基于像素不扩展视觉密码的光学彩色脆弱水印*

刘睿泽[1)] 祝玉鹏[2)3)] 周新隆[2)] 米沼锞[1)] 吴承哲[1)]
秦俏华[1)] 柯常军[3)] 史祎诗[2)3)†]

1) (河北工程大学数理科学与工程学院, 邯郸 056038)

2) (中国科学院大学光电学院, 北京 100049)

3) (中国科学院空天信息创新研究院, 北京 100094)

(2023 年 10 月 16 日收到; 2024 年 4 月 28 日收到修改稿)

本文提出了一种基于像素不扩展视觉密码的光学彩色脆弱水印系统. 一方面, 使用像素不扩展视觉密码对水印图像进行编码, 避免了因视觉密码引起的像素扩展问题, 使得后续可以选择与水印图像具有相同像素大小的彩色宿主图像, 大大减少了传输过程中所占用的网络带宽以及存储空间. 另一方面, 使用相位恢复算法对编码后水印图像进行处理得到用于嵌入宿主图像的相位信息, 以光学的方式进一步提高水印图像的安全性. 使用计算机模拟验证所提光学彩色脆弱水印的可行性、不可感知性, 并通过一系列仿真攻击实验验证所提水印具有良好的脆弱性, 在面对噪声污染以及旋转、运动模糊处理、滤波等常见的攻击下均可灵敏地检测出图像发生了篡改.

关键词: 光学彩色脆弱水印, 像素不扩展视觉密码, 相位恢复算法, 篡改检测

PACS: 42.30.–d, 42.30.Va, 42.30.Rx **DOI:** 10.7498/aps.73.20231652

1 引 言

近年来, 随着计算机技术的不断发展, 为人们获取图像信息带来了便利, 但与此同时, 图像信息的造假以及盗用也层出不穷, 因此信息安全愈发得到人们的关注. 当图像被用于医学、军事、法庭等用途时, 必须保证图像内容的真实性和完整性. 脆弱水印凭借其对篡改的敏感性被用于鉴定图像内容的真实性与完整性, 将水印信息嵌入到图像中, 与图像融为一体, 当需要检测图像信息的真实性与完整性时, 可通过检测提取出来的水印来判断图像是否可靠完整[1–7]. 1979 年 Sharmir 和 Blakey 提出了秘密共享的思想, 分别利用了 Lagrange 插值法和多维空间点的性质实现了第一个 (k, n) 门限方案, 此方案的特点是: 任意 k 或 k 个以上的参与者都可以恢复秘密信息, 而少于 k 个参与者无法得到秘密信息[8]. 基于此思想, 1994 年 Naor 和 Shamir[9] 在欧洲密码学年会上提出了一种既能够提供完整保密性又能够仅通过人类视觉系统解密的新型密码方案, 这就是视觉密码技术. 经典的 (k, n) 视觉密码方案是将待加密的二值图像编码为 n 个分享图像, 解密时只需要将不少于 k 个分享图像进行非相干叠加, 即可通过人类的视觉系统获知编码信息. 视觉密码一经提出, 就引起了研究人员的广泛关注. 在过去的二十多年里, 已经有很多改进方案被提出, 如优化对比度[10,11]、灰度图像加密[12,13]、彩色图像加密[14–16]、增强型视觉密码[17,18]、像素不

* 国家重点研发计划 (批准号: 2021YFB3602604)、国家自然科学基金 (批准号: 62131011, 62075221, 61975205)、中国科学院科教融合项目、中央高校基本科研业务费专项资金和河北省创新能力提升项目 (批准号: 20540302D) 资助的课题.

† 通信作者. E-mail: sysopt@126.com

扩展的视觉密码[19–22]. 传统的视觉密码会存在像素扩展问题, 使得分享图像比秘密图像具有更大的尺寸, 研究表明对于一个 (k, n) 视觉密码方案, 理想情况下的膨胀度为 $m = 2^{k-1}$, 即一个像素被加密成 2^{k-1} 个子像素[9]. 因此, 像素扩展为分享图像的存储和传输带来了不便, 并且嵌入水印时也会因为像素扩展的原因而被迫选择更大的彩色宿主图像, 而像素不扩展的视觉密码可以很好地避免上述问题.

第一个实用的迭代相位恢复算法是由 Gerchberg 和 Saxton[23,24] 在 1971 年研究电子显微成像中相位恢复问题时提出, 称为 Gerchberg-Saxton (GS) 算法, 该算法涉及到待测量光场所在平面以及衍射场所在平面, 其核心就是在两个平面上分别加以约束条件, 不断迭代求解出相位信息. 2017 年, 我们课题组提出了借助衍射光学的方式实现不可见的视觉密码, 将纯振幅图像隐藏在人眼和强度检测器所不可见的相位信息中, 进一步提高了视觉密码的安全性, 并开发了相应的光学隐藏系统[25,26].

本文根据以上内容提出了基于像素不扩展视觉密码的光学彩色脆弱水印系统, 使用像素不扩展视觉密码对水印图像进行编码可以避免因视觉密码带来的像素扩展问题, 后续可选择与水印图像相同大小的宿主图像, 并且将光学中菲涅耳域 GS 算法融入到对水印图像的处理过程中, 此过程中衍射距离、波长都可以作为密钥, 以光学的方式提高了水印图像的安全性.

