文章编号:2095-6134(2016)05-0604-08

双随机相位加密系统的无约束最优化攻击*

王国华[1,2], 李 拓[1,3], 张三国[1,2], 史祎诗[1,3†]

(1 中国科学院大学,北京 100049; 2 中国科学院大数据挖掘与知识管理重点实验室,北京 100049;
3 中国科学院光电研究院,北京 100094)

(2016 年 2 月 24 日收稿; 2016 年 3 月 31 日收修改稿)

Wang G H, Li T, Zhang S G, et al. Unconstrained optimization attack on double random phase cryptosystem[J]. Journal of University of Chinese Academy of Sciences, 2016,33(5):604-611.

摘 要 提出一种针对双随机光学相位加密系统的无约束最优化攻击算法.在已知明文条件下,首次将双随机相位加密系统的攻击问题转化为一个单目标无约束最优化模型.基于该模型,在相应的攻击算法设计中,采用拟牛顿矩阵代替 Hessian 矩阵以准确获取系统的密钥,避免传统牛顿法需要计算 Hessian 矩阵的逆等严重缺陷.同时,因有效利用拟牛顿矩阵的正定、对称、可迭代求逆的特点,新的攻击算法具有恢复效果好、收敛速度快、初值依赖弱、鲁棒性较强等优势.此外,本算法所需约束条件较少,可方便地移植到其他光学加密系统的攻击中.

关键词 光学信息安全; 双随机相位加密系统; 光学攻击; 非约束最优化

中图分类号:O438 **文献标志码**:A **doi**:10.7523/j.issn.2095-6134.2016.05.005

Unconstrained optimization attack on double random phase cryptosystem

WANG Guohua[1,2], LI Tuo[1,3], ZHANG Sanguo[1,2], SHI Yishi[1,3]

(1 *University of Chinese Academy of Sciences, Beijing* 100049, *China*; 2 *Key Laboratory of Big Data Mining and Knowledge Management, Chinese Academy of Sciences, Beijing* 100049, *China*; 3 *Academy of Opto-electronics, Chinese Academy of Sciences, Beijing* 100094, *China*)

Abstract An unconstrained optimization method is proposed to attack the double phase encryption system. Under the condition of knowing the plaintext, the new attack method builds an unconstrained optimization model and gets the accurate phase key via this model. Using the acquired phase key, the attacker decrypts the followed cipher. The new attack method transforms the problem of attacking the double phase encryption system into an unconstrained optimization model. The new attack method replaces Hessian matrix by quasi-Newton matrix to avoid computation of the reverse of Hessian matrix. The new attack method has fast convergence speed and strong robustness, and it is not too sensitive to the original values of the variables. This attack method can be applied to other encryption systems.

Key words optical information security; double random phase cryptosystem; optical attack; unconstrained optimization

* 国家自然科学基金(61575197)和中国科学院科学融合教育创新项目资助

† 通信作者,E-mail: shiyishi@ucas.ac.cn

近年来,随着光学理论的发展与加密技术的广泛应用,越来越多的研究开始集中于光学加密方法.在流行的光学加密方法中,双随机相位编码光学加密方法[1]一直受到人们的重视并在此基础上产出了大量的加密方法.但是由于双随机相位加密系统本质是一种线性系统,因此为破解提供了可能.至今为止,已经有大量的攻击方法[2-13]在不同条件下成功实现了对双随机相位加密系统的破解,这些方法主要分为选择密文攻击[2]、选择明文攻击[3-5]、已知明文攻击[6-12]及唯密文攻击[13].此外,还有一些其他的破解方法[14-16]用于光学加密系统的破解.在已知明文攻击算法中,Peng 等[3]提出的方法取得了较好的效果,但是有时恢复出的相位信息并不非常精确,而且在明文、密文变化后,仍需要重新进行破解.Gopinathan 等[10]利用模拟退火算法对双随机相位系统进行攻击,但是这种算法速度稍慢.

本文在已知明文的条件下,从数学中的最优化理论[17-23]出发,结合双随机相位加密系统的特点,首次将攻击问题转化为一个单目标无约束最优化问题.在双随机相位加密系统的破解过程中,由于最优化问题没有约束,所以可以采用传统的牛顿法进行求解.但传统的牛顿法由于要计算 Hessian 矩阵的逆矩阵,因而收敛速度较慢.我们针对 Hessian 矩阵正定、对称的特点,提出构造一个同样正定、对称的拟牛顿矩阵,并且拟牛顿矩阵能够通过迭代的方式快速求出逆矩阵.在迭代过程中,使用拟牛顿矩阵代替 Hessian 矩阵,可以极大地缩短计算时间,并且能够快速地收敛至目标函数最优值.该方法在目标函数为凸函数的情况下,能够表现出全局收敛性与超线性收敛速度[17-18].模拟实验表明,在已知明文条件下,新的攻击方法能够准确、快速地破解双随机相位加密系统,而且表现出较强的鲁棒性.该攻击方法与其他攻击方法相比,仅仅需要构造一个无约束最优化函数,对于其他的条件要求较少,以方便地推广到其他加密系统的攻击当中,因此具有一定的普遍意义.

