一种基于迭代振幅-相位恢复算法和非线性双随机相位编码的图像加密方法

陈翼翔[1] 汪小刚[2]

([1] 浙江传媒学院电子信息学院, 浙江 杭州 310018
[2] 浙江农林大学理学院, 浙江 临安 311300)

摘要 提出了一种基于迭代振幅-相位恢复算法和非线性双随机相位编码的图像加密方法。该方法利用两个公开密钥和一幅“假图像”在非线性双随机相位加密系统中生成密文,接着利用迭代非线性双随机相位编码生成两个私有密钥。待加密图像和密文作为迭代加密方法中的两个限定值。解密过程则可以在经典的基于 $4f$ 系统的线性的光学双随机相位编码系统中完成。该加密方法具有迭代收敛速度快、安全性高的优点。迭代该图像加密方法能够抵御最近提出的基于改进的振幅-相位恢复算法的攻击。理论分析和仿真实验都证明了此方法的有效性和可靠性。

关键词 傅里叶光学;双随机相位编码;振幅-相位恢复算法;非线性加密

中图分类号 O438 **文献标识码** A **doi**: 10.3788/AOS201434.0810003

Image Encryption Based on Iterative Amplitude-Phase Retrieval and Nonlinear Double Random Phase Encoding

Chen Yixiang[1] Wang Xiaogang[2]

([1] *School of Electronics Information, Zhejiang University of Media and Communications, Hangzhou, Zhejiang* 310018, *China*
[2] *School of Science, Zhejiang A & F University, Lin'an, Zhejiang* 311300, *China*)

Abstract A novel image encryption method based on iterative amplitude-phase retrieval and nonlinear double random phase encoding is proposed. In this method, a fake image is first used to generate the cipher text with the help of two public keys in the nonlinear double random phase encoding scheme. Two private keys are generated in the encryption process, where the original image to be encoded and the cipher text are applied as two constraints in the fast iterative amplitude-phase retrieval algorithm. The decryption processes can be finished in linear doubled random-phase encoding system based on $4f$ system. This encryption method has the advantages of fast convergence speed and high security. The proposed image encryption method has a resistance against on the amplitude-phase retrieval-based attack. The theoretical analysis and simulation experiments both validate the feasibility and security of the proposed scheme.

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

OCIS codes 100.2000; 100.4998

1 引 言

基于光学理论和方法的信息加密技术是近些年逐步发展起来的新一代的信息安全处理技术[1]。图像是信息载体的重要形式之一,具有直观生动的特

收稿日期: 2014-03-12; **收到修改稿日期**: 2014-04-04

基金项目: 国家自然科学基金(61205006)、浙江省高等学校访问学者专业发展项目(FX2013103)、浙江传媒学院校级科研项目(ZC12XJY003)

作者简介: 陈翼翔(1979—),男,博士,讲师,主要从事激光光学和光信息安全方面的研究。

E-mail: chenyix1979@163.com

点。在大量数据面临被窃取、非法复制和传播甚至被篡改的今天，探索和开发光学图像加密技术具有很高的学术和应用价值。1995 年，Refregier 等[2]提出了一种基于“双随机相位编码”的光学图像加密技术，它是光学理论在信息安全领域的重大运用。之后，世界各地的众多学者展开了多方面的深入研究并提出了不少新的图像加密方法[3-13]。譬如，Unnikrishnan 等[3-4]将双随机相位编码技术的应用从傅里叶变换域扩展到了分数傅里叶变换域，引入分数傅里叶变换阶数作为新的密钥；Situ 等[5-6]又将双随机相位编码技术的应用扩展到了菲涅耳域，简化了加密系统，将波长和衍射距离作为新的密钥，提高系统的安全性；Tao 等[7]则将两幅待加密图像复合为复振幅图像，并利用双随机相位编码技术实现了傅里叶域的双图像加密，2008 年又将该技术运用到多参数光学分数傅里叶变换中[8]；Liu 等[9-10]将双随机相位编码技术的应用扩展到了 Gyrator 变换域；此外，还有许多光学加密理论与技术已经在世界范围内得到广泛的研究[11-14]。