2 实现方案

基于像素不扩展视觉密码的光学彩色脆弱水印系统主要分为光学水印生成与嵌入部分以及水印提取两部分, 其中光学水印生成与嵌入过程如图 1 所示. 首先, 将原始图像转换为 QR 码图像, 并将 QR 码图像作为水印图像用于后续处理. 其次, 使用像素不扩展的视觉密码对水印图像进行编码, 编码后得到 3 张分享图像, 称作视觉密钥; 将 3 幅视觉密钥作为输出面光强分别使用 GS 算法得到输入平面的相位信息. 再次, 选择一张彩色宿主图像, 将其分解为 R, G, B 三分量图像. 最后将上述所得相位信息嵌入三分量图像后合成. 至此光学水印生成与嵌入部分结束.

水印提取过程为嵌入的逆过程, 如图 2 所示. 首先, 将含水印图像分解为 R, G, B 三分量图像; 使用含水印图像的三分量图像分别减去宿主图像的三分量图像后除以衰减系数, 即可提取出相位信息. 其次, 将相位信息作为输入平面, 使用正确波长的光照射并调整正确的衍射距离使其进行菲涅耳衍射, 可再现 3 幅输出面光强信息. 再次, 将光强信息叠加后对图像进行腐蚀处理可提取出水印图像. 这里为便于观看将叠加后的信息伪彩色显示, 后续处理依旧使用原图. 最后, 使用移动设备扫描提取出的水印图像即可得到原始图像.

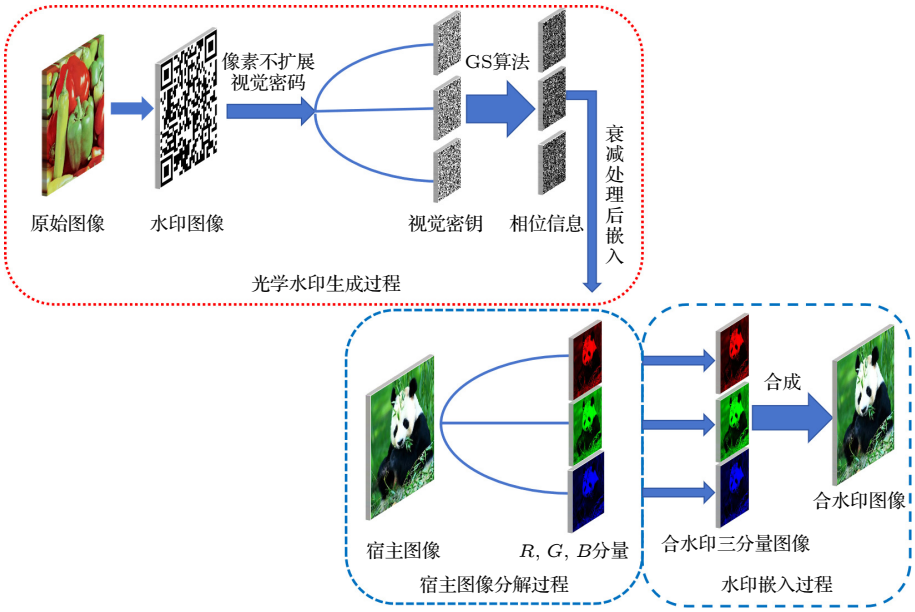

图 1 光学水印生成及嵌入过程

Fig. 1. Optical watermark generation and embedding process.

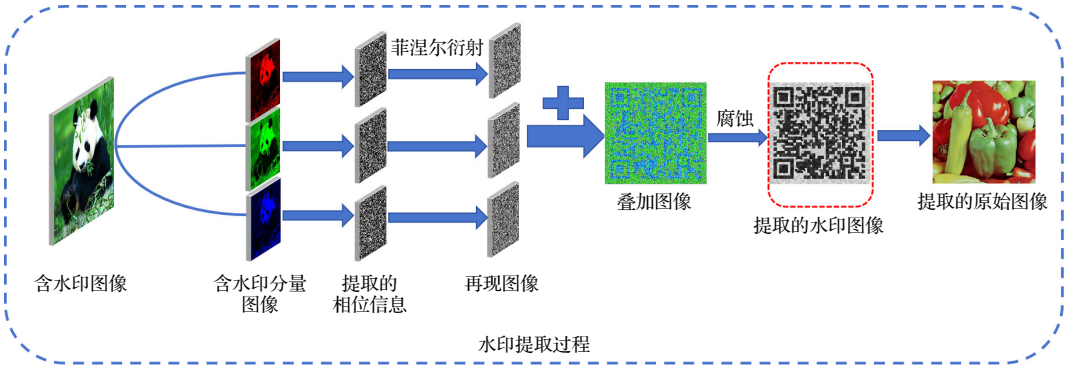

图 2 光学水印提取过程

Fig. 2. Optical watermark extraction process.

具体实施步骤如下.

步骤 1 首先, 选择一张原始图像将其转换为 QR 码图像, 并将 QR 码图像作为水印图像用做后续处理.

步骤 2 将水印图像使用像素不扩展视觉密码方案[21]编码, 像素不扩展视觉密码编码过程每次选取 2×2 大小的像素块. 根据像素块的黑白像素个数编码方案一共可分为以下 5 种情况, 如图 3 所示.

