激光与光电子学进展　先进成像

光学图像压缩加密技术研究进展

秦怡[1,2]，满天龙[1]，万玉红[1*]，王兴[2]

[1]北京工业大学理学部，北京 100124；

[2]南阳师范学院机电工程学院，河南 南阳 473061

摘要 光波作为信息载体具有高速并行处理二维信息的能力及天然优势。光波的波长、振幅、相位、偏振等为光波的调制提供不同的维度和多种可能，也使得光学加密技术和光学密码系统展现出巨大的应用价值。随着加密数据传输量的急剧增长，在进行加密的同时实现信息的压缩变得愈加重要，因为这将缩短处理这些数据所需的时间并有效节约存储空间。提出广义的光学图像压缩加密的概念，并将压缩策略分为明文压缩、密文压缩和明文密文同步压缩。在此基础上，介绍适合每种策略的具体压缩方法，并通过阐述这些压缩方法在一些实例中的应用，综述了光学图像压缩加密技术的研究进展，也对未来的研究方向进行了展望。

关键词 光学信息安全；压缩加密；图像压缩；光信息处理

中图分类号 O438　　**文献标志码** A　　**DOI**：10.3788/LOP221626

Advances in Optical Image Compression and Encryption Methods

Qin Yi[1,2], Man Tianlong[1], Wan Yuhong[1*], Wang Xing[2]

[1]*Faculty of Science, Beijing University of Technology, Beijing* 100124, *China*;

[2]*College of Mechanical and Electrical Engineering, Nanyang Normal University, Nanyang* 473061, *Henan, China*

Abstract Optical waves as information carriers can process two-dimensional information in parallel with high speed and have many degrees of freedom (e. g., wavelength, amplitude, phase, and polarization). Therefore, optical encryption technologies and optical cryptosystems demonstrate great potential for applications. With the rapid growth of encrypted data transmission volume, it becomes increasingly important to realize information compression while encrypting because it shortens the time required to process these data and substantially saves storage space. In this paper, we propose the concept of generalized optical image compression-encryption and categorize its compression strategies into three types, including plaintext, ciphertext, and synchronous compressions. On this basis, the specific compression methods suitable for each strategy are specified, and the research progress of optical image compression-encryption is introduced by describing the applications of these compression methods at some instances. Moreover, the potential future research directions of optical image compression-encryption are also presented.

Key words optical information security; compression and encryption; image compression; optical information processing

1 引　　言

随着全球经济信息化程度的不断提升，特别是互联网技术与各个行业的深度融合，信息技术和信息产业极大地改变了传统的生产和生活方式，成为社会经济增长的重要推动力之一。在这种背景下，旨在保护重要信息不被泄露、窃取、篡改的信息安全技术日益受到重视。基于光学原理的信息安全技术在近三十年来得到了广泛研究[1-10]。与传统的加密方法相比，光学密码技术具有独特的优势。首先，光波天然地具有并行处理二维信息的能力，特别适合于处理图像信息，且处理速度极快。需要处理的图像越复杂，信息量越大，这种优势就越突出。其次，与数字加密系统相比，光学方法可以在加密的过程中融合光波的各种自由度，例如波长、振幅、相位、偏振等，这些自由度构建出了极大的密钥空间，使得光学密码系统具有较高的安全性。

光学密码技术的代表性成果是 1995 年 Refregier 等[11]提出的双随机相位编码(DRPE)技术。他们在光

收稿日期：2022-05-17；**修回日期**：2022-06-17；**录用日期**：2022-07-14；**网络首发日期**：2022-07-24

基金项目：国家自然科学基金(61575009,61505091)、北京市自然科学基金(4182016)

通信作者：*yhongw@bjut.edu.cn

学 4*f*系统的输入面和频谱面分别放置两个统计独立的随机相位板，将位于输入平面的图像加密为复平稳白噪声。其光学实施方案如图 1 所示，其中图 1(a)表示图像加密过程，而图 1(b)表示密文的解密过程。之后，人们将双随机相位编码技术中的傅里叶变换改为菲涅耳变换，省去了透镜，从而简化了光路结构[12]；也将傅里叶变换更改为分数傅里叶变换，以提高安全性[13]。此外，研究者们也对双随机相位编码系统及其衍生系统的安全性进行了深入的研究[14-16]，并提出了一些改进安全性的方案[17-18]。双随机相位编码加密技术的提出和发展也促进了研究者们对光学加密技术的不断深入研究，提出了许多基于光学原理的新型密码系统[19-23]。光学联合变换相关器[19]、计算鬼成像[20]、干涉[21]、全息[22]、叠层成像[23]等许多光学技术被开发为新的光学密码系统。

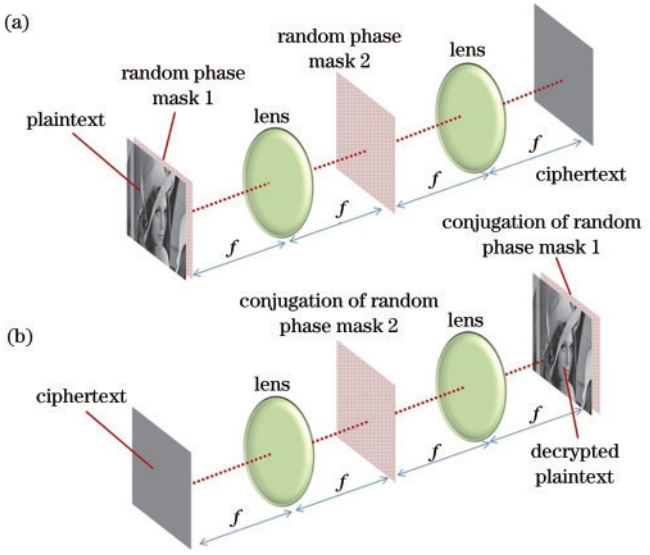

图 1　双随机相位编码光学加密和解密方法示意图。(a)加密过程；(b)解密过程

Fig. 1　Optical implementation of double random phase encoding. (a) Encryption; (b) decryption

近年来，各个行业信息化程度的快速提高带动了对信息安全的普遍需求，需要传输、储存、处理的加密信息量急剧增长，另外尺寸庞大的密文也不能适用于一些实时密码系统[4]。对图像的压缩加密或对密文的压缩是解决上述问题的有效途径，也是近年来光学密码技术领域研究的焦点之一[24-27]。已经有相当多的研究者对光学图像压缩加密技术进行了一系列的研究，并发展出了诸多有效的解决方案。例如：Situ 等[28]在双随机相位编码系统中提出波长复用技术，该技术在不增加密文尺寸的情况下实现了多图像加密；Durán 等[29]将压缩感知引入到计算鬼成像系统中，在实现加密的同时大幅压缩了密文尺寸；Naughton 等[30]先将量化压缩应用于光学密文，再采用无损压缩编码，实现了对密文的有效压缩。此外，作为光学信号处理中的一个重要的成果和工具，迭代相位恢复算法也在光学图像压缩加密中大放异彩，例如从经典的 Gerchberg-Saxton(G-S)算法[31]，到最近提出的混合模态相位恢复算法[32]，以及更具一般性的最优化方法[33]，改进后都被引入到光学密码系统中以实现压缩加密。近年来，随着人工智能技术的兴起，深度学习也在光学密文压缩中展现了良好的应用潜力[34]。本文将包括上述方法在内的、与光学原理和技术相结合的、能提升加密效率或实现密文尺寸压缩的图像加密技术，统称为光学图像压缩加密技术。在这个范畴内，对光学图像压缩加密技术进行综述。介绍光学图像压缩加密技术的分类和原理；介绍光学图像压缩加密技术的研究进展；讨论光学图像压缩加密技术未来的一些潜在的研究方向，并进行简单的总结。

2　光学图像压缩加密技术的基本原理

根据压缩对象的不同，光学图像压缩加密技术的压缩策略可分为明文压缩、密文压缩以及明文密文同步压缩。基于明文压缩的光学图像压缩加密系统的信息加密次序为“先压缩，后加密”。即在信息发送方，先对明文进行压缩，再实施加密；密文送达接收方后，需要先解密，再解压缩，才能正确地得到明文。基于密文压缩的光学图像压缩加密系统的信息加密次序为“先加密，后压缩”，即对密文实施压缩，密文达到接收方后，需要先解压缩，再解密，才能正确地解密密文。基于明文密文同步压缩的光学图像压缩加密系统中，加密和压缩在信息发送方同时进行，解密和解压缩在信息接收方也同步进行。对应三种不同压缩策略的加密系统的信息流程如图 2 所示。

此外，三种压缩加密策略中采用的具体压缩方法也不尽相同。对于明文压缩来说，被压缩的明文通常是自然图像，而自然图像在一些变换域(例如傅里叶变换域)内往往是稀疏的，因此适合变换域压缩。同时，自然图像在变换域内的稀疏性也使得其容易满足进行压缩感知采样所需要的条件，所以也可以采用压缩感知进行压缩。对于密文压缩来说，压缩的密文往往具有噪声图像的外貌，像素之间的相关性较弱，除了个别特例之外[35]，一般只能采用有损压缩法压缩，目前对其压缩的常见方法包括参数复用压缩、经典数据压缩及压缩感知等。对于明文密文同步压缩来说，在加密的同时实现密文的压缩，这往往需要借助迭代相位恢复算法和压缩感知。这三种压缩策略所对应的具体压缩方法如表 1 所示。

2.1　光学图像压缩原理

2.1.1　变换域压缩

变换域压缩是适合于明文压缩的压缩方法，这是因为几乎所有的自然图像在经过一些积分变换后，在变换域内呈现能量集中状态。例如，一幅自然图像在经过离散傅里叶变换(DFT)后，包含图像大部分能量

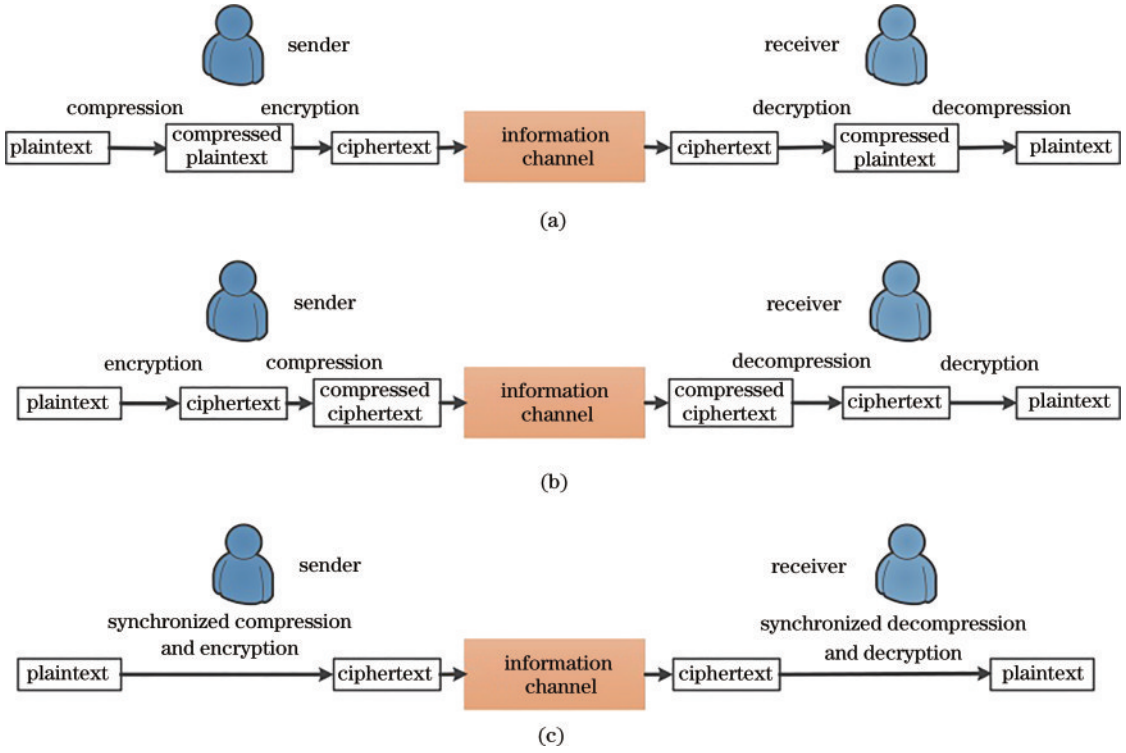

图 2　采用不同压缩策略的光学图像压缩加密系统的信息流程示意图。(a)明文压缩;(b)密文压缩;(c)同步压缩

Fig. 2　Information processing flowchart for different compression strategies in optical compression-encryption system. (a) Plaintext compression; (b) ciphertext compression; (c) synchronized compression

表 1　光学图像压缩加密技术的压缩策略和具体压缩方法

Table 1　Compression strategies and methods for optical image compression-encryption

Compression strategy	Compression method
Plaintext compression	Transform domain compression
	Compressive sensing
Ciphertext compression	Parameter multiplexing compression
	Classical compression
	Compressive sensing
Synchronized compression	Iterative phase retrieval algorithm
	Compressive sensing

的低频成分分布在频谱中心附近,而能量较小的高频成分则位于四周。如果舍去那些高于一定阈值的高频分量,仅利用余下的低频成分对图像进行重构,那么重构图像质量与原始图像非常接近(仅仅损失一些细节),在很多应用中完全可以接受。除了傅里叶变换之外,离散余弦变换(DCT)[36]、离散小波变换(DWT)等,都具有类似特性,这种能量集中性构成了图像变换域压缩的基础。变换域压缩在多图像压缩加密中应用尤其广泛,一种利用傅里叶域稀疏性进行信息压缩的例子如图 3 所示。假设有 4 幅待加密的明文图像,对它们分别进行 DFT,得到对应的频谱,对这些频谱进行低通滤波(滤波窗口为正方形,其边长为原频谱边长的 1/2),并将滤波后的频谱移位后再进行拼接,确保这 4 个频谱在空间上互不混叠,就得到了含有 4 幅图像频谱信息的复合频谱,其尺寸与单个图像的频谱的尺寸相同,实现了信息的有效压缩。加密时直接加密这个复合频谱,得到最终的密文。解密时,先解密得到复合频谱,再从复合频谱中分离 4 幅图像各自的频谱并进行傅里叶逆变换,得到原始明文。

2.1.2　参数复用压缩

参数复用压缩是适用于密文压缩的压缩方法,其前提是光学密码系统对拟复用参数(密钥)的敏感性,也就是说,当该复用参数发生微小的变化时,从对应密文得到的解密结果是与原始明文完全不相关的噪声图样。

假设某光学密码系统的加密算法表示为 $E[\cdot]$,待加密的明文图像序列为 $P_i, i=1,2,\cdots,N$。为每一个 P_i 指定一个不同的拟复用参数 K_i,同时假定拟复用参数外的其他密钥可以总体表示为 K_o,那么对应于 P_i 的密文 C_i 可以表示为

$$C_i = E[P_i; K_i; K_o]。\tag{1}$$

为了实现参数复用,将得到的 N 幅密文直接叠加,得到一个复合密文 $C=\sum C_i$。这样,所有原始明文的信息全部都融合到了 C 中,实现了信息的压缩。为了恢复某一个明文 $P_k, k=1,2,\cdots,N$,利用与其对应的加密复用参数 K_k 和其他密钥进行解密,可以得到

$$\tilde{P}_k = E^{\mathrm{inv}}[C; K_k; K_o] = E^{\mathrm{inv}}[C_k; K_k; K_o] + \sum_{i\neq k} E^{\mathrm{inv}}[C_i; K_k; K_o] = P_k + n_k,\tag{2}$$

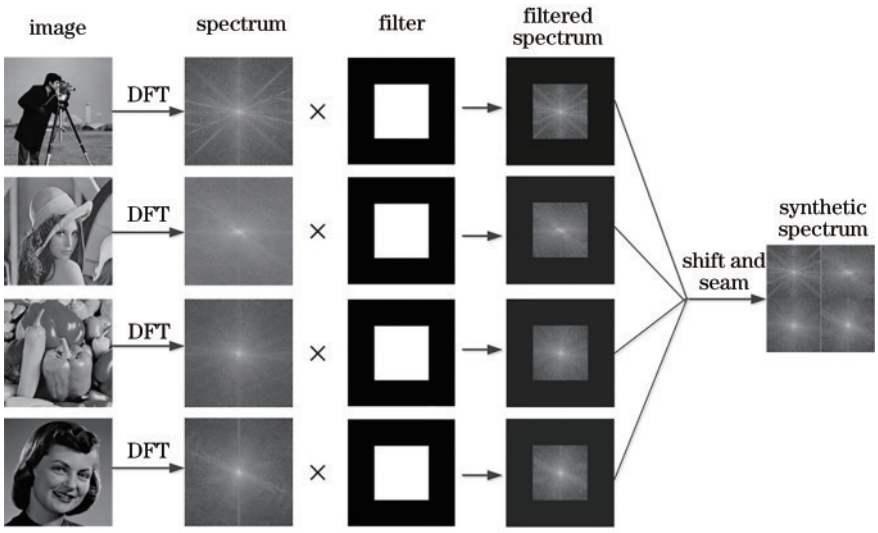

图 3　利用变换域能量集中性进行信息压缩的例子

Fig. 3　An example of information compression by using the concentration of energy in the transform domain

式中：$E^{\mathrm{inv}}[\cdot]$表示解密算法；$n_k=\sum_{i\neq k}E^{\mathrm{inv}}[C_i;\ K_k;\ K_0]$，代表复合密文中所有不与$K_k$相对应的密文采用$K_k$解密的结果之和。前面已经提到，复用技术的前提是解密结果对复用参数非常敏感，因此n_k为$N-1$个噪声图样的叠加结果，也必然是一个噪声图样。因此式(2)表明：在基于复用技术的加密系统中，解密结果是原始图像P_k与一个噪声干扰n_k的叠加。在n_k的干扰不太强的时候，原始图像可以被准确地恢复出来。

2.1.3　经典压缩

经典的数据压缩方法分为无损压缩和有损压缩两种[37]。无损压缩可以由压缩后的数据完全恢复出原始数据。著名的行程编码(RLE)和霍夫曼编码(HE)等属于无损压缩。但是，无损压缩所能达到的压缩比往往不高，一般情况下介于2∶1到5∶1之间。相比之下，有损压缩则无法由压缩后的数据完全恢复出压缩前的数据，但是往往能充分去除数据本身的冗余信息。冗余信息包括编码时未充分考虑统计信息产生的编码冗余、相邻像素之间的相关性造成的空间冗余、人类视觉系统对不同信息敏感性不同而造成的视觉冗余等，能够达到较高的压缩比。常见的有损压缩方法包括量化压缩、JPEG压缩编码、小波变换编码等。

