基于联合功率谱分区复用的光学多图像加密方法与实验

刘杰[1,2*]，白廷柱[2]，沈学举[1]，窦帅风[1]，林超[3]，陈琪[1]，武东生[1]

[1]陆军工程大学石家庄校区电子与光学工程系，河北 石家庄 050000；

[2]北京理工大学光电学院光电成像技术与系统教育部重点实验室，北京 100081；

[3]海军航空大学，山东 烟台 264001

摘要 针对光学多图像加密出现的串扰噪声大和复用容量小的问题，提出了一种基于联合功率谱(JPS)分区复用的光学多图像加密方法。该方法首先利用相位恢复算法开展相位模板优化设计，压缩了单通道 JPS 面积，然后在优化后的相位模板上叠加线性相位，使各通道 JPS 在频谱面上产生不同的位置平移，再经过窗口滤波，实现无串扰叠加。此外，以“密钥相位核＋偏转角数据包”形式进行密钥内容规划，在确保加密方法安全性以及密钥空间足够大的同时，压缩了需传递的密钥数据量。数值仿真结果表明，对 9 幅灰度图像进行加密，其解密图像与原始图像的相关系数值均达到 0.94 以上，解密效果显著。当解密质量评判阈值设定在 0.95 时，灰度图像和二值图像的最大压缩效率因子分别达到 12 和 32，密文压缩能力显著。最后，搭建光学实验系统，进一步验证了该方法的可行性。

关键词 光通信；光学加密；多图像；联合功率谱；相位恢复算法；联合变换相关器

中图分类号 O438.1；TN911.74 **文献标识码** A **doi**：10.3788/CJL201845.1209003

Experimental Research and Encryption Method of Optical Multi-Images Based on Joint Power Spectral Partition Multiplexing

Liu Jie[1,2*], Bai Tingzhu[2], Shen Xueju[1], Dou Shuaifeng[1], Lin Chao[3], Chen Qi[1], Wu Dongsheng[1]

[1]*Department of Electronics and Optics Engineering, Shijiazhuang Campus of the Army Engineering University, Shijiazhuang, Hebei* 050000, *China*;

[2]*Key Laboratory of Photoelectronic Imaging Technology and System, Ministry of Education, School of Optics and Photonics, Beijing Institute of Technology, Beijing* 100081, *China*;

[3]*Naval Aeronautical University, Yantai, Shandong* 264001, *China*

Abstract Aiming at the problems of large cross-talk noise and small multiplexing capacity in the optical multi-image encryption system, an optical multi-image encryption method based on joint power spectral (JPS) partition multiplexing is proposed. First, the phase retrieval algorithm is utilized for the optimal design of phase masks and the single-channel JPS area is thus compressed. Then, the corresponding linear phases are superimposed on the optimized phase masks and so that the each-channel JPS is shifted differently in its spectral plane. After the window filtering operation, the superposition without crosstalk is realized. In addition, the key content planning is carried out in the form of “key phase kernel plus deflection angle packet”. While the security of encryption method and the large enough key space are ensured, the key data needed to be transferred is compressed. The numerical simulation results show that, when nine gray-scale images are encrypted, the correlation coefficients between the decrypted images and the original images are over 0.94 and the decryption effect is obvious. When the evaluation threshold of decryption quality is set as 0.95, the maximum compression efficiency factors of gray-scale and binary images reach 12 and 32, respectively. The cipher-text compression ability is remarkable. Finally, an optical experiment system is built and the feasibility of this method is further verified.

收稿日期：2018-07-04；**修回日期**：2018-08-13；**录用日期**：2018-08-24

基金项目：河北省自然科学基金(F2016506014)

* **E-mail**：yclj07@163.com

Key words　optical communications; optical encryption; multi-image; joint power spectrum; phase retrieval algorithm; joint transform correlator

OCIS codes　060.4785; 100.4998; 070.4550

1　引　　言

自 Refregier 和 Javidi[1] 于 1995 年提出双随机相位编码技术以来，光学加密技术受到越来越多研究人员的关注。由于其具有并行性好、多维度编码以及容量大等诸多优势，已逐步成为信息安全领域的研究热点之一。近些年来，许多新的加密方法和改进方法相继被提出[2-13]。其中，Nomura 和 Javidi[3] 提出了基于联合变换相关器(JTC)的光学加密方法，该加密系统密钥模板不需要精确对准且不需要制作复共轭密钥，加密图像即联合功率谱(JPS)，便于记录和传输，因此成为一种具有实用性的光学加密方法。

由于光学多图像加密具有高存储效率的特点，在提高信息传输效率和多用户认证等方面具有重要应用前景，因此，一些新的多图像加密方法[14-25]不断被提出，主要利用波长复用[14]、位置复用[15]、偏振复用[16]、多孔径复用[17]、相位模板旋转复用[20]、螺旋相位模板拓扑荷数复用[25]等进行多图像加密。Situ 分别利用波长复用[14]以及位置复用[15]技术实现了多图像加密；Rueda 等[20]利用密钥相位模板的旋转实现了多图像加密并完成了实验验证；Chen 等[25]在 JTC 结构下利用螺旋相位模板拓扑荷数复用技术实现了多图像加密并完成了实验验证。但是，现有的多图像加密方法普遍存在各通道之间解密图像串扰噪声较大的问题，直接影响了多图像加密复用容量。

为了解决上述方法存在的问题，本文在简要分析 JTC 光学加密原理基础上，利用一种基于相位恢复算法的相位模板优化设计方法，实现了单通道密文压缩；在此基础上，利用叠加线性相位和窗口滤波处理等方法，实现了多通道密文之间的无串扰叠加。数值仿真和光学实验均验证了该方法的可行性。

