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

基于增强型视觉密码的光学信息隐藏系统

于韬 杨栋宇 马锐 祝玉鹏 史祎诗

Enhanced-visual-cryptography-based optical information hiding system

Yu Tao Yang Dong-Yu Ma Rui Zhu Yu-Peng Shi Yi-Shi

引用信息 Citation: Acta Physica Sinica, 69, 144202 (2020) DOI: 10.7498/aps.69.20200496
在线阅读 View online: https://doi.org/10.7498/aps.69.20200496
当期内容 View table of contents: http://wulixb.iphy.ac.cn

基于增强型视觉密码的光学信息隐藏系统*

于韬 杨栋宇 马锐 祝玉鹏 史祎诗†

(中国科学院大学光电学院, 北京 100049)

(2020 年 4 月 4 日收到; 2020 年 4 月 17 日收到修改稿)

提出了一种基于增强型视觉密码的光学信息隐藏系统. 该系统可将秘密图像分解为多幅有实际意义的分享图像, 然后将这些分享图像隐藏在相位密钥中, 相位密钥可以制成衍射光学元件, 以实体的形式保存和传输, 扩展了视觉密码的应用范围. 在提取过程中, 只需要使用激光照射衍射光学元件, 再现分享图像, 然后只需要将一定数量的分享图像进行非相干叠加即可提取秘密图像, 不需要额外掌握光学和密码学的知识, 其简单性让任何人都可以使用. 仿真实验和光学实验结果表明, 该系统可应用于实际, 并且具有良好的安全性.

关键词: 光学隐藏, 增强型视觉密码, 傅里叶光学, 相位密钥

PACS: 42.30.–d, 42.30.Rx **DOI**: 10.7498/aps.69.20200496

1 引 言

近年来, 随着信息技术的不断发展, 信息安全问题愈发得到人们的重视, 文献中已经报道了各种各样的加密方法来保护信息[1–17]. 这其中有一种奇特的加密方案被提出, 那就是 Naor 和 Shamir[18] 在 1994 年提出的视觉密码 (visual cryptography, VC) 方案, 该方案的安全性有门限特性保证, 解密过程依靠人类的视觉系统从中提取秘密信息. 视觉密码方案在过去二十多年里得到了很大的发展, 已经有很多改进方案被提出, 如优化对比度[19,20]、灰度图像加密[21–23]、彩色图像加密[24–26]、扩展信息容量[27–29]、提高分辨率[30,31] 等. 这些改进方案都是在编码方案的层面上进行改进, 在应用方面, 视觉密码依然局限于打印到透明胶片上叠加和使用电脑进行叠加. 在之前的工作中, 我们提出了不可见视觉密码方案, 并开发了相应的光学隐藏系统[32–35], 将传统的视觉密码编码后的分享图像转换为纯相位的衍射光学元件, 扩大了应用范围, 同时也增强了安全性.

本文继承了不可见视觉密码的概念, 提出一种基于增强型视觉密码 (extended visual cryptography, EVC) 的光学信息隐藏系统. 相较于之前的工作, 该系统可隐藏有意义的图像而不再是文本信息, 提高了隐蔽性, 并且信息容量大幅度提升.

2 实现方案

我们设计的增强型视觉密码光学隐藏系统 (EVC-based optical hiding system, EVCOH) 是一个具有门限性的图像隐藏系统, 可以将秘密图像分解成多个有意义图像并隐藏于衍射光学元件 (diffractive optical elements, DOEs) 中. 提取过程如图 1 所示, 使用指定波长 λ 的激光照射衍射光学元件, 这些 DOEs 的相位分布为 $\varphi_1(x,y), \varphi_2(x,y), \cdots, \varphi_n(x,y)$, 出射光波复振幅为 $\exp[\mathrm{j}\varphi_1(x,y)]$, $\exp[\mathrm{j}\varphi_2(x,y)], \cdots, \exp[\mathrm{j}\varphi_n(x,y)]$. 光波继续传播后再现有意义的分享图像, 这里传播过程以傅里叶变换为例, 再现图像的复振幅为 $P_1(u,v), P_2(u,v), \cdots, P_n(u,v)$.

* 国家自然科学基金 (批准号: 61575197) 和中国科学院青年创新促进会 (批准号: 2017489) 资助的课题.