需要指出的是，对于密文这种特殊的图像数据来说，要想对其进行有效的压缩，必须采用有损压缩法，这是因为密文本身具有噪声图像的特征，像素之间的关联性不强，无损压缩难以达到理想的压缩比。一般来说，采用有损压缩来压缩密文，必然导致密文信息的损失，相应地会导致解密结果质量的下降，这就需要以牺牲解密图像质量为代价来换取密文尺寸的压缩。

2.1.4　迭代相位恢复算法

迭代相位恢复算法是实现同步压缩的主要技术手段之一。相位恢复问题是光学成像领域的一个基本问题，它要解决的是如何由测得的强度信号来重新恢复复振幅(振幅和相位)。相位恢复方法目前已经形成几个重要的分支，包括迭代相位恢复算法(IPRA)、强度传输方程(TIE)、半定规划算法(SPA)等[38]。目前，在光学图像压缩加密领域内应用最广泛的是迭代相位恢复算法。最早的迭代相位恢复算法是由Gerchberg[31]提出的G-S算法，该算法利用信号傅里叶变换的振幅和信号自身的振幅恢复了信号的相位。G-S算法的基本原理如图4所示，其中g和G是已知量，分别表示空间域的信号的振幅及其傅里叶变换域的振幅，而信号的相位θ是未知量(待求量)。首先给θ赋予一个随机的初始值θ_0，并对信号进行傅里叶变换至频域，得到复振幅G'；此时，保留G'的相位，而用G取代其振幅$|G'|$，得到新的复振幅G''；对G''进行傅里叶逆变换，得到输入面复振幅g'，保留其相位并用g取代其振幅$|g'|$，得到更新后的输入面复振幅g''(即信号的新的估计值)。至此，一轮迭代结束，之后，重复上述迭代直至算法收敛。利用G-S算法，很容易将一幅图像隐藏于一个纯相位板中，例如在图4所示的框架中，如果令G为待隐藏的

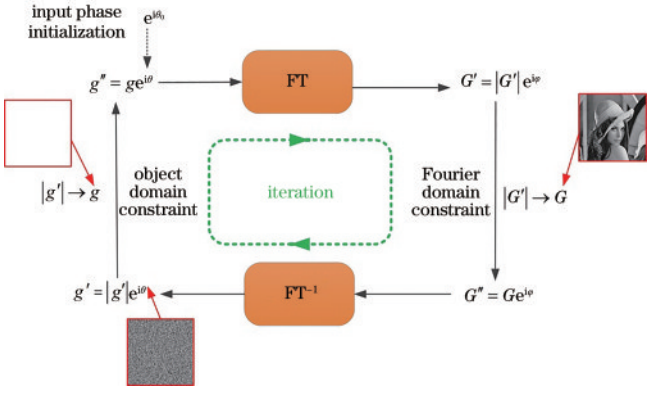

图 4　G-S算法的原理

Fig. 4　Principle of G-S algorithm

图像(以“Lena”为例),同时令 g 为一个所有元素取值都为 1 的矩阵,那么最后确定的相位板 $e^{i\theta}$ 就包含了原始图像的信息。无论是采用数字方法还是光学方法对该相位板进行傅里叶变换,都可以方便地复现原始图像。更一般地,根据杨国桢等[39]确定的振幅、相位恢复算法,也很容易在输入或输出面上对相位和振幅进行操纵,以实现加密的目的。这种迭代算法可以很容易地推广到存在多个级联相位板的光学密码系统中,这也是迭代相位恢复算法用于光学图像压缩加密的理论基础。

2.1.5　压缩感知

相比于上述几种压缩方法,压缩感知在光学图像压缩加密系统中具有一定的通用性,它既可以压缩明文,也可以压缩密文,还可以用来实现同步压缩。压缩感知又称为压缩采样,是信号处理领域进入 21 世纪以来最重要的成果之一。该理论指出:对于稀疏信号或可压缩信号,以远低于奈奎斯特采样定理要求的采样间隔对其进行采样,仍可以利用所采样的离散值对原始信号进行精确重建[40]。

假设感兴趣的信号为 $\boldsymbol{f}$,它是一个 K 维向量,采用一个维度为 $J\times K(J\ll K)$ 的观测矩阵 $\boldsymbol{\Phi}$ 对其进行观测,得到观测向量 $\boldsymbol{y}$:

$$\boldsymbol{y}=\boldsymbol{\Phi f}。\tag{3}$$

一般来说,由 $\boldsymbol{y}$ 来恢复 $\boldsymbol{f}$ 是一个不适定问题。压缩感知理论指出:如果原始信号具有稀疏性或在某个变换域是稀疏的,并且稀疏矩阵和观测矩阵非相干,则可以由 $\boldsymbol{y}$ 来精确地恢复 $\boldsymbol{f}$[40]。稀疏性要求 $\boldsymbol{f}$ 可以用一个 k 稀疏的向量 $\boldsymbol{\alpha}$ 表示,即

$$\boldsymbol{f}=\boldsymbol{\Psi\alpha}。\tag{4}$$

k 稀疏指在全部的 K 个分量中,至多有 k 个分量不等于 0。此外,$\boldsymbol{\Psi}$ 的大小为 $K\times K$,被称为稀疏矩阵。非相干性则指观测矩阵 $\boldsymbol{\Phi}$ 要与稀疏矩阵 $\boldsymbol{\Psi}$ 尽可能不相关。若稀疏性和非相干性两个条件得到满足,则可以通过求解凸优化问题来精确重建 $\boldsymbol{f}$[40],凸优化问题为

$$\min\|\boldsymbol{\alpha}\|_1\ \ \text{subject to}\ \boldsymbol{y}=\boldsymbol{\Phi\Psi\alpha},\tag{5}$$

式中:$\|\boldsymbol{\alpha}\|_1$ 表示 ℓ_1 范数,代表 $\boldsymbol{\alpha}$ 中非零元素的个数。在应用中,一种更为常见的重建 $\boldsymbol{f}$ 的算法是最小化其全变分(TV):

$$\min \mathrm{TV}(\boldsymbol{f})\ \ \text{subject to}\ \boldsymbol{y}=\boldsymbol{\Phi f},$$
$$\text{with}\ \mathrm{TV}(\boldsymbol{f})=\sum_{i,j}\sqrt{\left(f_{i+1,j}-f_{i,j}\right)^2+\left(f_{i,j+1}-f_{i,j}\right)^2}。\tag{6}$$

实际上,全变分可以视为梯度的 ℓ_1 范数。事实上,尽管式(5)和式(6)具有相同的思想内涵,但是后者在解决各种实际问题中应用更广泛。

压缩感知在光学成像领域最著名的一个应用实例是 Rice 大学提出的单像素相机[41],如图 5 所示。

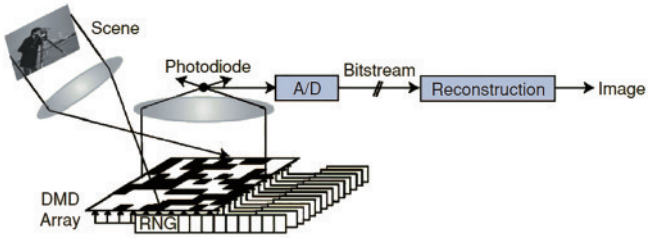

图 5　基于压缩感知的单像素相机[41]

Fig. 5　Single pixel camera based on compressive sensing[41]

进行采样时,待采样的图像经透镜成像在 digital micromirror device(DMD)所在平面,被 DMD 调制,再被第二个透镜会聚后其总强度被光电二极管(PD)所记录。其中,每次采样时 DMD 所生成的都是各不相同的随机图像。这样,将原始图像整形为列向量,即为式(3)中的 $\boldsymbol{f}$;将每次采样时 DMD 所显示的随机图像调整为行向量,对应于式(3)中的 $\boldsymbol{\Phi}$ 的一行;而每次由光电二极管记录的光强总强度,对应于式(3)中的 $\boldsymbol{y}$ 的一个元素。这样,单像素相机的成像过程就与压缩感知的采样模型完全对应起来了。在实际求解中,可以利用离散傅里叶变换等作为稀疏矩阵 $\boldsymbol{\Psi}$,在 $\boldsymbol{y}=\boldsymbol{\Phi\Psi\alpha}$ 约束下最小化 $\|\boldsymbol{\alpha}\|_1$,经优化算法求得稀疏的向量 $\boldsymbol{\alpha}$,然后对其进行傅里叶变换,即可恢复原始图像。

2.2　评价光学图像压缩加密技术的指标

评价光学图像压缩加密技术的指标大体上分为两类。第一类是评价所有光学密码系统的通用指标,例如密钥空间、加密/解密速度、对各种密码学分析的稳健性、解密图像质量等。第二类是专门用于评价光学图像压缩加密技术中压缩效率的指标,例如加密容量、密文压缩比等。在光学图像压缩加密技术中,尤其关注压缩效率及与其密切相关的解密图像质量,因此介绍评价压缩效率与解密图像质量的相关指标。

2.2.1　评价压缩效率的相关指标

许多基于参数复用的光学图像压缩加密技术都采用加密容量作为评价压缩效率的指标[28]。加密容量指在解密后的明文质量高于一定客观指标前提下,其单幅密文尺寸所能容纳的最大明文数量。这里单幅密文尺寸指没有采用参数复用时(仅加密单幅图像)的密文尺寸。在一些对密文实施压缩的场景下,使用压缩比能够更方便地描述系统的压缩效率。图像的压缩比[30]定义为

$$R=\frac{S_\mathrm{b}}{S_\mathrm{a}},\tag{7}$$

式中:S_b 为压缩前的图像尺寸;S_a 为压缩后的图像尺寸。

2.2.2　评价解密图像质量的相关指标

评价解密图像质量的指标有很多种,常见的包括均方误差(MSE)、峰值信噪比(PSNR)、结构相似性(SSIM)、相关系数(CC)等。其中,MSE 和 PSNR 计

算所依据的都是两个图像对应像素点之间的误差，其结果体现出各个像素点之间误差的平均偏离程度，这两个指标的局限性在于没有考虑人眼的视觉特性，时常会出现结果与人眼主观感受不一致的情况。相比之下，SSIM 指标充分考虑了两幅图像之间的亮度、对比度、结构三个要素，其评价结果与人眼主观评价一致性更好。此外，CC 从统计学的观点来分析两幅图像的相关程度，也能准确反映二者的相似程度。

3　光学图像压缩加密技术研究进展

已将光学图像压缩加密技术按照压缩策略分为三类，即明文压缩、密文压缩、明文密文同步压缩。将以这分类为依据，分别阐述明文压缩、密文压缩、明文密文同步压缩在光学图像压缩加密技术的应用及研究进展。同时，对于每一种压缩策略，又按照实现该策略的不同压缩方法分别论述。

3.1　基于明文压缩的光学图像压缩加密

3.1.1　基于变换域压缩的光学图像压缩加密

利用变换域压缩实现光学图像压缩加密的一个典型例子是由 Liu 等[42]提出的一种基于频谱剪切的光学多图像加密方法。他们通过舍弃图像傅里叶频谱的一部分高频信息，实现了频谱压缩。多个原始图像的压缩频谱经拼接后形成一个复合频谱，之后再将复合频谱送到双随机相位编码系统进行加密。与之类似的思路还有 Deng 等[43]提出的基于频谱剪切和空间复用的加密方法，尽管方法简单易行，但是这种直接的频谱剪切与拼接没有充分利用频谱之间信息共享的可能性。相比之下，Alfalou 等[44]提出的基于频谱融合的压缩加密方法更加高效，其加密过程如图 6 所示（以加密两幅图像为例）。首先对两幅明文图像进行离散傅里叶变换并获得对应的频谱，然后将这两个频谱平移，使彼此的中心位置在频域尽可能得分开。显然，即使如此，这些频谱如果直接叠加的话，仍然会出现重叠导致信息串扰和丢失的问题。因此 Alfalou 等根据参与叠加的两个频谱中对应元素的模的相对权重来确定叠加结果：如果二者的模的相对权重接近，则叠加后的频谱取

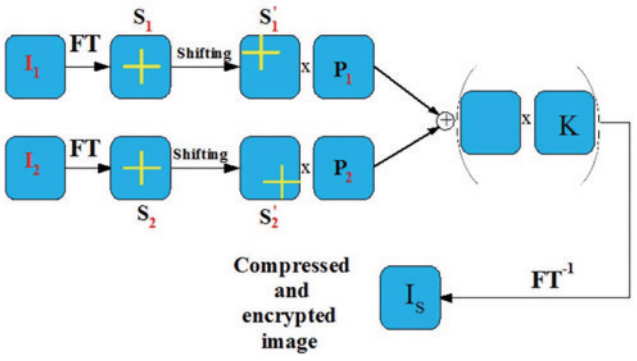

图 6　基于频谱融合的双图像加密方法[44]

Fig. 6　Double-image encryption based on frequency spectral fusion[44]

二者的均值；如果相对权重相差较大，则保留相对权重大的那一个元素。这样，融合后的频谱尺寸与原来每个图像的频谱尺寸相同，但是却充分地融合了两个图像的频谱信息，实现了信息压缩。之后，再将融合后的频谱送至随机相位编码系统进行加密。该方法对相似性较高的图像序列（例如视频序列）能够实现高质量重建，如图 7 所示。

在此基础上，Alfalou 等[45-46]又将离散傅里叶变换替换为离散余弦变换，提出了若干改进的光学图像压缩加密系统。最近，他们[47]又采用混沌方法生成这些系统中所用的密钥（随机相位板），因此不需要在通信系统传输密钥，而只需要传输生成密钥所需参数，提升了系统的实时性。受到这些工作的启发，本课题组[48]提出了在光学衍射成像加密系统中利用频谱融合和空间复用进行多图像加密的方法。需要指出的是，在这些基于变换域频谱融合的方法中，频谱的移位和剪切都需要采用数字方法进行后处理实现。而对于 Chirp-Z 变换来说，其频谱的中心位置和分布范围都可以通过调节变换参数来确定，尤其是 Chirp-Z 变换可以使用一种纯光学的方式来实现[49]。基于此，Mosso 等[50]提出了一种多图像加密方法，通过对比，在加密相同数量的灰度图像的情况下，其解密图像质量要优于 theta 调制法。之后，Mosso 等[51]又将 Chirp-Z 变换与双随机相位编码结合起来，提出了一种非对称多图像加密方法。

最近，Wu 等[52]利用 Radon 变换（RT）对自然图像频谱的压缩能力，提出一种多图像加密方法，其压缩和加密方案如图 8 所示。对于每一幅明文，首先对其进行极坐标变换；之后，以一定的角度间隔（1°）对极坐标图像扫描并进行 Radon 变换，得到 Radon 变换谱，注意到频谱上下两端黑色部分的数值均为零，因此对其进行切除以压缩频谱；最后将所有的压缩频谱直接拼接，得到复合频谱，之后将该复合频谱送入光学非对称加密系统[53]进行加密。需要指出，该方法中每个图像的 Radon 谱的尺寸取决于对其扫描的角度间隔，也即扫描次数。扫描间隔越小，则重建图像越准确。此外，这种 Radon 变换与空间复用的明文压缩结合的方法也被引入到鬼成像加密系统中实现多图像加密[54]。

3.1.2　基于明文压缩采样的光学图像压缩加密

利用压缩感知对明文进行压缩采样也是压缩明文所采用的另外一个主要技术手段。2013 年，Lu 等[55]将压缩感知与双随机相位编码相结合，在实现压缩的同时也提高了系统的安全性。他们将一幅 256 × 256 像素的灰度图像 Lena 通过传感矩阵采样为 192 × 192 像素的中间图像，再采用双随机相位编码对此中间图像进行加密，得到了大小也为 192 × 192 像素的密文。这样，就将原本应为 256 × 256 像素的密文压缩至 192 × 192 像素。最后将密文隐藏在一个宿主图像中。解密时先从宿主图像中提取密文。由于双随机相位编

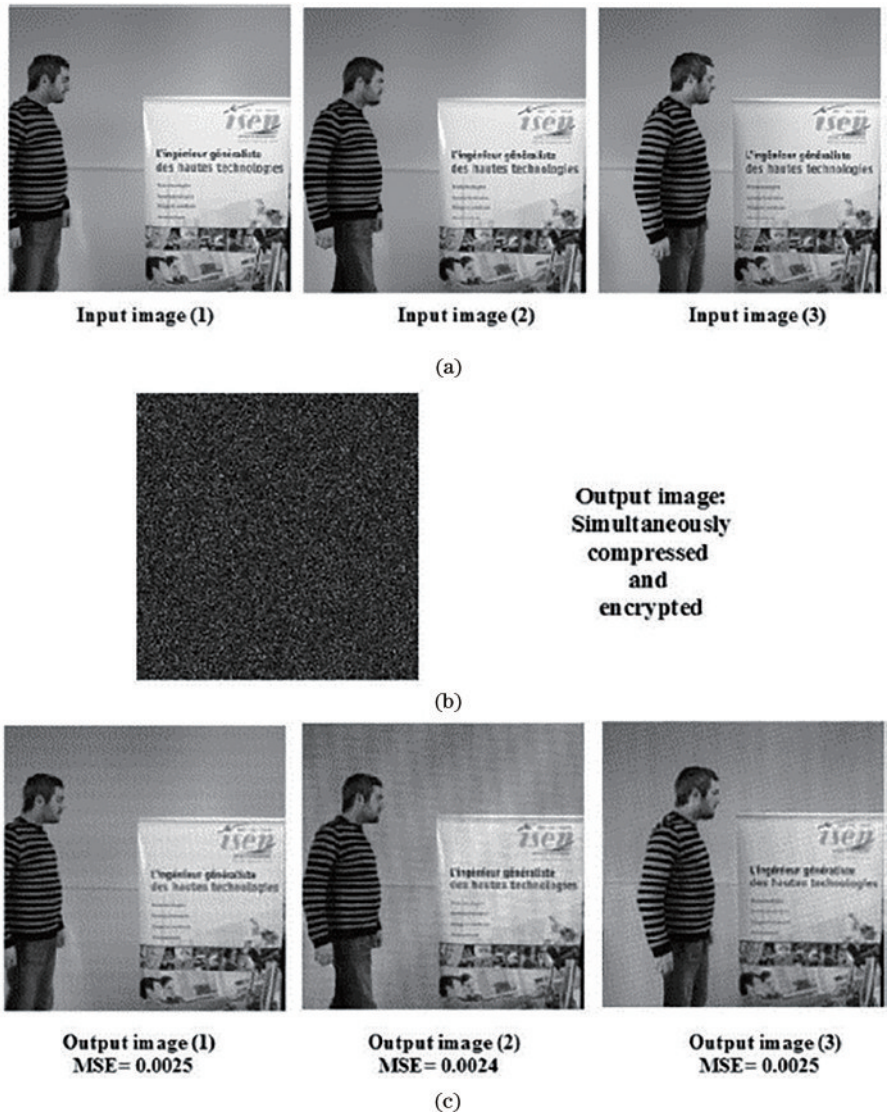

图 7　基于频谱融合的多图像加密方法的数值模拟结果[44]。(a)原始图像;(b)密文;(c)解密图像

Fig. 7　Simulation results of multiple-image encryption based on frequency spectral fusion[44]. (a) Original images; (b) ciphertext; (c) decrypted images

