非线性JTC光学图像加密系统及其消噪音和抗攻击特性研究

沈学举 刘旭敏 蔡 宁 蔡建俊 鲁 军
军械工程学院, 河北 石家庄 050003

摘要 分析联合变换相关器(JTC)光学加密系统解密图像噪音大、质量差的原因,提出一种非线性JTC光学加密系统。将JTC加密图像除以密钥功率谱作为新加密图像。一方面,新加密图像能够消除密钥傅里叶谱振幅分布不均匀引起的噪音,提高解密图像质量。仿真结果表明,Lena图像的消噪音解密图像和原始图像的相关系数可由0.4104增加到0.7190,均方根(RMS)从0.8154减小到0.7089。二值文本图像的消噪音解密图像和原始图像的相关系数由0.8458增加到0.9785,RMS从0.6887减小到0.4583;另一方面,新加密图像能抵御唯密文攻击(COA)算法的攻击,仿真结果表明,利用COA算法能从JTC加密图像恢复出高质量的原始图像信息,但不能从新加密图像恢复出任何原始图像信息,有效提高JTC加密系统的安全性。

关键词 图像处理; 光学图像加密; 联合变换相关; 密钥功率谱; 消噪音; 唯密文攻击
中图分类号 O438.1; TN911.74 **文献标识码** A
doi: 10.3788/CJL201542.0709003

Nonlinear Image Encryption System Based on JTC and Its Removing Noise and Resisting Attack Properties Research

Shen Xueju Liu Xumin Cai Ning Cai Jianjun Lu Jun
Ordnance Engineering College, Shijiazhuang, Hebei 050003, *China*

Abstract By analyzing the reason of big noise and low quality of decryption image in the joint transform correlation (JTC) encryption system, a kind of nonlinear JTC image encryption system is proposed. A new encryption image is obtained when JTC encryption image is divided by key power spectrum. On the one hand, new encryption image can remove noise caused by amplitude non-uniformity of key Fourier spectrum and improve the quality of decryption image. Simulation results show that the correlation coefficient between new Lena decryption image and original image increases from 0.4104 to 0.7190 and root mean square (RMS) value decreases from 0.8154 to 0.7089, and that the correlation coefficient between new binary text decryption image and original image increases from 0.8458 to 0.9785 and RMS value decreases from 0.6887 to 0.4583. On the other hand, new encryption image can resist chiphertext only attack (COA) arithmetic attack. Simulation results show that using the COA arithmetic, high quality original image can be restored from JTC encryption image, but information of original image can not be obtained from new encryption image. This system improve the security of JTC encryption system effectively.

Key words image processing; optical image encryption; joint transform correlation; key power spectrum; removing noise; ciphertext-only attack
OCIS codes 100.0100; 070.0070; 090.0090

1 引 言

Refregier等[1]提出双随机相位编码光学图像加密方法,由于该加密系统在结构上是4*f*系统,要求两相位模板在空间位置上精确对准;解密密钥是加密密钥的复共扼,实际中很难制作;输出加密图像为复振幅分

收稿日期: 2014-12-29; **收到修改稿日期**: 2015-03-18
基金项目: 河北省自然基金项目(F2014506004)
作者简介: 沈学举(1963—),男,教授,博士生导师,主要从事激光技术等方面的研究。E-mail: shxjoptics@aliyun.com

布，难以记录和传输，可实施性差。随着研究的深入，人们探索了多种光学图像加密方法[2-10]，白音布和等[6]提出了一种基于光学衍射成像原理的图像加密方法，只需记录单幅强度图像，不需要干涉装置，可提高记录效率；陈翼翔等[7]提出了一种基于双随机相位编码技术的非线性双图像加密方法，安全性更高，能抵御基于两步振幅相位恢复算法的特定攻击；朱薇等[8]针对菲涅耳域双随机相位编码提出了一种改进图像加密系统，在减小密钥体积的同时增大了密钥空间、增加了系统的复杂性。而Nomura等[9-10]提出的基于联合变换相关器(JTC)的光学加密系统，由于其不需要制作复共扼密钥，密钥模板不需要精确对准，加密图像为联合功率谱，是强度图像，方便记录和传输，可实施性好，成为学者的研究热点[11-16]。但这种加密方法的缺点之一是解密图像质量差，存在严重噪音。文献[17-19]利用G-S算法和模糊控制迭代算法设计密钥，使其傅里叶谱尽可能均匀，有效提高了解密图像质量。但这些方法需要较繁杂的数学计算和编程。

