基于位相抽取的三维信息加密算法研究*

史祎诗[1)†] 王雅丽[1)] 肖 俊[1)] 杨玉花[2)] 张静娟[1)]

1)(中国科学院研究生院,北京 100049)

2)(北京工业大学应用数理学院,北京 100124)

(2010 年 5 月 5 日收到;2010 年 5 月 27 日收到修改稿)

本文提出了以位相抽取为基础的三维信息加密算法. 构造由纯振幅和纯位相物体组成的简单三维信息作为加密对象. 先用标量衍射理论计算其复振幅并抽取相位分布,再结合双随机位相编码完成加密. 解密算法为上述算法的逆过程. 计算机模拟结果证实了该算法的有效性、鲁棒性和安全性,并揭示了位相抽取算法用于加密更大信息量三维信息的潜力.

关键词: 傅里叶光学, 光学信息安全, 三维信息加密, 位相抽取

PACS: 42.30.-d

1. 引 言

光学信息安全是光信息处理领域中一个较活跃的方向[1—4]. 近年来,加密技术不仅针对二维图像,也逐渐将三维信息纳为加密对象. 三维信息加密现有的典型技术方式是数字全息术与双随机位相编码的结合[5—10]. 前者可以方便地记录三维信息,后者则确保了信息加密的实现. 但是,受到数字全息记录器件(如 CCD)的尺寸限制,只能加密总体尺寸较小的三维信息,且有效分辨率也受到一定影响;此外,无法实施计算机生成的虚拟三维信息与数据的加密. 这些都较严重地限制了基于数字全息术的三维信息安全系统的实际应用. 为此,本文提出了基于相位抽取的三维信息加密算法. 由于作为本法核心的三维信息位相编码过程在计算机内即可完成,因而可一定程度解决上述问题.

2. 算法描述

本文提出的算法由两部分组成. 第一部分是基于相位抽取的三维信息编码. 这一部分是核心,其物理模型如图 1 所示. 我们在计算机中构建如图的简化三维信息作为秘密信息,即位于一定纵深内的三个垂直平面上的复振幅分布. 该三维信息可用一个三维函数 CAS (x, y, z) 表示,也可以表示为一个二维函数集合的形式 $\{C(x_1, y_1), A(x_2, y_2), S(x_3, y_3)\}$. 第一部分算法的主要目的就是将三维信息编码为二维的复振幅信息,并抽取出其位相分布函数. 具体做法如下:模拟平面波垂直入射,并依次受到三维信息复振幅调制而到达输出平面 $SLM(x_i, y_i)$ 的衍射过程,再抽取 SLM (x_i, y_i) 的位相部分. 若将波长为 λ、衍射距离为 z 的 Fresnel 衍射用 $FrT_{\lambda, z}\{\cdot\}$ 来表示,并且设 $Q(x_i, y_i)$ 为抽取出的位相函数,则上述编码过程可简写为

$$SLM(x_i, y_i) = FrT_{\lambda, z_3}\{FrT_{\lambda, z_2}\{FrT_{\lambda, z_1}\{C(x_1, y_1)\} \times A(x_2, y_2)\} \cdot S(x_3, y_3)\}, \quad (1)$$

$$Q(x_i, y_i) = SLM(x_i, y_i)/|SLM(x_i, y_i)|. \quad (2)$$

第二部分为 Fresnel 域内的双随机位相加密. 在光学系统实现中,可以将抽取出的位相 $Q(x_i, y_i)$ 加载到空间光调制器(SLM)上,并用双随机位相加密系统实施加密[1]. 通常而言,系统中的第一个随机位相板 RPM_1 紧贴于待加密的二维信息. 但由于使用了 SLM,因而就允许直接将 RPM_1 的随机位相分布与 $Q(x_i, y_i)$ 叠加,于是只需 RPM_2 即可达到同样目的. 设 RPM_1 和 RPM_2 的位相函数分别为 $R_1(x_i, y_i)$, $R_2(x_m, y_m)$,且密文为复振幅分布 $R_o(x_o, y_o)$. 为记录复振幅 $R_o(x_o, y_o)$,可引入一束参考光干涉

* 国家自然科学基金(批准号:60907004),中国博士后科学基金,中国科学院研究生院院长基金及香港王宽诚教育基金会资助的课题.