码是一种无损加密方法,所以利用提取到的密文可以先精确地恢复中间图像,再借助正交匹配追踪(OMP)算法和传感矩阵恢复原始图像。其详细的加密和解密流程如图 9 所示,而对应的实验结果如图 10 所示。结果表明,该方法可以实现对原始图像的高质量重建,解密结果[如图 10(f)所示]的峰值信噪比达 30.8874 dB。之后,Liu 等[56]在 Lu 等的方法中引入 Arnold 变换,进一步提升了系统的安全性。同样是为了提高系统安全性,Wang 等[57]将双随机相位编码中的平面波衍射改变为柱型波衍射,该系统所对应的压缩感知模型中的等效测量矩阵不再满足约束等距性质(RIP),潜在的攻击者无法通过单步的 ℓ_1 范数优化对系统进行破解。

Deepan 等[58]将空间复用技术与压缩感知相结合,在双随机相位编码系统中实现多图像加密。待加密的 4 幅图像的尺寸均为 256 × 256 像素,通过压缩采样,将其降为 128 × 128 像素。之后,这 4 幅 128 × 128 像素的图像直接通过空间复用(即拼接)成为 256 × 256 的矩阵,再将此矩阵送入双随机相位编码系统进行加密,整个加密过程如图 11 所示。解密过程如图 12 所示。需要指出的是,在对每一幅图像进行压缩采样时,所采用的观测矩阵为自适应矩阵。由于其采用的稀疏变换为傅里叶变换,Deepan 等提出的对观测矩阵的设计满足以下条件:对每个原始图像,都能够保留其全部 N 个傅里叶频谱值中模较大的 M 个。这样的设计不仅保证每个图像的观测矩阵各不相同,提升了系统的安全性,而且能够保持较高的图像重建质量,因为这 M 个值包含了原始图像的绝大部分信息。

此外,人们也将压缩感知技术与其他一些可以用光学系统实现的数学变换相结合,实现了图像的压缩加密。例如:Zhou 等[59]将压缩感知与分数 Mellin 变换(FMT)结合;Yi 等[60]将压缩感知与分数傅里叶变换(FrFT)结合,实现了图像的压缩加密;Yang 等[61]将压

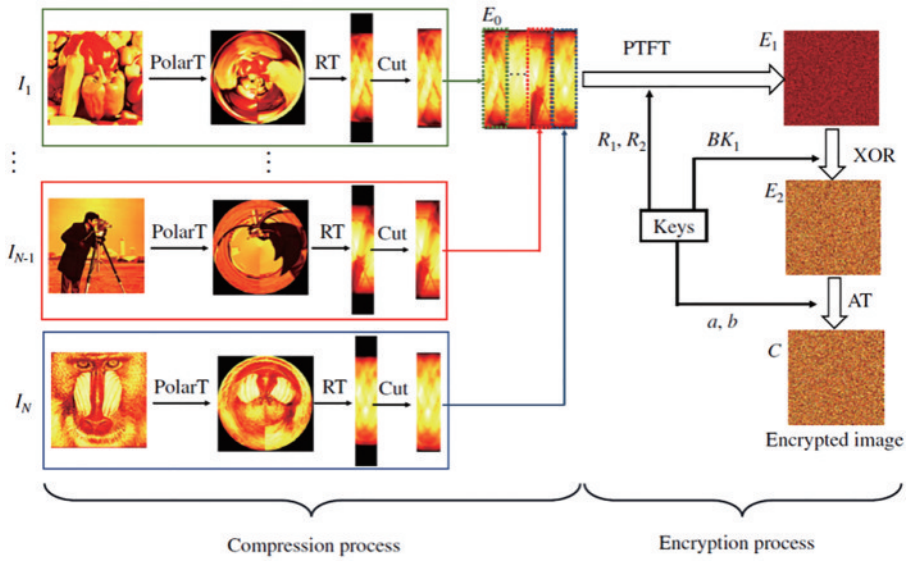

图 8　基于 Radon 变换的多图像压缩加密方法[52]

Fig. 8　Multiple-image compression and encryption based on Radon transform[52]

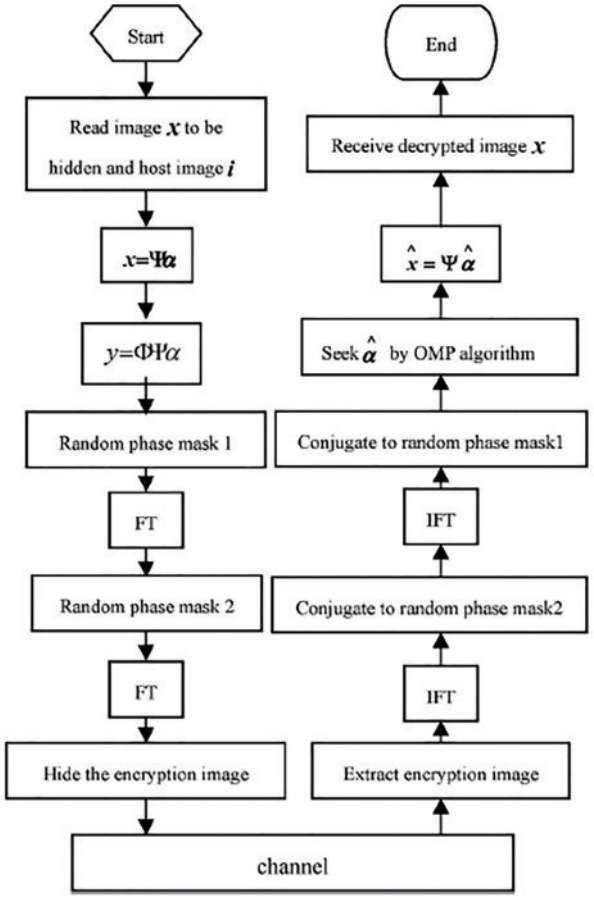

图 9　基于压缩感知和双随机相位编码系统的图像加密与解密流程[55]

Fig. 9　Image encryption and decryption process based on compression sensing and dual random phase coding system[55]

缩感知与编码孔径成像(CAI)系统结合，提出了一种新颖的图像压缩加密方法。

值得注意的是，在上述文献中，压缩感知的重建过程都是基于优化算法的，例如正交匹配追踪法、梯度投影(GP)法等。而近年来深度学习技术的兴起给类似压缩采样这种不适定问题提供了新的解决方案。Ni 等[62]提出了一种基于压缩感知和深度学习的多图像加密系统。他们采用压缩采样对明文进行压缩，采用深度神经网络对密文进行解压缩，相比于正交匹配追踪法，重建质量有较大提升。

3.2　基于密文压缩的光学图像压缩加密

3.2.1　基于参数复用压缩的光学图像压缩加密

Situ 等[28]提出的基于波长复用的多图像加密技术是采用参数复用压缩的代表性成果之一。在菲涅耳域双随机相位编码系统中，他们利用解密结果对波长这一参数的敏感性实现了多图像加密与解密，并分析了实现有效复用所需要的最小波长间隔和系统的加密容量。在另外一个工作中，Situ 等[63]也利用距离复用实现了多图像加密，其加密和解密原理如图 13 所示。在菲涅耳域双随机相位编码系统中，对不同的明文 f_n 采用不同的衍射距离 d_n 进行加密，得到了对应的一系列衍射结果 g_n，这些衍射结果直接相加得到密文 g。解密时，沿光轴方向移动 g 至不同的位置，即可在输出平面得到相应的解密结果。图 14 给出了同时加密 5 幅图像(同为汉字“学”)的数值实验结果。

基于各种参数的复用的技术被广泛挖掘和研究。Amaya 等将波长复用引入到光学联合变换相关加密系统中，分别研究了彩色图像加密[64]和多图像加密[65]。本课题组[66]将距离复用用于光学干涉加密这一密码系统中，在实现多图像加密的同时，消除了困扰该系统“轮廓像”的问题。Xiao 等[67]发现如果将双随机相位编码系统中的密钥改为圆形，那么解密结果对密钥旋转的角度特别敏感，他们在此基础上提出了利用密钥旋转复用的多图像加密技术。Rueda 等[68]基于光学联

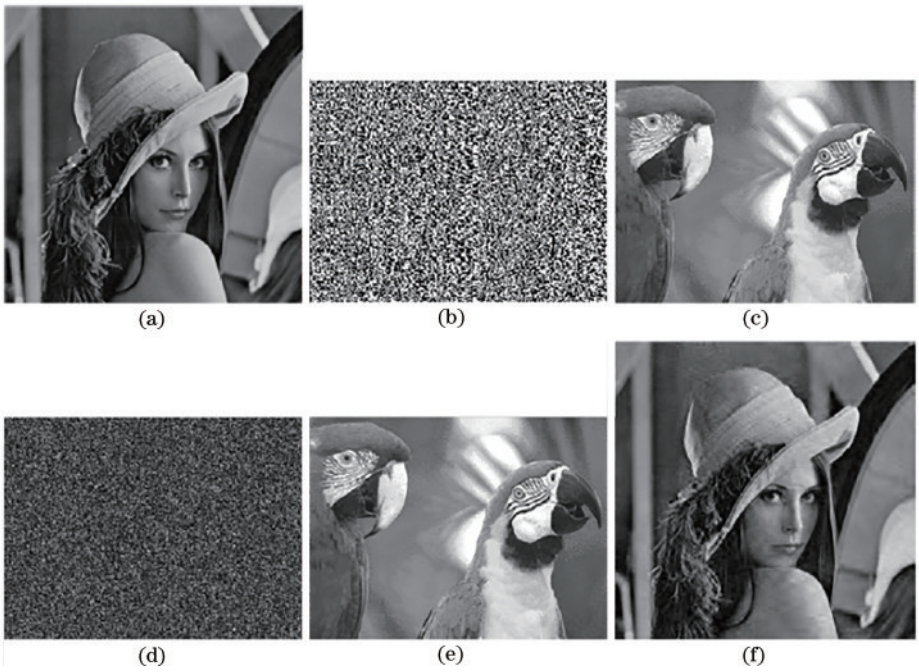

图 10　基于压缩感知和双随机相位编码的图像加密系统的仿真结果[55]。(a)原始图像;(b)经传感矩阵降采样后的图像;(c)宿主图像;(d)密文;(e)含密文信息的宿主图像;(f)重建图像

Fig. 10　Simulation results of image encryption system based on compression sensing and double random phase coding[55]. (a) Original image; (b) image downsampled by sensing matrix; (c) host image; (d) ciphertext; (e) combined image containing cipher information; (f) reconstructed image

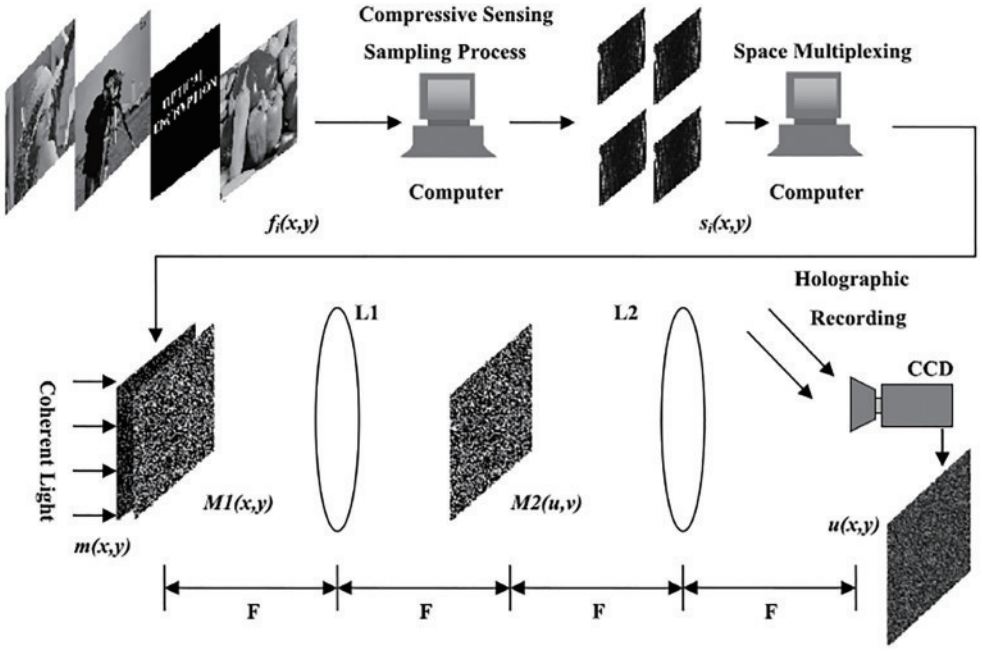

图 11　基于空间复用和压缩感知的光学加密过程示意图[58]

Fig. 11　Schematic of optical encryption process based on spatial multiplexing and compression sensing[58]

合变换相关密码系统中解密结果对相位板平移非常敏感这个事实,实现多图像加密,并给出了相应的实验结果。类似的复用方法还有拓扑电荷数复用[69]等。最近,密钥旋转复用也被引入到非相干光密码系统以实现多图像加密[70],不同的是,作者既采用了密钥围绕光轴方向的旋转复用,也采用了密钥围绕垂直于光轴方向的旋转复用。

尽管复用技术的可行性在多种光学密码系统中都得到了证实,但是该技术的缺陷也显而易见:受串扰噪声影响,解密图像质量不高,如图 14(b)所示,而且随着加密图像数量的增加,串扰噪声变得愈加严重,此时解密图像有可能完全淹没于噪声中。为了有效抑制串

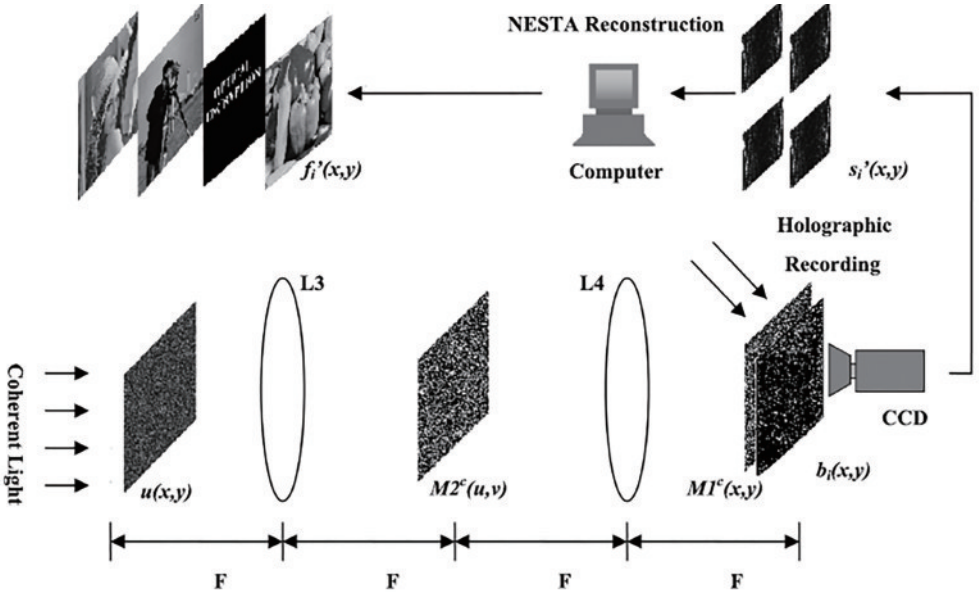

图 12　基于空间复用和压缩感知的光学解密过程示意图[58]

Fig. 12　Schematic of optical decryption process based on spatial multiplexing and compression sensing[58]

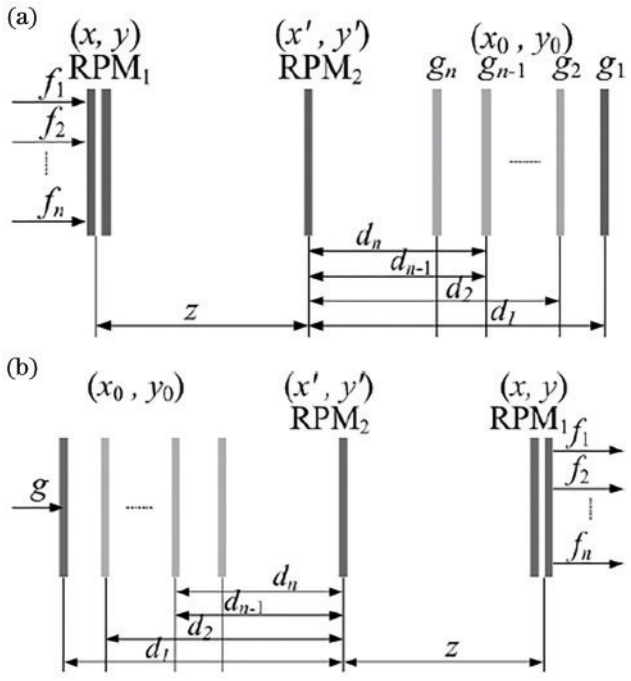

图 13　基于距离复用的多图像加密技术[63]。(a)加密过程；(b)解密过程

Fig. 13　Multiple-image encryption based on position multiplexing[63]. (a) Encryption; (b) decryption

