基于光学隐藏视觉密码的欺骗追踪系统*

吴承哲[1)] 刘睿泽[1)] 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 29 日收到; 2024 年 5 月 15 日收到修改稿)

提出了一种基于光学隐藏视觉密码的欺骗追踪系统. 该系统将秘密图像分解为多幅有实际意义的掩饰图像, 将其中一张掩饰图像嵌入脆弱水印, 作为检验密钥, 检验密钥单独传输. 然后将其余掩饰图像隐藏在相位密钥中, 进行传输时有很好的不可见性. 掩饰图像的像素排列若被不诚实的参与者篡改, 则称为欺骗图像. 将每张相位密钥分发给不同的参与者, 以保证在追踪到欺骗图像时可找到对应的欺骗者. 在提取过程中, 只需要对该相位密钥进行傅里叶变换, 即可得到掩饰图像. 检验时, 将检验密钥与任一掩饰图像进行非相干叠加, 以是否出现验证图像为条件, 就可检验掩饰图像是否被篡改, 以达到欺骗追踪的目的, 将数量大于等于门限 k 的掩饰图像和检验密钥进行非相干叠加即可得到秘密图像, 仿真实验结果表明, 该系统可应用于利用不可见视觉密码术传递实际信息时, 对内部欺骗者的追踪.

关键词: 光学隐藏, 视觉密码, 相位密钥, 欺骗追踪

PACS: 42.15.Eq, 42.25.Fx, 42.30.–d, 42.30.Rx **DOI:** 10.7498/aps.73.20231721

1 引 言

近年来, 伴随着科技不断进步, 信息安全的重要性也随之增高, 目前, 信息有很多种加密方法[1–12]. 其中, Naor 和 Shamir 在 1994 年提出的视觉密码 (visual cryptography, VC) 方案, 该方案的解密过程依靠人类的视觉系统从分享图像的叠加过程种提取秘密信息. 视觉密码方案在过去三十年里得到了很大的发展, 如优化对比度、灰度图像加密、彩色图像加密、扩展信息容量、提高分辨率等[13–18].

VC 方案是以参与者是诚实可信为前提的, 但是事实是每张分享图像在分配给不同的参与者后, 一些不诚实的参与者会通过修改自己的分享来欺骗其他的分享者, 以达到干扰恢复秘密图像的目的. 在秘密图像遭到欺骗攻击时, 为保证系统的纯洁性, 快速追踪到欺骗者尤为关键.

在之前的工作中, 我们提出了不可见视觉密码 (invisible visual cryptography, IVC) 方案, 并开发了相应的光学隐藏系统, 将传统的视觉密码编码后的分享图像转换为相位信息, 扩大了应用范围, 同时也增强了安全性[19–24].

本文继承了不可见视觉密码的概念, 将欺骗追踪视觉密码的编码方案与不可见视觉密码结合, 提出一种基于光学隐藏视觉密码的欺骗追踪系统[25]. 相较于之前的工作, 该系统有以下优势: 分享图像的内容不再是无意义的乱码, 而是可以包含内容的掩饰图像, 减小了秘密信息被怀疑的可能, 提高了秘密信息的隐蔽性; 脆弱水印的加入能判断检验密钥被攻击与否, 具有很强的隐蔽性和脆弱性; 该方案具有验证能力, 仅需将检验密钥和掩饰图像进行非相干叠加, 若出现验证图像则证明掩饰图像的内

* 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、中国科学院大学和中央高校基本科研业务费资助的课题.

† 通信作者. E-mail: shiyishi@ucas.ac.cn

容没有被篡改, 若没有出现则证明验证图像被篡改, 具有非常快速、简单的欺骗追踪功能.

2 实现方案

我们所设计的基于光学隐藏视觉密码的欺骗追踪系统是一个具有门限性的光学隐藏系统, 可分为: 分解秘密图像、隐藏掩饰图像、嵌入脆弱水印、再现掩饰图像、检验掩饰图像、恢复秘密图像总共 6 个步骤.

秘密图像、验证图像、掩饰图像的内容为有意义的图像. 这里秘密图像、验证图像、掩饰图像上的内容均使用字符图像. 水印图像可用任何可识别内容的图像.

其中, 再现、检验、恢复的步骤如图 1 所示, 再现掩饰图像时, 使用特定的激光对相位密钥进行衍射, 出射光波复振幅为 $\exp[\mathrm{j}\varphi_1(x,y)]$, $\exp[\mathrm{j}\varphi_2(x,y)]$, …, $\exp[\mathrm{j}\varphi_n(x,y)]$, 光波继续传播后再现有意义的掩饰图像, 传播过程以傅里叶变换为例, 再现图像的复振幅为

$$P_1(u,v)=\mathrm{FT}\{\exp[\mathrm{j}\varphi_1(x,y)]\}, \tag{1}$$

$$P_2(u,v)=\mathrm{FT}\{\exp[\mathrm{j}\varphi_2(x,y)]\}, \tag{2}$$

$$\cdots$$

$$P_n(u,v)=\mathrm{FT}\{\exp[\mathrm{j}\varphi_n(x,y)]\}. \tag{3}$$

将数量大于等于门限 k 的掩饰图像和检验密钥进行非相干叠加即可恢复秘密图像 $\mathrm{SC}(u,v)$, 可恢复秘密图像

$$|P_1(u,v)|^2+|P_2(u,v)|^2+\cdots+|P_{k-1}(u,v)|^2+|P_t(u,v)|^2=\mathrm{SC}(u,v), \tag{4}$$

其中 $P_t(u,v)$ 为检验密钥.

