一种无轮廓像干扰光学加密系统

秦 怡 巩 琼 李根全 杨兴强
(南阳师范学院物理与电子工程学院, 河南 南阳 473061)

摘要 将光学中的干涉与衍射原理相结合,提出了一种新的光学加密系统。该光学加密系统将图像信息隐藏于两个相位板(POM)及一个振幅板(AOM)中,其中振幅板使用计算机随机生成,两个相位板则通过解析方法得到。解密时,使用相干光照射两个相位板,并通过分束镜使二者的衍射光场进行相干叠加,此干涉场被振幅板调制,再经衍射一段距离后所得衍射场强度即为原始图像,此图像可以采用 CCD 等图像传感器件直接记录。本方法不但消除了先前提出的基于干涉原理加密方法存在的"轮廓像"问题,也对部分密钥泄露攻击具有很强的稳健性,具有较高的安全性。此外,本方法原理简单,加密过程无需迭代,解密系统易于物理实现。计算机模拟结果证实了本方法的有效性。

关键词 图像处理;光学加密;干涉及衍射原理;轮廓像问题;暴力攻击
中图分类号 TP751 **文献标识码** A **doi**: 10.3788/CJL201239.1209002

An Optical Encryption Method with Silhouette Removal

Qin Yi Gong Qiong Li Genquan Yang Xingqiang
(*College of Physics and Electronic Engineering, Nanyang Normal University, Nanyang, Henan* 473061, *China*)

Abstract A novel optical encryption system is proposed by combining the optical principle of interference and diffraction. In this system, the original image is hidden into three masks, including two phase only masks (POMs) and one amplitude only mask (AOM). The AOM is randomly generated by computer while the POMs are obtained analytically. For decryption, the diffraction field of the two POMs is first superposed by utilizing the beam splitters and then modulated by the amplitude mask. After that the wavefront propagates for a certain distance and the intensity of the complex field, which is exactly the original image, can be recorded by CCD camera. Compared with the existing interference-based method, the approach is simple and easy to be realized by optical elements. Moreover, the silhouette problem that exists in the method with two POMs can be solved in our method. At the same time, the proposal is also proved to be robust to partial key exposure attack. Simulation results are presented to verify the validity of the proposed approach.

Key words image processing; optical encryption; principle of interference and diffraction; silhouette problem; brute force attack
OCIS codes 070.4560; 070.1170; 090.2880

1 引 言

因为光学信号内在的高速并行处理能力,光学信息处理已经成为信号处理领域内一个重要的研究方向,其中光学信息安全在近 20 年内迅速崛起,成为信息安全领域内的研究热点[1~12]。该领域内的开拓性成果是由 Philippe 等[13]于 1995 年提出的双随机相位编码系统(DRPE)。该系统在光学 4f 系统的输入平面及傅里叶平面各放置一个随机相位板(POM),从而可将一幅图像加密成复平稳白噪声。随后,该系统又被推广至菲涅耳域与分数傅里叶域,其安全性得到进一步提高[14,15]。事实上,DRPE 系统除了安全性不高之外,由于其加密结果为复数场,传输起来也非常不便,尤其是解密系统难以使用光学方法实现[16,17],因为现有的空间光调制器不能对

收稿日期: 2012-07-26; **收到修改稿日期**: 2012-09-03
基金项目: 河南省科技厅科技攻关项目(112102210386)和南阳师范学院高层次人才启动资金项目(nytc2006k100)资助课题。
作者简介: 秦 怡(1981—),男,硕士,讲师,主要从事光电信息处理方面的研究。E-mail: 641858757@qq.com