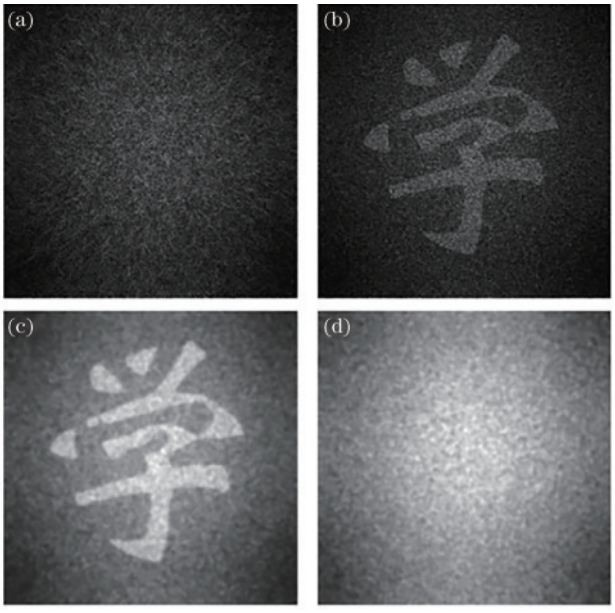

图 14　基于距离复用的多图像加密系统的数值仿真结果[63]。(a)密文；(b)对应于位置 d_5 的解密结果；(c)对图 14(b)所示的图像进行高斯滤波的结果；(d)对应于位置 $d_1-3.5\Delta d_{\min}$ 处的解密结果

Fig. 14　Numerical simulation results of multiple-image encryption scheme based on position multiplexing[63]. (a) Ciphertext; (b) decryption corresponding to position d_5; (c) result of Gaussian filtering on the image shown in Fig. 14 (b); (d) decryption corresponding to position $d_1-3.5\Delta d_{\min}$

扰噪声，研究人员提出了一系列对明文或者密文进行预处理的方法。Mosso 等[71]注意到密文在空域的直接叠加造成解密时无法将对应于各个明文的密文分离，因而产生了串扰噪声，因此他们利用 theta 调制方法对叠加之前的密文进行预处理，其加密方案如图 15 所示。在完成了第一步对明文序列的加密之后，得到了密文序列 $E_i, i=1, 2, 3, \cdots$；之后，对于每一个 E_i 分配一个正弦光栅，对其进行调制(theta 调制)，每个正弦光栅的参数(频率和方向)都不尽相同；然后，将调制后的密文相加，形成最终的复合密文。这样，虽然复合密文中各个密文成分在空域仍然不可分离，但是由于 theta 调制的作用，它们的频谱在复合密文的频域内已经互相分离。因而，只需要通过带通滤波操作，就可以将属于每个原始密文的频谱提取出来。再对其进行傅

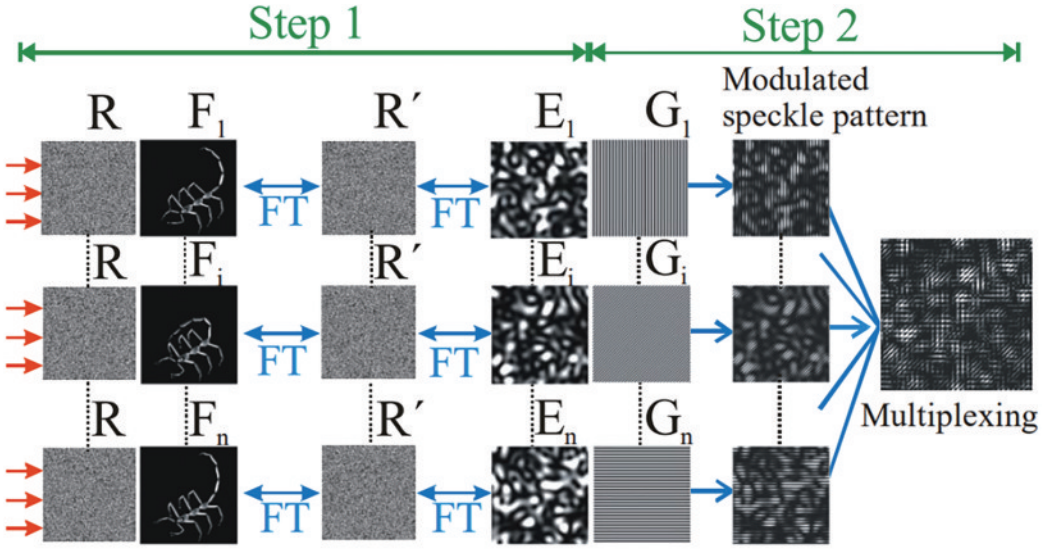

图 15　基于 theta 调制原理的多图像加密方案[71]

Fig. 15　Theta-modulation-based multiple-image encryption[71]

里叶逆变换，就可以准确地恢复对应的密文，其原理如图 16 所示。基于 theta 调制的多图像加密方案极大地抑制了串扰噪声，得到了较高质量的重建结果，如图 17 所示。受此启发，He 等[72]将 theta 调制原理引入到基于干涉原理的加密系统中，并结合相位恢复算法，提出了一种新的多图像加密方法。Qin 等[73]将 theta 调制引入到光学衍射成像加密系统中，提出了一种彩色图像加密方法。

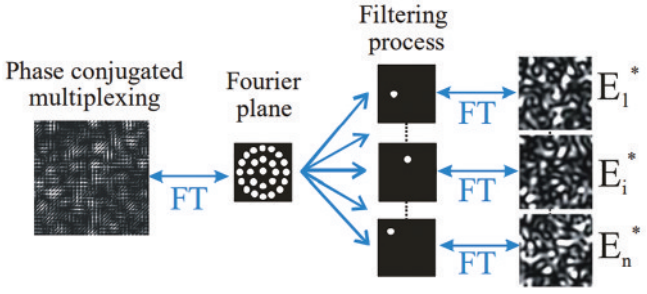

图 16　基于 theta 调制原理的多图像加密的密文重建方法[71]

Fig. 16　Reconstruction of ciphertexts in theta-modulation-based multiple-image encryption[71]

与 theta 调制具有相似技术原理的，还有基于全息原理的角度复用技术。Shen 等[74]在基于全息原理的光学密码系统中，对于每一幅原始图像所形成的物光波，都采用与光轴有不同夹角的参考光与之干涉，得到加密的全息图。这些不同的夹角控制了全息图频谱中 +1 和 −1 级频谱到 0 级频谱的距离。因此，将这些全息图（去除无关项）直接叠加，它们的频谱在频域中仍然能够分离开来。采用具有特定角度参考光的共轭波来照明全息图，对应的明文的光波将沿着光轴传播而被 CCD 记录，其他的噪声项则偏离光轴。最近，Xi 等[75]在全息加密系统里面利用 CCD 的旋转角度复用来实现多图像加密，其原理如图 18 所示。其中，物光

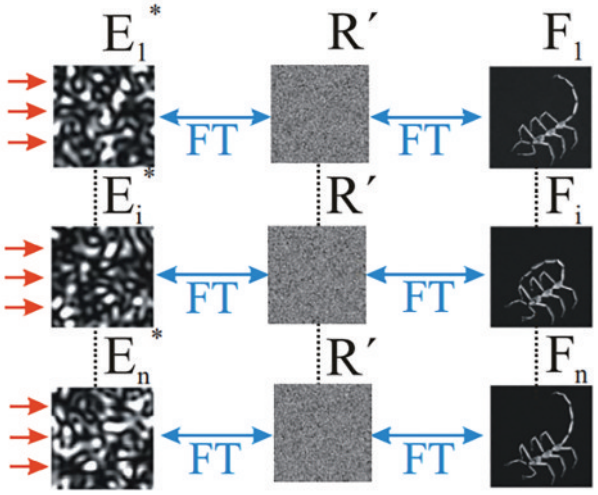

图 17　基于 theta 调制原理的多图像加密的明文重建结果[71]

Fig. 17　Reconstruction of plaintexts in theta-modulation-based multiple-image encryption[71]

与参考光的夹角 α_i 控制干涉条纹的周期，而 CCD 的旋转角度 θ_i 控制干涉条纹的方向。作者选择固定 α_i，而对 θ_i 进行复用：每加密一幅图像，就将 CCD 在 x-y 平面旋转至一个不同的角度，记录下对应的密文。待 4 幅明文全部加密完成后，将所有的密文直接相加得到复合密文。复合密文的频谱中，各个原始密文的频域在空间中互相分离，可以采用滤波的方法单独提取，如图 19 所示。

此外，人们也提出了一些特殊的参数复用的方法。例如 Li 等[76]提出了一种可以称为“强度复用”的多图像加密方案。其核心在于通过设计适当的光路，产生多个具有不同光强值的 quick response（QR）码图像（明文），并对它们直接进行非相干叠加形成一个总强度图像，实现了信息压缩。由于参与叠加的各个 QR 码的强度差异较大，强度最大的那个 QR 码可以直接

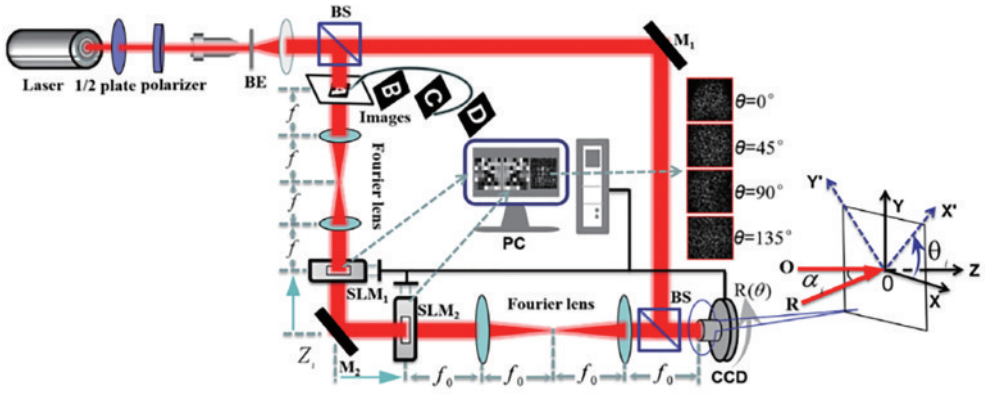

图 18　基于CCD旋转角度复用的多图像加密系统[75]

Fig. 18　Multiple-image encryption based on angular multiplexing of CCD[75]

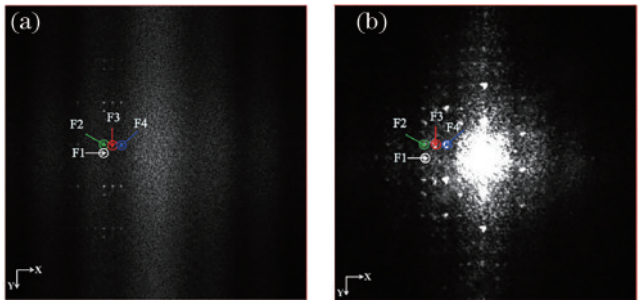

图 19　基于CCD旋转角度复用的多图像加密系统复合密文的频谱[75]。(a)模拟结果;(b)实验结果

Fig. 19　Spectrum of the synthetic ciphertext of multiple-image encryption based on angular multiplexing of CCD[75]. (a) Simulation result; (b) experimental result

被识别出来并通过二值化算法得到精确恢复;之后,从总强度图像中将强度最大的QR码减去,即可得到更新后的总强度图像;在更新后的总强度图像中,又可以将其中光强最大的那个QR码提取出来。以此类推,可将参与叠加的若干QR码都分别解压缩出来。

3.2.2　基于经典压缩的光学图像压缩加密

利用经典压缩算法压缩密文的一个代表性工作由Naughton等[30]所报道。他们先研究了无损压缩方法,包括Lempeland Ziv(LZ77)编码、Lempel-Ziv-Welch(LZW)编码、Huffman编码、Burrows-Wheeler(BW)编码,用于压缩密文,结果如表2所示。可以看出,这些方法所达到的压缩比都在1左右,表明这些无损压缩方法几乎无法压缩密文。

然而,如果将一种典型的有损压缩——量化压缩,先作用于密文,再对其实施无损压缩,则可以获得良好的压缩效果,结果如表3所示。可以看出,随着量化程度的增强(量化阶数的减少),压缩效果越来越好。例如,当量化阶数由8变为2的过程中,由LZ77压缩后的密文尺寸从5460 kB降低至47 kB。然而,由于量化压缩是一种有损压缩,随着压缩程度的提升,密文的信息损失逐渐增加,由其重建的明文质量也越来越差,如图20所示。因此,需要在明文的重建质量和压缩比之间进行折中考虑。

表2　经典压缩算法直接压缩密文的压缩效果[30]

Table 2　Results by applying several classical compression methods to the original ciphertext[30]

Hol. no.	Size(kB)	LZ77(kB)	LZW(kB)	Huff.(kB)	BW(kB)	Compression ratio			
						LZ77	LZW	Huff.	BW
1	65,536	62,651	65,536	62,529	63,869	1.05	1.00	1.05	1.03
2	65,536	62,644	65,536	62,519	63,836	1.05	1.00	1.05	1.03
3	65,536	62,645	65,536	62,515	63,823	1.05	1.00	1.05	1.03
4	65,536	62,643	65,536	62,515	63,825	1.05	1.00	1.05	1.03
5	65,536	62,641	65,536	62,513	63,825	1.05	1.00	1.05	1.03
Averages:						1.05	1.00	1.05	1.03

由于密文常常具有随机噪声的特性,所以必须采用有损压缩的方法进行压缩,因而导致由压缩后的密文恢复压缩前的密文是极其困难的“逆问题”。近年来,随着人工智能技术的发展,深度学习成为了解决此类“逆问题”的强大工具[77]。深度学习分支众多,其中应用最广泛的是有监督学习,即依靠大量的数据训练来使深度神经网络学习到一个未知系统的输入输出之间的复杂函数关系[78]。最早将深度学习技术用于恢复有损压缩过程中信息损失的是Dong等[79],他们利用深度学习来处理JPEG压缩所造成的图像质量下降问题。通过生成大量的原始图像和JPEG压缩图像数据对,训练神经网络,神经网络可以直接对一幅因JPEG压缩而降质的图像进行高质量复原。Jiao等[80]将JPEG用于对计算全息图的压缩并采用深度神经网络

表 3　经典压缩算法用于量化密文的压缩效果[30]

Table 3　Results by applying several classical compression methods to the quantized ciphertext[30]

Bits	Size(kB)	LZ77(kB)	LZW(kB)	Huff.(kB)	BW(kB)	Compression ratio			
						LZ77	LZW	Huff.	BW
2	65,536(16,384)	47	42	1027	32	1394(349)	1560(390)	64(16)	2048(512)
3	65,536(16,384)	1138	1006	1317	1097	58(14)	65(16)	50(12)	60(15)
4	65,536(16,384)	2120	1963	1991	2084	31(7.7)	33(8.3)	33(8.2)	31(7.9)
5	65,536(16,384)	3097	2969	3021	2985	21(5.3)	22(5.5)	22(5.4)	22(5.5)
6	65,536(16,384)	4003	4018	3923	3901	16(4.1)	16(4.1)	17(4.2)	17(4.2)
7	65,536(16,384)	4732	5124	4784	4795	14(3.5)	13(3.2)	14(3.4)	14(3.4)
8	65,536(16,384)	5460	6236	5613	5659	12(3.0)	11(2.6)	12(2.9)	12(2.9)

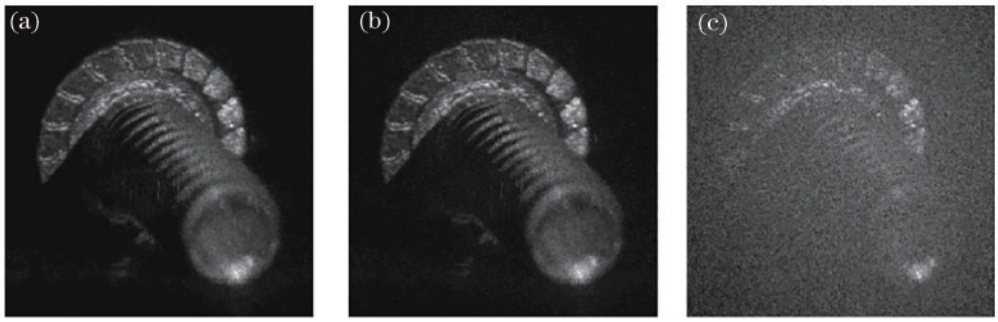

图 20　对密文中每个像素值进行不同阶数的量化而得到的解密结果[30]。(a) 4 阶;(b) 3 阶;(c) 2 阶

Fig. 20　Decrypted results obtained by quantizing each pixel value in the ciphertext by different orders[30]. (a) 4 bits; (b) 3 bits; (c) 2 bits

进行重建。Shimobaba 等[81]提出了一种基于误差扩散的全息图二值化压缩方法,并采用深度神经网络进行重建。需要指出的是,相比于计算全息图,光学密码系统的密文更难压缩,因为其像素之间的相关性更弱。在这种背景下,本课题组[82]提出了一种基于光学密码系统密文的通用压缩与解压缩方法,该方法原理性流程如图 21 所示。图 21(a)给出了压缩过程,先采用双线性插值将密文(CM)由 $N\times N$ 降采样至 $M\times M$,再利用 JPEG2000 对其进一步压缩。解密时,由训练好的深度神经网络直接从压缩后的密文预测原始密文。

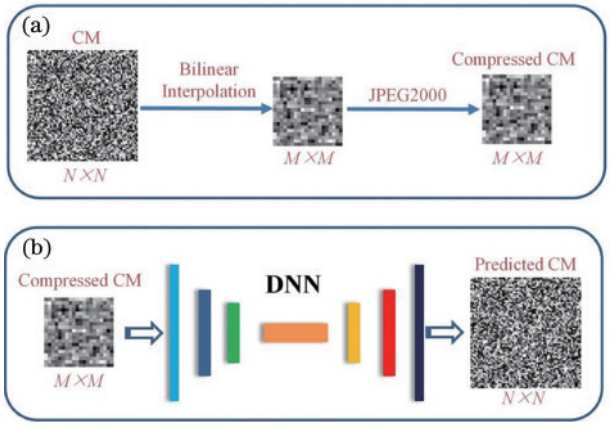

图 21　基于深度学习的光学密文压缩方法[82]。(a)压缩过程;(b)解压缩过程

Fig. 21　Optical ciphertext compression method based on deep learning[82]. (a) Compression; (b) decompression

