引用格式：GUO Yuan, WANG Xuewen, WANG Chong, et al. Ciphertext Multi-image Reversible Information Hiding Based on Datagram Reorganization and Optical Interference[J]. Acta Photonica Sinica, 2021, 50(12):1210002
郭媛,王学文,王充,等. 基于数据报重组与光学干涉的密文多图像可逆信息隐藏[J].光子学报,2021,50(12):1210002

基于数据报重组与光学干涉的密文多图像可逆信息隐藏

郭媛,王学文,王充,姜津霖
(齐齐哈尔大学 计算机与控制工程学院,黑龙江 齐齐哈尔 161006)

摘　要:针对现有可逆信息隐藏嵌入率低,无法一次隐藏多张不同图像问题,提出一种密文域光学多图像可逆信息隐藏方法。将多张不同类型、不同大小图像进行数据报重组得到重组多图像,无需提供任何信息可在一定噪声下重构多图像。载体图像经非对称双随机相位编码得到加密图像,再将重组多图像光强缩小1 000倍,与加密图像级联干涉得到载密图像,利用级联矢量分解可从载密图像中无损还原重组多图像和加密图像。载密图像可用解密密钥进行解密,也可用隐藏密钥无损还原重组多图像,当同时具有解密密钥与隐藏密钥时可无损还原载体图像,实现完全可逆、可分离。实验表明,当嵌入率为128比特/像素时,载密图像峰值信噪比大于32 dB,且可无损还原隐藏图像与载体。在1/2剪切或0.2的各种噪声下,各还原图像峰值信噪均大于11 dB,具有鲁棒性。3 s内可实现32比特/像素的嵌入、还原和解密,具有高效性。

关键词:密文可逆信息隐藏;数据报重组;光学干涉;矢量分解;多图像
中图分类号:TP 391　　**文献标识码**:A　　**doi**:10.3788/gzxb20215012.1210002

Ciphertext Multi-image Reversible Information Hiding Based on Datagram Reorganization and Optical Interference

GUO Yuan, WANG Xuewen, WANG Chong, JIANG Jinlin
(*School of Computer and Control Engineering, Qiqihar University, Qiqihar, Heilongjiang* 161006, *China*)

Abstract: Aiming at the problem that the existing reversible information hiding has a low embedding rate and can not hide multiple different images at once. An optical reversible information hiding method for multiple images in ciphertext domain is proposed. Multiple images of different types and sizes are reconstructed by datagram. Multiple images can be reconstructed under certain noise without providing any information. The carrier image is encoded with asymmetric double random phase coding to obtain an encrypted image. Then the light intensity of the recombined multi-image is reduced by 1 000 times, and it cascade interference with the encrypted image to obtain the carrying secret image. Using cascaded vector decomposition, multiple images and encrypted images can be restored losslessly from encrypted images. The carrying secret image can be decrypted with the decryption key, or hidden key can lossless restore reassemble multiple images from carrying secret image. The carrier image can be restored lossless when both the decryption key and the hidden key are available. Realize completely reversible and separable. The experiment shows: When the embedding rate is 128 bits/pixel, the peak signal-to-noise

基金项目:国家自然科学基金(No.61872204),黑龙江省自然科学基金(No. LH2021F056),黑龙江省教育厅科研面上项目(No. 1355091130),研究生研究项目研究生创新科研项目(No.YJSCX20200050)
第一作者:郭媛(1974—),女,教授,博士,主要研究方向为光学检测及信息处理。Email:guoyuan171@126.com;
通讯作者:王学文(1994—),男,硕士研究生,主要研究方向为图像处理。Email:857603360@qq.com
收稿日期:2021-05-25;**录用日期**:2021-07-28

ratio of the carrying secret image is greater than 32 dB. Hidden images and carriers can be restored lossless. Under clipping 1/2 or various noises of 0.2, the peak signal-to-noise ratio of each extracted and restored image is greater than 11 dB, has good robustness. 32 bits/pixel can be embedded, extracted and decrypted within 3 s, which is highly efficient.

Key words: Ciphertext reversible information hiding; Datagram reorganization; Vector decomposition; Optical interference; Multiple images

OCIS Codes: 100.4998; 200.3050; 070.2025; 070.1170; 110.3175

0 引言

近年来许多加密域可逆信息隐藏(Reversible Data Hiding in Encrypted Image, RDH-EI)算法被提出[1-11]。PUTEAUX P使用最重要的位(Most Significant Bit, MSB)进行加密域可逆数据隐藏,首先识别预测误差并存储于加密图像中,用隐藏信息替换可嵌入像素的MSB平面,嵌入率可达1比特/像素(bits/pixel, bpp)[3]。YIP和GUAN B在PUTEAUX P的基础上,分别通过提高MSB平面替换个数来增加嵌入率,嵌入率分别提高到1.24 bpp、3 bpp[4-5]。LI X先对图像进行Arnold和数独变换保留嵌入空间,再对隐藏信息进行半调变换、四叉树变换和S-BOX变换的预处理,嵌入率为1.38 bpp[6]。CHEN K提出一种基于像素差分压缩的加密域可逆数据隐藏算法,先对图像进行2×2块的块加密,再将每块像素划分为1个标记像素和3个可替换像素,而其中可替换像素用其压缩像素差值进行替换,腾出隐藏空间,该算法嵌入率高达1.35 bpp[7]。ZHANG R先对图像进行不重叠分块,每块分别进行同态有效加密,再采用基于预测误差扩展的直方图移动算法实现信息隐藏,嵌入率可达2 bpp[8]。WU Y先使用参数二叉树对加密图像进行标记,并在预测误差下进行像素分组,最后对可嵌入像素分组进行替换嵌入隐藏信息,嵌入率为2.5 bpp[9]。WENG S提出一种基于分组分类编码GCC和SIBRW的加密域可逆数据隐藏算法,其嵌入率可达2.66 bpp[10]。MALIK A先对图像进行加密,再利用奇偶值嵌入技术进行多层嵌入,并记录各层位置图与恢复阶段使用层数,最后进行置乱操作,其嵌入率可达4 bpp[11]。最近也出现许多光学信息隐藏方法。Lv提出一种基于方位多路复用的光学图像隐藏算法;将隐藏图像进行视觉键编码,利用基于方位角复用算法将视觉键隐藏于载体图像,可利用纯相位掩模旋转到特定的方位角提取信息[12]。YE Z等提出一种基于加加权光源的傅里叶单像素图像水印与隐藏算法;首先计算水印或隐藏图像的傅里叶系数。并加载进正弦结构照明模式中,实现高质量图像水印和隐藏[13]。GANG Q A提出一种彩色光学水印算法。首先用DCT基和bayer阵列生成的彩色图案来照亮目标彩色场景得到编码后的数据,再通过奇异值分解(Singular Value Decomposition, SVD)得到水印的主分量,最后将其嵌入到RIWD中主图像的子带LL的奇异值矩阵中[14]。经上述分析,无论光学信息隐藏还是密文域可逆信息隐藏算法嵌入率都低于8 bpp,不能同时嵌入多张相同尺寸的图像,无法更好满足用户需求。另一方面,现有多图像重组,需记住不同图像的尺寸、类型和数量,增加密钥传输[15]。