光波的相位和振幅同时进行调制。尽管先前提出的一些方法可以将原始图像加密成两个或者更多个相位板，但是这些方法都是采用迭代算法，比较耗时[11,18]。相比之下，Zhang 等[19]提出了一种基于干涉原理的图像加密方法（以下称为 Zhang 方法），将复数干涉场解析地隐藏到两个纯随机相位板中，整个加密过程无需迭代，并且原理非常简单。尽管如此，该加密系统存在一个安全瑕疵，即单独使用其中任一个随机相位板，均可以得到原始图像的轮廓，而这个轮廓提供了原始图像的足够信息，即所谓的“轮廓像”问题。“轮廓像”问题产生的原因在于被加密图像的频谱与两个相位板之间的密切关联。为了解决“轮廓像”问题，Zhang 等[20]又进一步提出随机交换两个相位板的对应部分，但是这大大增加了计算量，他们也提出通过将相位板进一步分解来解决该问题，但是随机相位板的数量增加到 4 个或者更多。最近 Wang 等[21]将 Zhang 方法进一步广义化，将原始图像解析地隐藏于三个相位板中，消除了“轮廓像”问题。但是在解密过程中，为了实现乘法运算，该方法要求两个随机相位板前后紧贴，这在物理上非常难于实现。此外，由于系统中引入了透镜，使得解密系统结构更为复杂。本文在 Zhang 方法的基础上，在干涉光路中引入一随机振幅板（AOM），提出一种非常简单的方法来解决“轮廓像”问题，成功地将原始图像隐藏于三个掩模板中。与 Wang 等[22]提出的方法相比，本方法解密时无需随机相位板互相紧贴的苛刻要求，也省去了用作傅里叶变换计算的凸透镜，解密所用的光学系统更加紧凑。文中给出了理论分析及计算机模拟结果。

2　理论分析

在本文所提的加密系统中，加密过程使用计算机进行数字运算实现，而解密过程既可以使用数字方法，也可以使用光学方法来实现。为了说明本方法的加密原理，首先在图 1 中给出了用于实现解密算法的光学系统结构。随机相位板 P1，P2 被波长为 λ 的单色平面光波照射，均经过距离为 l 的菲涅耳衍射到达随机振幅板 A 所在平面。之后，此干涉场被 A 进一步调制后，再经过距离为 d 的衍射到达输出平面 H。使用图像传感器（如 CCD 等）即可记录解密后的图像。可以看出，该解密系统非常简单，其中所用到的光学元件仅有分束镜。和文献[21]所述方法相比，既不需要两个随机相位板前后紧贴，同时又省去了用于傅里叶变换运算的凸透镜，物理实现更为容易。

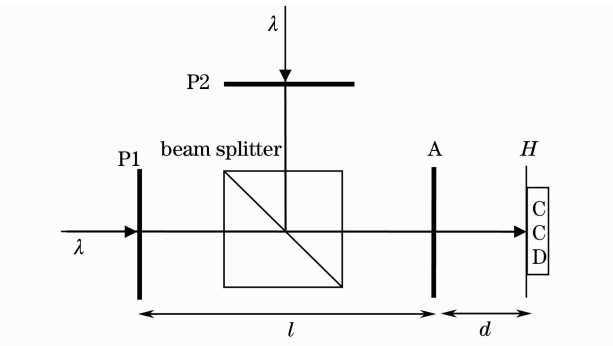

图 1　图像解密系统结构

Fig. 1　Schematic of the decryption setup

加密算法为上述解密过程的逆过程，即把原始图像信息隐藏于纯相位板 P1P2，以及振幅板 A 之中，其原理可描述如下。假设 $o(m,n)$ 为待加密的图像，首先给其分配一个随机的白噪声相位，得到一个新的函数

$$o'(m,n)=\sqrt{o(m,n)}\exp[\mathrm{i}2\pi\mathrm{rand}(m,n)],\quad(1)$$

式中 rand 函数产生位于(0,1)区间的随机数。根据图 1 所示的解密过程，可知

$$o'(m,n)=\{[\exp(\mathrm{i}p_1)*h(x,y,l)+\exp(\mathrm{i}p_2)*h(x,y,l)]\times a\}*h(x,y,d),\quad(2)$$

式中 $\exp(\mathrm{i}p_1)$，$\exp(\mathrm{i}p_2)$ 和 a 分别为相位板 P_1，P_2 和振幅板 A，$*$ 为卷积运算，$h(x,y,l)$，$h(x,y,d)$ 为自由空间衍射过程的脉冲响应函数，可表示为

$$h(x,y,l)=\frac{\exp(\mathrm{i}2\pi l/\lambda)}{\mathrm{i}\lambda l}\exp[\mathrm{i}\pi(x^2+y^2)/(\lambda l)],\quad(3)$$