另一方面，目前研究者们分别采用选择明文攻击(CPA)[20-21]、已知明文攻击(KPA)[22-23]和唯密文攻击(COA)[24]算法对JTC加密系统进行攻击，结果表明JTC加密系统存在安全性缺陷，在不同条件下利用上述算法均能从加密图像中恢复出较高质量的图像。

本文从分析JTC加密方法中解密图像产生噪音的原因出发，提出了一种简单，能抑制解密图像噪音，并能有效提高抗攻击能力的方法。

2　JTC加密系统

JTC加密解密系统原理示意图[6-7]如图1所示，其中图1(a)为加密系统示意图，首先将原始图像 $f(x,y)$ 和随机相位模板 $p(x,y)$ 重叠在一起，与纯相位密钥模板 $h(x,y)$ 分别置于 $(-a,0)$ 和 $(a,0)$ 处。单色平面波照射下，透镜后焦面上的联合功率谱 $I(u,v)$，即加密图像为

$$\begin{aligned} I(u,v)=&\left|\mathscr{F}[f(x+a,y)p(x+a,y)+h(x-a,y)]\right|^2=\left|F(u,v)*P(u,v)\right|^2+\left|H(u,v)\right|^2+\\ &[F(u,v)*P(u,v)]H^*(u,v)\exp(\mathrm{i}4\pi au)+[F(u,v)*P(u,v)]^*H(u,v)\exp(-\mathrm{i}4\pi au)\end{aligned},\tag{1}$$

式中 $\mathscr{F}$、$(\cdot)^*$、$(\cdot)*(\cdot)$ 分别表示傅里叶变换、复共轭、卷积运算；$F(u,v)$、$P(u,v)$、$H(u,v)$ 分别表示 $f(x,y)$、$p(x,y)$、$h(x,y)$ 的傅里叶变换。

图1(b)为解密系统示意图，将加密图像置于4f系统频谱面上，其中心与系统光轴重合，密钥置于输入面原位置不变，则输出面上复振幅分布为

$$g(\xi,\eta)=\mathscr{F}^{-1}[H(u,v)\exp(-\mathrm{i}2\pi au)I(u,v)],\tag{2}$$

式中 $\mathscr{F}^{-1}$ 表示傅里叶逆变换。如果密钥谱的振幅均匀，即 $\left|H(u,v)\right|=1$，由(2)式得：

$$\begin{aligned} g(\xi,\eta)=&\{[f(\xi,\eta)p(\xi,\eta)]\otimes[f(\xi,\eta)p(\xi,\eta)]\}*h(\xi,\eta)*\delta(\xi-a,\eta)+h(\xi,\eta)*\delta(\xi-a,\eta)+\\ &[f(\xi,\eta)p(\xi,\eta)]*\delta(\xi+a,\eta)+[f(\xi,\eta)p(\xi,\eta)]\otimes[h(\xi,\eta)*h(\xi,\eta)]*\delta(\xi-3a,\eta),\end{aligned}\tag{3}$$

由(3)式可以看出，由于 $p(x,y)$ 为纯相位函数，其第三项即为解密图像，处在 $(-a,0)$ 处。

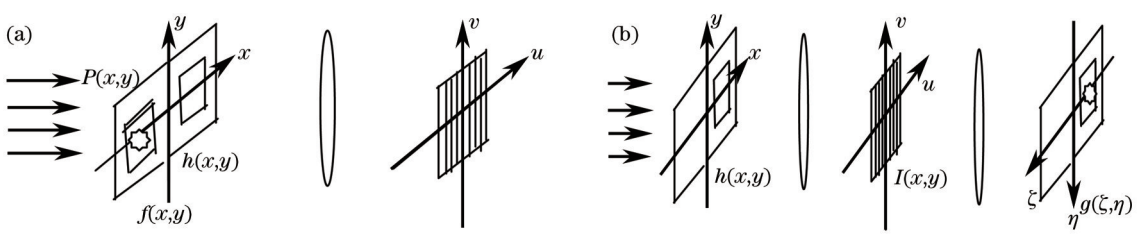

图1　JTC(a)加密、(b)解密系统示意图

Fig.1　Schematic diagrams of (a) encryption system, (b) decryption system based on JTC

