

## 结合计算全息和频移的 JTC 系统多图像光学加密方法

郑伟<sup>1</sup>, 席思星<sup>2</sup>, 王桂林<sup>1</sup>, 李永宏<sup>1</sup>, 姜其畅<sup>1</sup>

(1. 运城学院 物理与电子工程系, 山西 运城 044000;  
2. 河北工程大学 数理科学与工程学院, 河北 邯郸 056038)

**摘要:** 为了提高 JTC 光学图像加密系统的实用性, 解决其噪声问题, 提高其加密效率和安全性, 提出了一种基于计算全息和傅里叶变换频移特性的 JTC 系统多图像光学加密方法。首先多幅不同尺寸和类型的图像经过随机相位调制和傅里叶变换, 然后傅里叶频谱经过频移相位调制后叠加并编码为二元实值计算全息图, 最后经过 JTC 光学图像加密系统完成加密。解密时, 加密图像经过 4F 系统解密获得计算全息图, 二元实值计算全息图具有很强的抗噪性, 可消除噪声, 然后经过傅里叶变换获得多幅解密图像。仿真实验结果表明, 该方法可实现多幅不同尺寸和类型图像的并行加密和解密, 具有高加密效率, 同时多幅图像互为密钥和双重光学密钥使得该方法具有很高的安全性。

**关键词:** 光学图像加密; 信息安全; 计算全息; JTC 系统

中图分类号: O438.1; TP391 文献标志码: A DOI: 10.3788/IRLA20220175

## Multi-image optical encryption method of JTC system combining CGH and frequency shift

Zheng Wei<sup>1</sup>, Xi Sixing<sup>2</sup>, Wang Guilin<sup>1</sup>, Li Yonghong<sup>1</sup>, Jiang Qichang<sup>1</sup>

(1. Department of Physics and Electronic Engineering, Yuncheng University, Yuncheng 044000, China;  
2. School of Mathematics and Physics Science and Engineering, Hebei University of Engineering, Handan 056038, China)

**Abstract:** In order to improve the practicability of JTC optical image encryption system, solve its noise problem, improve its encryption efficiency and security, a multi-image optical encryption method based on computer generated hologram (CGH) and the frequency shift of Fourier transform was proposed. Firstly, each image with different size and type was modulated by random phase and Fourier transform, then the frequency spectrum of multiple images was modulated by frequency-shift phase and superimposed to be encoded into binary real-value CGH, finally the CGH was encrypted into joint power spectrum by JTC optical image encryption system. In the decryption process, the encrypted image was decrypted by 4F system to obtain the CGH. The binary real-value CGH has strong noise resistance to eliminate the effects of noise. Then, multiple decrypted images can be obtained after Fourier transform. Simulation results show that the proposed method can encrypt and decrypt multiple images of different sizes and types in parallel, and has high encryption efficiency. Meanwhile, multiple images with mutual keys and double optical keys ensure the security of the encryption system.

**Key words:** optical image encryption; information security; computer generated hologram (CGH); JTC system

收稿日期: 2022-03-13; 修订日期: 2022-04-05

基金项目: 国家自然科学基金 (11904073); 河北省自然科学基金 (F2019402351); 河北省教育厅青年拔尖人才项目 (BJ2020028); 山西省科技创新项目 (2019L0877); 来晋科研专项项目 (QZX-2018012); 运城学院博士科研启动项目 (YQ-2017015); 运城学院学科建设项目