式中 l 为衍射距离，λ 为相干照明所用波长。若能够根据(2)式及其他附件条件来确定 P_1，P_2，A，就实现了将图像信息隐藏于这三者之中的目的。首先确定振幅板 A，令

$$a=\mathrm{rand}(x,y),\quad(4)$$

rand 函数产生位于(0,1)区间的随机数，即振幅板 A 使用计算机随机产生，显然，其与被加密的原始图像无任何关联。在 A 确定之后，P1，P2 可随之确定。对(2)式进行调整，得

$$\mathscr{F}^{-1}\left\{\frac{\mathscr{F}[o'(m,n)]}{\mathscr{F}[h(x,y,d_3)]}\right\}\times p_3^{-1}=\exp(\mathrm{i}p_1)*h(x,y,l)+\exp(\mathrm{i}p_2)*h(x,y,l).\quad(5)$$

式中 $\mathscr{F}$ 及 $\mathscr{F}^{-1}$ 表示傅里叶变换及逆变换。为方便起见，令

$$c(m,n)=\mathscr{F}^{-1}\left\{\frac{\mathscr{F}[o'(m,n)]}{\mathscr{F}[h(x,y,d_3)]}\right\}\times p_3^{-1}.\quad(6)$$

于是(5)式变为

$$c(m,n) = \exp(\mathrm{i}p_1) * h(x,y,l) + \exp(\mathrm{i}p_2) * h(x,y,l). \quad (7)$$

相位板 P_1 和 P_2 除了满足(7)式之外，还满足条件

$$|\exp(\mathrm{i}p_1)| = |\exp(\mathrm{i}p_2)| = 1, \quad (8)$$

式中||表示取模运算。联合(7)式及(8)式，可以求得 $p_1(x,y)$和 $p_2(x,y)$的解析式分别为

$$p_1(x,y) = \arg(D) - \arccos[|D|/2], \quad (9)$$

$$p_2(x,y) = \arg\{D - \exp[\mathrm{i}p_1(x,y)]\}, \quad (10)$$

式中

$$D = \mathscr{F}^{-1}\left\{\frac{F[c(m,n)]}{\mathscr{F}[h(x,y,l)]}\right\}. \quad (11)$$

(4)、(9)、(10)式表明，相位板 P_1，P_2 以及振幅板 A 均已经得到。这样，原始图像 $o(m,n)$就成功地隐藏在了这三个掩模板之中，实现了加密的目的。利用图 1 所示解密装置或者使用数字方法均可对加密结果进行解密而得到原始图像。和解密方法相比，将图像加密至三个掩模板中并不直观，且仅能使用数字方法来实现。为了便于进行对比，在对本系统进行讨论之前，首先对 Zhang 方法中的“轮廓像”问题进行阐述。

3　“轮廓像”问题及其消除

如果在本文所提加密方法中令 $a=1$，即相当于移去随机振幅板 A，那么系统中用于隐藏原始图像的就只有相位板 P_1，P_2，本方法即转化为 Zhang 方法。因此，Zhang 方法可以视为本方法的一种特殊情况。这时 P_1，P_2 由以下公式给出[19]：

$$p_1(x,y) = \arg(D') - \arccos[|D'|/2], \quad (12)$$

$$p_2(x,y) = \arg\{D' - \exp[\mathrm{i}p_1(x,y)]\}, \quad (13)$$

式中

$$D' = \mathscr{F}^{-1}\left\{\frac{\mathscr{F}[o'(m,n)]}{\mathscr{F}[h(x,y,l+d)]}\right\}. \quad (14)$$

由(12)～(14)式可以看出，Zhang 方法中两个随机相位板 P_1 和 P_2 与 $o'(m,n)$的频谱有着密切的关系，而 $o'(m,n)$仅仅对原始图像 $o(m,n)$的相位做了随机调制，这就是“轮廓像”问题的根源。图 2 中给出了使用 Zhang 方法进行加密和解密的结果。图 2(a)中给出原始图像 “Lena”，大小为 512 pixel×512 pixel×8 bit，由(12)，(13)式所确定的相位板在图 2(b)，(c)中给出，在已知 P_1，P_2 及系统的正确参数情况下，解密的图像如图 2(d)所示。

