激光与光电子学进展 先进成像

# 基于指纹密钥的光学双图像加密

李天论[1]，徐文君[2]，苏永钢[1*]，刘帅奇[1]，赵杰[1]
[1]河北大学电子信息工程学院，河北 保定 071000；
[2]河北农业大学理学院，河北 保定 071001

**摘要** 为了提高图像的加密效率和安全性，提出一种基于指纹密钥的光学双图像加密方法。首先，两幅待加密图像分别经置于输入平面和Gyrator变换域平面的两块指纹随机相位板的调制后，再经1次Gyrator变换，然后将Gyrator变换后的结果合成为一幅复振幅图像。最后，对得到的复振幅图像进行相位截断和振幅截断操作，得到加密图像和两个相位密钥。解密时，指纹、振幅截断得到的相位密钥、混沌系统的初值和控制参数、Gyrator变换参数均可作为解密过程中的密钥。在所提方法中，由于密钥与用户身份关联，加密系统的安全性得以进一步提高。此外，由于无需传输相位板密钥，密钥管理更为便捷。数值模拟结果表明，所提加密方法切实可行，具有较高的安全性和鲁棒性。

**关键词** 双图像加密；指纹密钥；Gyrator变换；随机相位编码；混沌映射
**中图分类号** O438；TN918 **文献标志码** A **DOI**：10.3788/LOP220758

# Optical Double-Image Encryption Based on Fingerprint Key

Li Tianlun[1], Xu Wenjun[2], Su Yonggang[1*], Liu Shuaiqi[1], Zhao Jie[1]
[1]*College of Electronic and Information Engineering, Hebei University, Baoding* 071000, *Hebei, China*;
[2]*College of Science, Hebei Agricultural University, Baoding* 071001, *Hebei, China*

**Abstract** To improve the encryption efficiency and security of images, this study proposes an optical double-image encryption method based on fingerprint keys. First, two grayscale images to be encrypted are modulated by two fingerprint-based random-phase masks, one placed at the input plane, the other at the Gyrator transform plane. The modulated results are then Gyrator transformed and combined into a complex-valued image. Subsequently, the encrypted image and two phase keys are obtained via phase-amplitude truncation on the complex-valued image. During the decryption process, the decryption key can be any of the following: the fingerprint, either phase key obtained by amplitude truncation, initial values and control parameters of the chaotic map, or parameters of the Gyrator transform. In the proposed encryption method, the secret key is associated with user identity, thereby enhancing system security. It also allows more convenient management of the secret keys because the phase-mask keys do not need to be transmitted over the network. Numerical simulations indicate the feasibility of the proposed encryption method and its high security and robustness against various attacks.

**Key words** double-image encryption; fingerprint key; Gyrator transform; random phase encoding; chaotic mapping

## 1 引 言

图像因具有直观、生动形象及包含的信息量大等特点，目前已成为人类社会生活中常用的信息载体之一。随着计算机科学和现代通讯技术的迅速发展，图像在传递过程中易被非法拷贝、窃取等，如何保护图像的信息安全已成为军事通讯、医疗、金融等诸多领域关注的焦点，也是当今各国科研人员研究的热点和难点之一。作为保护图像信息安全的主要手段之一，基于光学理论的图像加密及隐藏技术以独特的优势，如高并行度、高速度、多维度和大容量等，引起了国内外众多科研人员的重视，并相继投入到这一领域的研究中[1-4]。

1995年，美国康涅狄格大学Javidi教授课题组[5]提出的基于傅里叶变换域的双随机相位编码方法开启了采用光学信息处理技术进行图像加密的新篇章。在该

**收稿日期**：2022-02-17；**修回日期**：2022-02-28；**录用日期**：2022-03-14；**网络首发日期**：2022-03-24
**基金项目**：河北省自然科学基金(F2019201151)、河北大学高层次人才科研启动经费项目(521000981370)
**通信作者**：*ygsu0726@163.com

方法中，两块相互独立的随机相位板被分别置于空间域和傅里叶变换域，待加密图像经两块随机相位板调制后被加密成一幅平稳白噪声图像。解密时，若这两个随机相位板密钥错误，则难以将原图像的有效信息恢复出来。之后，印度理工学院 Singh 教授课题组[6]通过将第二块随机相位板置于一般的分数域，成功地将双随机相位编码方法拓展到分数傅里叶变换域。中国科学院司徒国海和张静娟教授课题组[7]则将双随机相位编码方法拓展到菲涅耳变换域，通过引入波长和菲涅耳衍射距离密钥，加密系统的安全性得以进一步提高。类似地，哈尔滨工业大学刘正君和刘树田教授课题组[8]则将双随机相位编码方法拓展到 Gyrator 变换域。印度学者 Unnikrishnan 等[9]把双随机相位编码方法拓展到线性正则变换域。但是上述大都是单幅图像加密方案，为此，国内外学者又研究了多图像加密技术以提高传输效率。陈翼翔等[10]提出了一种基于双随机相位编码的非线性双图像加密方法，该方法利用双随机相位编码技术和傅里叶变换对两幅待加密图像复合的复振幅图像进行加密，提高了加密效率，但是存在轮廓显现问题，安全性较低。Rajput 等[11]利用分数阶傅里叶变换加密其中一幅图像，同时利用改进的 Gerchberg-Saxton（G-S）相位检索技术将加密图像转变为纯相位图像，最后将其作为另一幅图像的加密密钥，完成双图像加密。实验结果验证了其算法的有效性与安全性，但是 G-S 相位检索技术大幅增加了复杂度，降低了加密效率。此外，一些基于数字全息、计算全息、光学干涉理论、相位恢复算法、集成成像、鬼成像、空域叠层成像、傅里叶叠层成像的新型光学图像加密方法也相继被提出，进一步促进了光学图像加密领域的研究进展[12-21]。

