基于计算全息和随机相位编码的三维信息的加密与显示

孔德照[1,2] 沈学举[1] 赵 燕[2] 曹良才[2] 金国藩[2]

[1]石家庄军械工程学院电子与光学工程系, 河北 石家庄 050003

[2]清华大学精密仪器系, 精密测试技术及仪器国家重点实验室, 北京 100084

摘要 提出了一种基于计算全息和随机相位编码的三维信息的加密与显示方案,在计算全息三维显示系统中,将随机相位掩模放置到计算全息的频谱信息中,重现时放置相应随机相位的共轭,并将此作为解密的密钥,实现对计算全息图中三维物体的解密和显示。该方案光路结构简单,在实现对三维物体显示的同时保证了信息的安全性,提高了加密的效率和信息的容量,数值模拟验证了方案的可行性。

关键词 全息; 计算全息; 光学信息安全; 三维显示; 随机相位编码

中图分类号 O438 **文献标识码** A

doi: 10.3788/LOP52.100902

Encryption and Display of Three-Dimensional Information Based Computer Generated Hologram and Random Phase Encoding

Kong Dezhao[1,2] Shen Xueju[1] Zhao Yan[2] Cao Liangcai[2] Jin Guofan[2]

[1]*Department of Electronic and Optics, Shijiazhuang Mechanical Engineer College, Shijiazhuang, Hebei* 050003, *China*

[2]*Department of Precision Instrument, State Key Laboratory of Precision Measurement Technology and Instruments, Tsinghua University, Beijing* 100084, *China*

Abstract A scheme of three-dimensional (3D) object encryption and display based on computer generated hologram (CGH) and random phase is presented. In the scheme, according to the reconstruction system of three-dimensional objects, the random phase masks (RPMs) are embedded into spectral information of CGH, then the encrypted CGH (En-CGH) is obtained. When the En-CGH is decrypted, the conjugate random phases as the keys are placed in the right position, and the decryption and reconstruction of three-dimensional objects are realized. The system structure of this scheme is simple. The introduction of RPM improves the security of reconstruction system. The efficiency of the encryption and the capacity of information storage are both improved. The numerical simulation verifies the feasibility of the scheme.

Key words holography; computer generated hologram; optical information security; three-dimensional display; random phase encoding

OCIS codes 090.2870; 090.1760; 070.4560; 100.4998

1 引 言

近年来,光学信息安全已受到广泛的关注,基于光学信息处理的理念,基于双随机相位编码[1]、分数傅里叶变换[2]和联合相关变换[3-4]等,已广泛应用于图像加密、用户授权和数字水印等领域。同时,一些光学系统和光学技术也应用到信息安全领域,如全息技术[5]、偏振编码[6-7]、分数光学[8-9]等。另一方面,密码学的概念也被引入到光学信息安全领域,出现了新的加密方案,如非对称加密[10-12]等。文献[13-19]对基于双随机相位编码的方案进行了系统性的攻击和分析,如已知明文攻击方案[13-15]和选择明文攻击方案[16-19]等。上述工作大

收稿日期: 2015-01-14; **收到修改稿日期**: 2015-03-12; **网络出版日期**: 2015-09-15

基金项目: 国家973计划(2013CB328801)

作者简介: 孔德照(1989—),男,硕士研究生,主要从事光学信息安全方面的研究。E-mail: kongoptics@126.com

导师简介: 曹良才(1977—),男,博士,副研究员,主要从事全息及光学信息处理方面的研究。

E-mail: clc@tsinghua.edu.cn(通信联系人)

大促进了光学信息安全的发展。

目前常见的光学信息安全方案主要针对二维信息实现加解密，由于三维(3D)信息比二维信息拥有更大的容量和更丰富的内容，因而，三维信息的加解密三维信息能够提高信息的存储、传输、显示和加解密效率，拥有广阔的发展空间。此外，三维信息显示系统在数据可视化、遥感卫星、医疗成像设备和地质勘探等领域具有巨大的应用潜力[20-21]。因此，将三维信息的加密和显示相结合，不仅能够提高信息的容量来实现三维信息的显示，并且能够获得更高的安全性。