如图 1 所示, 在验证时, 将检验密钥与任一掩饰图像进行非相干叠加, 以是否出现验证图像为条件, 就可检验掩饰图像是否被篡改, 若有欺骗者对其掩饰图像进行了像素排布的篡改, 虽然掩饰图像看上去没有进行改变, 但是秘密图像已经无法恢复, 则可通过检验密钥与掩饰图像进行叠加来追踪到欺骗者, 经过篡改的欺骗图像在与检验密钥叠加时, 无法恢复出验证图像, 而正常的掩饰图像则可与检验密钥叠加出验证图像. 若无欺骗图像, 将数量大于等于门限 k 的掩饰图像和检验密钥进行非相干叠加即可得到秘密图像.

图 2 所示为分解、隐藏、嵌入脆弱水印的过程. 首先, 利用视觉密码术, 根据秘密图像、验证图像、掩饰图像的内容, 将秘密图像分解成若干掩饰图像. 将其中一张掩饰图像嵌入脆弱水印图像, 作为检验密钥, 其余掩饰图像利用相位恢复算法, 得到其相位信息. 将每张相位密钥分发给不同的参与者, 以保证在追踪到欺骗图像时可找到对应的欺骗者. 检验密钥和相位密钥可存放在硬盘、U 盘等可存放信息的介质中, 为保证检验密钥在传输时受到尽量小的影响, 直接保存检验密钥的矩阵数据进行传输, 而非图像数据.

2.1 欺骗追踪视觉密码加密方案

为了达到不同的图像可以很好地分辨, 并且掩饰图像有意义的效果, 这里选择将一个原图像素扩展为多个像素的方案, 然后利用不同的汉明重量来对 3 张图片进行加密. 其原理如图 3 所示, 选择大小相同的秘密图像、验证图像、掩饰图像共 3 张二值图, 根据 3 幅图相同位置像素排列的情况, 利用

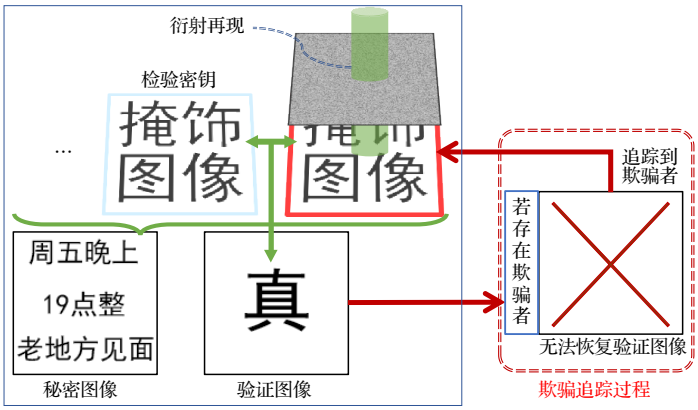

图 1 再现、检验、恢复过程

Fig. 1. Reproducing, verifying, and restoring process.

像素扩展的视觉密码术对秘密图像进行分解, 最终获得多张含有迷惑性信息的掩饰图像, 并且分解得到的任意两张掩饰图像叠加可得到验证图像.

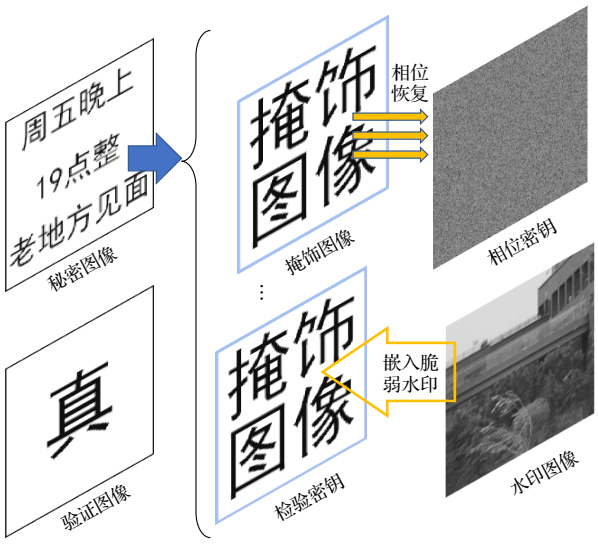

图 2 分解、隐藏、嵌入脆弱水印过程

Fig. 2. Decomposition, hiding, embedding fragile watermarking process.