然而，上述大多数光学图像加密方法中密钥与用户之间缺乏必要的联系，以致系统无法区分密钥使用者是合法用户还是恶意攻击者，影响系统的安全性。人体生物特征（包括生理特征和行为特征）由于具有广泛性、稳定性和唯一性，常被用于实现个人身份认证和鉴别。近年来，也有将人体生理特征和行为特征引入光学系统进行图像加密的研究报道。日本东京工业大学 Tashima 等[22]利用指纹特征和双随机相位编码构造了一种二值图像加密方法。哈尔滨工业大学冉启文教授课题组[23]利用指纹特征、相位恢复算法和 RSA 公钥算法构造了一种灰度图像加密方法。上海师范大学 Yan 等[24]利用指纹密钥和光学外差技术设计了一种三维物体加密系统。山东大学 Zhu 等[25]利用数字全息技术和指纹特征生成相位板密钥，并提出了一种基于指纹相位板密钥和计算鬼成像技术的二值图像加密方法。深圳大学彭翔教授课题组[26]利用由数字全息技术生成的指纹密钥、相位恢复算法和相位截断傅里叶变换，构造了一种光学非对称图像加密方法。印度理工学院 Verma 等[27]还提出了一种基于人脸随机相位密钥和相位截断傅里叶变换的灰度图像加密方法。天津大学 Tao 等[28]则提出了一种基于掌纹随机相位密钥和奇异值分解的非对称图像加密方法。本课题组[29-33]也在利用人体生物特征实现光学图像加密研究方面进行了有益尝试，分别利用指纹随机相位密钥和语音随机相位密钥，并结合散斑图样照明傅里叶叠层成像、相移数字全息等光学理论与技术，实现了灰度图像和彩色图像的光学加密。

然而，当前基于人体生物特征密钥的光学图像加密方法大都是针对单一图像设计的，随着互联网通信技术和大数据技术的快速发展，由于单图像加密系统的加密容量有限，因此难以满足人们日益增长的信息需求。为了提高加密效率，本文提出了一种基于指纹随机相位密钥的光学双图像加密方法。所提方法利用人体生物特征实现了双图像的光学加密，利用人体指纹特征构造随机相位板密钥，将光学密钥与身份认证相结合，进一步提高了加密系统的安全性。此外，所提方法通过相位截断和振幅截断在解密过程中引入两个额外的相位密钥，使加密系统不再是普通的对称加密；引入的两个相位密钥使加密系统的密钥空间得以进一步增大，从而提高了加密系统的安全性。最后，所提方法中随机相位板密钥无需通过网络传输，一方面避免了传输过程中密钥泄露的风险，另一方面也使得密钥管理更为便捷。

## 2 双图像加密方法

### 2.1 指纹随机相位板构造

指纹随机相位板的构造主要包括以下步骤。

1）利用安全哈希算法 SHA-256 计算得到指纹图像的哈希值 $H$：

$$H=\left[h_1,h_2,\cdots,h_{64}\right]。\tag{1}$$

2）利用 $H$ 序列的一些元素，生成 Lozi 混沌映射[33]的初值 $x$ 和 $y$：

$$\begin{cases}x=x_0+\mathrm{hex2dec}\left[H\left(h_i:h_{j+7}\right)\right]\times10^{-16}\\ y=y_0+\mathrm{hex2dec}\left[H\left(h_i:h_{j+7}\right)\right]\times10^{-16}\end{cases},\tag{2}$$

式中：$i$ 和 $j$ 分别是 $[1,57]$ 之间的正整数；$x_0$ 和 $y_0$ 分别为 Lozi 混沌映射的原始初值；hex2dec(·)为将十六进制数转换成十进制数的函数。

3）假设要构造的指纹随机相位板的大小是 $M\times N$，将以 $x$ 和 $y$ 为初值的 Lozi 混沌映射迭代 $(M\times N)/2$ 次，得到两个随机序列：

$$\begin{cases}X=\left\{x_1,x_2,\cdots,x_{(M\times N)/2}\right\}\\ Y=\left\{y_1,y_2,\cdots,y_{(M\times N)/2}\right\}\end{cases}。\tag{3}$$

4）将随机序列 $X$ 和 $Y$ 组合成新的随机序列 $Z$：

$$Z=\left\{x_1,x_2,\cdots,x_{(M\times N)/2};y_1,y_2,\cdots,y_{(M\times N)/2}\right\}。\tag{4}$$

5）将随机序列 $Z$ 转换成大小为 $M\times N$ 的二维随

机矩阵：

$$\boldsymbol{M}_{\mathrm{R}}=\mathrm{reshape}(Z,M,N),\tag{5}$$

式中：reshape(·)为矩阵调整函数。

6)最后将二维随机矩阵$\boldsymbol{M}_{\mathrm{R}}$编码为纯相位形式：

$$\boldsymbol{M}_{\mathrm{FRP}}=\exp(\mathrm{i}\cdot 2\pi\cdot\boldsymbol{M}_{\mathrm{R}}),\tag{6}$$

式中：$\boldsymbol{M}_{\mathrm{FRP}}$就是构造的指纹随机相位板。通过调整式(2)中的$i$和$j$，并重复步骤3)～6)，即可构造出一系列指纹随机相位板。

## 2.2　加密过程

图1所示的加密过程主要包括以下步骤。其中$I_1$和$I_2$分别表示原图像“Lena”和“Peppers”，$\boldsymbol{M}_{\mathrm{FRP1}}$和$\boldsymbol{M}_{\mathrm{FRP2}}$表示两个指纹随机相位板，$G_1$和$G_2$表示两次Gyrator变换，$P_1$和$P_2$表示两个相位密钥，AT表示振幅截断操作，PT表示相位截断操作，IE表示加密图像。

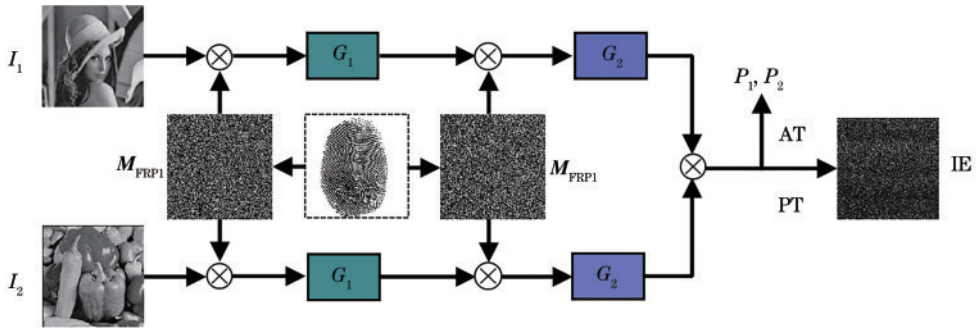


图1　加密过程示意图

Fig. 1　Schematic of the encryption process

1) 灰度图像$I_1$和$I_2$分别被指纹随机相位板调制后进行一次Gyrator变换，得到$I_1'$和$I_2'$：

$$I_k'=G_1(I_k\cdot\boldsymbol{M}_{\mathrm{FRP1}}),\tag{7}$$

式中：$k=1,2$。

2) $I_1'$和$I_2'$分别被指纹随机相位板调制后再进行一次Gyrator变换，得到$I_1''$和$I_2''$：

$$I_k''=G_2(I_k'\cdot\boldsymbol{M}_{\mathrm{FRP2}}).\tag{8}$$

3) 将$I_1''$和$I_2''$合并，然后进行振幅-相位截断，得到相位部分$I_{\mathrm{EP}}$和加密图像$I_{\mathrm{E}}$：

$$\begin{cases}I_3=I_1''\cdot I_2''\\ I_{\mathrm{EP}}=\mathrm{AT}(I_3),\\ I_{\mathrm{E}}=\mathrm{PT}(I_3)\end{cases}\tag{9}$$