作者简介: 郑伟, 男, 讲师, 博士, 主要从事光学信息处理和太赫兹功能器件方面的研究。

## 0 引言

自 1995 年 Refrefereer 和 Javidi 提出双随机相位光学图像加密系统以来<sup>[1]</sup>, 光学图像加密技术得到了迅速发展<sup>[2-5]</sup>。许多改进的光学图像加密系统不断被提出, 例如基于菲涅耳变换的加密系统<sup>[6]</sup>、基于数字全息加密系统<sup>[7-8]</sup>、基于压缩感知的加密系统<sup>[9-10]</sup>、基于混沌的加密系统<sup>[11-12]</sup>和基于偏振的加密系统<sup>[13-14]</sup>。其中最具代表性的是 Nomura 和 Javidi 于 2000 年提出的基于联合变换相关器 (JTC) 的光学图像加密系统, 由于其结构简单, 不需要制作复共轭相位密钥, 加密结果是一个振幅型的联合功率谱图像, 便于记录和传输, 因此成为研究热点<sup>[15-18]</sup>。然而, JTC 图像加密系统也存在严重缺陷, 一是解密图像质量差, 存在严重的噪声, 二是线性 JTC 图像加密系统安全性差, 易被攻击。为了提高解密图像的质量, G-S 算法和基于模糊控制理论的迭代算法 (IAFC)<sup>[19-20]</sup>被引入, 用于设计随机相位密钥, 使傅里叶频谱尽可能均匀来降低噪声。但此类方法需要复杂的数学迭代运算和编程。为了提高 JTC 加密系统的安全性, 像素置乱技术和分数傅里叶变换技术被引入, 安全性提高但系统的复杂性也随之增加, 且噪声问题仍未解决, 解密图像质量较差。近年来, 随着大数据技术的飞速发展和信息传输能力的提高, 传统的单幅图像加密技术已经不能满足日益增长的信息需求。因此, 光学多图像加密技术已成为研究热点之一<sup>[21-24]</sup>。由于 JTC 系统在信息加密方面的突出特点, 基于 JTC 系统的多图像加密方法也被提出。例如 Tebaldi 在 JTC 结构中利用波长复用技术实现了多图像光学加密<sup>[25]</sup>。Qin 等人提出了一种利用相位密钥旋转复用技术的 JTC 系统多图像加密方法<sup>[26]</sup>。然而, JTC 系统固有的噪声问题以及多图像之间的串扰问题都没有解决。计算全息技术具有操作灵活、重复性高和大容量等特性, 且本身具有一定的加密性质, 并能通过二维计算全息图实现三维信息的维度压缩, 具有更容易保存、传输和重建三维场景的优势, 成为图像信息加密领域研究的热点。例如基于计算全息和随机相位编码的三维信息加密方法<sup>[27]</sup>、基于计算全息和混沌的彩色图像加密方法等<sup>[28]</sup>。

针对 JTC 加密系统的固有噪声问题 and 安全性低

的问题, 文中将计算全息技术引入 JTC 系统, 提出一种基于计算全息图 (CGH) 和频移的 JTC 系统多图像光学加密方法, 将 CGH 引入 JTC 光学图像加密系统, 在解决其噪声和安全性问题的同时, 提高系统加密效率。首先多个不同类型和尺寸的图像被随机相位和傅里叶变换, 然后傅里叶频谱经过频移相位调制后叠加并编码为二元实值计算全息图。之后在 JTC 图像加密系统中对二进制实值加密 CGH 进行加密, 联合功率谱作为最终的加密图像。在解密过程中, 首先在 4F 解密系统中获得带有噪声的二进制实值 CGH, 然后通过数字图像处理去噪方法或手动去噪方法进行二元实值 CGH 的降噪复原, 最后经过正确光学密钥调制和傅里叶变换可以获得多幅解密图像。因此, 将 CGH 和频移技术引入 JTC 图像加密系统中, 解决了其固有的噪声问题, 极大地提高了其安全性和加密效率, 可实现多个不同类型和尺寸图像的并行加密, 不存在图像之间的串扰。因此, 该研究在网络安全和信息保护方面具有一定的应用前景和实用价值。

## 1 加密过程

待加密图像如图 1 所示, 其中图 1(a) 和 (b) 为两幅单个汉字的二值图像, 尺寸为 128×128 pixel; 图 1(c) 为一幅英文单词二值图像, 图 1(d) 为一幅灰度图像, 它们的尺寸为 128×256 pixel; 图 1(e) 为一幅 2 bit 量化的灰度图像, 尺寸为 256×128 pixel; 图 1(f) 为一幅二维码图像, 图 1(g) 为一幅灰度图像, 它们的尺寸为 256×256 pixel。