于此同时，关于光学图像加密方法安全性的研究也越来越受到科学人员的关注[15-17]。2006 年，位恒政等[15]人提出了选择明文攻击的方法，破解了双随机相位加密系统。2012 年，He 等[17]构造了一种结合选择明文和已知明文的两步攻击方法破解了在双随机相位编码系统的频域上增加振幅板的改进方案。为了消除线性双随机加密系统容易遭受攻击的缺点，Qin 等[18]在 2010 年提出了一种非线性双随机相位加密方法，它能有效抵御暴力攻击、已知明文攻击等多种攻击。随后，研究人员在此基础上提出了许多新的非线性图像加密方法[19-21]。需要指出的是，当傅里叶域的非线性双随机加密系统中的两个加密密钥暴露或作为公开密钥使用时，通过改进的振幅-相位恢复算法就可以迅速地破解出原始信息和两个解密密钥[22]。

本文提出了一种基于迭代非线性双随机相位编码的图像加密方法。该方法在非线性双随机相位编码的框架下，通过加密过程中采用迭代振幅-相位恢复算法生成两个解密密钥。解密过程则可以在经典的基于 $4f$ 系统的双随机相位编码系统中完成。利用计算机进行了仿真实验和攻击测试，实验结果表明，该加密方法能够抵御最近提出的基于改进的振幅-相位恢复算法的攻击。

2　非线性双随机相位编码及其安全性

在非线性双随机相位编码中，两块相互统计无关的随机相位板 $R_1(x,y)$ 和 $R_1'(u,v)$ 分别被放置在加密系统的输入面和傅里叶平面内，其中傅里叶平面内复振幅分布的振幅部分可表示为[18]

$$g(u,v)=\mathrm{PT}\{\mathscr{F}[f(x,y)\cdot R_1(x,y)]\},\quad(1)$$

式中 PT{ }代表相位切除运算，即除去复振幅的相位信息而只保留振幅信息，$\mathscr{F}[\ ]$表示傅里叶变换。接着在第二个随机相位板 $R_1'(u,v)$ 的作用下，图像 $f(x,y)$ 最终被加密成密文 $C(x,y)$，即

$$C(x,y)=\mathrm{PT}\{\mathscr{F}^{-1}[g(u,v)\cdot R_1'(u,v)]\}.\quad(2)$$

加密过程中生成的两个解密密钥分别为

$$K_1(x,y)=\mathrm{PR}\{\mathscr{F}^{-1}[g(u,v)\cdot R_1'(u,v)]\},\quad(3)$$

$$K_2(u,v)=\mathrm{PR}\{\mathscr{F}[f(x,y)\cdot R_1(x,y)]\},\quad(4)$$

式中 PR{ }代表取相位运算，即除去复振幅的振幅信息而只保留其相位信息.

在解密系统中，解密密钥 $K_1(x,y)$ 和 $K_2(u,v)$ 分别被放置在输入面和傅里叶平面内。解密的过程可以分成两步。首先，密文与解密密钥 $K_1(x,y)$ 相乘后进行傅里叶变换，并记录变换后的振幅信息。由(2)式和(3)式不难得到，该振幅信息就是 $g(u,v)$，即

$$g(u,v)=\mathrm{PT}\{\mathscr{F}[C(x,y)\cdot K_1(x,y)]\}.\quad(5)$$

接着，将复原得到的振幅信息 $g(u,v)$ 与 $K_2(u,v)$ 相乘，并进行一次逆傅里叶变换，对变换后得到的结果进行相位切除后得到的解密结果为

$$D_0(x,y)=\mathrm{PR}\{\mathscr{F}[g(u,v)\cdot K_1(u,v)]\},\quad(6)$$

由(1)式和(4)式容易证明 $D_0(x,y)=f(x,y)$。

非线性双随机相位编码实现了加密过程的非线性以及加密密钥与解密密钥的分离，相比经典的线性双随机相位编码技术，具有更高的安全性。它已被证明能抵抗暴力攻击、选择明文攻击等在内的多种攻击[18]。

