引用格式：YUAN Sheng, WANG Zhen, ZHOU Xin, *et al*. Blind Watermarking Method Based on Binarized Computational Ghost Imaging[J]. *Acta Photonica Sinica*, 2020, **49**(2): 0210003
袁胜,王真,周昕,等.基于二值化计算鬼成像的盲水印方法[J].光子学报,2020,**49**(2):0210003

基于二值化计算鬼成像的盲水印方法

袁胜[1],王真[1],周昕[2],邴丕彬[1]
(1 华北水利水电大学 物理与电子学院,郑州 450046)
(2 四川大学 电子信息学院,成都 610065)

摘 要:提出了一种基于二值化计算鬼成像的盲水印方法.首先将水印图像经计算关联成像加密系统加密,并将加密数据二值化,然后将其隐藏到宿主图像的离散余弦变换域,实现水印信息的嵌入.水印信息的提取和重建是隐藏和加密的逆过程,分别借助提取密钥和解密密钥获取水印信息.仿真实验证明,该方法具有很好的隐蔽性,在嵌入因子 $\alpha=10$ 时,嵌入水印仍具有较好的不可感知性,含水印图像的峰值信噪比在 38 dB 以上;另外,该方法也具有一定的容错能力,提取的加密数据错误率达 20%时,重建的水印信息仍能分辨和识别;与传统的计算鬼成像相比,加密数据的二值化为水印嵌入提供了方便,但是并未对重建图像带来严重恶化,其相关系数相差不足 0.1;水印信息的提取无需借助原始宿主图像,是一种盲提取方法.

关键词:光学信息安全;光学加密;盲水印;计算鬼成像;离散余弦变换
中图分类号:O438 **文献标识码**:A **doi**:10.3788/gzxb20204902.0210003

Blind Watermarking Method Based on Binarized Computational Ghost Imaging

YUAN Sheng[1], WANG Zhen[1], ZHOU Xin[2], BING Pi-bin[1]
(1 *College of Physics and Electronics, North China University of Water Resources and Electric Power, Zhengzhou* 450046, *China*)
(2 *College of Electronics and Information Engineering, Sichuan University, Chengdu* 610065, *China*)

Abstract: A blind watermarking method based on binarization computational ghost imaging was proposed. In this method, a watermark image is firstly encoded by the encryption system based on computational ghost imaging, and then the ciphertext is binarized and embedded in the discrete cosine transform domain of a host image to realize watermark embedding. The process of watermark extraction and reconstruction is the inverse process of embedding and encryption. The watermark is obtained by extraction key and decryption key. Simulation results show that this watermarking technique has good imperceptibility. When $\alpha=10$, the watermark is also imperceptible and the peak signal-to-niose ratio of the host image containing watermark is above 38 dB. In addition, this method also has some fault tolerance ability. When the error rate of the extracted encrypted data reaches 20%, the reconstructed watermark information can still be distinguished and recognized. Compared with the traditional computational ghost imaging, binarization for the ciphertext data brings convenience for watermark embedding, but does not bring serious deterioration to reconstructed image, and the difference of correlation coefficient is less than 0.1.

基金项目:国家自然科学基金(Nos. 61475104, 61601183, 51609086, 61205003),河南省科技攻关计划(Nos. 182102310731, 192102210081),河南省高等学校重点研发计划(No. 19A510003)
第一作者:袁胜(1979—),男,副教授,博士,主要研究方向为光学成像和光学信息安全. Email:shn.yuan@sohu.com
收稿日期:2019-10-06;**录用日期**:2019-12-02

In the process of watermark extraction, it is unnecessary for the original host image, so it belongs to a blind extraction method.

Key words: Optical information security; Optical encryption; Blind watermarking; Computational ghost imaging; Discrete cosine transformation

OCIS Codes: 100.3010; 060.4785; 110.1758; 110.6150

0 引言

近年来,随着计算机计算速度的不断提高以及现代网络和通信技术的迅猛发展,完全依赖于密码学和电子信息系统的传统信息安全技术面临日益严峻的挑战.然而与之相比,基于光学理论和方法的信息安全技术具有快速并行数据处理能力、多维度、大容量、高鲁棒性、大密钥空间等独特优势.自从 1995 年美国康涅狄格大学科学家 REFREGIER P 等[1]提出基于光学 4f 系统的双随机相位编码技术以来,光学信息安全技术已成为信息安全领域的研究热点[2,3].经过二十多年的发展,基于双随机相位编码的信息安全技术经受了各种各样的攻击[4],因此也不断涌现出许多新的光学信息安全技术[5-8].

目前,大多数基于双随机相位编码的信息安全技术都将实数明文图像加密为复值图像,为密文的传输和分发带来不便.近来兴起的基于计算鬼成像(Computational Ghost Imaging, CGI)的图像加密技术能够将二维图像加密为一维实值数据,极大地压缩了密文的数据量.之后,研究人员对此产生了浓厚的兴趣,并相继提出了多种基于计算鬼成像的图像加密方案[9-12].但是后续研究表明,仅仅依托于计算鬼成像的图像加密系统仍为线性系统,该系统难以抵抗选择明文攻击[13].最近,WANG Le[14]和 SUI Lian-sheng[15]又相继提出了基于计算鬼成像的信息隐藏技术,这些技术隐蔽了收发双方通信的存在,提高了信息传输的安全性.然而基于空域的信息隐藏技术难以抵抗滤波等攻击,基于频域的信息隐藏技术难以做到盲提取.

针对上述问题本文提出了一种基于二值化计算鬼成像(Binarized Computational Ghost Imaging, BCGI)的盲水印隐藏方法.该方法首先将水印图像利用计算鬼成像系统进行加密,然后对加密数据二值化,借助于两个随机序列(嵌入密钥(Embedding key))将其隐藏于宿主图像(Host image)的离散余弦变换(Discrete Cosine Transformation, DCT)域.仿真实验证明加密数据的二值化极大地压缩了密文的数据量,但并未对解密图像带来严重恶化,这为水印隐藏提供了方便.最后,借助于嵌入密钥提取秘密信息,利用计算鬼成像方法重建水印图像.计算鬼成像中的随机相位板(加密密钥(Encryption key))和嵌入密钥作为该信息隐藏方法的双重密钥保证了水印信息的安全.

