物理学报 Acta Physica Sinica

Chinese Physical Society

Institute of Physics, CAS

基于视觉密码与QR码的光学脆弱水印

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

Optical fragile watermarking based on visual cryptography and QR code

Zhou Xin-Long Zhu Yu-Peng Yang Dong-Yu Zhang Jun-Hao Lu Zhe Wang Hua-Ying Dong Zhao Ke Chang-Jun Shi Yi-Shi

引用信息 Citation: Acta Physica Sinica, 70, 244201 (2021) DOI: 10.7498/aps.70.20210964

在线阅读 View online: https://doi.org/10.7498/aps.70.20210964

当期内容 View table of contents: http://wulixb.iphy.ac.cn

基于视觉密码与 QR 码的光学脆弱水印*

周新隆[1)] 祝玉鹏[2)3)] 杨栋宇[2)3)] 张峻浩[2)3)] 卢哲[1)]
王华英[1)] 董昭[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)

(2021 年 5 月 21 日收到; 2021 年 7 月 11 日收到修改稿)

提出了一种基于视觉密码与 QR 码的图像认证和篡改检测的光学脆弱水印方法. 一方面, 将原始水印图像变换为 QR 码水印图像, 以提高水印隐藏容量. 另一方面, 将视觉密码与光学相位编码相融合来加密水印图像, 以增强系统安全性. 通过一系列的攻击与篡改测试了所提水印方法的可行性、脆弱性和不可感知性. 模拟结果表明, 所提水印方法不仅具有较好的不可感知性, 而且在任意攻击下都能灵敏地检测出图像发生了篡改, 具有很强的脆弱性.

关键词: 光学脆弱水印, 视觉密码, QR 码, 篡改攻击检测

PACS: 42.30.–d, 42.30.Va, 42.30.Kq **DOI:** 10.7498/aps.70.20210964

1 引 言

现今的数字多媒体时代给图像内容的创造和分配带来了便利, 不过, 与此同时, 复制和编辑的轻而易举为未经授权的使用、盗用和误传提供了条件. 当图像被用于法庭、医学、新闻和商业用途时, 必须保证图像内容的真实性和完整性需要确定其内容是否曾被修改、伪造或者特殊处理过[1–6]. 脆弱水印对数据变化的敏感性使得它被用于图像鉴定中, 图像鉴定系统适用于法律、医学、商业、国防和新闻领域. 在以往的工作中, 研究大多集中于数字水印的鲁棒性设计[7–22], 希望多媒体产品无论受到何种变形操作, 都能从中提取出水印来, 而对用于真实性和完整性保护的光学脆弱数字水印的研究相对较少.

近年来, QR 码在中国得到了广泛的应用, 由于其存储容量大、可读性强, 同时具有无损解密质量, 引发了广大学者对其应用的进一步探索[15]. 视觉密码技术的应用往往有以下三类: 加密、隐藏、认证. 视觉密码的主要思想是利用秘密共享原理. 经典的 (k, n) 图像秘密共享方案是将待加密图像的二值图像扩展为 n 个随机分布的纯振幅视觉密钥, 并分别置于透明片上, 得到 n 个分享图像, 解密时只需要将不少于 k 个的不同透明片进行非相干叠加, 即可直接通过人类的视觉系统获知编码信息[16–18]. 本文提出了一种基于视觉密码与 QR 码的光学脆弱水印方法, 使用光学方法及视觉密码编码方案对水印图像进行加密处理, 使得所提水印方法具有极高的安全性[23]. 首先将原始水印图像生

* 国家自然科学基金 (批准号: 62131011)、中国科学院科教融合项目、中国科学院青年创新促进会 (批准号: 2017489)、中国科学院大学优秀青年教师科研能力提升项目、中央高校基本科研业务费专项资金 (批准号: E1E46201X2) 和河北省自然科学基金重点项目 (批准号: F2018402285) 和河北省京津冀协同创新共同体建设专项 (批准号: 20540302D) 资助的课题.