综上所述两问题,本文提出一种基于数据报重组的光学多图像可逆信息隐藏算法。可实现多张不同大小、不同类型图像的可逆可分离隐藏,且算法嵌入率高、鲁棒性强,高效安全。

1 基本原理

1.1 多图像数据报重组与重构

为解决多图像重组时需记住不同图像的尺寸、类型和数量问题,本文采用数据报重组的方法。数据报分为数据区、分隔区、随机区与校验区。数据区用于存取图像像素信息;分隔区用于分隔不同图像的数据区,用100个零进行填充;随机区用于改变多图像数据报大小,采用随机值进行填充;校验区用于存放图像类型、尺寸以及数量,由图像数量区(存储图像数量)以及多个信息区(存储图像尺寸与类型信息)组成,每个信息区又可分为长区、宽区及类型区。由于图像长宽可能超过256,因此长区与宽区又分别分为两小区,分别存放长宽与256的整除数与余数,各区均包含100个相同数据。具体结构如图1所示。

将各图像顺序填入数据区,将各图像尺寸与类型按图像填入顺序填入信息区,同时将图像数量信息填

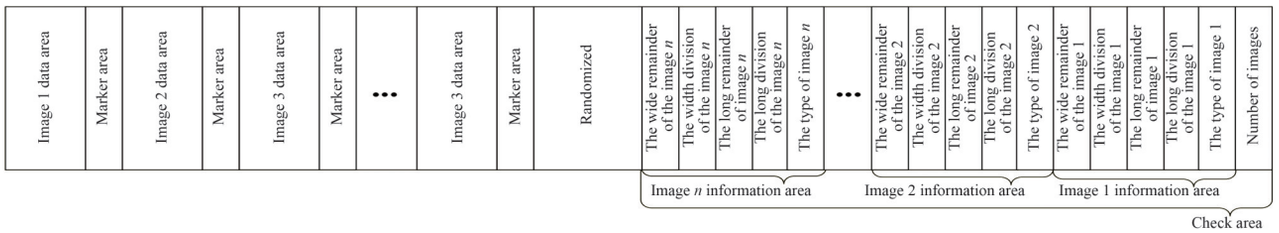


图1　数据报格式

Fig. 1　Datagram format

入数量区,扩展随机区得到数据报,最后将数据报按载体图像尺寸重组得到用于干涉隐藏重组多图像。

为更好从重组多图像中重构各图像,采用重复校验机制。1)将重组多图像组合为数据报;2)对图像数量区中值进行无重复排序;3)从排序列表中顺序取一个值s,按照式(1)计算数据报校验区的终止位置A;4)判断数据报终止位置是否为随机区的终止位置(向前取一定数量值看是否为随机值),否则转到3),直到判断正确;5)对信息区中各区间分别进行无重复排序;6)从一个信息区的各区排序列表中顺序取一个值为l_1, l_2, w_1, w_2, e,按照式(2)~(3)计算图像数据区的开始位置I与结束位置D;7)判断开始位置是否为分隔区的终止位置(向前取100个值看是否一半为零),结束位置是否为分隔区的起始位置(向后取100个值看是否一半为零),否则转到6),直到判断正确。

$$A = H - s \times 500 - 100 \tag{1}$$

式中,H为数据报长度。

$$D_i = \begin{cases} (256 \times l_1 + l_2) \times (256 \times w_1 + w_2) \times e + 100 & i = 1 \\ D_{i-1} + (256 \times l_1 + l_2) \times (256 \times w_1 + w_2) \times e + 100 & i > 1 \end{cases} \tag{2}$$

$$I_i = \begin{cases} 0 & i = 1 \\ I_{i-1} + (256 \times l_1 + l_2) \times (256 \times w_1 + w_2) \times e + 100 & i > 1 \end{cases} \tag{3}$$

式中,l_2为长整除数取值,l_1为长余数取值,w_2为宽整除数取值,w_1为宽余数取值,e为类型区取值。

1.2　矢量分解原理

光干涉是两道或两道以上的光波在空间中相遇时发生叠加或抵消从而形成新的光波的现象。矢量分解过程与干涉具有互逆性,可无损求解干涉光(E)中各光束(E_1,E_2)[16]。如图2所示。干涉过程为

$$E = E_1 + E_2 \tag{4}$$

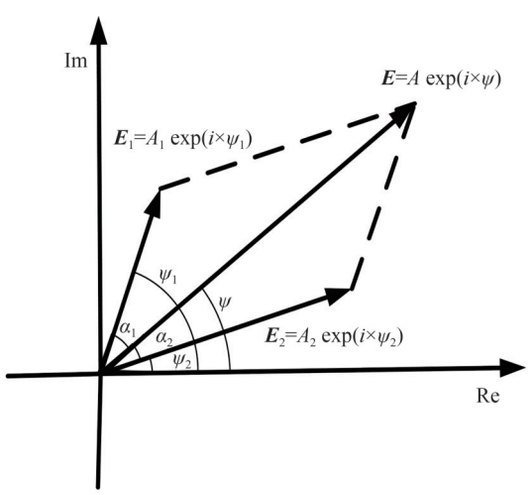


图2　干涉与矢量分解原理

Fig. 2　Principle of interference and vector decomposition

矢量分解过程由余弦定理可得

$$\begin{cases}\cos\alpha_1=\dfrac{A^2+A_1^2-A_2^2}{2AA_1}\\ \cos\alpha_2=\dfrac{A^2+A_2^2-A_1^2}{2AA_2}\end{cases}\tag{5}$$

其中 $\alpha_1,\alpha_2\in(-\pi,\pi)$，则 ψ_1,ψ_2 为

$$\begin{cases}\psi_1=\begin{cases}\psi-\arccos\dfrac{A^2+A_1^2-A_2^2}{2A_kA_{1k}},\psi_1\leqslant\psi_2\\ \psi+\arccos\dfrac{A^2+A_1^2-A_2^2}{2A_kA_{1k}},\psi_1>\psi_2\end{cases}\\ \psi_2=\begin{cases}\psi-\arccos\dfrac{A^2+A_2^2-A_1^2}{2AA_2},\psi_1\geqslant\psi_2\\ \psi+\arccos\dfrac{A^2+A_2^2-A_1^2}{2AA_2},\psi_1<\psi_2\end{cases}\end{cases}\tag{6}$$

则

$$\begin{cases}\boldsymbol{E}_1=A_1\exp(i\times\psi_1)\\ \boldsymbol{E}_2=A_2\exp(i\times\psi_2)\end{cases}\tag{7}$$