需要指出的是，由于非线性双随机加密系统的加密过程和解密过程均为非线性，因此与线性双随机相位编码技术相比，其光学加密和解密系统更为复杂。此外，最近的研究表明，当两个加密密钥 $R_1(x,y)$ 和 $R_1'(u,v)$ 被公开或者泄露时，该非线性双随机加密系统并不能抵御基于改进的振幅-相位恢复算法的攻击[22]。攻击的流程图如图 1 所示，两个公钥和密文作为迭代循环中的 3 个限定值。当迭代运算的次数达到预先设定的数值时，迭代终止，最终得到攻击结果。

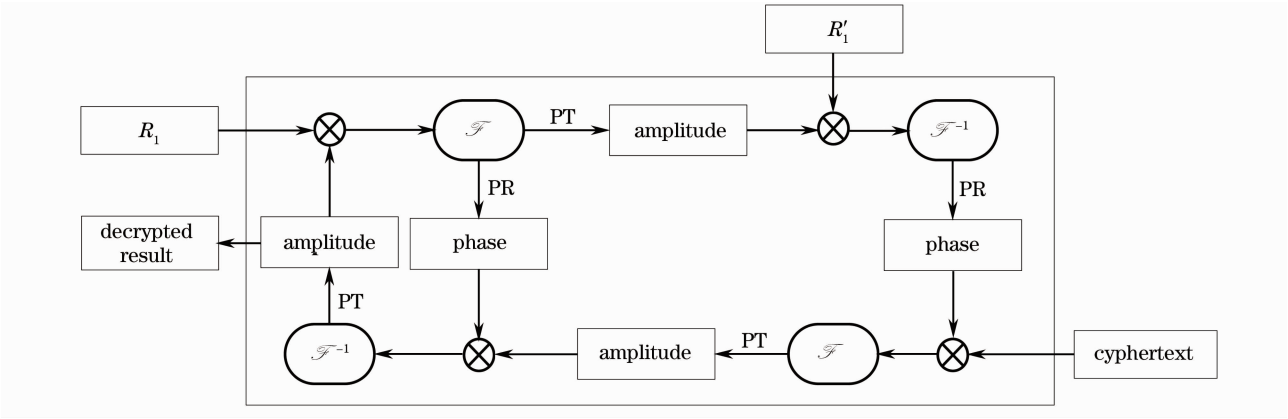

图 1 改进的振幅-相位恢复算法攻击的流程图

Fig. 1 Flowchart of the modified amplitude-phase retrieval based-attack

3 基于迭代非线性双随机相位编码的图像加密方法

3.1 图像的加密

基于迭代非线性双随机相位编码的加密方法的加密流程图如图 2 所示。其主要原理是：首先，利用“假图像”和两个公钥在非线性双随机相位加密系统中生成密文；接着在迭代的非线性双随机相位加密方法作用下产生两个私有密钥。利用“假图像”生成的密文和两个私有密钥，则可以解密得到原始图像（明文）。所谓的“假图像”在这里是指与明文同尺寸并用来保护明文的另一幅图像。