1　双随机相位加密系统及其已知明文攻击

1.1　双随机相位加密系统

双随机位相系统是一个经典的加密系统,采用标准的 4f 系统来实现.在加密系统中,$t(x^*,y^*)$代表一个 $N\times N$ 的物体.它可以是物面上的任何一个场,也可以是自由空间中传播的复光场.同时,$\boldsymbol{P}=(p_{il})$ 和 $\boldsymbol{B}=(b_{il})$ 代表 2 个相互独立的[0, 1]之间的均匀分布矩阵.加密过程中,信号 $t(x^*,y^*)$接受第 1 块相位板的随机相位调制,经过傅里叶变换后,接着在频率域被第 2 块相位板调制,再次经傅里叶变换,得到振幅与相位均为白噪声分布的加密场 $u(x^*,y^*)$,整个过程可以表示为

$$u(x^*,y^*)=F\{F\{t(x^*,y^*)\exp[\mathrm{j}2\pi\boldsymbol{P}]\}\exp[\mathrm{j}2\pi\boldsymbol{B}]\},\tag{1}$$

其中,F 表示傅里叶变换.加密过程中,相位矩阵 $\boldsymbol{P}$ 和 $\boldsymbol{B}$ 是随机产生的,因此整个过程具有较高的安全性.对应的解密过程可以表示为

$$t(x^*,y^*)=\left\|F^{-1}\{F^{-1}(u(x^*,y^*))\exp[-\mathrm{j}2\pi\boldsymbol{B}]\}\right\|.\tag{2}$$

首先,将输出的密文 $u(x^*,y^*)$ 进行傅里叶逆变换,然后与 $\exp[\mathrm{j}2\pi\boldsymbol{B}]$ 逆相乘,并再次进行傅里叶逆变换,得到原始图像 $t(x^*,y^*)$ 与相位函数的乘积 $t(x^*,y^*)\exp[\mathrm{j}2\pi\boldsymbol{P}]$,由于通常我们只对恢复图像的振幅感兴趣,因此直接取振幅信息(通过 CCD 强度探测器等方法)就可以得到原始图像.

1.2　针对双随机相位的已知明文攻击的无约束最优化数学模型

在进行整个加密系统破解之前,我们认为攻击者已经掌握若干密文(加密后的图像),并且还知道对应的明文(原始图像).假设攻击者取出其中的一个明文密文对 $\{t(x^*,y^*),u(x^*,y^*)\}$,其中 $t(x^*,y^*)\in R^{N\times N}$ 为明文,$u(x^*,y^*)\in C^{N\times N}$ 为密文.由双随机相位加密系统的加密过程可知,若能获取 2 个相位板 P 与 B 中的信息,便能够破解整个加密系统.因此根据式(1),首先将整个解密过程转化为一个带有约束的最优化问题:

最优化模型 Ⅰ
$$\min_{P,B}\|Q(\boldsymbol{P},\boldsymbol{B})-u(x^*,y^*)\|,\tag{3}$$
$$Q(\boldsymbol{P},\boldsymbol{B})=F\{F\{t(x^*,y^*)\exp[\mathrm{j}2\pi\boldsymbol{P}]\}\exp[\mathrm{j}2\pi\boldsymbol{B}]\},$$
$$0\leqslant p_{il}\leqslant 1,i=1,\cdots,N,l=1,\cdots,N,$$
$$0\leqslant b_{il}\leqslant 1,i=1,\cdots,N,l=1,\cdots,N.$$

正确的相位矩阵 $\boldsymbol{P}$ 与 $\boldsymbol{B}$ 的值必然会使式(3)取得最小值 0,因此通过求解最优化模型 Ⅰ,便

可以获得正确的密钥,进而破解整个加密系统. 由于 $Q(\boldsymbol{P},\boldsymbol{B})$ 中包含了 $2N^2$ 个未知量, 为计算方便,将这 2 个矩阵按照字母表的顺序拉成 2 个 $1\times N^2$ 的向量,再拼接成一个 $1\times 2N^2$ 的长向量,把这个长向量作为式(3)的自变量. 例如,若 $\boldsymbol{P}$ 与 $\boldsymbol{B}$ 均为 2×2 的矩阵,则按照此规则产生的自变量 $\boldsymbol{x}$ 为:

$$\boldsymbol{P}=\begin{pmatrix}p_{11} & p_{12}\\ p_{21} & p_{22}\end{pmatrix},\boldsymbol{B}=\begin{pmatrix}b_{11} & b_{12}\\ b_{21} & b_{22}\end{pmatrix},$$

$$\boldsymbol{x}=(p_{11},p_{21},p_{12},p_{22},b_{11},b_{21},b_{12},b_{22})^{\mathrm{T}}.$$