† 通信作者. E-mail: sysopt@126.com

成为 QR 码, 接着通过视觉密码方案将 QR 码编码成两块独立的视觉密钥 VK1 和 VK2, 将其分别视为振幅与相位进行调制, 调制后作为复振幅图像输入, 经过光学相位编码对复振幅图像进一步加密, 最后将得到的密文衰减处理后嵌入宿主图像中. 提取水印图像时, 使用含水印图像减去宿主图像, 即可获得被加密的水印信息. 衰减系数α作为密钥之一, 使得水印提取质量与衰减系数 α 无关. 使用衰减系数 α 解密后逆向输入光学相位编码系统, 得到复振幅噪声图像, 取复振幅图像的振幅信息与相位信息并相加即可得到 QR 码, 使用移动设备扫描, 即可获得原始水印图像. 通过一系列的攻击与篡改测试了所提出方法的有效性, 实验结果表明: 该方法对于恶意篡改及各类攻击、甚至任何微小的数据变化都十分敏感, 能够灵敏地检测出图像是否被攻击或篡改过, 任何攻击或篡改都会使得水印图像无法成功提取, 通过移动设备扫描得不到原始水印图像. 该方法不仅安全可靠、具有较好的不可感知性, 而且在不同的攻击下均能获得较高的篡改检测概率.

2 实验原理

基于视觉密码与 QR 码的光学脆弱水印系统主要包括水印加密、水印嵌入和原始水印图像提取三个阶段. 光学水印加密与嵌入过程如图 1 所示, 其中 (I) 表示将原始水印图像变换为 QR 码水印图像, 接着将生成的 QR 码水印图像通过视觉密码编码成两块表面置乱的视觉密钥 VK1 和 VK2, 将 VK1 视为振幅、VK2 视为相位进行调制, 得到复振幅图像 VK3. (II) 是指使用光学相位加密方法对 VK3 做进一步加密处理, 随机相位板 M1 紧贴着 VK3 位于透镜 L1 的前焦面上, 经过光学相位加密系统后得到独立的随机白噪声密文. (III) 表示嵌入过程, 是指将水印图像的密文衰减处理后嵌入到宿主图像中, 衰减器位于光学相位加密系统的输出面. 具体步骤以及对应数学表达如下:

步骤 1 将原始水印图像变换为 QR 码水印图像. 通过视觉密码的 2 × 2 编码方案将水印图像编码成两块表面置乱的视觉密钥 VK1 和 VK2.

步骤 2 将 VK1 视为振幅、VK2 视为相位, 调制后得到 VK3 作为复振幅输入. 调制公式为

$$\mathrm{VK3} = \mathrm{abs}\,(\mathrm{VK1}) \cdot \exp(\mathrm{i} \cdot \mathrm{VK2}).$$

步骤 3 将上述复振幅图像 VK3 输入光学相位编码系统进一步加密, 得到密文

$$\psi(x,y) = \mathrm{FT}\langle \mathrm{FT}\,\{\mathrm{VK3}\exp[\mathrm{i}2\pi n(x,y)]\} \cdot \exp[\mathrm{i}2\pi b(u,v)]\rangle.$$

步骤 4 根据水印图像密文的大小选择大小为 256 pixels × 256 pixels 的宿主图像, 嵌入衰减系数α, 将加密后的水印图像衰减处理后嵌入宿主图像$I(x,y)$中

$$H(x,y) = \alpha\psi(x,y) + I(x,y),$$

其中, $\exp[\mathrm{i}2\pi n(x,y)]$和$\exp[\mathrm{i}2\pi b(u,v)]$为随机相位函数, $H(x,y)$为携带水印密文的宿主图像.

提取原始水印图像的前提是成功提取出水印图像. 水印的提取过程为水印加密与嵌入的逆过程. 首先将水印的密文信息从传输图像中分离出来, 使用密钥对密文信息进行解密从而提取出水印, 接着对其作腐蚀膨胀处理, 使用移动通信设备扫描即可得到原始水印图像, 提取过程如图 2 所示,