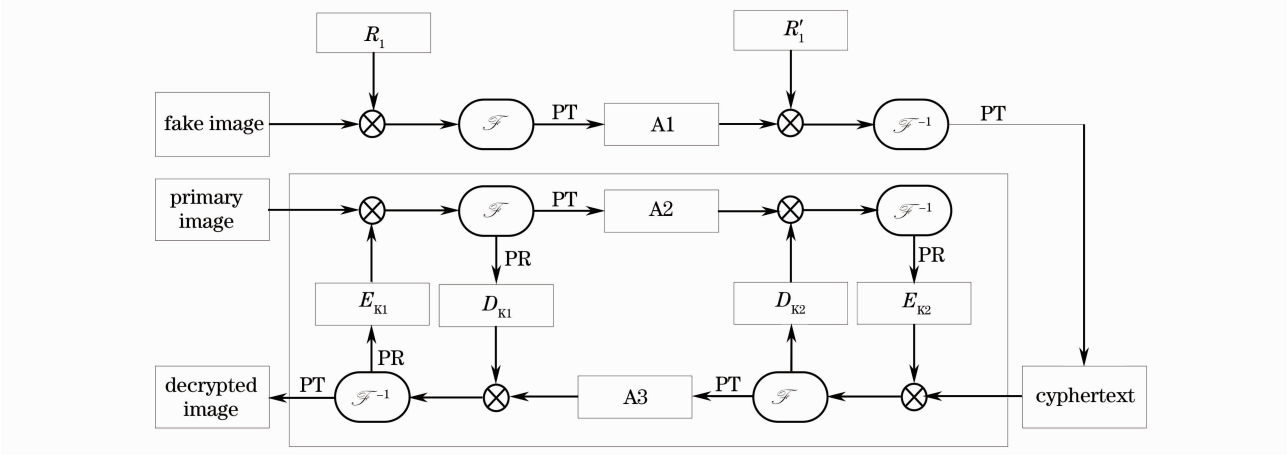

图 2 迭代加密过程流程图

Fig. 2 Flowchart of the iterative encryption process

图 2 中的公钥 1 和公钥 2 仍然分别用 $R_1(x,y)$ 和 $R_1'(u,v)$ 表示，“假图像”则用函数 $F(x,y)$ 表示。E_{K1}、E_{K2} 是迭代运算过程中的两个加密密钥，而 D_{K1} 和 D_{K2} 则是迭代运算过程中使用的两个解密密钥。振幅 A_1 和密文可分别表示为

$$g_0(u,v) = \mathrm{PT}\{\mathscr{F}[F(x,y)\cdot R_1(x,y)]\}, \quad (7)$$

$$E(x,y) = \mathrm{PT}\{\mathscr{F}^{-1}[g_0(u,v)\cdot R_1'(u,v)]\}. \quad (8)$$

接着进入迭代运算部分。如图 2 所示，原始图像和密文被用作迭代运算的两个限定值。如果用函数 $I(x,y)$ 原始图像，$R_k(x,y)$ 和 $R_k'(u,v)$ 表示在第 k 次迭代过程中使用的加密密钥 E_{K1} 和加密密钥 E_{K2}，则振幅 A_2 可表示成

$$g_k(u,v) = \mathrm{PT}\{\mathscr{F}[I(x,y)\cdot R_k(x,y)]\}. \quad (9)$$

解密密钥 D_{K1} 和解密密钥 D_{K2} 分别为

$$P_k(u,v) = \mathrm{PR}\{\mathscr{F}[I(x,y)\cdot R_k(x,y)]\}, \quad (10)$$

$$P_k'(x,y) = \mathrm{PR}\{\mathscr{F}^{-1}[g_k(u,v)R_k'(u,v)]\}, \quad (11)$$

由此不难看出，两个公钥已经被用作首次迭代过程中的两个加密密钥使用。

进一步，运用生成的两个解密密钥对密文进行解密。图中的振幅 A_3 可以表示为

$$g_k'(u,v) = \mathrm{PT}\{\mathscr{F}[E(x,y)P_k'(x,y)]\}. \quad (12)$$

在第 k 次迭代过程中最终获得的解密结果为

$$D_k(x,y) = \mathrm{PT}\{\mathscr{F}^{-1}[g'_k(u,v) \cdot P_k(u,v)]\}. \tag{13}$$