2　理论分析与系统构建

2.1　基于 JTC 的光学图像加密原理

基于 JTC 的光学加密系统如图 1(a)所示，叠加了随机相位模板的待加密单幅图像和对应的密钥模板分别放置在 y 轴两侧，共同组成输入面(x,y)，并放置于傅里叶透镜前焦面上。经过波长为 λ 的单色平面波照射后，在透镜后焦面(u,v)上形成 JPS，即密文，其可以表示为

$$\begin{aligned}J(u,v)=&\\ &\left|\mathcal{F}[h(x+a,y)e(x+a,y)+k(x-a,y)]\right|^2=\\ &|H*E|^2+(H*E)K^*\exp(\mathrm{j}4\pi au)+\\ &(H*E)^*K\exp(-\mathrm{j}4\pi au)+|K|^2,\end{aligned}\tag{1}$$

式中：$\mathcal{F}$ 为傅里叶变换运算符；e 和 E 分别为待加密图像及其傅里叶变换结果；h 和 H 分别为与待加密图像相叠加的随机相位模板及其傅里叶变换结果；k 和 K 分别为密钥相位模板及其傅里叶变换结果；a 为待加密图像中心和密钥相位模板中心至 y 轴的距离；$(\cdot)^*$ 表示复共轭；$*$ 表示卷积运算。位于输出面上的 JPS 为强度信息，可以通过 CCD 等强度记录器件对其进行采集，并对其进行存储与传输。

解密系统如图 1(b)所示。密钥放置于输入面(x,y)上，经过相同 λ 的单色平面波照射后，在透镜 1的后焦面上，其透过密文 $J(u,v)$后的光场复振幅分布为

$$\begin{aligned}D(u,v)=&K\exp(-\mathrm{j}2\pi au)J(u,v)=\\ &|H*E|^2K\exp(-\mathrm{j}2\pi au)+(H*E)\exp(\mathrm{j}2\pi au)+\\ &(H*E)^*KK\exp(-\mathrm{j}6\pi au)+K\exp(-\mathrm{j}2\pi au)。\end{aligned}\tag{2}$$

复振幅分布 $D(u,v)$位于透镜 2 的前焦面上，经过该透镜的一次傅里叶逆变换，在其后焦面上得到

$$\begin{aligned}d(x,y)=&\mathcal{F}^{-1}[D(u,v)]=\\ &(he)\oplus(he)*k*\delta(x-a)+(he)*\delta(x+a)+\\ &(he)\oplus k*k*\delta(x-3a)+k*\delta(x-a),\end{aligned}\tag{3}$$

式中：$\mathcal{F}^{-1}$ 为傅里叶逆变换运算符；$\oplus$ 表示相关运算；$\delta(\cdot)$为狄拉克函数。从(3)式中可以看出，第 1、3、4 项均为与解密图像无关的噪声项，只有第 2 项包含了叠加了随机相位模板 h 的加密图像 e，其图像中心位置为$(-a,0)$。由于解密结果通过 CCD 等强度记录器件采集，因此，h 将不会影响图像 e 的准确再现。至此，单幅加密图像将在$(-a,0)$处再现，解密过程完成。

2.2　密文压缩效率

对于基于数字全息技术的光学加密系统而言，其单份密文容量即为 CCD 等图像采集设备的单帧图像数据量。以分辨率为 768 pixel×576 pixel 的

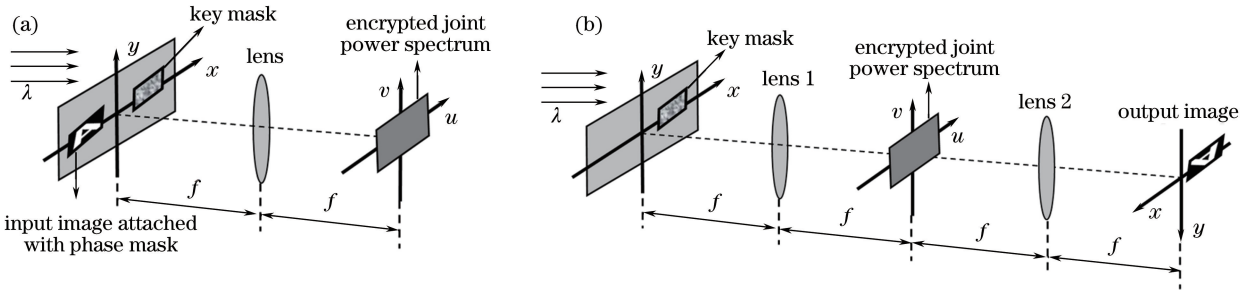

图 1　光学加密与解密系统示意图。(a)加密系统;(b)解密系统

Fig. 1　Diagrams of optical encryption and decryption systems. (a) Encryption system; (b) decryption system

8 位黑白 CCD 为例,其采集到的单份密文容量为 0.44 MB。如果以单帧加密的形式对一段 20 s(帧频为 50 Hz)的视频进行光学加密,则所需传输的密文容量将达到 440 MB。因此,对于多图像加密而言,如何高效率压缩密文容量是需要解决的关键问题。文献[26]提出了压缩效率因子 E_{f} 的概念,可对多图像加密的密文容量压缩能力进行定量描述,即

$$E_{\mathrm{f}}=\frac{V_{\mathrm{cip}}}{V'_{\mathrm{cip}}},\tag{4}$$

式中:V_{cip} 为压缩前的密文数据量;V'_{cip} 为压缩后的密文数据量。E_{f} 越大,表示该密文压缩方法的效果越好。当然,在压缩密文的同时,还需要考虑图像解密质量的变化。文献[14]给出了复用容量的概念,即达到设定的图像解密质量评判阈值时,该项复用技术可以加密的最大原始图像数量。基于此概念,本文给出最大压缩效率因子的概念,即

$$E_{\mathrm{fmax}}=\max\ [E_{\mathrm{f}}]_{\tau},\tag{5}$$

式中:τ 为解密质量评判阈值,根据图像解密质量需求以及解密图像类型(灰度图像或者二值图像)等设定该值;max[·]表示取最大值运算。

2.3　基于 JPS 分区复用的光学多图像加密原理

2.3.1　加密过程

基于一定大小的密文面积,通过压缩单图像密文面积和平移其位置,实现各通道在频谱面上 JPS 的分区配置。在进一步的空间滤波处理基础上,对多通道 JPS 进行无串扰数学叠加,实现光学多图像加密,其加密原理如图 2 所示。由该方法生成的多图像 JPS 可以表示为