该方法与 JPEG、JPEG2000 的压缩效果对比如图 22 所示。可以看出,若以相关系数(CC)为标准进行评价,在解压密文质量接近的情况下,所提出的方法压缩后的密文仅有 273B,远小于 JEPG 的 2382B 和 JPEG2000 的 1867B。

3.2.3　基于密文侧压缩采样的光学图像压缩加密

压缩感知在光学领域内最直接的应用就是单像素成像,而鬼成像正是基于单像素相机的成像技术,因此压缩感知被广泛地应用到此领域以实现压缩加密,所采用的压缩方式就是减少采样次数,从而实现密文压缩。可以看出,与参数复用压缩和经典压缩不同,压缩感知是在采样过程中实现密文压缩的,即“边采样边压缩”。

2011 年,Durán 等[29]在计算鬼成像加密的基础上,提出了压缩感知计算鬼成像加密。他们采用的加密光路如图 23 所示。为了实现加密,在空间光调制器(SLM)上依次加载 3500 个不同的随机相位板(密钥),并利用桶探测器(BD)记录相应的光强值(密文),实现了密文的大幅度压缩。他们分别采用常规解密算法和压缩感知解密算法,给出了相应的仿真结果,如图 24 所示。结果显示,在采样 3500 次的情况下,利用压缩感知重建的原始明文的信噪比为 18 dB,远远高于使用普通计算鬼成像重建图像的信噪比 2.5 dB。但是压缩感知也不能无限地压缩加密数据,例如将采样次数降低到 200 时,就无法正确地解密出结果。

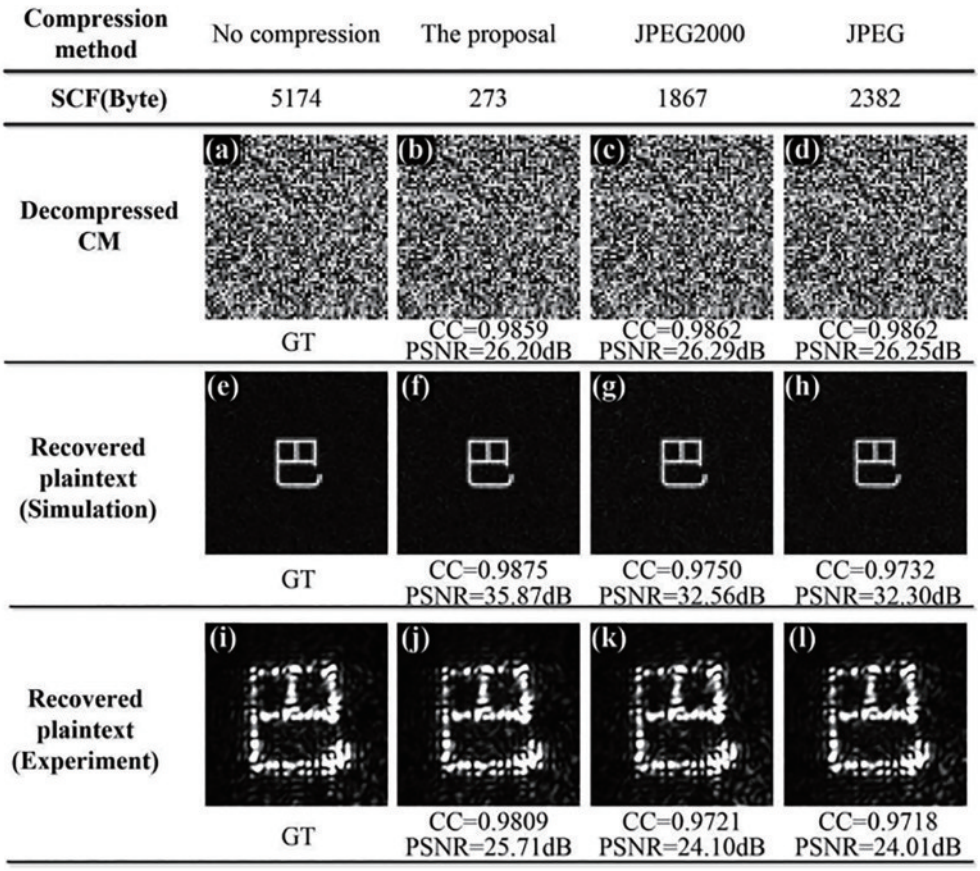

图 22　基于深度学习的光学密文压缩方法与 JPEG、JPEG2000 的对比[82]

Fig. 22　Comparison of the deep-learning-based optical ciphertext compression approach with JPEG and JPEG2000[82]

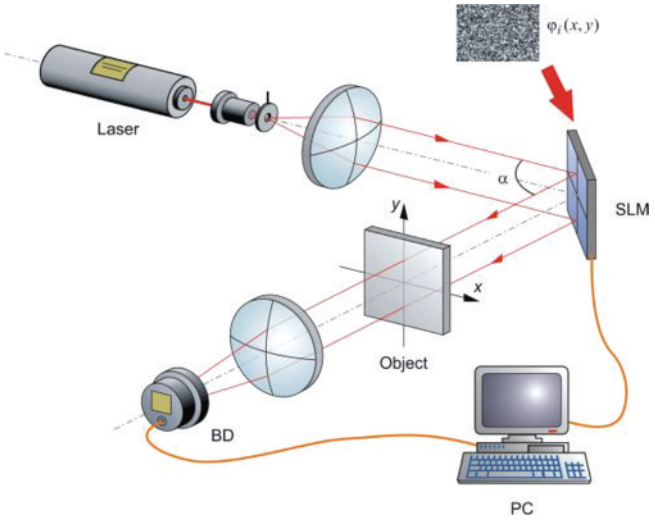

图 23　压缩感知计算鬼成像加密系统[29]

Fig. 23　Optical encryption based on compressive ghost imaging encryption[29]

研究人员对压缩鬼成像加密系统进行了许多的改进和拓展。Yuan 等[83]通过迭代算法先将灰度图像转换为二值图像，再送入压缩鬼成像系统中进行加密。由于恢复二值图像所需要的测量次数远远小于灰度图像，因此进一步压缩了密文尺寸。Zhu 等[84]采用离散小波变换先将图像变换为稀疏图像，再送至压缩鬼成像系统进行加密，也实现了对密文的有效压缩。与此同时，他们还对密钥（随机相位板）进行了复用，同时实现多光路（多幅图像）加密，提高了加密的效率并节约了存储密钥的空间。Zhang 等[85]基于压缩鬼成像加密系统提出了一种新颖的密钥生成方法：先生成一个随机的二值矩阵，把其中“1”的行序号和列序号作为生成密钥的参数，这样仅需一个矩阵就可以确定大量的密钥，提升了密钥传输速度并节省了存储密钥所需的空间。Zhao 等[86]将 QR 码引入到压缩鬼成像加密系统中，进一步实现了对密文的压缩，并提升了系统的安全性。他们首先将原始信息编码到 QR 码中，再送入到计算鬼成像系统中进行加密。由于 QR 码具有较强的容错性和抗干扰能力，因此即使解密的 QR 码质量较差，也能通过纠错算法完全恢复其所含信息，因而降低了鬼成像加密系统的测量次数，实现了对密文的有效压缩。近年来，一些学者利用变换域压缩和压缩鬼成像结合，进一步提升了鬼成像加密系统的效率，这些变换包括离散傅里叶变换[87]、举升小波变换（LWT）[88]、离散余弦变换[89]等。

除了直接在单像素成像加密系统中进行压缩采样，人们也利用压缩感知对其他光学密码系统的密文进行压缩采样。Li 等[90]将单像素成像、相移全息以及随机相位编码相结合，提出了一种新的压缩加密系统，

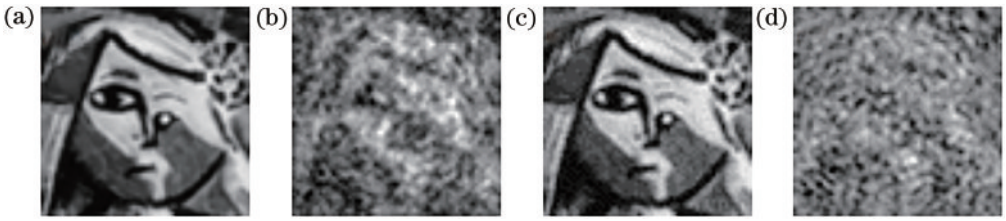

图 24　压缩鬼成像加密的解密结果[29]。(a)明文;(b)采样 3500 次时常规方法的解密结果;(c)采样 3500 次时压缩感知的解密结果;(d)采样 200 次时压缩感知的解密结果

Fig. 24　Decrypted results using compressive ghost imaging[29]. (a) Plaintext; (b) decrypted result obtained by conventional method under 3500 samplings; (c) decrypted result obtained by compressive sensing under 3500 samplings; (d) decrypted result obtained by compressive sensing under 200 samplings

其加密光路如图 25 所示。图像经双随机相位编码后形成的物光和参考光在 DMD 所在平面干涉,形成全息图,再由 DMD 及相关附件构成的单像素成像系统对全息图进行压缩成像。解密时,先由压缩感知算法重建全息图,再由相移算法计算得到物光波复振幅,最后通过双随机相位解码得到原始图像。该方法对灰度图像的解密结果如图 26 所示。需要指出的是,尽管该方法的有效性得到了证实,但是其重建图像质量不高。其原因在于:该系统采用压缩感知对全息图这一特殊对象进行压缩采样,相比于自然图像,全息图的稀疏性特征并不明显,压缩感知的前提条件难以得到较好的满足。Li 等[91]还将单像素成像与光学联合变换相关系统和二步相移数字全息系统结合[92],实现了对图像的压缩加密。

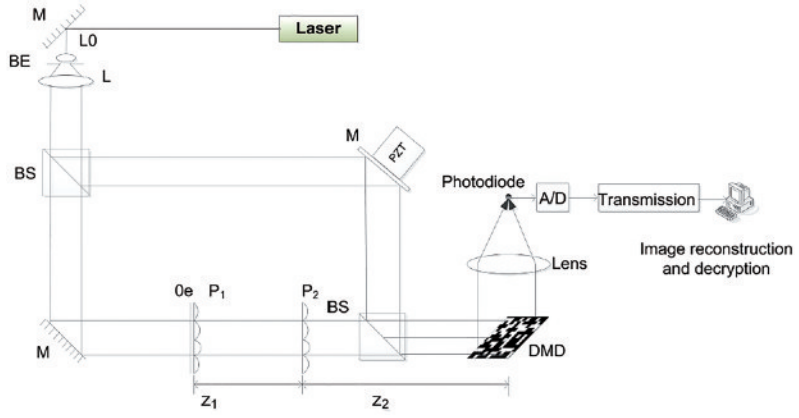

图 25　基于单像素成像、相移全息以及随机相位编码的加密系统[90]

Fig. 25　Encryption system based on single pixel imaging, phase shifting holography, and random phase coding[90]

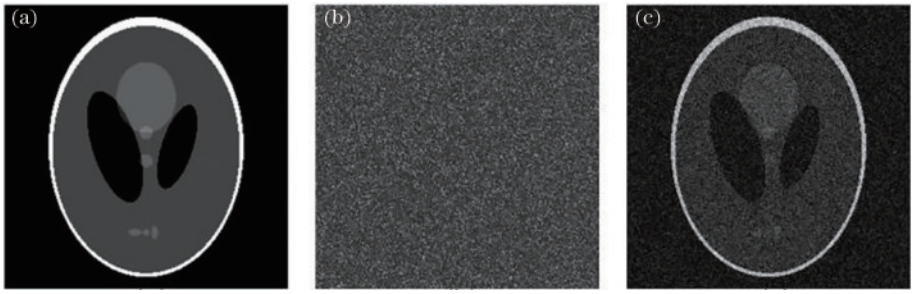

图 26　加密系统对灰度图像的解密结果[90]。(a)明文;(b)DMD 平面的全息图之一;(c)约 256×256×42.1% 次测量的重建结果,其中 256×256 为像素数,42.1% 为采样比例

Fig. 26　Decryption result of gray image obtained by encryption system[90]. (a) Plaintext; (b) one of the encrypted holograms on the DMD plane; (c) retrieved image of about 256×256×42.1% measurements, where 256×256 denotes the pixel count and 42.1% denotes the sampling ratio

3.3　明文密文同步压缩的光学图像压缩加密

基于迭代相位恢复算法的图像压缩加密有“迭代加密,光学解密”和“光学加密,迭代解密”两种基本框架。“迭代加密,光学解密”指通过迭代算法将图像加密至若干相位/振幅板中,解密时通过相干光照射这些相位/振幅板构成的光学系统,直接在输出平面得到解密图像。

“光学加密，迭代解密”框架通常将若干幅原始图像置于含有波前调制器件（例如相位板或振幅板）的光学系统中，通过相干光照射，直接采用强度敏感器件（例如CCD）记录衍射图样，再采用迭代相位恢复算法进行解密。

3.3.1　基于“迭代加密，光学解密”框架的光学图像压缩加密

基于“迭代加密，光学解密”框架的一个典型例子是由Chen等[93]提出的基于多平面相位恢复和干涉原理的多图像加密系统。其光学解密方法如图27所示。其中M2和M3是两个纯相位板，采用相干的两束平行光分别照射它们，就可以在P1、P2、P3、P4四个不同的平面得到对应的原始明文。M1是一个纯相位板，是加密算法中的一个中介值。该系统的加密算法先将4幅原始明文记作I1、I2、I3、I4，通过迭代算法加密到相位板M1中，再进一步将M1分解为相位板M2和M3。所使用的迭代算法的示意图如图28所示，包含以下过程。

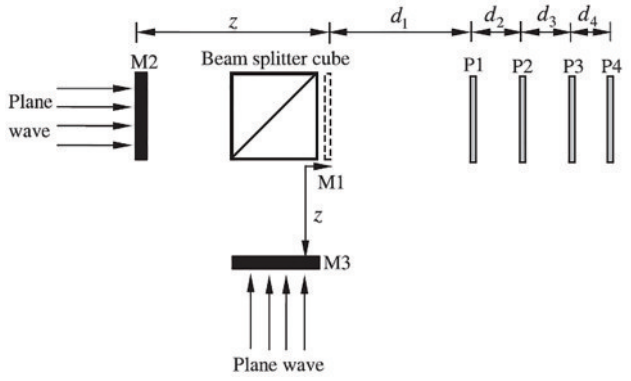

图27　基于多平面相位恢复和干涉原理的多图像加密系统的光学解密方案[93]

Fig. 27　Optical decryption scheme of multi-image encryption system based on multi-plane phase recovery and interference principle[93]

1）给M1赋予随机的初始值作为其估计值，前向衍射至P1平面，得到复振幅。保留此复振幅的相位，同时采用I1来替换此复振幅的部分振幅，形成一个新的复振幅。将此新的复振幅逆衍射至M1平面，仅保留其相位，作为M1的新的估计值。

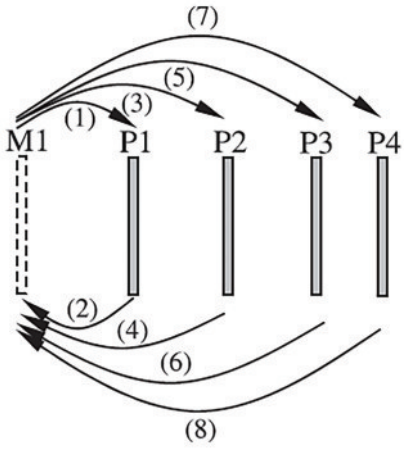

图28　基于多平面相位恢复算法和干涉原理的多图像加密系统的迭代算法[93]

Fig. 28　Iterative algorithm of multi-image encryption system based on multi-plane phase recovery algorithm and interference principle[93]

2）将上述M1的新的估计值前向衍射至P2平面，保留波前的相位并用I2来替换波前的部分振幅，形成新的复振幅，同样将其逆衍射至M1平面，取其相位得到M1的新的估计值。以此类推，重复上述过程，直至将4个输出平面全部计算完毕。

3）利用M1的当前估计值，计算4个输出平面的重建结果与对应原始明文的相关系数。如果相关系数高于设定的阈值，则停止迭代；否则，转入步骤1）继续迭代，直至算法收敛。

在上述方法的基础上，Chen等[94]进一步将图像加密拓展到三维空间，其设计方案如图29所示，目的是将多个图像加密至相位板M中。其关键在于将每一幅原始图像都切割为互不重叠的小像素块（作者称为“粒子”）并沿着光轴分离。如图29所示，组成三个明文的粒子分别分布在三个立方体所示的空间内。将三个立方体内沿光轴方向重叠的三个粒子为一组进行迭代，直至将所有像素块遍历完毕，迭代方法与图28所示方法类似。该方法的主要优势在于：构成这些明文的像素块与相位板M的距离各不相同，要想正确地解密明文必须掌握这些距离，这就极大地增加了密钥空间，提升了系统的安全性。

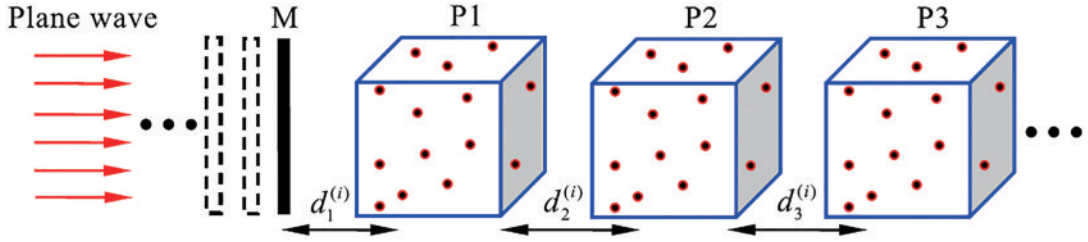

图29　基于三维空间和相位恢复算法的多图像加密方法[94]

Fig. 29　Multiple-image encryption based on 3D space and phase retrieval algorithm[94]