同时，在第 k 次迭代运算的解密过程中生成用于下一轮迭代的新的加密密钥 E_{K1} 和加密密钥 E_{K2}，它们分别可以写成

$$R_{k+1}(x,y) = \mathrm{PR}\{\mathscr{F}^{-1}[g'_k(u,v)P_k(u,v)]\}, \tag{14}$$

$$R'_{k+1}(u,v) = \mathrm{PR}\{\mathscr{F}[E(x,y)P'_k(x,y)]\}. \tag{15}$$

当迭代次数达到预设的值时，迭代过程结束。假定迭代 n 次后结束，由(10)、(11)式最终得到两个解密密钥 $P_n(u,v)$ 和 $P'_n(x,y)$。需要指出的是，由图 3可以看出，不同的明文将会对应不同的解密密钥，这意味着系统具有抵御选择明文攻击的能力。

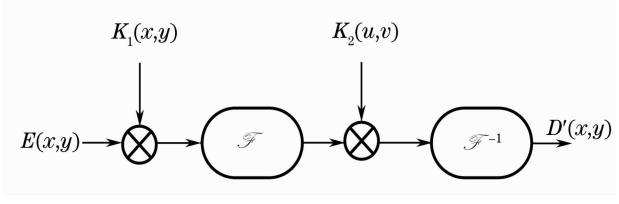

图 3　解密过程流程图

Fig. 3　Flowchart of the decryption process

3.2　图像的解密

由(12)式和(13)式可知，n 次迭代后得到的最终解密结果为

$$D_n(x,y) = \mathrm{PT}\{\mathscr{F}^{-1}\{\mathrm{PT}\{\mathscr{F}[E(x,y)P'_n(x,y)]\} \times P_n(u,v)\}\}, \tag{16}$$

为了提高解密的效率，本方法采用经典的双随机相位编码系统进行解密。如图 3 所示，令 $K_1(x,y)$、$K_2(u,v)$ 是本方法中用来解密的两个私有密钥，通过基于 $4f$ 系统的双随机相位编码技术进行解密后的结果可以表示为

$$D'(x,y) = \mathrm{PT}\{\mathscr{F}^{-1}\{\mathscr{F}[E(x,y)K_1(x,y)]\} \times K_2(u,v)\}. \tag{17}$$

式中两个私钥在加密过程中生成，它们的表达式分别为

$$K_1(x,y) = P'_n(x,y), \tag{18}$$

$$K_2(u,v) = P_n(u,v)[R'_{n+1}(u,v)]^*, \tag{19}$$

式中 * 表示复共轭运算。将(18)、(19)式代入(17)式，由(12)、(15)式不难证明 $D'(x,y) = D_n(x,y)$。由此，通过对迭代过程中生成的解密密钥进行调制后，实现了图像的线性解密。

由此可知，提出的加密方法可以看成是两个加密部分的组合，即“假图像”和两个公钥在非线性双随机相位加密系统中生成密文，以及该密文与原始图像在迭代的非线性双随机相位加密方法作用下产生两个私有密钥。对于前一组成部分，密文是通过利用“假图像”在公钥的作用下获得，反之，也以通过密文得到“假图像”。因此，对于攻击者而言，已知“假图像”等价于已知密文。对于后一组成部分，虽然两个公钥作为首次迭代过程中的两个加密密钥使用，但在其后的迭代循环过程中，加密密钥被不断更新并且最终生成两个解密密钥。因此，系统的安全性主要取决于后一加密部分。通过迭代算法的设计，保证了攻击者无法对两个解密密钥进行有效的破解，从而保证了整个加密系统的安全。

4　仿真实验及结果

在 Matlab R2009b 软件平台上，仿真测试了基于迭代非线性双随机相位编码的光学加密系统的可行性和安全性。选择大小均为 256 pixel×256 pixel 的归一化图像“Lena”和“screen”作为待加密图像和“假图像”，分别如图 4(a)、(b)所示。

图 4　(a)原始图像“Lena”；(b)假图像“Screen”

Fig. 4　(a) Primary image “Lena”; (b) fake image “Screen”