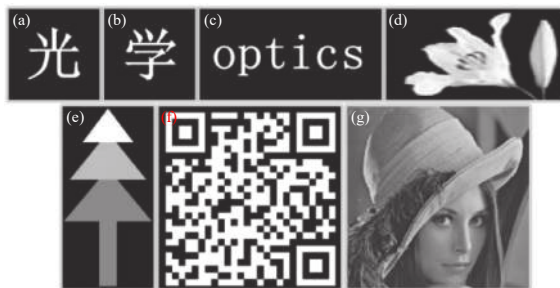


图 1 七幅不同尺寸和类型的待加密图像

Fig.1 Seven images of different sizes and types to be encrypted

文中多个图像加密分为两步完成, 第一步为随机相位和频移相位调制及计算全息编码, 加密过程如图 2 所示。

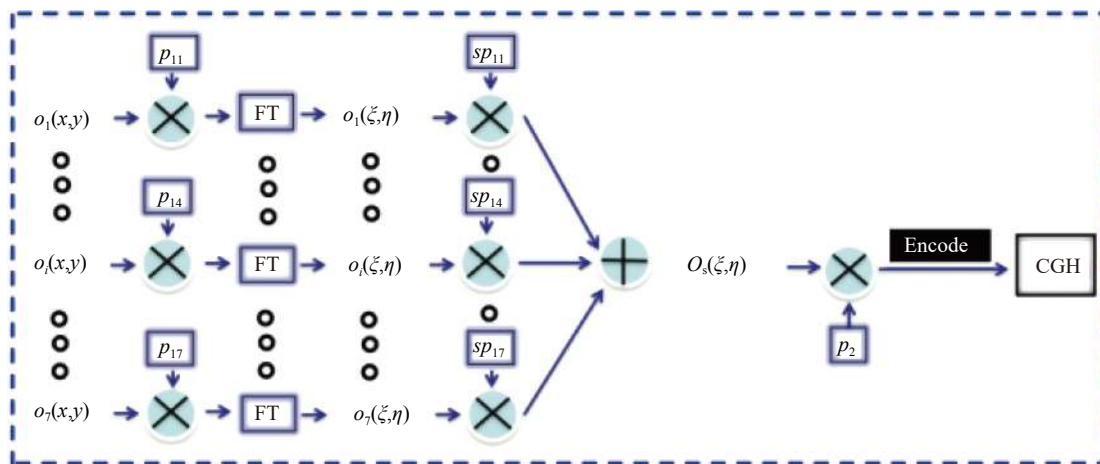


图 2 频移和 CGH 编码过程示意图

Fig.2 Schematic diagram of frequency shift and CGH coding process

假设待加密图像为 $o_i(x,y)$ , 其中 $i$ 的取值为 1~7, 首先待加密图像经过第一个随机相位 $p_{1i}(x,y)$ 调制,  $p_{1i}(x,y) = \exp[j2\pi \times \text{rand}(x,y)]$ , 其中 $\text{rand}(x,y)$ 表示 0~1 的随机分布。然后经过傅里叶变换之后的频谱分布为:

$$o_i(\xi,\eta)N_i(\xi,\eta) = FT[o_i(x,y)p_{1i}(x,y)] \quad (1)$$

式中:  $FT[\cdot]$ 表示傅里叶变换;  $o_i(\xi,\eta)$ 为频谱;  $N_i(\xi,\eta)$ 为相位。利用傅里叶变换的频移特性, 各个频谱被频移相位调制后叠加, 叠加后的频谱分布可表示为:

$$O_s(\xi,\eta) = \sum_{i=1}^{i=7} o_i(\xi,\eta)N_i(\xi,\eta)sp_{1i}(\xi,\eta) \quad (2)$$

式中:  $sp_{1i}(\xi,\eta)$ 表示每个图像的频移相位。可表示为:

$$sp_{1i}(\xi,\eta) = \exp[j2\pi \times (a_i \times \xi + b_i \times \eta)] \quad (3)$$

该多图像加密方法可以实现多个图像的并行加密和解密, 这里以加密七个不同类型和尺寸的图像为例验证该方法的可行性和有效性。根据待加密图像的尺寸和位置,  $(a_i, b_i)$ 的取值分别为 $(-0.375, -0.375)$ ,  $(-0.125, -0.375)$ ,  $(-0.375, 0)$ ,  $(-0.125, 0)$ ,  $(-0.25, 0.375)$ ,  $(0.25, -0.25)$ 和 $(0.25, 0.25)$ 。经过第二个随机相位调制后的光场为:

$$c(\xi,\eta) = O_s(\xi,\eta)p_2(\xi,\eta) = O_s(\xi,\eta)\exp[j2\pi \times \text{rand}(\xi,\eta)] \quad (4)$$

最后利用罗曼型迂回相位编码方法将公式(4)表示的光场编码为二元实值 CGH, 编码结果如图 3 所示<sup>[23]</sup>。

由图 3 可见, 七幅不同类型和尺寸的待加密图像

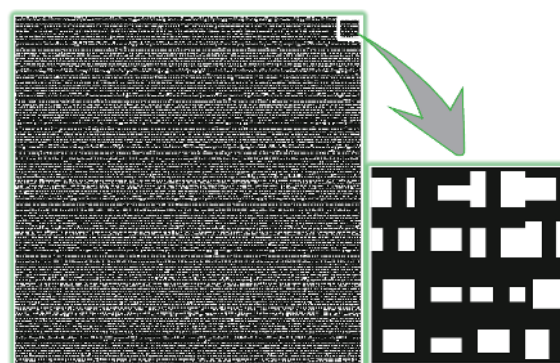


图 3 计算全息加密图像

Fig.3 CGH encrypted image

经过频移和计算全息编码成为单幅二元实值 CGH, 隐藏了所有原始图像的全部信息。此外, 罗曼型迂回相位编码的 CGH 具有很强的抗噪性能, 使其能够应对 JTC 加密系统的固有噪声问题。下一步是 CGH 在改进的 JTC 系统中进行加密, 加密系统如图 4 所示。

