文章编号：1005-5630(2023)01-0060-07 **DOI**: 10.3969/j.issn.1005-5630.2023.001.009

基于级联相位检索与关联成像的多图像加密研究

张雷洪[1]，苏亚慧[2]，王凯民[1]，张大伟[1]，彭 伟[3]，吴丰收[3]，周 洁[4]
（1. 上海理工大学 光电信息与计算机工程学院，上海 200093；
2. 上海理工大学 出版印刷与艺术设计学院，上海 200093；
3. 中船勘察设计研究院有限公司，上海 200063；
4. 上海工程技术大学 图书馆，上海 201620）

摘要：光学信息处理技术本身具有高速度、并行性、信息容量大的特点。同时，光波又具有振幅、相位、波长、偏振等多种属性，是多维信息的载体。因此，光学加密在信息安全传输领域意义重大。现有的图像加密方法存在效率低、安全性差、加密容量小等问题。为了实现多图像二次加密传输，提出了一种基于级联相位迭代与计算关联成像的多图像加密算法。该方法可以同时对多幅图像进行高效加密，计算简单，安全可靠，传输数据少。利用相关系数指标评估了该方法的加密效果，并通过仿真实验验证了该方法的有效性和安全性。

关键词：级联相位检索算法；计算关联成像；图像处理；多图像加密
中图分类号：TP 309.7 **文献标志码：**A

Multiple image encryption studies based on a cascaded phase retrieval and ghost imaging

ZHANG Leihong[1], SU Yahui[2], WANG Kaimin[1], ZHANG Dawei[1],
PENG Wei[3], WU Fengshou[3], ZHOU Jie[4]
（1. School of Optical-Electrical and computer Engineering, University of Shanghai for Science and Technology, Shanghai 200093, China;
2. College of Communication and Art Design, University of Shanghai for Science and Technology, Shanghai 200093, China;
3. China Shipbuilding Industry Institute of the Engineering Investigation and Design Co., Ltd., Shanghai 200063, China;
4. Library, Shanghai University of Engineering Science, Shanghai 201620, China）

Abstract: Optical information processing technology has the characteristics of high speed and parallelism. The wavelength of light is short and the information capacity is large. At the same time, it has many attributes such as amplitude, phase, wavelength and polarization, which could be the carrier of multi-dimensional information. Therefore, optical encryption is of great significance in

收稿日期：2022-09-08
基金项目：国家自然科学基金 (61775140，61875125)；上海市自然科学基金 (18ZR1425800)
第一作者：张雷洪 (1981—)，男，教授，研究方向为印刷包装技术与数据模拟仿真。E-mail：zlh12345_2004@sina.com.cn
通信作者：苏亚慧 (1996—)，女，硕士研究生，研究方向为光学图像加密、图像处理。E-mail：yhsucn@163.com

the field of information security transmission and is widely used in the field of image encryption. For multiple image encryption, this paper proposes a multi image encryption algorithm based on cascaded phase iteration and computational ghost imaging. This method can encrypt multiple images efficiently at the same time, which is simple, safe and reliable, and has less transmission data. The encryption effect of this method is evaluated by using correlation coefficient, and the effectiveness and security of this method are verified by simulation.

Keywords: cascaded phase retrieval algorithm; computational ghost imaging; image processing; multi-image encryption

引　言

光学信息安全技术有着高维度、高并行处理速度以及能快速实现卷积和相关运算的特点[1-3]，在信息安全领域，光学信息安全技术的优势越来越明显。其中，相位检索算法在光学安全领域引起了广泛的关注。但基于单图像的研究不能满足当下人们对信息处理效率的要求。与单幅图像的光学加密技术相比，多图像加密技术可以在一幅图像中包含多重图像的信息，提高加密图像的容量和效率，这是多用户认证和内容分散的基础。