使用均方误差函数(MSE)衡量解密图像的品质以及迭代运算的收敛性。第 k 次迭代运算中得到的解密图像 $D_k(x,y)$ 与原始图像 $I(x,y)$ 之间的 MSE 值可以由下式得到：

$$M_{\mathrm{SE}}(I,D_k) = \frac{1}{M \times N}\sum_{i=1}^{M}\sum_{j=1}^{N}|I(i,j) - D_k(i,j)|, \tag{20}$$

式中 M,N 表示图像的尺寸，$I(i,j)$ 和 $D_k(i,j)$ 分别表示两幅图像在像素点(i,j) 的值。

由加密流程图图 1 得到的加密结果如图 5(a)所示，迭代运算 30 次后得到的两个私有密钥 K_1，K_2 的相位分布分别如图 5(b)、(c)所示。使用两个正确的私有密钥 K_1，K_2 对密文进行解密后得到的解密结果则如图 5(d)所示，它与原始图像之间的 M_{SE}值为 2.684×10^{-4}。从图 5(d)可以看出，原始图像已经得到了很好的恢复，很难从视觉上分辨出

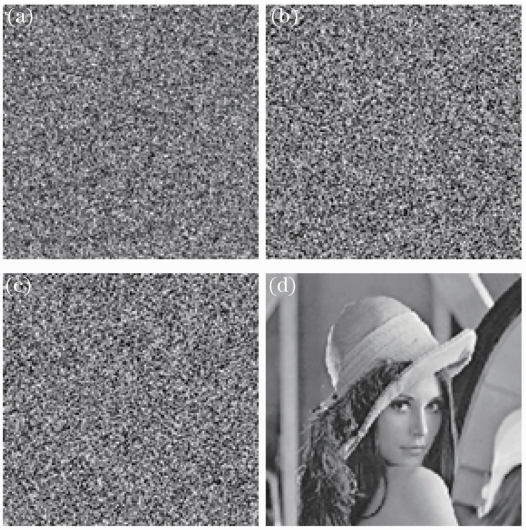

图 5 (a)加密结果 E；(b) K_1；(c) K_2；(d)正确的解密结果

Fig. 5 (a) Encrypted result E; (b) K_1; (c) K_2; (d) correctly decrypted result

解密图像与原始图像两者之间的区别。

加密过程中，$I(x,y)$和 $D_k(x,y)$的 M_{SE}值与迭代次数的关系图如图 6 所示. 可以看出，本加密方法的迭代过程收敛非常快，当迭代次数在 10 次以后，M_{SE}值基本保持不变。

为了考察迭代次数对解密效果的影响，给出了加密过程采用不同的迭代次数后，最终得到的解密结果。图 7(a)、(b)对应的加密过程中采用的迭代次数分别为 10、30，与之对应的 M_{SE}值则分别为 3.0079×10^{-4}和 2.684×10^{-4}。

下面讨论系统可能面临的攻击并进行相应的测试。首先是暴力攻击。当解密密钥 K_1 出错而 K_2 正确的情况下得到的解密结果如图 8(a)所示；当解密密钥 K_2 出错而 K_1 正确的情况下得到的解密结果则如图8(b)所示；当两个解密密钥都发生错误

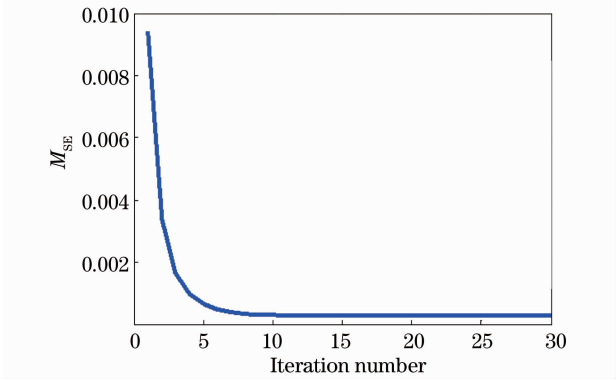

图 6 迭代加密过程中(I 和 D_k 之间的)M_{SE}值与迭代次数的关系图

Fig. 6 M_{SE} values between I and D_k with respect to iteration numbers

图 7 采用不同迭代次数加密时对应的正确解密结果。(a) 10 次；(b) 30 次

Fig. 7 Encrypted results corresponding to the iteration number of (a) 10 and (b) 30