† 通信作者. E-mail: sysopt@126.com

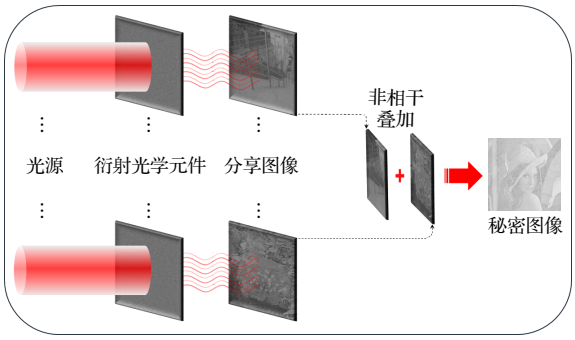

图 1 增强型视觉密码光学隐藏系统: 提取过程

Fig. 1. EVC-based optical hiding system: The extraction process.

$$\begin{aligned} P_1(u,v) &= \mathrm{FT}\{\exp[\mathrm{j}\varphi_1(x,y)]\},\\ P_2(u,v) &= \mathrm{FT}\{\exp[\mathrm{j}\varphi_2(x,y)]\},\\ &\vdots\\ P_n(u,v) &= \mathrm{FT}\{\exp[\mathrm{j}\varphi_n(x,y)]\}. \end{aligned} \tag{1}$$

将数量大于门限 k 的分享图像进行非相干叠加即可恢复秘密图像 $S(u,v)$. 如选取前 k 幅分享图像叠加, 即可恢复秘密图像:

$$|P_1(u,v)|^2+\cdots+|P_k(u,v)|^2=S(u,v). \tag{2}$$

提取操作并不复杂, 不需要掌握光学或者密码学知识亦可提取出秘密信息, 保留了视觉密码的简单性. 该系统的隐藏过程如图 2 所示, 分为两个步骤.

2.1 增强型视觉密码方案编码

选定秘密信息和掩饰图像, 使用增强型视觉密码方案编码后, 获得分享图像. 增强型视觉密码是一种有效的加密技术, 是 Ateniese 等[36] 于 2001 年初次提出, 其本质是一个 (k, n) 秘密分享问题. 在给定了秘密图像和掩饰图像后, 生成 n 幅分享图像, 分享图像是掩饰图像经过编码后生成的半色调图像, 如图 3 中第一幅分享图像. 当任意 k 幅或更多的分享图像叠在一起时, 就可获取秘密图像; 而少于 k 幅时, 就无法恢复出秘密图像.

该方案的编码方法是将秘密信息和分享图像编码为二值化的半色调图像, 原始图像中每个像素的灰度值决定了扩展后子像素中黑白像素数量, 子像素的排序并不影响半色调带来的视觉效果. 但是排序的不同会使分享图像在叠加后得到不同的结果. 以图 4 为例, 两幅分享图像中相同位置的像素的灰度分别为 4/9 和 5/9, 那么转换成半色调图片时, 排序不同, 则叠加后图片的灰度不同. 增强型视觉密码方案正是利用了这一点, 让分享图像叠加后得到预期想要的灰度. 增强型视觉密码在实现对图像加密的同时, 密文变成了有意义的图像, 提高了密文的可信度. 同时, 解密过程不需要任何密码学的知识, 也不需要计算, 其简单性让任何人都可以使用. 而且, 相较于传统视觉密码, 分享图像不再是无意义的随机噪声, 而是有意义的图像, 大幅度提高了信息容量, 也降低了被怀疑的可能性. 图 3 所示是两幅分享图像, 叠加后可以直接分辨出秘密信息.

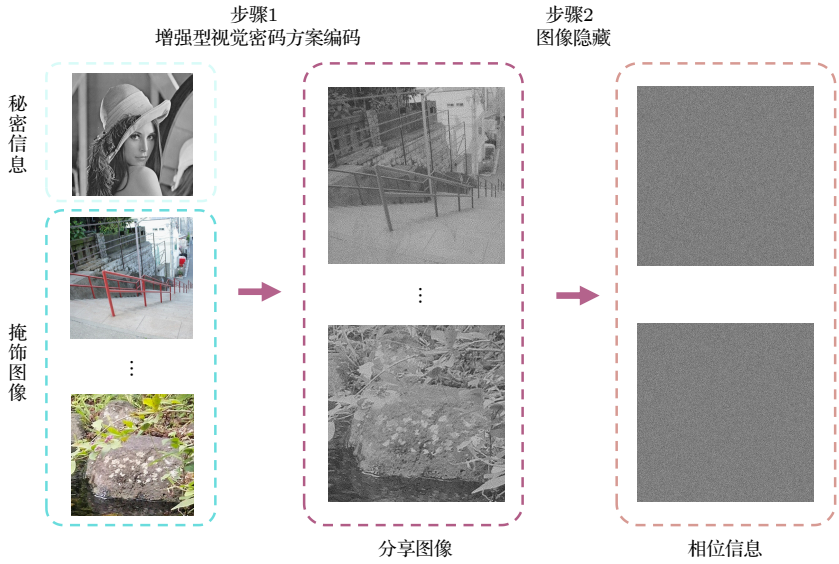

图 2 增强型视觉密码图像隐藏系统: 隐藏过程

Fig. 2. Extended-visual-cryptographic-based optical hiding system: The hiding process.