式中：AT(·)和PT(·)分别表示振幅截断操作和相位截断操作。

4) 最后由相位部分$I_{\mathrm{EP}}$生成相位密钥$P_1$和$P_2$：

$$\begin{cases}P_1=I_{\mathrm{EP}}/I_2''\\ P_2=I_{\mathrm{EP}}/I_1''\end{cases}.\tag{10}$$

## 2.3　解密过程

图2所示的解密过程主要包括以下步骤，其中$\mathrm{ID}_1$和$\mathrm{ID}_2$分别表示解密得到的“Lena”和“Peppers”。

1) 利用相位密钥$P_2$和$P_1$，由加密图像得到$I_{\mathrm{D1}}''$和$I_{\mathrm{D2}}''$：

$$\begin{cases}I_{\mathrm{D1}}''=I_{\mathrm{E}}\cdot P_2\\ I_{\mathrm{D2}}''=I_{\mathrm{E}}\cdot P_1\end{cases}.\tag{11}$$

2) 对$I_{\mathrm{D1}}''$和$I_{\mathrm{D2}}''$分别施以$G_2$的逆变换($I_{G_2}$)，然后再与随机相位板$\boldsymbol{M}_{\mathrm{FRP2}}$的复共轭相乘，得到$I_{\mathrm{D1}}'$和$I_{\mathrm{D2}}'$：

$$I_{\mathrm{D}k}'=I_{G_2}(I_{\mathrm{D}k}'')\cdot\boldsymbol{M}_{\mathrm{FRP2}}^{*}.\tag{12}$$

3) 对$I_{\mathrm{D1}}'$和$I_{\mathrm{D2}}'$分别施以$G_1$的逆变换($I_{G_1}$)，然后再与随机相位板$\boldsymbol{M}_{\mathrm{FRP1}}$的复共轭相乘，得到解密图像$I_{\mathrm{D1}}$和$I_{\mathrm{D2}}$：

$$I_{\mathrm{D}k}=I_{G_1}(I_k')\cdot\boldsymbol{M}_{\mathrm{FRP1}}^{*}.\tag{13}$$

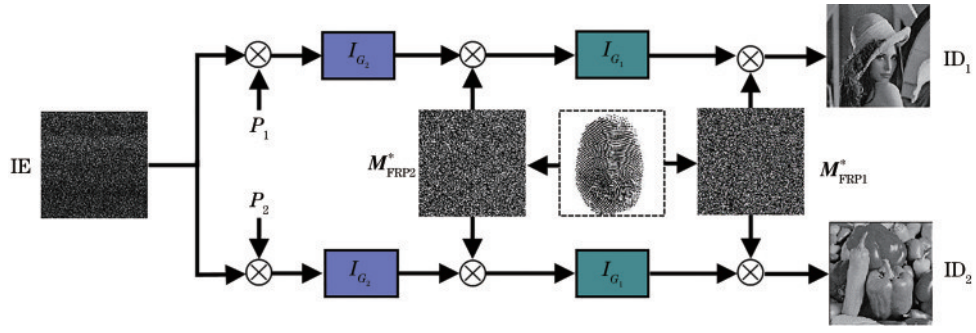


图2　解密过程示意图

Fig. 2　Schematic of the decryption process

## 3　计算机模拟结果与分析

为了验证所提方法的可行性、安全性和鲁棒性，利用 Matlab 2020b 进行数值模拟实验。在模拟实验中，Lozi 混沌映射的原始初值、控制参数分别设置为 $x_0=0.34$ 和 $y_0=0$、$a_0=1.75$ 和 $b_0=0.33$；两次 Gyrator 变换的参数分别设置为 $\alpha_1=0.5$，$\alpha_2=0.6$。用于测试的两幅灰度图像（其大小均为 256×256 个像素）分别如图 3(a)和图 3(b)所示；用于加密的指纹如图 3(c)所示；利用指纹构造的其中一块随机相位板如图 3(d)所示；由相位部分 $I_{EP}$ 生成的其中一个相位密钥如图 3(e)所示。采用所提方法对图 3(a)和图 3(b)所示的两幅灰度图像进行加密得到的结果如图 3(f)所示。由图 3(f)可以看出，两幅灰度图像的信息被成功隐藏到一幅类噪声图像中。当利用正确密钥对图 3(f)所示的加密图像进行解密时，得到的解密结果如图 3(g)和图 3(h)所示。由图 3(g)和图 3(h)可以看出，当密钥完全正确时可以从加密图像中将两幅原图像很好地解密出来。解密图像与原图像之间的相似性可由相关系数（CC）来定量评价，相关系数的定义为

$$C=\frac{E\left\{\left[I_{\mathrm{O}}-E(I)\right]\left[I_{\mathrm{D}}-E(I_{\mathrm{D}})\right]\right\}}{\left\{E\left\{\left[I_{\mathrm{O}}-E(I)\right]^2\right\}E\left\{\left[I_{\mathrm{D}}-E(I_{\mathrm{D}})\right]^2\right\}\right\}^{1/2}},\tag{14}$$

式中：$E\{\cdot\}$ 表示期望算符；$I_{\mathrm{O}}$ 和 $I_{\mathrm{D}}$ 分别表示原图像与解密图像。CC 值越大（最大值为 1），说明解密图像与原图像之间的差别越小。通过计算，两幅解密图像与各自对应的原图像之间的 CC 值均为 1，说明当密钥完全正确时，两幅原图像均可从加密图像中被无损地恢复出来。