† E-mail: sysopt@126.com

得到强度分布. 如不考虑参考光,且 Fresnel 域内 SLM 到 RPM_2 和输出平面的衍射距离为分别为 z_{I}, z_{II},则第二部分算法可表示如下:

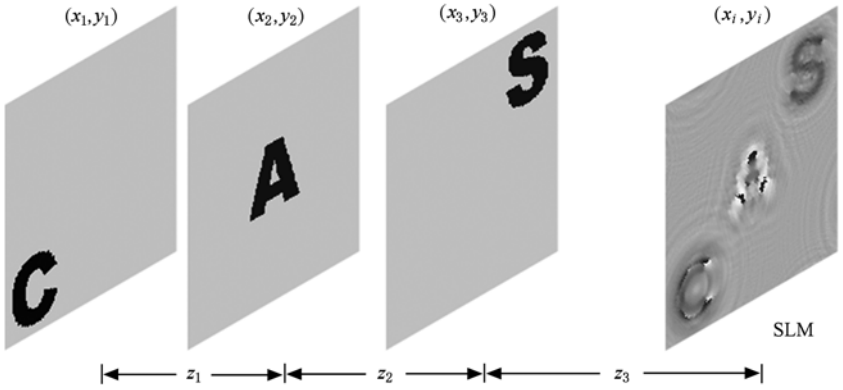

图 1 基于位相抽取的三维信息编码示意图

$$\begin{aligned} R_o(x_o, y_o) = \mathrm{FrT}_{\lambda, z_{\mathrm{II}}}\{ \mathrm{FrT}_{\lambda, z_{\mathrm{I}}}\{ \exp[\mathrm{j}Q(x_i, y_i)] \\ \times \exp[\mathrm{j}\, R_1(x_i, y_i)]\} \\ \times \exp[\mathrm{j}\, R_2(x_m, y_m)]\}. \end{aligned} \quad (3)$$

下面简述解密算法. 解密过程是上述两部分算法的逆过程. 若用 $\mathrm{IFrT}_{\lambda, z}\{\cdot\}$ 表示逆 Fresnel 变换,则可先得到 $\mathrm{DeSLM}(x_i, y_i)$ 如下:

$$\begin{aligned} \mathrm{DeSLM}(x_i, y_i) = \mathrm{IFrT}_{\lambda, z_{\mathrm{I}}}\{ \mathrm{IFrT}_{\lambda, z_{\mathrm{II}}} \\ \times \{ \exp[\mathrm{j}\, R_o(x_o, y_o)] \\ \times \exp[-\mathrm{j}R_2(x_m, y_m)]\} \\ \times \exp[-\mathrm{j}R_1(x_i, y_i)]\}. \end{aligned} \quad (4)$$

再经过一系列的逆 Fresnel 变换,就可以得到解密出的三维信息 $\mathrm{DeCAS}(x, y, z)$,又即解密出的二维函数集合 $\{\mathrm{DeC}(x_1, y_1), \mathrm{DeA}(x_2, y_2), \mathrm{DeS}(x_3, y_3)\}$:

$$\mathrm{DeC}(x_1, y_1) = \mathrm{IFrT}_{\lambda, z_1}\{ \mathrm{DeSLM}(x_i, y_i)\}, \quad (5)$$

$$DeA(x_2, y_2) = \mathrm{IFrT}_{\lambda, z_2}\{ \mathrm{DeSLM}(x_i, y_i)\}, \quad (6)$$

$$DeS(x_3, y_3) = \mathrm{IFrT}_{\lambda, z_3}\{ \mathrm{DeSLM}(x_i, y_i)\}. \quad (7)$$

可用相关系数值 Co 来评价解密二维函数集合的质量[11],从而判定三维信息的整体解密质量.

$$\mathrm{Co}(g, g_o) = \mathrm{cov}(g, g_o)(\sigma_t \cdot \sigma_{t_o})^{-1}, \quad (8)$$

其中 $\mathrm{cov}(g, g_o)$ 表示解密信息 g 和原始秘密信息 g_o 之间的互协方差,σ 为标准偏差. Co 取值范围为 [0,1],其越接近 1 表明解密信息的质量越高. 需注意的是,运用 Co 判定复振幅分布时,须分别对比两者的实部与虚部,或者振幅与位相.