1.3 多图像干涉可逆信息隐藏

两图像进行干涉，若其中一图像光强缩小1 000倍如式(8)，其干涉图像与另一图像相似，具有信息隐藏作用。如图3所示。因矢量分解可无损求解干涉中各光束，所以可利用缩小干涉进行可逆信息隐藏。

$$\boldsymbol{E}=\boldsymbol{E}_1+0.001\boldsymbol{E}_2\tag{8}$$

(a) $\boldsymbol{E}_1$ (b) $\boldsymbol{E}_2$ (c) $\boldsymbol{E}$

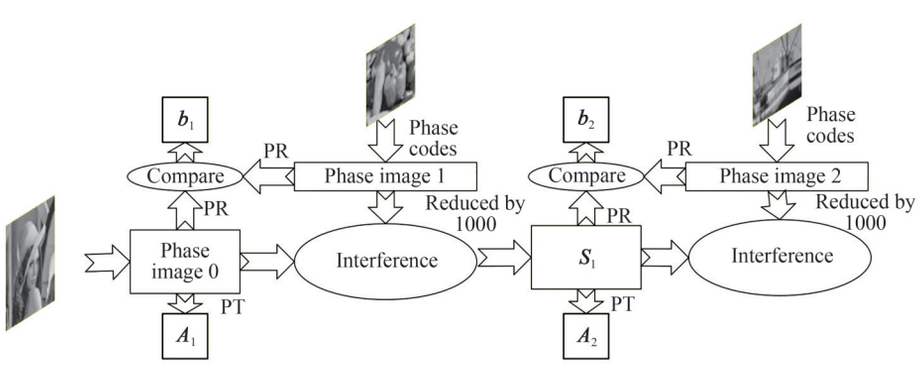
图3 缩小干涉

Fig. 3 Minimized interference

多光束干涉后其光强强度为各光束矢量和，则可利用缩小干涉进行多图像可逆信息隐藏，其嵌入过程如图4，表达式为

$$\boldsymbol{E}=\boldsymbol{E}_1+0.001\boldsymbol{E}_2+\cdots+0.001\boldsymbol{E}_n\tag{9}$$

图4中PT表示相位截断，PR表示振幅截断，$\boldsymbol{A}_1,\boldsymbol{A}_2,\cdots,\boldsymbol{A}_n$ 为相位截断的振幅。$\boldsymbol{b}_1,\boldsymbol{b}_2,\cdots,\boldsymbol{b}_{n-1}$ 为载密图像与隐藏图像的相位角比较矩阵，若载密图像相位角大则为1，否则为0。



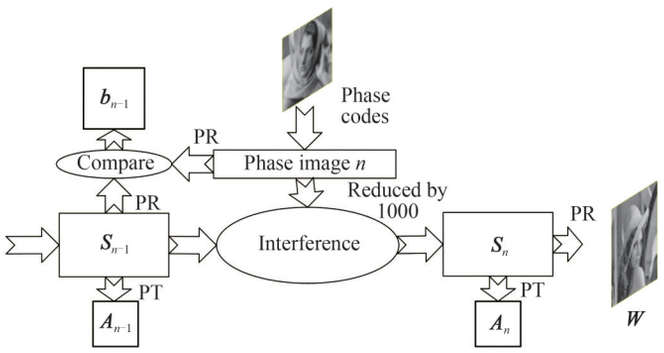


图4　多图像干涉可逆信息隐藏嵌入过程

Fig. 4　Reversible information hiding embedding process with multi-image interference

图4主要采用级联干涉。主要步骤为1)对载体图像与一张隐藏图像进行相位编码;2)对两相位编码进行振幅截断PR操作得到相位角,比较两相位角大小得到比较矩阵$\boldsymbol{b}_1$;3)对载体相位编码进行相位截断PT操作得到振幅$\boldsymbol{A}_1$;4)将隐藏图像相位编码光强缩小1 000倍,与载体相位编码进行干涉得到载密相位图像$\boldsymbol{S}_1$;5)载密相位图像$\boldsymbol{S}_1$与余下隐藏图像进行上述操作;6)对载密相位图像$\boldsymbol{S}_n$进行PT操作得到振幅$\boldsymbol{A}_n$以及PR操作得到载密图像$\boldsymbol{W}$。

可利用矢量分解原理无损提取隐藏信息与恢复载体图像,提取过程如图5。

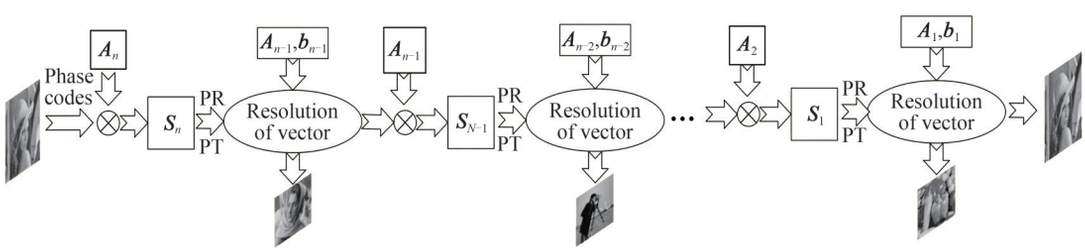


图5　多图像干涉可逆信息隐藏提取过程

Fig. 5　Extraction process of multi-image interference reversible information hiding

图5主要采用级联矢量分解。主要步骤为:1)载密图像$\boldsymbol{W}$进行相位编码;2)将$\boldsymbol{W}$的相位编码与振幅$\boldsymbol{A}_n$相乘得到载密相位图$\boldsymbol{S}_n$,同时获取其振幅与相位角;3)将$\boldsymbol{S}_n$的振幅与相位角、振幅$\boldsymbol{A}_{n-1}$以及比较矩阵$\boldsymbol{b}_{n-1}$代入矢量分解式(6)~(7)得到载密图像$\boldsymbol{W}_{n-1}$以及一张隐藏图像(隐藏图像的振幅为1);4)不断重复上述2)~3)操作,最终提取出所有隐藏图像以及恢复载体图像。

2　密文域可逆信息隐藏算法

2.1　多图像可逆信息隐藏

本文嵌入算法主要分为3部分:1)载体图像光学加密;2)多图像数据报重组;3)重组图像与载体密文干涉可逆信息隐藏。多图像可逆信息隐藏原理如图6。

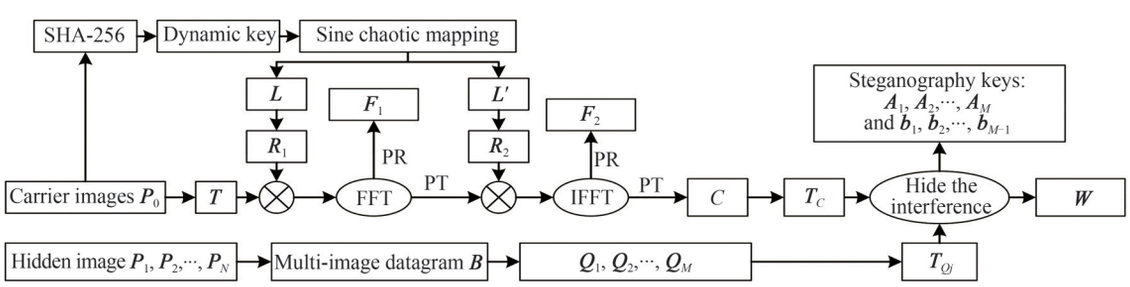


图6　多图像可逆信息隐藏原理

Fig. 6　Reversible information hiding theory of multiple images

多张隐藏图像按照数据报格式重组得到重组图像$\boldsymbol{Q}_1,\boldsymbol{Q}_2,\cdots,\boldsymbol{Q}_M$,载体图像$\boldsymbol{P}_0$经非对称双随机相位编码系统加密得到密文$\boldsymbol{C}$,重组图像与密文级联干涉得到载密图像$\boldsymbol{W}$以及隐藏密钥。具体步骤为

