非线性光学图像加密

侯俊峰[1,2] 黄素娟[1] 司徒国海[2*]

1上海大学通信与信息工程学院, 上海 200072

2中国科学院上海光学精密机械研究所, 上海 201800

摘要 结合传统的双随机相位编码和非线性光学技术的优点,提出一种基于光折变晶体自相位调制原理的非线性光学图像加密技术,并分析了其稳健性和安全性。该技术通过两个统计独立的随机相位板和两次非线性传播把明文图像加密成平稳的复随机白噪声。解密是加密的逆过程,既可以用光学的方法实现,也可以用非线性数字全息的方法实现。数值模拟结果证明,该加密系统在受加性噪声和乘性噪声影响的情况下,具有良好的稳健性,与传统的线性加密技术相比,该技术可以有效抵御选择明文和已知明文攻击。

关键词 傅里叶光学; 非线性加密; 非线性相位恢复; 双随机相位编码

中图分类号 O438 **文献标识码** A

doi: 10.3788/AOS201535.0807001

Nonlinear Optical Image Encryption

Hou Junfeng[1,2] Huang Sujuan[1] Situ Guohai[2]

[1]*School of Communication and Information Engineering, Shanghai University, Shanghai* 200072, *China*

[2]*Shanghai Institute of Optics and Fine Mechanics, Chinese Academy of Sciences, Shanghai* 201800, *China*

Abstract Taking the advantages of the traditional double random phase encoding and nonlinear optics techniques, a novel nonlinear optical image encryption technique based on self-phase modulation of photorefractive crystal is proposed, the robustness and security are analyzed. The plaintext image is encrypted into a stationary complex random white noise via two statistically independent random phase masks and two sequential nonlinear propagations. The decryption is the inverse process of the encryption, which can be implemented either optically or digitally using nonlinear digital holography. Numerical simulation results demonstrate that the proposed nonlinear optical image encryption technique is robust against additive and multiplicative noise, resists effectively against the chosen plaintext attack or known plaintext attack based on phase retrieval in comparison with the traditional linear encryption techniques.

Key words Fourier optics; nonlinear encryption; nonlinear phase retrieval; double random phase encoding

OCIS codes 070.1170; 060.4785; 100.5070; 110.1758

1 引 言

随着对双随机相位编码技术[1]研究的深入,研究者发现明文与经系统加密的密文之间具有线性关系[2],容易遭受选择明文[3-4]、已知明文[5-6]等多种攻击。例如:在选择明文攻击[3]中,攻击者将一个中心 δ 函数输入双随机相位加密系统,在系统的输出端得到频域相位密钥的频谱,从而破解加密系统。文献[4]利用多个 δ 函数作为选择明文,得到了该系统的空域相位密钥,继而得出频域相位密钥。文献[5]是在已知一对明文-密文对的情况下用混合输入输出(HIO)算法[7]恢复相位密钥,文献[6]则是利用多对已知明文-密文对的G-S算法[7-8]恢复相位密钥,取得了更好的破解效果。可以看出突破光学加密系统的线性对光学信息安全技术的进一步发展有直

收稿日期: 2015-03-14; **收到修改稿日期**: 2015-05-05

基金项目: 国家自然科学基金(61377005)、中国科学院创新交叉团队项目(1403331X00)

作者简介: 侯俊峰(1988—),男,硕士研究生,主要从事光学图像加密方面的研究。E-mail:houjunfengyx@163.com

导师简介:黄素娟(1968—),女,博士,教授,主要从事数字全息、图像处理方面的研究。E-mail:sjhuang@shu.edu.cn

*通信联系人。E-mail:ghsitu@siom.ac.cn

接的促进意义。近年来，人们已提出了几种非线性的图像加密方案[9-11]。但在这些方案中，明文依然是在一个线性系统里加密的，只是对密文进行一些非线性处理，或者是先对明文进行非线性处理，然后在一个线性系统里加密，我们将这些方案统称为半非线性加密技术。并且文献[11]提出的方法只适用于虚拟光学系统，并不能在实际的光学加密系统中应用。有别于此，本文提出了一种完全的非线性光学图像加密技术，即明文通过一个非线性光学系统来实现加密，并对该加密技术的安全性进行分析，发现该技术能有效抵抗上述密码学攻击。