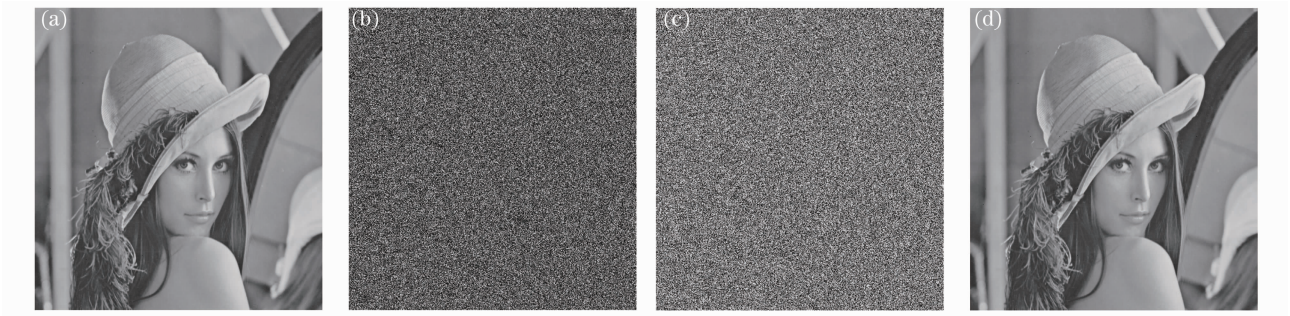

图 2　加密及解密结果。(a)原始图像；(b) P_1 相位分布；(c) P_2 相位分布；(d)解密图像

Fig. 2　Encryption and decryption results with Zhang′s method. (a) Primary image; (b) phase distribution of P_1; (c) phase distribution of P_2; (d) reconstructed image

为了便于对比，采用相关系数来描述恢复出来的图像 R 与原始图像 O 之间的符合程度。相关系数被定义为[18]

$$\rho = \frac{E\{[O-E(O)][|R|-E(|R|)]\}}{\{E\{[O-E(O)]^2\}E\{[|R|-E(|R|)]^2\}\}^{1/2}}, \quad (15)$$

式中 E 为求数学期望。这里为了方便，省略了坐标。使用(15)式来计算 Zhang 方法的重建结果与原始图像之间的相关系数，结果为 $\rho=0.9987$，这表明使用 Zhang 方法可以无损地恢复出来原始图像的信息。但是该方法存在“轮廓像”问题，即利用 P_1，P_2 中任何一个进行恢复均能得到原始图像的轮廓。图 3(a)，(b)分别给出了单独采用 P_1 或 P_2 进行解密时的解密结果，可以看出，解密的结果提供了有关原始图像相当多的信息，这就是 Zhang 方法所谓的“轮廓像”问题。从密钥空间的角度来分析，假定攻击者采用穷举法对 Zhang 方法进行攻击，已知图像规格为 512 pixel×512 pixel×8 bit，那么理论上 Zhang 方法的密钥空间应为 $2^{8\times512\times512}\times2^{8\times512\times512}$。实际上，由于“轮廓像”问题的存在，两个相位板 P_1，P_2 并不独立，且使用一个相位板即可获取足够信息，那么 Zhang 方法的实际密钥空间只有 $2^{8\times512\times512}$。因此可以说，“轮廓像”问题是 Zhang 方法固有的重要安全隐患，需要进一步改进。

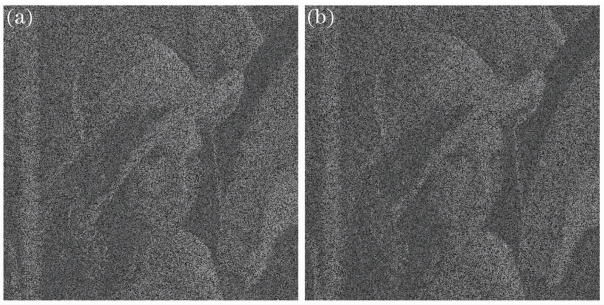

图 3　解密时单独使用(a)P_1 及(a)P_2 时的解密结果

Fig. 3　Decryption results with (a) P_1 and (b) P_2, respectively

正如前面所述，产生“轮廓像”问题的原因在于两个相位板与 $o'(m,n)$ 的频谱之间存在紧密关系。本方法正是通过破坏这个紧密关系，来消除“轮廓像”问题，这由(5)式可以看出。将 $o'(m,n)$ 进行距离为 d 的逆衍射之后，除以随机振幅板 A，所得结果再用来产生两个随机相位板 P_1，P_2。由于 A 是完全由计算机产生的随机振幅板，与原始图像 $o(m,n)$ 互相独立，因此用来产生两个随机相位板 P_1，P_2 的 $c(m,n)$ 既对原始图像进行了振幅随机调制，也进行了相位随机调制，因而 $c(m,n)$ 与原始图像 $o(m,n)$ 的相关性大大降低。因此可以推测，当使用本方法将原始图像加密到三个掩模板之后，单独使用任何一个进行解密均不会得到原始图像的信息，因而可以消除“轮廓像”问题。