$$J(u,v)=\sum_{i=1}^{n}J'_i(u-m_i,v-n_i),\tag{6}$$

式中:J_i' 为第 i 个通道对应的经过面积压缩处理后的 JPS;m_i 和 n_i 分别为 J_i' 在频谱面上的中心坐标。

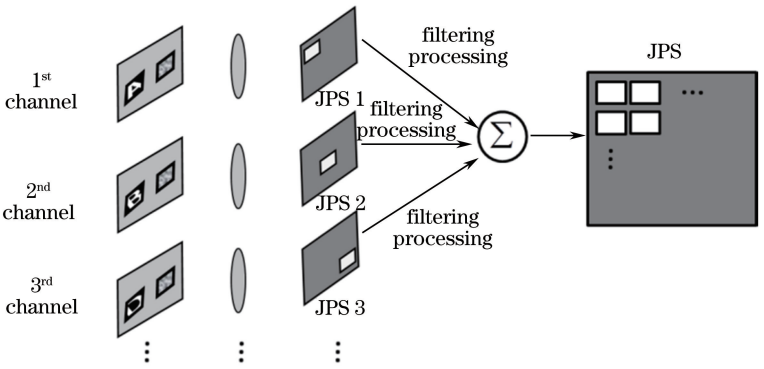

图 2　基于 JPS 分区复用的光学多图像加密原理示意图

Fig. 2　Schematic of optical multi-image encryption based on JPS partition multiplexing

压缩单图像密文面积是实现 JPS 分区复用的关键步骤之一。文献[27]提出的迭代算法通过限制相位模板对应傅里叶谱尺寸来开展相位模板设计,进而实现与光学系统空间带宽的匹配。基于该思路 $C\{\cdot\}$ 表示频谱面上的单图像密文面积约束操作,即位于约束面积范围外的傅里叶谱赋为 0 值,位于编写相位恢复算法,开展相位模板优化设计,实现各通道密文面积的压缩,算法流程如图 3 所示。

设 $m_0(x,y)$ 为初始随机相位模板,经过光学傅里叶变换后,其对应的傅里叶谱表示为 $M_N(u,v)$。约束面积范围内的复振幅保留原值。经过此处理的傅里叶谱表示为 $M_N'(u,v)$,其再经过光学傅里叶逆

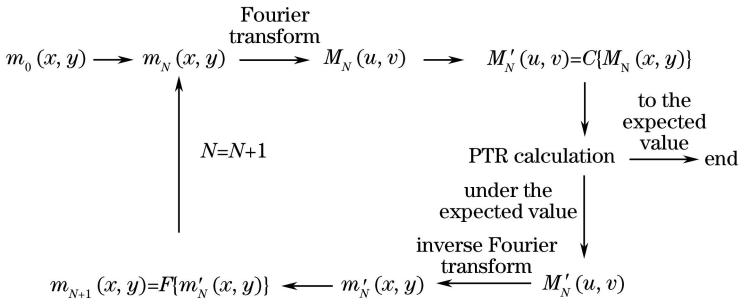

图 3　相位模板设计流程图

Fig. 3　Flow chart of phase mask design

变换后，将得到经面积压缩处理后新的相位模板 $m'_N(x,y)$。$F\{\cdot\}$表示振幅的归一化操作，其结果表示为 $m_{N+1}(x,y)$，并进入下一个循环运算。其中，约束面积范围内的能量透过率(PTR)将作为循环运算的判据[27]，表示为

$$P_{\mathrm{TR}}=\frac{\sum\limits_{(u,v)\in\Omega}|M|^2}{\sum\limits_{(u,v)}|M|^2},\tag{7}$$

式中：M 为相位模板对应的傅里叶谱；Ω 为约束区域。当约束面积范围内的 PTR 达到设定阈值时，循环运算结束，输出结果即为设计生成的新相位模板。

对于设计出的新相位模板，各通道所对应的压缩后 JPS 中心仍位于频谱面中心，各通道 JPS 叠加后的多图像 JPS 依然存在串扰问题。为了解决该问题，依据傅里叶变换位移定理[28]，在各通道相位模板上叠加各自的线性相位，使各通道 JPS 中心平移到频谱面上不同的位置，进而实现在不同区域的配置，避免直接叠加引起的相互串扰。设傅里叶透镜焦距为 f，则(6)式中 J_i'在频谱面上的中心横坐标 m_i 和纵坐标 n_i 分别表示为

$$m_i=f\theta_{xi},\quad n_i=f\theta_{yi},\tag{8}$$

式中：θ_{xi}和θ_{yi}分别为第 i 个通道 JPS 中心相对光轴在水平和垂直方向上的偏转角。根据频谱面位置坐标(u,v)与空间频率(f_x,f_y)的关系 $f_x=u/(\lambda f)$和$f_y=v/(\lambda f)$，可计算得到第 i 个通道相位模板需要叠加的线性相位为

$$p_i=\exp\left[-\mathrm{j}\frac{2\pi}{\lambda}(x\theta_{xi}+y\theta_{yi})\right]。\tag{9}$$

至此，第 i 个通道输入面物窗口和密钥窗口的相位模板分别表示为

$$h'_i=h'p_i,\quad k'_i=k'p_i,\tag{10}$$

式中：h'和 k'分别为经过相位恢复算法生成的物窗口相位模板和密钥相位模板。

为了确保各通道JPS之间的零串扰叠加，当CCD依次采集到各通道单帧JPS图像后，对其进行窗口滤波，即各通道采集图像中的JPS能量集中区域保留，其余赋为0值。由于滤波后的各通道JPS互不重叠，直接相加后，即可用同样为一帧图像大小的密文图像表征多通道JPS零串扰叠加后的新密文数据，即

$$J(u,v)=\sum_{i=1}^{n}F_{\mathrm{filter}}\{J'_i(u-f\theta_{xi},v-f\theta_{yi})\},\tag{11}$$