多图像光学加密技术作为光学加密的一个重要分支，不仅提高了加密能力，而且减少了密文传输数据。以关联成像（ghost imaging, GI）为基础的多图像加密方法相继被提出。Li 等[4] 提出了一种基于关联成像和坐标采样的多图像加密方法，将改进的 Logistic 映射和坐标采样与关联成像相结合，减少了密文的传输量。Li 等[5] 提出了基于计算关联成像（computational ghost imaging, CGI）和提升小波变换并结合异或操作的多图像加密方法，提高了加密系统的安全性。Wu 等[6] 利用位置复用将测量的不同衍射距离的矢量强度进行迭加并与 GI 结合，提高了图像的传输效率。Zhang 等[7] 将相位恢复与 GI 相结合，提出了一种基于相位恢复算法和 GI 的多图像全息加密技术。Sui 等[8] 提出了一种基于强度方程传输的光学多图像认证方法，并应用强度方程传输技术实现了光学多图像认证。目前，这些多图像加密方法虽然提高了加密图像的数量，但也增加了系统的复杂性。同时，随着加密容量的增加，数据处理的时间和复杂度也随之增加。而且由于单一技术加密方法的局限性，这些多图像加密方法大多是基于多种技术手段的组合[9-11]。

本文提出了一种级联相位检索算法（cascaded phase retrieval algorithm, CPRA）与 CGI 相结合的方法。它可以在没有串扰的情况下大大增强加密容量。首先，利用输入图像与目标图像之间的相位检索算法，对每个输入图像进行相位编码，得到目标图像与输入图像之间的相位掩膜对。然后，将得到的最终目标图像经一组调制散斑照明，并由桶探测器记录测量数据，获得最终的密文。该系统的密钥由 CPRA 加密阶段的两个相位掩膜、CPRA 输出平面上的相位分布以及关联成像阶段的调制相位组成，大大提升了密钥空间的维度。本文通过仿真实验验证了加密系统的性能。实验结果表明，所提出的加密系统不仅具有较好的安全性，而且能够抵抗噪声、裁剪等攻击，同时也具有较好的加密容量。

1　基于 CPRA 与 CGI 的多图像加密原理

1.1　CPRA 加密原理

基于单一的 4f 相关器的光学加密系统的体系结构如图 1 所示。输入输出平面和傅里叶平面的坐标分别用 (x,y) 和 (u,v) 表示；$f(x,y)$ 表示待加密图像；$g(x,y)$ 表示目标图像。随机相位掩码 $RPM1$ 和 $RPM2$ 分别写为 $\exp[\mathrm{i}\theta(x,y)]$ 和 $\exp[\mathrm{i}\varphi(u,v)]$。因此，将 $f(x,y)$ 加密到 $g(x,y)$ 的过程实际上是一个寻找正确的相位掩膜对 $\exp[\mathrm{i}\theta(x,y)]$ 和 $\exp[\mathrm{i}\varphi(u,v)]$ 的问题。CPRA 可以在待加密图像

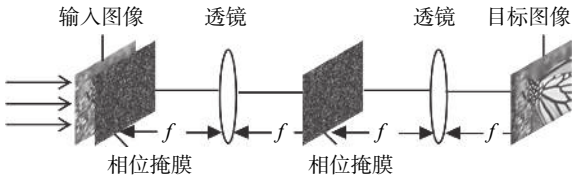


图 1 4*f* 相关器的光学加密系统

Fig. 1 Optical encryption system for the 4*f* correlator

$f(x,y)$和目标图像$g(x,y)$之间的强度约束下进行搜索[12]。CPRA 由多个循环迭代组成，它受两个强度或振幅图像的约束，每个循环都涉及正向和反向传播。在第$k(k=1,2,3\cdots)$步的前向迭代中，这两个相位分布函数可以描述为$\theta^k(x,y)$和$\varphi^k(u,v)$。因此，执行每次前向迭代后的输出图像可以写为

$$\begin{aligned} g^k(x,y)\exp\left[\mathrm{i}\phi^k(x,y)\right]=&\\ IFT\left(FT\left\{f(x,y)\exp\left[\mathrm{i}\theta^k(x,y)\right]\right\}\times&\\ \exp\left[\mathrm{i}\varphi^k(u,v)\right]\right)& \end{aligned} \tag{1}$$