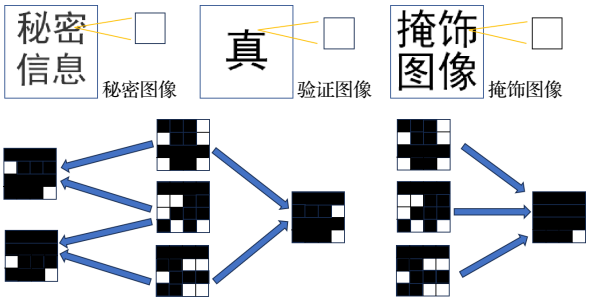

图 3 当秘密图像、验证图像、掩饰图像相同位置的像素均为白色时的编码方案

Fig. 3. Encoding scheme when the pixels in the same position of secret image, verification image, and masking image pixels are all white.

这里以 (3.3) 方案为例, 即将一幅秘密图像分解成 3 张掩饰图像, 3 张掩饰图像叠加可得到秘密图像的方案. 选择把一个原像素扩展为 16 个扩展像素的方案. 视觉密码术的具体加密流程如下: 首先, 选择秘密图像, 验证图像, 掩饰图像共 3 幅大小相同的二值图, 则相同位置的像素选择则有 8 种情况. 在选定 3 幅图后, 需要对这 3 幅图像素一一进行加密, 编码的规则要满足: 在相同位置上, 当掩饰图像为白色像素, 则扩展像素中有 5 个白色像素, 黑色则有 4 个白色像素; 当验证图像为白色像素时, 则任意两个扩展像素叠加之后有 2 个白色像素, 黑色则有 1 个白色像素; 当秘密图像为白色像素, 则 3 个扩展像素叠加之后有 1 个白色像素, 黑色则叠加后没有白色像素. 将所有像素依次进行加密后, 即可得到 3 张包含信息的掩饰图像.

如图 3 所示为秘密图像、验证图像、掩饰图像相同位置的像素均为白色时的编码方案. 其余 7 种像素排列方式不一一列图举例, 遵照编码规则设计加密矩阵即可.

2.2 图像隐藏

利用相位恢复算法将掩饰图像隐藏到相位密钥中. 将掩饰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、杨顾算法等, 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 4 所示.

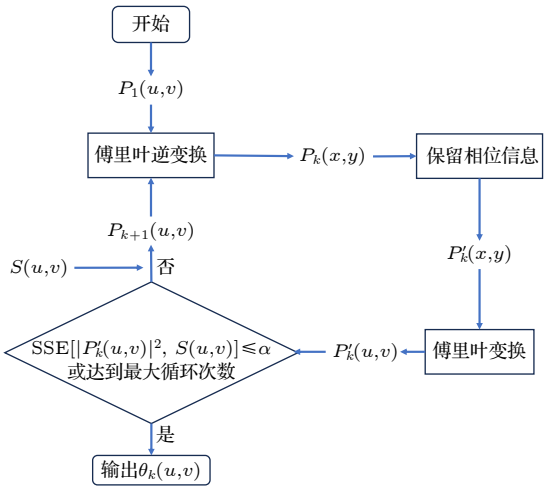

图 4 GS 算法流程

Fig. 4. GS algorithm flow.

1) 将掩饰图像 $S(u,v)$ 作为输出面光强, 赋予随机相位 $\varphi_1(u,v)$ 信息 , 得到输出面复振幅 $P_1(u,v)$:

$$P_1(u,v)=S(u,v)\exp[\mathrm{j}\varphi_1(u,v)]. \tag{5}$$

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

$$\begin{aligned}P_k(x,y)&=\mathrm{IFT}\{P_k(u,v)\}\\&=|P_k(x,y)|\exp[\mathrm{j}\theta_k(x,y)].\end{aligned} \tag{6}$$

3) 保留输入面复振幅的相位信息:

$$P'_k(x,y)=\exp[\mathrm{j}\theta_k(x,y)]. \tag{7}$$

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

$$P'_k(u,v) = \mathrm{FT}\{P'_k(x,y)\} = |P'_k(u,v)|\exp[\mathrm{j}\varphi'_k(u,v)]. \tag{8}$$

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

6) 若和方差不符合标准, 或者未达到设定的循环次数, 则用掩饰图像作为光强替换输出平面振幅, 得到新输出面分振幅 $P_{k+1}(u,v)$, 重复步骤 2)—6):

$$P_{k+1}(u,v) = \sqrt{S(u,v)}\exp[\mathrm{j}\varphi'_k(u,v)]. \tag{9}$$

7) 若和方差符合标准或者达到最大循环次数之后, 则将 $\theta_k(x,y)$ 作为结果输出. 经过上面的步骤后, 掩饰图像就被隐藏在相位密钥中.