在加密系统中, 一个空间光调制器 (SLM) 经过一个透镜成像于第二个 SLM, 物像距与两个 SLM 的像素尺寸匹配。第二个 SLM 分为两部分, 分别加载随机相位 $p_3(\xi,\eta)$ 和 $p_4(\xi,\eta)$ , 第一个 SLM 加载的 CGH 成像于 $p_3(\xi,\eta)$ , 最后经过一次傅里叶变换, 联合功率谱被 CCD 接收为加密结果图像, 加密结果可表示为:

$$I(u,v) = |FT[c(\xi-b,\eta)p_3(\xi-b,\eta) + p_4(\xi+b,\eta)]|^2 = |c(u,v) * d_3(u,v)|^2 + |e_4(u,v)|^2 + c(u,v) * d_3(u,v)e_4^*(u,v)\exp(-j4\pi bu) + [c(u,v) * d_3(u,v)]^* e_4(u,v)\exp(j4\pi bu) \quad (5)$$

式中:  $b$ 为两个随机相位 $p_3(\xi,\eta)$ 和 $p_4(\xi,\eta)$ 到光轴 (SLM

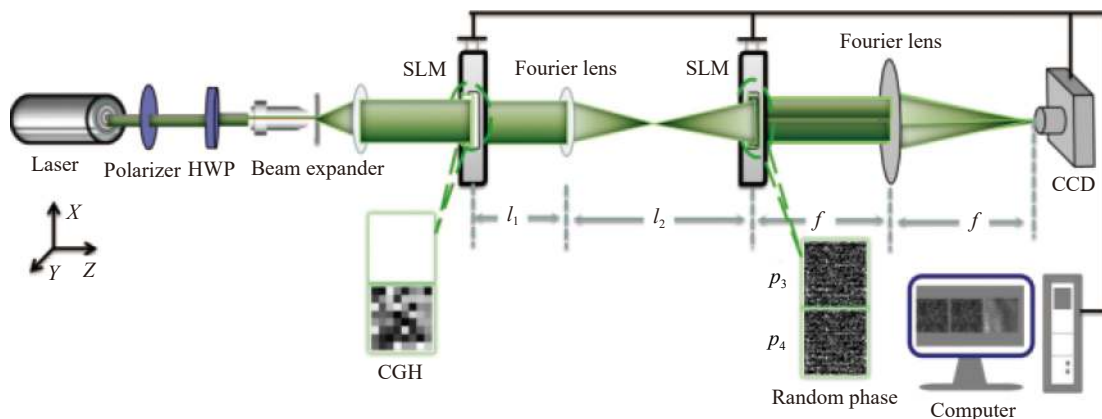


图 4 改进的 JTC 光学图像加密系统

Fig.4 Improved JTC optical image encryption system

中心) 的距离;  $(\cdot) * (\cdot)$  表示卷积运算;  $(\cdot)^*$  表示复共轭;  $c(u, v)$ 、 $d_3(u, v)$  和  $e_4(u, v)$  分别为  $c(\xi, \eta)$ 、 $p_3(\xi, \eta)$  和  $p_4(\xi, \eta)$  的傅里叶变换。

## 2 解密过程

第一步的 4F 解密系统如图 5 所示, 其中随机相位密钥  $p_4(\xi, \eta)$  仍然加载到置于输入平面的 SLM 中  $(-b, 0)$  处, 加密图像  $I(u, v)$  则加载到置于频谱面的 SLM 中  $(0, 0)$  处。第二个 SLM 出射的光场分布可表示为:

$$e_4(u, v) \exp(j2\pi ub) I(u, v) = (|c(u, v) * d_3(u, v)|^2 + |e_4(u, v)|^2) e_4(u, v) \exp[-j2\pi ub] + c(u, v) * d_3(u, v) \exp(-j2\pi bu) + [c(u, v) * d_3(u, v)]^* (e_4(u, v))^2 \exp(j6\pi bu) \quad (6)$$