式中：$F_{\mathrm{filter}}\{\cdot\}$表示窗口滤波处理。因此，根据(4)式，对于 n 个通道的多图像加密而言，其密文压缩效率因子 E_{f} 即为 n。

2.3.2　密钥内容规划

在传统的JTC结构多图像加密方法中，一般一个密钥对应一幅图像，因此对于较大数量图像的加密场合而言，密钥数据量巨大。如何在确保加密方法安全性以及密钥空间足够大的同时进行密钥数据量的压缩，逐步引起了研究人员的关注。自 Situ 提出波长复用[14]和位置复用[15]技术实现多图像加密以来，“一份密钥和一组可变参量”的新型密钥内容形式不仅满足了多图像加密需求，还在一定程度上压缩了密钥数据量。在此基础上，针对JTC结构开展的旋转角度复用[20]和拓扑荷数复用[25]多图像加密技术也实现了上述功能。沿用上述思路，结合JPS分区复用技术的特点，以“密钥相位核＋偏转角数据包”形式进行密钥内容规划，如图4所示。首先将由相位恢复算法设计生成的密钥相位模板 k'作为“密钥相位核”发送给解密方，然后将加密过程中各通道涉及的 θ_{xi}和θ_{yi}进行串行组合(以总通道数 N 为字头，用于接收检验)，作为偏转角数据包单独向解密方发送，由解密方将接收到的“密钥相位核”依次与偏转角数据包中 θ_{xi}和θ_{yi}对应的线性相位进行叠加，恢复出各通道的密钥相位模板，即可用于各通道的光学图像解密。该密钥内容规划方式具有密钥数据量小和分发管理可操作性强的优点。

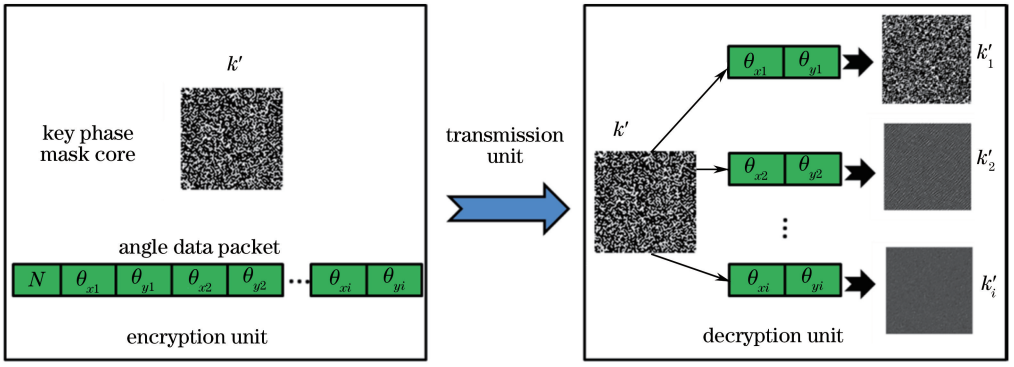

图 4　密钥内容规划示意图

Fig. 4　Schematic of key content planning

2.3.3　解密过程

解密系统如图 1(b)所示。解密方将密钥相位核 k' 与某通道偏转角 θ_{xi} 和 θ_{yi} 对应的线性相位叠加后生成的 k_i' 置于透镜 1 的前焦面上，在其后焦面上获得 k_i' 对应的傅里叶谱区域。由于前面所述的面积压缩和位置线性平移处理，该傅里叶谱区域中心将位于频谱面上 $(f\theta_{xi}, f\theta_{yi})$ 处，并且能量集中在一定区域内。由 CCD 采集 k_i' 对应的功率谱图像，并将其能量集中区域作为滤波窗口对接收到的密文 $J(u,v)$ 进行空间滤波，窗口以内密文数据保留，窗口以外数据赋为 0 值，从而获得一帧图像大小的该通道对应密文 $J_{Si}''(u-f\theta_{xi}, v-f\theta_{yi})$。由 k_i' 的傅里叶谱对放置于透镜 1 后焦面上的密文进行照射，再将照射结果经过透镜 2 的一次光学傅里叶逆变换后，在输出面上得到

$$d_i(x,y)=\mathscr{F}^{-1}\{K_iJ_i''(u-f\theta_{xi}, v-f\theta_{yi})\}。\tag{12}$$

通过第 2.1 节中(3)式可知，在输出面上将依次再现各通道图像 $d_i(x,y)$，这些图像被 CCD 采集记录，完成多图像解密过程。

3　数值仿真与分析

数值仿真依托 Matlab 7.11.0 (R2010b)软件进行。仿真过程中，激光波长选取 632.8 nm，输入面物窗口和参考窗口尺寸均为 500 pixel×500 pixel，两个窗口中心与垂直坐标轴之间的距离均为 300 pixel，透镜焦距选择 400 mm。为了定量评估图像解密效果，引入了解密图像与原始图像的相关系数(CC)[29]作为评价指标，表示为

$$C=\frac{\left|\sum_{i=1}^{M}\sum_{j=1}^{N}[f(i,j)-\bar{f}][I(i,j)-\bar{I}]\right|}{\sqrt{\sum_{i=1}^{M}\sum_{j=1}^{N}[f(i,j)-\bar{f}]^2}\sqrt{\sum_{i=1}^{M}\sum_{j=1}^{N}[I(i,j)-\bar{I}]^2}},\tag{13}$$

式中：i 和 j 分别表示在垂直和水平方向上的像素位置；f 和 $\bar{f}$ 分别为待加密图像某像素点的灰度值和所有像素点的灰度平均值；I 和 $\bar{I}$ 分别为解密图像某像素点的灰度值和所有像素点的灰度平均值；M 和 N 分别为图像在垂直和水平方向上的总像素数。