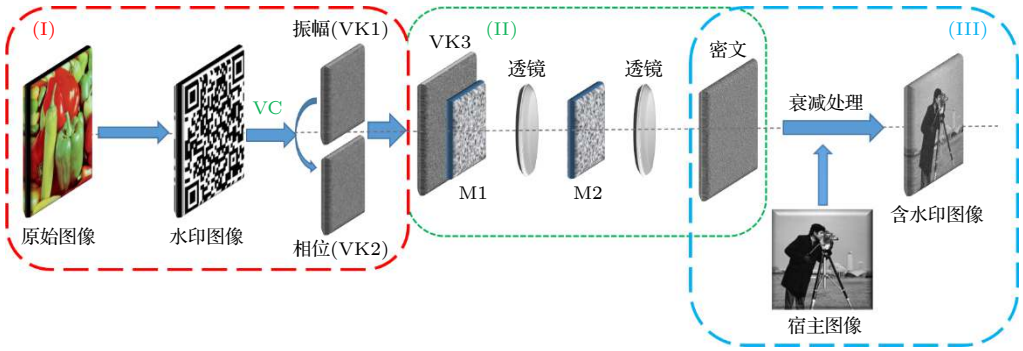

图 1 光学水印生成与嵌入过程

Fig. 1. Optical watermark generation and embedding process. (I) is the process of transforming the original image into a QR code and encoding it through visual-cryptographic (VC denotes visual- cryptography encoding). (II) is the process of optical phase encryption. (III) is the embedding process of watermark.

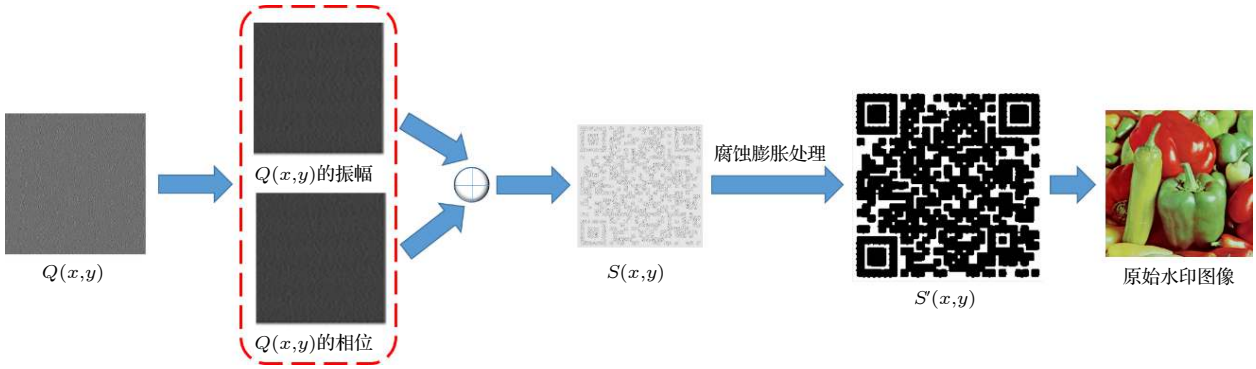

图 2 原始水印图像提取过程

Fig. 2. Optical watermark embedding and extraction process.

具体步骤如下:

步骤 5 将水印密文信息$T(x,y)$从水印图像$H(x,y)$中分离出来, 得到

$$T(x,y)=[H(x,y)-I(x,y)]\cdot\alpha^{-1}.$$

步骤 6 将分离出来的水印密文信息逆向输入光学相位编码系统, 进而得到复振幅图像

$$Q(x,y)=\mathrm{IFT}\{\mathrm{IFT}[T(x,y)]\cdot\exp[-\mathrm{i}2\pi b(u,v)]\}\times\exp[-\mathrm{i}2\pi n(x,y)].$$

步骤 7 取复振幅图像$Q(x,y)$的振幅与相位, 并进行非相干叠加, 即可得到水印图像

$$S(x,y)=\mathrm{abs}[Q(x,y)]+\mathrm{angle}[Q(x,y)],$$

其中, $\exp[-\mathrm{i}2\pi n(x,y)]$和$\exp[-\mathrm{i}2\pi b(u,v)]$为随机相位函数的复共轭.

步骤 8 对水印图像作腐蚀膨胀处理得到可以扫描的 QR 码图像$S'(x,y)$; 使用移动通信设备对恢复的 QR 码信息进行扫描得到原始水印图像.

3 模拟与分析

3.1 可行性分析

本文提出的光学脆弱水印方法利用系统对数据变化的极度敏感性检测宿主图像是否真实与完整. 当嵌入水印的图像未受到任何攻击或篡改时, 使用正确的密钥能够成功提取出 QR 码水印图像, 并通过移动设备扫描出原始水印图像; 一旦含水印图像数据发生了改动, 便无法提取出水印图像, 由此判断出图像的真实性与完整性遭到了破坏.

