基于二维码和可逆可视水印的图像隐私保护方案

姚远志，王锋，严文博，俞能海
（中国科学技术大学信息科学技术学院，安徽 合肥 230027）

摘 要：针对图像在网络传输中的隐私信息泄露问题，提出了一种基于二维码和可逆可视水印的图像隐私保护方案。为了保护图像拍摄时间、拍摄地点和详细描述等隐私信息，首先将这类隐私信息加密后存储在云平台，并生成能够链接到加密隐私信息的统一资源定位符。该方案将统一资源定位符编码成二维码，并将该二维码作为可视水印可逆地嵌入图像中，实现对隐私信息的访问权限控制。在该方案中，使用视觉感知模型选择适合的水印嵌入参数，以平衡水印的可视性和载密图像的视觉质量。实验结果表明，该方案能够保证载密图像具有良好的视觉质量，同时不影响二维码的正确识别和解码。使用所提方案在保障图像传输质量的同时，也降低了隐私泄露的风险。

关键词：二维码；可逆信息隐藏；可视水印；隐私保护
中图分类号：TP309.2
文献标识码：A
doi: 10.11959/j.issn.1000–436x.2019220

Image privacy preservation scheme based on QR code and reversible visible watermarking

YAO Yuanzhi, WANG Feng, YAN Wenbo, YU Nenghai
School of Information Science and Technology, University of Science and Technology of China, Hefei 230027, China

Abstract: With the privacy leakage problem of image delivery in networks, an image privacy preservation scheme based on QR code and reversible visible watermarking was proposed. In order to preserve the privacy information including shooting time, shooting location and detailed description, the encrypted privacy information was stored in cloud platforms and corresponding universal resource locator was generated firstly. Secondly, the universal resource locator was encoded as the QR code and it was embedded into the cover image using reversible visible watermarking. Therefore, the access control for privacy information could be achieved. The visual perceptual model was utilized to select adaptive watermark embedding parameters to balance watermark visibility and marked image quality. Experimental results demonstrate that the good visual quality of marked images can be obtained and the embedded QR code can be correctly decoded. The proposed scheme can guarantee marked image quality and reduce the risk of private information leakage.

Key words: QR code, reversible data hiding, visible watermarking, privacy preservation

1 引言

移动互联网技术的快速发展和移动智能终端的普遍应用极大地改善了人们的生活品质。用户在享受高效便捷的生活方式的同时，也潜在地承担着日趋严峻的个人隐私信息泄露风险[1]。据调查显示，截至 2018 年 12 月，我国手机上网用户规模达 8.17 亿人，用户使用手机上网的比例达 98.6%[2]。其中，个人隐私信息泄露已成为主要的互联网安全事件。发生该类事件的主要原因在于大多数移动智能终

收稿日期：2019–07–08；**修回日期**：2019–09–05
基金项目：国家自然科学基金资助项目（No.61802357）；国家重点研发计划基金资助项目（No.2018YFB0804102）
Foundation Items: The National Natural Science Foundation of China (No.61802357), The National Key Research and Development Program of China (No.2018YFB0804102)

端和移动通信应用程序提供基于位置服务（LBS, location-based service）的功能。用户在使用位置服务的同时，其位置信息会被无感知地发送给服务提供商作为提供服务所需的必要数据[3]。然而，一旦提供给服务商的这些隐私信息被恶意用户获取，通过大数据分析技术就可以挖掘出更深层次的用户画像信息（如兴趣爱好、工作地点和生活习惯等），使个人信息安全受到严重的威胁。因此，保护移动互联网中的用户隐私信息已成为重要的研究课题。

得益于移动智能终端日益完善的拍摄功能和移动互联网的广泛普及，采集数字图像并在网络中发布的成本变得更加低廉。用户在社交网站和移动通信应用程序中发布和分享图像可以获得良好的用户体验。但是，伴随这类通信行为，用户的个人隐私信息也会面临泄露的风险[4]。在移动通信应用程序发布图像时，很多用户会选择上传原图以获得视觉质量更好的体验效果。上传的原始图像通常带有拍摄时间、拍摄地点和详细描述等隐私信息，具有强大计算能力的服务提供商可以使用大数据分析技术对用户进行画像。根据以上分析，使用社交网络和移动通信应用程序发布图像的通信行为伴随着隐私信息泄露问题。