3　非线性JTC加密系统

3.1　JTC加密系统消噪音分析

由于JTC加密系统中密钥模板面积有限，为一截断纯相位模板，因此其傅里叶谱不可能是一纯相位函数，即 $\left|H(u,v)\right|\neq 1$，使(3)式变为

$$g(\xi,\eta)=\{[f(\xi,\eta)p(\xi,\eta)]\otimes[f(\xi,\eta)p(\xi,\eta)]\}*h(\xi,\eta)*\delta(\xi-a,\eta)+[h(\xi,\eta)\otimes h(\xi,\eta)]*h(\xi,\eta)*\delta(\xi-a,\eta)+[f(\xi,\eta)p(\xi,\eta)]*[h(\xi,\eta)\otimes h(\xi,\eta)]*\delta(\xi+a,\eta)+[f(\xi,\eta)p(\xi,\eta)]\otimes[h(\xi,\eta)*h(\xi,\eta)]*\delta(\xi-3a,\eta),\tag{4}$$

从(4)式中第三项可以看出，由于密钥功率谱 $|H(u,v)|^2\neq 1$，解密图像为原始图像和密钥相关函数的卷积，不能完全恢复出原始图像，解密图像中存在严重噪音。

由于密钥是已知量，且解密图像噪音源为 $|H(u,v)|^2$。因此，为消除解密图像噪音，将加密图像 $I(u,v)$ 除以 $|H(u,v)|^2$ 得到新加密图像 $G(u,v)$ 为

$$G(u,v)=\frac{I(u,v)}{|H(u,v)|^2}=\frac{|F(u,v)*P(u,v)|^2}{|H(u,v)|^2}+1+\frac{[F(u,v)*P(u,v)]}{H(u,v)}\exp(\mathrm{i}4\pi au)+\frac{[F(u,v)*P(u,v)]^*}{H^*(u,v)}\exp(-\mathrm{i}4\pi au),\tag{5}$$

将新加密图像 $G(u,v)$ 置于图1(b)所示的解密系统频谱面上，则单色平面波照射下，输出面上得到的场分布为

$$g'(\xi,\eta)=\mathscr{F}^{-1}[G(u,v)H(u,v)\exp(-\mathrm{i}2\pi au)]=[f(\xi,\eta)p(\xi,\eta)]\otimes[f(\xi,\eta)p(\xi,\eta)]*r(\xi,\eta)*\delta(\xi-a,\eta)+h(\xi,\eta)*\delta(\xi-a,\eta)+[f(\xi,\eta)p(\xi,\eta)]*\delta(\xi+a,\eta)+[f(\xi,\eta)p(\xi,\eta)]\otimes h(\xi,\eta)*r'(\xi,\eta)*\delta(\xi-3a,\eta),\tag{6}$$

式中 $r(\xi,\eta)=\mathscr{F}^{-1}\left[\frac{1}{H^*(\xi,\eta)}\right]$，$r'(\xi,\eta)=\mathscr{F}^{-1}\left[\frac{H(\xi,\eta)}{H^*(\xi,\eta)}\right]$。由(6)式第三项看出，消噪音处理后，输出面上 $\xi=-a$ 处由电荷耦合元件(CCD)可以接收到和原始图像相同的解密图像。

3.2 非线性JTC加密系统及其抗攻击特性分析

从光学加密系统的攻击[20-24]研究中可知，之所以能利用各种攻击算法从加密图像中恢复出原始图像，其根本原因在于光学加密系统是一线性系统。

由3.1节中JTC加密系统消噪音原理看出，将加密图像 $I(u,v)$ 即联合功率谱除以密钥功率谱后，尽管解密系统和加密系统各自仍然是线性系统，但解密系统输出面的光场和加密系统输入面的光场之间不再是线性关系，即解密系统和加密系统整体上是非线性系统。

由于加密图像经密钥功率谱处理后，JTC加解密系统成为非线性JTC加解密系统，利用原有的攻击方法将无法从新加密图像中恢复出原始图像信息。因此进行上述处理后整个系统将极大提高其抗攻击能力。