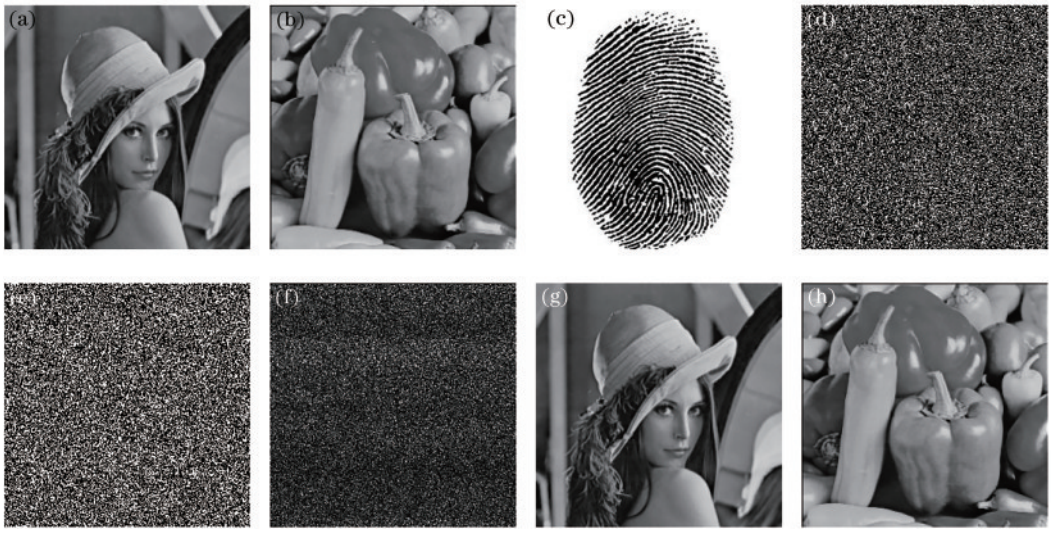


图 3　两张原图像和其加解密结果。(a) (b)原始图像 Lena 和 Peppers；(c)指纹图像；(d) $\boldsymbol{M}_{\mathrm{FRP1}}$；(e)相位密钥 $P_1$；(f)加密图像；(g) (h)正确密钥得到的解密图像 Lena 和 Peppers

Fig. 3　Two original images and their encryption and decryption results. (a) (b) Original images Lena and Peppers; (c) fingerprint; (d) $\boldsymbol{M}_{\mathrm{FRP1}}$; (e) phase key $P_1$; (f) encrypted image; (g) (h) decrypted images Lena and Peppers obtained by correct keys

### 3.1　加密效果分析

峰值信噪比（PSNR）是一种衡量图像质量的指标，其值越高，就证明图像间的差距越小。峰值信噪比的定义为

$$E_{\mathrm{MSE}}=\frac{1}{T}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}\left\|I_{\mathrm{O}}(i,j)-I_{\mathrm{E}}(i,j)\right\|^2,\tag{15}$$

$$P_{\mathrm{SNR}}=10\cdot\lg\frac{M_{\mathrm{I}}^2}{E_{\mathrm{MSE}}},\tag{16}$$

式中：$T$ 是灰度图像像素个数；$I_{\mathrm{O}}(i,j)$ 和 $I_{\mathrm{E}}(i,j)$ 分别是原图像和密文图像的像素值；$M_{\mathrm{I}}$ 是密文图像上最大的像素值。表 1 给出了所提方法、文献[34]中的方法、文献[28]中的方法得到的三组共 6 幅原图像和密文图像的 PSNR。由表 1 可以看出，所提方法得到的密文图像与原图像差距更大，加密效果更好。

表 1　密文图像与原图像的峰值信噪比

Table 1　PSNR of ciphertext images and original images

| Method | Lena | Peppers | Cameraman | Einstein | Elaine | Fiore |
|---|---|---|---|---|---|---|
| Method in Ref. [34] | 11.4391 | 10.8246 | 10.2781 | 11.7649 | 8.7428 | 13.5697 |
| Method in Ref. [28] | 9.4884 | 8.5878 | 8.0731 | 9.8262 | 6.8562 | 12.7532 |
| Proposed method | 8.1579 | 7.0187 | 6.4063 | 8.0492 | 5.7965 | 11.5553 |

### 3.2　解密效果分析

结构相似性(SSIM)是一种衡量图像相似度的指标，其值越高，说明图像结构越相似。结构相似性的定义为

$$S_{\mathrm{SIM}}=\left(\frac{2\mu_x\mu_y+C_1}{\mu_x^2\mu_y^2+C_1}\right)^{\alpha}\times\left(\frac{2\sigma_x\sigma_y+C_2}{\sigma_x^2\sigma_y^2+C_2}\right)^{\beta}\times\left(\frac{\sigma_{xy}+C_3}{\sigma_x\sigma_y+C_3}\right)^{\gamma},\tag{17}$$

式中：$\mu_x$、$\mu_y$、$\sigma_x$、$\sigma_y$和$\sigma_{xy}$分别是图像$x$和$y$的局部均值、标准差和互协方差；$\alpha$、$\beta$和$\gamma$是三个大于0的参数；$C_1$、$C_2$和$C_3$是三个常数。表2给出了所提方法、文献[34]中的方法、文献[28]中的方法得到的三组共6幅原图像和解密图像的SSIM。由表2可以看出，所提方法得到的解密图像与原图像更为相似，解密效果更好。

表2　原图像与解密图像的结构相似性

Table 2　SSIM of original images and decrypted images

| Method | Lena | Peppers | Cameraman | Einstein | Elaine | Fiore |
|---|---|---|---|---|---|---|
| Method in Ref. [34] | 0.9568 | 0.9572 | 0.9685 | 0.9692 | 0.9534 | 0.9596 |
| Method in Ref. [28] | 0.9821 | 0.9853 | 0.9967 | 0.9982 | 0.9986 | 0.9979 |
| Proposed method | 0.9987 | 0.9979 | 0.9994 | 0.9991 | 0.9983 | 0.9979 |

### 3.3　密钥敏感性分析

所提图像加密方法中，指纹、混沌参数、GT参数、两个相位密钥都可作为解密密钥。图4和图5分别为某一密钥错误而其他密钥完全正确时得到的解密图像“Lena”和“Peppers”。其中，图4(b)和图5(b)分别为利用如图4(a)和图5(a)所示的错误指纹解密得到的“Lena”和“Peppers”；图4(c)～(f)和图5(c)～(f)分别为利用错误混沌参数解密得到的“Lena”和“Peppers”；图4(g)～(h)和图5(g)～(h)分别为利用错误的GT参数解密得到的“Lena”和“Peppers”；而图4(i)和图5(i)分别为利用错误的相位密钥解密得到的“Lena”和“Peppers”。图4(b)～(i)与图3(a)之间的CC值分别是0.0316、0.0346、0.0264、0.0267、0.0308、0.0234、0.0626、0.0586；图5(b)～(i)和图3(b)之间的CC值分别是0.0679、0.0621、0.0624、0.0613、0.0640、0.0597、0.0973、0.0902。结果表明，只要有一个密钥错误(即使其他密钥完全正确)，就不能解密出原图像的任何有效信息。