1 方案与理论分析

1.1 基于计算鬼成像的水印图像加密系统

为了保证水印信息的安全,在水印嵌入之前通常先将水印图像 $w(x,y)$ 进行加密.本文采用基于计算鬼成像的图像加密技术[10],其系统如图 1 所示.

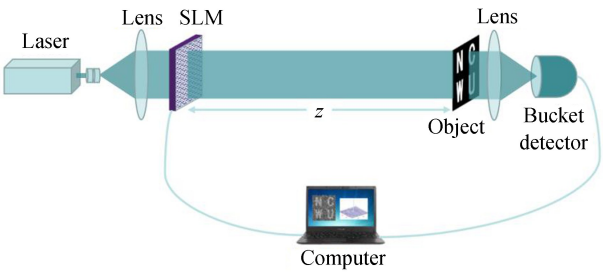


图 1 计算鬼成像加密系统示意图

Fig.1 Schematic diagram of the encryption system based on CGI

由激光器生成的相干光束经空间光调制器(Spatial Light Modulator, SLM)产生的一系列随机相位 $\{\varphi_r(x,y)\}$ 调制,$r=1,2,\cdots,N$,N 为测量次数.调制后的光束经菲涅尔衍射投射到距离为 z 的待测物体 $w(x,y)$(即水印图像)上,然后被单像素(桶)探测器(Single-pixel (or bucket) detector)探测.该过程可表示为

$$C_r=\iint \mathrm{d}x\,\mathrm{d}y I_r(x,y)w(x,y) \tag{1}$$

式中,$\{C_r\}$为探测数据,$I_r(x,y)$表示光束经随机相位板调制后投射到物体上的光强,即

$$I_r(x,y)=\left|\mathrm{FrT}_z[\varphi_r(x,y)]\right|^2 \tag{2}$$

$\mathrm{FrT}_z[\cdot]$表示光场传输轴向距离 z 的菲涅尔衍射变换.

上述基于计算鬼成像的加密系统以 SLM 产生的随机相位$\{\varphi_r(x,y)\}$作为加密密钥,桶探测器获取光强强度$\{C_r\}$作为密文(Ciphertext),该加密过程如图 2 所示.基于计算鬼成像的图像加密系统具有光学系统独有的快速并行数据处理能力[10],能够将二维图像加密为一维实值序列,具有数据压缩能力.为了便于隐藏,本文涉及的方法进一步将密文$\{C_r\}$二值化,即

$$B_r=\begin{cases}1 & C_r>T\\ -1 & C_r\leqslant T\end{cases} \tag{3}$$

式中,$T=[\max(C)+\min(C)]/2$ 为阈值,$\max(C)$和 $\min(C)$分别为密文$\{C_r\}$的最大值和最小值.根据 CGI 原理,其解密过程为二值化数据$\{B_r\}$与投射到物平面上的光场强度$\{I_r(x,y)\}$的关联运算,即

$$G(x,y)=\frac{1}{N}\sum_{r=1}^{N}(B_r-\langle B\rangle)(I_r(x,y)-\langle I(x,y)\rangle)=\langle BI(x,y)\rangle-\langle B\rangle\langle I(x,y)\rangle \tag{4}$$

式中,$G(x,y)$为解密图像,$\langle\cdot\rangle$表示取平均值.后续仿真实验证明,密文数据$\{C_r\}$的二值化并未对解密图像带来严重影响.

1.2 基于 DCT 域的水印嵌入方法

相比于空域信息隐藏方法,基于频域的信息隐藏具有较强的抗攻击能力,在 DCT 域的中频部分嵌入水印信息具有较好的隐蔽性和鲁棒性[16-20],且 DCT 系数为实值数据,便于二进制实值水印信息的嵌入,因此本文采用基于 DCT 的水印嵌入方法.设宿主图像为 $\boldsymbol{h}$,将二值化的水印信息 $\boldsymbol{B}_r$ 在其 DCT 域进行隐藏.具体步骤如图 2 所示.