4 数值模拟及分析

为验证非线性JTC加解密系统的消噪音效果和抗攻击能力，按(1)、(3)、(5)、(6)式以及文献[24]中的COA算法分别对Lena和文本图像进行加、解密和攻击的仿真，并对结果进行分析。

4.1 消噪音仿真及分析

4.1.1 解密图像质量表征参量

为定量表征解密图像质量，采用加、解密图像的相关系数和均方根(RMS)表征加、解密图像的差异。

相关系数定义为

$$c=\frac{\sum_{i=1}^{M}\sum_{j=1}^{N}\left|\left[f(i,j)-\bar{f}(i,j)\right]\left[I(i,j)-\bar{I}(i,j)\right]\right|}{\sqrt{\sum_{i=1}^{M}\sum_{j=1}^{N}\left[f(i,j)-\bar{f}(i,j)\right]^2}\sqrt{\sum_{i=1}^{M}\sum_{j=1}^{N}\left[I(i,j)-\bar{I}(i,j)\right]^2}},\tag{7}$$

RMS定义为

$$R_{\mathrm{RMS}}=\sqrt{\frac{\sum_{i=1}^{M}\sum_{j=1}^{N}[f(i,j)-I(i,j)]^2}{\sum_{i=1}^{M}\sum_{j=1}^{N}[f(i,j)]^2}},\tag{8}$$

式中 i、j 分别是图像像素的横纵坐标，M、N 分别是像素的横纵坐标总数，$f(i,j)$ 是原始图像中像素(i,j)的灰度值，$\bar{f}(i,j)$ 是原始图像中所有像素的灰度平均值，$I(i,j)$ 是解密图像中像素(i,j)的灰度值，$\bar{I}(i,j)$ 是解密图像中所有像素的灰度平均值。相关系数 c 越接近1，R_{RMS} 越接近0，解密图像和原始图像差别越小，图像解密效果越好。

4.1.2 消噪音特性模拟及分析

为分析消噪音效果，分别对Lena图像和二值文本图像进行消噪音处理。

图2为按照图1(b)所示的解密系统得到的Lena的解密图像消噪音情况比较。其中图2(a)为原始图像；图2(b)为加密图像 $I(u,v)$；图2(c)是 $I(u,v)$ 的解密图像，即未消噪音解密图像，与原始图像的 c 值为0.4104，R_{RMS} 为0.8154，图像解密效果较差。图2(d)是新加密图像 $G(u,v)$ 的解密图像，即消噪音解密图像，与原始图像的 c 值为0.5679，R_{RMS} 为0.7416，解密效果变好。由于消噪音是用加密图像除以密钥功率谱作为新加密图像，当密钥功率谱中有零值时，会影响图像解密效果，因此把密钥功率谱中一些近零值剔除。图2(e)是剔除密钥功率谱中一些近零值后的消噪音解密图像，此时与原始图像的 c 值为0.7190，R_{RMS} 为0.7089，解密效果进一步变好。尽管此时解密效果还不是非常好，但作为一种简单的去噪方法，已经明显改善了图像解密效果。

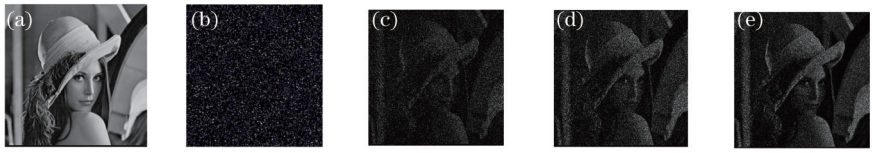

图2 Lena的解密图像消噪音效果比较。(a) 原始图像；(b) 加密图像 $I(u,v)$；(c) $I(u,v)$ 的解密图像；(d) 新加密图像 $G(u,v)$ 的解密图像；(e) 剔除密钥功率谱中一些近零值后的消噪音解密图像

Fig.2 Removing noise effect comparison of decryption images of Lena. (a) Original image; (b) encryption image $I(u,v)$; (c) decryption image of $I(u,v)$; (d) decryption image of new encryption image $G(u,v)$; (e) decryption image of $G(u,v)$ after eliminating approximate zero values in the key spectrum

