激光技术 2013, 37(5) 577-581 DOI: 10.7510/jgjs.issn.1001-3806.2013.05.004 ISSN: 1001-3806 CN: 51-1125/TN

光通信与光信息技术

基于球面波照射的非对称光学图像加密

丁湘陵

怀化学院 物理与信息工程系, 怀化 418008

摘要:

为了克服基于相位截断傅里叶变换的非对称光学图像加密系统不能抵御已知明文攻击的缺陷,采用球面波的自带因子扰乱输入图像空间信息的方法实现图像的加解密,并通过理论分析和实验仿真进行了研究。结果表明,该方法既能抵御已知明文攻击和保持非线性特性,又能获得原系统加解密图像的效果,同时还能减少相位掩膜数量,简化系统设置。这一结果对于改进基于相位截断傅里叶变换的非对称光学图像加密系统的安全性是有帮助的。

关键词: 信息光学 图像加密 球面波 已知明文攻击 非线性特性

Asymmetric optical image cryptosystem based on spherical wave illumination

DING Xiang-ling

Department of Physics and Information Engineering, Huaihua College, Huaihua 418008, China

Abstract:

In order to overcome the known plaintext attack which the asymmetric optical image cryptosystem based on phase-truncated Fourier transforms can not resist, an encryption method based on phase-truncated Fourier transforms was proposed by employing the phase factor of the spherical wave under the spherical wave illumination. The theoretical analysis and experiment results indicate that the proposed encryption method can maintain the asymmetric characteristic of the cryptosystem and avoid various types of the currently existing attacks, especially the known plaintext attack, which the asymmetric cryptosystem based on phase-truncated Fourier transforms can not resist. The results are helpful for the security improvement of the asymmetric optical image cryptosystem based on phase-truncated Fourier transform.

Keywords: information optics image encryption spherical wave known plaintext attack asymmetric characteristic

收稿日期 2013-01-04 修回日期 2013-01-21 网络版发布日期 2013-07-25

DOI: 10.7510/jgjs.issn.1001-3806.2013.05.004

基金项目:

怀化市创新团队基金资助项目(2012-16)

通讯作者:

作者简介: 丁湘陵(1981-),男,讲师,硕士,主要从事信息光学的研究。E-mail:dingxl1981@163.com

作者Email:

参考文献:

[1] REFREGIER P, JAVIDI B. Optical image encryption based on input plane and Fourier plane random encoding[J]. Optics Letters,1995,20(7):767-769.
[2] SITU G H, ZHANG J J. Double random phase encoding in the Fresnel domain[J]. Optics Letters,2004,29(14):1584-1586.
[3] LIN R, LIU Q N, ZHANG C L. A new fast algorithm for gyrator transform[J]. Laser Technology,2012,33(1):50-53(in Chinese).
[4] NISHCHAL N K, JOSEPH J, SIGN H K. Optical encryption using cascaded extended fractional Fourier transform[J]. Optical Memory & Neural Networks,2003,12(2): 139-145.
[5] HWANG H E, CHANG H T, LIE W N. Fast double-phase retrieval in Fresnel domain using modified Gerchberg-Saxton algorithm for lensless optical security systems[J]. Optics Express,2009,17(16):13700-

13710.
[6] HENNELLY B, SHERIDANJ T. Optical image encryption by random shifting in fractional Fourier domains[J]. Optics Letters,2003,28(4): 269-271.
[7] DENG X P. Optical image encryption using double phase mask based on spherical wave illumination [J]. Laser Technology,2006,30(4):442-444(in Chinese).
[8] DENG X P, XIANG G X, WANG Sh F. Optical image encryption using only one random phase mask based on spherical wave illumination[J]. Laser Journal,2005,26(5): 52-53(in Chinese).
[9] DENG X P, ZOU K. Optical image encryption using one random phase mask based on spotlight illumination in the Fresnel domain[J]. Laser Technology,2006,30(3):327-328(in Chinese).
[10] DENG X P. Optical image encryption based on asymmetric abnormal Fourier transform[J]. Journal of Applied Optics,2007,28(3):262-264(in Chinese).
[11] PENG X, ZHANG P, WEI H Zh, *et al*. Known-plaintext attack on optical encryption based on double random phase keys[J]. Optics Letters,2006,31(8):1044-1046.
[12] PENG X, WEI H Zh, ZHANG P. Chosen-plaintext attack on lensless double-random phase encoding in the Fresnel domain[J]. Optics Letters,2006,31(8):3261-3263.
[13] GOPINATHAN U, MONAGHAN D S, NAUGHTON T J, *et al*. A known-plaintext heuristic attack on the Fourier plane encryption[J]. Optics Express,2006,14(8):3181-3186.
[14] FRAUEL Y, CASTRO A, NAUGHTON T J, *et al*. Resistance of the double random phase encryption against various attacks[J]. Optics Express,2007,15(16):10253-10265.
[15] WANG Q, PENG X. Asymmetric cryptosystem based on phase-truncated Fourier transforms[J].Optics Letters,2010,35(2): 118-120.

本刊中的类似文章

1．黄妙娜 黄佐华 蔡文鑫 雷水玉.位相板的制作及其在相衬法实验中的应用 [J]. 激光技术, 2010,34(1): 81-81

2．邵珺 沈学举 周中亮 严世华.基于光学相关的运动目标跟踪识别技术研究 [J]. 激光技术, 2009,33(6): 630-630

3．邵珺 华文深 周中亮 高鸿启.神经网络和遗传算法在相关峰判读中的应用研究 [J]. 激光技术, 2009,33(4): 422-422

4．邓晓鹏.基于干涉的二值图像逻辑运算加密技术 [J]. 激光技术, 2010,34(3): 401-401

5．黄振芬 张启灿 候志凌.相位展开中基于调制度轮廓线的极点连接算法 [J]. 激光技术, 2009,33(5): 462-462

6．杨锋涛 王殿元 刘志强 吕晓旭.相位展开的六种算法比较 [J]. 激光技术, 2008,32(3): 323-323

7．王敏.柯林斯公式的近似计算及应用研究 [J]. 激光技术, 2007,31(3): 295-295

8．张斌.使用双波带板径向剪切干涉仪检测非球面透镜 [J]. 激光技术, 2007,31(1): 37-37

9．杨初平 翁嘉文 杨玲玲 张子邦.二维载频条纹傅立叶变换轮廓术 [J]. 激光技术, 2010,34(4): 0-0

10．张海花 李勇 张海燕 王江.采用虚拟标准平面标定相位测量轮廓术系统 [J]. 激光技术, 2010,34(5): 0-0