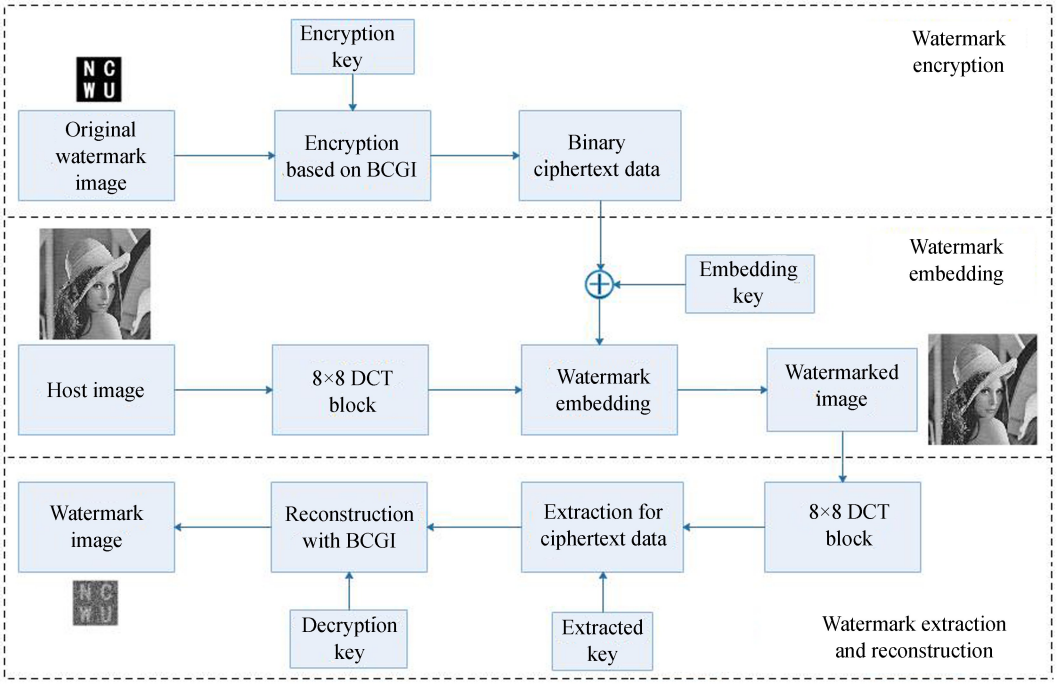


图 2 基于二值化计算鬼成像的水印方法流程图

Fig.2 Flow chart of watermarking method based on BCGI

1)将宿主图像 $\boldsymbol{h}$ 以 8×8 的大小分成 $m\times n$ 块,并对划分出的每一块 $\boldsymbol{h}'$进行 DCT 变换,图像子块的 DCT 系数为 $\boldsymbol{H}'(i,j)=\mathrm{DCT}\{h'\}$,$1\leqslant i,j\leqslant 8$;

2)提取加密水印信息的一维实值数据 $\boldsymbol{B}_r$,将其转换为 $m\times n$ 的矩阵 $\boldsymbol{S}(m,n)$,即每一个数据对应于宿主图像的每一个 8×8 子块;

3)产生两个含有 8 个元素的随机数列 k_1、k_2 作为嵌入密钥,将其以一定权重叠加到宿主图像每个 8×8 图像子块的中频 DCT 系数(即 45°对角线上的 8 个元素,$\boldsymbol{H}'(i,j)$,$i+j=9$)中.叠加规则为

$$\boldsymbol{H}''(i,j)=\begin{cases}\boldsymbol{H}'(i,j)+\alpha k_1(i) & \boldsymbol{S}(m,n)=1 \text{ and } (i+j)=9\\ \boldsymbol{H}'(i,j)+\alpha k_2(i) & \boldsymbol{S}(m,n)=-1 \text{ and } (i+j)=9\\ \boldsymbol{H}'(i,j) & i+j\neq 9\end{cases} \tag{5}$$

式中,α 为尺度因子,控制水印添加的强度,决定了频域系数被修改的幅度,$\boldsymbol{H}'$ 和 $\boldsymbol{H}''$ 分别为嵌入水印前后的 DCT 系数,k_1、k_2 为选择的随机数列.

4)将嵌入信息的 DCT 系数进行二维 DCT 逆变换,得到含水印图像 $\boldsymbol{h}_w$,完成加密水印信息的隐藏.

1.3 水印提取和重建方法

水印的提取和重建是嵌入和加密的逆过程(如图 2(c)所示),具体实现过程为

1)将嵌入水印的宿主图像 $\boldsymbol{h}_w$ 进行 8×8 分块,并对每个图像子块 $\boldsymbol{h}_w'$ 进行 DCT 变换,图像子块的离散余弦变换系数为 $\boldsymbol{H}_w'=\mathrm{DCT}\{\boldsymbol{h}_w'\}$.

2)读取每一个 8×8 图像子块的离散余弦系数 $\boldsymbol{H}_w'$,提取图像子块的 8 个中频段系数,记为 $\boldsymbol{p}$.将 $\boldsymbol{p}$ 与嵌入密钥 k_1,k_2 序列进行相关运算,通过比较相关系数的大小提取二值化加密信息 $\boldsymbol{S}'(m,n)$,即

$$\boldsymbol{S}'(m,n)=\begin{cases}1 & \mathrm{CC}(\boldsymbol{p},k_1)>\mathrm{CC}(\boldsymbol{p},k_2)\\ -1 & \mathrm{CC}(\boldsymbol{p},k_1)<\mathrm{CC}(\boldsymbol{p},k_2)\end{cases} \tag{6}$$

式中,CC 表示两个序列(或图像)的相关系数,即 $\mathrm{CC}=E\{[\boldsymbol{p}-E(\boldsymbol{p})]-[k-E(k)]\}/\sigma_p\sigma_k$.$E\{\cdot\}$ 为数学期望,σ 为标准差,CC 的值越大,表示两个序列(或图像)的相似度越高.

3)利用计算鬼成像加密系统的解密密钥 $\{I_r\}$ 与提取的二值化加密信息 $\boldsymbol{S}'(m,n)$ 进行关联运算(如式(4)所示),完成水印图像的重建.

从上述过程可以看出,水印的提取和重建仅仅需要借助密钥和嵌入水印的宿主图像,而无需原始宿主图像,是一种盲提取方法.

2 仿真实验结果及分析

2.1 CGI 与 BCGI 加解密性能比较

为了定量评价图像质量,本文引入了峰值信噪比(Peak Signal-to-Noise Ratio, PSNR)来评价水印不可感知性的好坏.PSNR 的计算公式为

$$\mathrm{PSNR}=20\times\log_{10}\left(\frac{M\times(2^n-1)}{\sqrt{\sum\left(\boldsymbol{H}'(x,y)-\boldsymbol{H}(x,y)\right)^2}}\right) \tag{7}$$

式中,n 为图像像素灰度值的 bit 位,$\boldsymbol{H}(x,y)$ 和 $\boldsymbol{H}'(x,y)$ 分别表示原始图像和改变后的图像,M 为图像的像素数.PSNR 越大,说明图像失真程度越低,水印的不可感知性越好.

此外,本文还引入了非线性相关(NC)运算检测水印是否存在.非线性相关运算定义为

$$\mathrm{NC}(x,y)=\left|\mathrm{IFT}\left[\frac{\{\mathrm{FT}[G(x,y)]\}\{\mathrm{FT}[w(x,y)]\}}{|\{\mathrm{FT}[G(x,y)]\}\{\mathrm{FT}[w(x,y)]\}|^{1-\rho}}\right]\right|^2 \tag{8}$$

式中,FT[·]和 IFT[·]分别代表二维傅里叶变换与反变换,ρ 为非线性强度.