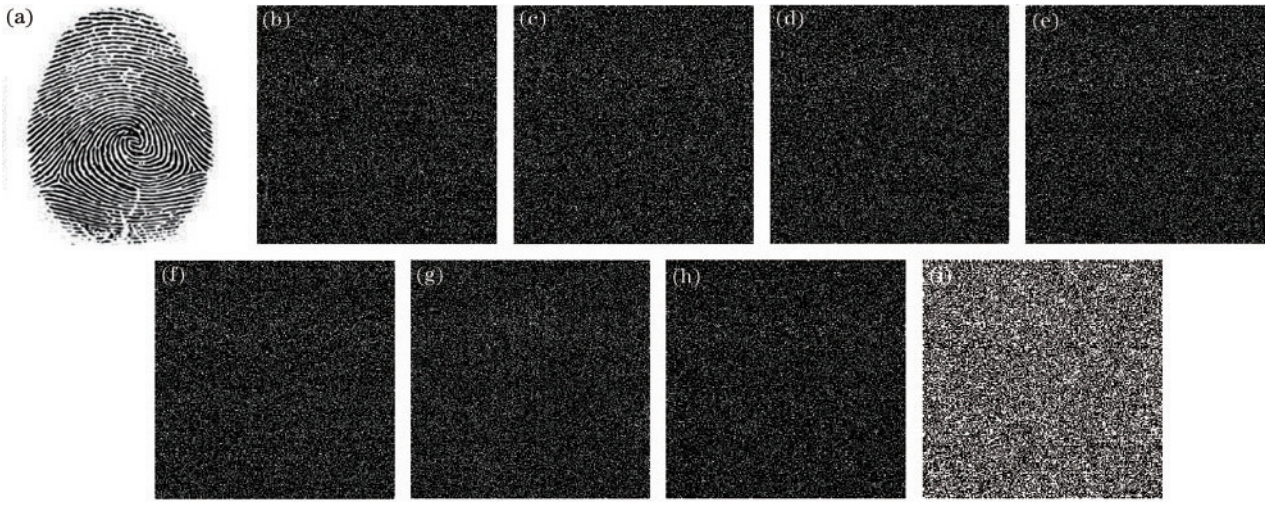


图4　使用错误密钥得到的解密图像Lena。(a)错误指纹；(b)由错误指纹得到的解密图像；(c)～(f)由错误混沌参数$a_0'=1.75+10^{-15}$，$b_0'=0.33+10^{-15}$，$x_0'=0.34+10^{-15}$，$y_0'=10^{-15}$得到的解密图像；(g)～(h)由错误Gyrator参数$\alpha_1'=0.5+10^{-2}$，$\alpha_2'=0.6+9\times10^{-3}$得到的解密图像；(i)由错误相位密钥$P_1$得到的解密图像

Fig. 4　Decrypted results of image Lena with incorrect keys. (a) Incorrect fingerprint; (b) decrypted result with the incorrect fingerprint; (c)-(f) decrypted results with the incorrect parameters of the chaotic map $a_0'=1.75+10^{-15}$, $b_0'=0.33+10^{-15}$, $x_0'=0.34+10^{-15}$, $y_0'=10^{-15}$; (g)-(h) decrypted results with the incorrect parameter of the Gyrator transform $\alpha_1'=0.5+10^{-2}$, $\alpha_2'=0.6+9\times10^{-3}$; (i) decrypted result with the incorrect phase key $P_1$

### 3.4　统计分析攻击

为了验证所提方法抵抗统计分析攻击的能力，进行直方图分析和相邻像素间的相关性分析。图6为两幅原图像和加密图像对应的直方图，由图6可以看出，加密图像的直方图完全不同于两幅原图像的直方图。表3给出了两幅原图像和由所提方法、文献[34]中的方法、文献[28]中的方法得到的加密图像中相邻像素在三个方向上的相关性。由表3可以看出，所提方法

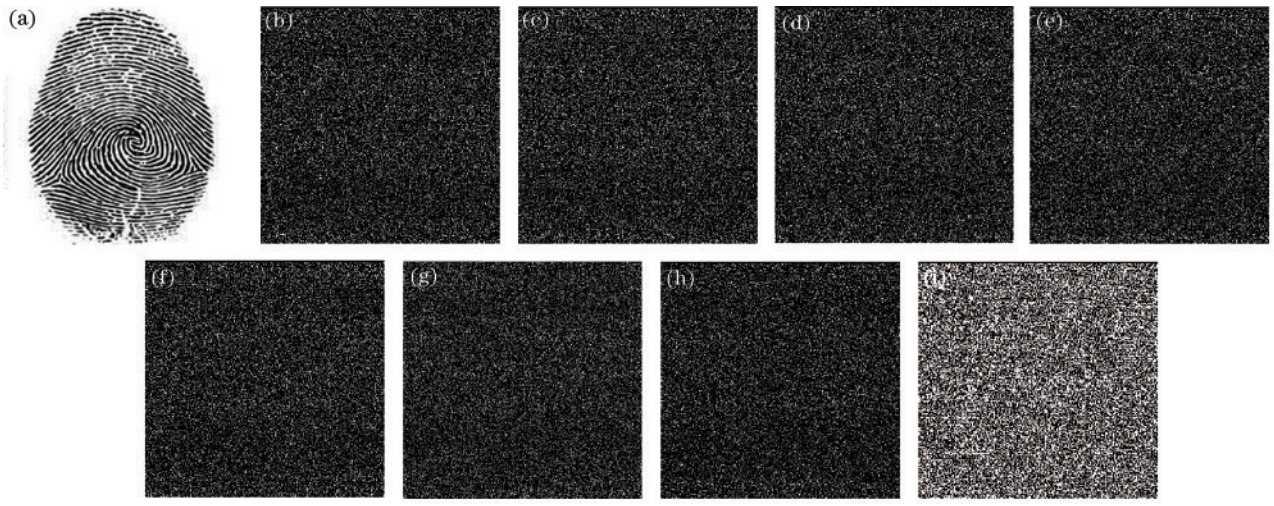


图 5　使用错误密钥得到的解密图像 Peppers。(a)错误指纹;(b)由错误指纹得到的解密图像;(c)～(f)由错误混沌参数 $a_0'=1.75+10^{-15}$, $b_0'=0.33+10^{-15}$, $x_0'=0.34+10^{-15}$, $y_0'=10^{-15}$ 得到的解密图像;(g)～(h)由错误 Gyrator 参数 $\alpha_1'=0.5+10^{-2}$, $\alpha_2'=0.6+9\times10^{-3}$ 得到的解密图像;(i)由错误相位密钥 $P_2$ 得到的解密图像