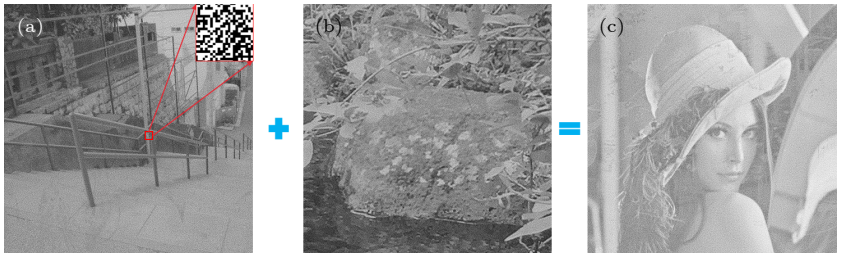

图 3 两幅分享图像 (a), (b) 和叠加后恢复出的秘密信息 (c)

Fig. 3. Two shares (a), (b) are stacked together to recover the secret information (c).

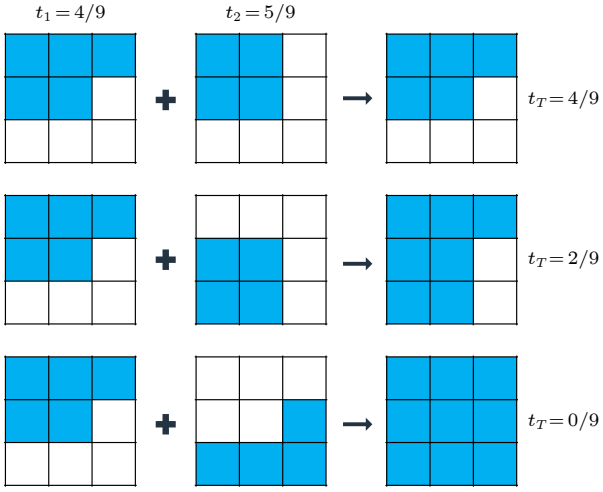

图 4 两个扩展后的子像素不同排序叠加示例, 灰度值为 4/9 和 5/9 的两个像素扩展后按图中方式排序叠加后灰度可以是 4/9, 2/9 和 0/9

Fig. 4. Examples of subpixel arrangements. Arranging two subpixels with $t_1=4/9$ $t_1=4/9$ and $t_2=5/9$ $t_2=5/9$ as the examples make $t_T=4/9$, $t_T=2/9$ and $t_T=0/9$.

2.2 图像隐藏

利用相位恢复算法将图像隐藏到相位密钥中. 将编码后的分享图像作为输出平面的振幅信息, 利用相位恢复算法, 如 GS 算法[37]、杨顾算法[38]等, 计算得到输入平面的相位信息. 这里以 GS 算法为例, 流程如图 5 所示.

1) 将分享图像 $S(u,v)$ 作为输出面光强, 赋予随机相位信息 $\phi_1(u,v)$, 得到输出面复振幅 $P_1(u,v)$:

$$P_1(u,v)=S(u,v)\exp[\mathrm{j}\varphi_1(u,v)]; \tag{3}$$

2) 对输出面复振幅做傅里叶逆变换, 得到输入面复振幅 $P_k(x,y)$:

$$P_k(x,y)=\mathrm{IFT}\{P_k(u,v)\}=|P_k(x,y)|\exp[\mathrm{j}\theta_k(x,y)]; \tag{4}$$

3) 保留输入面复振幅的相位信息:

$$P'_k(x,y)=\exp[\mathrm{j}\theta_k(x,y)]; \tag{5}$$

4) 对输入面复振幅做傅里叶变换, 得到输出面复振幅 $P'_k(u,v)$:

$$P'_k(u,v)=\mathrm{FT}\{P'_k(x,y)\}=|P'{}_k(u,v)|\exp[j\varphi'_k(u,v)]; \tag{6}$$

5) 计算输出面光强和分享图像的和方差 $\mathrm{SSE}[|P'{}_k(u,v)|^2,S(u,v)]$;

6) 若和方差不符合标准, 则用分享图像作为光强替换输出平面振幅, 得到新的输出面分振幅 $P_{k+1}(u,v)$, 重复步骤 2)—6):

$$P_{k+1}(u,v)=\sqrt{S(u,v)}\exp[\mathrm{j}\varphi'_k(u,v)]; \tag{7}$$

7) 若和方差符合标准, 则将 $\theta_k(x,y)$ 作为结果输出.

经过上面的步骤后, 秘密信息就被隐藏在相位密钥中, 实际应用中可将相位密钥制作成衍射光学元件, 将分享图像实体化并且隐蔽性更强.