图3为二值文本图像的解密图像消噪音效果比较。其中图3(a)为原始图像；图3(b)为加密图像；图3(c)是 $I(u,v)$ 的解密图像，即未消噪音解密图像，与原始图像的 c 值为0.8458，R_{RMS} 为0.6887，与图2(c)相比，解密效果较好；图3(d)是新加密图像 $G(u,v)$ 的解密图像，即消噪音解密图像，与原始图像的 c 值为0.9751，R_{RMS} 为0.5196，解密效果好。图3(e)是剔除密钥功率谱中近零值后的消噪音解密图像，与原始图像的 c 值为0.9785，R_{RMS} 为0.4583。从图3中可以看出JTC加解密系统对简单的二值文本图像的解密效果比复杂图像的好。由于灰度图像结构复杂，其傅里叶谱中高频成份多，而二值图像结构简单，其傅里叶谱中高频成份少。因此，灰度图像在输出平面上由原始图像和密钥相关函数卷积产生的噪音大；而二值图像在输出平面上由原始图像和密钥相关函数卷积产生的噪音小。由于图2和图3中的图像是将最大灰度值归为255显示的，噪音分布情况显示的不明显。若将图2和图3中的噪音放大，如图4所示，可以看出JTC结构的光学加密系统对于二值图像解密时输出面上的噪音明显小于灰度图像，因此该消噪音方法对二值图像效果更好。

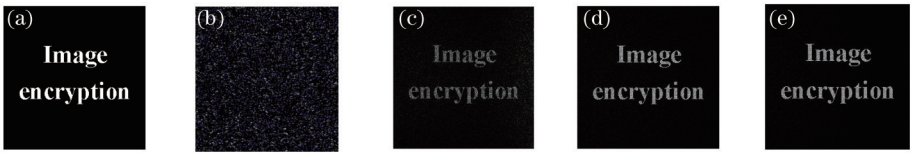

图3 文本文件的解密图像消噪音效果比较。(a) 原始图像；(b) 加密图像 $I(u,v)$；(c) $I(u,v)$ 的解密图像；(d) 新加密图像 $G(u,v)$ 的解密图像；(e) 剔除密钥功率谱中一些近零值后的消噪音解密图像

Fig.3 Removing noise effect comparison of decryption images of text file. (a) Original image; (b) encryption image $I(u,v)$; (c) decryption image of $I(u,v)$; (d) decryption image of new encryption image $G(u,v)$; (e) decryption image of $G(u,v)$ after eliminating approximate zero values in the key spectrum

4.2 抗攻击仿真和分析

为验证消噪音处理后的加密图像的抗攻击性能，使用文献[24]中的COA算法分别对加密图像 $I(u,v)$ 和新加密图像 $G(u,v)$ 进行攻击，攻击算法框图如图5所示。

攻击算法中所用判据均方差(MSE)为

$$M_{\mathrm{MSE}}=\frac{1}{M\times N}\sum_{i=1}^{M}\sum_{j=1}^{N}\left[\left|g_{k+1}(x_i,y_j)\right|-f(x_i,y_j)\right]^2, \tag{9}$$

式中 f 为原始图像，g_{k+1} 是第 k 次迭代后的估算图像。攻击时所取判据 M_{MSE} 值越小，攻击所得图像与原始图像差别越小。

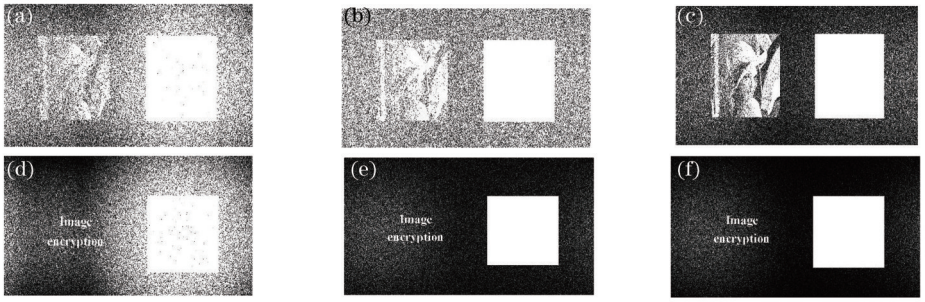

图4 解密系统输出面上的噪音分布。(a) 当仿真灰度值除以10^9时输出面上图2(c)及噪音; (b) 当仿真灰度值乘以10时输出面上图2(d)及噪音; (c) 当仿真灰度值乘以10时输出面上图2(e)及噪音; (d) 当仿真灰度值除以10^9时输出面上图3(c)及噪音; (e) 当仿真灰度值乘以10时输出面上图3(d)及噪音; (f) 当仿真灰度值乘以10时输出面上图3(e)及噪音