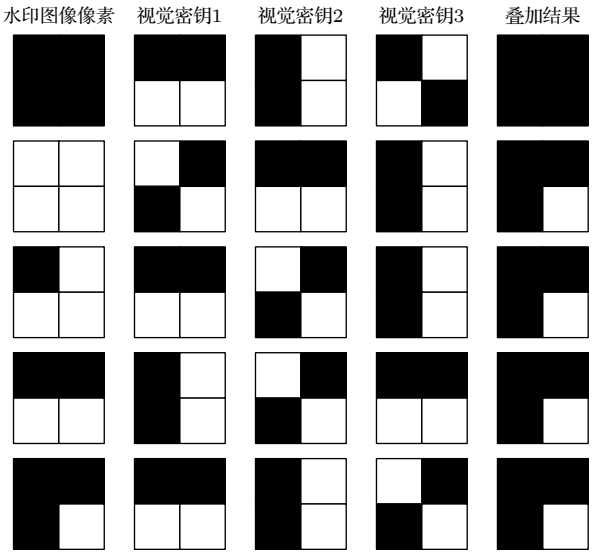

图 3 像素不扩展视觉密码编码方案

Fig. 3. Pixel-free expansion visual cryptography encoding scheme.

由图 3 可知, 当秘密图像中含有白色像素时, 视觉密钥所叠加结果相同, 则该方案所对应的基础矩阵为两个, 分别是

$$\boldsymbol{S}^0=\begin{bmatrix}1010\\1001\\1100\end{bmatrix},\quad \boldsymbol{S}^1=\begin{bmatrix}1010\\1100\\0110\end{bmatrix}. \tag{1}$$

其中 1 代表黑色, 0 代表白色, 当水印图像像素块中存在白色像素时, 利用基础矩阵 $\boldsymbol{S}^1$ 进行分享, 只有当 4 个像素均为黑像素时, 则选择 $\boldsymbol{S}^0$ 进行分享. 针对 4 个像素中黑白像素个数不同, 可分为 4 种情况讨论分享算法.

1) 当 4 个像素全为黑色像素时, 则对 $\boldsymbol{S}^0$ 进行随机列变换, 并将变换后的基础矩阵的每一行对应到相应的视觉密钥.

2) 当 4 个像素全为白色像素时, 则对 $\boldsymbol{S}^1$ 进行随机列变换, 并将变换后的基础矩阵的每一行对应到相应的视觉密钥.

3) 如果 4 个像素的颜色为 3 个黑色一个白色, 则让这个白色像素对应于 $\boldsymbol{S}^1$ 的全 0 列, 其他 3 列进行随机列变换, 并将变换后的基础矩阵的每一行对应到相应的视觉密钥.

4) 如果 4 个像素的颜色中有两个及以上的白色像素, 则随机选择一个白色像素对应于 $\boldsymbol{S}^1$ 的全 0 列, 其他 3 列进行随机列变换, 并将变换后的基础矩阵的每一行对应到相应的视觉密钥.

步骤 3 将编码后的视觉密钥作为输出平面的光强信息, 利用菲涅耳域 GS 算法得到输入平面相位信息, 具体过程如下.

1) 设输入面初始随机相位为 $\theta_1(x,y)$, 输入面振幅为 $A(x,y)$, 使用初始随机相位与已知输入面振幅组合为初始的输入面复振幅 $P_1(x,y)$:

$$P_1(x,y)=A(x,y)\exp\left[\mathrm{j}\theta_1(x,y)\right]. \tag{2}$$

2) 对输入面复振幅 $P_k(x,y)$ 做菲涅耳变换, 得到输出面复振幅 $P_k(u,v)$:

$$\begin{aligned}P_k(u,v)&=FrT\left\{P_k(x,y)\right\}\\&=\left|P_k(u,v)\right|\exp\left[\mathrm{j}\varphi_k(u,v)\right].\end{aligned} \tag{3}$$

3) 用视觉密钥 $O(u,v)$ 作为输出面光强替换输出面振幅, 得到新的输出面复振幅 $P'_k(u,v)$:

$$P'_k(u,v)=\sqrt{O(u,v)}\exp\left[\mathrm{j}\varphi_k(u,v)\right]. \tag{4}$$

4) 对新的输出面复振幅做逆菲涅耳变换, 得到输入面复振幅 $P'_k(x,y)$:

$$\begin{aligned}P'_k(x,y)&=FrT^{-1}\left\{P'_k(u,v)\right\}\\&=\left|P'_k(x,y)\right|\exp\left[\mathrm{j}\theta'_k(x,y)\right].\end{aligned} \tag{5}$$

5) 保留输入面复振幅的相位信息, 用已知的 $A(x,y)$ 替换 $|P'_k(x,y)|$, 得到新的输入面复振幅 $P_{x+1}(x,y)$:

$$\begin{aligned}P_{k+1}(x,y)&=A(x,y)\exp\left[\mathrm{j}\theta'_k(x,y)\right]\\&=\left|P_{k+1}(x,y)\right|\exp\left[\mathrm{j}\theta_{k+1}(x,y)\right].\end{aligned} \tag{6}$$

6) 重复步骤 2)—5), 直到达到设定好的迭代次数, 将相位信息 $\theta_k(x,y)$ 作为结果输出.

步骤 4 根据水印图像大小选择相同大小的彩色宿主图像.

1) 将彩色宿主图像分解为 R, G, B 三分量图像, 将上述相位信息 $\theta_k(x,y)$ 嵌入到三分量宿主图像中, 这里以 R 分量为例, G, B 分量嵌入过程相同. 假设 R 分量图像为 $R(x,y)$:

$$H(x,y)=R(x,y)+\alpha\theta_k(x,y). \tag{7}$$

其中, $H(x,y)$ 为 R 分量含水印图像.