其中, 第三项经过傅里叶变换被 CCD 接收, 即为 CGH 解密图像:

$$E_3(\xi, \eta) = |FT[c(u, v) * d_3(u, v) \exp(-j2\pi bu)]|^2 = |c(\xi + b, \eta) p_3(\xi + b, \eta)|^2 \quad (7)$$

但在实际 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, 即随机相位密钥功率谱  $|e_4(u, v)|^2 \neq 1$ , 公式 (6) 应修改为:

$$e_4(u, v) \exp[j2\pi ub] I(u, v) = (|c(u, v) * d_3(u, v)|^2 + |e_4(u, v)|^2) e_4(u, v) \exp[j2\pi ub] + c(u, v) * d_3(u, v) |e_4(u, v)|^2 \exp(-j2\pi bu) + [c(u, v) * d_3(u, v)]^* (e_4(u, v))^2 \exp(j6\pi bu) \quad (8)$$

所以公式 (8) 中第三项被 CCD 接收的解密图像可表示为:

$$E_3(\xi, \eta) = |FT[c(u, v) * d_3(u, v) |e_4(u, v)|^2 \exp(-j2\pi bu)]|^2 = |c(\xi + b, \eta) p_3(\xi + b, \eta) * p_4(\xi + b, \eta) \otimes p_4(\xi + b, \eta)|^2 \quad (9)$$

式中:  $(\cdot) \otimes (\cdot)$  表示相关。由公式 (9) 可见, 解密图像为 CGH 和随机相位密钥相关函数的卷积, 解密图

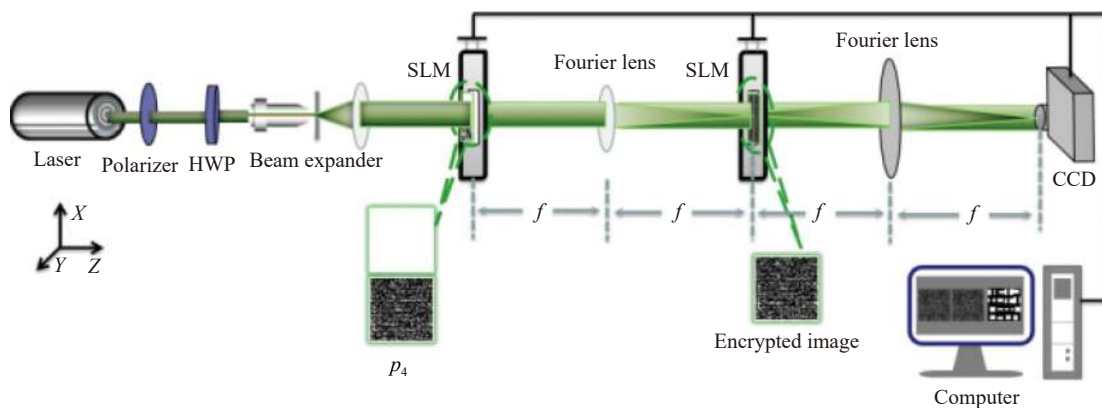


图 5 4F 系统解密光路图

Fig.5 Optical path of decryption based on 4F system

像中含有严重噪声,不能完全恢复出 CGH,解密结果图像如图 6(a)所示,这也是 JTC 加密系统的固有缺陷。在文中的加密方法中, JTC 加密系统的图像为二元实值 CGH,具有极强的抗噪性能,通过数字图像处理(按编码单元寻矩形开孔)去噪方法或手动去噪方法,以及深度学习去噪方法都可恢复 CGH,准确率皆超过 98%。去噪 CGH 如图 6(b)所示,可见 CGH 的引入能够克服 JTC 图像加密系统的固有噪声问题。

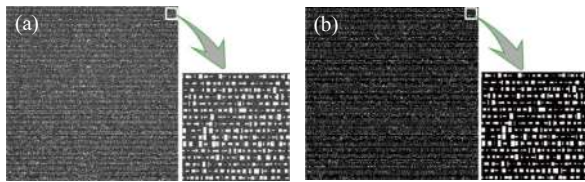


图 6 (a) 解密含噪 CGH 图; (b) 去噪 CGH 图

Fig.6 (a) Decrypted CGH with noise; (b) CGH after noise removal

解密过程第二步为 CGH 调制再现,解密光学系统如图 7 所示, SLM 分为两个区域,分别加载 CGH 和随机相位密钥  $p_2(\xi, \eta)$ , 两个区域通过一个 4F 成像系统连接,相当于密钥  $p_2(\xi, \eta)$  紧贴 CGH 放置。在该过程中,随机相位密钥  $p_2(\xi, \eta)$  需要编码为与 CGH 加密图像同尺寸的相位图,单个编码单元的尺寸也相同。因为同一个 SLM 的像素完全相同,编码单元与编码单元的对准方式降低了像素对准的难度<sup>[23]</sup>,然后  $p_2(\xi, \eta)$  调制的 CGH 经过一次傅里叶变换完成再现,