Fig.4 Noise distributions on the output planes in the decryption system.(a) Fig.2(c) and noise on output plane when simulation grey value is divided by 10^9; (b) Fig.2(d) and noise on output plane when simulation grey value is multiplied by 10; (c) Fig.2(e) and noise on output plane when simulation grey value is multiplied by 10; (d) Fig.3(c) and noise on output plane when simulation grey value is divided by 10^9; (e) Fig.3(d) and noise on output plane when simulation grey value is multiplied by 10; (f) Fig.3(e) and noise on output plane when simulation grey is value multiplied by 10

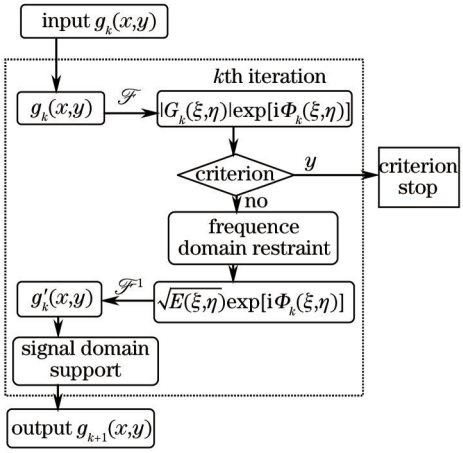

图5 COA算法框图

Fig.5 Diagram of COA arithmetic

对图2(b)所示的Lena加密图像$I(u,v)$进行COA攻击,攻击时取判据M_{MSE}分别为0.05、0.005、0.0005,结果如图6所示,其中图6(a)是原始图像;图6(b)是M_{MSE}= 0.05时的攻击结果,迭代次数为1917次;图6(c)是M_{MSE}=0.005时的攻击结果,迭代次数为1953次;图6(d)是M_{MSE}=0.0005时的攻击结果,迭代次数为1433次。从中可以看出,取M_{MSE}=0.0005时的迭代次数反而比取M_{MSE}=0. 05和M_{MSE}=0. 005时还少,原因是攻击程序中,所用的第一幅图像是计算机生成的随机图像,它一定程度上也影响到迭代次数。对确定的加密图像,给定M_{MSE}值,进行多次攻击,由于随机图像会发生变化,需要的迭代次数也会发生变化,但变化不会很大。

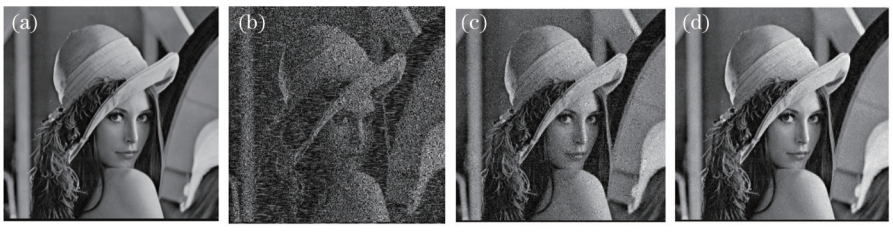

图6 Lena加密图像$I(u,v)$的COA攻击结果。(a) 原始图像; (b) M_{MSE}=0.05时的攻击恢复图像; (c) M_{MSE}=0.005时的攻击恢复图像; (d) M_{MSE}=0.0005时的攻击恢复图像

Fig.6 COA attack results of Lena encryption image $I(u,v)$. (a) Original image; (b) attack restored image when M_{MSE}=0.05; (c) attack restored image when M_{MSE}=0.005; (d) attack restored image when M_{MSE}=0.0005