3.1　加、解密仿真与分析

以 9 幅 500 pixel×500 pixel 灰度图像作为待加密图像，如图 5 所示。首先，利用相位恢复算法生成密钥相位核 k' 和物窗口相位核 h'，基本流程如下：由于本次仿真采用了频谱面上 JPS 横向拼接方案，如图 6 所示，即从左至右依次为第 1～9 通道的 JPS，因此迭代运算过程中频谱面限制为第 5 通道(9 个通道的中间位置)对应的条形区域，当 PTR 阈值设置为 0.996、迭代循环次数为 36 时，即可输出相位模板，耗时约 26 s(仿真计算机配置为 Intel© Core™ i7-4790 CPU @ 3.6 GHz，内存 8 GB)。图 7(a)、(b)分别为生成的 k' 和 h'，由于采用 JPS 横向拼接方案，因此 9 个通道对应的 θ_{yi} 均为 0，θ_{xi} 值如表 1 所示。图 7(c)为第 1 通道中 k' 与 θ_{x1} 叠加生成的密钥相位模板 k_1'，图 7(d)为 h' 与 θ_{x1} 叠加生成的物窗口相位模板 h_1'。

图 5　待加密图像

Fig. 5　Images to be encrypted

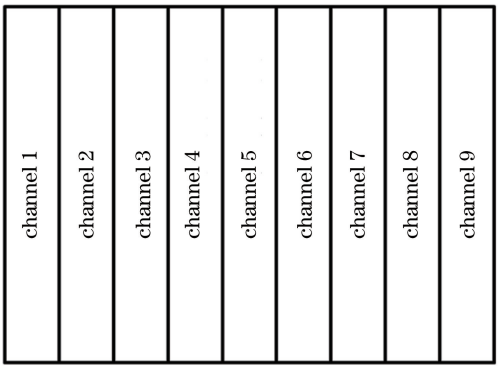

图 6　JPS 横向拼接示意图

Fig. 6　Schematic of spliced JPS in horizontal direction

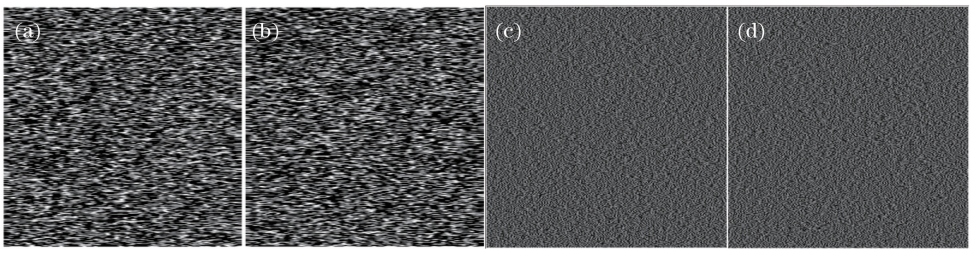

图 7　相位模板。(a)密钥相位核 k';(b)物窗口相位核 h';(c)生成的密钥相位模板 k_1';(d)生成的物窗口相位模板 h_1'

Fig. 7　Phase masks. (a) Key phase kernel k'; (b) object window phase kernel h'; (c) generated key phase mask k_1'; (d) generated object window phase mask h_1'

表 1　偏转角参数

Table 1　Parameters of deflection angle

Deflection angle	Value
θ_{x1} /mrad	22.8711
θ_{x2} /mrad	17.5333
θ_{x3} /mrad	11.4356
θ_{x4} /mrad	5.7178
θ_{x5} /mrad	0
θ_{x6} /mrad	−5.7178
θ_{x7} /mrad	−11.4356
θ_{x8} /mrad	−17.5333
θ_{x9} /mrad	−22.8711

第 1 通道图像加密输入面如图 8(a)所示，其对应的 JPS 如图 8(b)所示。依此方法，采集各通道 JPS 并进行消噪声[29]以及窗口滤波处理，最后进行 9 个通道的零串扰叠加，获得图 8(c)所示的密文。在第 1 通道解密过程中，当输入面仅放置密钥模板 k_1'时，其对应功率谱如图 8(d)所示，进一步验证了上述解密过程中利用密钥模板功率谱区域进行相应通道密文滤波的可行性。图 8(e)为 9 个通道解密图像，CC 值均达到 0.94 以上，解密效果显著。

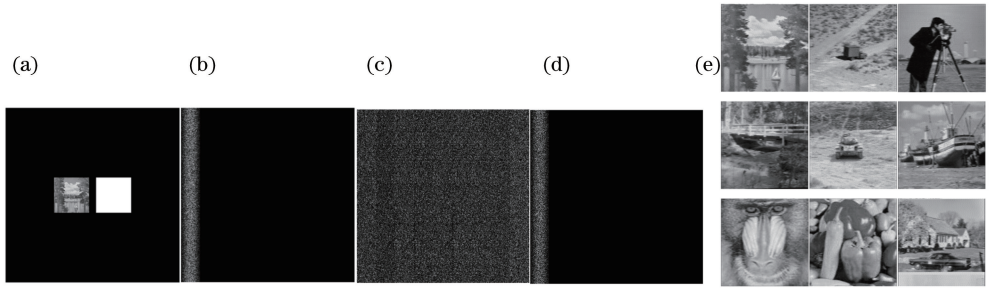

图 8　加、解密过程示意图。(a)第 1 通道输入面;(b)第 1 通道 JPS;(c) 9 个通道的叠加密文;(d)第 1 通道密钥模板功率谱;(e) 9 个通道的解密图像

Fig. 8　Schematic of encryption and decryption processes. (a) Input plane of channel 1; (b) JPS of channel 1; (c) superimposed cipher-text of nine channels; (d) power spectrum from key mask of channel 1; (e) decrypted images of nine channels

图 9(a)为利用正确的第 8 通道对应解密密钥 k_8'进行解密的输出图像；图 9(b)为利用错误的解密密钥进行解密的输出图像，很明显无法获取任何信息。此外，作为本方法中的重要传输数据，偏转角的安全性与敏感性也是十分关键的。图 10 给出了解密过程中 9 个通道的水平偏转角偏移量与 CC 值变化曲线图，图中水平坐标轴上的刻度为负值表示向左偏转，刻度为正值表示向右偏转，0 值两侧曲线基本对称。从图 10 中可以看出，9 个通道的 CC 值随着水平偏转角偏移量变化的趋势基本一致。当水平偏转角偏置达到 0.06 mrad 时，CC 值均低于 0.2，因此攻击者难以在仅截获密钥相位核情况下获取加密图像，具有一定安全性。当水平偏转角偏置达到0.015 mrad时，CC 值在 0.8 附近，解密图像质量依然较高；当偏置达到 0.03 mrad时，CC 值在 0.5 附近，图像内容信息部分可辨。因此，本系统中的水平偏转角偏移量具有一定的容错能力，有利于控制传输过程中的偏转角度取值精度以及降低光学解密过程中的对准难度。