为了验证所提出的光学脆弱水印方法具有一定的可行性, 使用 MATLAB2016 进行了数字仿真. 实验选用 256 pixels × 256 pixels 的经典灰度图像“cameraman”作为宿主图像, 选择 256 pixels × 256 pixels 的彩色图像“peppers”作为原始水印图像. 图 3(a)—(c) 分别给出了宿主图像、原始水印图像以及由原始水印图像生成的 QR 码水印图像, 将图 3(c) 加密处理并衰减后嵌入到宿主图像中. 提取水印图像的第一步就是将含水印图像中的密文信息分离出来, 在提取的过程中, 宿主图像相当于一种噪声, 因此分离结果的好坏将直接影响水印图像的提取质量. 基于视觉密码学和 QR 码的光学脆弱水印方法可以完全分离出密文信息, 这就会消除宿主图像对水印图像提取质量的影响. 图 3(d) 和图 3(e) 分别为嵌入水印后的图像以及无任何攻击和篡改, 且使用正确密钥提取出来的水印图像. 为了消除提取出来的水印图像的噪声, 使其轮廓清晰可见, 对其进行腐蚀膨胀处理, 结果如图 3(f) 所示, 使用移动设备扫描即可获得原始水印图像, 如图 3(g) 所示. 由此证明宿主图像是真实、完整的. 模拟结果表明, 基于视觉密码与 QR 码的光学脆弱水印符合上述理论推导, 通过模拟仿真验证了其可行性.

3.2 不可感知性分析

脆弱水印作为数字水印的一种, 要求其具有不可感知性. 不可感知性的主要要求是水印嵌入后, 宿主图像的质量不应下降, 人的视觉系统无法察觉出图像发生了变化. 为了测试所提方法不可感知性方面的性能, 选取三张大小为 256 pixels × 256 pixels 的宿主图像进行不可感知性测试, 如图 4(a)—(c) 所示. 使用衰减系数$\alpha=0.01$将水印密文分别嵌入到 woman, panda, baboo 三张宿主图像中, 结果如图 4(d)—(f) 所示. 嵌入水印后的图像与宿主图像几乎相同.

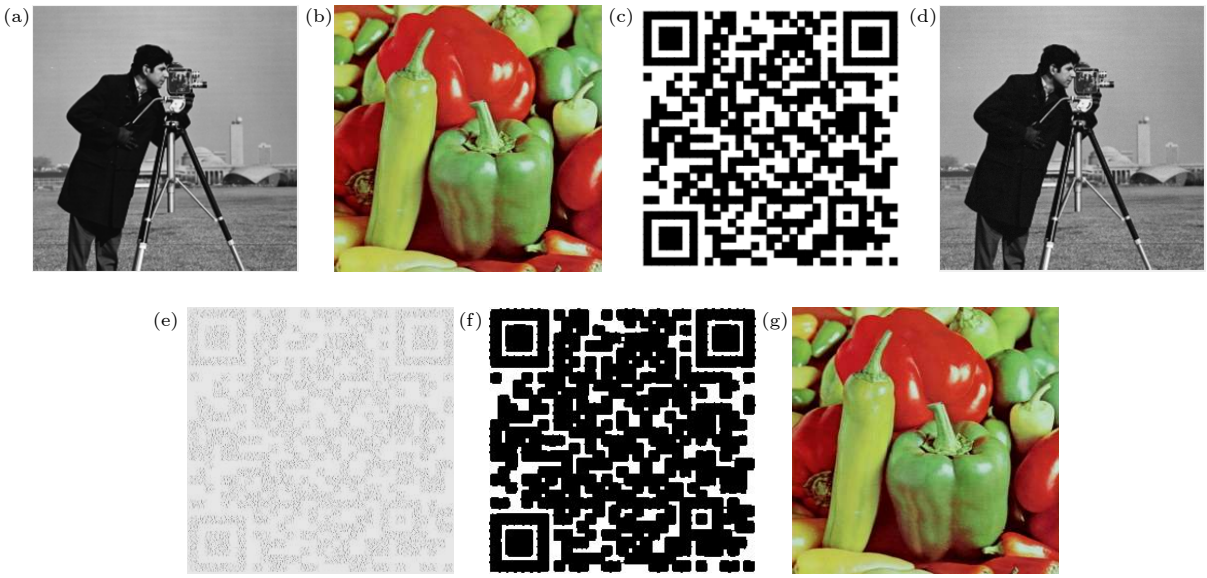

图 3 未受到任何攻击与篡改的水印提取结果 (a) 宿主图像; (b) 原始水印图像; (c) 由原始水印图像生成的 QR 码水印图像; (d) 嵌入水印后的图像; (e) 无任何攻击和篡改, 且使用正确密钥提取出来的水印图像; (f) 腐蚀膨胀处理后的 QR 码水印图像; (g) 使用移动设备扫描得到的原始水印图像

Fig. 3. Watermark extraction results without any attack and tampering: (a) Host image; (b) original watermark image; (c) QR code watermark image generated from original watermark image; (d) watermarked image; (e) watermark image without any attack or tampering, and using the correct key to extract the watermark; (f) QR code watermark image after corrosion expansion; (g) original watermark image scanned by mobile device.