Step 1:读取隐藏图片$\boldsymbol{P}_1,\boldsymbol{P}_2,\cdots,\boldsymbol{P}_N$。将其按照数据报格式进行组合,再对随机区进行填充使数据报大小满足载体图像尺寸重组需求,得到数据报$\boldsymbol{B}$。

Step 2:将数据报$\boldsymbol{B}$重组为与载体图像相同尺寸的重组图像$\boldsymbol{Q}_1,\boldsymbol{Q}_2,\cdots,\boldsymbol{Q}_M$。

Step 3:读取载体图像$\boldsymbol{P}_0$,获得其哈希值$\boldsymbol{H}=\{H_1,H_2,\cdots,H_{64}\}$。再根据式(10)产生动态密钥。

$$x=\left(\sum_{i=1}^{32}H_i\times16^{i-1}\right)/10^{14},\phi=\left(\sum_{i=33}^{64}H_i\times16^{i-1}\right)/10^{14} \tag{10}$$

Step 4:将x,ϕ代入式(11)产生长度为$2\times n\times m+1\,000$的序列,去掉前1 000个序列值以抵消暂态效应的影响,最终得到混沌序列$L=\{L_1,L_2,\cdots,L_{n\times m}\}$与$L'=\{L_{n\times m+1},L_{n\times m+2},\cdots,L_{2\times n\times m}\}$,其中$n,m$为载体图像$\boldsymbol{P}_0$的长宽。再将其转化为相位掩模版$\boldsymbol{R}_1$、$\boldsymbol{R}_2$,即式(12)。

$$z_{n+1}=\phi\sin(\pi z_n) \tag{11}$$

$$\begin{cases}\boldsymbol{R}_1=\exp(\mathrm{i}\times2\pi\times L)\\ \boldsymbol{R}_2=\exp(\mathrm{i}\times2\pi\times L')\end{cases} \tag{12}$$

Step 5:对载体图像$\boldsymbol{P}_0$进行相位编码,即

$$\boldsymbol{T}=\exp(\mathrm{i}\times\boldsymbol{P}_0) \tag{13}$$

Step 6:将$\boldsymbol{T}$与相位掩模版$\boldsymbol{R}_1$、$\boldsymbol{R}_2$代入傅里叶变换的非对称双随机相位编码系统,得到密文$\boldsymbol{C}$以及解密密钥F_1、F_2,即

$$\boldsymbol{C}=\mathrm{PT}\left\{\mathrm{IFFT}\left[\mathrm{PT}\left\{\mathrm{FFT}(\boldsymbol{T}\cdot\boldsymbol{R}_1)\right\}\cdot\boldsymbol{R}_2\right]\right\} \tag{14}$$

式中,FFT为傅里叶变换,IFFT为傅里叶逆变换。

Step 7:将密文$\boldsymbol{C}$归一化,并同时与重组多图像$\boldsymbol{Q}_1,\boldsymbol{Q}_2,\cdots,\boldsymbol{Q}_M$进行相位编码,即

$$\boldsymbol{T}_{\boldsymbol{Q}_j}=\exp(\mathrm{i}\times\boldsymbol{Q}_j)\quad 1\leqslant j\leqslant M \tag{15}$$

$$\boldsymbol{T}_C=\exp(\mathrm{i}\times\boldsymbol{C}) \tag{16}$$

Step 8:利用多图像干涉可逆信息隐藏原理将重组多图像相位$\boldsymbol{T}_{\boldsymbol{Q}_j}$嵌入载体图像密文相位$\boldsymbol{T}_C$中,得到载密图像$\boldsymbol{W}$、各级相位截断产生的振幅$\boldsymbol{A}_1,\boldsymbol{A}_2,\cdots,\boldsymbol{A}_M$以及各级载密图像与重组图像的相位角比较矩阵$\boldsymbol{b}_1,\boldsymbol{b}_2,\cdots,\boldsymbol{b}_{M-1}$。

2.2 隐藏图像提取与载体图像恢复

Step 1:利用$\boldsymbol{A}_1,\boldsymbol{A}_2,\cdots,\boldsymbol{A}_M$以及$\boldsymbol{b}_1,\boldsymbol{b}_2,\cdots,\boldsymbol{b}_{M-1}$从载密图像$\boldsymbol{W}$中提取重组图像$\boldsymbol{Q}_1,\boldsymbol{Q}_2,\cdots,\boldsymbol{Q}_M$和恢复密文$\boldsymbol{C}$。

Step 2:将恢复密文$\boldsymbol{C}$以及F_1、F_2代入傅里叶变换的非对称双随机相位编码系统,恢复载体图像$\boldsymbol{P}_0$。

Step 3:将提取的多图像$\boldsymbol{Q}_1,\boldsymbol{Q}_2,\cdots,\boldsymbol{Q}_M$按照数据报重构算法还原各隐藏图片$\boldsymbol{P}_1,\boldsymbol{P}_2,\cdots,\boldsymbol{P}_N$。

3 实验分析

本文从实验效果、干涉可逆信息隐藏、多图像数据报重组鲁棒性以及抗噪声等方面进行分析。

3.1 实验效果分析

为验证本文光学多图像可逆信息隐藏的可行性与有效性,采用pycharm作为实验平台,选取灰度图Barbara(256×256)、Cameraman(256×256)与Animal(512×341)、彩色图Monarch(256×256×3)与Baboon(512×512×3)作为隐藏图像。灰度图Lena(512×512)为载体图像。图7展示了算法主要阶段效果图。

从图7可知,隐藏图像7(a)~(e)经多图像数据报重组后与加密图像进行级联干涉得到载密图像7(h);利用解密密钥解密载密图像得到含密还原图像7(j),利用隐藏密钥从载密图像中提取得到还原隐藏图像7(k)~(o);利用隐藏密钥对载密图像进行信息提取,再利用解密密钥进行解密得到还原图像7(i)。还原图像、含密还原图像与载体图像在人眼视觉上无明显差异。各隐藏图像与还原隐藏图像之间无明显差异。验证了本算法的有效性、可行性。为进一步客观描述各图像之间差异,使用峰值信噪比(Peak Signal-to-Noise Ratio, PSNR)与结构相似性(Structural Similarity, SSIM)进行客观描述。结果如表1所示。