时，得到的解密结果如图 8(c)所示。实验结果表明该加密系统能够抵抗住暴力攻击。对于已知明文攻击，即攻击者在掌握加密过程和解密过程的情况下，任意选择一幅不同于明文的“假图像”生成两个解密密钥，然后利用这两个“假密钥”进行解密。由加密过程流程图 1 和第 3 部分加密过程的说明很容易得知，解密结果恰恰是“假图像”自身。

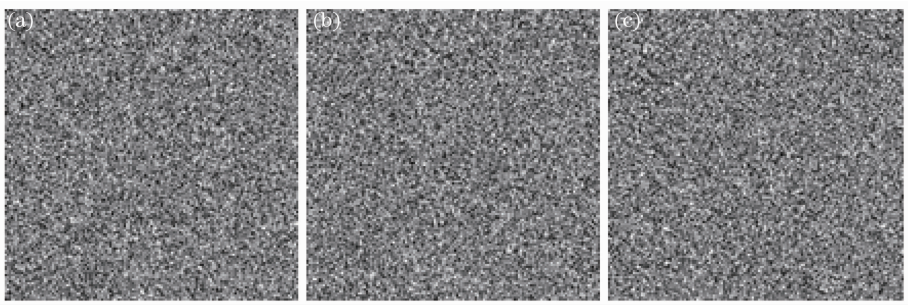

图 8 使用不正确的解密密钥得到的结果。(a) K_1 错误；(b) K_2 错误；(a) K_1、K_2 均错误

Fig. 8 Decrypted image with wrong keys. (a) Incorrect K_1; (b) incorrect K_2; (c) incorrect K_1 and K_2

接着研究令非线性双随机相位加密系统失效的基于改进的振幅-相位恢复算法攻击方法[22]。利用图 1 所示的振幅-相位恢复算法对本方法展开攻击。当迭代次数分别为 10 和 100 时，对应的攻击结果分

别如图 9(a)和 9(b)所示。可以看出，攻击的结果显示出的是“假图像”的信息。这充分表明所提出的加密方法不仅具有抵抗改进的振幅-相位恢复算法攻击的能力，还起到了误导攻击者的作用。

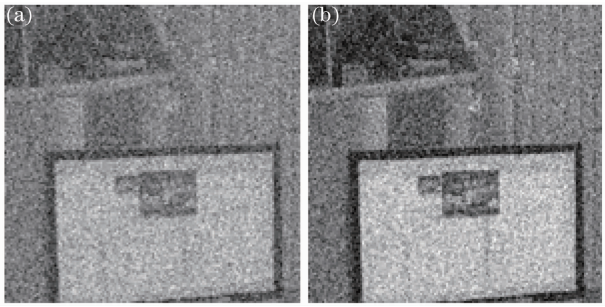

图 9　采用不同迭代次数进行攻击的结果。(a) 10 次；(b) 100 次

Fig. 9　Decrypted results corresponding to the iteration number of (a) 10 and (b) 100

5　结　　论

本文提出了一种基于迭代非线性双随机相位编码的图像加密方法。结合利用非线性双随机相位编码技术和迭代振幅-相位恢复算法，实现了加密密钥的更新，大大提高了系统的抗攻击能力。在该加密系统中，两个私有密钥在加密过程中生成，并且不同的明文对应于不同的解密密钥。由于解密过程具有线性的特点，因此可以通过光学系统，即经典的双随机相位编码系统实现光学解密。仿真实验充分表明该加密方法能够抵御最近提出的基于改进的振幅-相位恢复算法的攻击。

参　考　文　献

1 Peng Xiang, Wei Hengzheng, Zhang Peng. Introduction of Optical Information Security [M]. Beijing: Science Press, 2008. 5－7.
彭　翔，位恒政，张　鹏. 光学信息安全导论[M]. 北京：科学出版社，2008. 5－7.