仿真中,光波波长 $\lambda=632.8$ nm,SLM 与物平面的轴向距离 $z=50$ cm.物平面的水印图像分别采用 64×64 像素的二值图(Binary Image, BI)“NCWU”(图 3(a))和灰度图(Grayscale Image, GI)“Panda”(图 3(f)),然后进行 4096 次加密采样,CGI 和 BCGI 的加密结果如图 3(b)、(c)和(g)、(h)所示.从图 3(d)、(e)和(i)、(j)所示的解密结果可以看出,与 CGI 解密结果相比,二值化并未对解密图像带来严重恶化.当然与 CGI 相同,BCGI 的重建图像质量也与测量次数有关(如图 4 所示),测量次数越多,CC 越大,重建图像越清晰.

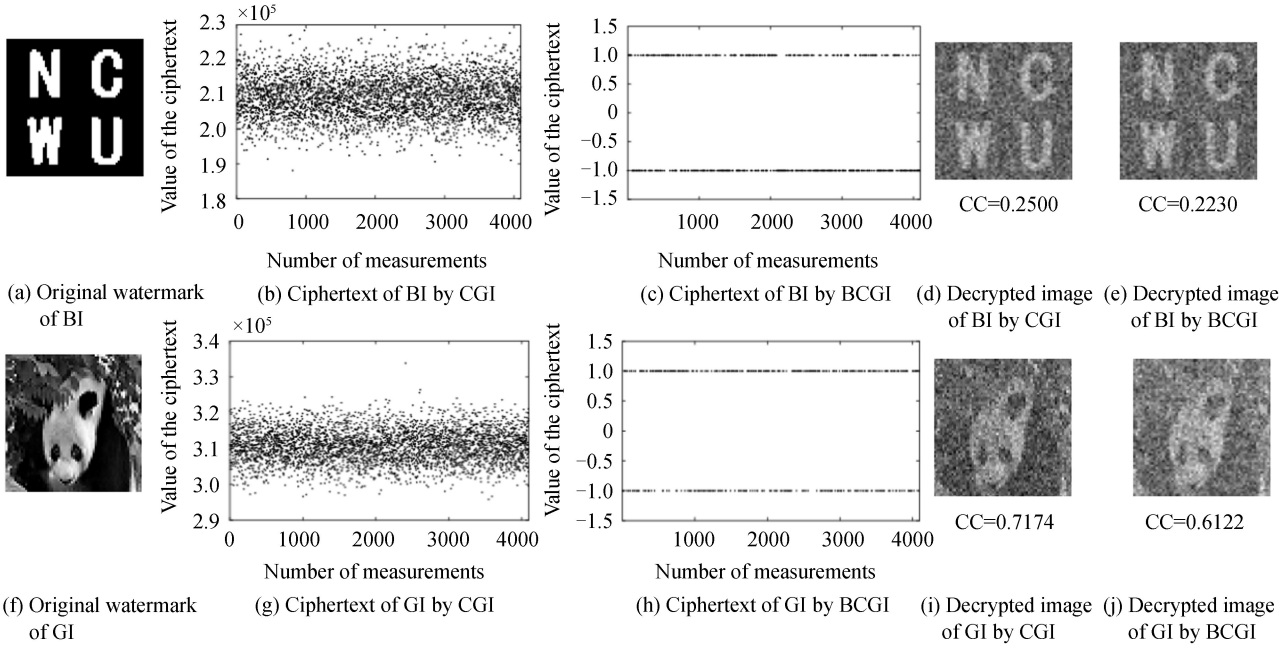


图 3　水印图像的计算鬼成像和隐藏重建结果

Fig.3　Retrieved watermark images by CGI, BCGI and hiding technique

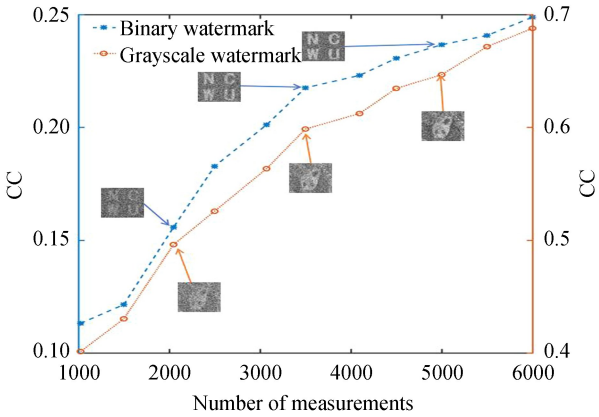


图 4　BCGI 重建水印图像的相关系数(CC)随采样次数变化关系

Fig.4　Plot of CCs of the retrieved watermark by BCGI varying with the number of measurements

2.2　隐藏效果分析

由式(5)和(6)可知,嵌入尺度因子 α 的大小对水印的不可感知性和密文信息的提取结果有重要影响.为了进行定性分析,本文以二值图“NCWU”为例,测试了嵌入水印图像的 PSNR 和解密图像的 CC 值随尺度因子 α 的变化趋势(如图 5 所示).仿真中用 PSNR 衡量水印的不可感知性,用 CC 大小衡量重建水印图像质量的好坏,宿主图像如图 6(a)所示.结果表明尺度因子越大,解密图像越清晰,但隐藏信息的不可感知性越差.已有的实验证明,当嵌入水印图像的 PSNR 达到 38 dB 以上时,嵌入信息具有较好的不可感知性[21].为了满足这一条件,本文选用嵌入因子 $\alpha=10$.