4　计算机模拟

在计算机上使用 Matlab 7.0 对本文所提加密系统进行了模拟验证。模拟中，所取参数分别为 $l=100$ mm，$d=50$ mm，照明所用光波波长 $\lambda=632.8$ nm。图 4 给出了使用本文所提方法的加密结果。图 4(a)～(c)分别为相位板 P_1，P_2 以及振幅板 A，原始图像信息即隐藏在这三个掩模板中，这三个掩模板即为系统的密钥。可以看出，这三个掩模板均具有类似于白噪声的特性，这在一定程度上增加了系统的安全性。在解密参数正确的情况下，使用上述 P_1，P_2，A，并利用图 1 所示解密系统解密得到的结果在图 4(d)中给出，经计算该解密图像与原始图像之间的相关系数为 $\rho=0.9999$，这表明本方法可以无损地解密图像，没有造成原始图像信息的丢失。

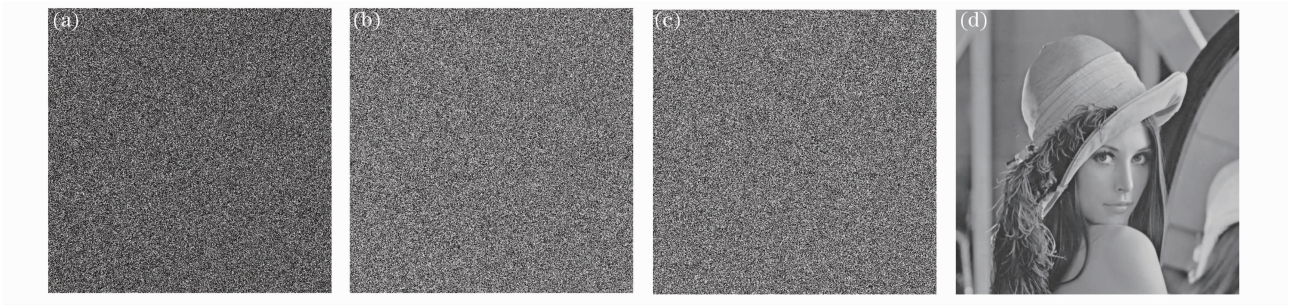

图 4　使用本文所提算法加密及解密结果。(a) P_1；(b) P_2；(c) A；(d) 解密结果

Fig. 4　Encryption and decryption results with our method. (a) P_1; (b) P_2; (c) A; (d) decryption of Lena

为了证实本方法对于“轮廓像”问题的消除，在其他参数正确的情况下，在图 1 所示解密系统中分别单独使用 P_1，P_2，A 进行解密，对应的解密结果在图 5中给出，这 3 幅解密图像与图像的相关系数分别为 $\rho=0.0111$，$\rho=-0.0620$，$\rho=-1.3799\times10^{-4}$，这些数值表明，解密图像已与原始图像不具备相关性。同时，与原始图像相比解密结果已经看不出任何有用的信息。这说明，单独获取这三个掩模板中的任意一个，不会得到与原始图像相关的任何信息。这说明本文所提方法已经消除了 Zhang 方法中的“轮廓像”问题。为了保证数据安全，这个三个掩模板需交付三个不同的保密者手中保管。

同时，和 Wang 方法相比，本方法更加实质地解决了“轮廓像”问题，在对于“部分密钥泄露”攻击方面表现出了更强的稳健性。从 Wang 方法的原理可知，若攻击者窃取到 3 个相位板中的两个可能的组合(P_1+P_3 或者 P_2+P_3)，那么就相当于获取了 Zhang 方法中的一个相位板，依然会有轮廓像问题的存在，然而使用本方法却不存在这个问题。假设攻击者截获了三个密钥中任意两个，但是缺少第三个密钥。模拟在这种情况下，攻击者随机选取第三个密钥进行解密的结果，在图 6 中给出。图 6(a)～(c)分别为在解密密钥 P_1，P_2，A 错误的情况下的解密结果，其对应的相关系数分别为 $\rho=-0.0019$，$\rho=0.0015$，$\rho=0.0832$。可见，使用任何一个错误密钥，即使在其他两个密钥正确的情况下，攻击者仍然得不到任何有关原始图像的信息。