本文基于计算全息和随机相位编码实现了对三维信息的显示，并通过将随机相位编码到计算全息图的频谱中，来实现对三维信息的加密，可以提高显示信息的安全性。仅仅使用特定的密钥，才能够恢复获得原始三维信息，实现三维信息的加密和显示的有效结合，也拓展了光学信息安全领域的研究内容。

2 计算全息三维显示模型

基于计算全息的三维显示技术主要包含两个关键：1) 利用算法(本文是通过角谱算法)将原始的三维物体编码到计算全息图中；2) 利用实验系统，上载计算全息图，将原始的三维信息恢复重建，具体可参照文献[21]。其系统的结构如图1所示。将平行光束入射到反射式的相位型空间光调制器(SLM)，SLM加载预生成的三维信息全息图，计算光学重建三维图像的距离。然后，三维图像由傅里叶透镜 L_2 和 L_3 组成的4f系统进行放大，其中，f_2 和 f_3 分别是 L_2 和 L_3 的焦距，系统的横向和轴向放大倍数同为f_3/f_2。利用该计算全息显示系统，根据显示距离，三维信息可以得到相应的放大和重现，显示的场景能够反映出三维信息的景深和多样信息。

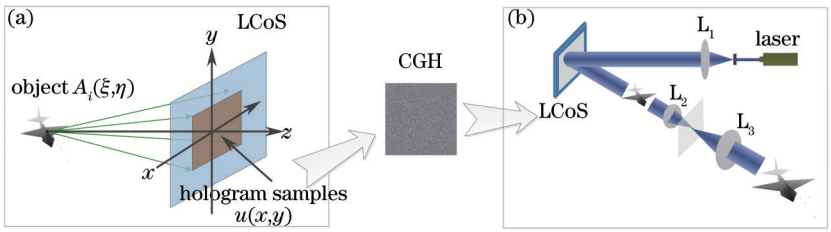

图1 基于计算全息的三维显示和重现基本原理图。

Fig.1 3D encryption and reconstruction based on CGH

3 三维信息加解密方案

基于计算全息三维信息重建的显示系统的加解密方案如图2所示。图2(a)表示加密过程，主要包括用于表达和传递三维信息的计算全息图的计算和产生过程。该过程通过计算机来实现：

1) 将随机相位掩模 $r_1(x,y)$ 置于放大显示的4f系统的频谱面上，完成对三维信息的随机调制，并得到相应的密钥Key1— $r_1^*(x,y)$ 和加密三维图像如下：

$$u(x,y)=\mathrm{FT}\left\{\mathrm{FT}\left[A_i(\xi,\eta)\right]\cdot r_1(x,y)\right\}, \tag{1}$$

式中 $A_i(\xi,\eta)$ 表示初始三维信息，FT (·)表示傅里叶变换；

2) 对于全息图而言，相位信息重要程度远大于振幅信息，提取 $u(x,y)$ 中的相位信息 $v(x,y)$，并进一步编码；

3) 运用角谱算法，通过第二块随机相位掩模 $r_2(x,y)$ 对相位信息 $v(x,y)$ 进行调制，获得密钥Key2— $r_2^*(x,y)$ 和最终加密的计算全息图 $h(x,y)$ 如下：

$$h(x,y)=v(x,y)\cdot r_2(x,y). \tag{2}$$

如图2(b)所示，解密过程也是三维信息的重建过程，将密钥放置到其相应的位置，就能够实现三维信息的重建实现解密，获得不同深度层次的三维信息，其过程如下：

1) 光路经扩束准直后，将Key1— $r_1^*(x,y)$ 置于重建光路中，可得相位 $v(x,y)$ 为

$$v(x,y)=h(x,y)\cdot r_2^*(x,y). \tag{3}$$

2) 将密钥Key1— $r_1^*(x,y)$ 放置于4f系统的频谱面上，经过两次傅里叶变换，便可重建出初始的三维信息 $A_i(\xi,\eta)'$ 为

$$A_i(\xi,\eta)'=\mathrm{FT}^{-1}\left\{\mathrm{FT}^{-1}\left[u(x,y)\right]\cdot r_1^*(x,y)\right\}. \tag{4}$$