式中：FT和IFT分别表示傅里叶变换和傅里叶反变换；$g^k(x,y)$是第k次迭代近似振幅图像；$\phi^k(x,y)$是输出平面上的第k次迭代相位；$f(x,y)$是每个前向迭代中的约束条件，并保持不变。反向迭代中的图像也可以用同样的方式来处理。在这种情况下，在每次反向迭代中，$g^k(x,y)$被$g(x,y)$作为加密的目标图像。而这两个相位分布函数在每个循环中都可以被更新为

$$\begin{aligned} \varphi^{k+1}(u,v)=&angle\left\{\frac{FT\left\{g(x,y)\exp\left[\mathrm{i}\phi^k(x,y)\right]\right\}}{FT\left\{f(x,y)\exp\left[\mathrm{i}\theta^k(x,y)\right]\right\}}\right\}\\ \theta^{k+1}(x,y)=&angle\left\{IFT\left(FT\left\{g(x,y)\exp\left[\mathrm{i}\phi^k(x,y)\right]\right\}\times\right.\\ &\left.\exp\left[-\mathrm{i}\varphi^{k+1}(u,v)\right]\right)\Big\} \end{aligned} \tag{2}$$

式中，$angle\{\cdot\}$表示相位提取操作。在每个循环中，两个相位分布同时被修改。初始阶段$\theta^1(x,y)$和$\varphi^1(u,v)$随机分布在区间$[0,2\pi]$上。对于不同的初始相分布，获得的相位对如式(2)所示，是不同的。该算法的迭代次数由$g(x,y)$和$g^k(x,y)$之间的相关系数(correlation coefficient, CC)来控制。*CC*可以表示为

$$CC=\frac{cov\left[g(x,y),g^k(x,y)\right]}{\sigma_g\sigma_{g^k}} \tag{3}$$

式中：$cov\left[g(x,y),g^k(x,y)\right]$是$g(x,y)$和$g^k(x,y)$之间的协方差；$\sigma_g$和$\sigma_{g^k}$是$g(x,y)$和$g^k(x,y)$的标准差。当$g(x,y)$与$g^k(x,y)$之间的*CC*值大于设定的阈值，则迭代过程将停止。为了得到加密的目标图像，对输入平面上的$f(x,y)\exp\left[\mathrm{i}\theta^k(x,y)\right]$进行傅里叶变换，并乘以相位项$\exp\left[\mathrm{i}\varphi^k(u,v)\right]$，然后对它们进行傅里叶反变换，最后进行绝对值运算，得到加密的目标图像。最终得到的振幅图像$g^k(x,y)$近似于目标图像$g(x,y)$。根据参考文献[13]可知，在迭代次数达到 10 次后，便可以获得较为不错的效果。

1.2 CGI 加密原理

GI 作为一种非局域成像方式，在成像时，经过空间光调制器调制的光束先被分成参考光路和物体所在光路，然后经光学器件收集光学信息。参考光路和物体光路的光学信息经过二阶关联计算，可以实现对信息的重构[14]。而 CGI 方法则简化了装置，省略了参考光路，见图 2。

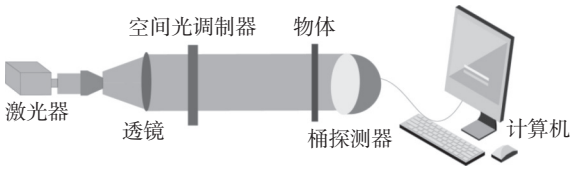


图 2 CGI 原理图

Fig. 2 Schematic diagram of CGI

在 CGI 过程中，只需要一个桶探测器来获取密文B_i。B_i可表示为

$$B_i=\int T(x,y)\,I_i\left(x_p,y_q\right)\mathrm{d}x\mathrm{d}y \tag{4}$$

式中，$T(x,y)$为要加密的图像。在加密过程中，将大小为$n\times n$的二维图像$T(x,y)$转化为一个一维列向量($n^2\times1$)。由式(4)可以得到第i次的光强分布函数为$I_i\left(x_p,y_q\right)$，其中$i=1,2,\cdots,N$；$p,q=1,2,\cdots,n$。光强分布函数的矩阵表达式为

$$\boldsymbol{I}_i=\begin{vmatrix} I_{11}^i & \cdots & I_{1n}^i \\ \vdots & & \vdots \\ I_{n1}^i & \cdots & I_{nn}^i \end{vmatrix} \tag{5}$$