本算法与系统的密钥为位相密钥和附加密钥组成. 位相密钥就是第二部分算法中双随机位相板 RPM_1 和 RPM_2 的位相分布函数,附加密钥则包括波长 λ 和衍射距离 $\{z_{\mathrm{I}}, z_{\mathrm{II}}\}$. 它们共同确保了系统的安全性.

3. 计算模拟与分析

3.1. 基本结果

我们在计算机模拟中所采用的加密对象就是图 1 中所示的三维信息“CAS”. 为简单起见而又不失一般性,我们将三维信息 $\{\mathrm{C}(x_1, y_1), \mathrm{A}(x_2, y_2), \mathrm{S}(x_3, y_3)\}$ 中的 $\mathrm{A}(x_2, y_2)$ 取为纯振幅函数,其余两者取为纯位相函数,且除去字母覆盖区域复振幅皆为零,如图 2 所示. 其中 $\mathrm{A}(x_2, y_2)$ 为灰度化表示

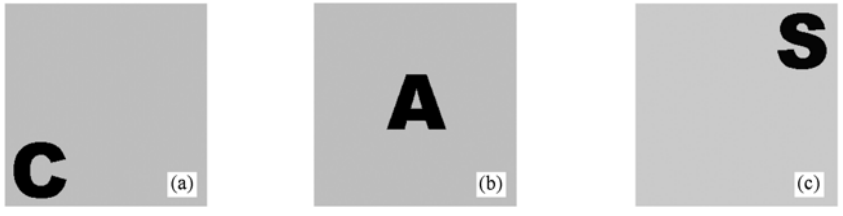

图 2 三维信息 (a) $\mathrm{C}(x_1, y_1)$;(b) $\mathrm{A}(x_2, y_2)$;(c) $\mathrm{S}(x_3, y_3)$

(下文凡涉及纯位相分布函数的图像形式也同样表示). 模拟中的波长取为 632.8 nm,有效采样点数为 256 pixels × 256 pixels,像素大小为 8 μm,衍射距离 $\{z_1, z_2, z_3\}$ 分别取为 {20, 30, 20} mm.

经过基于位相抽取的三维信息编码后, SLM 平面上的振幅与位相函数分布 $|\mathrm{SLM}(x_i, y_i)|$, $Q(x_i, y_i)$ 分别如图 3(a) 和 (b) 所示. 抽取 SLM 平面的位相分布函数 $Q(x_i, y_i)$ 由双随机位相加密,所得到密文 $R_o(x_o, y_o)$ 的振幅和位相分别如图 3(c) 和 (d) 所示. 其中,衍射距离 $\{z_\mathrm{I}, z_\mathrm{II}\}$ 取为 {30, 40} mm.

以下为解密过程. 当位相密钥和附加密钥的取值正确时,按照前述解密算法首先得到解密的二维分布 $\mathrm{DeSLM}(x_i, y_i)$,其振幅和位相分布分别如图 4 (a) 和 (b) 所示. 图 4(b) 与图 3(a) 对应的 Co 值等于 1,即解密出的二维位相分布 $|\mathrm{DeSLM}(x_i, y_i)|$ 与原始位相分布 $|\mathrm{SLM}(x_i, y_i)|$ 相同.