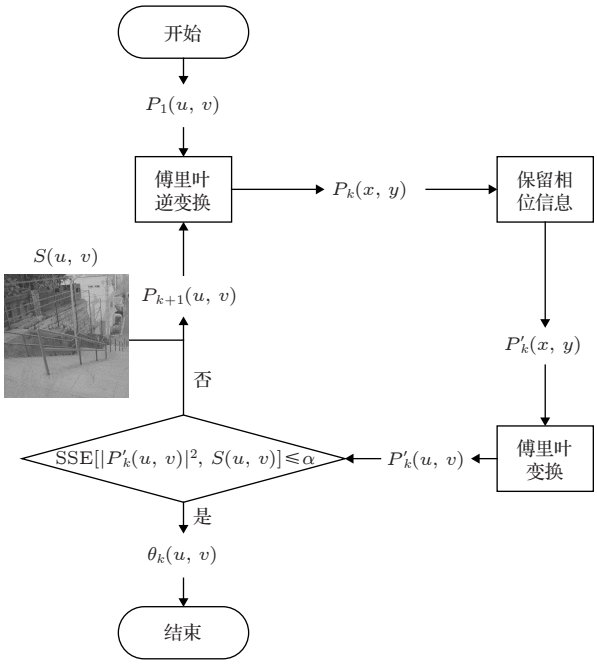

图 5 图像隐藏过程中相位密钥生成算法例: GS 算法流程示意图

Fig. 5. A example of phase-keys generation algorithms: GS algorithm flow diagram.

3 实验与分析

3.1 仿真实验

为简便起见, 我们使用了 (2, 2) 增强型视觉密码方案编码, 以图 6(a),(b) 作为分享图像的掩饰图像, 图 6(c) 作为秘密信息, 分辨率为 512 × 152, 编码后得到分享图像图 6(d), (e), 原图中 1 个像素扩展成 4 × 4 的子像素, 分辨率扩展为 2048 × 2048, 叠加后得到图 6(f), 可以分辨出秘密信息. 将两幅分享图像作为输出平面的振幅信息, 利用前文举例的 GS 算法, 计算得到输入平面相位信息如图 6(g), (h) 所示. 至此, 秘密信息便隐藏在这两幅相位信息中, 这些相位信息可以作为密钥, 若制成衍射光学元件, 秘密信息隐藏在透明元件中, 隐蔽性极高. 模拟仿真提取过程, 将前面所得相位密钥作为输入平面, 计算得到输出平面光强信息如图 6(i), (j). 将两幅光强信息叠加后得到图 6(k), 完成了提取过程, 从图中依然可以分辨出秘密信息, 提取成功.

3.2 光学实验

通过光学实验来验证该方案是否可应用于实际. 搭建了如图 7 所示的光路, 激光器使用的是 THORLABS 公司的 HNL-S008 R 型号氦氖激光器, 波长 632.8 nm, 空间光调制器的型号是 HOLOEYE PLUTO-VIS, CCD 相机使用的是 Mikrotron 公司的 EoSens3 CL 型号相机. 实验时, 氦氖激光器发出的光, 经过显微物镜、针孔和凸透镜组成的扩束系统扩束后, 使用偏振片调整光束偏振方向与空间光调制器的长边一致, 之后光束透过分光棱镜照射到空间光调制器上, 空间光调制器上加载相位密钥, 调制后的光束经过分光棱镜的反射, 再通过傅里叶透镜后被 CCD 相机接收.

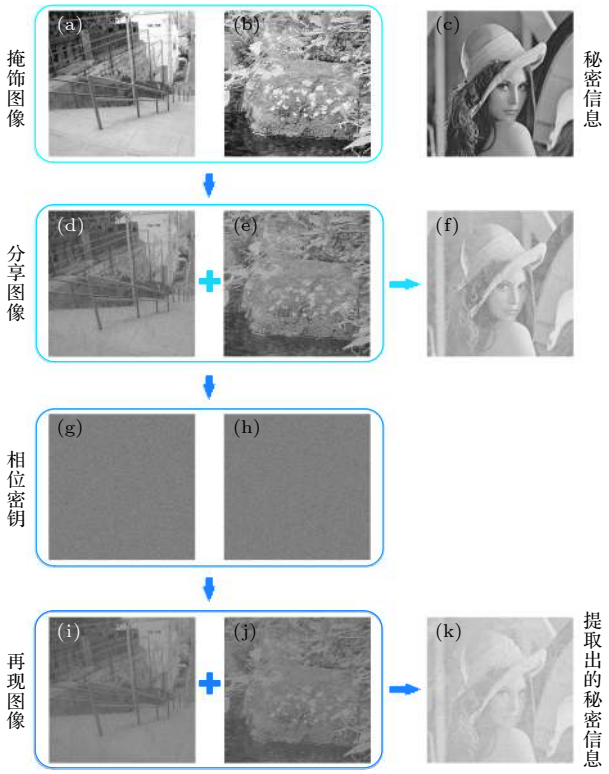

图 6 (a), (b) 分享图像的掩饰图像; (c) 秘密信息; (d), (e) 编码后的分享图像; (f) (d), (e) 叠加后的秘密信息; (g), (h) 隐藏了分享图像的相位密钥; (i), (j) 利用 (g), (h) 再现的分享图像; (k) (i), (j) 非相干叠加后提取的秘密信息

Fig. 6. (a), (b) The original images of shares; (c) the secret image; (d), (e) the shares; (f) the secret images decrypted by stacked (d), (e) together; (g), (h) the phase keys; (i), (j) the reconstructed shares using (g), (h); (k) the recover secret images by stacking (i), (j) together.