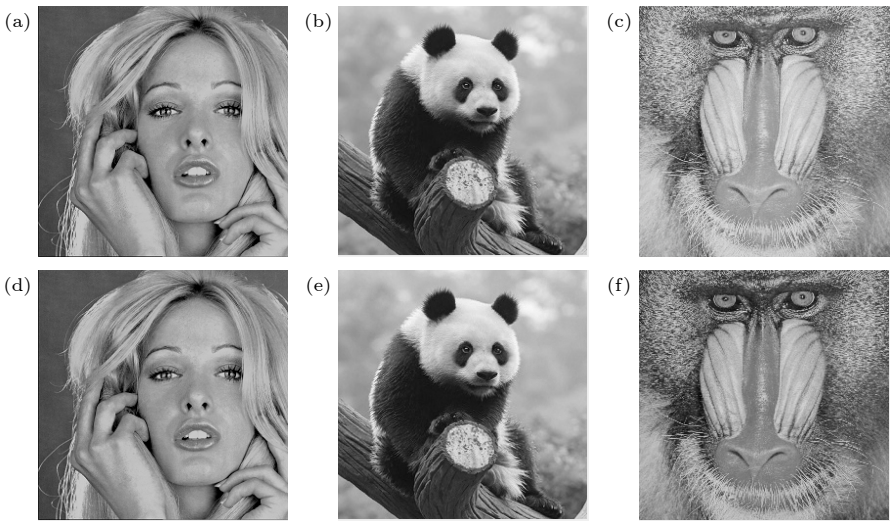

图 4 (a)—(c)woman, panda, baboo 宿主图像; (d)—(f) 对应的含水印图像

Fig. 4. (a) Host image of woman; (b) host image of panda; (c) host image of baboo; (d) watermarked image of woman; (e) watermarked image of panda; (f) watermarked image of baboo.

图 5 给出了以衰减系数 α 为变量, 以相关系数 $C_{\rm O}$ 为像质评价标准的关系曲线, 可以看出, 嵌入水印的三张图像与对应宿主图像之间的相关系数均在 0.90 以上, 说明含水印图像与宿主图像具有较高的相关性.

为了进一步衡量含水印图像与宿主图像之间的不可感知性, 定义峰值信噪比 (peak signal to noise ratio, PSNR) 为

$$R_{\rm PSNR} = 10\log 10\left[\frac{255\times 255}{\dfrac{1}{m\times n}\displaystyle\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[c_{\rm w}(i,j)-c_0(i,j)]^2}\right].$$

PSNR 越高, 说明系统的不可感知性越好. 图 6 为上述三张含水印图像质量随衰减系数α的变化曲线. 可以看出, 本文提到的脆弱水印系统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, 含水印图像质量下降. 在本文提出的方法中, 三张图像的 PSNR 值均在 34—50 dB 之间, 根据人眼视觉特性, 当 PSNR 值大于 30 dB 时, 两幅图像在视觉上没有差异, 因此本文方法具有较好的不可感知性.

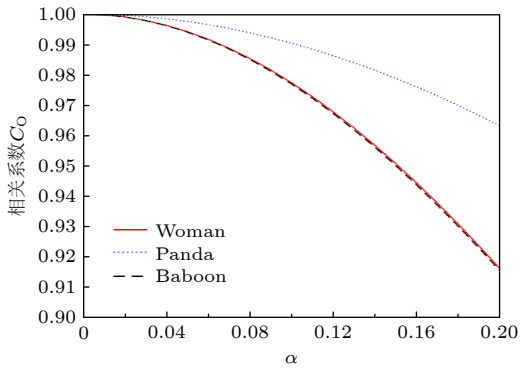

图 5 含水印图像与对应宿主图像之间的相关系数

Fig. 5. Correlation coefficient between watermarked images and corresponding host images.