需要指出，在上述两种密码系统中，关键都是利用“距离”这个自由度来区分不同的目标图像，进而借助迭代相位恢复算法实现压缩加密。这一技术也可以称为相位恢复算法中的“距离复用”。从这一点推广出去，凡是能够影响光波衍射结果的其他参数，也都具有潜在的复用可能性。例如，Lü等[95]提出了一种基于角度复用和相位恢复算法的多图像加密方案，其解密方法如图 30 所示。两个纯相位板 DOE1 和 DOE2 都位于原始位置时，解密得到的是图像 VK_1；当它们分别转动角度 ω 和 θ 后，解密得到的是另外一个图像 VK_2。其加密算法与图 28 所示方法类似，基本迭代约束仍然是输入面的纯相位约束（丢弃振幅信息）以及输出面的振幅约束（目标图像）。区别在于，每次往返迭代结束，切换到下一轮迭代（输出面采用新的目标图像进行约束）时，需要相应地更改相位板的旋转角度而非衍射距离。最近，Lu等[96]对此算法进行进一步改进，使不同的解密图像质量更加均衡。

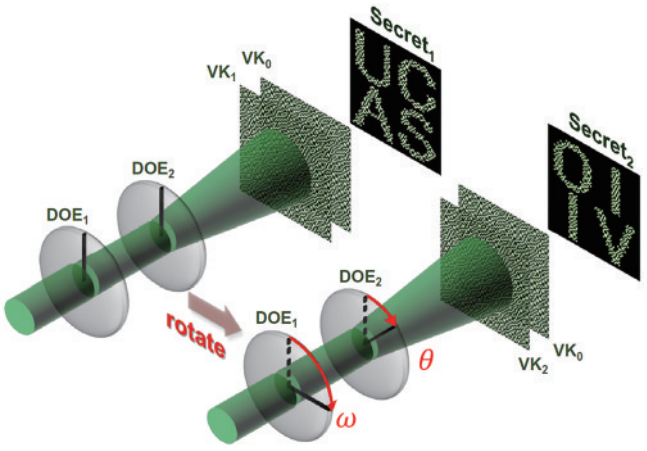

图 30　基于角度复用和相位恢复算法的多图像加密方法[95]

Fig. 30　Multiple-image encryption based on azimuth multiplexing and phase retrieval algorithm[95]

此外，Wu等[97]基于空间复用和迭代相位恢复算法提出了一种多图像加密方法。其中对于某一幅图像，其解密光路和迭代方案如图 31 所示。基本原理也是通过输入和输出平面的振幅约束进行迭代，最终将一幅图像加密至一个纯相位板中。不同的是，其在输入平面施加了振幅约束[如图 31(b)所示，白色方块代表“1”，黑色区域代表“0”]，这样上述相位板有效的相位数据被限制在白色方块所占据的区域内，而黑色区域则成为了冗余空间。显然，如果对若干幅图像在输入平面所实施的振幅约束互不重叠，那么这些数据就可以在输入面直接进行叠加而互不干扰，从而形成一个包含若干密文的复合密文，如图 32 所示。

基于“迭代加密，光学解密”框架的另外一个典型实例是采用级联相位恢复算法的多图像加密系统[98]。由于该系统由多个 $4f$ 加密系统级联而来，以第一级 $4f$

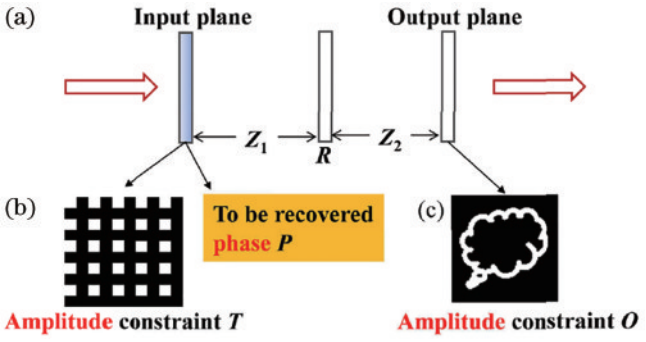

图 31　基于输入面振幅约束的迭代加密系统[97]。(a)解密光路和迭代算法依据；(b)输入平面的振幅约束；(c)输出平面振幅约束（即期望解密得到的明文）

Fig. 31　Iterative cryptosystem based on amplitude constraint in input plane[97]. (a) Decryption optical path and iterative algorithm basis; (b) amplitude constraint in input plane; (c) amplitude constraint in output plane

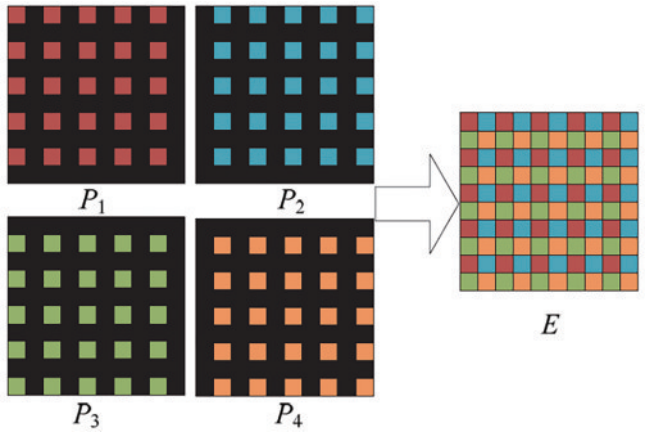

图 32　基于空间复用的密文合成方法[97]

Fig. 32　Ciphertext combination method based on spatial multiplexing[97]

系统的加密算法为例来说明，解密方案如图 33 所示，其中 $g(x,y)$ 为期望解密得到的明文图像，$f(x,y)$ 为密钥，两个相位板 RPM1 和 RPM2 为密文，其相位值分别表示为 θ 和 φ，且其初始值随机。在第 k 次迭代中，输入平面和输出平面有以下函数关系：

$$g^k(x,y)\exp\left[\mathrm{i}\phi^k(x,y)\right]=\mathrm{FT}^{-1}\left\{\mathrm{FT}\left\{f(x,y)\times\exp\left[\mathrm{i}\theta^k(x,y)\right]\right\}\exp\left[\mathrm{i}\varphi^k(\mu,\nu)\right]\right\},\tag{8}$$

利用所期望解密的明文图像 $g(x,y)$ 来代替 $g^k(x,y)$，并更新 $\varphi^k(\mu,\nu)$ 和 $\theta^k(x,y)$：

$$\varphi^{k+1}(\mu,\nu)=\mathrm{angle}\left\{\frac{\mathrm{FT}\left\{g(x,y)\exp\left[\mathrm{i}\phi^k(x,y)\right]\right\}}{\mathrm{FT}\left\{f(x,y)\exp\left[\mathrm{i}\theta^k(x,y)\right]\right\}}\right\},\tag{9}$$

$$\theta^{k+1}(x,y)=\mathrm{angle}\left\{\mathrm{FT}^{-1}\left\{\mathrm{FT}\left\{g(x,y)\times\exp\left[\mathrm{i}\phi^k(x,y)\right]\right\}\exp\left[-\mathrm{i}\varphi^k(\mu,\nu)\right]\right\}\right\},\tag{10}$$

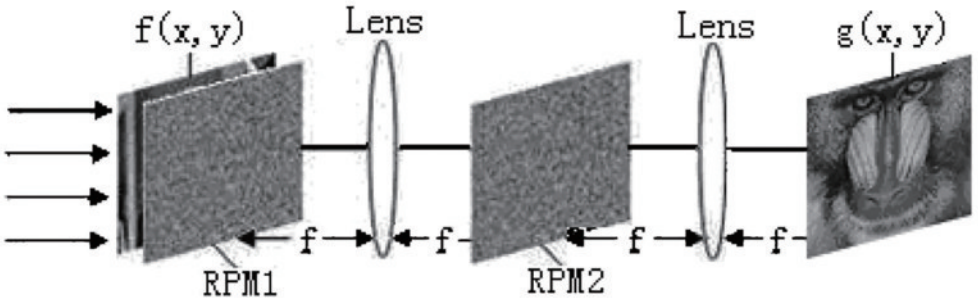

图 33　基于光学 4*f* 系统的图像加密[98]

Fig. 33　Optical encryption based on 4*f* correlator[98]

式中：angle(·)表示取幅角。如果解密图像与原始图像之间的相关系数大于设定的阈值，则迭代停止，否则继续迭代。需要指出的是，后面级联的若干 4*f* 系统的加密方法与第一级类似，不同的是，其输入不再是一个灰度图像，而是前一级的输出(复振幅)，因此在迭代过程中要考虑本级输入面上相位的影响。与该方法具有类似原理的，还有 Huang 等[99]提出的无透镜多图像加密系统，解密过程中只需要用到一系列位于不同轴向位置的纯相位板，系统得以大大简化。此外，作为“迭代加密，光学解密”框架的一个特例，Liu 等[100]基于分数傅里叶变换提出了一种双图像加密系统。

需要指出的是，在实际应用中，纯相位板制作的难度很大，因为传统的制作方法都是依靠光程累积来实现对波前的相位调控的。此外，利用空间光调制器实现纯相位调制则需要考虑周期性结构和有效像元之间的“死区”对结果的影响，实施难度较大。因此，上述文献仅仅给出了数值仿真结果，而没有采用实验进行证实。近年来，超颖表面展现了对波前调控的强大能力，它可以在亚波长的尺度上任意调节入射光波的振幅、相位及偏振态[101]；同时，它的加工难度和制造成本都相对不高，易于物理实现[102]。基于超颖表面，Georgi 等[33]提出了一种秘密共享(多图像加密)系统，成功地将三幅图像隐藏于两个纯相位板中，其解密方案如图 34 所示。其中 Share 1 和 Share 2 是由超颖表面制作的纯相位板，采用相干光照射其中任何一个，都能重建出隐藏其中的图像；同时，如果把它们级联起来，采用同样的相干光照射，则可以重建出第三幅图像，如图 34 中的“69”。需要指出的是，求解两个纯相位板的过程并非以 G-S 算法为基础，而是在迭代过程中，分别计算每个重建结果与目标图像的 MSE，将这些 MSE 的平均值作为目标函数。通过梯度下降法优化两个相位板的相位值，目标函数取得最小值。此外，研究者也利用超颖表面对光波偏振态[103]和轨道角动量[104]的敏感性提出了相应的复用方案，实现了对图像的压缩加密。

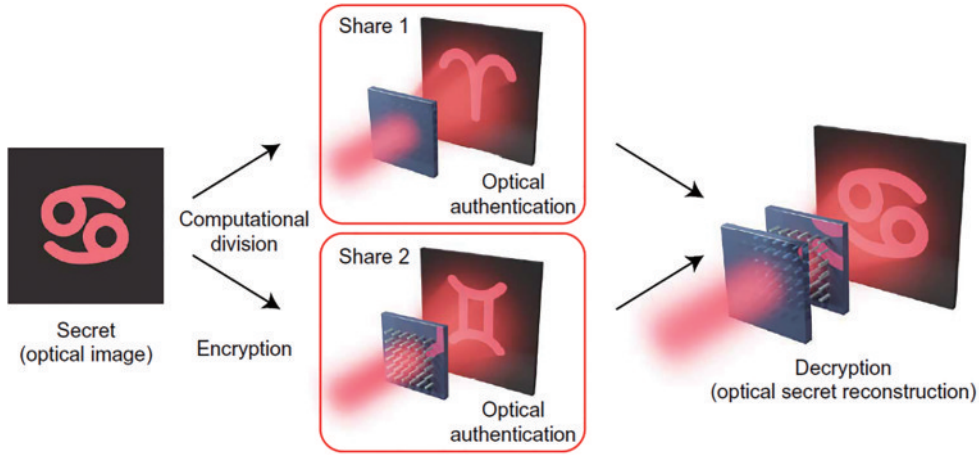

图 34　基于超颖表面和迭代算法的秘密共享(多图像加密)系统[33]

Fig. 34　Secret sharing (multiple-image encryption) system based on metasurface and iterative algorithm[33]

3.3.2　基于“光学加密，迭代解密”框架的光学图像压缩加密

光学衍射成像加密系统是一种具有代表性的基于“光学加密，迭代解密”框架的光学密码系统。该系统一种典型的加密光路如图 35 所示，其中 U 为待加密的明文，M_1、M_2、M_3 为 3 个统计独立的随机相位板。该系统的特点在于采用纯光学的方法加密，加密速度快，适用于需要对信息进行高速加密的场合。其解密方案采用迭代相位恢复算法。一般来说，要想准确地解密明文，需要改变系统参数(例如相位板的横向位置[105]

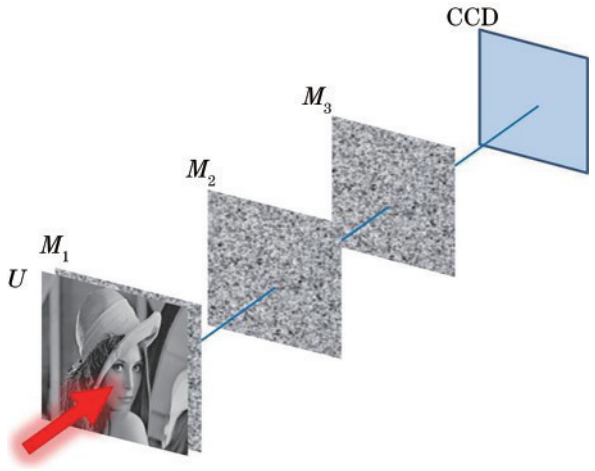

图 35　光学衍射成像加密系统

Fig. 35　Optical diffractive-imaging-based encryption scheme

或CCD的轴向位置[106])并多次曝光(记录多幅衍射强度图像),才能由迭代相位恢复算法来准确重建明文,但完成加密非常耗时,且密文数据较多。为解决这个问题,本课题组[107]基于光学衍射成像加密系统提出了简化的密文重建算法,将恢复明文所需要的衍射图像减少到1幅,实现了对密文的大幅压缩。该算法对文献[105]中所述的常规算法进行改造,分为两个阶段进行:在第一阶段,由输出面逆衍射至输入平面后,所得复振幅的强度并不直接作为明文的估计值,而是先对其进行中值滤波,再作为明文的估计值进入下一轮迭代,当本阶段的迭代进行到一定程度发生停滞时,转入第二阶段;在第二阶段,将中值滤波操作从迭代中去除,将迭代算法恢复为常规算法。所提出算法的效果如图36所示,所恢复出来的明文[如图36(a)所示]无论是主观感受还是客观指标,都达到了一个较好的程度。图36(c)和图36(d)描述了在解密所涉及的迭代过程中,中值滤波操作去除前后相关系数的变化情况。

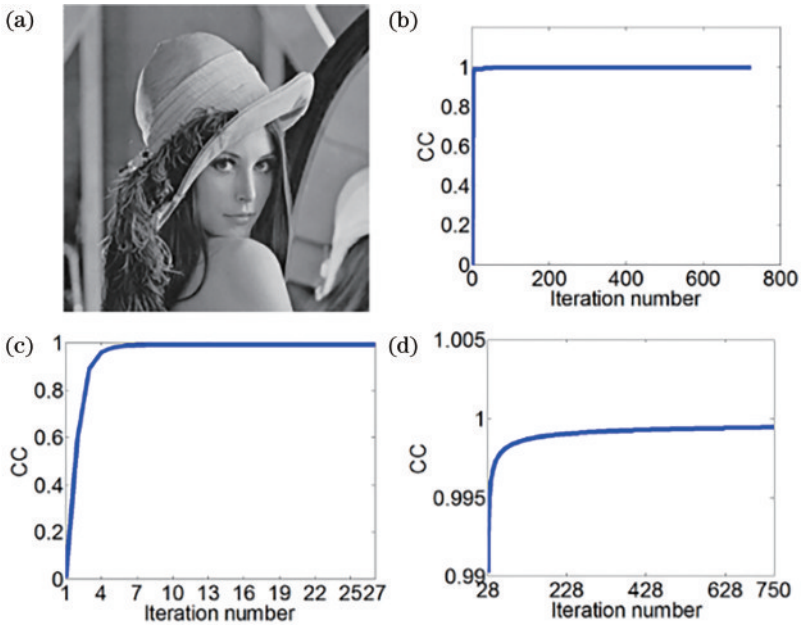

图 36　单次曝光光学衍射成像加密系统的解密算法效果[107]。(a)解密图像;(b)相关系数与迭代次数的关系;(c)第一阶段相关系数随迭代次数的变化;(d)第二阶段相关系数随迭代次数的变化

Fig. 36　Effect of decryption algorithm of single exposure optical diffraction imaging encryption system[107]. (a) Decrypted image; (b) dependence of CC on iteration number; (c) dependence of CC on iteration number corresponding to the first iterative procedure; (d) dependence of CC on iteration number corresponding to the second iterative procedure

近年来,随着一些新的相位恢复算法的出现,光学衍射成像加密系统的加密效率得到进一步提升[108-109]。例如,He等[110]提出了基于多模态相位恢复算法和焦距复用的多图像加密系统,其加密原理如图37所示,其中EFTL为电子变焦透镜。对于第k幅明文图像,仅记录一幅与之对应的衍射强度图像I_k;并且,需要在记录中为每一幅明文设置不同的透镜焦距,使得记录每一幅衍射强度图像所采用的焦距都各不相同;最后,将这些衍射强度图像直接相加,形成最后的密文($I=\sum I_k$)。显然,这种图像的直接叠加大幅压缩了密文的尺寸。提出的解密迭代算法如下。

1)假设上一轮迭代完成后,得到的第k幅待解密的明文图像的估计值为g_k(如果是第1轮迭代则赋予随机的初始值),按照加密时所采用的参数将其前向衍射至输出平面,得到对应的复振幅U_k。此操作对所有明文图像并行进行。

2)在输出平面,更新复振幅U_k:

$$\tilde{U}_k=\frac{I}{\sqrt{\sum|U_k|^2}}U_k。\tag{11}$$

3)将步骤2)得到的更新后的复振幅逆衍射传播

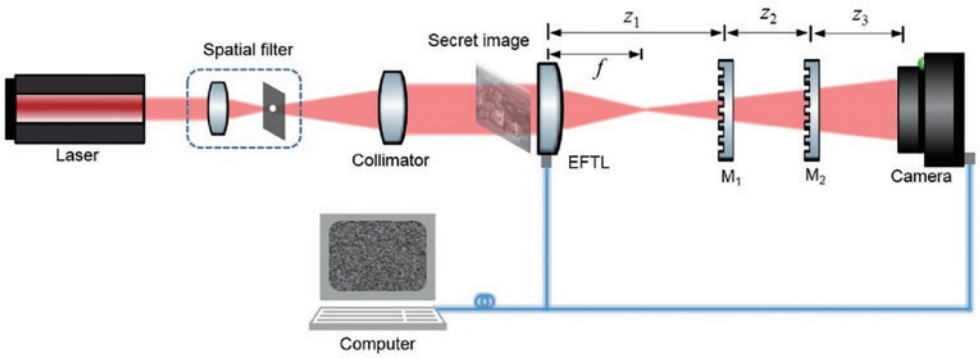

图 37　基于多模态相位恢复算法和焦距复用的多图像加密系统[110]