2) 将含水印图像的 R, G, B 三分量合成, 得到彩色的含水印图像. 至此, 光学水印生成及嵌入过程结束.

水印的提取为嵌入的逆过程, 具体步骤如下.

1) 首先将含水印图像分解为 R, G, B 三分量含水印图像, 其次将水印信息从三分量中提取出来. 以 R 通道为例, G, B 通道提取过程相同:

$$\theta_k(x,y)=\left[H(x,y)-R(x,y)\right]\times\alpha^{-1}. \tag{8}$$

2) 将提取出来的水印信息作为输入平面, 使其发生菲涅耳衍射得到输出面光强信息.

3) 将输出面光强信息叠加并对图像做腐蚀运算, 即可提取出水印图像.

4) 使用移动设备扫描提取出的水印图像, 即可得到原始图像.

3 仿真实验

本文所提出的光学脆弱水印利用系统对数据变化的敏感性来检测宿主图像是否真实与完整, 当含水印图像未受到任何攻击与篡改时, 使用正确的密钥能够提取出水印图像, 其中衰减系数 α, 衍射时所使用的波长以及衍射距离均可以作为密钥. 一旦含水印图像数据发生了改动, 便无法提取出水印图像, 由此可以验证图像的真实性与完整性遭到了破坏.

为了验证本文所提的可行性, 使用计算机进行模拟仿真验证, 实验中选择 256 像素×256 像素的彩色图像“熊猫”作为宿主图像, 选择一幅 256 像素×256 像素“蔬菜”图像作为原始图像, 图 4(a)—(c) 分别给出了原始图像, 水印图像以及彩色宿主图像, 将图 4(b) 使用像素不扩展视觉密码编码得

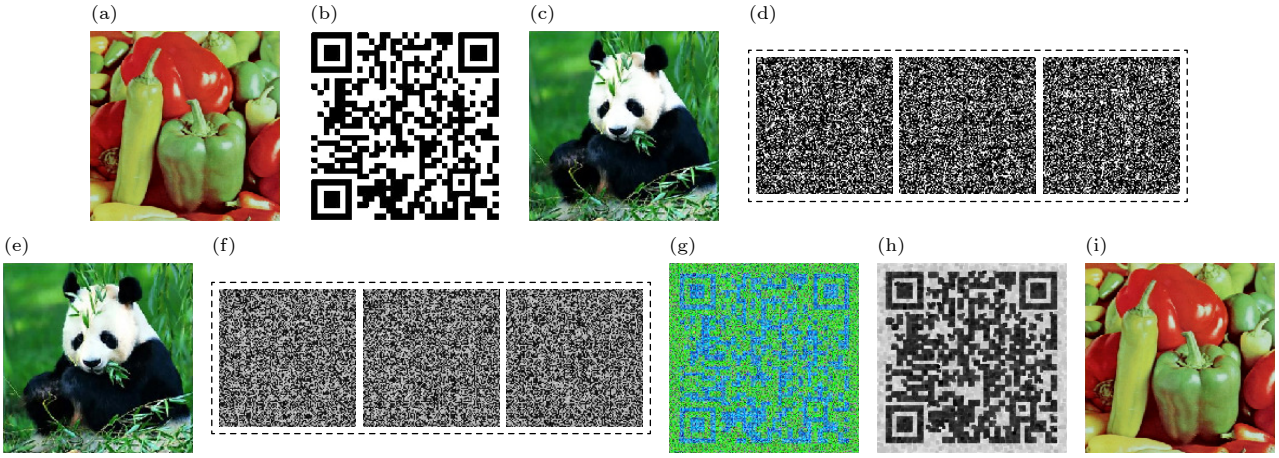

图 4 仿真结果图 (a) 原始图像; (b) 水印图像; (c) 彩色宿主图像; (d) 相位信息; (e) 彩色含水印图像; (f) 再现图像; (g) 叠加图像; (h) 提取的水印图像; (i) 提取的原始图像

Fig. 4. Simulation result diagram: (a) Original image; (b) watermark image; (c) color host image; (d) phase information; (e) color images with watermarks; (f) reproduced image; (g) overlay image; (h) extracted watermark image; (i) extracted original image.

到 3 幅视觉密钥, 将视觉密钥使用上文所提 GS 算法即可得如图 4(d) 所示的 3 张相位信息. 将相位信息衰减后嵌入图 4(c) 的 R, G, B 三分量后, 合成可得如图 4(e) 所示的彩色含水印图像. 在提取过程中, 将宿主图像看成一种噪声, 因此分离结果的好坏直接影响水印图像的提取质量. 本文所提方案可以完全分离出水印图像, 图 4(f) 表示从彩色含水印图像中提取出相位信息后, 使用菲涅耳衍射后再现的输出面光强信息. 图 4(g) 表示图 4(f) 叠加后的图像, 为了使其轮廓清晰可见, 对叠加后图像进行腐蚀运算提取出如图 4(h) 所示的水印图像, 使用移动设备扫描可得到如图 4(i) 所示的原始图像.

4 结果分析

4.1 验证视觉密码 (k, n) 门限方案

(k, n) 门限方案指的是, 经过视觉密码编码后得到的任意 k 或 k 个以上图像叠加可以观察到秘密信息, 少于 k 个叠加则无法得到秘密信息. 针对本文所使用的 (3, 3) 像素不扩展视觉密码方案, 当任意两幅图像叠加, 结果应该是杂乱无章的, 不包含任何有效信息的. 为验证本文所提系统满足视觉密码 (k, n) 门限方案, 分别将仿真所得 3 张再现图像两两相加, 其中图 5(a)—(c) 分别表示第 1 张再现图像与第 2 张再现图像叠加、第 1 张再现图像与第 3 张再现图像叠加、第 2 张再现图像与第 3 张再现图像叠加.