2 光的非线性传播

在稳态傍轴近似下，光波在非线性光折变晶体中的传播可以用非线性薛定谔方程描述[12]

$$\frac{\partial \psi}{\partial z}=\left[\mathrm{i}\frac{1}{2kn_0}\nabla_{\perp}^2+\mathrm{i}k\Delta n\left(\left|\psi\right|^2\right)\right]\psi\equiv\left[D+N\left(\left|\psi\right|^2\right)\right]\psi, \tag{1}$$

式中$\psi(x,y,z)$表示光波复振幅，$k=2\pi/\lambda$ 是波数，λ 是自由空间中的光波长，n_0 表示晶体的线性折射率，$\Delta n\left(\left|\psi^2\right|\right)$表示非线性折射率变化，$D$ 描述光的衍射，是一种线性作用，而 $N\left(\left|\psi^2\right|\right)$则描述光与非线性介质的非线性作用。在诸多非线性效应中，着重考察光折变晶体对光的自相位调制效应。当光沿着垂直于光折变晶体晶轴 C 的方向传播时，若对晶体施加一个沿晶轴 C 方向的负偏压 E_0，就能使晶体对入射光产生一种自散焦效应。以铌酸锶钡晶体（SBN:75）为例，由沿晶轴 C 方向偏振的偏振光引起的折射率变化为[13-14]

$$\Delta n\left(\left|\psi^2\right|\right)=\frac{1}{2}n_0^3r_{\mathrm{eff}}E_0\frac{\bar{I}}{1+\bar{I}}, \tag{2}$$

式中 r_{eff} 是晶体有效电光系数，$\bar{I}$ 是输入光强 I 相对于暗电流的归一化强度，其中 $I=\left|\psi\right|^2$。由于色散、散射和吸收效应通常不会影响到光波的重建[15]，可以对此忽略不计。

晶体中光波的演化可以使用分步傅里叶法来对非线性薛定谔方程进行数值计算，对每个传播距离增量 $\mathrm{d}z$，线性与非线性算子单独作用

$$\psi(z+\mathrm{d}z)\approx\exp(\mathrm{d}z\cdot D)\exp\left[\mathrm{d}z\cdot N\left(\left|\psi\right|^2\right)\right]\psi(z), \tag{3}$$

光波的反向传播本质上是一个初始值问题，其输出是原来的输入值。反向方程可以写为

$$\psi(z)\approx\exp(-\mathrm{d}z\cdot D)\exp\left[-\mathrm{d}z\cdot N\left(\left|\psi\right|^2\right)\right]\psi(z+\mathrm{d}z), \tag{4}$$

用(4)式就可以进行光波的数值重建。

3 非线性光学图像加密

3.1 加密原理

提出的非线性光学图像加密系统如图1所示。输入平面、变换域平面以及输出平面的坐标分别表示为 (x,y)，(x',y') 和 (u,v)。加密过程可以写为

$$g(u,v)=\mathrm{NLT}_2\left\{\mathrm{NLT}_1\left\{f(x,y)\exp\left[\mathrm{i}\varphi_1(x,y)\right]\right\}\exp\left[\mathrm{i}\varphi_2(x',y')\right]\right\}, \tag{5}$$

式中$f(x,y)$ 表示原始明文图像，M_1和M_2为随机相位板，其相位 $\varphi_1(x,y)$ 和 $\varphi_2(x',y')$ 是 0~2π 之间的均匀分布，而且相互统计无关。NLM_1和NLM_2表示非线性介质，其长度分别为 Z_1 和 Z_2。$g(u,v)$为密文复振幅，需用干涉法记录。NLT_1和NLT_2分别表示光波在NLM_1和NLM_2中的非线性传播，以方程(1)所示的薛定谔方程来描述。