对图3(b)所示的二值文本加密图像 $I(u,v)$ 进行COA攻击，攻击时取判据 M_{MSE} 分别为0.05、0.005、0.0005，结果如图7所示；其中图7(a)是原始图像；图7(b)是 M_{MSE}=0.05时的攻击结果，迭代次数为754次。图7(c)是 M_{MSE}=0.005时的攻击结果，迭代次数为1485次；图7(d)是 M_{MSE}=0.0005时的攻击结果，迭代次数为1818次。尽管需要较长的运算时间，但攻击恢复出的图像质量还是很好的。

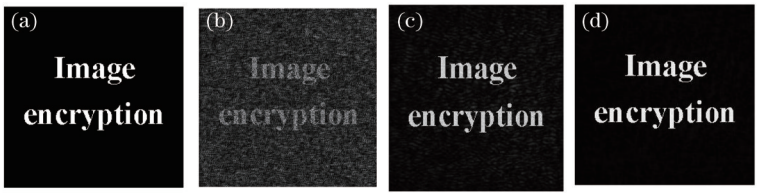

图7　文本加密图像 $I(u,v)$ 的COA攻击结果。(a) 原始图像；(b) M_{MSE}=0.05时的攻击恢复图像；(c) M_{MSE}=0.005时的攻击恢复图像；(d) M_{MSE}=0.0005时的攻击恢复图像

Fig.7　COA attack results of text file encryption image $I(u,v)$. (a) Original image; (b) attack restored image when M_{MSE}=0.05; (c) attack restored image when M_{MSE} =0.005; (d) attack restored image when M_{MSE} =0.0005

将Lena和二值文本的加密图像 $I(u,v)$ 分别除以密钥功率谱得到新加密图像 $G(u,v)$，取 M_{MSE}=0.05对其进行COA攻击，当迭代次数超过20000次时，攻击结果如图8所示，可以看出结果中没有任何原始图像信息。由于新加密图像破坏了解密系统和加密系统间的线性关系，该方法在提高图像解密效果的同时，具有很好的抗COA攻击能力，有效提高了JTC加密系统的安全性。

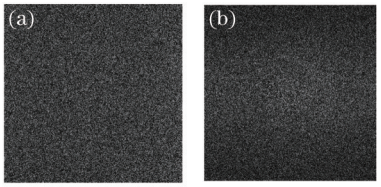

图8　超过20000次迭代时新加密图像 $G(u,v)$ 的COA攻击结果。(a) Lena; (b) 文本文件

Fig.8　COA attack results of new encryption images $G(u,v)$ when iterations are more than 20000 times. (a) Lena; (b) text file

5　结　论

通过分析JTC光学加、解密的原理，表明其解密图像噪音大、质量差的原因在于密钥模板的傅里叶谱振幅分布不均匀，解密图像为原始图像和密钥相关函数的卷积。为消除噪音，提高解密图像质量，将加密图像除以密钥功率谱得到新的加密图像。仿真结果表明通过消噪音处理后，Lena解密图像和原始图像的相关系数可从0.4104增加到0.7190，RMS从0.8154减小到0.7089；二值文本解密图像和原始图像的相关系数可由0.8458增加到0.9785，RMS从0.6887减小到0.4583。同时COA攻击算法不能恢复出新加密图像中的任何原始图像信息。新加密图像不仅可以提高解密图像质量，而且能抵抗COA算法的攻击，有效提高加密系统安全性。

参 考 文 献

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

2 G Unnikrishnan, J Joseph, K Singh. Optical encryption by double-random phase encoding in the fractional Fourier domain[J]. Opt Lett, 2000, 25(8): 887-889.

3 G H Situ, J J Zhang. Double random phase encoding in the Fresnel domain[J]. Opt Lett, 2004, 29(12): 1584-1586.

4 Chao Lin, Xueju Shen, Baochen Li. Four-dimensional key design in amplitude, phase, polarization and distance for optical encryption based on polarization digital holography and QR code[J]. Optics Express, 2014, 22(17): 20727-20739.

5 Kong Dezhao, Shen Xueju, Xu Qinzu, *et al*.. Multiple-image encryption scheme based on cascaded fractional Fourier transform[J]. Appl Opt, 2013, 52(12): 2619-2625.

6 Bai Yinbuhe, Li Genquan, Lü Linxia, *et al*.. Optical image encryption with ciphertext of a single diffraction intensity Pattern[J]. Laser & Optoelectronics Progress, 2014, 51(10): 100701.