2.3 脆弱水印

在图片通过不可信信道传输时, 通常会受到各种攻击, 这些会导致图片的可分辨性下降, 对于一些敏感图片确认图片被攻击与否非常重要. 当脆弱水印被成功提取时, 便可以认为图片未受到攻击.

如图 5 所示, 为嵌入脆弱水印的方案基于 QR 分解和傅里叶变换的嵌入流程, 具体步骤为如下所示.

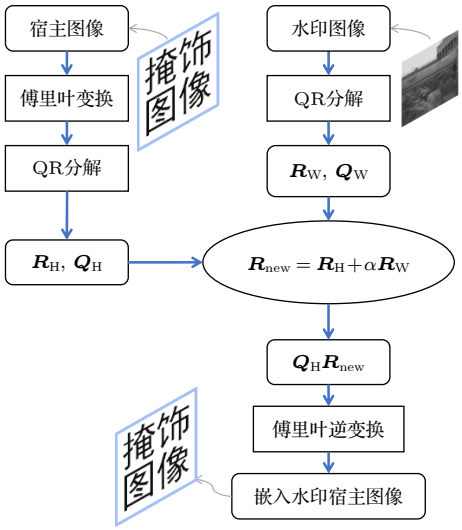

图 5 嵌入脆弱水印流程

Fig. 5. Fragile watermark embedding process.

1) 输入宿主图像 (host image): $H(x,y)$, 水印图像 (water image): $W(x,y)$.

2) 对宿主图像 $H(x,y)$ 进行傅里叶变换得到 $\mathrm{FH}(x,y)$:

$$\mathrm{FH}(x,y) = \mathrm{FT}\{H(x,y)\}. \tag{10}$$

3) 对 $\mathrm{FH}(x,y)$, $W(x,y)$ 分别进行 QR 分解, 得到 $\boldsymbol{R}_\mathrm{H}(x,y)$, $\boldsymbol{Q}_\mathrm{H}(x,y)$ 和 $\boldsymbol{R}_\mathrm{W}(x,y)$, $\boldsymbol{Q}_\mathrm{W}(x,y)$,

$$\mathrm{FH}(x,y) = \boldsymbol{R}_\mathrm{H}(x,y)\cdot\boldsymbol{Q}_\mathrm{H}(x,y), \tag{11}$$

$$W(x,y) = \boldsymbol{R}_\mathrm{W}(x,y)\cdot\boldsymbol{Q}_\mathrm{W}(x,y), \tag{12}$$

其中 $\boldsymbol{R}$ 为上三角矩阵, $\boldsymbol{Q}$ 为正交矩阵.

4) 将 $\boldsymbol{R}_\mathrm{W}(x,y)$ 乘上衰减系数嵌入 $\boldsymbol{R}_\mathrm{H}(x,y)$ 中, 得到新的上三角矩阵 $\boldsymbol{R}_\mathrm{new}(x,y)$:

$$\boldsymbol{R}_\mathrm{new}(x,y) = \boldsymbol{R}_\mathrm{H}(x,y) + \alpha\boldsymbol{R}_\mathrm{W}(x,y), \tag{13}$$

其中 α 为衰减系数.

5) 将 $\boldsymbol{Q}_\mathrm{H}(x,y)$ 乘上新的上三角矩阵 $\boldsymbol{R}_\mathrm{new}(x,y)$, 然后进行傅里叶逆变换就能得到嵌入脆弱水印的宿主图像 $H_\mathrm{new}(x,y)$:

$$H_\mathrm{new}(x,y) = \mathrm{IFT}\{Q_H(x,y)\cdot\boldsymbol{R}_\mathrm{new}(x,y)\}. \tag{14}$$

如图 6 所示为脆弱水印的提取过程, 具体步骤如下所示.

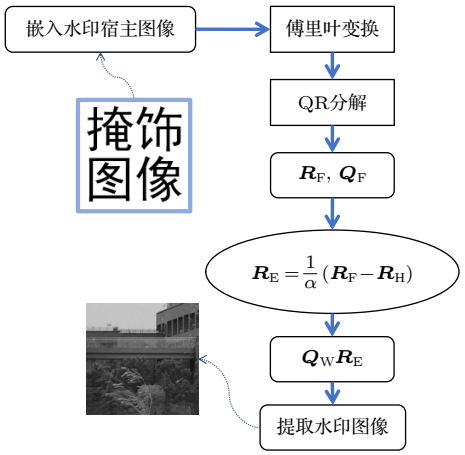

图 6 提取脆弱水印图像流程

Fig. 6. Process of extracting fragile watermark image.