4.2 脆弱性分析

脆弱的水印系统应该尽可能的检测出含水印图像遭到了攻击与篡改, 这是脆弱水印最基础的要求, 并且也是可靠地测试图像真实性与完整性的要求. 脆弱性水印要求对任何可能影响图像信息的微小操作如添加噪声、滤波等合法操作都非常敏感[4]. 因此当含水印图像受到了噪声污染或者攻击时, 将无法正确提取出原始图像, 从而达到脆弱性的要求, 并且也是测试图像真实性与完整性的要求.

为了测试本系统在遭到攻击时的性能, 对含水印图像进行了一系列的攻击, 这其中包括分别在含水印图像的 R, G, B 三通道各自添加高斯噪声、椒盐噪声以及均匀噪声, 对彩色含水印图像进行旋转、运动模糊处理、高斯低通滤波处理以及剪切和 JPEG 压缩. 具体仿真结果如图 6 所示, 图 6(a)—(c) 的第 1 行分别表示对彩色含水印图像添加高斯噪声、椒盐噪声以及均匀噪声的结果, 第 2 行为对应提取出的水印信息, 图 6(d)—(f) 的第 1 行分别表示对彩色含水印图像旋转 10°、运动模糊处理以及高斯低通滤波处理结果, 第 2 行为对应提取出的水印信息, 图 6(g), (h) 第 1 行表示对彩色含水印图像进行剪切和 JPEG 压缩后的结果, 第 2 行为对应提取出的水印信息.

以上结果可以表明, 本文所提出的脆弱水印对噪声以及一系列常见的攻击敏感. 当含水印图像遭到篡改时, 将无法正确的提取出水印图像. 因此本方案具有良好的脆弱性, 可以很好地鉴别图像的真实性与完整性.

4.3 不可感知性分析

脆弱水印要求在嵌入水印后, 得到的含水印图像与宿主图像在视觉上没有明显的差别, 没有明显的失真. 为了衡量各分量含水印图像与各分量宿主

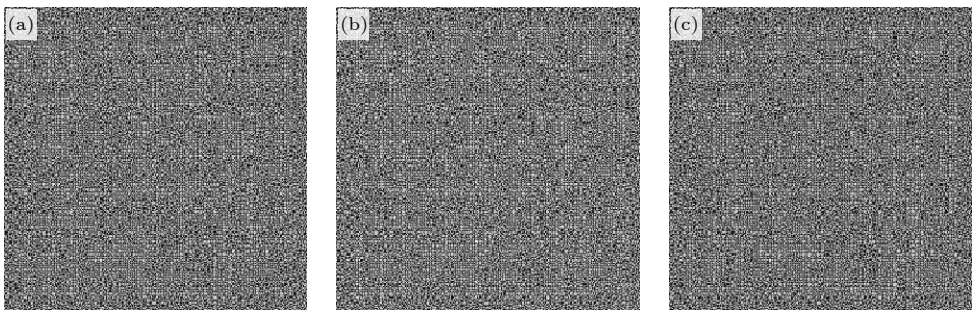

图 5 任意两张再现图像叠加结果图 (a) 第 1 张再现图像与第 2 张再现图像叠加; (b) 第 1 张再现图像与第 3 张再现图像叠加; (c) 第 2 张再现图像与第 3 张再现图像叠加

Fig. 5. Overlay results of any two reproduced images: (a) Overlay of the first reproduced image and the second reproduced image; (b) overlay the first reproduced image with the third reproduced image; (c) overlay of the second and third reproduced images.