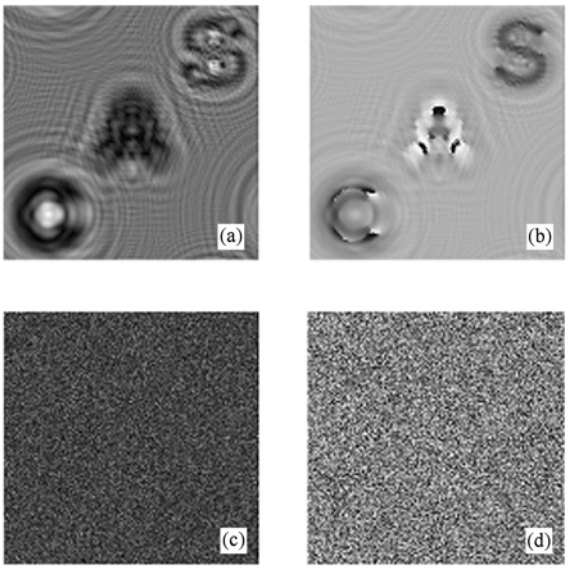

图 3 (a) $|\mathrm{SLM}(x_i, y_i)|$; (b) $Q(x_i, y_i)$; (c) $|R_o(x_o, y_o)|$; (d) $R_o(x_o, y_o)/|R_o(x_o, y_o)|$

将位相分布函数 $|\mathrm{DeSLM}(x_i, y_i)|$ 依相应的衍射距离进行逆 Fresnel 变换,可最终解密出三维信息 $\mathrm{DeCAS}(x, y, z)$,即 $\{\mathrm{DeC}(x_1, y_1), \mathrm{DeA}(x_2, y_2), \mathrm{DeS}(x_3, y_3)\}$,如图 5(a)—(c) 所示. 运用数字图像处理中的形态学方法可方便地将相应的信息增强并提取出来,使相应的振幅或位相分布清晰可见. 至此,计算机模拟结果证明了基于位相抽取的三维信息加密算法的有效性.

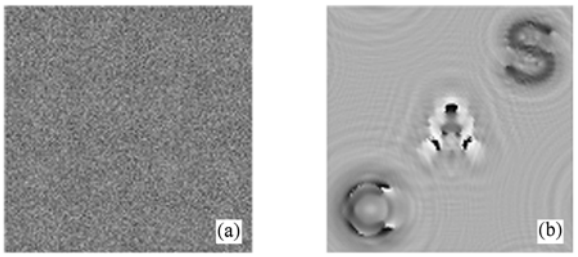

图 4 (a) $|\mathrm{DeSLM}(x_i, y_i)|$; (b) $\mathrm{DeSLM}(x_i, y_i)/|\mathrm{DeSLM}(x_i, y_i)|$

3.2. 算法分析

作为面向数据加密应用的算法,通常最为关心的是其鲁棒性和安全性. 以下将从本算法与系统的特点出发,着重分析其在对抗各类噪声、SLM 的台阶量化以及算法密钥失真时所表现出的性质,并对其应对光学密码攻击的安全性作了初步分析.

首先分析算法对抗各类噪声的鲁棒性. 我们模拟了高斯噪声、椒盐噪声、泊松噪声等对算法的影响. 其中,因算法对高斯噪声的效果相对最差,所以我们给出了将均值为 0,方差为 0.01 高斯噪声分别加到密文 $R_o(x_o, y_o)$ 的振幅和相位上时的解密结果,分别如图 6 (a)—(c) 和 图 6 (d)—(f) 所示. 将受噪声影响和无噪声情况下解密的结果对比求 Co 值发现,当高斯噪声分别加到振幅、位相上时,三者的平均 Co 值分别为 0.7340 和 0.4420. 同时从图 6 的直观结果中综合可知,本算法对抗各类噪声的效果均较好.