1) 输入嵌入水印的宿主图像 $H_\mathrm{new}(x,y)$, 并对其进行傅里叶变换得到 $\mathrm{FH}_\mathrm{new}(x,y)$:

$$\mathrm{FH}_\mathrm{new}(x,y) = \mathrm{FT}\{H_\mathrm{new}(x,y)\}. \tag{15}$$

2) 对 $\mathrm{FH}_\mathrm{new}(x,y)$ 进行 QR 分解, 得到 $\boldsymbol{R}_\mathrm{F}(x,y)$, $\boldsymbol{Q}_\mathrm{F}(x,y)$, 其中

$$\mathrm{FH}_\mathrm{new}(x,y) = \boldsymbol{R}_\mathrm{F}(x,y)\cdot\boldsymbol{Q}_\mathrm{F}(x,y) . \tag{16}$$

3) 分离出水印图像的上三角矩阵 $R_\mathrm{E}(x,y)$:

$$\boldsymbol{R}_\mathrm{E}(x,y) = \alpha^{-1}\cdot\{\boldsymbol{R}_\mathrm{F}(x,y) - \boldsymbol{R}_\mathrm{H}(x,y)\}. \tag{17}$$

4) 将水印图像的正交矩阵 $\boldsymbol{Q}_\mathrm{W}(x,y)$ 和分离出水印图像的上三角矩阵 $\boldsymbol{R}_\mathrm{E}(x,y)$ 相乘后进行傅里叶逆变换即可得到水印图像:

$$W_{\mathrm{E}}(x,y)=\mathrm{FT}\left\{\boldsymbol{Q}_{\mathrm{W}}(x,y)\cdot\boldsymbol{R}_{\mathrm{E}}(x,y)\right\}. \tag{18}$$

3 模拟与分析

3.1 可行性分析

本文提出的基于光学隐藏视觉密码的欺骗追踪系统, 使用 (3, 3) 视觉密码方案, 所使用的图片均为 128×128 的图像, 扩展后的掩饰图像像素为 512×512. 当有欺骗者拿到相位密钥, 私自获得掩饰图像的内容并篡改其像素排列顺序时, 即使掩饰图像的内容看上去没有变化, 但是秘密图像内容却无法被恢复出来. 需要迅速找到欺骗者的存在, 如图 7 所示. 图 7(a) 为检验密钥; 图 7(b) 为欺骗者篡改掩饰图像的像素排列, 重新隐藏以后衍射得到的欺骗图像; 图 7(c) 为正常的相位密钥衍射出来的掩饰图像; 图 7(d) 为检验密钥和欺骗图像叠加得到的结果, 无法恢复出验证图像的内容; 图 7(e) 为检验密钥和正常的掩饰图像叠加得到的结果; 图 7(f) 为存在欺骗图像存在时, 无法恢复秘密图像. 证明这个过程可以很迅速地找到欺骗图像的存在, 进而找到欺骗者. 为便于呈现相关信息, 采用了伪彩色对图像进行统一增强, 如图 7(d)—(f) 所示.

如图 8 所示, 图 8(a)—(h) 为对脆弱水印的功能实现和攻击测试. 利用衰减系数 $\alpha=0.1$, 将水印图像嵌入宿主图像中. 图 8(a) 为其中一张掩饰图像, 图 8(b) 为水印图像, 图 8(c) 为嵌入水印后的宿主图像, 将嵌入水印的宿主图像与原宿主图像进行对比, 相关系数为 1, 证明该脆弱水印方案具有很强的隐蔽性, 图 8(d) 为提取出来的水印图像.

图 8(e)—(h) 为攻击测试, 分别为添加 0.01 椒盐噪声, 0.01 高斯噪声, 图像压缩, 10×10 像素裁剪攻击后的提取的水印, 证明其具有脆弱性.

在确认检验密钥的脆弱水印是完好后, 可使用其检验的功能, 如图 9 所示, 图 9(a) 为检验密钥, 图 9(b), (c) 为相位密钥经过傅里叶变换得到的掩饰图像, 图 9(d), (e) 为检验密钥分别和两张掩饰图像叠加的结果, 可以得到验证图像的内容“真”, 证明掩饰图像没有被篡改, 3 张图像叠加可恢复出如图 9(f) 的秘密图像. 为便于呈现相关信息, 采用了伪彩色对图像做了统一增强, 如图 9(d)—(f) 所示.

3.2 容量分析

GS 算法为基础的衍射成像可以很好地还原原像素的排布, 所以该方案对秘密信息内容的分辨是否清晰取决于构成字符像素的多少, 并且由于采用的是扩展像素的视觉密码方案, 系统中的秘密图像内容的黑色像素密度仅为未进行加密的秘密图像的 1/16, 构成有效内容的像素排列较稀疏, 因此对不同像素大小的文字图像进行分析, 得到恢复出的秘密图像, 图 10(a)—(f) 的原图像的文字大小分别