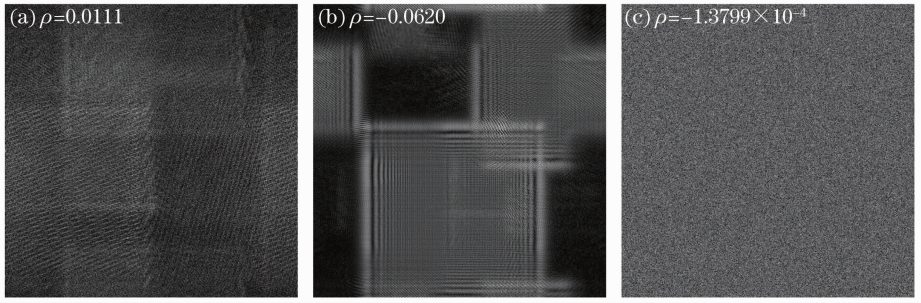

图 5　单独使用(a) P_1，(b) P_2 及(c) A 时得到的解密结果

Fig. 5　Decryption results with (a) P_1, (b) P_2 and (c) A respectively

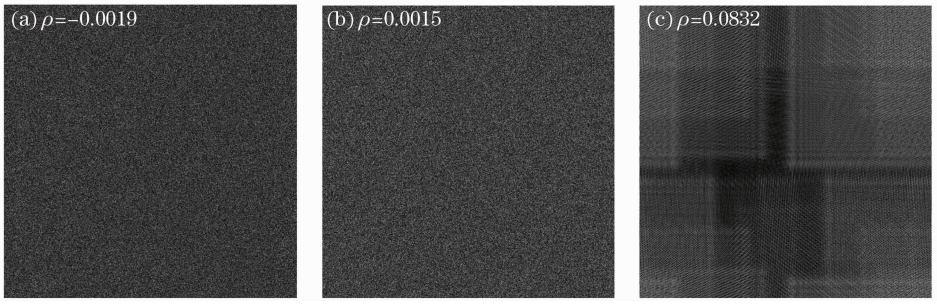

图 6　密钥(a) P_1，(b) P_2 及(c) A 错误的情况下的解密结果

Fig. 6　Decryption results with the wrong mask of (a) P_1, (b) P_2, and (c) A

从系统的安全性来分析，在不考虑距离、波长等附加参数的情况下，Wang 方法中，获取 3 个相位板中的两个即可得到原始图像的轮廓像，因此尽管有 3 个密钥，实际上只有两个可以认为相互独立，所以其实际密钥空间为 $2^{2\times8\times512\times512}$，相比于 Zhang 方法而言密钥空间扩大了 1 倍。而由图 6 的模拟结果可以看出，本方法中 3 个掩模板均近似相互独立，因此将本方法的密钥空间进一步扩展到 $2^{3\times8\times512\times512}$。这是一个相当巨大的密钥空间，暴力攻击无法实现破解。

5　结　　论

从光学的干涉与衍射理论出发，提出了一种光学加密系统。该光学加密系统将原始图像信息解析地隐藏在两个相位板及一个振幅板中，完全消除了 Zhang 方法中的轮廓像问题。该系统加密过程非常简单，无需先前所提算法中复杂的迭代过程。同时，解密系统同样非常紧凑，与文献[21]所述方法相比，在没有增加掩模板数量的情况下，本方法不要求解密时两个随机相位板互相紧贴，也省去了解密系统中的凸透镜，降低了系统的精度要求，使得光学解密过程更加容易实现。同时，计算机模拟也表明了本方法对部分密钥泄露攻击的稳健性。

参　考　文　献

1 Nanrun Zhou, Yixian Wang, Lihua Gong *et al*.. Novel single-channel color image encryption algorithm based on chaos and fractional Fourier transform[J]. *Opt. Commun.*, 2011, **284**(12): 2789～2796

2 Nanrun Zhou, Yixian Wang, Lihua Gong. Novel optical image encryption scheme based on fractional Mellin transform[J]. *Opt. Commun.*, 2011, **284**(13): 3234～3242