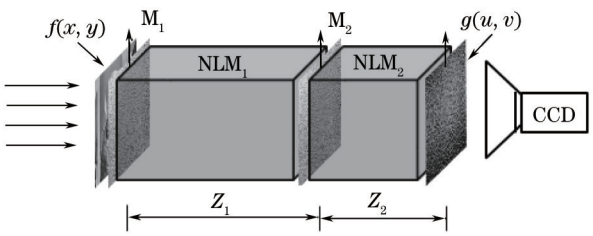

图1 非线性加密系统的光学结构

Fig.1 Optical setup of nonlinear image encryption system

3.2 解密原理

解密过程可以用光学方法实现，也可以用非线性数字全息的方法实现。在解密过程中，用正确的系统参数、相位密钥以及照明光波长，就可以由密文 $g(u,v)$，得到相应的明文 $f(x,y)$。解密是加密的逆过程

$$f(x,y)=\mathrm{INLT}_1\left\{\mathrm{INLT}_2\left[g(u,v)\right]\exp\left[-\mathrm{i}\varphi_2(x',y')\right]\right\}\exp\left[-i\varphi_1(x,y)\right], \tag{6}$$

式中 INLT_1 和 INLT_2 分别表示光波在 NLM_1 和 NLM_2 中非线性传播的逆过程，可由(4)式来表示。

4 模拟实验及结果

为了验证非线性光学图像加密技术的可行性和有效性，运用 Matlab 软件进行数值模拟。选择大小为 256 pixel×256 pixel 的图像 lena 作为原始明文图像，如图 2(a)所示。由于在衍射和自散焦的共同作用下，计算载有明文图像的光束在非线性晶体中的传播会溢出计算窗口，需要对图像作零填充预处理，得到大小为 512 pixel×512 pixel 的图像。在数值仿真过程中，取像素尺寸为 2 μm×2 μm，自由空间波长 $\lambda=532$ nm，沿晶轴 C 方向的电压 $E_0=-1000$ V/m，$n_0=2.3$，$r_{\mathrm{eff}}=1340\times10^{-12}$ m/V，Z_1 和 Z_2 分别为 8 mm 和 6 mm，沿非线性传播方向的步长 $dz=20$ μm。通过对(5)式的计算，在输出平面得到密文 $g(u,v)$，其振幅如图 2(b)所示。不难验证，其分布是平稳复随机白噪声。图 2(c)是用正确密钥恢复的解密图像，可以看到原始明文图像已经被完全恢复。

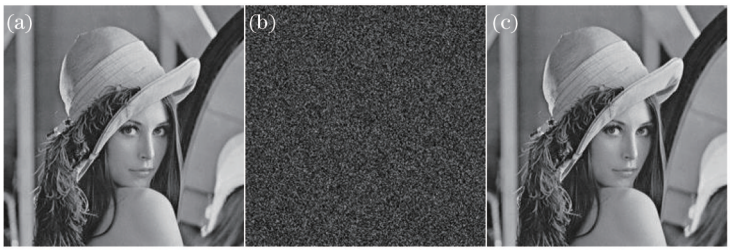

图 2 (a) 原始明文图像 lena; (b) 图(a)对应的密文; (c) 正确密钥解密图像

Fig. 2 (a) Original plaintext image lena; (b) encrypted image corresponding to image (a); (c) decrypted image with correct keys

分析该非线性加密系统的稳健性。当系统存在噪声或者解密密钥偏离加密密钥时，通过(6)式所描述的解密过程所获得的解密图像将存在噪声。为了量化原始明文图像和解密图像之间的差异，定义原始明文图像 lena 和解密图像之间的相对误差(RE)为

$$f_{\mathrm{RE}}=\frac{\sum\sum\left|\left|f(x,y)\right|-\left|\bar{f}(x,y)\right|\right|^2}{\sum\sum\left|f(x,y)\right|^2}, \tag{7}$$