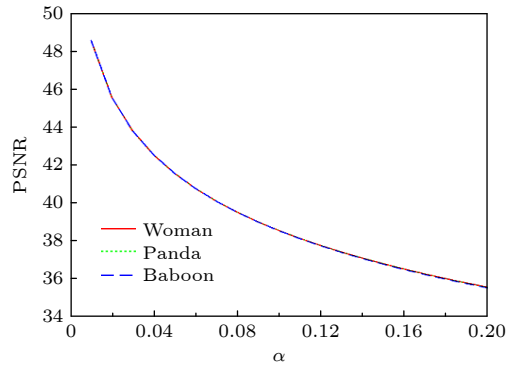

图 6 含水印图像质量随衰减系数α的变化曲线

Fig. 6. PSNR of the watermarked images for different α.

在传统的光学隐藏与水印方法中, 衰减系数α的选取与水印提取质量和不可感知性矛盾. 在一般的水印方法中, 衰减系数越大, 不可感知性越差, 提取的水印质量越好. 而本文提到的水印方法, 提取的水印图像质量与衰减系数无关. 选取 256 pixels × 256 pixels 的 cameraman 为宿主图像, 以α为自变量, 以 PSNR 为像质评价标准, 提取出的水印图像质量与α的关系曲线如图 7 所示, 可以看出, 衰减系数α的变化不会影响水印提取质量.

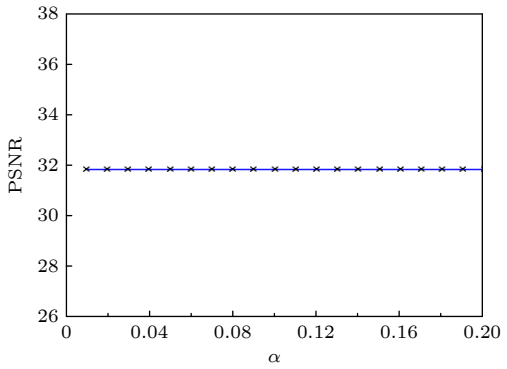

图 7 水印恢复质量随衰减系数的变化曲线

Fig. 7. PSNR of the recovered images for different α.

3.3 脆弱性分析

一个脆弱的水印系统应该以高可能性检测出水印图像遭到了任意篡改与攻击. 这是脆弱水印最基础的特性, 并且也是可靠地测试图像真实性与完整性的要求.

3.3.1 篡改攻击

实验分别对宿主图像与含水印图像进行了复制粘贴和文本添加篡改. 在复制粘贴攻击中, 通过在图像中插入一艘船来修改含水印的帆船图像, 插入的船从同一宿主图像中复制. 从同一图像中复制粘贴进行篡改攻击的图像如图 8(d) 所示. 图 8(a)—(c) 分别为宿主图像、水印图像以及嵌入水印后的图像, 图 8(e) 为篡改后的水印提取结果, 从中无法获取水印信息, 使用移动设备扫描无法得到原始水印图像.

文本添加篡改是指在嵌入水印后的图像中插入文字, 如图 9(d) 所示. 图 9(a)—(c) 分别为宿主图像、水印图像以及嵌入水印后的图像, 实验中进行的修改是在含水印图像的左上角添加文本“PLANE”, 图 9(e) 为篡改后的水印提取结果, 得到的是杂乱无序的噪声图像, 从中无法获得原始水印图像.

3.3.2 攻击实验

为了测试本文所提方法在恶意攻击下的性能, 对嵌入水印后的图像进行了一系列的攻击实验, 将受到攻击的图像作为水印提取算法的输入. 所考虑的攻击包括添加不同的噪声、JPEG 压缩、高斯低通滤波处理、运动模糊和旋转. 图 10 给出了在上述攻击下的水印提取结果, 其中图 10(a)—(c) 分别表示对含水印图像添加高斯噪声、椒盐噪声及斑点

(a) (b) (c) (d) (e)

图 8 复制粘贴篡改后水印提取结果 (a) 宿主图像; (b) 水印图像; (c) 嵌入水印后的图像; (d) 篡改后的图像; (e) 篡改后的水印提取结果

Fig. 8. Result of watermark extraction after copying and pasting: (a) Host image; (b) watermark image; (c) watermarked image; (d) tampered image; (e) result of watermark extraction.