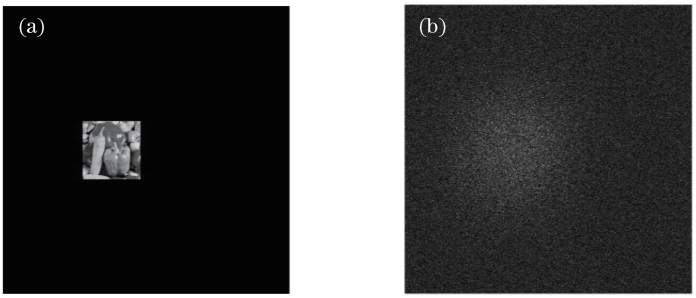

图 9　解密图像。(a)正确密钥解密图像；(b)错误密钥解密图像

Fig. 9　Decrypted images. (a) Decrypted image with correct key; (b) decrypted image with incorrect key

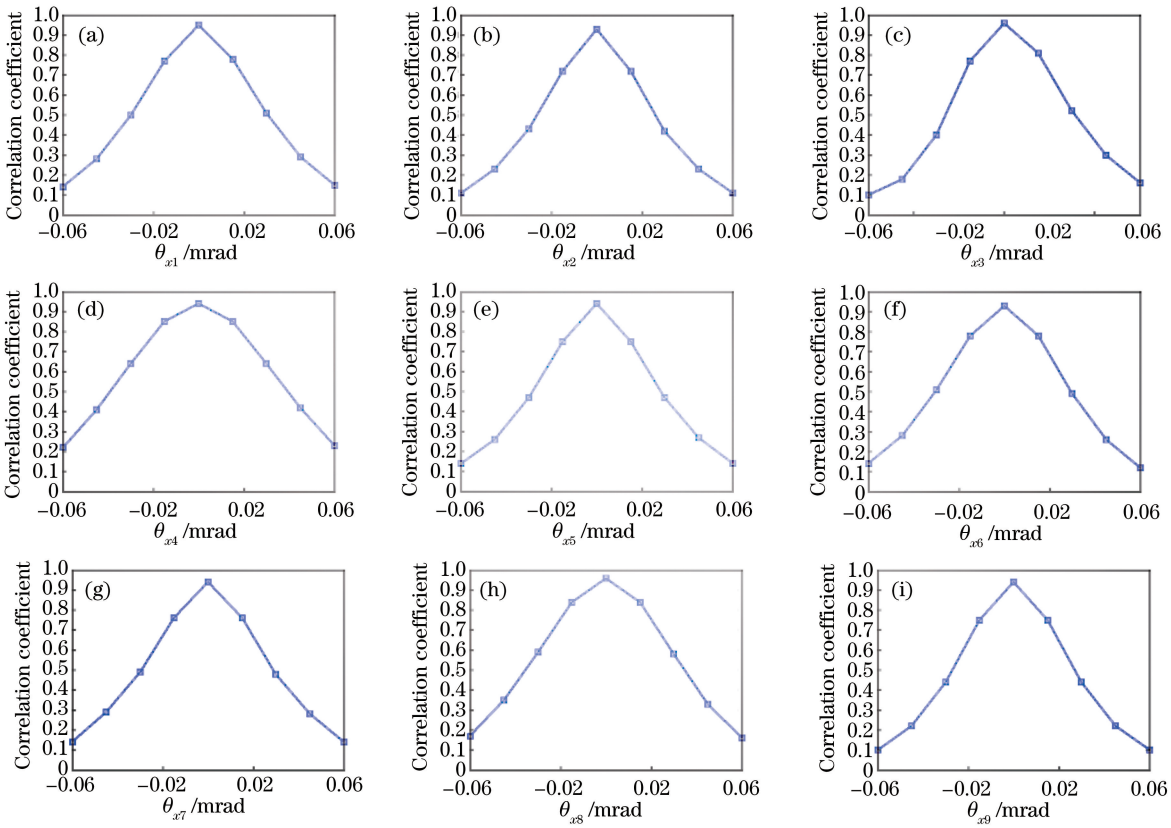

图 10　水平偏转角偏移量与 CC 值关系曲线图。(a)通道 1；(b)通道 2；(c)通道 3；(d)通道 4；(e)通道 5；(f)通道 6；(g)通道 7；(h)通道 8；(i)通道 9

Fig. 10　Relationship between CC value and horizontal offset of deflection angle. (a) Channel 1; (b) channel 2; (c) channel 3; (d) channel 4; (e) channel 5; (f) channel 6; (g) channel 7; (h) channel 8; (i) channel 9

3.2　最大压缩效率分析

对于多图像加密而言，基于一定大小的密文面积，在确保一定图像解密质量的同时，探讨其最大压缩效率是具有重要意义的。基于第 3.1 节所述 JPS 配置方案，通过改变单通道密文面积（以第 8 通道为例），分析了压缩效率因子 E_f 与 CC 值的变化关系，如图 11 所示。当 E_f 达到 32 时，灰度图像“pepper”对应 CC 值仍然达到 0.86，二值图像“A”对应 CC 值可以达到 0.95，该项指标目前远远优于其他多图像加密方法，主要原因在于本文采用的多通道 JPS 零串扰叠加技术。根据(5)式中的 E_{fmax} 概念，将解密质量评判阈值 τ 设定在 0.95，此时针对灰度图像“pepper”的 E_{fmax} 为 12，针对二值图像“A”的 E_{fmax} 为 32，密文压缩能力显著。