式中 $f(x,y)$ 表示原始明文图像，$\bar{f}(x,y)$ 表示相应的解密图像。假设密文受到加性噪声的影响，受加性噪声影响的密文可以写成[16]

$$g_{\mathrm{ad}}(x,y)=g(x,y)+n_{\mathrm{ad}}(x,y), \tag{8}$$

式中 $n_{\mathrm{ad}}(x,y)$ 是零均值均匀分布的实随机函数，并且 $g_{\mathrm{ad}}(x,y)$ 的信噪比(SNR)为 1。图 3(a)是受加性噪声影响的解密图像，图像噪声为高斯分布，其 RE 为 0.12。在受乘性噪声影响的情况下，可以获得类似的结果。受乘性噪声影响的密文可以写成[1]

$$g_{\mathrm{mu}}(x,y)=g(x,y)\left[1+n_{\mathrm{mu}}(x,y)\right], \tag{9}$$

式中 $n_{\mathrm{mu}}(x,y)$ 是零均值均匀分布的实随机函数，$g_{\mathrm{mu}}(x,y)$ 的信噪比为 1。受乘性噪声影响的解密图像如图 3(b)所示，其 RE 为 0.12。以上结果表明，非线性加密系统在受加性噪声和乘性噪声影响的条件下具有良好的稳健性。

分析加密系统参数、相位密钥以及照明光波长对加密和解密所造成的影响，可将 Z_1，Z_2，$\varphi_2(x',y')$，r 和 r_{nl} 对系统的影响进行单独考察，即在其它所有参数都是正确的条件下，研究某一参数的变化对解密效果的影响。其中线性系数 r 和非线性系数 r_{nl} 分别为

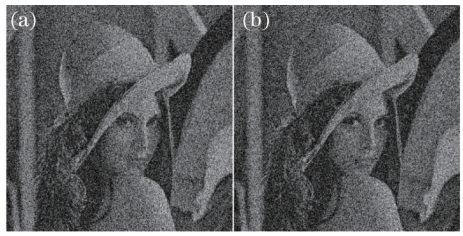

图3 (a) 受加性噪声影响的解密图像; (b) 受乘性噪声影响的解密图像

Fig. 3 (a) Decrypted image with additive noise; (b) decrypted image with multiplicative noise

$$r = kn_0 = \frac{2\pi n_0}{\lambda}, \tag{10}$$

$$r_{nl} = \frac{1}{2}kn_0^3 r_{eff} E_0 = \frac{\pi}{\lambda} n_0^3 r_{eff} E_0 . \tag{11}$$

非线性传播距离 Z_1 和 Z_2 分别对RE的影响如图4(a)所示,线性系数对RE的影响如图4(b)所示。在数值仿真结果中,当RE大于0.4时,解密图像如图4(c)所示,无法分辨出明文信息。也就是说,当 $|\Delta Z_2|$ 大于0.1 mm,或者 $|\Delta r/r|$ 大于0.02时,解密图像已经完全淹没在其产生的噪声之中。由图4(a)可知,解密图像对 Z_1 的敏感性相对于对 Z_2 来说要小很多,这是因为 Z_2 导致的误差会在相位密钥解密时被放大,而 Z_1 导致的误差则不会。另外数值模拟结果表明解密图像对非线性系数 r_{nl} 是不敏感的,这是因为与线性系数 r 相比,非线性系数 r_{nl} 非常小。尽管如此,系统的非线性对加密系统的安全仍然起着至关重要的作用。例如,将一个或多个 δ 函数输入非线性加密系统时,不能在系统的输出端得到系统的冲击响应,保证了加密系统的安全性。当用随机产生的错误相位密钥解密时,在系统输出端无法获得正确的解密图像。因此,NLT_2 的长度 Z_2,M_2 的相位分布 $\varphi_2(x',y')$ 以及线性系数 r 都可以作为加密系统的密钥。