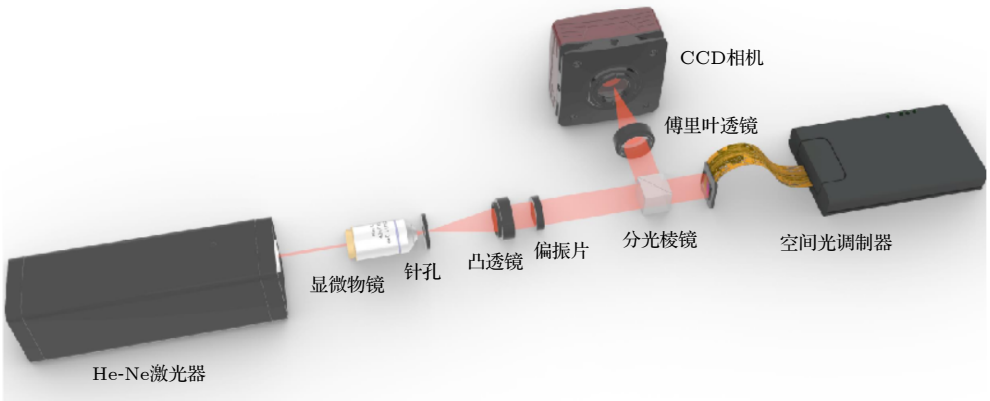

图 7 图像隐藏系统提取实验光路图

Fig. 7. Optical setup for the extraction process of EVCOH.

为了简单起见, 选择较为简单的字母“H”图案作为秘密信息, 字母“A”, “B”作为分享图像的掩饰图案, 通过增强型视觉密码方案编码后的分享图像如图 8(a),(b), 分辨率是 48 × 48, 叠加后可以分辨出秘密信息. 为了再现时有较好的效果, 我们将分享图像扩展至 192 × 192, 通过相位恢复算法计算得到相位密钥如图 8(d),(e), 分辨率为 192 × 192, 计算时假设再现光束是平面波. 将两幅相位密钥加载到空间光调制器上, 我们接收到的图像如图 8(f),(g), 由于原图较暗, 这里调整亮度方便观看, 后续处理依旧使用的采集到的原图. 使用 MATLAB 将两幅采集到的图片叠加, 生成图 8(h), 可以看出虽然光束只是经过扩束系统扩束, 没有特殊调整, 再现光依旧是高斯分布, 但是图中仍可以分辨出秘密信息, 可见系统对于再现光是否是平面波有一定容忍程度. 至此初步验证了该方案可应用于实际.

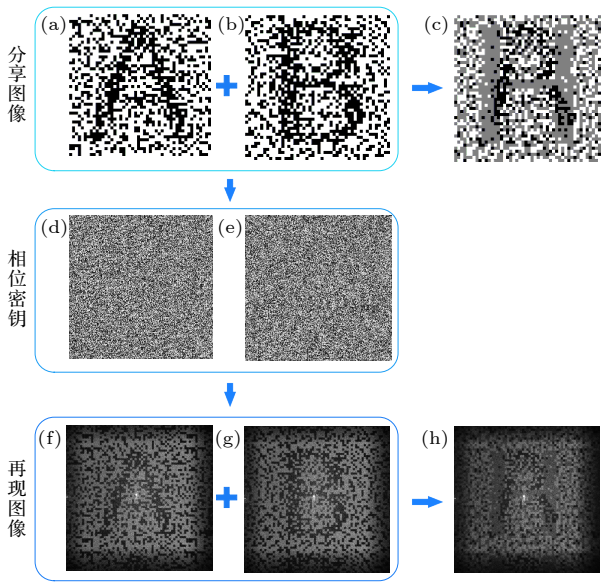

图 8 (a), (b) 分享图像; (c) (a), (b) 叠加后的秘密信息; (d), (e) 隐藏了分享图像的相位密钥; (f), (g) CCD 相机采集到的再现后分享图像; (h) 非相干叠加后的秘密信息

Fig. 8. (a), (b) The shares, (c) the secret images decrypted by stacked (a), (b) together; (d), (e) the phase keys; (f), (g) the reconstructed shares that were taken with a CCD camera; (h) the recover secret images by stacking (f), (g) together.