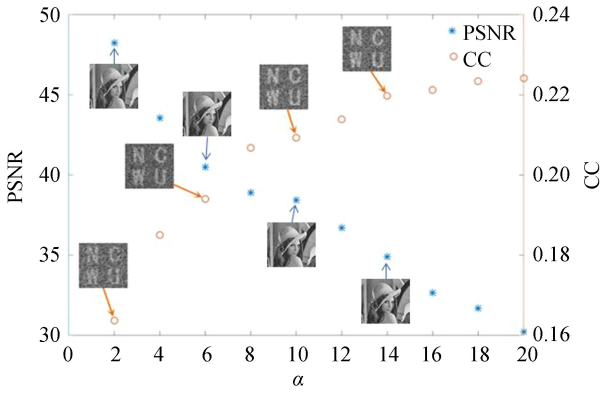
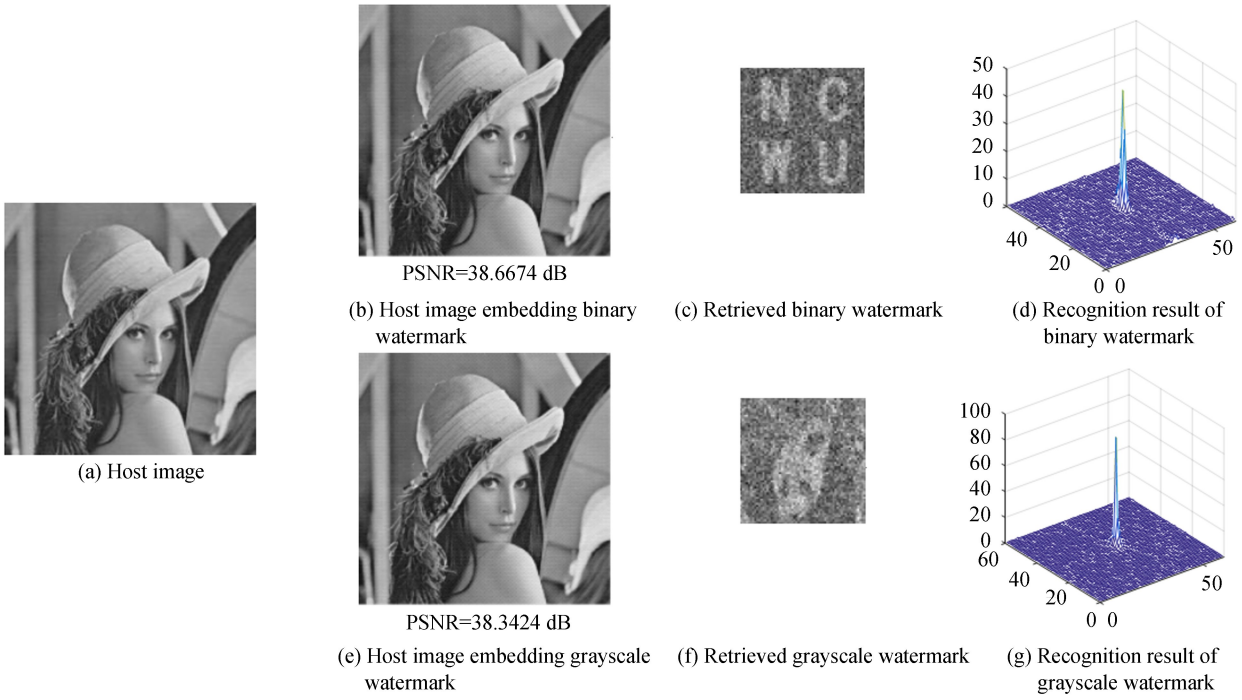


图 5　嵌入水印宿主图像的 PSNR 随嵌入因子的变化关系

Fig.5　Plot of PSNRs of the embedding images varying with different embedding factors



(a) Host image

(b) Host image embedding binary watermark

(c) Retrieved binary watermark

(d) Recognition result of binary watermark

(e) Host image embedding grayscale watermark

(f) Retrieved grayscale watermark

(g) Recognition result of grayscale watermark

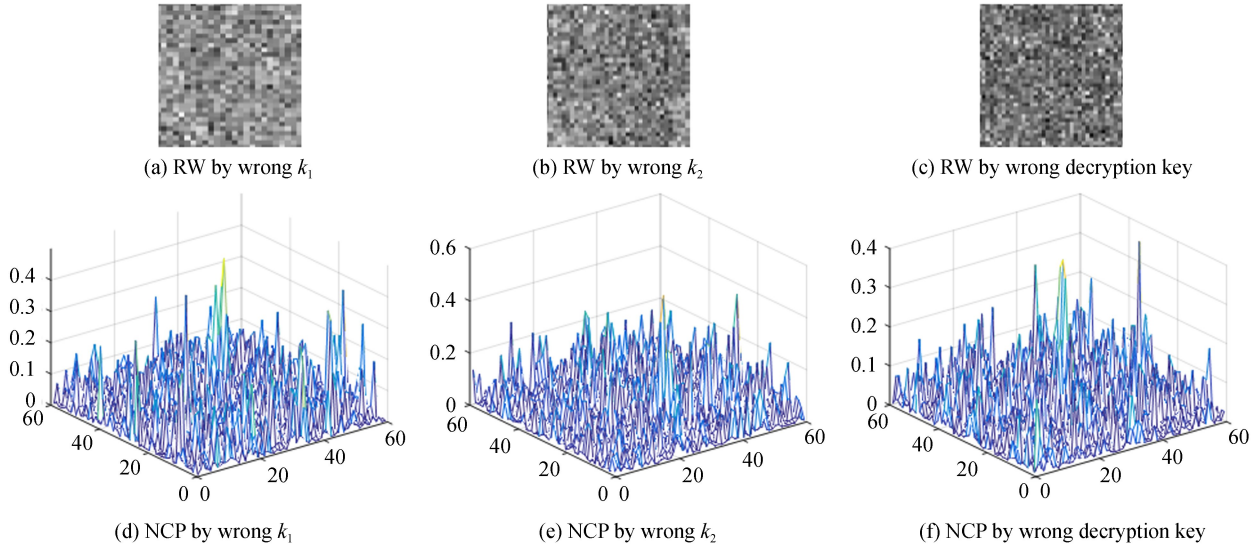
图 6 二值与灰度水印图像的隐藏和提取结果

Fig.6 Results of hiding and extraction for binary and grayscale watermarks

随后，将二值化后的两组加密数据分别嵌入到宿主图像的离散余弦变换域中进行隐藏，嵌入水印的宿主图像如图 6(b)和(e)所示，直观上看宿主图像并无明显变化，秘密信息具有较好的不可感知性，其峰值信噪比(PSNR)分别为 38.667 4 dB 和 38.342 4 dB.重建水印图像如图 6(c)和(f)所示，相关系数分别为 0.220 1 和 0.608 8.通过式(8)所示的非线性相关运算，也得到了明显的相关峰，如图 6(d)和(g)所示.