在解出正确的 $\boldsymbol{x}$ 后,再将 $\boldsymbol{x}$ 重新排列,即可获得正确的 $\boldsymbol{P}$ 与 $\boldsymbol{B}$ 的值. 由于最优化模型Ⅰ是一个有约束的非凸问题,一般情况下,这种问题的解法是转化为它的对偶问题并求出 KKT 点,或是通过坐标下降法寻找解析解. 但是由于问题中约束条件的限制,很多方法都会对目标函数做一些假设,例如单峰、连续、可微,而且利用局部展开性质确定的搜索方向会与优化函数整体最优解的目标产生抵触,因而常常不能得到理想的结果. 其他的一些启发式算法在训练模型时会消耗大量的时间,导致整个算法的效率不高. 与有约束的最优化问题相比,无约束的最优化问题相对更容易求解. 常用的无约束优化算法如牛顿法、信赖域法、共轭梯度法、坐标下降法等,这些方法对优化问题的要求较少,可以比较方便地求解. 因此我们希望将最优化模型Ⅰ转化为一个无约束的最优化问题.

为了将最优化模型Ⅰ转化为一个无约束问题,引入正弦函数的平方,将自变量的值通过正弦函数的平方全部转化为 [0,1] 之间,因此可以满足原有的约束条件. 在这种变换下,整个最优化问题变为:

$$\text{最优化模型 Ⅱ}\quad \min_{x}\|f(x)\|, \tag{4}$$

$$\begin{aligned}f(x)&=F\{F\{t(x^*,y^*)\exp[\mathrm{j}2\pi\boldsymbol{P}]\}\\&\quad\exp[\mathrm{j}2\pi\boldsymbol{B}]\}-u(x^*,y^*),\\ \boldsymbol{x}&=(x_1,x_2,\cdots,x_{2N}),\\ p_{il}&=\sin^2(x_{N\times(l-1)+i}),\\ b_{il}&=\sin^2(x_{N^2+N\times(l-1)+i}),\\ i&=1,\cdots,N,l=1,\cdots,N.\end{aligned}$$

从最优化模型Ⅱ的构造方式可以看出,最优化模型Ⅱ的解一定也是最优化模型Ⅰ的解. 虽然最优化模型Ⅱ是一个多解问题,但只需要取它的任一组解,然后通过正弦函数转化为相位矩阵的真实值即可. 由于最优化模型Ⅱ是一个单目标无约束的最优化问题,因此在计算时需要较少的假设,方便求解. 由此将原始的双随机相位系统破解问题(2)转化为了一个单目标的无约束最优化问题. 通过求解最优化模型Ⅱ,便能够获得完整的相位板信息,从而破解整个加密系统.

2 无约束最优化攻击算法

无约束最优化模型Ⅱ是一个类似于二次型的优化函数,但是在相位矩阵 $\boldsymbol{P}$ 与 $\boldsymbol{B}$ 中,优化变量是以指数形式出现的,因此传统的二次型优化求解方法在这里并不适用. 针对未知变量的这个特点,本文引入拟牛顿矩阵来寻找最优化模型Ⅱ的最小值. 新的攻击算法是一种类似于牛顿法的非线性优化算法. 牛顿法需要计算 Hessian 矩阵的逆矩阵,在变量个数较多的情况下,这需要很大的计算量,会使算法的计算速度大幅下降,收敛速度也相应变慢. 在双随机相位板加密系统中,即使是 10×10 的相位板,变量个数也达到 200 个,因此利用牛顿法会非常耗时. 针对牛顿法需要计算 Hessian 矩阵的逆矩阵的劣势,新的攻击算法引入拟牛顿矩阵,这个矩阵一方面保留了 Hessian 矩阵对称、正定等主要特性,另一方面在每次迭代时,拟牛顿的逆矩阵可以通过迭代快速求出,避免直接计算逆矩阵而带来的巨大运算量.

下面详细阐述无约束最优化模型Ⅱ的算法过程:

步骤 1 选择初值 $\boldsymbol{x}_0$, 设置初始叠代次数 $k=0$,并设置最大迭代次数 K.

步骤 2 定义一个搜索方向 $\boldsymbol{d}_k$, 沿该方向 $\boldsymbol{x}_k$ 的值是减少的,并有

$$\begin{aligned}\boldsymbol{B}_0&=\boldsymbol{I},\\ \boldsymbol{d}_k&=-\boldsymbol{H}_k\boldsymbol{g}_k,\\ \boldsymbol{B}_{k+1}&=\boldsymbol{B}_k-\frac{\boldsymbol{B}_k\boldsymbol{s}_k\boldsymbol{s}_k^{\mathrm{T}}\boldsymbol{B}_k}{\boldsymbol{s}_k^{\mathrm{T}}\boldsymbol{B}_k\boldsymbol{s}_k}+\frac{\boldsymbol{y}_k\boldsymbol{y}_k^{\mathrm{T}}}{\boldsymbol{s}_k^{\mathrm{T}}\boldsymbol{y}_k},\\ \boldsymbol{H}_{k+1}&=\boldsymbol{H}_k-\frac{\boldsymbol{H}_k\boldsymbol{y}_k\boldsymbol{s}_k^{\mathrm{T}}+\boldsymbol{s}_k\boldsymbol{y}_k^{\mathrm{T}}\boldsymbol{H}_k}{\boldsymbol{y}_k^{\mathrm{T}}\boldsymbol{s}_k}+\\ &\quad\left(1+\frac{\boldsymbol{y}_k^{\mathrm{T}}\boldsymbol{H}_k\boldsymbol{y}_k}{\boldsymbol{s}_k^{\mathrm{T}}\boldsymbol{y}_k}\right)\frac{\boldsymbol{s}_k\boldsymbol{s}_k^{\mathrm{T}}}{\boldsymbol{s}_k^{\mathrm{T}}\boldsymbol{y}_k}.\end{aligned}$$