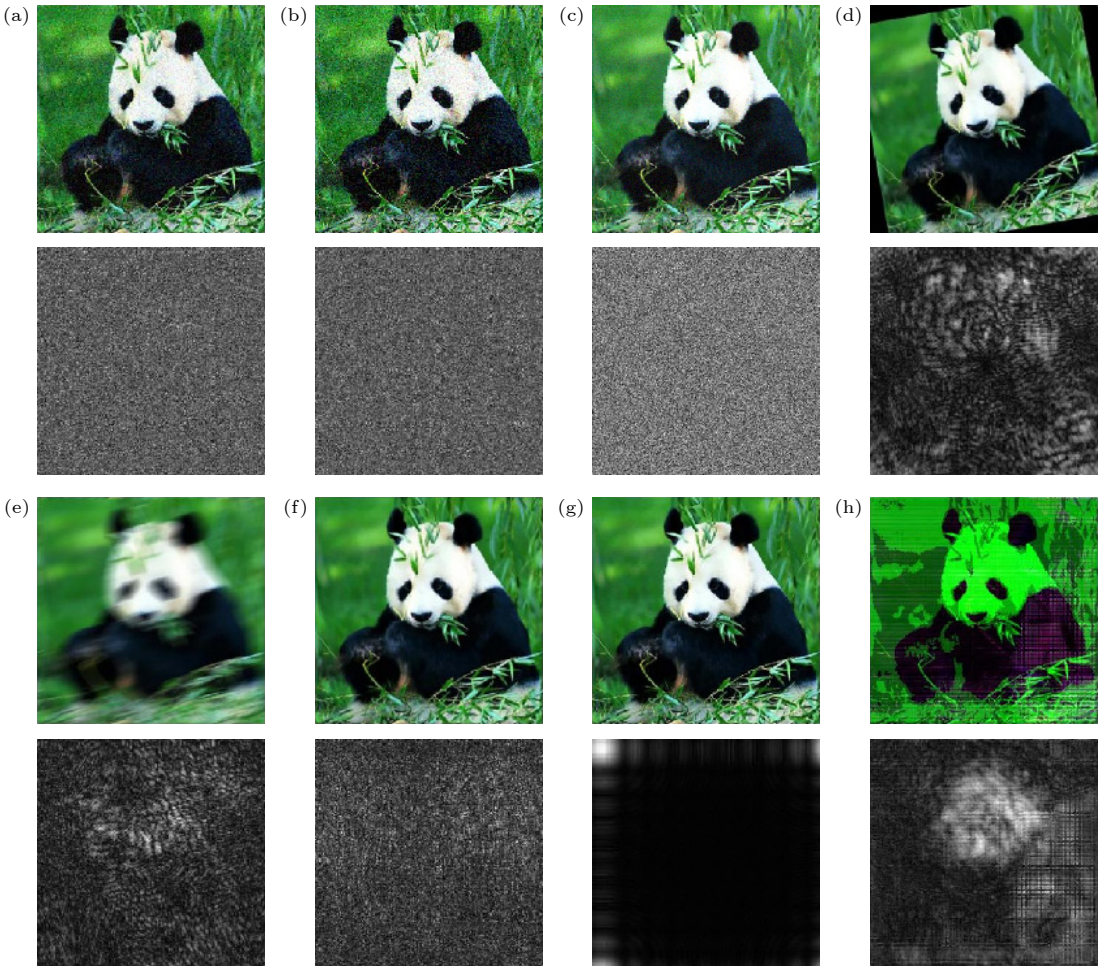

图 6 攻击实验结果图 (a)—(c) 高斯噪声、椒盐噪声、均匀噪声; (d)—(h) 旋转、运动模糊、高斯低通滤波、裁剪、JPEG 压缩

Fig. 6. Attack experiment results: (a)–(c) Gaussian noise, salt and pepper noise, uniform noise; (d)–(h) rotation, motion blur, Gaussian low-pass filtering, cropping, JPEG compression.

图像之间的不可感知性, 定义峰值信噪比 (peak signal to noise ratio, PSNR) 为

$$R_{\mathrm{PSNR}} = 10\lg\left[\frac{255\times 255}{\dfrac{1}{m\times n}\displaystyle\sum_{i=0}^{m=1}\sum_{j=0}^{n=1}\left[c_{\mathrm{w}}(i,j)-c_{\mathrm{o}}(i,j)\right]^2}\right], \quad (9)$$

其中, 各分量的 PSNR 与衰减系数的关系曲线如图 7 所示.

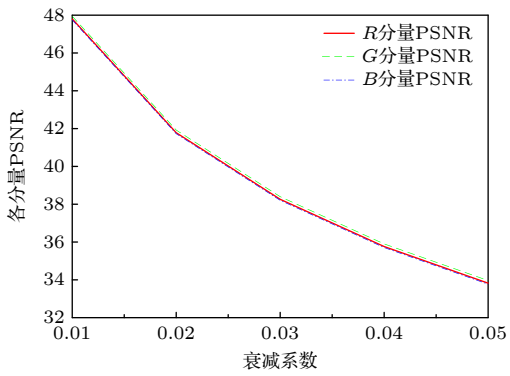

图 7 各分量的 PSNR 与衰减系数的关系

Fig. 7. Relationship between PSNR of each component and attenuation coefficient.

当 PSNR 值越高时, 说明系统的不可感知性越好, 本文所提到的脆弱水印的不可感知性与衰减系数有关. $\alpha = 0.01$ 时, PSNR 较高, 不可感知性较好, 随着 α 的增大, 系统的不可感知性下降. 在本文所提的方法中, 三分量的 PSNR 值均达到 30 dB 以上, 这可以说明两幅图像在视觉上没有差异, 此水印系统具有良好的不可感知性. 为了进一步验证所提方法所具有的不可感知性, 选取了 3 张 256 像素×256 像素的彩色宿主图像进行不可感知性测试, 使用衰减系数 $\alpha = 0.01$ 将水印密文分别嵌入到 3 张不同的宿主图像. 图 8(a)—(c) 分别表示 “flower”, “fruit” “panda”. 图 8(d)—(f) 分