式中，I_{nn}^i是第i次测量矩阵中，第n行第n列的元素。光强分布矩阵的大小为$n\times n$，将矩阵拉伸成一个一维行向量，其大小为($1\times n^2$)，该向

量可表示为

$$\boldsymbol{I}_i=\left[\begin{array}{cccccc} I_{11}^i & I_{12}^i & \cdots & I_{1n}^i & I_{21}^i & I_{22}^i & \cdots \\ I_{nn-1}^i & I_{nn}^i \end{array}\right] \tag{6}$$

但 CGI 的检测和重构时间较长。为解决这一问题，有学者提出一种压缩感知（compressed sensing, CS）的 CGI 算法。它利用压缩感知的特性，以较少的测量次数恢复出高质量的图像。当测量次数为 M（$M<n^2$）时，将生成 M 个大小为 $n\times n$ 的一维行向量。由此得到一个大小为 $M<n^2$ 测量矩阵，以此用作 CGI 的测量矩阵。桶探测器接收到的总强度 $\{B_i\}_{i=1}^M$ 可以表示为：

$$\left[\begin{array}{c} B_1 \\ B_2 \\ \vdots \\ B_M \end{array}\right]=\left[\begin{array}{ccccc} I_{11}^1 & \cdots & I_{1n}^1 & \cdots & I_{nn}^1 \\ I_{11}^2 & \cdots & I_{1n}^2 & \cdots & I_{nn}^2 \\ \vdots & & \vdots & & \vdots \\ I_{11}^M & \cdots & I_{1n}^M & \cdots & I_{nn}^M \end{array}\right]\cdot \left[\begin{array}{c} T_{11} \\ \vdots \\ T_{1n} \\ \vdots \\ T_{nn} \end{array}\right] \tag{7}$$

在解密过程中，光强分布函数 $I_i(x,y)$ 和探测得到的光强分布数据 B_i 联合计算可解出秘密图像信息，可以表示为：

$$T_{\mathrm{CS}}(x,y)=\langle B_i I_i(x,y)\rangle-\langle B_i\rangle\langle I_i(x,y)\rangle \tag{8}$$

式中，$\langle\cdot\rangle$ 表示平均操作。

根据 CS 重建原始信号的原理，可以通过凸优化算法重建原始图像。

$$T_{\mathrm{CS}}=T',\arg\min\left\|\Psi\{T'(x,y)\}\right\| \tag{9}$$

2　基于 CPRA 与 CGI 的多图像加解密流程

加密流程：

结合基于 4f 的 N 个单图像加密方法对多图像进行编码，如图 3 所示。在该方法中，N 个目标图像对应 N 个输入图像，利用输入图像 $g_{0n}^k(x,y)$ 与目标图像 $g_{0n+1}(x,y)$ 之间的相位检索算法，对每个输入图像编码不同的 $\exp(\mathrm{j}\varphi_k)$ 和

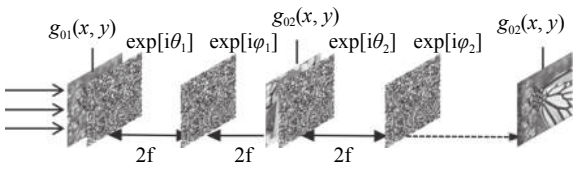


图 3　CPRA 加密系统

Fig. 3　CPRA encryption system

$\exp(\mathrm{j}\theta_k)$。通过使用这些相位掩码，可以对图像 $g_{0n}^k(x,y)$ 进行如下编码

$$g_{0n+1}^k\exp(\mathrm{i}\phi_n)=IFT\left\{FT\left[g_{0n}^k\exp(\mathrm{i}\theta_n)\right]\exp(\mathrm{i}\varphi_n)\right\} \tag{10}$$

式中：下标 n 表示图像的数量。由此输入图像 g_{0n}^k 则是由 $g_{0n}^k\exp(\mathrm{i}\phi_{n-1})$ 经过光学加密系统加密所得，$g_{0n+1}^k\exp(\mathrm{i}\phi_n)$ 则可以表示为

$$\begin{aligned} g_{0n+1}^k\exp(\mathrm{i}\phi_n)=&IFT\left\{FT\left[g_{0n}^k\exp(\mathrm{i}\phi_{n-1})\exp(-\mathrm{i}\phi_{n-1})\times\right.\right. \\ &\left.\left.\exp(\mathrm{i}\theta_n)\right]\exp(\mathrm{i}\varphi_n)\right\} \end{aligned} \tag{11}$$