3 Chen Daqing, Zhou Hao, Tao Zhi *et al*.. Fourier computer-generated hologram digital watermarking with nonlinear amplitude limiting [J]. *Acta Optica Sinica*, 2011, **31**(2): 0207002
陈大庆，周　皓，陶　智 等. 非线性限幅傅里叶计算全息的数字水印方法[J]. 光学学报，2011，**31**(2)：0207002

4 Li Juan, Feng Yong, Yang Xuqiang. 3D chaotic encryption scheme for compressed image [J]. *Acta Optica Sinica*, 2010, **30**(2): 399～404
李　娟，冯　勇，杨旭强. 压缩图像的三维混沌加密算法[J]. 光学学报，2010，**30**(2)：399～404

5 Xi Sixing, Sun Xin, Liu Bing *et al*.. New image encryption technology of image based on computer generated hologram[J]. *Laser & Optoelectronics Progress*, 2012, **49**(4): 040902
席思星，孙　欣，刘　兵 等. 基于计算全息的双随机相位图像加密技术[J]. 激光与光电子学进展，2012，**49**(4)：040902

6 Wei Jia, Fung Jacky Wen, Yuk Tak Chow *et al*.. Binary image encryption based on interference of two phase-only masks[J]. *Appl. Opt.*, 2012, **51**(21): 5253～5258

7 M. R. Abuturab. Color image security system using double random-structured phase encoding in gyrator transform domain [J]. *Appl. Opt.*, 2012, **51**(15): 3006～3016

8 Bo Wang, Yan Zhang. Double images hiding based on optical interference[J]. *Opt. Commun.*, 2009, **282**(17): 3439～3443

9 Yujing Han, Yunhai Zhang. Optical image encryption based on two beams′ interference [J]. *Opt. Commun.*, 2010, **283**(9):

1690～1692

10 S. K. Rajput, N. K. Nishchal. Image encryption based on interference that uses fractional Fourier domain asymmetric keys [J]. *Appl. Opt.*, 2012, **51**(10): 1446～1452

11 Wen Chen, Xudong Chen, Colin J. R. Sheppard. Optical image encryption based on diffractive imaging[J]. *Opt. Lett.*, 2010, **35**(22): 3817～3819

12 Xiaogang Wang, Daomu Zhao. Single-channel color image encryption based on asymmetric cryptosystem[J]. *Opt. Laser Technol.*, 2012, **44**(1): 136～140

13 R. Philippe, J. Bahram. Optical image encryption based on input plane and Fourier plane random encoding[J]. *Opt. Lett.*, 1995, **20**(7): 767～769

14 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

15 Guohai Situ, Jingjuan Zhang. Double random-phase encoding in the Fresnel domain[J]. *Opt. Lett.*, 2004, **29**(14): 1584～1586

16 Peng Xiang, Tang Hongqiao, Tian Jindong. Ciphertext-only attack on double random phase encoding optical encryption system [J]. *Acta Physica Sinica*, 2007, **56**(5): 2629～2635
彭　翔，汤红乔，田劲东. 双随机相位编码光学加密系统的唯密文攻击[J]. 物理学报, 2007, **56**(5): 2629～2635

17 Peng Xiang, Zhang Peng, Wei Hengzheng *et al*.. Known_plaintext attack on double phase encoding encryption technique [J]. *Acta Physica Sinica*, 2006, **55**(3): 1130～1135
彭　翔，张　鹏，位恒政 等. 随机相位加密系统的已知明文攻击[J]. 物理学报, 2006, **55**(3): 1130～1135

18 B. Yang, Z. Liu, B. Wang *et al*.. Optical streamcipher-like system for image encryption based on Michelson interferometer [J]. *Opt. Express*, 2011, **19**(20): 2634～2642

19 Yan Zhang, Bo Wang. Optical image encryption based on interference[J]. *Opt. Lett.*, 2008, **33**(21): 2443～2445

20 Yan Zhang, Bo Wang, Zhili Dong. Enhancement of image hiding by exchanging two phase masks[J]. *J. Opt. A*, 2009, **11**(12): 125406

21 Xiaogang Wang, Daomu Zhao. Optical image hiding with silhouette removal based on the optical interference principle[J]. *Appl. Opt.*, 2012, **51**(6): 686～691

栏目编辑：何卓铭