步骤 3 定义步长,利用 Wolfe 算法确定步长 α, 使得 $f(\boldsymbol{x}_k+\alpha\boldsymbol{d}_k)$ 在该方向上函数值下降,并且构造 $\boldsymbol{x}_{k+1}=\boldsymbol{x}_k+\alpha\boldsymbol{d}_k$, 一般来说, α 的计算要满足以下 2 个条件:

$$f(\boldsymbol{x}_k) - f(\boldsymbol{x}_k + \alpha \boldsymbol{d}_k) \geqslant -\alpha b_1 \boldsymbol{d}_k^{\mathrm{T}} \nabla f(\boldsymbol{x}_k),$$

$$\boldsymbol{d}_k^{\mathrm{T}} \nabla f(\boldsymbol{x}_k + \alpha \boldsymbol{d}_k) \geqslant b_2 \boldsymbol{d}_k^{\mathrm{T}} \nabla f(\boldsymbol{x}_k).$$

其中,b_1 和 b_2 是 2 个常数且满足 $0 < b_1 \leqslant b_2 < 1$. 第 1 个不等式保证选择的步长会使函数值下降,第 2 个不等式保证步长不会太小. 这样的步长选择方法能够快速选择出合适的步长. 一般采用二次差值的方法求出步长 α.

步骤 4　若 $k \geqslant K$,停止并输出一个 $\boldsymbol{x}_{k+1}$,否则设 $k = k + 1$,并且重复步骤 2—3,直至迭代满足条件.

在仅有一组明文密文对的情况下,有时需要进行多次求解. 由于在密钥准确的时候,目标函数 $f(x)$ 的值必然为 0,因此在模拟实验中,通过观测目标函数 $f(x)$ 的值,可以确定获得的密钥是否为正确的密钥. 一般来说,新的攻击方法一般 3 ~ 4 次求解就可以确定出密钥的准确值.

3　模拟实验及其分析

假定攻击者已经掌握一个明文密文对,明文为灰度图(10 像素 × 10 像素,256 灰阶),如图 1(a)所示,对应的经过双随机相位加密系统加密后的密文如图 1(b)所示. 利用均方误差 MSE 与相关系数 Co 来比较恢复值与原始值之间的差异. 恢复值的 MSE 与相关系数 Co 的计算公式如下:

$$\mathrm{MSE}(\boldsymbol{x}_1, \boldsymbol{x}_2) = \frac{\|\boldsymbol{x}_1 - \boldsymbol{x}_2\|_2}{\sqrt{n}},$$

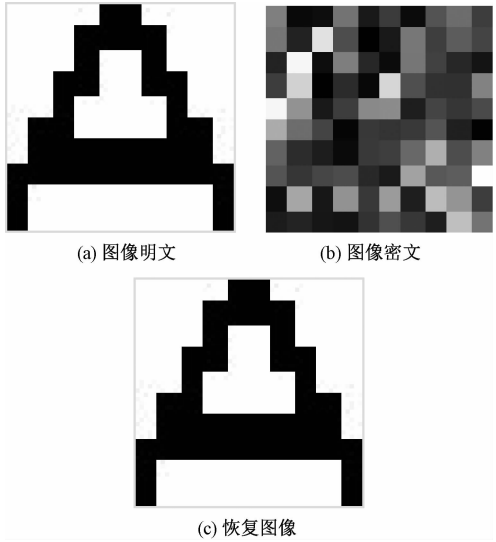
$$Co(\boldsymbol{x}_1, \boldsymbol{x}_2) = \frac{\boldsymbol{x}_1 \cdot \boldsymbol{x}_2}{\|\boldsymbol{x}_1\|_2 \|\boldsymbol{x}_2\|_2},$$

其中,$\boldsymbol{x}_1$ 是原始值,$\boldsymbol{x}_2$ 是恢复值,n 为 $\boldsymbol{x}_1$ 的维数. 实验环境为英特尔 i7 CPU,主频为 2.2 GHz,8 G 内存,软件为 Matlab 2013a.

3.1　基本结果分析

我们采用无约束最优化的攻击方法对加密系统进行攻击. 新的攻击算法在攻击过程中,每一次迭代运算都需要选择在下降方向上前进的步长. 步长的选择方法分为精确法和非精确法. 精确法是精确地算出使函数在下降方向下降最多的步长,但是在大型计算中,这种精确求出步长的方法计算量很大,计算效率很低,而且很多问题中,并不需要每次都解出精确的步长. 一般的非精确步长选择方法有 Armijo 法、Wolfe 法等,这些方法的步长选择标准都是保证每次选取的步长一定让函数值下降,同时保证步长不能太小. Armijo 法比较简单,选择速度快,但有可能将最优的步长排除在选择范围之外;Wolfe 法是 Armijo 法的改进,保证了最优步长一定在备选区间之中. 所以在整个模拟实验过程中,我们选择 Wolfe 搜索法确定步长.