进一步整理多图像加密的等式为

$$\begin{aligned} g_{0n+1}^k\exp(\mathrm{i}\phi_n)=&IFT\left[FT\left\{g_{0n}^k\exp(\mathrm{i}\phi_{n-1})\times\right.\right. \\ &\left.\left.\exp[\mathrm{i}(\theta_n-\phi_{n-1})]\right\}\right]\exp(\mathrm{i}\varphi_n) \end{aligned} \tag{12}$$

将最后一张目标图像经一组调制散斑照明，并由桶探测器记录测量数据，过程见公式（7）。将获取的密文 B_i、每对输入图像与目标图像之间相位掩码 $\exp(\mathrm{j}\varphi_k)$ 和 $\exp(\mathrm{j}\theta_k)$ 以及光强分布函数 $I_i(x,y)$ 传输给接收方，加密过程就完成了。

解密流程：

在解密过程中，光强分布函数 $I_i(x,y)$ 和探测得到的光强分布数据 B_i 联合计算可解出秘密图像信息，具体过程可以表示为公式（8），得到初级加密后的最后一张目标图像。多图像编码方法的解密阶段计算为

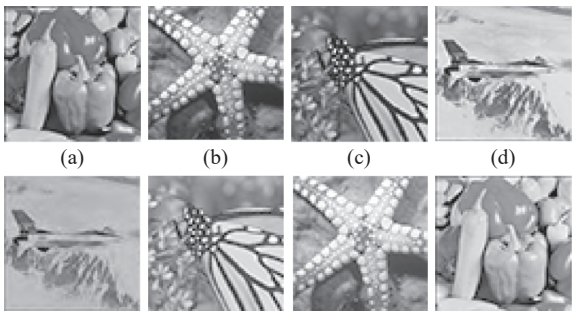
$$\begin{aligned} g_{0n}^k\exp(\mathrm{i}\phi_{n-1})=&IFT\left[FT\left\{g_{0n+1}^k\exp(\mathrm{i}\phi_n)\times\right.\right. \\ &\left.\left.\exp(-\mathrm{i}\varphi_n)\right\}\right]\times\exp[-\mathrm{i}(\theta_n-\theta_{n-1})] \end{aligned} \tag{13}$$

由此可以依次解密出第 $N,N-1,N-2,\cdots,1$ 张明文图像。

3　仿真与分析

利用 CPRA 与 CGI 相结合的方法，将 4 张明文图像加密成最终的桶探测器值，使用正确密

钥解密结果如图 4 所示。图 4(a)为输入图像，图 4(b)~(d)为目标图像，图 4(e)~(h)为密钥完全正确情况下解密结果。解密图像与原输入图像间 *CC* 值分别为 0.9975，0.9932，0.9951，0.9967。结果表明，该系统解密图像的质量非常好。



(a)输入图像，(b)~(d)目标图像，(e)~(h)解密图像

图 4　加解密结果

Fig. 4　Encryption and decryption of the results

为了验证该加密系统的级联特性，在图 5 中给出不同阶次相位掩码错误时的解密情况。图 5(a)~(d)显示了 CPRA 解密阶段最后一个编码图像的相位密钥错误时的解码图像；图 5(e)~(h)显示了二阶编码图像的相位掩码错误时对应的解密图像；图 5(i)~(l)显示了在第一阶编码的图像的相位掩码错误时对应的解密图像。从图中可以看出，如果在解密的第一阶段使用了错误的密钥，则无法访问图像。这是由于其级联特性，各用户在接收端相互依赖。在解密前一个图像之前，当前的图像将不会被解密，因为输入的图像是连续加密的。

在信息的加密和传输过程中，噪声的影响是不可避免的。因此，一个合格的加密系统需要具有一定的鲁棒性。引入了标准差(σ)分别为 0.1，0.2，0.3 时的高斯噪声来模拟由光学器件引起的热噪声。