Fig. 5　Decrypted results of image Peppers with incorrect keys. (a) Incorrect fingerprint; (b) decrypted result with the incorrect fingerprint; (c)-(f) decrypted results with the incorrect parameters of the chaotic map $a_0'=1.75+10^{-15}$, $b_0'=0.33+10^{-15}$, $x_0'=0.34+10^{-15}$, $y_0'=10^{-15}$; (g) - (h) decrypted results with the incorrect parameter of the Gyrator transform $\alpha_1'=0.5+10^{-2}$, $\alpha_2'=0.6+9\times10^{-3}$; (i) decrypted result with the incorrect phase key $P_2$

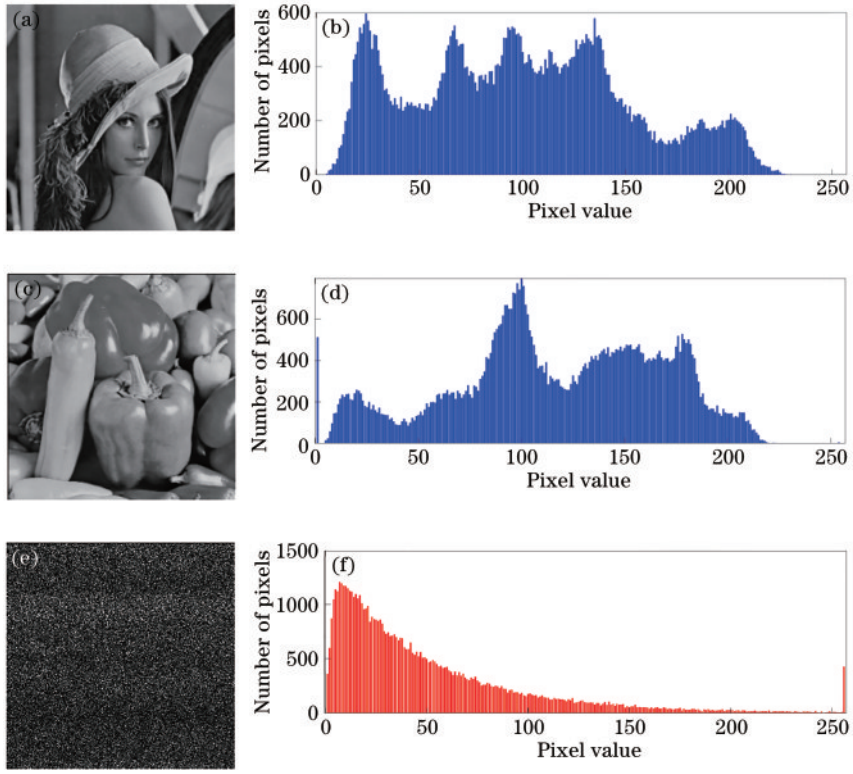


图 6　原图像及加密图像的直方图。(a)原图像 Lena;(b)原图像 Lena 的直方图;(c)原图像 Peppers;(d)原图像 Peppers 的直方图;(e)加密图像;(f)加密图像的直方图

Fig. 6　Histograms of the original image and encrypted image. (a) Original image Lena; (b) histogram of Lena; (c) original image Peppers; (d) histogram of Peppers; (e) encrypted image; (f) histogram of the encrypted image

可以有效打破原图像中相邻像素间的高相关性,并且所提方法的表现优于文献[34]中的方法和文献[28]中的方法。结果表明,所提方法可以有效抵抗统计分析攻击。

### 3.5　抗剪切和抗噪声攻击分析

由于加密图像在传输和存储过程中可能由于破损而造成信息丢失,因此对所提方法从破损加密图像中恢复原图像的能力进行了测试,并与文献[34]

表 3　原图像和加密图像中相邻像素间的相关系数

Table 3　Correlation coefficients of adjacent pixels in original and encrypted images

| Direction | Original image | | Encrypted image | | |
|---|---|---|---|---|---|
| | Lena | Peppers | Method in Ref. [34] | Method in Ref. [28] | Proposed method |
| Level | 0.9728 | 0.9448 | 0.0388 | 0.0307 | −0.0270 |
| Vertical | 0.9389 | 0.9527 | 0.0164 | −0.0074 | 0.0044 |
| Diagonal | 0.9138 | 0.8967 | 0.0365 | 0.0049 | 0.0013 |

中的方法和文献[28]中的方法进行了比较。图 7(a)～(d)分别为剪切掉 12.5%、25%、37.5% 和 50% 信息的加密图像。图 8 为密钥完全正确时，不同方法从不同破损比例的加密图像中得到的解密图像的 PSNR 和 CC 值。由图 8 可以看出，所提方法在抗剪切攻击方面的表现优于文献[34]中的方法和文献[28]中的方法。结果表明，所提方法具有较强的抗剪切攻击能力。

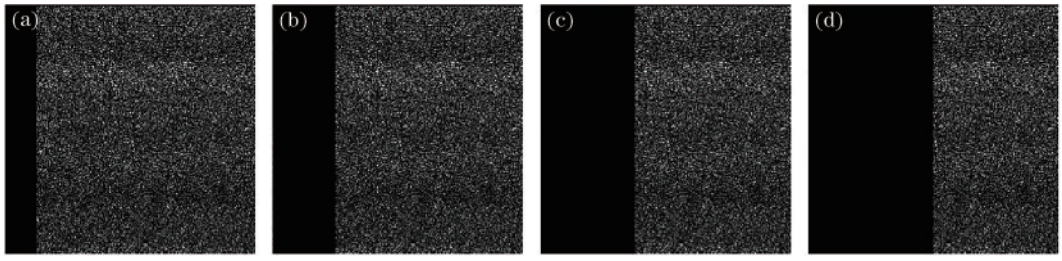


图 7　不同破损比例下的加密图像。(a)～(d)破损比例分别为 12.5%、25%、37.5%、50%

Fig. 7　Encrypted images with different occlusion sizes. (a)-(d) Occlusion size is 12.5%, 25%, 37.5%, 50% respectively