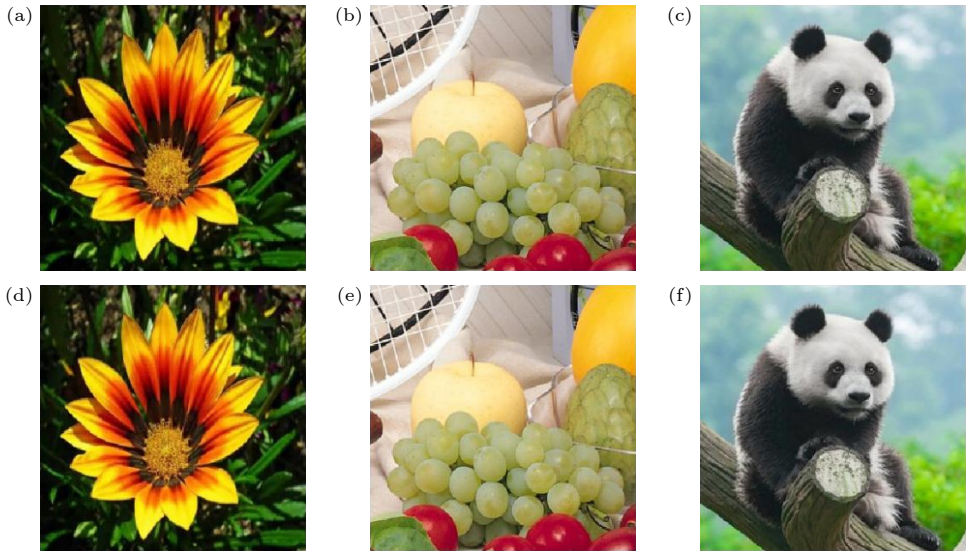

图 8 不同宿主图像与含水印图像对比 (a)—(c) “flower”宿主图像、“fruit”宿主图像、“panda”宿主图像; (d)—(f) “flower”彩色含水印图像, “fruit”彩色含水印图像, “panda”彩色含水印图像

Fig. 8. Comparison between different host images and watermarked images: (a)–(c) “flower” host image, “fruit” host image, “panda” host image; (d)–(f) “flower” color watermarked image, “fruit” color watermarked image, “panda” color watermarked image.

别表示“flower”, “fruit”, “panda”三张彩色含水印图像, 可以看出嵌入水印后的图像与宿主图像几乎相同, 并使用计算机计算了 PSNR(省略虚部). 从表 1 可知, 测试结果表明嵌入水印后的宿主图像与原始图像几乎无差别.

表 1 不同宿主图像的 PSNR

Table 1. PSNR of different host images.

实验次数	Flower	Fruit	Panda
	PSNR	PSNR	PSNR
1	50.4512	50.3216	50.4309
2	50.3675	50.3364	50.3374
3	50.2660	50.4510	50.4138
4	50.4219	50.4544	50.3442
5	50.2407	50.2530	50.3409
6	50.5150	50.4241	50.4853
7	50.4227	50.4452	50.4365
8	50.4355	50.4863	50.3971
9	50.5024	50.4492	50.3321
10	50.3872	50.4446	50.2862
平均	50.4001	50.4066	50.3794

5 结 论

本文提出了一种基于像素不扩展视觉密码的光学彩色脆弱水印, 仿真结果表明, 该水印系统具有良好的脆弱性, 当含水印图像面对噪声以及常见的攻击时, 都无法提取出正确的原始图像, 对数据变化敏感. 因此可用来检测图像真实性以及完整性, 并且像素不扩展视觉密码可以使得宿主图像大小与水印图像大小相同, 减少了传输过程中所消耗的网络带宽以及存储空间. 将像素不扩展视觉密码与相位恢复算法结合对水印图像进行处理得到用于嵌入的相位信息, 以光学的方式进一步提高了水印图像的安全性. 同时, 本文所提水印方法还具有良好的不可感知性, 使得含水印图像不易被察觉. 该方案对医学图像、军事作战图、以及法律证据方面有着重要意义. 因此, 从理论角度和应用角度来看, 开展关于脆弱性水印的研究不但具有重要的学术意义, 而且还具有一定的实用价值.

参考文献

[1] Thanki R 2021 *Int. J. Digit. Crime Fourensics* **13** 35

[2] Zhang F Y 2014 *M. S. Thesis* (Chengdu: Southwest Jiaotong University) (in Chinese) [张凤英 2014 硕士学位论文 (成都: 西南交通大学)]

[3] Shen J Q 2019 *M. S. Thesis* (Wuhan: Huazhong University of Science and Technology) (in Chinese) [沈嘉琪 2019 硕士学位论文 (武汉: 华中科技大学)]

[4] Zhou X L, Zhu Y P, Yang D Y, Zhang J H, Lu Z, Wang H Y, Dong Z, Ke C J, Shi Y S 2021 *Acta Phys. Sin.* **70** 244201 (in Chinese) [周新隆, 祝玉鹏, 杨栋宇, 张峻浩, 卢哲, 王华英, 董昭, 柯常军, 史祎诗 2021 物理学报 **70** 244201]

[5] Yang Y Z 2023 *M. S. Thesis* (Jingzhou: Yangtze University)