Fig. 37　Multi-image encryption system based on multimode phase retrieval algorithm and focal length multiplexing[110]

至输入平面，取其强度作为待解密图像的新估计值。

4）重复步骤 1）～3），直至迭代收敛。

其中，步骤 2），即输出平面的约束，是多模态相位恢复算法的核心。它是所有明文的衍射的实际总强度与所有明文估计值的衍射的总强度的比值，作为输出面约束条件，通过迭代促使二者相等。显然，这种算法充分考虑了各个明文所产生的衍射强度对密文的贡献，有力地抑制了可能出现的串扰噪声。该方法的解密效果如图 38 所示，8 幅解密的灰度图像质量（以相关系数进行评价）随着迭代次数的增加快速提升，最终都接近于 1，实现了图像的高质量解密。

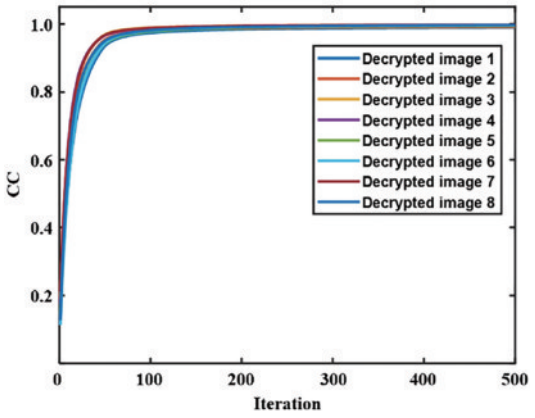

图 38　基于多模态相位恢复算法和焦距复用的多图像加密系统中解密图像质量（CC）随迭代次数的变化[110]

Fig. 38　Relationship between the quality of the decrypted images (CC) and the iteration number in the multi-image encryption system based on multimode phase retrieval algorithm and focal length multiplexing[110]

与上述方法具有类似技术原理的，还有 He 等[111]提出的单次曝光彩色图像加密技术，其加密方案如图 39 所示。不同之处在于：在上述方法中，多次曝光后需要人工地将多幅衍射图像强度叠加以形成密文；而在单次曝光彩色图像加密技术中，采用三束不同波长的激光照射彩色图像，从每束光都能提取图像中对应的颜色信息。由于波长不同，三束光携带的 R、G、B 信息经过随机相位板调制的衍射光波在输出面自然地进行了非相干叠加。这样，借助上述多模态相位恢复算法，就可以准确重建 R、G、B 三个分量。在此基础上，He 等[112]将多模态相位恢复算法与压缩感知技术相结合，又提出了基于同时波长和距离复用的多图像加密方法。

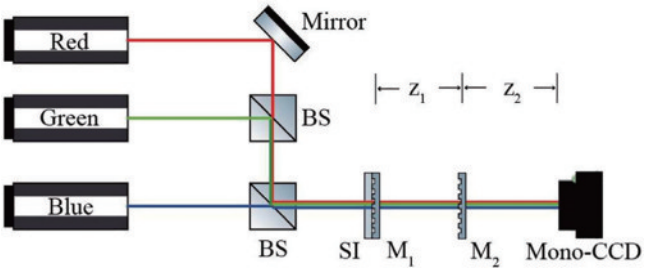

图 39　基于多模态衍射成像的单次曝光彩色图像加密系统[111]

Fig. 39　Single exposure color image encryption system based on multimodal diffraction imaging[111]

3.4　基于同步压缩采样的光学图像压缩加密

已经介绍，压缩感知既能单独对明文进行压缩采样，也能单独对密文进行压缩采样。事实上，压缩感知还可以对明文和密文进行同步压缩采样。例如 Di 等[113]在光学扫描全息（OSH）系统中同时加密沿着轴向排列的两幅图像，并利用压缩感知进行重建，实现了同步压缩的目的。然而，利用光学扫描全息加密系统实现加密时，数据采集时间较长。因此，开发使用数据并行采集的压缩感知加密系统具有重要的意义。从这一点出发，本课题组[114]提出了一种利用多光束干涉和压缩感知的多图像加密系统，其加密方法如图 40 所示。该系统中，每一幅明文（Image）都被一个随机相位板（RPM）调制，对应的物光波衍射到 CCD 平面。所有待加密图像的物光波与参考光波进行相干叠加，形成全息图。空间光调制器上依次显示 4 个相差 $\pi/2$ 的相位，以获得相移全息图。通过相移算法，可以准确重建 CCD 平面的物光波的复振幅，而该复振幅与这些明文图像有明确的函数关系。通过将此函数关系表示为符合压缩感知框架的数学模型，利用正则化项进行约束，利用优化算法正确重建明文图像。数值实验表明，该方法无论是对二值图像还是对灰度图像，都能实现高质量的解密。图 41 给出了该系统对灰度图像的

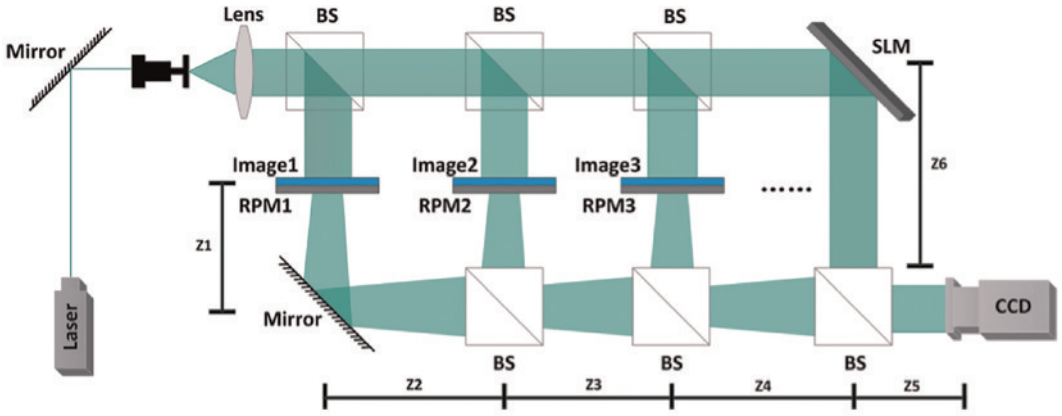

图 40　基于压缩全息的多图像加密系统[114]

Fig. 40　Multiple-image encryption based on compressive holography[114]

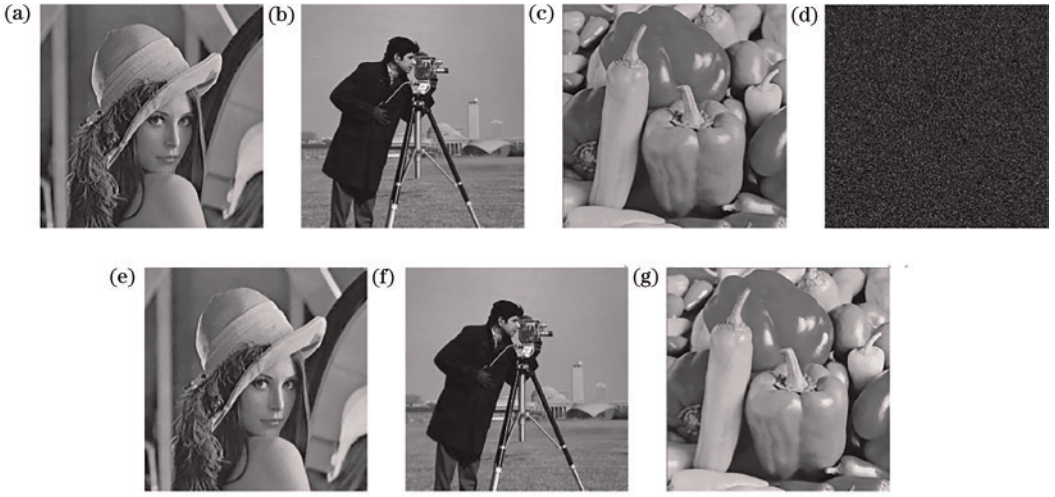

图 41　基于压缩全息的多图像加密系统的解密结果[114]。(a)～(c)明文；(d)全息图之一；(e)～(g)解密结果

Fig. 41　Decrypted results of multiple-image encryption based on compressive holography[114]. (a)-(c) Plaintexts; (d) one of the holograms; (e)-(g) decrypted results

加密和解密结果。此外，基于同步压缩采样原理的还有 Zhang 等[115]提出的一种基于随机卷积和随机下采样技术的光学密码系统。该系统类似于双随机相位编码系统，直接对密文进行随机下采样，实现压缩加密。通过建立起明文和压缩密文之间的压缩感知模型，对明文直接重建。该方法在密文采样率为 6.25% 的情况下依然得到了较好的重建结果。

3.5　各种具体压缩算法的对比与分析

对所介绍的各种具体压缩方法进行总结，表 4 给出了这些压缩方法各自的一些优势与不足。

4　展望与总结

光学图像压缩加密技术成为了光学信息安全的重要研究分支，而且近年来的研究文献呈逐年增多的趋势。这是因为，随着互联网的普及和数据交换量的高速增长，实现数据加密的同时实现数据的压缩无疑具有重要的意义。在研究方向上，以下两个方面仍将是本领域的研究重点。

1）发展新的光学图像压缩加密技术

为了适用于各种潜在的应用场景，发展出具有高压缩比、高安全性、高解密质量的新的光学图像压缩加密技术是研究者们不断追求的目标。从目前的研究报道来看，实现这个目标有两种主要的途径。其一，寻求现有压缩方法与现有光学密码系统新的结合。例如，尽管针对光学衍射成像加密系统已经有不少成果，但是据我们所知，将压缩感知应用于该系统的研究尚未报道。事实上，该系统与压缩感知结合有望进一步提升压缩比，是一个潜在的研究切入点。其二，引入新技术或新方法来发展新的光学图像压缩加密技术。一些信号处理领域和光学成像领域内的新技术或新方法往往会成为光学密码系统的设计灵感和源头。正如已经在文中所看到的，压缩感知理论的诞生极大地推动了对光学图像压缩加密技术的研究。而光学成像领域的混合态相位恢复算法的出现则直接催生了单次曝光彩色图像加密这种新型密码系统。近年来，深度学习技术的出现，又为该方向的研究注入了新的动力。已经

表 4 各种具体压缩方法的对比与分析

Table 4 Comparison and analysis of the aforementioned compression methods

Compression strategy	Compression method	Frame	Advantages and disadvantages
Plaintext compression	Transform domain compression		This method always offers high quality decryption, but the independence between the compression/decompression and the encryption/decryption leads to time consumption.
	Compressive sensing		This method always offers high quality decryption, but the decompression is time-consuming; meanwhile, the independence between the compression/decompression and the encryption/decryption leads to time consumption.
Ciphertext compression	Parameter multiplexing compression		This method always suffers from low-quality decrypted results caused by cross-talk noise, but the decompression and decryption are always carried out simultaneously with a pure optical manner. Some preprocessing or postprocessing approaches can be adopted to alleviate the cross-talk noise at the cost of time.
	Classical compression		The independence between the compression/decompression and the encryption/decryption leads to time consumption. The quality of the decryption will seriously degrade in the case of a high compression ratio; however, deep learning provides a new avenue for coping with such issues.
	Compressive sensing		This method enables simultaneously compression and encryption, and it is widely used in cryptosystems based on ghost/single-pixel imaging. This method can always achieve a high compression ratio, but the decryption (decompression) is time-consuming.
Synchronized compression	Iterative phase retrieval algorithm	Iteratively encryption, optically decryption	The encryption procedure is time-consuming, but the decryption (decompression) can always be performed optically. The quality of the decrypted images is relatively high.
		Optically encryption, iteratively decryption	The encryption procedure can always be performed optically, but the decryption (decompression) procedure is time-consuming. The quality of the decrypted images is relatively high.
	Compressive sensing		This method enables simultaneously compression and encryption with a pure optical manner, but the decryption (decompression) procedure is time-consuming.

提到，本课题组利用深度学习提出了一种新的图像压缩加密方案，相比经典的压缩方法 JPEG2000 和 JPEG，实现了大的压缩比。实际上，几乎一切有损压缩的解压缩过程都可以归结为不适定问题，而解决不适定问题正是深度学习相比于传统方法的优势所在，因此深度学习技术为发展新的光学图像压缩加密技术提供了巨大的潜在可能性。此外，超颖表面这种新技术的出现，给参数复用赋予了新的内涵。众所周知，在传统的基于参数复用的光学图像压缩加密技术中[63]，图像间的串扰噪声只能抑制而无法完全去除，这种噪声严重影响解密图像质量。而基于超颖表面的一些参数复用设计方案，则可以从根本上消除这种串扰。以角度复用为例，同一个超颖表面微结构，可以对正入射和 30°斜入射的两束入射光产生不同的相位调制量，而且这两个相位调制量可以通过改变微结构的参数而任意控制，这种特性是传统的衍射光学元件所无法具备的，基于这种特性可以实现无串扰的双图像加密[116]。除了角度复用之外，偏振复用[103]和轨道角动量复用[104]都可以实现无串扰压缩加密。从超颖表面所能实现的奇特的物理性质来看，它仍然是未来光学图像压缩加密值得深入挖掘的研究领域之一。

2）光学图像压缩加密技术的实验研究

目前对于所提出光学图像压缩加密方法，相当一部分只能采用计算机仿真来实现。事实上，有两种主要的因素制约了光学图像压缩加密系统的物理实现。一是光学密码系统对于元件相对位置的敏感性。以双随机相位编码系统为例，Wang 等[117]证实其中一个解密密钥在横向平面内偏移 2 μm 就会导致完全错误的解密结果。尽管目前单个电控精密平移台的定位精度可以达到微米级以及更高，但是以如此精密的单位来

控制两个独立光学元件之间的相对位置仍然较为困难。而且，光学密码系统中相当一部分以级联的多个随机相位板为基础来构建，因此这类系统实验难度极大。需要指出的是，基于光学联合变换相关的光学密码系统的实验报道较多，其原因就在于该系统非常紧凑，密钥和明文位于同一平面，且解密结果对密钥位置不敏感[118-120]。除了相位板的横向错位，在搭建实际光学系统中，相位板的倾斜、相对旋转等多种潜在的误差，也都可能会对实验结果产生严重的影响，这都在一定程度上增加了实验的难度。二是光学元件的性能局限和非理想特性。以 Chen 等[105]提出的光学衍射成像加密系统为例，其加密过程采用光学方法，而解密过程采用相位恢复算法。这意味着，采用数字迭代算法解密时，需要精确掌握相位板对相位的调制函数。然而，无论是采用空间光调制器或者是超颖表面来实现相位调制功能，都难以准确掌握它们的实际相位调制量。同时，解密结果对相位值的误差非常敏感，因而实验难度较大。因此，我们认为，利用光学实验来证实现有的加密系统将是未来光学图像压缩加密技术的研究重点之一。显然，要想实现这个目的，一方面有赖于光学器件相对位置的高精密定位方法的出现（例如实现对两个独立光学元件相对位置的纳米级定位），另一方面则依赖于光学器件制造技术的发展（制造出理论特性与实际特性高度一致的光学器件）。

本文提出了广义的光学图像压缩加密技术的概念，在此基础上，将光学图像压缩加密技术的压缩策略分为三个类型，即明文压缩、密文压缩和明文密文同步压缩。介绍了适用于每种策略的常见压缩方法，并通过阐述这些压缩方法在具体系统中的应用，介绍了光学图像压缩加密技术的研究进展。可以看出，光学图像压缩加密技术的研究进程与光学成像、信号处理、编码理论的发展与进步密切相关，这些领域内新的理论和技术往往会成为推动光学图像压缩加密向前发展的动力。同时也指出，光学图像压缩加密技术的实验验证仍然是该技术面临的一个难点。解决这个问题，有赖于散斑抑制方法、精密定位技术、光电器件制造技术的进步和发展。

参 考 文 献

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

[2] Javidi B, Carnicer A, Yamaguchi M, et al. Roadmap on optical security[J]. Journal of Optics, 2016, 18(8): 083001.

[3] Liu S, Guo C L, Sheridan J T. A review of optical image encryption techniques[J]. Optics & Laser Technology, 2014, 57: 327-342.

[4] Alfalou A, Brosseau C. Optical image compression and encryption methods[J]. Advances in Optics and Photonics, 2009, 1(3): 589-636.

[5] Chen W, Javidi B, Chen X D. Advances in optical security systems[J]. Advances in Optics and Photonics, 2014, 6(2): 120-155.

[6] 吴克难，胡家升，乌旭. 信息安全中的光学加密技术[J]. 激光与光电子学进展，2008，45(7)：30-38.
Wu K N, Hu J S, Wu X. Optical encryption for information security[J]. Laser & Optoelectronics Progress, 2008, 45(7): 30-38.

[7] 彭翔，位恒政，张鹏. 光学信息安全导论[M]. 北京：科学出版社，2008.
Peng X, Wei H Z, Zhang P. Introduction to optical security[M]. Beijing: Science Press, 2008.

[8] 鲍震杰，薛茹. 基于自动编码器的光学图像加密方法[J]. 激光与光电子学进展，2021，58(22)：2210011.
Bao Z J, Xue R. Optical image encryption method based on autoencoder[J]. Laser & Optoelectronics Progress, 2021, 58(22): 2210011.

[9] 陶冶，祝玉鹏，杨栋宇，等. 基于视觉密码的远距离光学信息认证系统[J]. 光学学报，2021，41(16)：1607001.
Tao Y, Zhu Y P, Yang D Y, et al. Remote optical information authentication system based on visual cryptography[J]. Acta Optica Sinica, 2021, 41(16): 1607001.