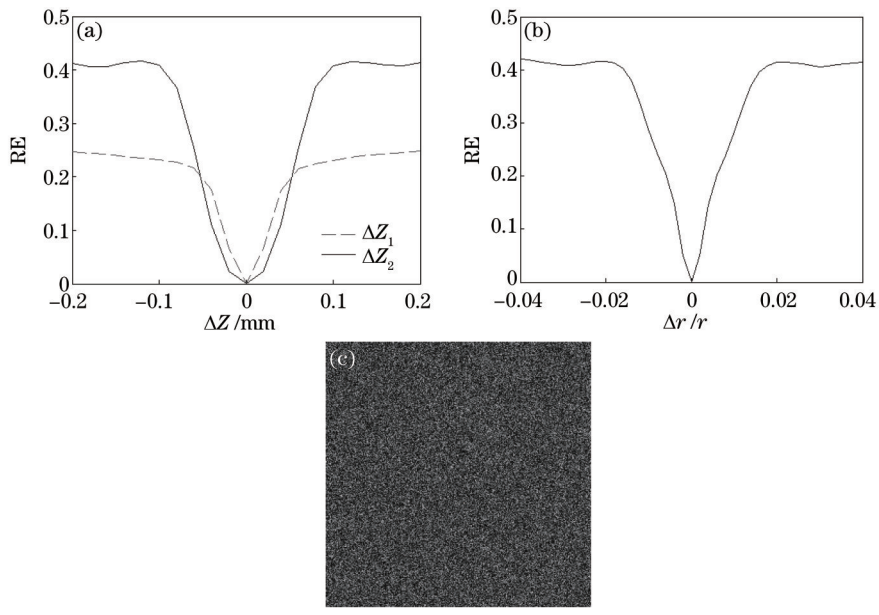

图4 (a) Δz_1 和 Δz_2 对RE的影响; (b) $\Delta r/r$ 对RE的影响; (c) RE大于0.4时的解密图像

Fig. 4 (a) Behavior of the RE versus Δz_1 and Δz_2; (b) behavior of the RE versus $\Delta r/r$; (c) decrypted image when RE is larger than 0.4

分析加密系统的安全性。假设攻击者用文献[3]、[4]中提到的方法,即在加密系统输入端输入一个中心 δ 函数或多个 δ 函数进行选择明文攻击,由于系统的参数以及外加电压是未知的,这种方法并不能得到相位密钥,相位密钥为 $\exp[i\varphi_1(x,y)]$。此外,由于加密系统是非线性的,利用 δ 函数作为选择明文攻击并不能在系统输出端得到系统的冲击响应,因此传统选择明文攻击的方法是无效的。本文选择使用已知明文攻击的方法进行测试。假设攻击者不仅知道除相位密钥 $\varphi_1(x,y)$ 和 $\varphi_2(x',y')$ 以外加密系统的全部信息,同时也知道一对或多对明文和密文。若已知一对明文和密文 $f_1(x,y)$ 和 $g_1(u,v)$,则在变换域平面,图像的模为

$$\left|g_1(x',y')\right| = \left|\mathrm{INLT}_2\left[g_1(u,v)\right]\right|, \tag{12}$$

输入图像的模为 $\left|f_1(x,y)\right|$。参照文献[5]所用的相位恢复算法,并将其应用到非线性变换中,即用已知一对明文-密文对的非线性G-S相位恢复算法,恢复出随机相位板 M_1 的相位为 $\bar{\varphi}_1(x,y)$。解密密钥为

$$\exp\left[\mathrm{i}\bar{\varphi}_2(x',y')\right] = \frac{\mathrm{INLT}_2\left[g_1(u,v)\right]}{\mathrm{NLT}_1\left\{f_1(x,y)\exp\left[\mathrm{i}\bar{\varphi}_1(x,y)\right]\right\}}, \tag{13}$$

将解密密钥代入(6)式,就可以得到解密图像

$$\bar{f}(x,y) = \mathrm{INLT}_1\left\{\mathrm{INLT}_2\left[g(u,v)\right]\exp\left[-\mathrm{i}\bar{\varphi}_2(x',y')\right]\right\}\exp\left[-\mathrm{i}\bar{\varphi}_1(x,y)\right]. \tag{14}$$