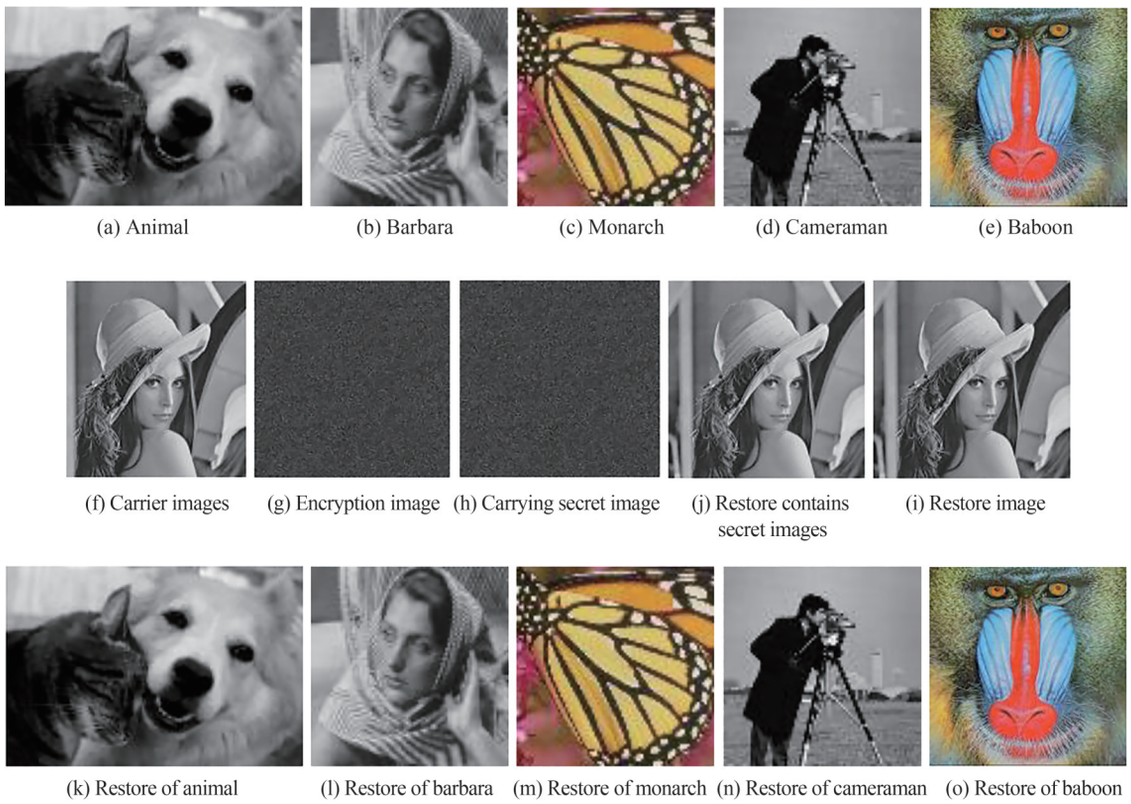


图 7　嵌入与还原

Fig. 7　Embedding and Restore

表 1　各阶段图像的 PSNR 与 SSIM

Table 1　PSNR and SSIM of images at each stage

Image	Animal	Barbara	Monarch	Cameraman	Baboon	Restore image	Restore contains secret images
PSNR/dB	inf	inf	inf	inf	inf	inf	42.050 057
SSIM	1	1	1	1	1	1	0.982 350

从表 1 可知,含密还原图像的 PSNR 为 42.05 dB,SSIM 为 0.982 4,表示载密图像的解密图为载体图像,表明算法的解密与还原是分离的。还原隐藏图像与还原图像的 PSNR 为无穷大,SSIM 为 1,表示还原隐藏图像和还原图像与原始图像相同,说明本文算法可无损还原各图像。

3.2　干涉可逆信息隐藏分析

为验证本文所出的干涉可逆信息隐藏的有效性。选取 Uncompressed Color Image Database(UCID)中大小为 512×512 图像作为隐藏图像,只进行密文域干涉可逆信息隐藏。

3.2.1　安全性分析

Lena 为载体图像的加密图像、不同嵌入率的载密图像及对应直方图如图 8 所示。表 2 为对应的信息熵。

由图 8 中可知,载体图像直方图 8(a)与载密图像直方图 8(c)~(g)明显不同,但载密图像直方图与加密图像直方图 8(b)非常相似。随着嵌入率增加,载密图像直方图变化较小。由表 2 可知,载体图像与载密图像信息熵差距较大,且载密图像与加密图像信息熵差距较小,信息熵随嵌入率增加变化较小。载密图像的直方图及信息熵与载体截然不同,而与加密图像相似,说明攻击者无法判断加密图像中是否嵌入隐藏图像,达到图像隐蔽性要求。

表 3 为以 Lena 为载体图像不同嵌入率的还原隐藏图像、还原图像和含密还原图像的 PSNR 与 SSIM 值。

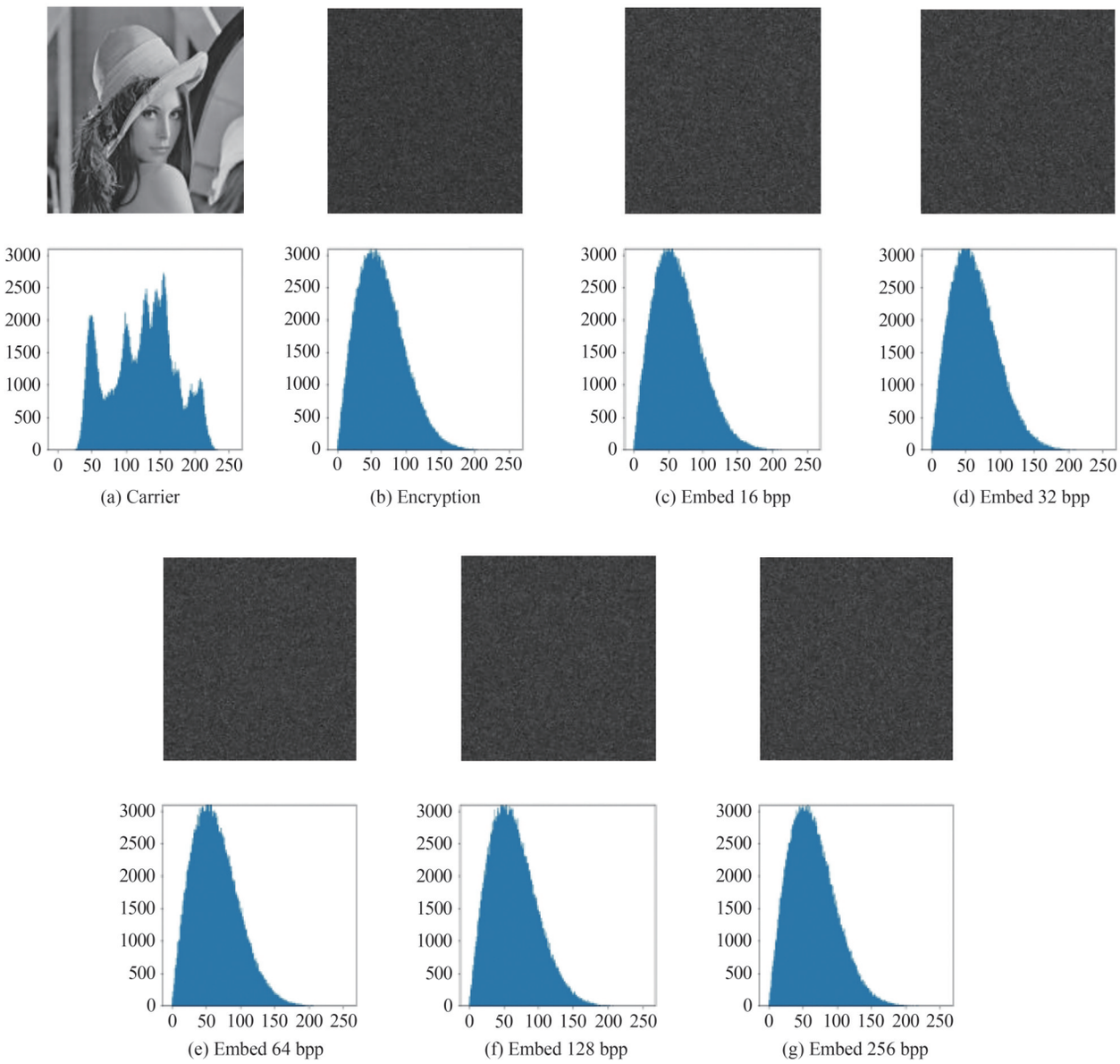


图 8 嵌入图像及直方图

Fig. 8 Embedded image and histogram

表 2 不同嵌入率下密文图像及嵌入图像的信息熵

Table 2 Information entropy of ciphertext images and embedded images at different embedding rates