从表 1 可以看出：(1)对于高斯噪声，随着标准差的增加，重构效果呈下降趋势；(2)当噪声标准差达到 0.3 时，解密图像与原始图像之间的 *CC* 保持在 0.48 以上，仍能得到图像的部分信息。结果表明，系统中光学器件产生的热噪声对图像的解密质量有较大的影响，但该系统具有一定的抗噪声攻击能力。

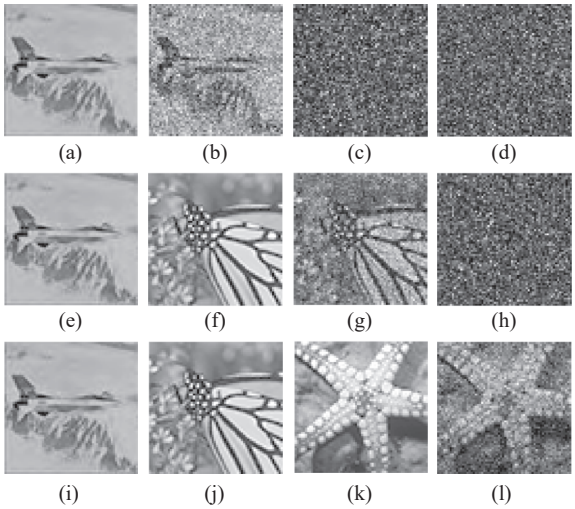


图 5　CPRA 阶段不同阶次相位掩码错误时的解密情况

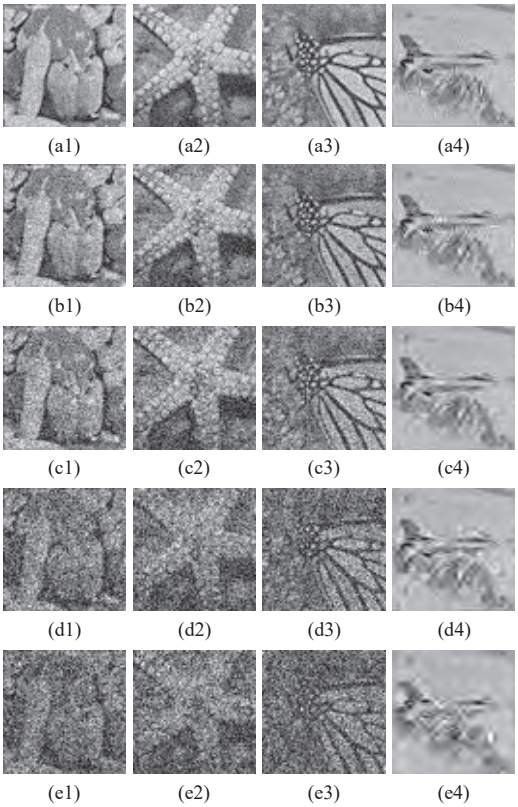
Fig. 5　Decryption of different orders of subphase mask errors in the CPRA

表 1　不同标准差下明文图像与解密图像的相关系数

Tab. 1　Correlation coefficient between plaintext images and decrypted images at different standard deviations

标准差	相关系数			
	辣椒	海星	蝴蝶	飞机
$\sigma=0.1$	0.8888	0.9129	0.9137	0.8739
$\sigma=0.2$	0.6794	0.7296	0.7159	0.8970
$\sigma=0.3$	0.4843	0.5475	0.5539	0.8100

对密文在不同位置进行不同程度的裁剪，选用 *CC* 作为评价指标来验证加密系统的抗裁剪攻击性能。由表 2 和图 6 可知：(1)随着密钥裁剪面积的增加，重构图像与原始图像之间的 *CC* 值逐渐减小，重构图像的清晰度越低，越难分辨出原始图像的信息；(2)当裁剪比例为 30% 时，重构出的图像与原始图像的 *CC* 值均在 0.78 以上，能够大致地分辨出原始图像的细节信息，重构的效果较好；(3)当密钥的裁剪比例为 50% 时，重构出的图像与原始图像的 *CC* 值均大于 0.50，仍可分辨出加密图像的部分信息，说明该方法能够较好地抵抗裁剪攻击。综上可得：本文所提出的加密系统不仅对噪声攻击表现出良好的鲁棒性，而且能够抵抗裁剪攻击，进一步表明该加密系统具有较好的鲁棒性。