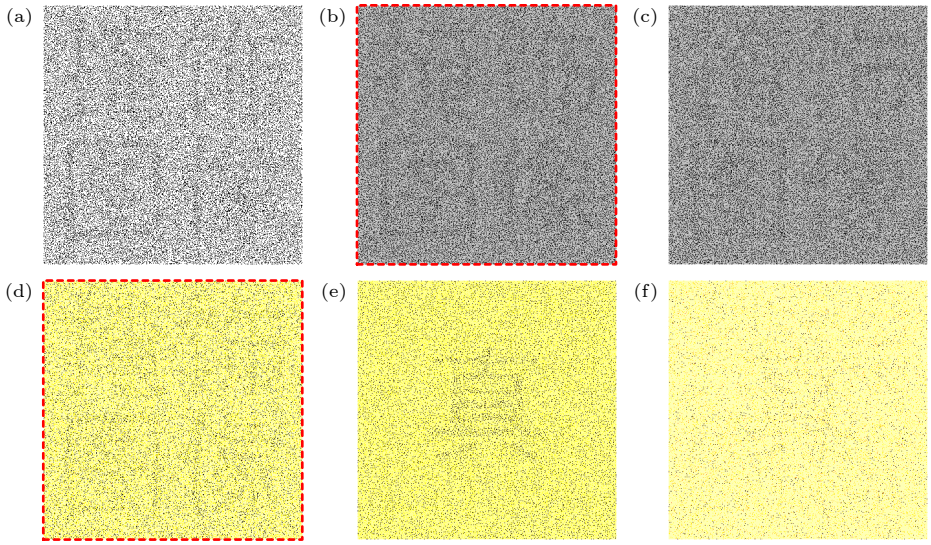

图 7 欺骗追踪过程 (a) 检验密钥; (b) 被篡改像素排列顺序的欺骗图像; (c) 从相位密钥恢复的掩饰图像; (d) 检验密钥与欺骗图像叠加结果; (e) 检验密钥与掩饰图像叠加结果; (f) 无法恢复秘密图像的结果

Fig. 7. Spoofing tracking process: (a) Test key; (b) spoofing images with altered pixel arrangement order; (c) masking image recovered from phase key; (d) test key and spoofing image superposition result; (e) test key and masking image superposition result; (f) failure to recover secret image.

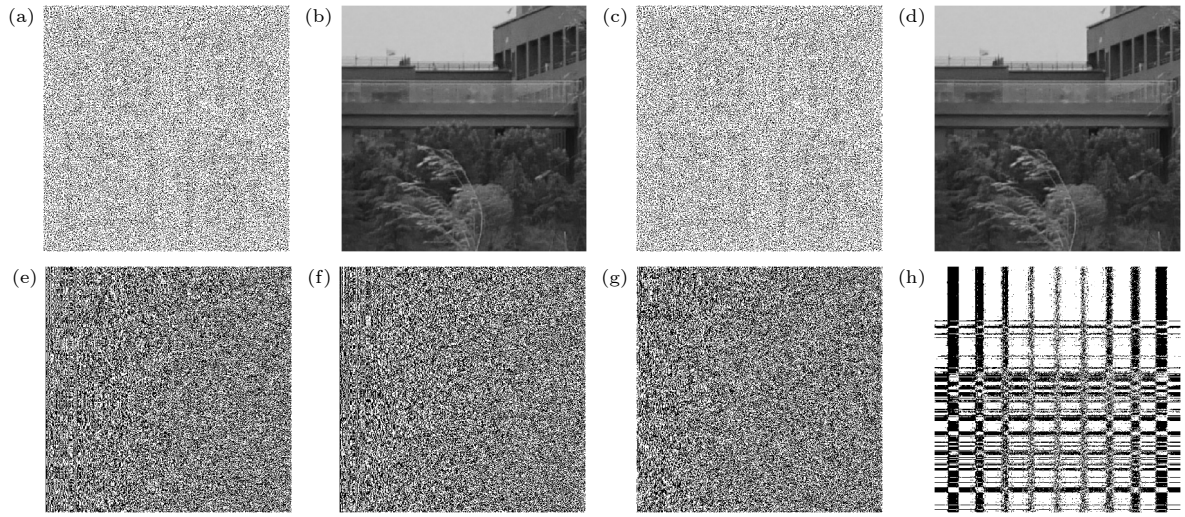

图 8 脆弱水印功能验证 (a) 宿主图像; (b) 水印图像; (c) 嵌入脆弱水印的宿主图像; (d) 提取水印图像; (e) 0.01 椒盐噪声攻击提取的水印; (f) 0.01 高斯噪声攻击提取的水印; (g) 图像压缩后提取的水印; (h) 10×10 像素裁剪攻击后提取的水印

Fig. 8. Fragile watermarking function verification: (a) Host image; (b) watermarked image; (c) host image embedded with fragile watermark; (d) extract watermark image; (e) watermark extracted by 0.01 salt and pepper noise attack; (f) watermark extracted by 0.01 Gaussian noise attack; (g) watermark extracted after image compression; (h) watermark extracted after 10×10 pixel cropping attack.