(a) (b) (c) (d) (e)

图 9 文本添加篡改后水印提取结果 (a) 宿主图像; (b) 水印图像; (c) 嵌入水印后的图像; (d) 篡改后的图像; (e) 篡改后的水印提取结果

Fig. 9. Result of watermark extraction after the text is added in watermarked image: (a) Host image; (b) watermark image; (c) watermarked image; (d) tampered image; (e) result of watermark extraction.

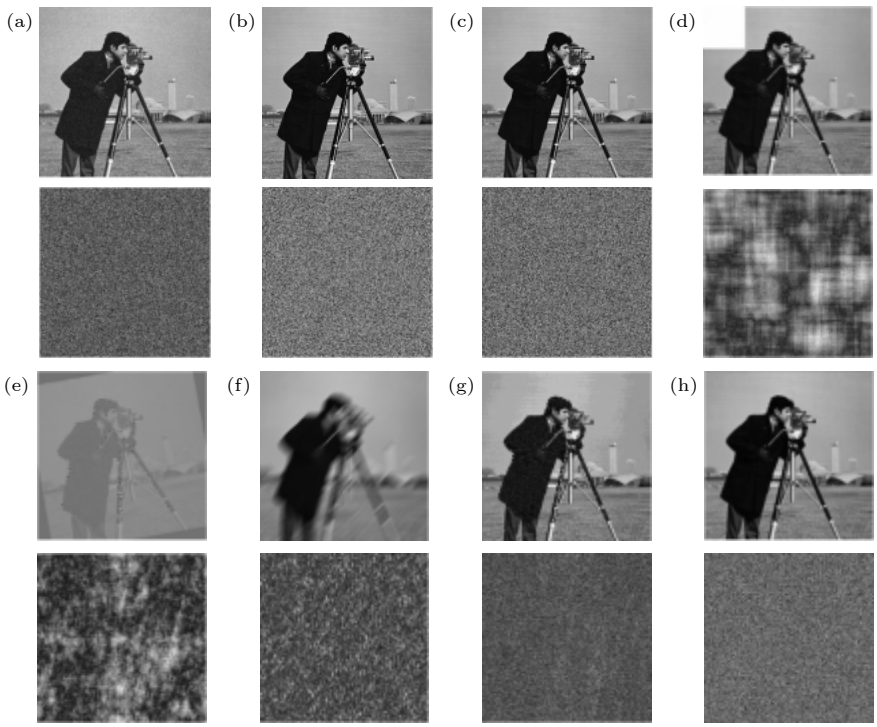

图 10 常见攻击下的水印提取结果 (a)—(c) 高斯噪声攻击、椒盐噪声攻击、斑点噪声攻击; (d)—(h) 剪切、旋转、运动模糊、JPEG 压缩、高斯低通滤波

Fig. 10. Results of common attacks for watermarked images: (a)–(c) Gaussian noise attack, salt and pepper noise attack, speckle noise attack; (d)–(h) shear, rotation, motion blur, JPEG compression, gaussian low pass filtering.

噪声, 图 10(d)—(h) 为对含水印图像进行剪切、旋转、运动模糊、JPEG 压缩以及高斯低通滤波攻击. 可知, 含水印图像一旦受到了恶意攻击, 将无法从中提取出水印图像, 由此判断图像遭到了破坏.

以上结果表明, 本文提出的脆弱水印方法对恶意篡改以及常见的攻击非常敏感, 系统遭到任意的篡改或攻击都无法提取出水印图像, 因此本方法对图像的真实性与完整性检测具有较好的性能.

4 结 论

提出了一种用于图像真实性以及完整性检测的脆弱水印方法, 实验结果表明, 本方法具有较高的灵敏性, 对数据的变化十分敏感, 即使是非常轻微的修改都会造成水印图像无法提取, 因此能够以较高的可能性检测图像是否被攻击或篡改, 对一些要求极其精确的数字媒体, 如文档、医学图像、法律证据等具有深远意义. 同时, 本文所提水印方法还具有较好的不可感知性、较高的水印容量, 使用光学加密方法对水印进行加密, 使得水印系统具有高度的安全性. 从理论角度和应用角度来看, 开展对脆弱性数字水印技术的研究, 不但具有重要的学术意义, 还有极为重要的经济意义.