Carrier images	Encryption image	Insert 16 bpp	Insert 32 bpp	Insert 64 bpp	Insert 128 bpp	Insert 512 bpp
7.445 5	7.042 8	7.040 6	7.036 3	7.041 2	7.039 8	7.046 5

表 3 不同嵌入率下各还原图像的 PSNR 与 SSIM

Table 3 PSNR and SSIM of each restored image at different embedding rates

Embedding rate	Restore hidden image (PSNR/SSIM)	Restore image (PSNR/SSIM)	Restore contains secret images (PSNR/SSIM)
16 bpp	inf/1.0	inf/1.0	52.201 1 dB/0.997 7
32 bpp	inf/1.0	inf/1.0	47.613 4 dB/0.993 5
64 bpp	inf/1.0	inf/1.0	40.997 1 dB/0.971 7
128 bpp	inf/1.0	inf/1.0	33.831 3 dB/0.883 9
512 bpp	inf/1.0	inf/1.0	27.105 6 dB/0.663 8

如表3所示，各还原隐藏图像与还原图像在不同嵌入率下PSNR为无穷大，SSIM为1。含密还原图像的PSNR与SSIM随着嵌入率的增加减小，当嵌入率为128 bpp时，PSNR大于33 dB，SSIM大于0.85。各还原图像与其对应图像完全相同，隐藏图像的嵌入对加密图像影响较小，解密图像的解密与隐藏图像的提取相互独立。验证了算法的完全可逆、可分离。算法隐蔽性、完全可逆和可分离保证了算法的安全性。

3.2.2　嵌入率及含密还原图像质量质量分析

嵌入率是衡量隐藏算法性能的重要指标。嵌入率越高，隐藏算法能够满足更多的用户需求；较高的含密还原图像PSNR可反应算法的隐蔽性。图9为不同嵌入率下不同载体的含密还原图像的PSNR。

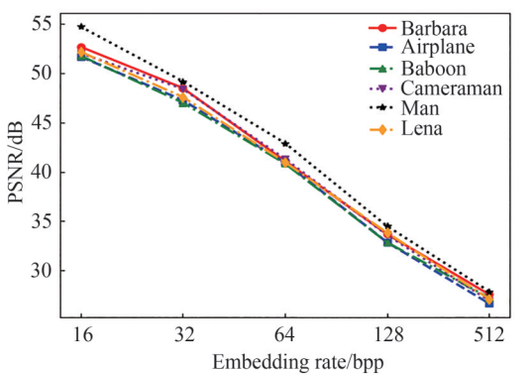


图9　不同嵌入率下不同载体的含密还原图像的PSNR

Fig. 9　PSNR of restore contains secret images with different carriers at different embedding rates

从图9中可知，不同载体随着嵌入率的增加，含密还原图像的PSNR逐渐降低；当嵌入率为128 bpp时，不同载体PSNR都大于32 dB。同时相同嵌入率下不同载体PSNR相差无几，说明干涉可逆信息隐藏在高嵌入率下，含密还原图像也具有高质量，且不受载体图像的影响，具有强适用性。

为进一步说明本文嵌入算法具有高嵌入率和含密还原图像质量，与不同算法进行对比，如表4。

表4　不同算法的嵌入率和对应含密还原图像的PSNR对比

Table 4　Comparison of the maximum embedding rate of different algorithms and PSNR of restore contains secret images

Carrier images	Embedding rate/bpp					PNSR/dB				
	Literature [7]	Literature [8]	Literature [11]	Literature [12]	This Paper	Literature [7]	Literature [8]	Literature [11]	Literature [12]	This Paper
Lena	1.412 2	0.5	1.985 3	8	32	46.12	46.37	44.19	35.86	47.61
Airplane	1.696 5	0.5	2.318 4	8	32	43.27	46.45	41.09	35.18	47.29
Barbara	0.855 5	0.5	1.457 4	8	32	49.85	40.22	45.31	35.32	48.53
Baboon	0.290 2	0.5	0.581 0	8	32	56.42	29.74	53.49	35.49	47.05
Man	1.387 4	0.5	1.734 2	8	32	45.43	44.86	45.23	35.47	48.44
Cameraman	1.641 9	0.5	1.618 3	8	32	43.84	43.42	45.36	35.43	49.21
Average	1.063 6	0.5	1.615 8	8	32	47.49	41.84	45.78	35.46	48.02

由表4可知，本文隐藏算法的嵌入率更高，获得含密还原图像质量更好；在平均嵌入率分别是文献[7，8，11]的30、60、19倍情况下，含密还原图像PSNR也均高0.53 dB左右。同时与光学水印技术[12]相比PSNR高12.56 dB左右。说明本文算法在高嵌入率下具有更好的解密图像质量。

3.2.3　缩小倍数分析

本文将隐藏图像光强进行缩小，可减小其对载体图像的影响。图10为在不同嵌入率下不同缩小倍数的含密还原图像的PSNR。

如图10所知，同一嵌入率下，其含密还原图像的PSNR随着缩小倍数的增加而增加。说明较大的缩小倍数有利用提高载体图像嵌入率。故本文选取缩小1 000倍。

光强缩小后，若载密图像进行量化处理，产生的误差必然影响后续还原过程。本文利用嵌入率为

128 bpp下不同缩小倍数的载密图像经8-bit量化处理后各还原图像的PSNR表示，如图11所示。开始嵌入载体密文中的数值都为大数值，随着缩小倍数的增加，数值逐渐变为小数值，对载体加密图像的影响急速降低；当增加到一定程度，由于嵌入数据较小，在经8-bit量化时存在四舍五入问题，使影响具有波动性；因此含密还原图像的PNSR值整体表现为先增加后降低最后趋于平缓。在矢量分解中各光振幅不随缩小倍数改变，既公式(6)中φ_1，φ_2只与φ有关；当缩小倍数增加时，经8-bit量化处理后φ变化逐渐变小，因此还原隐藏图像与还原图像的PNSR值逐渐增加。