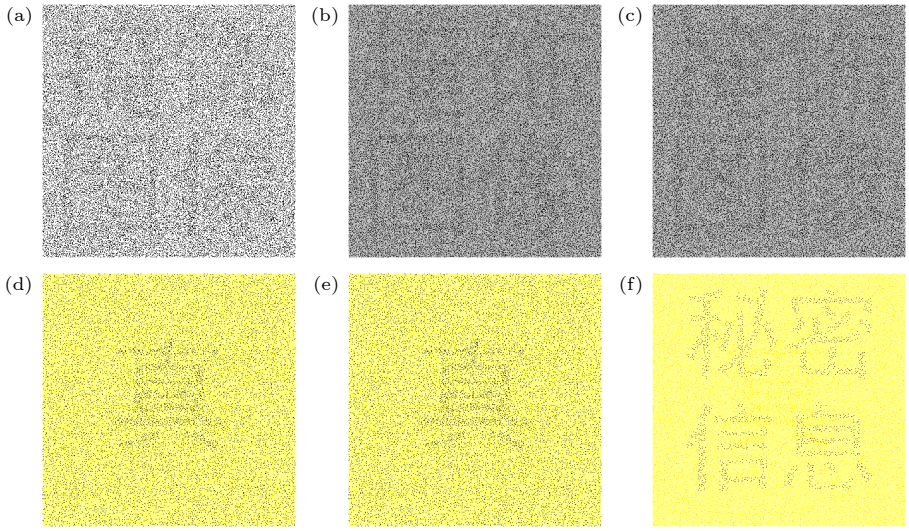

图 9 获得秘密图像的过程 (a) 检验密钥; (b) 从相位密钥恢复出的掩饰图像 1; (c) 从相位密钥恢复出的掩饰图像 2; (d) 检验密钥和掩饰图像 1 叠加得到的验证图像; (e) 检验密钥和掩饰图像 2 叠加得到的验证图像; (f) 3 张图像叠加恢复的秘密图像

Fig. 9. Process of obtaining secret image: (a) Test key; (b) masking image 1 recovered from phase key; (c) masking image 2 recovered from phase key; (d) the verification image obtained by superimposing the test key and the masking image 1; (e) verification images obtained by superimposing the test key and masking image 2; (f) the secret image recovered by superimposing three images.

为 14, 16, 18, 20, 24, 30 像素, 可得出原图像构成一个文字的像素越少, 在衍射出来的秘密图像的可辨识度就会越低, 由于字母的复杂度更高, 在小于 16 像素时字母达到不可辨识的地步, 而这一像素值大小对数字而言则为 14. 为便于呈现相关信息, 采用了伪彩色对图像做了统一增强, 如图 10(a)—(f) 所示.

3.3 鲁棒性分析

考虑到实际应用中, 由于每个掩饰图像的信息要分发给不同的分享者携带, 并且要区分正常的噪声影响和主动的欺骗, 因此要在参与者的掩饰图像上进行模拟噪声处理, 如图 11 所示, 在添加的椒盐噪声密度为 0.1 时, 文字大小为 30 像素的衍射

图 10 (a)—(f) 分别为 14, 16, 18, 20, 24, 30 像素大小的字符图像信息

Fig. 10. (a)–(f) The character images information with the size of 14, 16, 18, 20, 24 and 30 pixels respectively.

后叠加的秘密图像还可保持 0.85 以上的相关系数, 该相关系数其内容也可被识别. 由于其相位密钥的脆弱性, 细微的变化就会无法恢复出原有的验证图像, 因此欺骗者无法在相位中进行欺骗, 否则, 无需进行验证即可发现欺骗者.

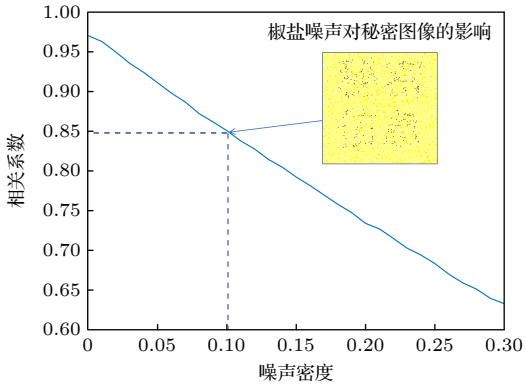

图 11 对掩饰图像进行加噪声处理后秘密图像的相关系数曲线

Fig. 11. Correlation coefficient curves of secret images after noise processing of masking image.

3.4 实用性分析

本论文采用的视觉密码分解方案为 (3, 3) 视觉密码方案, 将一幅秘密图像分解为三张掩饰图像, 将其中一张掩饰图像作为验证图像. 本系统对不可见视觉密码术进行优化, 增加了对内部欺骗者进行快速追踪功能, 在实际进行传输信息时, 可利用本系统来提高内部自检性. 理论上只要分解秘密图像的矩阵设计合理, 就可将秘密图像分解为更多张掩饰图像, 但是其像素扩展将更多, 复杂度会急剧提升, 因此, 在实际应用中可基于本系统, 通过多次分解秘密图像的方式, 来提高掩饰图像的数量, 每次分解就可获得一个检验密钥和两个掩饰图像, 每个检验密钥参与其同时产生的两张掩饰图像的检验与解密.