最后解密图像被 CCD 接收。

CGH 经过随机相位密钥  $p_2(\xi, \eta)$  调制后的频谱表示为:

$$-1 \text{ 级: } FT[O_s(\xi, \eta)p_2(\xi, \eta)p_2(\xi, \eta)] \quad (10)$$

$$+1 \text{ 级: } FT[O_s^*(\xi, \eta)p_2^*(\xi, \eta)p_2(\xi, \eta)] =$$

$$\sum_{i=1}^{i=7} o_i(x, y)p_{1i}^*(x, y) * FT[sp_{1i}^*(\xi, \eta)] = \sum_{i=1}^{i=7} o_i(x - a_i, y - b_i)p_{1i}^*(x - a_i, y - b_i) \quad (11)$$

+1 级频谱的强度:

$$\sum_{i=1}^{i=7} o_i(x - a_i, y - b_i) = \left| \sum_{i=1}^{i=7} o_i(x - a_i, y - b_i)p_{1i}^*(x - a_i, y - b_i) \right| \quad (12)$$

被 CCD 接收,可见七幅原始图像可被解密获得,解密结果如图 8 所示。

由图 8 可见,当密钥正确时,七幅不同类型的和尺寸的原图像能够被并行解密获得,且七幅图像之间不存在串扰问题。文中的罗曼型迂回相位编码单元为  $7 \times 7$  pixel,导致 CGH 再现的解密结果也是  $7 \times 7$  重复单元分布,每个单元包含七幅解密图像。每一幅解密图像的位置由频移相位中的  $(a_i, b_i)$  控制,如果  $(a_i, b_i)$  太大,解密结果图像会与其他单元重叠,因此该方法的加密容量和编码单元与 CGH 加密结果的尺寸