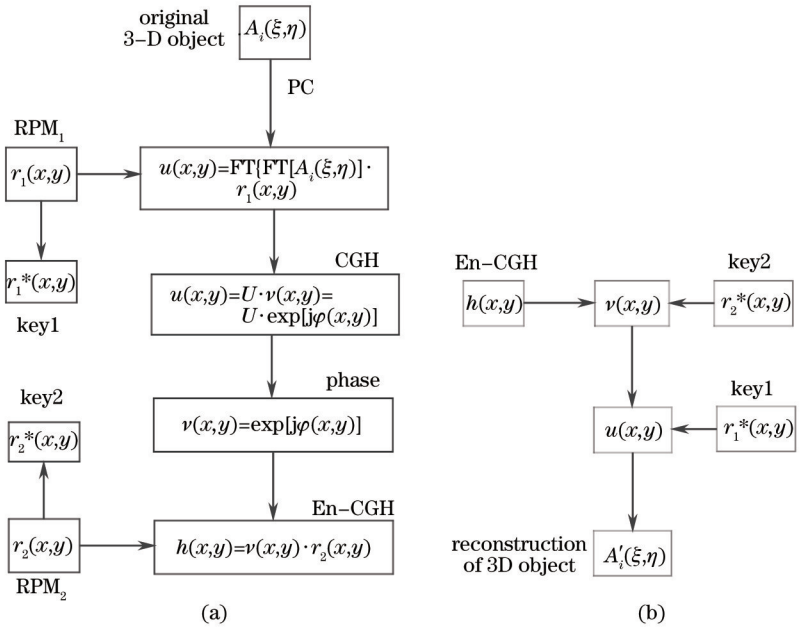

图2 三维信息加密和重现方案流程图。(a) 加密过程; (b) 重建过程

Fig.2 Encryption and reconstruction of 3D object. (a) Encryption; (b) decryption

一种典型的三维显示和解密的实现结构如图3所示，其中RPM$_1$和RPM$_2$表示随机相位掩模，L$_1$、L$_2$和L$_3$表示透镜，LCoS表示相位型空间光调制器。在该系统中，由于随机相位掩模具有很大的密钥空间，能够很好地保护三维信息，此外，对三维信息观察的位置选取对于显示效果有较大影响，若没有在焦距附近位置观察，获得的三维信息也将是模糊的，从另一方面保护了信息的安全。

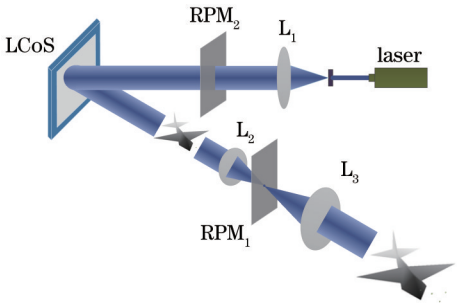

图3 一种典型的三维显示和加密的实现结构

Fig.3 A typical setup of 3D decryption and reconstruction

4 数值模拟和讨论分析

本文应用数值模拟的方法验证加密和重建方案的可行性和安全性。原始物体“飞机”大小13 mm×9 mm×15 mm，如图4(a)所示，激光的波长为633 nm，在4f系统中，两个透镜的焦距分别为100 mm和200 mm焦距。根据结构设计，将用于加密的随机相位掩膜编码到三维信息的计算全息图中，作为加密图像，如图4(b)；解密时，若不加密钥，显示的图像无法获得原始的三维信息，如图4(c)；在三维信息显示系统相应位置放置正确的密钥，可在不同距离得到不同深度的信息，成功显示了三维信息，解密和显示的图像在不同距离显示为图4(d)~(f)。另一幅三维对象“ABC”如图5(a)，其成功解密后在不同距离的显示图像如图5(b)~(d)，更直观地反映了方案加密显示的有效性。