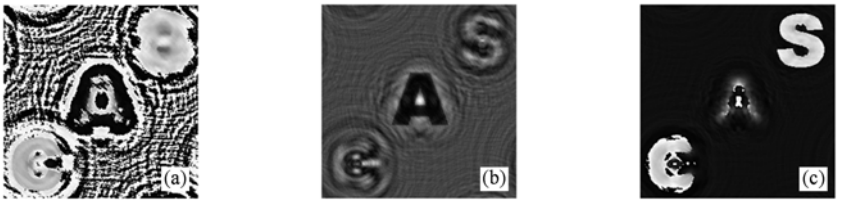

图 5 解密出的三维信息 (a) $\mathrm{DeC}(x_1, y_1)$; (b) $\mathrm{DeA}(x_2, y_2)$; (c) $\mathrm{DeS}(x_3, y_3)$

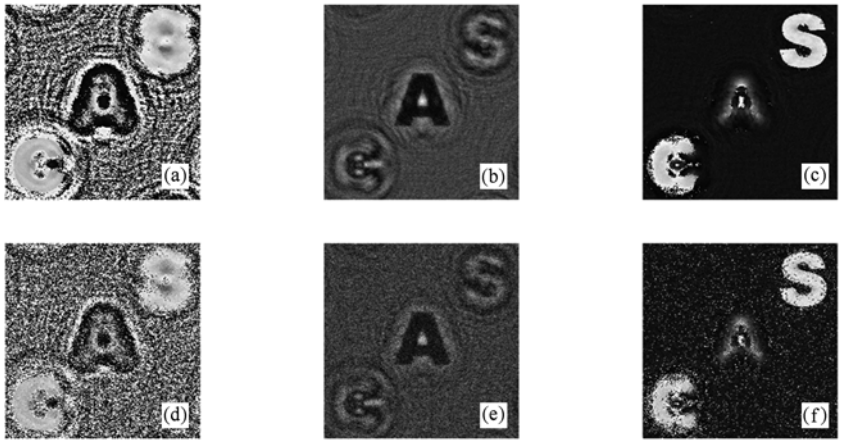

图 6 高斯噪声加到 $R_o(x_o, y_o)$ 振幅上时所解密出的三维信息:(a) DeC(x_1, y_1);(b) DeA(x_2, y_2);(c) DeS(x_3, y_3). 高斯噪声加到其位相上时的解密信息:(d) DeC(x_1, y_1);(e) DeA(x_2, y_2);(f) DeS(x_3, y_3)

其次,分析 SLM 的台阶量化对算法的影响. 由于现有 SLM 工艺还无法实现连续的位相变化,因而我们模拟了实际系统在 SLM 分别取 128,64,32,16 量化台阶条件下所受到的影响. 研究发现,采用位相抽取的方式对简单三维信息条件下的编码较为成功. 甚至于在 16 台阶量化的情况下,仍然能够得到较高保真度的解密三维信息,平均 Co 值仍可达 0.6759,结果如图 7 所示. 其根本原因在于位相保留了三维信息的大部. 由于较低的相位量化台阶数尚可保留较大量的三维信息,因此这一结果启示我们,有可能进一步充分挖掘位相抽取方法的潜力,以适应三维信息的信息量与复杂度增加的客观要求.

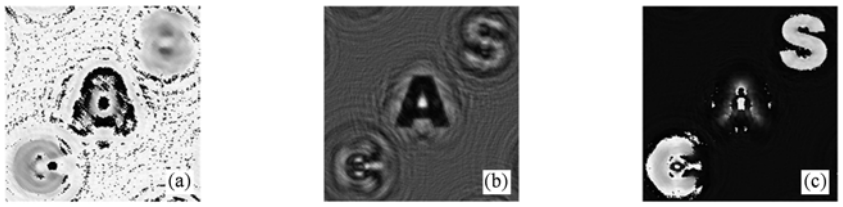

图 7 SLM 量化为 16 台阶时解密出的三维信息 (a) DeC(x_1, y_1);(b) DeA(x_2, y_2);(c) DeS(x_3, y_3)

同时,我们从密钥失真研究了算法与系统的安全性. 图 8 显示了将附加密钥中的衍射距离 $\{z_{\mathrm{I}}, z_{\mathrm{II}}\}$ 改变 0.02,0.03,0.04 mm(≤1%)时分别解密出的三维信息中 DeC(x_1, y_1)的灰度化分布. 发现不仅其解密质量十分差,且无法运用适合的图像增强方法提取有用信息. 此外,用错误的波长密钥或随机位相密钥,也都将导致解密失败. 限于篇幅,相应结果不再给出. 由于在双随机位相加密之前就采取了位相抽取,而鉴于位相的敏感性比振幅更高,因此本算法进一步发扬了双随机位相加密的安全