(in Chinese) [杨雅姿 2023 硕士学位论文 (荆州: 长江大学)]
[6] Chen Z Y 2013 *Signal Process. Image Commun.* **28** 301
[7] Gong X H 2019 *M. S. Thesis* (Beijing: Beijing University of Posts and Telecommunications) (in Chinese) [龚馨慧 2019 硕士学位论文 (北京: 北京邮电大学)]
[8] Yu B, Fu Z X, Shen G, Fang L G 2014 *Visual Cryptography* (Hefei: University of Science and Technology of China Press) pp2–3 (in Chinese) [郁滨, 付正欣, 沈刚, 房礼国 2014 视觉密码 (合肥: 中国科学技术大学出版社) 第 2—3 页]
[9] Naor M, Shamir M 1994 *Lect. Notes Comput. Sci.* **950** 1
[10] Zhao Y K 2023 *Ph. D. Dissertation* (Tianjin: Nankai University) (in Chinese) [赵永康 2023 博士学位论文 (天津: 南开大学)]
[11] Blundo C, Bonis A D, Santis A D 2001 *Designs Codes Cryptogr.* **24** 255
[12] Blundo C, Santis A D, Naor M 2000 *Inf. Proc. Lett.* **75** 255
[13] Lin C C, Tsai W H 2003 *Pattern Recognit. Lett.* **24** 349
[14] Hou Y C 2003 *Pattern Recognit.* **36** 1619
[15] Yamamoto H, Hayasaki Y, Nishida N 2004 *Opt. Express* **12** 1258
[16] Machizaud J, Fournel T 2012 *Opt. Express* **20** 22847
[17] Yu T, Yang D Y, Ma R, Shi Y S 2020 *Acta Phys. Sin* **69** 144202 (in Chinese) [于韬, 杨栋宇, 马锐, 史祎诗 2020 物理学报 **69** 144202]
[18] Ateniese G, Blundo C, Santis A D, Stinson D R 2001 *Theor. Coumpt. Sci.* **250** 143
[19] Shyu S J 2007 *Pattern. Recogn.* **40** 1014
[20] Shyu S J 2009 *Pattern. Recogn.* **42** 1582
[21] Wang H J, Ma D H, Zhang E Q, Zhao T F 2018 *Eng. J. Wuhan Univ.* **51** 1123 (in Chinese) [王洪君, 马冬鹤, 张恩绮, 赵腾飞 2018 武汉大学学报 (工学版) **51** 1123]
[22] Hu H, Yu B, Shen G 2015 *Comput. Sci.* **42** 103 (in Chinese) [胡浩, 郁滨, 沈刚 2015 计算机科学 **42** 103]
[23] Gerchberg R W, Saxton W O 1972 *Optik* **35** 237
[24] Zhang H X 2021 *M. S. Thesis* (Hangzhou: Zhejiang University) (in Chinese) [张鹄翔 2021 硕士学位论文 (杭州: 浙江大学)]
[25] Shi Y S, Yang X B 2017 *J. Opt.* **19** 115703
[26] Shi Y S, Yang X B 2017 *Chin. Phys. Lett.* **34** 114204

Optical color fragile watermark based on pixel-free expansion visual cryptography*

Liu Rui-Ze [1)] Zhu Yu-Peng [2)3)] Zhou Xin-Long [2)] Mi Zhao-Ke [1)]
Wu Cheng-Zhe [1)] Qin Qiao-Hua [1)] Ke Chang-Jun [3)] Shi Yi-Shi [2)3)†]

1) (*School of Mathematics and Physics Science and Engineering, Hebei University of Engineering, Handan* 056038, *China*)

2) (*School of Optoelectronics, University of Chinese Academy of Sciences, Beijing* 100049, *China*)

3) (*Aerospace Information Research Institute, Chinese Academy of Sciences, Beijing* 100094, *China*)

(Received 16 October 2023; revised manuscript received 28 April 2024)

Abstract

In recent years, with the continuous development of computer technology, it has brought convenience to people to obtain image information. However, at the same time, the falsification and theft of image information have also emerged, so information security has received increasing attention. When images are used for medicine, military, court, and other purposes, it is necessary to ensure the authenticity and integrity of the image content. Fragile watermarks are used to verify the authenticity and integrity of image content due to their sensitivity to tampering. The watermark information is embedded in the image and integrated with the image. When it is necessary to detect the authenticity and integrity of image information, the extracted watermark can be used to determine whether the image is reliable and complete. Therefore, we propose an optical color fragile watermarking system based on pixel-free expansion visual cryptography. On the one hand, encoding watermark images by using pixel-free expansion visual cryptography avoids pixel expansion issues caused by visual cryptography, allowing for the selection of color host images with the same pixel size as the watermark image in the future, greatly reducing the network bandwidth and storage space occupied during transmission. On the other hand, phase recovery algorithm is used to process the encoded watermark image to obtain phase information for embedding into the host image, further improving the security of the watermark image in an optical way. The feasibility and imperceptibility of the proposed optical color fragile watermark are verified through computer simulation, and its good fragility is verified through a series of simulation attack experiments. It can sensitively detect image tampering in the face of common attacks such as noise pollution, rotation, motion blur processing, filtering, etc.

Keywords: optical color fragile watermark, pixel-free expansion visual cryptography, phase recovery algorithm, tamper detection

PACS: 42.30.–d, 42.30.Va, 42.30.Rx **DOI:** 10.7498/aps.73.20231652

* Project supported by the National Key Research and Development Program of China (Grant No. 2021YFB3602604), the National Natural Science Foundation of China (Grant Nos. 62131011, 62075221, 61975205), the Fusion Foundation of Research and Education of Chinese Academy of Sciences, University of Chinese Academy of Sciences, the Fundamental Research Funds for the Central Universities of China, the Innovation Capability Improvement Plan of Hebei Province, China (Grant No. 20540302D).

† Corresponding author. E-mail: sysopt@126.com

物理学报 Acta Physica Sinica
Chinese Physical Society
Institute of Physics, CAS

基于像素不扩展视觉密码的光学彩色脆弱水印

刘睿泽 祝玉鹏 周新隆 米沼锞 吴承哲 秦俏华 柯常军 史祎诗

Optical color fragile watermark based on pixel-free expansion visual cryptography

Liu Rui-Ze Zhu Yu-Peng Zhou Xin-Long Mi Zhao-Ke Wu Cheng-Zhe Qin Qiao-Hua Ke Chang-Jun Shi Yi-Shi

引用信息 Citation: Acta Physica Sinica, 73, 134202 (2024) DOI: 10.7498/aps.73.20231652
在线阅读 View online: https://doi.org/10.7498/aps.73.20231652
当期内容 View table of contents: http://wulixb.iphy.ac.cn