在该加密方案中，加密计算全息图的应用提高了三维信息重现的灵活性和简易性，两块随机相位掩模可以提供足够的密钥空间，为重现三维信息限制了苛刻的条件，提供了充分的安全性。因此，本方案可以有效实现三维信息的加密和显示，能够为三维信息提供必要的加密，保证了其安全性。

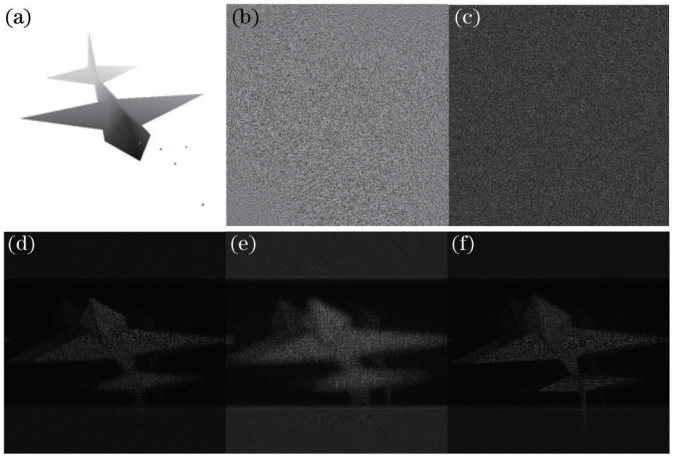

图4 “飞机”图像的加密。(a) 原始三维物体; (b) 加密的计算全息图; (c) 没有密钥解密得到的信息; (d) 正确解密时在190 mm处重建的图像; (e) 正确解密时在200 mm处重建的图像; (e) 正确解密时在210 mm处重建的图像

Fig.4 Encryption of‘jet’. (a) Original 3D object jet; (b) encrypted CGH; (b) decrypted image without keys; (d) decrypted image at 190 mm; (e) decrypted image at 200 mm; (f) decrypted image at 210 mm

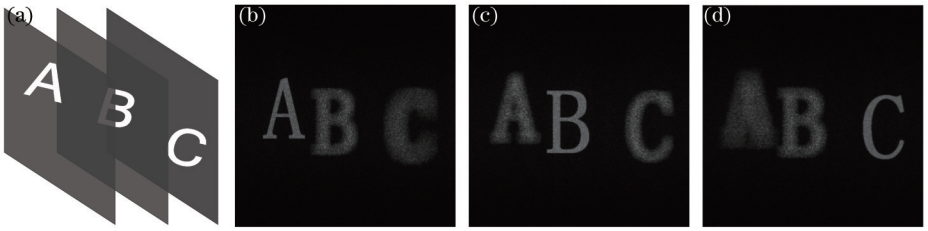

图5 三维图像“ABC”的加密。 (a) 三维图像“ABC”; (b) 解密和重建图像“A”; (c) 解密和重建图像“B”; (d) 解密和重建图像“C”

Fig.5 Encryption of ‘ABC’; (a) Original 3D object ‘ABC’; (b) decrypted image ‘A’; (c) decrypted image ‘B’; (d) decrypted image ‘C’

5 结 论

本文基于计算全息三维显示和随机相位编码,提出了一种基于计算全息和随机相位的三维信息的加密与显示方案,具体是利用角谱算法将随机相位编码到计算全息图频谱信息中,实现了对三维信息的加密,并通过密钥和三维显示系统实现了对三维信息的重建。数值模拟验证了该方案的可行性,随机相位掩模的加入使其具有很高的安全性。方案实现光路简单,重建的图像形象生动,具有一定的景深,不仅提高了三维信息加密的容量和效率,也提高了三维信息传输过程中的安全性,二者有效地结合,拓展了光学信息安全领域的研究方向,对于大数据量信息的存储、传输、加密、显示具有重要的发展潜力。

参 考 文 献

1 Réfrégier P, Javidi B. Optical image encryption based on input plane and Fourier plane random encoding[J]. Opt Lett, 1995, 20(70): 767-769.