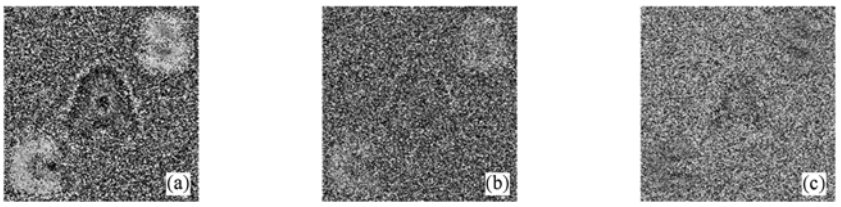

图 8 附加密钥 $\{z_{\mathrm{I}}, z_{\mathrm{II}}\}$ 失真分为 (a) 0.02 mm,(b) 0.03 mm 和(c) 0.04 mm 时解密出的 DeC(x_1, y_1)

性优势.

鉴于本算法仍属光学对称密码算法的范畴,我们还初步分析了其对光学密码攻击的安全性. 密码学分析方法包括选择密文攻击[12]、唯密文攻击[13]、已知明文攻击[14]和选择明文攻击[15]等几类典型方法[16]. 值得注意,本算法的特殊性在于,虽然原始明文为三维信息,但后续双随机位相编码的对象却是其相应的二维位相分布. 于是,只能适用于明文为纯振幅而非复振幅的选择密文攻击和唯密文攻击这两类分析方法将失效. 另一方面,尽管选择明文攻击甚至是无损的[13],但该法需要选择多个冲击函数作为明文,而这在实际中较容易从系统设计的角度预先加以防止[12].

因此,综合考虑实际应用中攻击的合理性与实现难度,需重点研究本算法对于已知明文攻击这类分析方法的安全性. 该方法的基本思想是主要运用相位恢复算法,由一个明密文对依次恢复出两个随机位相密钥[14, 16]. 针对本算法加密过程采用 Fresnel 双随机位相编码的特点,我们假定波长等附加密钥已知,以降低攻击难度. 若已知的就是上述 3.1 节中的明文位相分布函数 $Q(x_i, y_i)$ 及其密文 $R_o(x_o, y_o)$,则经过混合输入输出法的 1500 次迭代后可依次解出的双随机位相密钥. 图 9 给出了用攻击所得密钥与相应密文所解得的三维信息,其有用信息已经受到噪声的严重影响. 更甚之,如果我们用其它的明密文对攻击得到的双随机位相密钥来进行解密则只能得到如图 8(b)和(c)一类的噪声分布. 其主要原因如下:本算法加密的实际对象是三维信息转化而来的二维位相分布,而已知明文攻击对位相形式密文的部分局限性以及其在恢复成三维信息过程中误差的进一步扩大,导致了该法攻击本算法的有效性整体下降. 至此,理论分析与模拟结果初步说明了本算法对抗已知明文攻击等密码分析方法的安全性.

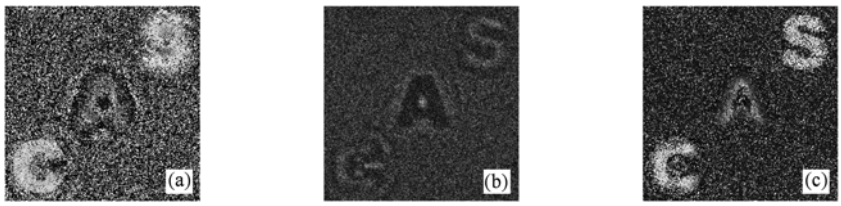

图 9 用已知明文攻击思想攻击解密出的三维信息 (a) $DeC(x_1, y_1)$;(b) $DeA(x_2, y_2)$;(c) $DeS(x_3, y_3)$

4. 结 论

本文提出并模拟证实了基于位相抽取的三维信息加密算法的有效性、鲁棒性和安全性. 该算法可快速加密虚拟的三维信息,也可用于光电联合的三维信息加密系统. 此外,模拟结果还显示了该加密算法在承载更大信息量三维信息的应用潜力.