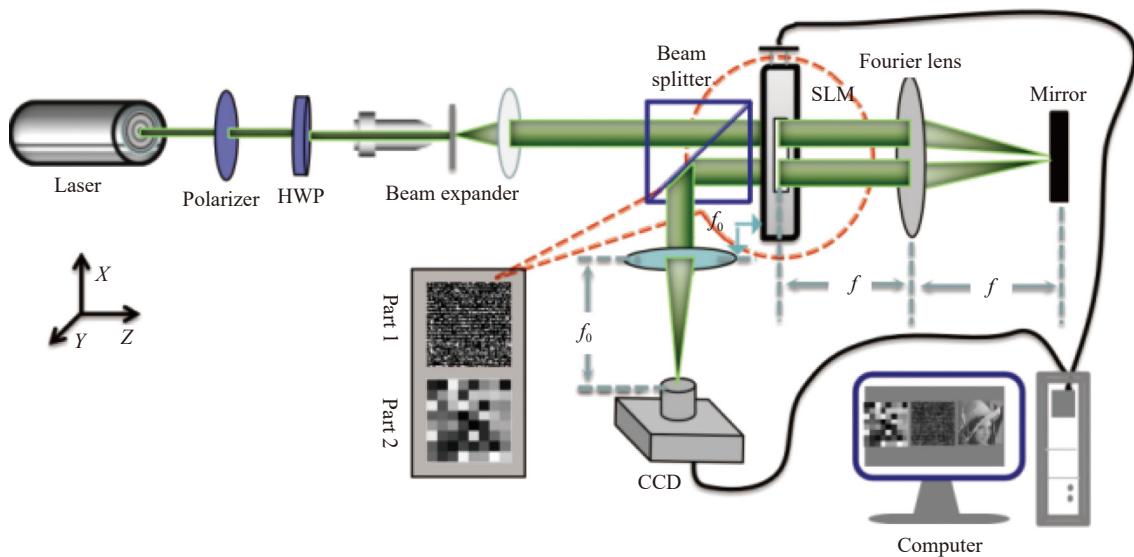


图 7 CGH 再现解密系统

Fig.7 Optical decryption and reconstruction system for the CGH

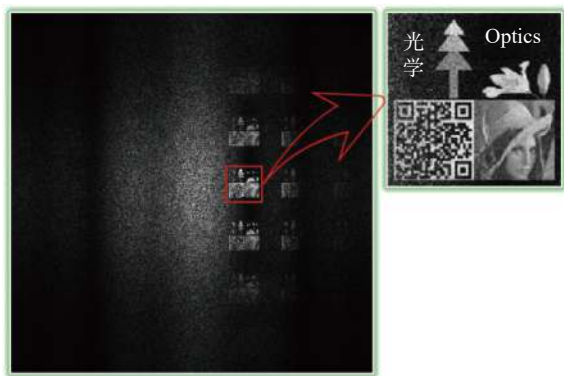


图 8 正确密钥解密结果图

Fig.8 Decrypted results with all correct keys

有关。由公式 (10) 和 (11) 所示, +1 级、+2 级和+3 级衍射图像为正确解密结果, 但解密图像受到 CGH 采样和量化编码误差影响, 存在一定噪声, 且 CGH 衍射级次越大, 噪声越大, 因此, +1 级解密图像质量最佳。该噪声可通过增加 CGH 编码单元的尺寸来降低。因此, 文中提出的多图像加密方法实现了多个不同类型和尺寸的图像的并行加密和解密。

### 3 安全性分析

为了验证文中提出多图像加密方法的安全性和有效性, 引入相关系数 (cc) 来评估原始图像和解密图像之间的相似性。相关系数的计算公式如下:

$$cc = \frac{\sum_x \sum_y (o(x,y) - \bar{o})(o'(x,y) - \bar{o}')}{\sqrt{\sum_x \sum_y (o(x,y) - \bar{o})^2 \sum_x \sum_y (o'(x,y) - \bar{o}')^2}} \quad (13)$$

式中:  $\bar{o}$  和  $\bar{o}'$  分别表示  $\bar{o}(x,y)$  和  $\bar{o}'(x,y)$  的平均值。当所有密钥正确时 (如图 8 所示), 原始图像和解密结果的 cc 值分别为 0.9484、0.9471、0.9398、0.9481、0.8682、0.9247 和 0.8519, 可见解密效果良好, 获得了高质量的解密图像。同时, 在解密过程中, 当随机相位密钥  $p_2(\xi, \eta)$  和  $p_4(u, v)$  错误时的解密结果如图 9(a) 和 (b) 所示。显然, 当随机相位密钥错误时, 七幅原始图像的任何信息无法获得, 在这种情况下, 七幅解密图像的 cc 值都小于 0.02。

由图 9 可见, 将 CGH 引入 JTC 加密系统后, 双重密钥极大地提高了多图像加密系统的安全性, 解决了 JTC 系统的安全性问题。

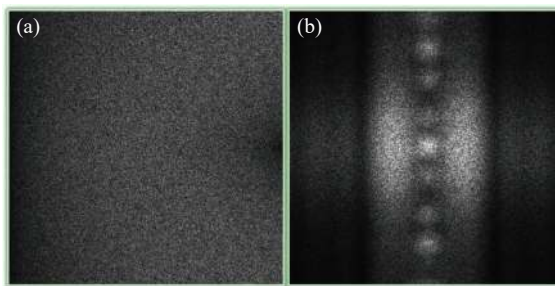


图 9 (a)  $p_4$  错误时的解密结果; (b)  $p_2$  错误时的解密结果

Fig.9 (a) Decryption result with wrong key  $p_4$ ; (b) Decryption result with wrong key  $p_2$

### 4 结论

文中提出了一种基于计算全息和频移的 JTC 系统多图像光学加密方法, 实现了多幅不同类型、不同尺寸图像的并行加密和解密, 解决了 JTC 图像加密系统的固有噪声和安全性问题, 同时提高了系统加密效率。因此, 文中提出的多图像光学加密方法在信息安全领域具有广阔的应用前景。

#### 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] Guo Yuan, Jing Shiwei, Xu Xin, et al. Asymmetric optical image encryption based on vector decomposition and phase-truncated [J]. *Infrared and Laser Engineering*, 2020, 49(4): 0426001. (in Chinese)
- [3] He Fengtao, Zhang Min, Bai Ke, et al. Image encryption method based on laser speckle and Henon mapping [J]. *Infrared and Laser Engineering*, 2016, 45(4): 0428003. (in Chinese)
- [4] Li Meixuan, Li Hong, Zhang Siqu, et al. Design of diffractive optical element based on discrete sampling encryption algorithm [J]. *Infrared and Laser Engineering*, 2019, 48(9): 0916004. (in Chinese)
- [5] Tang Shiwen, Annovazzi-lodi Valerio, Wang Zhao. Recent advances in optical cryptography [J]. *Chinese Journal of Optics*, 2014, 7(1): 89-97. (in Chinese)
- [6] Situ G, Zhang J. Double random-phase encoding in the Fresnel domain [J]. *Optics Letters*, 2004, 29(14): 1584-1586.
- [7] Tajahuerce E, Javidi B. Encrypting three-dimensional information with digital holography [J]. *Applied Optics*, 2000, 39(25): 6595-6601.
- [8] Javidi B, Nomura T. Securing information by use of digital