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

3 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.

4 Banghe Zhu, Shutian Liu, Qiwen Ran. Optical image encryption based on multifractional Fourier transforms [J]. Opt Lett, 2000, 25(16): 1159－1161.

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

6 Guohai Situ, Jingjuan Zhang. Multiple-image encryption by wavelength multiplexing [J]. Opt Lett, 2005, 30(11): 1306－1308.

7 Ran Tao, Yi Xin, Yue Wang. Double image encryption based on random phase encoding in the fractional Fourier domain [J]. Opt Express, 2007, 15(24): 16067－16079.

8 Ran Tao, Jun Lang, Yue Wang. Optical image encryption based on the multiple-parameter fractional Fourier transform [J]. Opt Lett, 2008, 33(6): 581－583.

9 Zhengjun Liu, Lie Xu, Chuang Lin, *et al*.. Image encryption by encoding with a nonuniform optical beam in gyrator transform domains [J]. Appl Opt, 2010, 49(29): 5632－5637.

10 Zhengjun Liu, Qing Guo, Lie Xu, *et al*.. Double image encryption by using iterative random binary encoding in gyrator domains [J]. Opt Express, 2010, 18(11): 12033－12043.

11 Yishi Shi, Jingjuan Zhang. Research on the phase retrieval algorithm used for multiple-image encryption with region multiplexing [J]. Acta Optica Sinica, 2009, 29(10): 2705－2708.
史祎诗，张静娟. 相位恢复算法用于分区复用多图像加密的研究[J]. 光学学报，2009，29(10)：2705－2708.

12 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.

13 Qin Yi, Gong Qiong, Li Genquan, *et al*.. An optical encryption method with silhouette removal [J]. Chinese J Lasers, 2012, 39(12): 1209002.
秦　怡，巩　琼，李根全，等. 一种无轮廓像干扰光学加密系统[J]. 中国激光，2012，39(12)：1209002.

14 Qin Yi, Li Jing, Ma Maofen, *et al*.. System for optical multiple binary image encryption by random phase mask multiplexing [J]. Acta Optica Sinica, 2014, 34(3): 0307001.
秦　怡，李　婧，马毛粉，等. 一种基于随机相位板复用的光学多二值图像加密系统[J]. 光学学报，2014，34(3)：0307001.

15 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.

16 A Carnicer, M Montes-Usategui, S Arcos, *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.

17 Wenqi He, Xiang Peng, Xiangfeng Meng. A hybrid strategy for cryptanalysis of optical encryption based on double-random phase-amplitude encoding [J]. Opt & Laser Technol, 2012, 44(5): 1203－1206.

18 Wan Qin, Xiang Peng. Asymmetric cryptosystem based on phase-truncated Fourier transforms [J]. Opt Lett, 2010, 35(2): 118－120.

19 Wen Chen, Xudong Chen. Optical color image encryption based on an asymmetric cryptosystem in the Fresnel domain [J]. Opt Commun, 2011, 284(16-17): 3913－3917.

20 Wei Liu, Zhengjun Liu, Shutian Liu. Asymmetric cryptosystem using random binary phase modulation based on mixture retrieval type of Yang-Gu algorithm [J]. Opt Lett, 2013, 38(10): 1651－1653.

21 S K Rajput, N K Nishchal. Fresnel domain nonlinear optical image encryption scheme based on Gerchberg-Saxton phase-retrieval algorithm [J]. Appl Opt, 2014, 53(3): 418－425.

22 Xiaogang Wang, Yixiang Chen, Chaoqing Dai, *et al*.. Discussion and a new attack of the optical asymmetric cryptosystem based on phase-truncated Fourier transform [J]. Appl Opt, 2014, 53(2): 208－213.

栏目编辑：何卓铭