4 安全性分析

对该系统进行适应性选择密文攻击, 以验证该系统的不可区分性安全. 假设 A 作为攻击者, B 作为挑战者, EVCOH 隐藏过程步骤 1 使用 (k, n) 增强型视觉密码. 阶段 1: 攻击者 A 向挑战者 B 发送密文 c, 要求提取秘密信息, B 对密文 c 提取获得明文图像 M, 将 M 发送给 A. 这一阶段 A 可以自由选择密文, 并在满意后进入阶段 2. 阶段 2: 攻击者 A 串通 $k-1$ 个解密者. 阶段 3: 攻击者选择两个等大的图像 M0, M1, 将它们发送给挑战者 B. 阶段 4: 挑战者 B 随机选择一个图像进行加密, 获得 n 幅密文, 将密文分发给 n 位解密者. 阶段 5: $k-1$ 位解密者将密文 c* 透露给攻击者 A 后, A 可以继续要求解密服务, 如阶段 1, 但是不能对 c* 进行询问. 阶段 6: A 做出对挑战者选择的猜测. 攻击过程结束.

阶段 1 中, 攻击者可以对通过尝试对 EVCOH 系统进行猜测分析. 该系统生成的密钥是相位密钥, 制成 DOEs 后具有极高的隐蔽性, 外观上很难察觉不同密钥之间的区别. 假设攻击者对光学领域较为熟悉, 判断出密钥是相位密钥, 可以再现图像. 然而这些图像是具有实际意义的图像, 弥补了传统视觉密码中类似噪声的分享图像容易引起怀疑的缺点, 攻击者找出一幅明文图像和多个密文图像之间的关系极为困难. 即便在阶段 1 中攻击者反复尝试破解了该系统, 得知了密文需要使用激光照射再现分享图像后叠加提取, 并且我们极为宽容地让攻击者串通了 $k-1$ 位解密者, 获得了 $k-1$ 幅密文. 由于只获得了 $k-1$ 幅密文, 小于门限阈值 k, 叠加后是不会得到秘密信息的. 而且, 隐藏过程中分享图像的掩饰图是自行选择的, 两次加密过程之间相互毫无关系, 即便这一阶段 A 继续要求解密服务也无法得到更多的密文. 所以攻击者 A 无法区分是对哪个明文进行加密. 因此该系统是不可区分适应性选择密文安全, 具有很高的安全性.

5 鲁棒性分析

考虑到实际应用中, 对提取过程造成影响的可归结为相位密钥在存储或传输过程中受到的噪声干扰. 因此将噪声直接添加到相位密钥中, 为简化分析, 直接使用前面仿真实验所得相位密钥, 台阶数为 256 阶, 将噪声添加到两幅密钥中. 这里使用了三种噪声进行测试, 分别是随机噪声、高斯噪声和瑞利噪声, 信噪比为 0—70 dB. 使用增强型视觉密码编码后所得分享图像叠加后的解密图像与有噪声的情况下的提取图像之间的相关系数来评价

提取质量. 如图 9 所示, 随着信噪比的提高, 噪声减小, 相关系数提高. 添加高斯噪声的情况下, 信噪比 14 dB 就可以提取出秘密信息, 随机噪声和瑞利噪声也在信噪比 18 dB 时可以提取出秘密信息, 在加入噪声的信噪比大于 20 dB 时, 相关系数基本稳定且接近于 1. 为了接近实际应用情况, 我们设计了台阶数为 4 阶的相位密钥, 使用上面的方法测试, 信噪比 0—30 dB, 结果如图 10 所示. 相较于台阶数 256 阶时, 抗噪声能力有所提升, 添加高斯噪声时, 信噪比 7 dB 时就可以分辨出秘密信息, 随机噪声和瑞利噪声也在 13 dB 和 12 dB 时可以分辨秘密信息. 但是 4 台阶的相位密钥对于秘密信息的细节体现不足, 相关系数只能稳定在 0.8 左右. 由此可以证明, 该系统在抗噪声方面一般, 相较于本课题组之前提出的视觉密码光学隐藏系统 (visual-cryptography-based optical hiding system, VCOH)[32–35], 鲁棒性有所下降. 分析原因是该系统加密图像和分享图像都是有意义图像, 相较于 VCOH 系统, 再现分享图像时要求还原度更高, 因此鲁棒性较为一般.

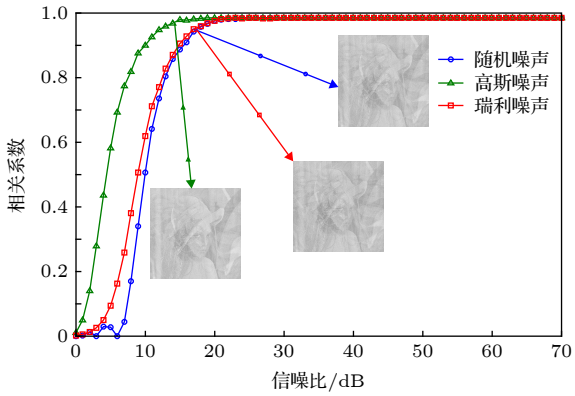

图 9 系统的噪声分析

Fig. 9. Noise analysis of EVCOH.