已知明文如图5(a)所示,图5(b)是其相应的密文。$\bar{\varphi}_1(x,y)$ 是用非线性G-S算法迭代500次后得到的相位,然后用计算出的解密密钥解密原始明文图像lena的密文[图2(b)],图5(c)是相应的解密图像。解密图像包含已知明文图5(a)的信息,但是不能分辨出其相应明文lena的任何信息。估算的相位 $\bar{\varphi}_1(x,y)$ 与初始相位 $\varphi_1(x,y)$ 之差如图5(d)所示,它是一个无规则的随机分布,并不是一个常数。这说明通过非线性G-S算法并不能精确恢复 M_1 的相位 $\varphi_1(x,y)$。因为薛定谔方程的对称性本质导致了相位的简并,所以在时域和变换域的模相等的情况下有无穷多解[17],也就是说非线性G-S算法与传统G-S算法、HIO算法一样,是一种非凸集投影算法,在迭代过程中会收敛到局部最小解,而得不到唯一解。在线性光学系统中,通过多次不同的强度测量,利用这种多样性,G-S算法能比较容易地收敛到唯一解。所以,在线性光学加密系统中,利用多对已知明文和密文进行已知明文攻击,可以比较准确地找到相位密钥。然而,在非线性系统中,由于非线性折射率的改变与光强分布有关,基于多对已知明文-密文对的非线性G-S算法会受到不同图像光强分布的影响,无法恢复真实的相位。因此,文献[6]的已知明文攻击方法对非线性光学加密系统是无效的。

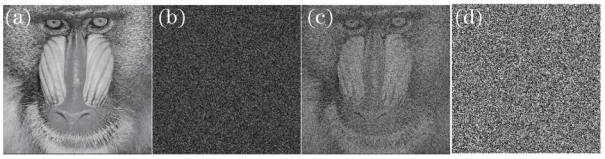

图5 (a) 已知明文; (b) 已知密文; (c) 已知明文攻击解密图像; (d) 估算相位与初始相位之差

Fig. 5 (a) Known plaintext; (b) known ciphertext; (c) decrypted image using known plaintext attack; (d) difference between the estimated and original phase

5 结 论

提出了一种基于光折变晶体自相位调制原理的非线性光学图像加密技术。该方法结合双随机相位编码和非线性光学技术,使加密系统成为一个非线性系统。与传统的双随机相位编码技术相比,非线性光学加密技术具有很高的安全性,可以很好地抵御选择明文攻击和已知明文攻击。同时,该系统在受加性噪声和乘性噪声影响的情况下,都具有良好的稳健性。

参 考 文 献

1 Refregier P, Javidi B. Optical image encryption based on input plane and Fourier plane random encoding[J]. Opt Lett, 1995, 20(7): 767-769.

2 Frauel Y, Castro A, Naughton T J, *et al*.. Resistance of the double random phase encryption against various attacks[J]. Opt Express, 2007, 15(16): 10253-10265.

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

4 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.

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

6 Situ G, Gopinathan U, Monaghan D S, *et al*.. Cryptanalysis of optical security systems with significant output images[J]. Appl Opt, 2007, 46(22): 5257-5262.

7 Fienup J R. Phase retrieval algorithms: A comparison[J]. Appl Opt, 1982, 21(15): 2758-2769.

8 Gerchberg R W. A practical algorithm for the determination of phase from image and diffraction plane pictures[J]. Optik, 1972, 35: 237.

9 Cheng X C, Cai L Z, Wang Y R, *et al*.. Security enhancement of double-random phase encryption by amplitude modulation[J]. Opt Lett, 2008, 33(14): 1575-1577.

10 Liu J, Xu X, Wu Q, *et al*.. Information encryption in phase space[J]. Opt Lett, 2015, 40(6): 859-862.

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

12 Barsi C, Wan W, Fleischer J W. Imaging through nonlinear media using digital holography[J]. Nature Photonics, 2009, 3(4): 211-215.

13Wan W, Fleischer J W. Superfluid-like shock waves in nonlinear optics[C]. APS March Meeting Abstracts, 2006, 1: 8011P.

14 Wan W, Jia S, Fleischer J W. Dispersive superfluid-like shock waves in nonlinear optics[J]. Nature Physics, 2007, 3(1): 46-51.

15 Tsang M, Psaltis D, Omenetto F G. Reverse propagation of femtosecond pulses in optical fibers[J]. Opt Lett, 2003, 28(20): 1873-1875.

16 Javidi B, Sergent A, Zhang G, *et al*.. Fault tolerance properties of a double phase encoding encryption technique[J]. Opt Eng, 1997, 36 (4): 992-998.

17 Lu C H, Barsi C, Williams M O, *et al*.. Phase retrieval using nonlinear diversity[J]. Appl Opt, 2013, 52(10): D92-D96.

栏目编辑: 苏 岑