2.3 安全性分析

仍以二值图像“NCWU”为例，测试本文提出水印方法的安全性.水印的提取和重建是嵌入和加密的逆过程，只有准确获知提取密钥 k_1 和 k_2，以及解密密钥 $\{\varphi_r(x,y)\}$，才能重建水印图像.下面测试了任一密钥错误对重建结果的影响.图 7(a)～(c)分别为提取密钥 k_1、k_2 和解密密钥 $\{\varphi_r(x,y)\}$ 错误时恢复的水印图像(Retrived Watermark，RW)，图 7(d)～(f)为对应密钥错误时水印图像的非线性相关峰(Nonlinear Correlation Peak，NCP).以上仿真结果表明系统中任一密钥错误时都无法重建水印图像，且恢复的水印与



(a) RW by wrong k_1

(b) RW by wrong k_2

(c) RW by wrong decryption key

(d) NCP by wrong k_1

(e) NCP by wrong k_2

(f) NCP by wrong decryption key

图 7 错误密钥下重建的水印图像和识别结果

Fig.7 Retrieved watermarks and authentication results when the key is wrong

原图的非线性相关运算也没有产生相关峰,即所有密钥缺一不可,只有全部密钥正确时才能重建和识别水印图像,因此本方法具有较高的安全性.

2.4 鲁棒性分析

对系统的鲁棒性进行测试.对嵌入水印的宿主图像进行不同类型的攻击,如噪声、高斯低通滤波(Gaussian Low-Pass Filtering, GLPF)以及 JPEG 压缩攻击.在恢复机制相同的情况下,重建图像及非线性相关峰如图 8 所示,表 1 给出了上述各种攻击下宿主图像的 PSNR 和恢复水印图像的 CC 值.

图 8(a)为遭受均值为 0,方差为 0.02 的高斯白噪声(Gaussian White Noise, GWN)攻击时嵌入水印的宿主图像,其 PSNR=30.816 2 dB.重构的水印图像如图 8(e)所示,CC=0.201 0,非线性相关峰如图 8(i)所示.图 8(b)为遭受密度为 0.002 的椒盐噪声(Salt & Pepper Noise, SPN)攻击时嵌入水印的宿主图像,其 PSNR=31.204 5 dB.重构的水印图像如图 8(f)所示,CC=0.200 2,非线性相关峰如图 8(j)所示.图 8(c)为嵌入水印的宿主图像经过通频带半径为 0.2 高斯低通滤波后的结果,其 PSNR=32.852 9 dB.重构的水印图像如图 8(g)所示,CC=0.206 5,非线性相关峰如图 8(k)所示.图 8(d)为嵌入水印的宿主图像经压缩因子为 20 的 JPEG 压缩后的结果,其 PSNR=33.601 6 dB.重构的水印图像如图 8(h)所示,CC=0.204 0,非线性相关峰如图 8(l)所示.仿真结果表明即使系统遭受上述攻击,水印信息仍然能够在一定程度上恢复和识别,因此该水印方法能够抵御一定量的攻击,具有较好的鲁棒性.