在攻击中,我们将初始相位矩阵中的值全部设定为 1,并且进行 500 次迭代计算,得到相位板的恢复信息,并利用恢复的相位信息得到原始图像. 图 1(c)为利用破解的相位板信息得到的恢复图像,从图中看出,它与原始图像的相似度非常高. 图 2 表示的是在 500 次迭代过程中,恢复的密钥信息与原始密钥的均方误差与相关系数,图 2(a)显示在迭代次数达到 200 次后,恢复的密钥与原始密钥的均方误差就已经小于 0.001,而图 2(b)则显示在 200 次迭代后,恢复密钥与原始密钥的相关系数为 0.82,并且已经达到平稳. 整个攻击过程(迭代 500 次)的耗时为 308 s,这说明我们的攻击算法具有很快的破解速度. 同时,当采用[0,1]之间的均匀分布作为初始值的时候,多次模拟也都准确恢复出了原始图像,这说明我们的攻击方法具有较弱的初值依赖性. 在模拟中,可以固定初始值,这样能够避免因设置随机初值而造成的不稳定情况.

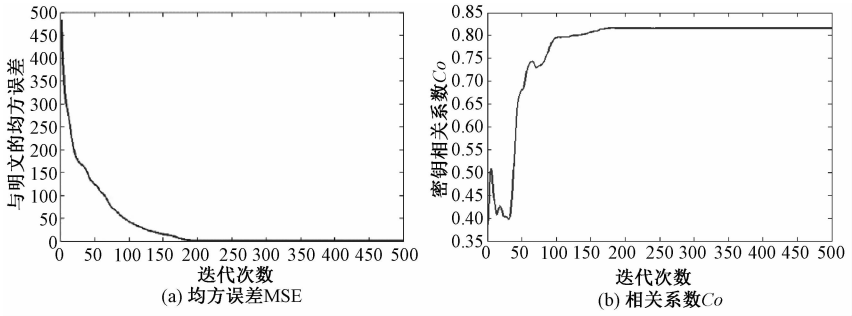


(a) 图像明文　(b) 图像密文　(c) 恢复图像

图 1　对二值图像的攻击结果

Fig. 1　Result of attacking two-value figure

在密钥不变的情况下,选择 10 像素 × 10 像素的灰度图像来测试恢复效果,结果如图 3 所示. 与真实图像相比较,可以发现恢复图像的 MSE 已经小于 0.001,而二者的相关系数达到 0.898,因

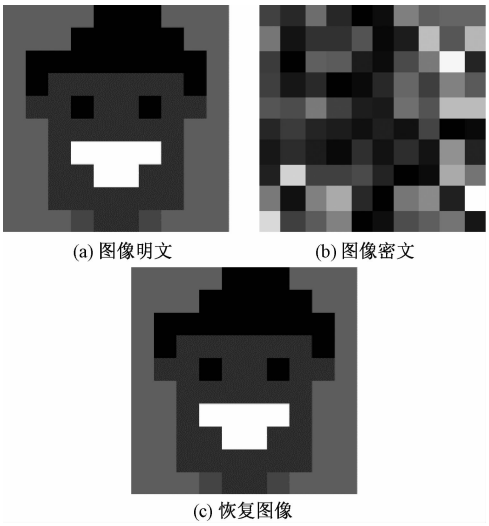


(a) 均方误差MSE (b) 相关系数Co

图 2 恢复的相位板信息的 MSE 与相关系数随迭代次数收敛的情况

Fig. 2 Convergency of MSE and correlation with iteration number

此恢复质量非常好. 这说明利用新的攻击方法而获得的密钥也可以很好地恢复被同样密钥加密的灰度图像.