(a1)~(a4)、(b1)~(b4)、(c1)~(c4)、(d1)~(d4)、(e1)~(e4)裁剪比例分别是 10%，20%，30%，40%，50%

图 6　不同裁剪程度下的明文图像解密结果

Fig. 6　Decryption results of plaintext images under different cropping degrees

表 2　不同裁剪程度下明文图像与解密图像的相关系数

Tab. 2　Correlation coefficient between plaintext images and decrypted images under different cropping process rates

裁剪比例	相关系数			
	辣椒	海星	蝴蝶	飞机
10%	0.9458	0.9547	0.9555	0.9807
20%	0.8766	0.8912	0.8934	0.9589
30%	0.7877	0.8285	0.8294	0.9024
40%	0.6306	0.6671	0.6728	0.8341
50%	0.5298	0.5715	0.5710	0.7530

4　结 论

本文提出了一种基于 CPRA 和 CGI 的多图像加密方法，该方法可以通过纯光学方法实现。与传统的 CPRA 方法相比，系统中增加了 CGI 加密过程，不仅增加了密钥空间，提高了整个系统的安全性，而且密文的形式为一系列桶探测器值，利于传输与存储，由此提高了整个加密系统的抗裁剪攻击能力。该方法拓展了 CGI 加密的容量，具有更好的实用性和应用前景。

参考文献：

[1] MATOBA O, NOMURA T, PEREZ-CABRE E, et al. Optical techniques for information security[J]. Proceedings of the IEEE, 2009, 97(6): 1128 – 1148.

[2] XIAO D, LI X W, LIU S J, et al. Encryption and display of multiple-image information using computer-generated holography with modified GS iterative algorithm[J]. Optics Communications, 2018, 410: 488 – 495.

[3] JAVIDI B. Optical information processing for encryption and security systems[J]. Optics & Photonics News, 1997, 8(3): 28.

[4] LI X Y, MENG X F, YANG X L, et al. Multiple-image encryption based on compressive ghost imaging and coordinate sampling[J]. IEEE Photonics Journal, 2016, 8(4): 3900511.

[5] LI X Y, MENG X F, YANG X L, et al. Multiple-image encryption via lifting wavelet transform and XOR operation based on compressive ghost imaging scheme[J]. Optics and Lasers in Engineering, 2018, 102: 106 – 111.

[6] 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.

[7] ZHANG L H, ZHANG Z S, YE H L, et al. Multi-image holographic encryption based on phase recovery algorithm and ghost imaging[J]. Applied Physics B, 2020, 126(8): 136.

[8] SUI L S, ZHAO X Y, HUANG C T, et al. An optical multiple-image authentication based on transport of intensity equation[J]. Optics and Lasers in Engineering, 2019, 116: 116 – 124.

[9] WANG Y, ZHANG L H, ZHANG D W, et al. Research on multiple-image encryption scheme based on joint power spectral division multiplexing and ghost imaging[J]. Laser Physics, 2021, 31(5): 055204 (12pp).

[10] ZHAO T Y, CHI Y Y. Hierarchical visual cryptography for multisecret images based on a modified phase retrieval algorithm[J]. Multimedia

Tools and Applications, 2020, 79(17/18): 12165 – 12181.

[11] MEI X D, WANG C L, FANG Y M, et al. Influence of the source's energy fluctuation on computational ghost imaging and effective correction approaches[J]. Chinese Optics Letters, 2020, 18(4): 042602.

[12] HAZER A, YILDIRIM R. A review of single and multiple optical image encryption techniques[J]. Journal of Optics, 2021, 23(11): 113501.

[13] XIAO Y L, ZHOU X, YUAN S, et al. Multiple-image optical encryption: an improved encoding approach[J]. Applied Optics, 2009, 48(14): 2686 – 2692.

[14] KANG Y, ZHANG L H, YE H L, et al. One-to-many optical information encryption transmission method based on temporal ghost imaging and code division multiple access[J]. Photonics Research, 2019, 7(12): 1370 – 1380.

（编辑：李晓莉）