白音布和, 李根全, 吕林霞, 等. 以单幅衍射强度图像为密文的光学衍射成像加密系统[J]. 激光与光电子学进展, 2014, 51(10): 100701.

7 Chen Yixiang, Wang Xiaogang. Nonlinear double images encryption based on double random phase encoding[J]. Acta Optica Sinica, 2014, 34(7): 0710001.
陈翼翔, 汪小刚. 基于双随机相位编码的非线性双图像加密方法[J]. 光学学报, 2014, 34(7): 0710001.

8 Zhu Wei, Yang Geng, Chen Lei, *et al*.. An improved image encryption algorithm based on double random phase encoding and chaos[J]. Acta Optica Sinica, 2014, 34(6): 0607001.
朱　薇, 杨　庚, 陈　蕾, 等. 基于混沌的改进双随机相位编码图像加密算法[J]. 光学学报, 2014, 34(6): 0607001.

9 T Nomura, B Javidi. Optical encryption using a joint transform correlator architecture[J]. Opt Eng, 2000, 39(8): 2031-2035.

10 Nomura T, Javidi B. Optical encryption system with a binary key code[J]. Appl Opt, 2000, 39(26): 4783-4787.

11 S J Park, J Y Kim, J K Bae, *et al*.. Fourier-plane encryption technique based on removing the effect of phase terms in a joint transform correlator[J]. Opt Rev, 2001, 8(6): 413-415.

12 C La Mela, C Iemmi. Optical encryption using phase-shifting interferometry in a joint transform correlator[J]. Opt Lett, 2006, 31(17): 2562-2564.

13 D Amaya, M Tebaldi, R Torroba, *et al*.. Multichanneled encryption via a joint transform correlator architecture[J]. Appl Opt, 2008, 47(31): 5903-5907.

14 D Amaya, M Tebaldi, R Torroba, *et al*.. Digital color encryption using a multi-wavelength approach and a joint transform correlator[J]. Journal of Optics A Pure and Applied Optics, 2008, 10(10): 104031.

15 D Amaya, M Tebaldi, R Torroba, *et al*.. Wavelength multiplexing encryption using joint transform correlator architecture[J]. Appl Opt, 2009, 48(11): 2099-2104.

16 E Rueda, J F Barrera, R Henao, *et al*.. Optical encryption with a reference wave in a joint transform correlator architecture[J]. Opt Commun, 2009, 282(16): 3243-3249.

17 Cheng C J, Lin L C, Wang C M, *et al*.. Optical joint transform encryption using binary phase difference key mask[J]. Opt Rev, 2005, 12(5): 367-371.

18 Lin L C, Cheng C J. Optimal key mask design for optical encryption based on joint transform correlator architecture[J]. Opt Commun, 2006, 258(2): 144-154.

19 Wu Ke′nan, Hu Jiasheng, Lin Yong. A novel method of key design in optical encryption system based on JTC architecture[J]. Optics and Precision Engineering, 2007, 15(4): 577-581.
吴克难, 胡家升, 林　勇. 基于JTC的光学加密系统密钥设计新方法[J]. 光学精密工程, 2007, 15(4): 577-581.

20 J F Barrera, C Vargas, M Tebaldi, *et al*.. Chosen-plaintext attack on a joint transform correlator encrypting system[J]. Opt Commun, 2010, 283(20): 3917-3921.

21 W Qin, X Peng, X Meng. Cryptanalysis of optical encryption schemes based on joint transform correlator architecture[J]. Opt Eng, 2011, 50(2): 028201.

22 J F Barrera, C Vargas, M Tebaldi, *et al*.. Known-plaintext attack on a joint transform correlator encrypting system[J]. Opt Lett, 2010, 35(21): 3553-3555.

23 M Liao, W He, X Peng, *et al*.. Cryptanalysis of optical encryption with a reference wave in a joint transform correlator architecture[J]. Opt Laser Technol, 2013, 45: 763-767.

24 C Zhang, M Liao, W He, *et al*.. Ciphertext-only attack on a joint transform correlator encryption system[J]. Optics Express, 2013, 21(23): 28523-28530.

栏目编辑：张　雁