(a) 图像明文 (b) 图像密文 (c) 恢复图像

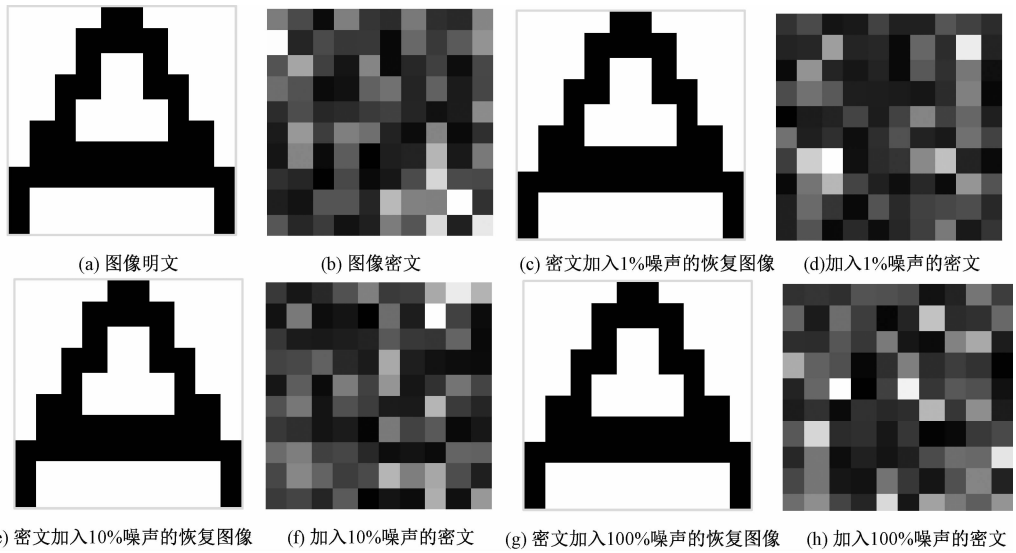
图 3 灰度图像攻击测试

Fig. 3 Test for grayscale figure

上述模拟表明,新的攻击方法具有攻击速度快、恢复效果好、算法稳定等优势. 而且通过攻击二值图像获得的密钥,也同样可以用于恢复被相同密钥加密的灰度图像,这个特性降低了破解难度,也使得破解出的密钥有较广泛的应用范围.

3.2 性能提升分析

为测试新的攻击算法的抗干扰性能,在原来的二值图像密文中加入噪声,观察新的攻击算法的恢复效果. 依然选用图 1 作为明文密文对,并在密文中分别加入 1%、10% 与 100% 的均匀分布 $U[0,1]$ 噪声,恢复结果如图 4 所示. 从图中可以看出,3 幅恢复图像都能很好地还原原始图像的主要信息,且边缘清晰,信息丢失少. 实验表明,在 3 种噪声水平下,随着迭代次数的增加,破解出的密钥与真实密钥的均方误差迅速减小,在 200 次后均小于 0. 1,真实密钥与恢复密钥的相关系数也一直保持在 0. 8 以上,这充分说明恢复出的密



(a) 图像明文 (b) 图像密文 (c) 密文加入1%噪声的恢复图像 (d)加入1%噪声的密文

(e) 密文加入10%噪声的恢复图像 (f) 加入10%噪声的密文 (g) 密文加入100%噪声的恢复图像 (h) 加入100%噪声的密文

图 4 密文加入不同程度均匀分布噪声 $U[0,1]$ 的已知明文攻击

Fig. 4 Known plaintext attack with different levels of uniform noise $U[0,1]$ added on the ciphertext

钥的准确性. 整个破解过程快速,且每个模拟均能够一次恢复出结果,这说明新的攻击方法具有较好的鲁棒性.

再将破解出的密钥应用于灰度图像的恢复上,测试新的算法在灰度图像恢复中的鲁棒性能. 在图 5 中,采用 2 幅不同的灰度图像进行测试,并使用 100% 的噪声水平做干扰. 从结果可以看到,在 100% 噪声水平下,利用破解出的密钥均能准确地恢复出真实地灰度图像,并且在边缘细节的恢复上也有很好的表现. 进一步分析显示,2 幅还原的灰度图像与真实图像的 MSE 均小于 0.5,而相关系数也都在 0.73 以上,达到非常高的水平,也表明了破解出的密钥的准确性. 以上模拟结果充分说明利用新的无约束最优化攻击算法获取的密钥同样可以很好地恢复灰度图像,且具备较强的鲁棒性.

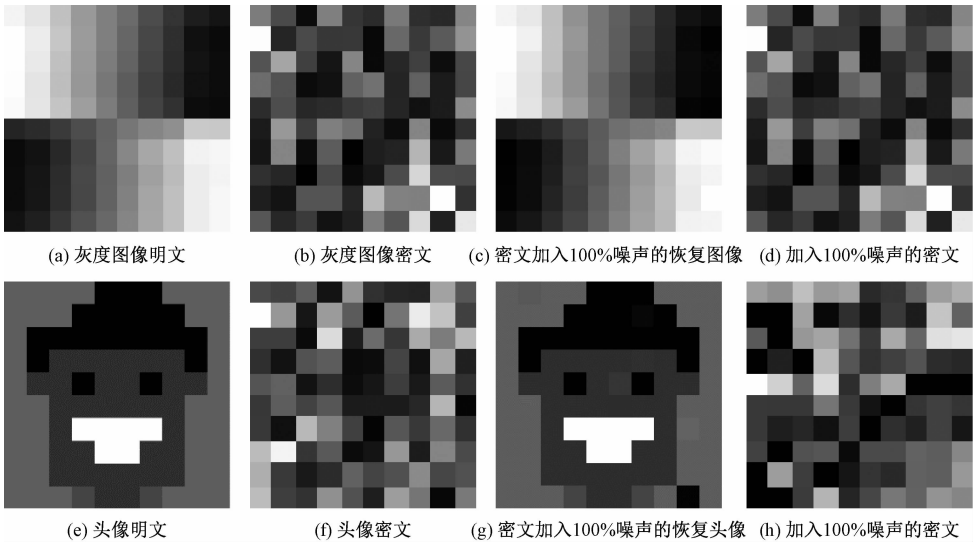


图 5　灰度图像密文加入 100% 均匀分布噪声 $U[0,1]$ 的已知明文攻击

Fig. 5　Known plaintext attack with 100% of uniform noise $U[0,1]$ added on the ciphertext of grey scale figure