[1] Réfrégier P, Javidi B 1995 *Opt. Lett.* **20** 767
[2] Zhang J J, Shi Y S, Situ G H 2006 *Journal of the Graduate School of the Chinese Academy of Sciences* **23** 289 (in Chinese). [张静娟、史祎诗、司徒国海 2006 中国科学院研究生院学报 **23** 289]
[3] Yang X P, Gao L J, Wang X L, Zhai H C, Wang M W 2009 *Acta Phys. Sin.* **58** 1662 (in Chinese) [杨晓苹、高丽娟、王晓雷、翟宏琛、王明伟 2009 物理学报 **58** 1662]
[4] Peng X, Zhang P, Wei H Z, Yu B 2006 *Acta Phys. Sin.* **55** 1130(in Chinese) [彭 翔、张 鹏、位恒政、于 斌 2006 物理学报 **55** 1130]
[5] Tajahuerce E, Javidi B 2000 *Appl. Opt.* **39** 6595
[6] Kishk S, Javidi B 2003 *Opt. Lett.* **28** 167
[7] Kishk S, Javidi B 2003 *Opt. Exp.* **11** 874
[8] Fan Z B, Li J C 2010 *Chin. Phys.* B **19** 2457
[9] Wang M W, Yang X P, Zhai H C 2008 *Acta Phys. Sin.* **57** 847 (in Chinese) [王明伟、杨晓苹、翟宏琛 2008 物理学报 **57** 847]
[10] Niu C H, Zhang Y, Gu B Y 2005 *Chin. Phys.* **14** 1996
[11] Shi Y S, Situ G H, Zhang J J 2008 *Opt. Lett.* **33** 542
[12] Carnicer A, Montes-Usategui M, Arcos S, Juvells I 2005 *Opt. Lett.* **30** 1644
[13] Peng X, Tang H Q, Tian J D 2007 *Acta Phys. Sin.* **56** 2629(in Chinese) [彭 翔、汤红乔、田劲东 2007 物理学报 **56** 2629]
[14] Peng X, Zhang P, Wei H Z, Yu B 2006 *Opt. Lett.* **31** 1044
[15] Peng X, Wei H Z, Zhang P 2006 *Opt. Lett.* **31** 3261
[16] Peng X, Wei H Z, Zhang P 2007 *Acta Phys. Sin.* **56** 3924 (in Chinese) [彭 翔、位恒政、张 鹏 2007 物理学报 **56** 3924]

Research on the algorithm of three-dimensional information encryption based on the phase extraction*

Shi Yi-Shi[1)†] Wang Ya-Li[1)] Xiao Jun[1)] Yang Yu-Hua[2)] Zhang Jing-Juan[1)]

1) (*Graduate University of the Chinese Academy of Sciences, Beijing* 100049, *China*)

2) (*College of Applied Science, Beijing University of Technology, Beijing* 100124, *China*)

(Received 5 May 2010; revised manuscript received 27 May 2010)

Abstract

The algorithm for three-dimensional information encryption based on the phase extraction is proposed. The three-dimensional information with the pure amplitude and pure phase are constructed as the encryption target. First, the complex amplitude of the three-dimensional information is calculated under the scalar diffraction theory. Then its phase distribution is extracted independently and it is encrypted with the double random phase encoding. The decryption algorithm is just the inverse process as the above. Computer simulations demonstrate the feasibility, the robustness and the security of the algorithm. Further, it is revealed the potential of applying the algorithm for the three-dimensional information encryption with much larger information quantity.

Keywords: Fourier optics, optical encryption, three-dimensional information encryption, phase extraction

PACS: 42.30.-d

* Project supported by the National Natural Science Foundation of China (Grand No. 60907004), China Postdoctoral Science Foundation, the President Fund of GUCAS and K. C. Wong Education Foundation, Hong Kong.

† E-mail: sysopt@126.com