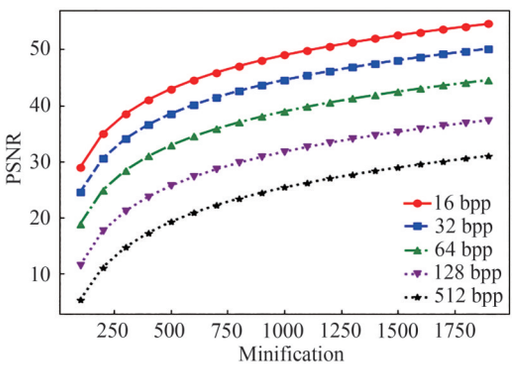


图10 缩小倍数分析结果

Fig. 10 Results of reduction multiple analysis

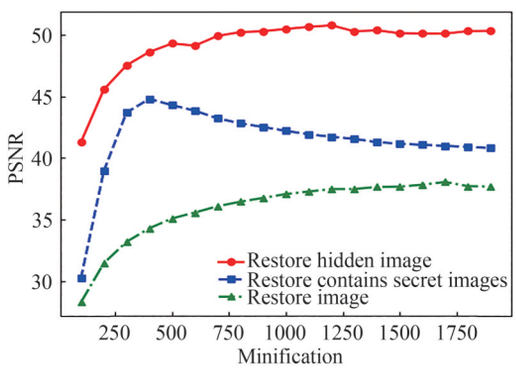
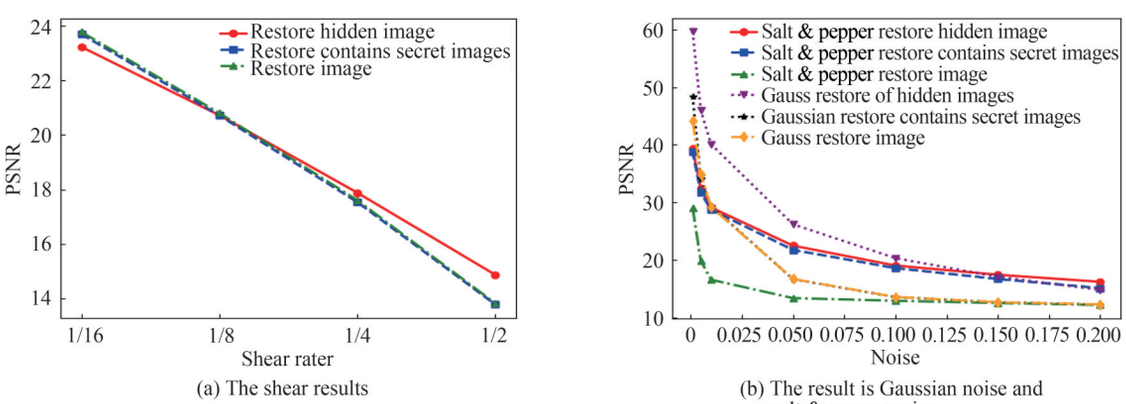


图11 量化处理分析结果

Fig. 11 Quantitative analysis results

3.2.4 鲁棒性分析

将隐藏图像嵌入载体加密图像中，若载密图像被污染或剪切必然会对解密图像和还原隐藏图像产生影响。为验证干涉可逆信息隐藏的鲁棒性，本文选择嵌入率为32 bpp下，不同噪声与剪切的情况下各还原图像的PNSR值来体现。PNSR越大，鲁棒能力越好。实验结果如图12所示。



(a) The shear results

(b) The result is Gaussian noise and salt & pepper noise

图12 鲁棒性分析结果

Fig. 12 Robust analysis results

由图12(a)可知，各还原图像PNSR值随剪切率增加而减小；当剪切1/2时，各图像PNSR值仍在14 dB附近；当剪切率相同时，各图像PNSR值相近，验证了算法的良好抗剪切能力。由图12(b)可知，各还原图像PNSR值随着噪声增加而减小；当各种噪声达0.2时，各图像PNSR值仍大于11 dB；噪声相同时，不同噪声的还原隐藏图像PNSR值最大。并且椒盐还原图像与椒盐还原隐藏图像的PNSR值相近，高斯还原图像与高斯含密还原图像的PNSR值相近。说明本文隐藏算法具有良好抗噪声能力，椒盐噪声对含密还原图像影响较大，高斯噪声对还原图像影响较小。综上本文隐藏算法具有良好的鲁棒性。

3.3 多图像数据报重组鲁棒性分析

多图像数据报重组是将图像种类、尺寸以及数量信息放入校验区中，进而无需额外信息重构多图像，若校验区被污染或剪切必会影响重构。为验证多图像数据报重组鲁棒性，本文只进行多图像数据报重组，并

在不同噪声与剪切下看是否能够重构。实验结果如表5所示。

表5　多图像数据报重组鲁棒性分析结果

Table 5　Robust analysis results of multi-image datagram reconstruction

Crop	Can reconstruct	Gaussian noise	Can reconstruct	Salt & pepper noise	Can reconstruct
200×200(Not cut to check area)	Yes	0.001	Yes	0.01	Yes
400×400(Not cut to check area)	Yes	0.002	Yes	0.1	Yes
99×99(Cut to check area)	Yes	0.003	Yes	0.25	Yes
100×100(Cut to check area)	No	0.004	No	0.26	No

由表5可知,未剪切到校验区时未导致图像信息丢失,因此能够重构。剪切到校验区时,由于剪切按块进行,当校验区各区长度大于剪切块长度时,各区有正确值,可取到正确值重构多图像;反之会导致校验区中存在信息全部丢失的小区,使算法无法重构。本文校验区各区长度为100,故剪切长度超过99时无法重构。当高斯噪声为0.003或椒盐噪声为0.25时,校验区中各小区存在未修改的值及各分隔区一半为零,故可重构。综上可见多图像数据报重组具有一定鲁棒性。

3.4　噪声分析

上述实验可知,多图像数据报重组及干涉可逆信息隐藏具有一定抗噪声。为验证本文多图像可逆信息隐藏算法的抗噪声,在一定高斯噪声或椒盐噪声下还原图像。实验结果如图13所示。

