectronics Progress*, 2008, **45**(7): 30～38
吴克难，胡家升，乌 旭. 信息安全中的光学加密技术[J]. 激光与光电子学进展, 2008, **45**(7): 30～38