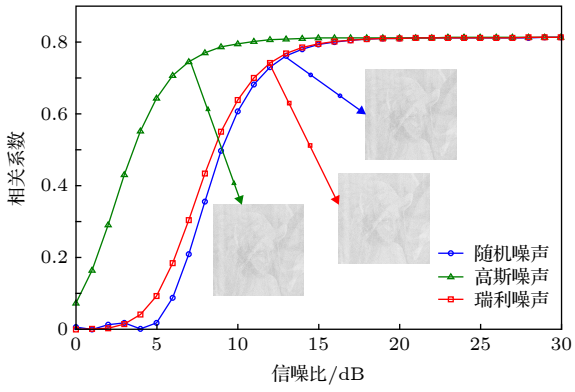

图 10 相位密钥台阶数为 4 时, 系统噪声分析

Fig. 10. Noise analysis of EVCOH when the phase keys are four steps.

6 结 论

我们提出了一种基于增强型视觉密码的光学信息隐藏系统, 可将秘密图像拆分成多个有意义的分享图像, 并隐藏于相位密钥中, 相较于之前的工作, 该系统可隐藏有意义的图像, 而不再是文本信息, 大幅度提高了信息容量. 隐藏过程分为两步. 首先, 使用增强型视觉密码方案将秘密信息隐藏在多个有意义的图像中. 然后, 利用相位恢复算法将分享图像转换为相位信息, 这些相位信息作为密钥便可以制作成衍射光学元件, 秘密信息便隐藏于这些元件中. 通过仿真实验和光学实验验证了方案的可行性, 并对该系统进行了详细分析. 该系统保留了视觉密码的简单性, 同时还具有很高的安全性, 并且扩展了视觉密码的应用范围, 不再局限于胶片和数字信息两种形式. 由于实验条件限制, 光学实验选取图像较为简单, 提高光学实验效果, 实现更复杂的图像隐藏实验是本课题组进一步的研究目标.

参考文献

[1] Khan M, Shah T 2014 *3 D Res.* **5** 29
[2] Chen W, Javidi B, Chen X D 2014 *Adv. Opt. Photonics* **6** 120
[3] Liu S, Guo C L, Sheridan J T 2014 *Opt. Laser Technol.* **57** 327
[4] Shi Y S, Situ G H, Zhang J J 2007 *Opt. Lett.* **32** 1914
[5] Shi Y S, Situ G H, Zhang J J 2008 *Opt. Lett.* **33** 542
[6] Yang Y H, Shi Y S, Wang Y L, Xiao J, Zhang J J 2011 *Acta Phys. Sin.* **60** 034202 (in Chinese) [杨玉花, 史祎诗, 王雅丽, 肖俊, 张静娟 2011 物理学报 **60** 034202]
[7] Shi Y S, Li T, Wang Y L, Gao Q K, Zhang S G, Li H F 2013 *Opt. Lett.* **38** 1425
[8] Gao Q H, Wang Y L, Li T, Shi Y S 2014 *Appl. Optics* **53** 4700
[9] Liu X L, Pan Z, Wang Y L, Shi Y S 2015 *Acta Phys. Sin.* **64** 234201 (in Chinese) [刘祥磊, 潘泽, 王雅丽, 史祎诗 2015 物理学报 **64** 234201]
[10] Chanana A, Paulsen A, Guruswamy S, Nahata A 2016 *Optica* **3** 1466
[11] Xu W H, Xu H F, Luo Y, Li T, Shi Y S 2016 *Opt. Express* **24** 27922
[12] Yao L L, Yuan C J, Qiang J J, Feng S T, Nie S P 2016 *Acta Phys. Sin.* **65** 214203 (in Chinese) [姚丽莉, 袁操今, 强俊杰, 冯少彤, 聂守平 2016 物理学报 **65** 214203]
[13] Kong D Z, Shen X J, Cao L C, Jin G F 2017 *Appl. Opt.* **56** 3449
[14] Xu F H, Shulkind G, Thrampoulidis C, Shapiro J H, Torralba A, Wong F N C, Wornell Gr W 2018 *Opt. Express* **26** 9945