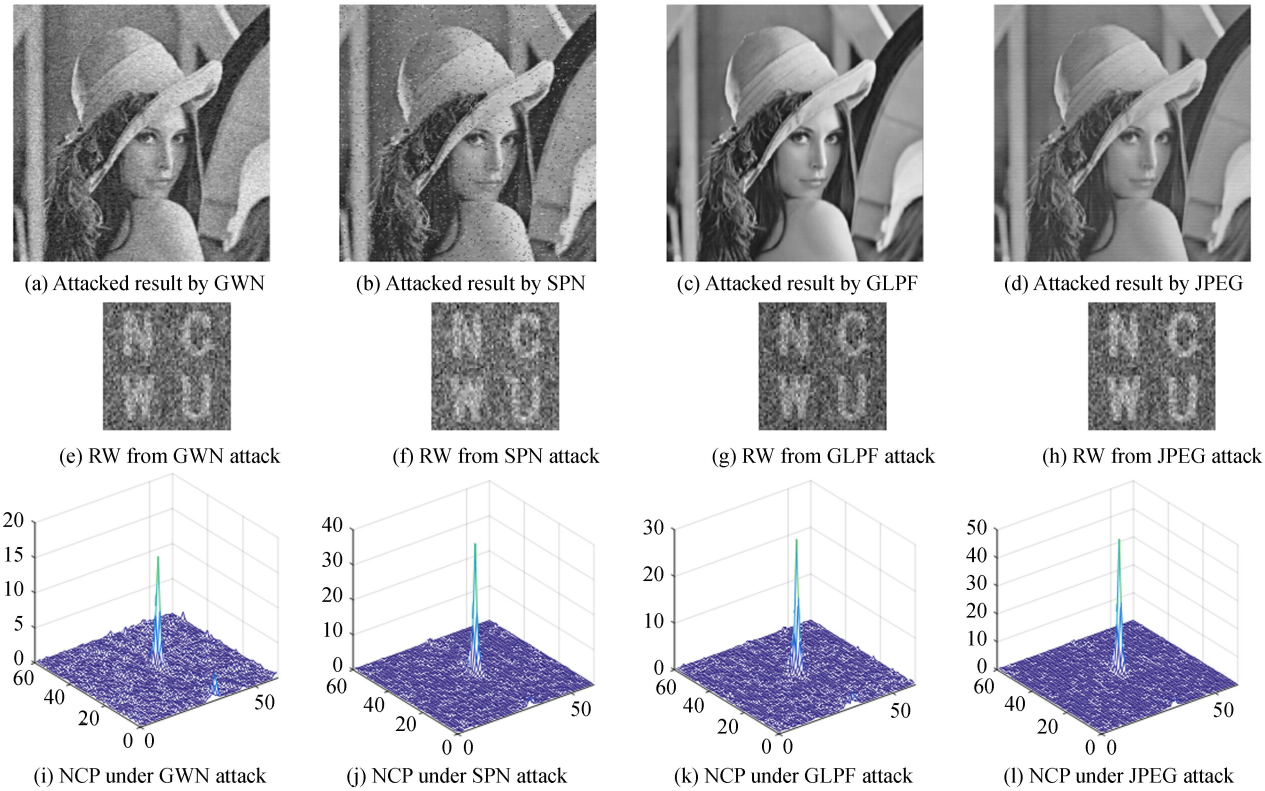


图 8 受到不同攻击的仿真结果

Fig.8 Simulation results of different attacks

表 1 不同攻击下重构水印的 PSNR 和 CC

Table 1 PSNRs and CCs of the retrieved watermarks under several kinds of attacks

Attack	PSNR of the host image embedding watermark/dB	CC of the retrieved watermark image
GWN	30.816 2	0.201 0
SPN	31.204 5	0.200 2
GLPF	32.852 9	0.206 5
JPEG compression	33.601 6	0.204 0

2.5 容错性分析

在水印的嵌入和提取中，存在许多不可预知的外部干扰，导致提取的二值化信息有可能存在异化，这将影响重建水印的图像质量和识别效果.本文对系统的容错性能进行了测试分析.以二值图“NCWU”为例，测试了提取的二值化信息差错率(Error Rate，ER)为 10%、20%、30%和 40%情况下恢复的水印图像及其非线性相关峰，结果如图 9 所示.其中，提取的二值化信息存在 10%错误下重建的水印图像(图 9(a))仍可辨认，其 CC 值为 0.183 5；识别结果(图 9(e))中也具有明显的非线性相关峰.在错误率为 20%和 30%时，重建的水印图像已模糊难辨(如图 9(b)和(c)所示)，CC 值分别只有 0.145 5 和 0.091 1；但是识别结果中仍具有尖锐的相关峰，分别如图 9(f)和(g)所示.当错误率为 40%时，在恢复的图像中已经无法辨认原始的水印信息，且识别结果中几乎不存在非线性相关峰，如图 9(d)和(h)所示.重建水印图像的 CC 值随提取数据错误率的变化趋势如图 10 所示.从上述仿真结果可知，提取的秘密信息部分出现异常(错误率低于大约 20%)时，恢复的水印图像仍可辨认识别.因此，该系统具有一定的容错能力.

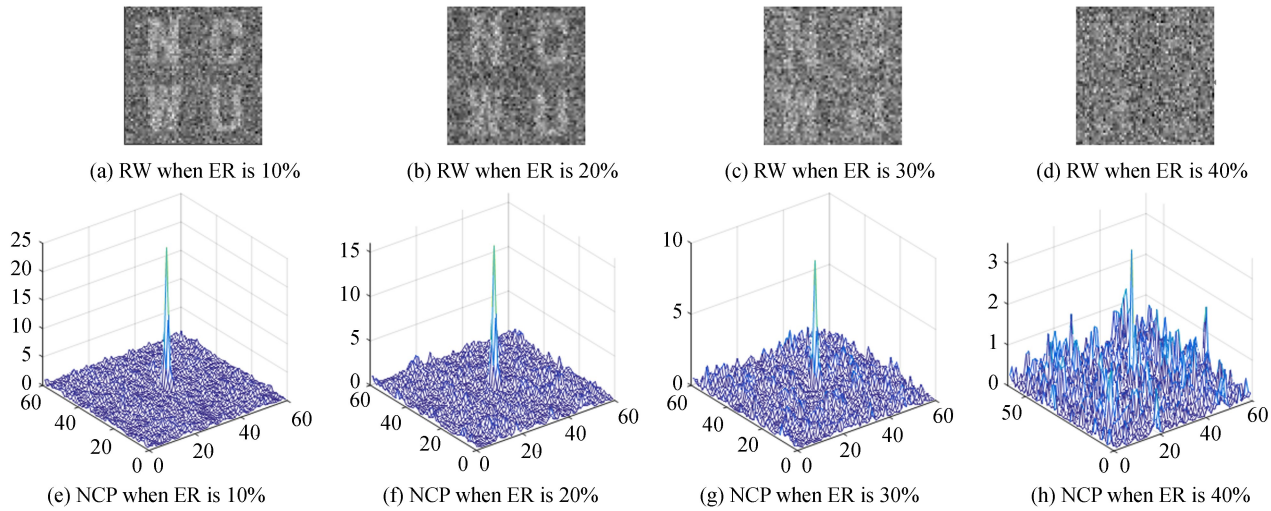


图 9 容错能力分析

Fig.9 Analysis on the capability of fault tolerance

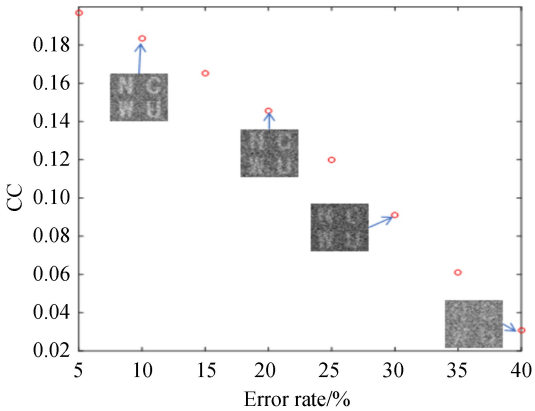


图 10 重建水印图像相关系数(CC)随提取数据错误率的变化图

Fig.10 Plot of CCs of the retrieved watermark images varying with the error rates in the extracted data

3 结论

本文提出了一种基于二值化计算鬼成像的盲水印方法.该方法首先将水印信息经过 CGI 系统进行加密，生成密文，然后为了便于隐藏将密文二值化，压缩了密文的数据量，最后，利用嵌入密钥将二值化的密文数据隐藏于宿主图像的 DCT 域，完成水印的嵌入.仿真结果表明，与 CGI 相比，密文的二值化并未对水印图像的重建带来严重恶化.该水印方案具有双重密钥，任一密钥错误都不能获取水印信息，具有较高的安全性；水印

图像的提取和重建无需借助原始宿主图像，是一种盲提取方法；该方案能够抵抗噪声、滤波、压缩等攻击，具有较好的鲁棒性和容错能力.本文提出的水印方法是一种通用方法，目前已有的许多改善计算鬼成像质量的方法都可用于本文提出的水印方法中，提高水印的重建质量.