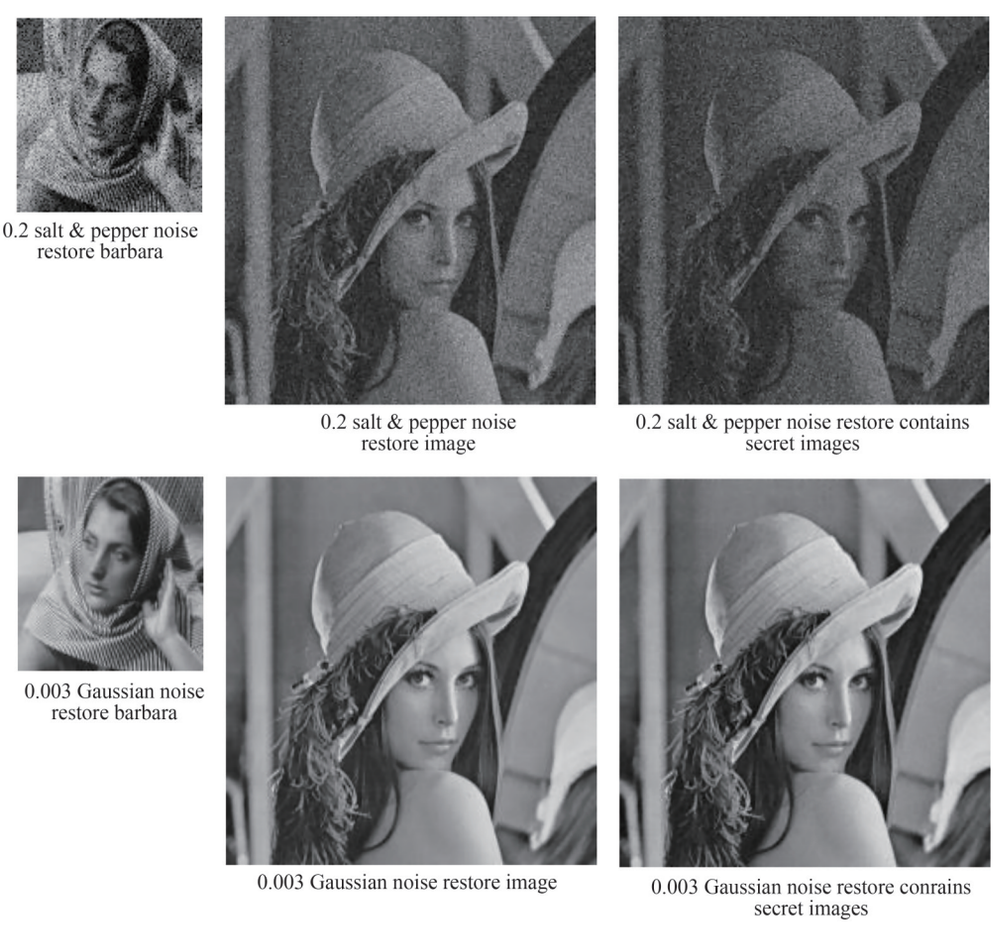


图13　添加噪声还原效果图

Fig.13　Add noise reduction renderings

由图13可知,在0.2的椒盐噪声或0.003的高斯噪声下,算法能够重构;且还原Barbara、还原图像及含密还原图像都能清晰可见,说明算法具有一定抗噪声。

3.4 运行时间分析

密文域可逆信息隐藏包含载体所有者、信息隐藏者、隐藏信息接收者和载体接收者四方以不同嵌入率分析四方所用时间，结果如表6。

表6 不同嵌入率下各所有者所用时间(s)

Table 6 Time spent by each owner at different embedding rates(s)

Embedding rate	Carrier owner	Information hider	Hidden information receiver	Carrier receiver
16 bpp	0.496 7	0.213 4	0.746 0	0.807 8
32 bpp	0.496 9	0.442 8	1.492 0	1.555 8
64 bpp	0.495 7	0.849 7	2.930 1	2.996 9
128 bpp	0.496 6	1.655 5	5.883 2	5.947 1
512 bpp	0.497 6	3.298 1	11.708 6	11.771 5

由表6可知，不嵌入率下载体所有者加密时间接近，信息隐藏者嵌入信息时间、隐藏信息接收者提取信息、时间和载体接收者提取解密时间随嵌入率的增加成倍增加。当嵌入率为32 bpp时，各用户所用时间小于2 s，嵌入信息时间低于0.5 s，说明本文算法的信息嵌入快，整体具有高效性。

4 结论

基于光学干涉原理，提出一种密文光学多图像可逆信息隐藏。多张不同类型图像经数据报重组得到重组多图像，无需额外信息可在一定噪声下重构多图像。载体图像经非对称双随机相位编码加密，使载体密文更加适应级联干涉，再将重组多图像光强缩小1 000倍级联干涉隐藏于载体密文中，可利用级联矢量分解无损恢复。实验验证，当嵌入率为128 bpp时，在人眼视觉下加密图像无明显改变，本文算法具有高嵌入率、高效性、完全可逆、可分离以及良好的鲁棒性。

参考文献

[1] WU Youyou, GUO Yutang, TANG Jin, et al. A reversible ciphertext information hiding algorithm based on adaptive Huffman coding [J]. Chinese Journal of Computers, 2021, 44(4): 846-858.
吴友情, 郭玉堂, 汤进, 等. 基于自适应哈夫曼编码的密文可逆信息隐藏算法[J]. 计算机学报, 2021, 44(4): 846-858.

[2] WANG Jijun, LI Guoxiang, XIA Guoen, et al. Image interpolation space fully reversible separable ciphertext field information hiding algorithm [J]. Acta Electronica Sinica, 2020, 48(1): 92-100.
王继军, 李国祥, 夏国恩, 等. 图像插值空间完全可逆可分离密文域信息隐藏算法[J]. 电子学报, 2020, 48(1): 92-100.

[3] PUTEAUX P, PUECH W. An efficient MSB prediction-based method for high-capacity reversible data hiding in encrypted images[J]. IEEE Transactions on Information Forensics and Security, 2018, 13(7): 1670-1681.

[4] YI P, YIN Z, QIAN Z. Reversible data hiding in encrypted images with two-MSB prediction[C]. Proceedings of the 2018 IEEE International Workshop on Information Forensics and Security (WIFS), Hong Kong, China, 2018.

[5] GUAN B, XU D. An efficient high-capacity reversible data hiding scheme for encrypted images[J]. Journal of Visual Communication and Image Representation, 2019, 66 : 102744.

[6] LI X, ZHOU X, ZHOU Q, et al. High-capacity reversible data hiding in encrypted images by information preprocessing[J]. Complexity, 2020, 6: 1-12.

[7] CHEN K. High capacity reversible data hiding based on the compression of pixel differences[J]. Mathematics, 2020, 8(9): 1435.

[8] ZHANG R, LU C, LIU J. A high capacity reversible data hiding scheme for encrypted covers based on histogram shifting[J]. Information Security Technical Report, 2019, 47(8): 199-207.

[9] WU Y, XIANG Y, GUO Y, et al. An improved reversible data hiding in encrypted images using parametric binary tree labeling[J]. IEEE Transactions on Multimedia, 2020, 22(8): 1929-1938.

[10] WENG S, ZHANG C, ZHANG T, et al. High capacity reversible data hiding in encrypted images using SIBRW and GCC[J]. Journal of Visual Communication and Image Representation, 2020, 75: 102932.

[11] MALIK A, HE P, WANG H, et al. High-capacity reversible data hiding in encrypted images using multi-layer embedding[J]. IEEE Access, 2020, 8: 148997-149010.

[12] LV W, SUN X, YANG D, et al. Optical multiple information hiding via azimuth multiplexing[J]. Optics and Lasers in Engineering, 2021, 141: 106574.

[13] YE Z, QIU P, WANG H, et al. Image watermarking and fusion based on Fourier single-pixel imaging with weighed light source[J]. Optics Express, 2019, 27(25): 36505-36523.

[14] GANG Q A, XM A, XY A, et al. Optical color watermarking based on single-pixel imaging and singular value decomposition in invariant wavelet domain - ScienceDirect[J]. Optics and Lasers in Engineering, 2020,137(4): 106376.

[15] GUO Yuan, ZHOU Yanyan, JING Shiwei. Multi-image encryption based on image reconstruction and bit scrambling[J]. Acta Photonica Sinica, 2020, 49(4): 0410002.
郭媛, 周艳艳, 敬世伟. 基于图像重组和比特置乱的多图像加密[J]. 光子学报, 2020, 49(4): 0410002.

[16] GUO Yuan, JING Shiwei. Lossless compressed optical image encryption based on L-L cascading chaos and vector decomposition [J]. Acta Photonica Sinica, 20, 49(7): 0710002.
郭媛, 敬世伟. 基于L-L级联混沌与矢量分解的无损压缩光学图像加密[J]. 光子学报, 2020, 49(7): 0710002.

Foundation item: National Natural Science Foundationof China (No. 61872204), Natural Science Foundationof Heilongjiang Province, (No.LH2021F056), Heilongjiang Provincial Institutions of Higher Learning Basic Scientific Research Funds Scientific Research Project (No. 1355091130), Postgraduate Research Project Postgraduate Innovation Research Project (No.YJSCX20200050)