[15] Zhang L H, Yuan X, Zhang D W, Chen J 2018 *Curr. Opt. Photon.* **2** 315
[16] Xi S X, Yu N N, Wang X L, Zhu Q F, Dong Z, Wang W, Liu X H, Wang H Y 2019 *Acta Phys. Sin.* **68** 110502 (in Chinese) [席思星, 于娜娜, 王晓雷, 朱巧芬, 董昭, 王微, 刘秀红, 王华英 2019 物理学报 **68** 110502]
[17] Wang X G, Li M, Yu N N, Xi S X, Wang X L, Lang L Y 2019 *Acta Phys. Sin.* **68** 240503 (in Chinese) [王雪光, 李明, 于娜娜, 席思星, 王晓雷, 郎利影 2019 物理学报 **68** 240503]
[18] Naor M, Shamir M 1994 *Lect. Notes Comput. Sci.* **950** 1
[19] Blundo C, Bonis A D, Santis A D 2001 *Designs Codes Cryptogr.* **24** 255
[20] Cimato S, Santis A D, Ferrara A L, Masucci B 2005 *Inf. Process. Lett.* **93** 199
[21] Blundo C, Santis A D, Naor M 2000 *Inf. Proc. Lett.* **75** 255
[22] Lin C C, Tsai W H 2003 *Pattern Recognit. Lett.* **24** 349
[23] Lukac R, Plataniotis K N 2005 *Pattern Recognit.* **38** 767
[24] Hou Y C 2003 *Pattern Recognit.* **36** 1619
[25] Yamamoto H, Hayasaki Y, Nishida N 2004 *Opt. Express* **12** 1258
[26] Machizaud J, Fournel T 2012 *Opt. Express* **20** 22847
[27] Wu H C, Chang C C 2005 *Comput. Stand. Interfaces* **28** 123
[28] Feng J B, Wu H C, Tsai C S, Chang Y F, Chu Y P 2008 *Pattern Recognit.* **41** 3572
[29] Mishra A, Gupta A 2018 *J. Inf. and Optim. Sci.* **39** 631
[30] Blundo C, Cimato S, Santis A D 2006 *Theor. Comput. Sci.* **369** 169
[31] Chen Y F, Chan Y K, Huang C C, Tsai M H, Chu Y P 2007 *Inf. Sci.* **177** 4696
[32] Shi Y S, Yang X B 2017 *J. Opt.* **19** 115703
[33] Shi Y S, Yang X B 2017 *Chin. Phys. Lett.* **34** 114204
[34] Yang N, Gao Q K, Shi Y S 2018 *Opt. Express* **26** 31995
[35] Li Z F, Dong G Y, Yang D Y, Li G L, Shi Y S, Bi K, Zhou J 2019 *Opt. Express* **27** 19212
[36] Ateniese G, Blundo C, Santis A D, Stinson D R 2001 *Theor. Comput. Sci.* **250** 143
[37] Gerchberg R W, Saxton W O 1972 *Optik* **35** 237
[38] Yang G Z, Gu B Y 1981 *Acta Phys. Sin.* **30** 410 (in Chinese) [杨国桢, 顾本源 1981 物理学报 **30** 410]

Enhanced-visual-cryptography-based optical information hiding system*

Yu Tao Yang Dong-Yu Ma Rui Zhu Yu-Peng Shi Yi-Shi †

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

(Received 4 April 2020; revised manuscript received 17 April 2020)

Abstract

Recent years, with the rapid development of information technology, the information security has received more and more attention. A variety of encryption methods to protect the information have been reported. Visual cryptography is one of the encryption methods, which has highly security because of its threshold feature. And the cryptographic information can be explained by a naked eye in the decryption process. In the application of visual cryptography, however, each shared image is limited to transparency films and overlapping on computer. In our previous work, we proposed the scheme of invisible visual cryptography and developed the visual-cryptography-based optical hiding system (VCOH), which transformed the conventional visual cryptography shares into diffraction optical elements (DOEs). It not only increases the application range of visual cryptography, but also enhances security. In this paper, we propose an optical information hiding system based on the extended visual cryptography, which inherits the concept of invisible visual cryptography. In contrast to our previous work, the method proposed in this work can hide a meaningful image instead of text messages. Meanwhile, the capacity and imperceptibility of the method are greatly increased. The hiding process of the system contains two steps. Firstly, the secret image is converted into meaningful shares through the extended visual cryptography algorithm. Secondly, the meaningful shares are able to hide in phase-keys through an iterative phase retrieval algorithm, such as Gerchberg-Saxton algorithm and Yang-Gu iterative algorithm. Then the phase-keys can be made into diffraction optical elements (DOEs) to store and transport in a physical way. In the decryption process, DOEs are illuminated with the laser beam to reconstruct the meaningful shares. The secret image can be explained by the direct overlapping of the reconstructed shares without any optical or cryptographic knowledge. The simulation and optical experimental results show that the proposed method has good performance of security and validate the feasibility of the proposed method. Besides, in this paper the robustness and security issues are also analyzed. This system has a high security because of its indistinguishability under adaptive chosen ciphertext attack (IND-CCA2) security. Additionally, this system is relatively less robust than the VCOH because it shares meaningful images with highly complex and detailed structures.

Keywords: optical hiding, extended visual cryptography, Fourier optics, phase-only keys

PACS: 42.30.–d, 42.30.Rx **DOI:** 10.7498/aps.69.20200496

* Project supported by the National Natural Science Foundation of China (Grant No. 61575197) and the Youth Innovation Promotion Association Chinese Academy of Sciences (Grant No. 2017489).

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