参考文献

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

[2] KISHK S, JAVIDI B. Information hiding technique with double phase encoding[J]. *Applied Optics*, 2002, **41**(26): 5462-5470.

[3] WANG Xi, CHEN Wei, CHEN Xu-dong. Fractional Fourier domain optical image hiding using phase retrieval algorithm based on iterative nonlinear double random phase encoding[J]. *Optics Express*, 2014, **22**(19): 22981-22995.

[4] FRAUEL Y, CASTRO A, NAUGHTON T J, *et al*. Resistance of the double random phase encryption against various attacks[J]. *Optics Express*, 2007, **15**(16): 10253-10265.

[5] JIAO Shu-ming, ZHOU Chang-yuan, SHI Yi-shi, *et al*. Review on optical image hiding and watermarking techniques [J]. *Optics and Laser Technology*, 2019, **109**(1): 370-380.

[6] CHEN Wen, JAVIDI B, CHEN Xu-dong. Advances in optical security systems[J]. *Advances in Optics Photonics*, 2014, **6**(2): 120-155.

[7] ZENG Da-kui, MA Li-hong, LIU Jian, *et al*. Amplitude image optical encryption based on two-step-only quadrature phase- shifting interferometry[J]. *Acta Photonica Sinica*, 2012, **41**(1): 72-76.
曾大奎，马利红，刘健，等. 基于两步正交相移干涉的振幅图像光学加密技术[J]. 光子学报，2012，**41**(1)：72-76.

[8] GUO Yuan, XU Xin, JING Shi-wei, *et al*. Virtual optical image encryption method based on Hybrid Chaotic system[J]. *Acta Photonica Sinica*, 2019, **48**(7): 0710002.
郭媛，许鑫，敬世伟，等. 一种混合混沌虚拟光学图像加密方法[J]. 光子学报，2019，**48**(7)：0710002.

[9] LIU Yu-jia, JIANG Zhao-guo, XU Xi-ping, *et al*. Optical watermarking method based on hyper-chaotic phase mask in Gyrator transform domain[J]. *Acta Optica Sinica*, 2019, **39**(9): 0907001.
刘禹佳，姜肇国，徐熙平，等. Gyrator 变换域下基于超混沌相位掩模的光学水印方法[J]. 光学学报，2019，**39**(9)：0907001

[10] BROMBERG Y, KATZ O, SILBERBERG Y. Ghost imaging with a single detector[J]. *Physical Review A*, 2009, **79**(5): 053840.

[11] CLEMENTE P, DURAN V, TAJAHUERCE E, *et al*. Optical encryption based on computational ghost imaging[J]. *Optics Letters*, 2010, **35**(14): 2391-2393.

[12] TANHA M, KHERADMAND R, AHMADIKANDJANI S. Gray-scale and color optical encryption based on computational ghost imaging[J]. *Applied Physics Letters*, 2012, **101**(10): 101108.

[13] JIAO Shu-ming, YANG Gao, TING Lei, *et al*. Known-plaintext attack and ciphertext-only attack for encrypted single-pixel imaging[J]. *IEEE Access*, 2019, **7**(1): 119557-119565.

[14] WANG Le, ZHAO Sheng-mei, CHENG Wei-wen. Optical image hiding based on computational ghost imaging[J]. *Optics Communications*, 2016, **366**(9): 314-320.

[15] SUI Lian-sheng, CHENG Yin, TIAN Ai-ling, *et al*. An optical watermarking scheme with two-layer framework based on computational ghost imaging[J]. *Optics and Lasers in Engineering*, 2018, **107**(8): 38-45.

[16] WANG Shi-qiang, MENG Xiang-feng, YIN Yong-kai, *et al*. Optical image watermarking based on singular value decomposition ghost imaging and lifting wavelet transform[J]. *Optics and Lasers in Engineering*, 2019, **114**(3): 76-82.

[17] ZHANG Xue, MENG Xiang-feng, YIN Yong-kai, *et al*. Two-level image authentication by two-step phase-shifting interferometry and compressive sensing[J]. *Optics and Lasers in Engineering*, 2018, **100**(1): 118-123.

[18] DAS C, PANIGRAHI S, SHARMA V K, *et al*. A novel robust image watermarking in DCT domain using inter-block coefficient correlation[J]. *International Journal of Electronics and Communications*, 2014, **68**(3): 244-253.

[19] ROY S, PAL A K. A blind DCT based color watermarking algorithm for embedding multiple watermarks[J]. *AEU-International Journal of Electronics and Communications*, 2017, **72**(2): 149-161.

[20] HU Gao-ping, WEI Jia, TANG Yi. An improved frequency domain digital watermarking algorithm based on DCT transform[J]. *Journal of Communication University of China (Science and Technology)*, 2018, **25**(6): 19-27.
胡高平，魏佳，汤艺. 一种基于 DCT 变换的频域数字水印改进算法[J]. 中国传媒大学学报(自然科学版)，2018，**25**(6)：19-27.

[21] 王朔中，张新鹏，张开文. 数字密写与密写分析[M]. 北京：清华大学出版社，2005.

Foundation item: National Natural Science Foundation of China (Nos. 61475104, 61601183, 51609086, 61205003), Science and Technology Department Henan Province (Nos. 182102310731, 192102210081), Project Plan of Key Scientific Research in University of Henan Province (No.19A510003)