除均匀分布噪声,我们还在密文中加入不同程度的高斯分布 $N[0,1]$ 噪声,获得了与密文中加入均匀分布噪声相似的攻击结果. 这说明新的攻击方法在密文加入多种噪声类型的情况下中均能较好恢复出真实图像,表现出很好的可移植性与鲁棒性.

之前的分析表明新的攻击算法具有很好的鲁棒性与可移植性,接下来,分析新的攻击算法对于丢失数据的补偿能力. 依然假设已知一对明文、密文对,并在密文中随机丢弃一部分的信息,观测新的攻击算法的破解效果. 如图 6 所示,比较真实图像与恢复的图像,可以看到在这两种密文信息缺失水平下,恢复的二值图像依然还原了真实图像的主要信息,虽然背景有些模糊,但是边缘清晰,具有很高的辨识度,显示出较高的恢复水平. 实验表明,破解的密钥在迭代 200 次后也达到了稳定,最终 MSE 均小于 10,而且破解密钥与原始密钥的相关系数也分别稳定在 0.8 与 0.7. 整个破解过程用时稍长于密文没有信息缺失的情况,而且两种密文缺失水平下,3 次就能破解出密钥,说明新的攻击算法在密文缺失一部分信息的情况下依然能够稳健地恢复出真实图像,具有一定的抗信息丢失的能力. 图 6(i) 显示利用获得的密钥攻击密文有 5% 信息缺失的灰度图像的结果. 从图中可看到恢复出的灰度图像依然能够还原出一部分原始图像的信息,但是模糊情况较为严重. 恢复图像的 MSE 为 31.1,而 2 幅图像的相关系数则为 0.581. 这说明密文的信息缺失对于灰度图像的恢复影响较为明显,这主要由于灰度图像的灰阶较多,包含的信息更为复杂,所以密文信息的丢失对于图像的恢复影响较为强烈.

以上模拟分析表明,新的攻击算法具有较强的抗噪能力与一定的抗信息丢失能力. 在不同类型与不同程度的噪音水平下,新的攻击算法均能快速准确地破解出真实的密钥,而且可以将密钥用于其他二值图像与灰度图像的恢复中,这说明新的攻击算法具有良好的可移植性. 同时在密文缺失部分信息的情况下,虽然新的攻击算法在灰

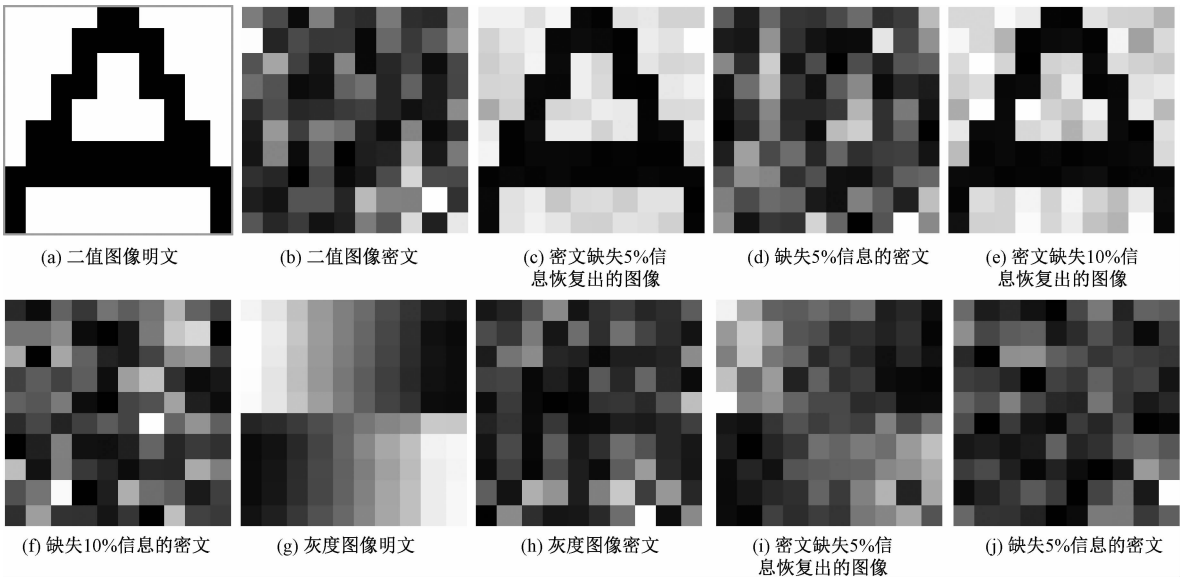


图 6 密文缺失不同程度信息的已知明文攻击

Fig. 6 Known plaintext attack with ciphertext missing different levels of information

度图像的恢复中表现稍差,但是在二值图像的恢复中有良好的表现,因此还是具备一定的抗信息丢失能力的.