参考文献

[1] Thanki, Rohit 2021 *Int. J. Digit. Crime Forensics* **13** 35

[2] Yu S W 2013 *iChina* **8** 204 (in Chinese) [余朔望 2013 中国信息化 **8** 204]

[3] Bravo-Solorio S, Nandi A K 2011 *Signal Process.* **91** 728

[4] Chen Z Y 2013 *Signal Process. Image Commun.* **28** 301

[5] Zheng Q M, Liu N 2020 *Comput. Sci.* **47** 332 (in Chinese) [郑秋梅, 刘楠 2020 计算机科学 **47** 332]

[6] Ruan T, Yang D, Shi Y 2021 *Appl. Opt.* **60** 3071

[7] Shi Y, Li T, Wang Y, Gao Q, Zhang S, Li H 2013 *Opt. Lett.* **38** 1425

[8] Liu X L, Pan Z, Wang Y L, Shi Y S 2015 *Acta Phys. Sin.* **23** 234201 (in Chinese) [刘祥磊, 潘泽, 王雅丽, 史祎诗 2015 物理学报 **23** 234201]

[9] Xu W H, Xu H F, Luo Y, Li T 2016 *Opt. Express* **24** 27922

[10] Li C, Wang Y, Ma B, Zhang Z 2012 *Comput. Stand. Interfaces* **34** 367

[11] Shi Y S, Yang X 2017 *J. Opt.* **19** 115703

[12] Zeng G R, Qiu Z D 2010 *Acta Phys. Sin* **59** 5870 (in Chinese) [曾高荣, 裘正定 2010 物理学报 **59** 5870]

[13] Ma R, Li Y, Jia H Z, Shi Y S, Xie X D, Huang T J 2021 *Opt. Lasers Eng.* **141** 106569

[14] Zhu Y P, Xu W H, Shi Y S 2019 *Opt. Commun.* **435** 426

[15] Lv W J, Sun X K, Yang D Y, Zhu Y P, Tao Y, Shi Y S 2021 *Opt. Lasers Eng.* **141** 106574

[16] 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]

[17] Yang N, GAO Q K, Shi Y S 2018 *Opt. Express* **26** 31995

[18] Li Z F, Dong G Y, Yang D Y, Li G L, Shi Y S, Bi K, Zhou J 2019 *Opt. Express* **27** 19212

[19] Sun X K, Zhang S G, Ma R, Tao Y, Zhu Y P, Yang D Y, Shi Y S 2020 *Opt. Express* **28** 31832

[20] Jiao S M, Zhou C Y, Shi Y S, Zou W B, Li X 2019 *Opt. Laser Technol.* **109** 370

[21] Xu R Q, Lv P, Xu F J, Shi Y S 2021 *Opt. Laser Technol.* **136** 106787

[22] Refregier P, Bahram B 1995 *Opt. Lett.* **20** 767

[23] Kishk S, Javidi B 2002 *Appl. Opt.* **41** 5462

Optical fragile watermarking based on visual cryptography and QR code*

Zhou Xin-Long [1)] Zhu Yu-Peng [2)3)] Yang Dong-Yu [2)3)] Zhang Jun-Hao [2)3)]
Lu Zhe [1)] Wang Hua-Ying [1)] Dong Zhao [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 21 May 2021; revised manuscript received 11 July 2021)

Abstract

An optical fragile watermarking method is proposed based on visual cryptography and QR code for image authentication and tamper detection. On the one hand, the original image is transformed into a QR watermark image to improve the watermark hiding capacity. On the other hand, the visual cryptography and optical phase coding are fused to encrypt the watermark image to enhance system security. The feasibility, vulnerability and imperceptibility of the proposed scheme are tested through a series of attacks and tampering. The simulation results show that the proposed method can not only have good imperceptibility, but also achieve high detection performance under different attacks and tampering.

Keywords: optical fragile watermarking, visual cryptography, QR code, tamper detection

PACS: 42.30.–d, 42.30.Va, 42.30.Kq **DOI:** 10.7498/aps.70.20210964

* Project supported by the National Natural Science Foundation of China (Grant No. 62131011), the Fusion Foundation of Research and Education of the Chinese Academy of Sciences, China, the Youth Innovation Promotion Association of the Chinese Academy of Sciences, China (Grant No. 2017489), the Scientific Research Capability Improvement Project for Outstanding Young Teachers of University of Chinese Academy of Sciences, China, the Fundamental Research Fund for the Central Universities, China (Grant No. E1E46201X2), the Key Program of the Natural Science Foundation of Hebei Province, China (Grant No. F2018402285), the Project of Hebei Province Innovation Capability Improvement Plan, China (Grant No. 20540302D).

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