- holography [J]. *Optics Letters*, 2000, 25(1): 28-30.
- [9] Zhou N, Zhang A, Zheng F, et al. Novel image compression-encryption hybrid algorithm based on key controlled measurement matrix in compressive sensing [J]. *Optics & Laser Technology*, 2014, 62(10): 152-160.
- [10] Zhang L, Zhou Y, Huo D. Multiple-image encryption based on double random phase encoding and compressive sensing by using a measurement array preprocessed with orthogonal-basis matrices [J]. *Optics & Laser Technology*, 2018, 105: 162-170.
- [11] Jin Cong, Liu Hui. Image encryption system based on quantum chaos and folding algorithm [J]. *Optics and Precision Engineering*, 2017, 25(3): 749-755. (in Chinese)
- [12] Wang Di, Deng Jiaxian, Deng Xiaomei, et al. Joint algorithm of image compression and encryption using hyperchaotic system [J]. *Optics and Precision Engineering*, 2014, 22(9): 2528-2535. (in Chinese)
- [13] Wang Q, Xiong D, Alfalou A. Optical image encryption method based on incoherent imaging and polarized light encoding [J]. *Optics Communications*, 2018, 415: 56-63.
- [14] Rajput S K, Nishchal N K. Image encryption using polarized light encoding and amplitude and phase truncation in the Fresnel domain [J]. *Applied Optics*, 2013, 52(18): 4343-4352.
- [15] Nomura T, Javidi B. Optical encryption using a joint transform correlator architecture [J]. *Optical Engineering*, 2000, 39(8): 2031-2035.
- [16] Rueda E, Barrera J F, Henao R, et al. Optical encryption with a reference wave in a joint transform correlator architecture [J]. *Optics Communications*, 2009, 282(16): 3243-3249.
- [17] Rajput S K, Nishchal N K. Image encryption and authentication verification using fractional nonconventional joint transform correlator [J]. *Optics and Lasers in Engineering*, 2012, 50(10): 1474-1483.
- [18] Mehra I, Rajput S K, Nishchal N K. Cryptanalysis of an image encryption scheme based on joint transform correlator with amplitude and phase truncation approach [J]. *Optics and Lasers in Engineering*, 2014, 52: 167-173.
- [19] Cheng C J, Lin L C, Wang C M, et al. Optical joint transform encryption using binary phase difference key mask [J]. *Optical Review*, 2005, 12(5): 367-371.
- [20] Lin L C, Cheng C J. Optimal key mask design for optical encryption based on joint transform correlator architecture [J]. *Optics Communications*, 2006, 258: 144-154.
- [21] Matoba O, Javidi B. Encrypted optical storage with angular multiplexing [J]. *Applied Optics*, 1999, 38(35): 7288-7293.
- [22] Xi S X, Yu N N, Wang X L, et al. Optical encryption scheme for multiple-image based on spatially angular multiplexing and computer generated hologram [J]. *Optics and Lasers in Engineering*, 2020, 127: 105953.
- [23] Xi S X, Wang X L, Song L P, et al. Experimental study on optical image encryption with asymmetric double random phase and computer-generated hologram [J]. *Optics Express*, 2017, 25(7): 8212-8222.
- [24] Rueda E, Rios C, Henao R, et al. Experimental multiplexing approach via code key rotations under a joint transform correlator scheme [J]. *Optics Communications*, 2011, 284: 2500-2504.
- [25] Amaya D, Tebaldi T, Torroba R, et al. Wavelength multiplexing encryption using joint transform correlator architecture [J]. *Applied Optics*, 2009, 48(11): 2099-2104.
- [26] Qin Y, Lu X D, Gong Q, et al. Additional key rotation multiplexing encryption using joint transform correlator architecture [J]. *Acta Optica Sinica*, 2013, 33(3): 103-109. (in Chinese)
- [27] Wu Jun, Wang Gang, Xu Gang. Color image encryption method combining CGH and chaos [J]. *Journal of Optics*, 2021, 41(19): 113-132.
- [28] Kong Dezhao, Shen Xueju, Zhao Yan, et al. Encryption and display of three-dimensional information based computer generated hologram and random phase encoding [J]. *Laser & Optoelectronics Progress*, 2015, 52(10): 100902. (in Chinese)