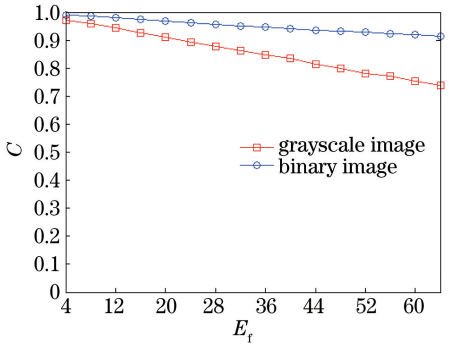

图 11　E_f 与 CC 值关系图

Fig. 11　Relationship between CC value and E_f

4　光学实验研究

为进一步验证本系统的可行性，开展了相关光学实验研究。其中，多图像加密过程由光学方法实现，实验系统原理与实物如图 12 所示。其中，光源选取了 He-Ne 激光器（QJHP-270A，上海埃波激光仪器有限公司，中国），波长为 632.8 nm；空间光调制器（SLM，纯相位反射式 PLUTO-VIS-014 型，Holoeye 公司，德国）的空间分辨率为 1920 pixel×1080 pixel，像素尺寸为 8 μm；CCD 分辨率为 768 pixel×576 pixel，像素尺寸为 8.3 μm；透镜焦距为 400 mm。

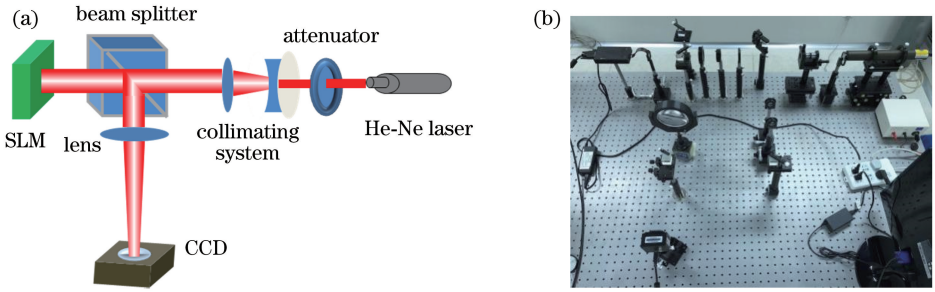

图 12　加密光学实验系统图。(a)示意图；(b)实验平台

Fig. 12　Experimental system of optical encryption. (a) Schematic; (b) experimental platform

本次光学实验拟对 6 个通道的二值图像进行加解密研究，分别为字符“A”、“B”、“D”和数字“6”、“8”、“4”。图 13 为实验过程中使用的 2 个相位核以及第 5 通道对应的密钥相位模板 k_5' 和物窗口相位模板 h_5'。将 h_5' 和待加密二值图像“8”进行叠加后，与 k_5' 共同组成输入面，如图 14(a) 所示，加载至 SLM 上；图 14(b)为 CCD 实际记录的 JPS，图 14(c)为仅加载 k_5' 后由 CCD 记录的功率谱，其位置信息再次验证了上述解密过程中利用密钥模板功率谱区域进行相应通道密文滤波的可行性；图 14(d)为对 6 个通道的消噪声后 JPS 进行窗口区域滤波处理后完成数学叠加后的效果图。解密过程中，由于实验条件的限制，需要在实验系统内引入一路参考光来记录解密光束的相位信息，后续步骤由计算机数值解密来完成。图 14(e)为各通道解密图像，尽管存在一些由于实验器件等因素引入的噪声，但是各通

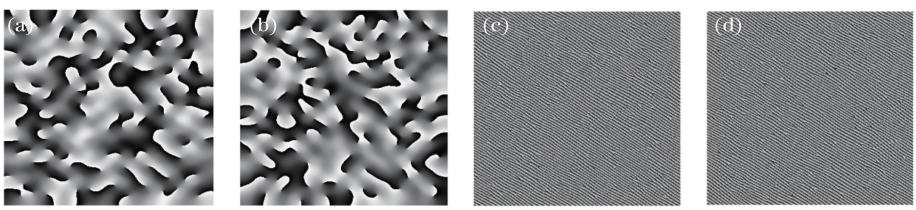

图 13　实验用密钥图。(a)密钥相位核 k'；(b)物窗口相位核 h'；(c)密钥相位模板 k_5'；(d)物窗口相位模板 h_5'

Fig. 13　Keys used in experiment. (a) Key phase kernel k'; (b) object window phase kernel h'; (c) key phase mask k_5'; (d) object window phase mask h_5'

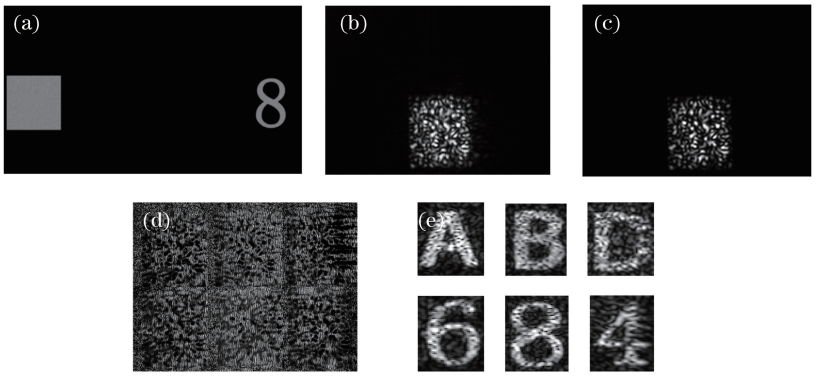

图 14　加、解密过程示意图。(a)第 5 通道输入面;(b)第 5 通道对应的 JPS;(c)第 5 通道对应的密钥功率谱;(d) 6 个通道叠加后的密文;(e) 6 个通道的解密图

Fig. 14　Schematic of encryption and decryption processes. (a) Input plane of channel 5; (b) JPS of channel 5; (c) power spectrum from key mask of channel 5; (d) superimposed cipher-text of six channels; (e) decrypted images of six channels