2 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.

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

4 T Nomura, B Javidi. Optical encryption using a joint transform correlator architecture[J]. Opt Eng, 2000, 39(8): 2031-2035.

5 B Javidi, T Nomura. Securing information by use of digital holography[J]. Opt Lett, 2000, 25(1): 28-30.

6 Zhu N, Wang Y T, Liu J, *et al.*. Optical image encryption based on interference of polarized light[J]. Opt Express, 2009, 17(16): 13418-13424.

7 A Alfalou, C Brosseau. Dual encryption scheme of images using polarized light [J]. Opt Lett, 2010, 35(13): 2185-2187.

8 Chen L F, Zhao D M. Optical image encryption based on fractional wavelet transform[J]. Opt Commun, 2005, 254(4-6): 361-367.

9 Zhou N R, Wang Y X, Gong L H. Novel optical image encryption scheme based on fractional Mellin transform[J]. Opt Commun, 2011, 284(13): 3234-3242.

10 Wang X G, Zhao D M. Multiple-image encryption based on nonlinear amplitude- truncation and phase-truncation in fourier domain[J]. Opt Commun, 2011, 284(1): 148-152.

11 Liu W, Liu Z J, Liu S T. Asymmetric cryptosystem using random binary phase modulation based on mixture retrieval type of Yang-Gu algorithm[J]. Opt Lett, 2013, 38(10): 1651-1653.

12 Chen B, Wang H. Optically-induced-potential-based image encryption[J]. Opt Express, 2011, 19(23): 22619-22627.

13 Carnicer A, Usategui M M, Vulnerability to chosen-cyphertext attacks of optical encryption schemes based on double random phase keys[J]. Opt Lett, 2005, 30(13): 1644-1646.

14 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.

15 Peng X, Wei H, Zhang P, Chosen-plaintext attack on lensless double-random phase encoding in the Fresnel domain[J]. Opt Lett, 2006, 31(22): 3261-3263.

16 Peng X, Zhang P, Wei H, *et al*.. Know-plaintext attack on optical encryption based on keys[J]. Opt Lett, 2006, 31(8): 1044-1046.

17 Qin W, Peng X. Vulnerability to known-plaintext attack on optical encryption schemes based on two fractional Fourier transform order keys and double-random phase keys[J]. J Opt A: Pure Appl, 2009, 11(7): 075402.

18 Wei Hengzheng, Peng Xiang. Known-plaintext attack on optical cryptosystem based on projection-onto-constraint-sets algorithm and a 4*f* correlator[J]. Acta Optica Sinica, 2008, 28(3): 429-434.
位恒政, 彭 翔. 约束集投影算法和4*f*相关器的光学密码系统的已知明文攻击[J]. 光学学报, 2008, 28(3): 429-434.

19 Guohai Situ, Giancarlo Pedrini, Wolfgang Osten. Strategy for cryptanalysis of optical encryption in the Fresnel domain [J]. Appl Opt, 2010, 49(3): 457-462.

20 P A Blanche, A Bablumian, R Voorakaranam, *et al*.. Holographic three-dimensional telepresence using large-area photorefractive polymer[J]. Nature, 2010, 468 (7320): 80-83.

21 Hao Zhang, Qiaofeng Tan, Guofan Jin. Holographic display system of a three- dimensional image with distortion-free magnification and zero-order elimination[J]. Opt Eng, 2012, 51(7): 075801.

栏目编辑: 何卓铭