[10] 王岩，牛宏伟. 基于光学空频域变换的自适应图像分块隐藏技术[J]. 激光与光电子学进展，2021，58(16)：1609001.
Wang Y, Niu H W. Adaptive image block hiding technology based on optical spatial-frequency domain transform[J]. Laser & Optoelectronics Progress, 2021, 58(16): 1609001.

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

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

[13] 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.

[14] 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): 1044-1046.

[15] Liao M H, Zheng S S, Pan S X, et al. Deep-learning-based ciphertext-only attack on optical double random phase encryption[J]. Opto-Electronic Advances, 2021(5): 12-23.

[16] Liu X L, Wu J C, He W Q, et al. Vulnerability to ciphertext-only attack of optical encryption scheme based on double random phase encoding[J]. Optics Express, 2015, 23(15): 18955-18968.

[17] Cheng X C, Cai L Z, Wang Y R, et al. Security enhancement of double-random phase encryption by amplitude modulation[J]. Optics Letters, 2008, 33(14): 1575-1577.

[18] Jiao S M, Zhuang Z Y, Zhou C Y, et al. Security enhancement of double random phase encryption with a

hidden key against ciphertext only attack[J]. Optics Communications, 2018, 418: 106-114.
[19] Nomura T, Javidi B. Optical encryption using a joint transform correlator architecture[J]. Optical Engineering, 2000, 39(8): 2031-2035.
[20] Clemente P, Durán V, Torres-Company V, et al. Optical encryption based on computational ghost imaging [J]. Optics Letters, 2010, 35(14): 2391-2393.
[21] Zhang Y, Wang B. Optical image encryption based on interference[J]. Optics Letters, 2008, 33(21): 2443-2445.
[22] Javidi B, Nomura T. Securing information by use of digital holography[J]. Optics Letters, 2000, 25(1): 28-30.
[23] Shi Y S, Li T, Wang Y L, et al. Optical image encryption via ptychography[J]. Optics Letters, 2013, 38 (9): 1425-1427.
[24] Maniccam S S, Bourbakis N G. Lossless image compression and encryption using SCAN[J]. Pattern Recognition, 2001, 34(6): 1229-1245.
[25] Zhou N R, Zhang A D, 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: 152-160.
[26] Schonberg D, Draper S C, Yeo C, et al. Toward compression of encrypted images and video sequences[J]. IEEE Transactions on Information Forensics and Security, 2008, 3(4): 749-762.
[27] Zhang X P, Ren Y L, Shen L Q, et al. Compressing encrypted images with auxiliary information[J]. IEEE Transactions on Multimedia, 2014, 16(5): 1327-1336.
[28] Situ G H, Zhang J J. Multiple-image encryption by wavelength multiplexing[J]. Optics Letters, 2005, 30 (11): 1306-1308.
[29] Durán V, Clemente P, Torres-Company V, et al. Optical encryption with compressive ghost imaging[C]// 2011 Conference on Lasers and Electro-Optics Europe and 12th European Quantum Electronics Conference, May 22-26, 2011, Munich, Germany. New York: IEEE Press, 2011.
[30] Naughton T J, Javidi B. Compression of encrypted three-dimensional objects using digital holography[J]. Optical Engineering, 2004, 43(10): 2233-2238.
[31] Gerchberg R W. A practical algorithm for the determination of phase from image and diffraction plane pictures[J]. Optik, 1972, 35: 237-246.
[32] Thibault P, Menzel A. Reconstructing state mixtures from diffraction measurements[J]. Nature, 2013, 494 (7435): 68-71.
[33] Georgi P, Wei Q S, Sain B, et al. Optical secret sharing with cascaded metasurface holography[J]. Science Advances, 2021, 7(16): eabf9718.
[34] Li Q, Meng X, Yin Y, et al. A multi-image encryption based on sinusoidal coding frequency multiplexing and deep learning[J]. Sensors, 2021, 21(18): 6178.
[35] 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.
[36] Ahmed N, Natarajan T, Rao K R. Discrete cosine transform[J]. IEEE Transactions on Computers, 1974, C-23(1): 90-93.
[37] Sayood K. Introduction to data compression[M]. San Francisco: Morgan Kaufmann, 2017.
[38] Shechtman Y, Eldar Y C, Cohen O, et al. Phase retrieval with application to optical imaging: a contemporary overview[J]. IEEE Signal Processing Magazine, 2015, 32(3): 87-109.
[39] 杨国桢, 顾本源. 光学系统中振幅和相位的恢复问题[J]. 物理学报, 1981, 30(3): 410-413.
Yang G Z, Gu B Y. On the amplitude-phase retrieval problem in optical systems[J]. Acta Physica Sinica, 1981, 30(3): 410-413.
[40] Candes E J, Wakin M B. An introduction to compressive sampling[J]. IEEE Signal Processing Magazine, 2008, 25 (2): 21-30.
[41] Baraniuk R G. Compressive sensing[J]. IEEE Signal Processing Magazine, 2007, 24(4): 118-121.
[42] Liu Z J, Zhang Y, Zhao H F, et al. Optical multi-image encryption based on frequency shift[J]. Optik, 2011, 122 (11): 1010-1013.
[43] 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.
[44] Alfalou A, Brosseau C. Exploiting root-mean-square time-frequency structure for multiple-image optical compression and encryption[J]. Optics Letters, 2010, 35 (11): 1914-1916.
[45] Alfalou A, Brosseau C, Abdallah N. Simultaneous compression and encryption of color video images[J]. Optics Communications, 2015, 338: 371-379.
[46] Alfalou A, Brosseau C, Abdallah N, et al. Simultaneous fusion, compression, and encryption of multiple images [J]. Optics Express, 2011, 19(24): 24023-24029.
[47] Jridi M, Alfalou A. Real-time and encryption efficiency improvements of simultaneous fusion, compression and encryption method based on chaotic generators[J]. Optics and Lasers in Engineering, 2018, 102: 59-69.
[48] Qin Y, Gong Q, Wang Z P, et al. Optical multiple-image encryption in diffractive-imaging-based scheme using spectral fusion and nonlinear operation[J]. Optics Express, 2016, 24(23): 26877-26886.
[49] Ngo N Q. Optical chirp z-transform processor: design and application[J]. Journal of Lightwave Technology, 2015, 33(11): 2213-2221.
[50] Mosso E, Bolognini N. Dynamic multiple-image encryption based on chirp z-transform[J]. Journal of Optics, 2019, 21 (3): 035704.
[51] Mosso E, Suárez O, Bolognini N. Asymmetric multiple-image encryption system based on a chirp z-transform[J]. Applied Optics, 2019, 58(21): 5674-5680.
[52] Wu J J, Li S W. Optical multiple-image compression-encryption via single-pixel Radon transform[J]. Applied Optics, 2020, 59(31): 9744-9754.
[53] Qin W, Peng X. Asymmetric cryptosystem based on phase-truncated Fourier transforms[J]. Optics Letters,

2010, 35(2): 118-120.
[54] Zhang L H, Wang Y, Zhang D W. Research on multiple-image encryption mechanism based on Radon transform and ghost imaging[J]. Optics Communications, 2022, 504: 127494.
[55] Lu P, Xu Z Y, Lu X, et al. Digital image information encryption based on compressive sensing and double random-phase encoding technique[J]. Optik, 2013, 124(16): 2514-2518.
[56] Liu X Y, Cao Y P, Lu P, et al. Optical image encryption technique based on compressed sensing and Arnold transformation[J]. Optik, 2013, 124(24): 6590-6593.
[57] Wang J, Wang Q H, Hu Y H. Image encryption using compressive sensing and detour cylindrical diffraction[J]. IEEE Photonics Journal, 2018, 10(3): 7801014.
[58] Deepan B, Quan C, Wang Y, et al. Multiple-image encryption by space multiplexing based on compressive sensing and the double-random phase-encoding technique [J]. Applied Optics, 2014, 53(20): 4539-4547.
[59] Zhou N R, Li H L, Wang D, et al. Image compression and encryption scheme based on 2D compressive sensing and fractional Mellin transform[J]. Optics Communications, 2015, 343: 10-21.
[60] Yi J W, Tan G Z. Optical compression and encryption system combining multiple measurement matrices with fractional Fourier transform[J]. Applied Optics, 2015, 54(36): 10650-10658.
[61] Yang X L, Wu H Z, Yin Y K, et al. Multiple-image encryption base on compressed coded aperture imaging [J]. Optics and Lasers in Engineering, 2020, 127: 105976.
[62] Ni R J, Wang F, Wang J, et al. Multi-image encryption based on compressed sensing and deep learning in optical gyrator domain[J]. IEEE Photonics Journal, 2021, 13(3): 7800116.
[63] Situ G, Zhang J. Position multiplexing for multiple-image encryption[J]. Journal of Optics A: Pure and Applied Optics, 2006, 8(5): 391-397.
[64] Amaya D, Tebaldi M, Torroba R, 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.
[65] Amaya D, Tebaldi M, Torroba R, et al. Wavelength multiplexing encryption using joint transform correlator architecture[J]. Applied Optics, 2009, 48(11): 2099-2104.
[66] Qin Y, Gong Q. Interference-based multiple-image encryption with silhouette removal by position multiplexing[J]. Applied Optics, 2013, 52(17): 3987-3992.
[67] Xiao Y L, Su X Y, Li S K, et al. Key rotation multiplexing for multiple-image optical encryption in the Fresnel domain[J]. Optics & Laser Technology, 2011, 43(4): 889-894.
[68] Rueda E, Ramírez J F B, Henao R H, et al. Lateral shift multiplexing with a modified random mask in a joint transform correlator encrypting architecture[J]. Optical Engineering, 2009, 48(2): 027006.
[69] 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.
[70] Shi Y Y, Liu Y W, Sheng W, et al. Multiple-image double-encryption via 2D rotations of a random phase mask with spatially incoherent illumination[J]. Optics Express, 2019, 27(18): 26050-26059.
[71] Mosso F, Barrera J F, Tebaldi M, et al. All-optical encrypted movie[J]. Optics Express, 2011, 19(6): 5706-5712.
[72] He W Q, Peng X, Meng X F. Optical multiple-image hiding based on interference and grating modulation[J]. Journal of Optics, 2012, 14(7): 075401.
[73] Qin Y, Wang Z P, Pan Q N, et al. Optical color-image encryption in the diffractive-imaging scheme[J]. Optics and Lasers in Engineering, 2016, 77: 191-202.
[74] Shen X J, Lin C, Kong D Z. Fresnel-transform holographic encryption based on angular multiplexing and random-amplitude mask[J]. Optical Engineering, 2012, 51(6): 068201.
[75] 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.
[76] Li W, Chang X Y, Yan A M, et al. Asymmetric multiple image elliptic curve cryptography[J]. Optics and Lasers in Engineering, 2021, 136: 106319.
[77] LeCun Y, Bengio Y, Hinton G. Deep learning[J]. Nature, 2015, 521(7553): 436-444.
[78] Lucas A, Iliadis M, Molina R, et al. Using deep neural networks for inverse problems in imaging: beyond analytical methods[J]. IEEE Signal Processing Magazine, 2018, 35(1): 20-36.
[79] Dong C, Deng Y B, Loy C C, et al. Compression artifacts reduction by a deep convolutional network[C]// 2015 IEEE International Conference on Computer Vision, December 7-13, 2015, Santiago, Chile. New York: IEEE Press, 2015: 576-584.
[80] Jiao S M, Jin Z, Chang C L, et al. Compression of phase-only holograms with JPEG standard and deep learning[J]. Applied Sciences, 2018, 8(8): 1258.
[81] Shimobaba T, Blinder D, Makowski M, et al. Dynamic-range compression scheme for digital hologram using a deep neural network[J]. Optics Letters, 2019, 44(12): 3038-3041.
[82] Qin Y, Wan Y H, Wan S J, et al. Optical compressive encryption via deep learning[J]. IEEE Photonics Journal, 2021, 13(4): 7800208.
[83] Yuan S, Yang Y R, Liu X M, et al. Optical image transformation and encryption by phase-retrieval-based double random-phase encoding and compressive ghost imaging[J]. Optics and Lasers in Engineering, 2018, 100: 105-110.
[84] Zhu J N, Yang X L, Meng X F, et al. Optical image encryption scheme with multiple light paths based on compressive ghost imaging[J]. Journal of Modern Optics,

2018, 65(3): 306-313.
[85] Zhang C G, Han B N, He W Q, et al. A novel compressive optical encryption via single-pixel imaging [J]. IEEE Photonics Journal, 2019, 11(4): 7801208.
[86] Zhao S M, Wang L, Liang W Q, et al. High performance optical encryption based on computational ghost imaging with QR code and compressive sensing technique[J]. Optics Communications, 2015, 353: 90-95.
[87] Zhang L H, Pan Z L, Wu L Y, et al. High-performance compression and double cryptography based on compressive ghost imaging with the fast Fourier transform [J]. Optics and Lasers in Engineering, 2016, 86: 329-337.
[88] 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.
[89] 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.
[90] Li J, Li J S, Pan Y Y, et al. Compressive optical image encryption[J]. Scientific Reports, 2015, 5: 10374.
[91] Li J, Jia B, Dai X, et al. Compressive optical image encryption using phase-shifting interferometry on a joint transform correlator[J]. Optica Applicata, 2017, 47(2): 245-256.
[92] Li J, Li H B, Li J S, et al. Compressive optical image encryption with two-step-only quadrature phase-shifting digital holography[J]. Optics Communications, 2015, 344: 166-171.
[93] Chen W, Chen X D. Optical multiple-image encryption based on multiplane phase retrieval and interference[J]. Journal of Optics, 2011, 13(11): 115401.
[94] Chen W. Optical multiple-image encryption using three-dimensional space[J]. IEEE Photonics Journal, 2016, 8 (2): 6900608.
[95] Lü W J, Sun X K, Yang D Y, et al. Optical multiple information hiding via azimuth multiplexing[J]. Optics and Lasers in Engineering, 2021, 141: 106574.
[96] Lu Z, Lü W J, Zhu Y P, et al. Optical information encryption based on partially-update iterative system with azimuth multiplexing[J]. Optics Communications, 2022, 510: 127899.
[97] Wu J J, Wang J C, Nie Y G, et al. Multiple-image optical encryption based on phase retrieval algorithm and fractional Talbot effect[J]. Optics Express, 2019, 27(24): 35096-35107.
[98] 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.
[99] Huang J J, Hwang H E, Chen C Y, et al. Lensless multiple-image optical encryption based on improved phase retrieval algorithm[J]. Applied Optics, 2012, 51 (13): 2388-2394.
[100] Liu Z J, Liu S T. Double image encryption based on iterative fractional Fourier transform[J]. Optics Communications, 2007, 275(2): 324-329.
[101] 李天佑, 黄玲玲, 王涌天. 超颖表面原理与研究进展[J]. 中国光学, 2017, 10(5): 523-540, 701.
Li T Y, Huang L L, Wang Y T. The principle and research progress of metasurfaces[J]. Chinese Optics, 2017, 10(5): 523-540, 701.
[102] Zheng G X, Mühlenbernd H, Kenney M, et al. Metasurface holograms reaching 80% efficiency[J]. Nature Nanotechnology, 2015, 10(4): 308-312.
[103] Zhao R Z, Sain B, Wei Q S, et al. Multichannel vectorial holographic display and encryption[J]. Light: Science & Applications, 2018, 7: 95.
[104] Zhou H Q, Sain B, Wang Y T, et al. Polarization-encrypted orbital angular momentum multiplexed metasurface holography[J]. ACS Nano, 2020, 14(5): 5553-5559.
[105] Chen W, Chen X D, Sheppard C J R. Optical image encryption based on diffractive imaging[J]. Optics Letters, 2010, 35(22): 3817-3819.
[106] Chen W, Chen X D, Anand A, et al. Optical encryption using multiple intensity samplings in the axial domain[J]. Journal of the Optical Society of America. A, Optics, Image Science, and Vision, 2013, 30(5): 806-812.
[107] Qin Y, Gong Q, Wang Z P. Simplified optical image encryption approach using single diffraction pattern in diffractive-imaging-based scheme[J]. Optics Express, 2014, 22(18): 21790-21799.
[108] Bao P, Zhang F C, Pedrini G, et al. Phase retrieval using multiple illumination wavelengths[J]. Optics Letters, 2008, 33(4): 309-311.
[109] Batey D J, Claus D, Rodenburg J M. Information multiplexing in ptychography[J]. Ultramicroscopy, 2014, 138: 13-21.
[110] He X L, Jiang Z L, Kong Y, et al. Optical multi-image encryption based on focal length multiplexing and multimode phase retrieval[J]. Applied Optics, 2020, 59 (26): 7801-7812.
[111] He X L, Tao H, Liu C, et al. Single-shot color image encryption based on mixed state diffractive imaging[J]. Optics and Lasers in Engineering, 2018, 107: 112-118.
[112] He X L, Tao H, Jiang Z L, et al. Single-shot optical multiple-image encryption by jointly using wavelength multiplexing and position multiplexing[J]. Applied Optics, 2019, 59(1): 9-15.
[113] Di H, Zheng K F, Zhang X, et al. Multiple-image encryption by compressive holography[J]. Applied Optics, 2012, 51(7): 1000-1009.
[114] Wan Y H, Wu F, Yang J H, et al. Multiple-image encryption based on compressive holography using a multiple-beam interferometer[J]. Optics Communications, 2015, 342: 95-101.
[115] Zhang Y S, Zhang L Y. Exploiting random convolution and random subsampling for image encryption and compression[J]. Electronics Letters, 2015, 51(20): 1572-1574.
[116] Kamali S M, Arbabi E, Arbabi A, et al. Angle-multiplexed metasurfaces: encoding independent wavefronts in a single metasurface under different illumination angles

[J]. Physical Review X, 2017, 7(4): 041056.

[117] Wang B, Sun C C, Su W C, et al. Shift-tolerance property of an optical double-random phase-encoding encryption system[J]. Applied Optics, 2000, 39(26): 4788-4793.

[118] 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.

[119] Barrera J F, Tebaldi M, Ríos C, et al. Experimental multiplexing of encrypted movies using a JTC architecture [J]. Optics Express, 2012, 20(4): 3388-3393.

[120] Dou S F, Shen X J, Zhou B, et al. Experimental research on optical image encryption system based on joint Fresnel transform correlator[J]. Optics & Laser Technology, 2019, 112: 56-64.