4 结 论

提出了一种基于光学隐藏视觉密码的欺骗追踪系统. 该系统在传统不可见视觉密码的基础上, 加入了欺骗追踪的功能. 仿真实验结果表明, 该系统可应用于实际信息传递时, 对内部欺骗者的追踪. 同时, 对该系统进行了容量分析和鲁棒性分析, 使利用该系统时可找到合适的像素大小来加密文字信息. 本文继承了不可见视觉密码将分享图样隐藏在相位密钥的隐蔽性, 不仅可以利用有意义的掩饰图像来降低秘密信息被怀疑的可能, 更为重要的是其简单、快捷的欺骗追踪功能使得这种信息加密系统具有追踪内部欺骗者的作用.

参考文献

[1] Khan M, Shah T 2014 *3D Research* **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] 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]
[12] 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]
[13] Machizaud J, Fournel T 2012 *Opt. Express* **20** 22847
[14] Wu H C, Chang C C 2005 *Comput. Stand. Interfaces* **28** 123
[15] Feng J B, Wu H C, Tsai C S, Chang Y F, Chu Y P 2008 *Pattern Recognit.* **41** 3572
[16] Mishra A, Gupta A 2018 *J. Inf. Optim. Sci.* **39** 631
[17] Blundo C, Cimato S, Santis A D 2006 *Theor. Comput. Sci.* **369** 169
[18] Chen Y F, Chan Y K, Huang C C, Tsai M H, Chu Y P 2007 *Inf. Sci.* **177** 4696
[19] 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]
[20] 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]
[21] Shi Y S, Yang X B 2017 *J. Opt.* **19** 115703
[22] Shi Y S, Yang X B 2017 *Chin. Phys. Lett.* **34** 114204
[23] Yang N, Gao Q K, Shi Y S 2018 *Opt. Express* **26** 31995
[24] Li Z F, Dong G Y, Yang D Y, Li G L, Shi Y S, Bi K, Zhou J 2019 *Opt. Express* **27** 19212
[25] Yu B, Fu Z X, Shen G, Fang L G 2014 *Visual Cryptography* (Vol. 1) (Hefei: University of Science and Technology of China Press) p69 (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 69 页]

Optical-hidden-visual-cryptography-based spoofing tracking system*

Wu Cheng-Zhe [1)] Liu Rui-Ze [1)] 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 29 October 2023; revised manuscript received 15 May 2024)

Abstract

A deception tracking system based on optical hidden visual code is proposed. The system uses visual cryptography to decompose the secret image into a number of realistic masked images, which can be used to conceal the secret information. One of the masked images is embedded with a fragile watermark to ensure that it is not modified. This image serves as an inspection key to verify the other images, and the inspection key is transmitted separately. The rest of the camouflaged image is hidden in the phase key using the phase recovery algorithm, which ensures good invisibility during transmission. If the pixel arrangement of the masked image is tampered with by a dishonest participant, it is called a fraudulent image. Each phase key is distributed to different participants to ensure that the corresponding deceiver can be identified when the spoofing image is traced. In the extraction process, only the diffraction transformation of the phase key is needed to obtain the mask image. During the inspection, the inspection key is incoherently superimposed with any masked image, and the appearance of the verification image indicates whether the masked image has been tampered with, thereby achieving the purpose of deception tracking. The secret image can be obtained by incoherently superimposing the masking images, provided that the number of superimposed masking images is is greater than or equal to the threshold k, along with the inspection key. When the inspection key is superimposed with any masked image, if there is a spoofed image, no verification image will appear, and as a result, the secret image will not be restored. If there is no spoofed image, the verification image will appear, indicating that the secret image can be restored by covering all the images. The system can be used to track internal fraudsters when actual information is transmitted through invisible visual cryptography.

Keywords: optical hiding, visual cryptography, phase key, spoofing tracking

PACS: 42.15.Eq, 42.25.Fx, 42.30.–d, 42.30.Rx **DOI:** 10.7498/aps.73.20231721

* 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, and the Fundamental Research Funds for the Central Universities of China.

† Corresponding author. E-mail: shiyishi@ucas.ac.cn

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

基于光学隐藏视觉密码的欺骗追踪系统

吴承哲　刘睿泽　史祎诗

Optical-hidden-visual-cryptography-based spoofing tracking system

Wu Cheng-Zhe　Liu Rui-Ze　Shi Yi-Shi

引用信息 Citation: Acta Physica Sinica, 73, 144201 (2024)　DOI: 10.7498/aps.73.20231721
在线阅读 View online: https://doi.org/10.7498/aps.73.20231721
当期内容 View table of contents: http://wulixb.iphy.ac.cn