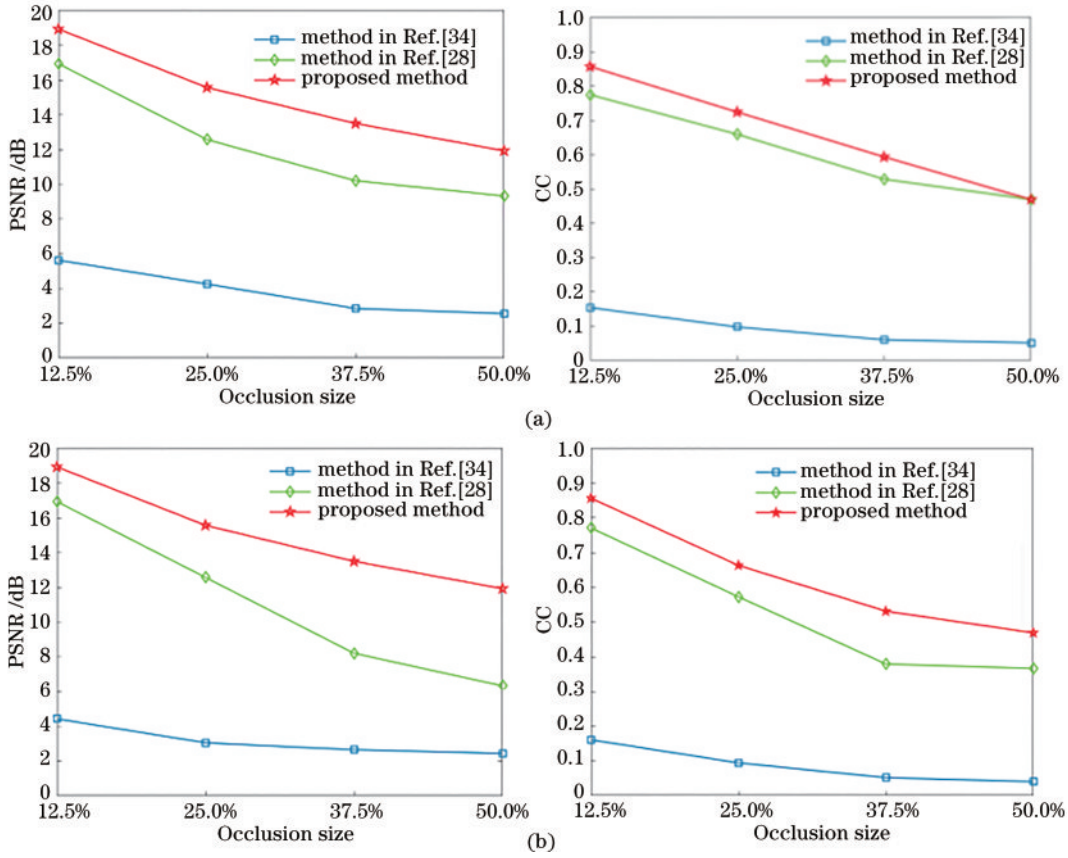


图 8　解密图像的 PSNR 和 CC 值随破损比例变化的曲线。(a) Lena；(b) Peppers

Fig. 8　PSNR and CC curves of decrypted images versus different occlusion sizes. (a) Lena; (b) Peppers

由于加密图像在传输和存储过程中还有可能会被噪声污染，因此对所提方法从被噪声污染的加密图像中恢复原图像的能力也进行了测试，并与文献[34]中的方法和文献[28]中的方法作比较。首先，对加密图

像添加不同强度的高斯随机噪声，然后利用正确密钥从被噪声污染的加密图像中对两幅原图像进行解密。

$$I_{\mathrm{E}}'=I_{\mathrm{E}}\cdot(1+K\cdot G),\tag{18}$$

式中：$I_{\mathrm{E}}$和$I_{\mathrm{E}}'$分别表示加密图像和被噪声污染的加密图像；$G$表示均值为0、方差为1的高斯随机噪声；$K$表示添加的噪声强度。图9为所提方法、文献[34]中的方法和文献[28]中的方法从被添加不同强度高斯噪声的加密图像中得到的PSNR和CC值。由图9可以看出，所提方法在抗噪声攻击方面的表现优于文献[34]中的方法和文献[28]中的方法。结果表明，所提方法具有较强的抗噪声攻击能力。

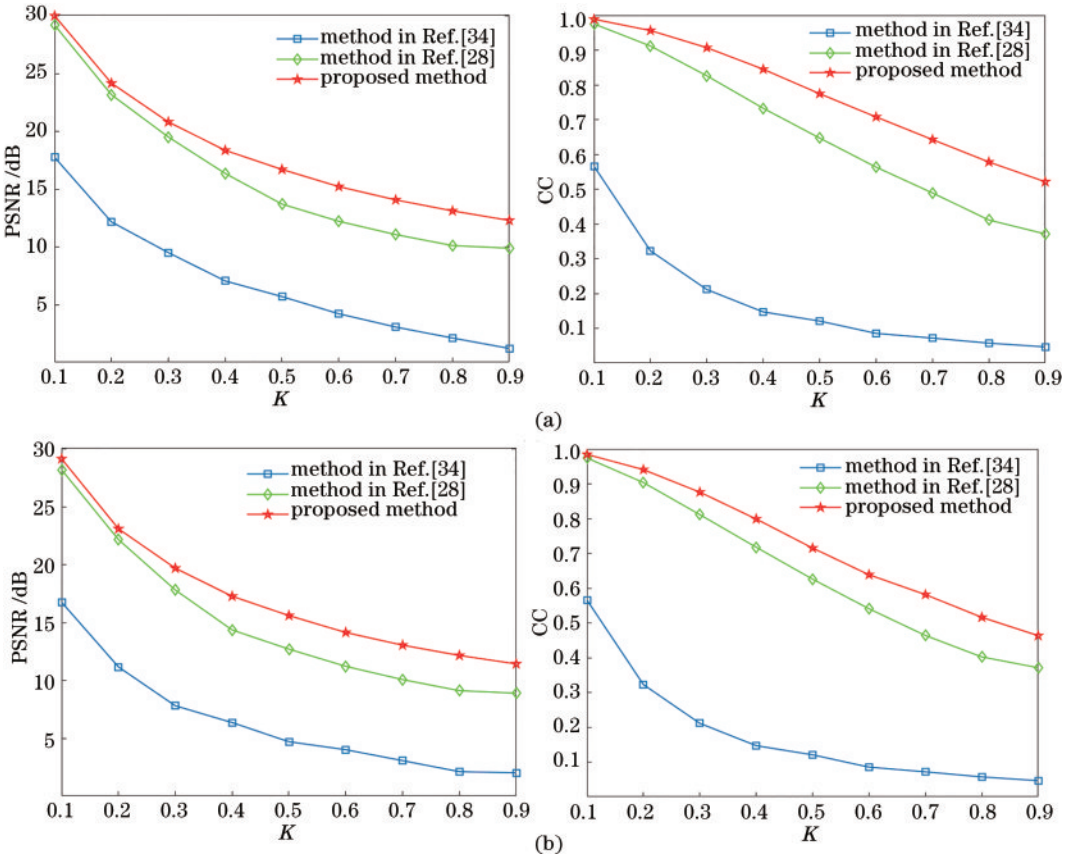


图9　解密图像的PSNR和CC值随噪声强度变化的曲线。(a) Lena；(b) Peppers

Fig. 9　PSNR and CC curves of decrypted images versus different intensity of Gaussian noise. (a) Lena; (b) Peppers