道图像信息均清晰可辨。

5　结　　论

提出了一种基于 JPS 分区复用的光学多图像加密方法。在分析基于 JTC 的光学图像加解密原理基础上,通过优化相位模板、叠加线性相位以及窗口滤波处理,实现了各通道密文在一定密文面积内的无串扰叠加。数值仿真结果表明,该方法有效提升了密文压缩效率,当解密质量评判阈值 τ 设定在 0.95 时,灰度图像和二值图像的 E_{fmax} 分别达到 12 和 32,密文压缩效果显著。从仿真过程中还可以看出,提出的"密钥相位核+偏转角数据包"密钥内容规划形式具有传递密钥数据量小和分发管理可操作性强的优点,对光学多图像加密领域的密钥分发与管理具有启发意义。最后,搭建光学实验系统验证了该方法的可行性,同时可为光学多图像加密系统的工程化设计提供一定的参考。

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] Unnikrishnan G, Singh K. Double random fractional Fourier domain encoding for optical security [J]. Optical Engineering, 2000, 39(11): 2853-2859.

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

[4] Unnikrishnan G, Joseph J, Singh K. Optical encryption by double-random phase encoding in the fractional Fourier domain[J]. Optics Letters, 2000, 25(12): 887-889.

[5] Peng X, Cui Z Y, Tan T N. Information encryption with virtual-optics imaging system[J]. Optics Communications, 2002, 212(4/5/6): 235-245.

[6] Situ G H, Zhang J J. Double random-phase encoding in the Fresnel domain[J]. Optics Letters, 2004, 29(14): 1584-1586.

[7] Jin W M, Yan C J, Ma L H, *et al*. Joint extended fractional Fourier transform correlator [J]. Optics Communications, 2006, 268(1): 34-37.

[8] Zhang Y, Wang B. Optical image encryption based on interference[J]. Optics Letters, 2008, 33(21): 2443-2445.

[9] Zhou N R, Wang Y X, Gong L H. Novel optical image encryption scheme based on fractional Mellin transform[J]. Optics Communications, 2011, 284(13): 3234-3242.

[10] Kong D Z, Shen X J, Cao L C, *et al*. Three-dimensional information hierarchical encryption based on computer-generated holograms[J]. Optics Communications, 2016, 380: 387-393.

[11] Qin Y, Wang Z P, Wang H J, *et al*. Binary image encryption in a joint transform correlator scheme by aid of run-length encoding and QR code[J]. Optics & Laser Technology, 2018, 103: 93-98.

[12] Liu X Y, Cao Y P, Lu P. Research on optical image encryption technique with compressed sensing [J]. Acta Optica Sinica, 2014, 34(3): 0307002.
刘效勇, 曹益平, 卢佩. 基于压缩感知的光学图像加密技术研究[J]. 光学学报, 2014, 34(3): 0307002.

[13] Cao F, Zhao S M. Optical encryption scheme with double secret keys based on computational ghost imaging [J]. Acta Optica Sinica, 2017, 37(1): 0111001.
曹非, 赵生妹. 基于计算鬼成像的双密钥光学加密方案[J]. 光学学报, 2017, 37(1): 0111001.

[14] Situ G H, Zhang J J. Multiple-image encryption by

wavelength multiplexing[J]. Optics Letters, 2005, 30(11): 1306-1308.

[15] Situ G H, Zhang J J. Position multiplexing for multiple-image encryption[J]. Journal of Optics A: Pure and Applied Optics, 2006, 8(5): 391-397.

[16] Barrera J F, Henao R, Tebaldi M, *et al*. Multiplexing encrypted data by using polarized light [J]. Optics Communications, 2006, 260(1): 109-112.

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

[18] Wang X G, Zhao D M. Multiple-image encryption based on nonlinear amplitude-truncation and phase-truncation in Fourier domain[J]. Optics Communications, 2011, 284(1): 148-152.

[19] Chang H T, Hwang H E, Lee C L. Position multiplexing multiple-image encryption using cascaded phase-only masks in Fresnel transform domain [J]. Optics Communications, 2011, 284(18): 4146-4151.

[20] Rueda E, Rios C, Barrera J F, *et al*. Experimental multiplexing approach via code key rotations under a joint transform correlator scheme[J]. Optics Communications, 2011, 284(10/11): 2500-2504.

[21] Deng X P, Zhao D M. Multiple-image encryption using phase retrieve algorithm and intermodulation in Fourier domain [J]. Optics & Laser Technology, 2012, 44(2): 374-377.

[22] Wu J J, Xie Z W, Liu Z J, *et al*. Multiple-image encryption based on computational ghost imaging[J]. Optics Communications, 2016, 359: 38-43.

[23] Deng P K, Diao M, Shan M G, *et al*. Multiple-image encryption using spectral cropping and spatial multiplexing [J]. Optics Communications, 2016, 359: 234-239.

[24] Wang Q, Alfalou A, Brosseau C. Security enhanced multiple-image authentication based on cascaded optical interference and sparse phase mixed encoding [J]. Optics Communications, 2016, 372: 144-154.

[25] Chen Q, Shen X J, Dou S F, *et al*. Topological charge number multiplexing for JTC multiple-image encryption[J]. Optics Communications, 2018, 412: 155-160.

[26] Trejos S, Barrera J F, Velez A, *et al*. Optical approach for the efficient data volume handling in experimentally encrypted data[J]. Journal of Optics, 2016, 18(6): 065702.

[27] Nomura T, Javidi B. Optical encryption based on the input phase mask designed for the space bandwidth of the optical system [J]. Proceedings of SPIE, 2005, 5908: 59080B.

[28] Lü N G. Fourier optics[M]. Beijing: China Machine Press, 1988: 24-32.
吕乃光. 傅里叶光学[M]. 北京: 机械工业出版社, 1988: 24-32.

[29] Shen X J, Liu X M, Cai N, *et al*. Nonlinear image encryption system based on JTC and its removing noise and resisting attack properties research [J]. Chinese Journal of Lasers, 2015, 42(7): 0709003.
沈学举, 刘旭敏, 蔡宁, 等. 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[J]. 中国激光, 2015, 42(7): 0709003.