4 结论

本文提出针对双随机相位加密系统的无约束最优化攻击算法. 我们将双随机相位加密系统的攻击问题转化为一个单目标无约束最优化模型,并在相应的攻击算法设计中,采用拟牛顿矩阵代替 Hessian 矩阵以准确获取系统的密钥,同时充分利用拟牛顿矩阵正定、对称、可迭代求逆的特点. 从而,本法使得攻击者只需通过一对明文、密文对, 即可获得 4*f* 系统输入平面的随机相位函数密钥和频谱平面的随机相位函数密钥. 模拟结果表明,新的攻击算法恢复效果好、收敛速度快、初值依赖弱、鲁棒性较强. 因本法所需约束条件较少,或可移植于其他光学加密系统的攻击中而具有一定的普遍价值.

参考文献

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

[2] Arturo C, Mario M U, Sergio A, et al. Vulnerability to chosen-cyphertext attacks of optical encryption schemes based on double random phase keys[J]. Optics Letters, 2010, 30(30): 1 644-1 646.

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

[4] He W Q, Peng X, Meng X F. A hybrid strategy for cryptanalysis of optical encryption based on double-random phase-amplitude encoding [J]. Optics & Laser Technology, 2012, 44(5): 1 203-1 206.

[5] He W Q, Peng X, Meng X F, et al. Collision in optical image encryption based on interference and a method for avoiding this security leak [J]. Optics & Laser Technology, 2013, 47(47): 31-36.

[6] Situ G H, Peolrini G, Osten W. Strategy for cryptanalysis of optical encryption in the Fresnel domain[J]. Applied Optics, 2010, 49(3): 457-462.

[7] Peng X, Zhang P, Wei H Z, et al. Known-plaintext attack on optical encryption based on double random phase keys [J]. Optics Letters, 2006, 31(8): 1 044-1 046.

[8] John Fredy B, Carlos V, Myrian T, et al. Known-plaintext attack on a joint transform correlator encrypting system [J]. Optics Letters, 2010, 35(21): 3 553-3 555.

[9] Wang X G, Chen Y X, Dai C Q, et al. Discussion and a new attack of the optical asymmetric cryptosystem based on phase-truncated Fourier transform [J]. Applied Optics, 2014, 53(2): 208-213.

[10] Gopinathan U, Monaghan D S, Naughton T J, et al. A known-plaintext heuristic attack on the Fourier plane encryption algorithm [J]. Optics Express, 2006, 14(8): 3 181-3 186.

[11] Yann F, Albertina C, Naughton T J, et al. Resistance of the double random phase encryption against various attacks [J]. Optics Express, 2014, 15(16): 10 253-10 265.

[12] Li T, Wang Y L, Zhang J, et al. Analytic known-plaintext

attack on a phase-shifting interferometry-based cryptosystem [J]. Applied Optics, 2015, 54(2): 306-311.

[13] Zhang C G, Liao M H, He W Q, et al. Ciphertext-only attack on a joint transform correlator encryption system [J]. Optics Express, 2013, 21(23): 28 523-28 530.

[14] 史祎诗, 王雅丽, 肖俊,等. 基于位相抽取的三维信息加密算法研究 [J]. 物理学报, 2011, 60(3): 236-241.

[15] 刘祥磊, 潘泽, 王雅丽, 等. 基于叠层衍射的数字水印算法研究 [J]. 物理学报, 2015, 64(23): 234201.

[16] Li T, Shi Y S. Security risk of diffractive-imaging-based optical cryptosystem [J]. Optics Express, 2015, 23(16): 21 384-21 391.

[17] Fukushima M, Li D H. On the global convergence of the bfgs method for nonconvex unconstrained optimization problems [J]. Siam J Optim Vol, 2001, 11(4): 1 054-1 064.

[18] Liu D C, Nocedal J. On the limited memory BFGS method for large scale optimization [J]. Mathematical Programming, 1989, 45(3): 503-528.

[19] Hoffmann K H, Christoph M, Hanf M. Optimizing simulated annealing [C] // Parallel Problem Solving from Nature. Springer Berlin Heidelberg, 1991: 221-225.

[20] Romeijn H E, Smith R L. Simulated annealing for constrained global optimization [J]. Journal of Global Optimization, 1994, 5(2): 101-126.

[21] Anthony M, Bartlett P L. Neural network learning: theoretical foundations[J]. Ai Magazine, 2001, 22(2): 99-100.

[22] Jones G, Willett P, Glen R C, et al. Development and validation of a genetic algorithm for flexible docking [J]. Journal of Molecular Biology, 1997, 267(3): 727-748.

[23] Deb K, Pratap A, Agarwal S, et al. A fast and elitist multiobjective genetic algorithm: NSGA-II, IEEE Trans. on Evol [J]. IEEE Transactions on Evolutionary Computation, 2002, 6(2): 182-197.