## 4　结　　论

提出了一种基于指纹随机相位密钥的光学双图像加密方法。一方面，该方法利用人体指纹特征建立起光学随机相位密钥与用户之间的联系，可以有效提升加密系统的安全性。另一方面，由于无需存储和传输随机相位板密钥，因此使得密钥管理更为便捷。此外，数值模拟结果表明：只有当所有密钥都完全正确时才能从加密图像中将两幅原图像无损地解密出来；当某一密钥与正确密钥存在微小偏差时，即使其他密钥都完全正确，也不能从加密图像中解密得到原图像的任何有效信息。另外，数值模拟结果还表明，所提方法能够有效抵抗统计分析攻击、剪切攻击和噪声攻击。

## 参　考　文　献

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

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

[3] Jiao S M, Zhou C Y, Shi Y S, et al. Review on optical image hiding and watermarking techniques[J]. Optics & Laser Technology, 2019, 109: 370-380.

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

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

[6] 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.

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

[8] Liu Z J, Xu L, Lin C, et al. Image encryption scheme by using iterative random phase encoding in gyrator transform domains[J]. Optics and Lasers in Engineering, 2011, 49(4): 542-546.

[9] Unnikrishnan G, Singh K. Optical encryption using quadratic phase systems[J]. Optics Communications, 2001, 193: 51-67.

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

[11] Rajput S K, Nishchal N K. Optical double image security using random phase fractional Fourier domain encoding and phase-retrieval algorithm[J]. Optics Communications, 2017, 388(4): 38-46.

[12] 苏永钢, 徐文君. 基于数字全息和混沌随机相位编码的双图像加密[J]. 光电子·激光, 2020, 31(9): 939-946.
Su Y G, Xu W J. Double image encryption based on digital holography and chaotic random phase encoding[J]. Journal of Optoelectronics·Laser, 2020, 31(9): 939-946.

[13] Kong D Z, Cao L C, Jin G F, et al. Three-dimensional scene encryption and display based on computer-generated holograms[J]. Applied Optics, 2016, 55(29): 8296-8300.

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

[15] 吴军, 王刚, 徐刚. 结合计算全息与混沌的彩色图像加密方法[J]. 光学学报, 2021, 41(19): 1909001.
Wu J, Wang G, Xu G. Color image encryption method based on computer generated hologram and chaos[J]. Acta Optica Sinica, 2021, 41(19): 1909001.

[16] Chen W, Chen X D, Sheppard C J R. Optical image encryption based on diffractive imaging[J]. Optics Letters, 2010, 35(22): 3817-3819.

[17] Li X W, Wang Y, Li Q, et al. Optical 3D object security and reconstruction using pixel-evaluated integral imaging algorithm[J]. Optics Express, 2019, 27(15): 20720-20733.

[18] 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.

[19] Shi Y S, Li T, Wang Y L, et al. Optical image encryption via ptychography[J]. Optics Letters, 2013, 38(9): 1425-1427.

[20] Pan A, Wen K, Yao B L. Linear space-variant optical cryptosystem via Fourier ptychography[J]. Optics Letters, 2019, 44(8): 2032-2035.

[21] 刘杰, 白廷柱, 沈学举, 等. 基于联合功率谱分区复用的光学多图像加密方法与实验[J]. 中国激光, 2018, 45(12): 1209003.
Liu J, Bai T Z, Shen X J, et al. Experimental research and encryption method of optical multi-images based on joint power spectral partition multiplexing[J]. Chinese Journal of Lasers, 2018, 45(12): 1209003.

[22] Tashima H, Takeda M, Suzuki H, et al. Known plaintext attack on double random phase encoding using fingerprint as key and a method for avoiding the attack[J]. Optics Express, 2010, 18(13): 13772-13781.

[23] Zhao T Y, Ran Q W, Yuan L, et al. Image encryption using fingerprint as key based on phase retrieval algorithm and public key cryptography[J]. Optics and Lasers in Engineering, 2015, 72: 12-17.

[24] Yan A M, Wei Y, Hu Z J, et al. Optical cryptography with biometrics for multi-depth objects[J]. Scientific Reports, 2017, 7: 12933.

[25] Zhu J N, Yang X L, Meng X F, et al. Computational ghost imaging encryption based on fingerprint phase mask [J]. Optics Communications, 2018, 420: 34-39.

[26] Verma G, Liao M H, Lu D J, et al. An optical asymmetric encryption scheme with biometric keys[J]. Optics and Lasers in Engineering, 2019, 116: 32-40.

[27] Verma G, Sinha A. Optical image encryption system using nonlinear approach based on biometric authentication [J]. Journal of Modern Optics, 2017, 64(13): 1321-1329.

[28] Tao S, Tang C, Shen Y X, et al. Optical image encryption based on biometric keys and singular value decomposition[J]. Applied Optics, 2020, 59(8): 2422-2430.

[29] Su Y G, Xu W J, Zhao J, et al. Optical color image encryption based on chaotic fingerprint phase mask in various domains and comparative analysis[J]. Applied Optics, 2020, 59(2): 474-483.

[30] Su Y G, Xu W J, Zhao J. Optical image encryption based on chaotic fingerprint phase mask and pattern-illuminated Fourier ptychography[J]. Optics and Lasers in Engineering, 2020, 128: 106042.

[31] Su Y G, Xu W J, Li T L, et al. Optical color image encryption based on fingerprint key and phase-shifting digital holography[J]. Optics and Lasers in Engineering, 2021, 140: 106550.

[32] Su Y G, Xu W J, Zhao J. Optical color image encryption based on a voice key under the framework of speckle-illuminated Fourier ptychography[J]. OSA Continuum, 2020, 3(11): 3267-3279.

[33] Jackson E A, Hübler A. Periodic entrainment of chaotic logistic map dynamics[J]. Physica D: Nonlinear Phenomena, 1990, 44(3): 407-420.

[34] Wang X G, Zhao D M, Chen Y X. Double-image encryption without information disclosure using phase-truncation Fourier transforms and a random amplitude mask[J]. Applied Optics, 2014, 53(23): 5100-5108.