针对上述隐私信息泄露问题，本文提出了一种基于二维码和可逆可视水印的图像隐私保护方案。为了保护图像拍摄时间、拍摄地点和详细描述等隐私信息，首先对原始图像进行去隐私信息处理，并将这类隐私信息加密后存储在云平台，同时生成能够链接到加密隐私信息的统一资源定位符。由于二维码存储信息具有较强的稳健性[5]，该方案将统一资源定位符编码成二维码，并将该二维码作为可视水印可逆地嵌入图像中。只有授权的用户才可以根据统一资源定位符得到隐私信息，并获得原始图像，实现对隐私信息的访问权限控制。在该方案中，使用视觉感知模型选择适合的水印嵌入参数，以平衡水印的可视性和载密图像的视觉质量。实验结果验证了该方案在载密图像视觉质量、水印可视性和可逆性等方面的优势。所提方案具有保障图像传输质量和降低隐私泄露风险的能力。本文的主要贡献如下。

1) 提出了一种基于二维码和可逆可视水印的图像隐私保护方案，该方案重点考虑用户使用移动通信应用程序发布图像时的隐私泄露问题。

2) 提炼并解决水印的可视性和载密图像的视觉质量之间的均衡分析问题，作为所提图像隐私保护方案中的关键问题。

3) 对所提图像隐私保护方案的安全性进行分析，证明对图像隐私保护的有效性。

2 相关工作

本文提出的基于二维码和可逆可视水印的图像隐私保护方案重点是将二维码作为可视水印嵌入需要保护的图像中。在获得访问权限的情况下，扫描嵌入的二维码即可得到与图像关联的隐私信息。因此，二维码的正确识别和解码是授权用户得到隐私信息的前提条件。另外，载密图像的视觉质量决定一般用户的体验效果。增强二维码的嵌入强度，可以增强水印的可视性，从而提高二维码正确识别和解码的能力，但是会降低载密图像的视觉质量。平衡水印的可视性和载密图像的视觉质量，是图像隐私保护方案需要解决的关键问题。

一般而言，可视水印嵌入会降低载密图像的视觉质量。可视水印的基本要求是嵌入的水印不能明显掩盖水印嵌入区域的图像内容[6]。可逆信息隐藏是一种将数据嵌入数字媒体（如音频、图像和视频等）并且可以在提取数据之后无损恢复原始数字媒体的技术[7]。结合可视水印和可逆信息隐藏，可以实现可逆可视水印。目前，已经有很多经典的针对图像可逆可视水印的算法[8-15]被提出。Hu 等[8]通过像素比特平面替换的方法嵌入可视水印，为了保证可逆性，水印嵌入区域的图像像素需要压缩并作为边信息嵌入载体图像。Yip 等[9]分别利用像素值匹配和像素位置平移提出了 2 种图像可逆可视水印算法。Tsai 等[10]和 Liu 等[11]使用一对一像素值匹配设计了图像可逆可视水印算法。Yang 等[12]提出自适应调节像素值来嵌入可视水印，并在载体图像中嵌入重构数据分组用于图像恢复。在 Mohammad 等[13]提出的算法中，通过像素值循环移位在块截断编码（BTC, block truncation coding）图像中嵌入可逆可视水印。Lin 等[14]提出了一种离散余弦变换（DCT, discrete cosine transform）域的图像可逆可视水印算法。但是该算法只有在获得原始水印图像的情况下才可以无损恢复原始载体图像。Yao 等[15]提出了一种加密图像的可逆可视水印算法，为了平衡水印可视性和载密图像视觉质量，该算法在图像加密之前通过视觉感知模型选择适合的水印嵌入位置。由于信号在加密域的弱相关性，使用传统的可逆信息隐藏算法在图像加密之前预留水印嵌入空间。因此，数

据嵌入者可以基于水印嵌入位置的像素比特位替换，方便地在加密图像中嵌入可视水印。

上述的图像可逆可视水印算法[8-15]嵌入的水印通常是二值图像，通过人类视觉系统高超的感知能力可以识别嵌入的水印，具有可视性。但是，这些算法不能满足二维码作为可视水印时的嵌入要求。在二维码作为可视水印的情况下，如果水印可视性不强，可能导致二维码无法正确识别和解码。在本文提出的图像隐私保护方案中，无法正确识别和解码二维码会导致授权用户不能得到图像隐私信息。Huang 等[16]针对二维码提出了图像可逆可视水印算法，该算法使用差值扩展技术嵌入二维码，可以保证足够的水印可视性，但是嵌入的二维码几乎完全掩盖了水印嵌入区域的图像内容，得到的载密图像视觉质量不高。综合以上分析，水印的可视性和载密图像的视觉质量之间的均衡分析问题是亟待解决的关键问题。

3　图像隐私保护方案

3.1　图像隐私保护方案框架

本文提出的基于二维码和可逆可视水印的图像隐私保护方案主要由图像发送方、云平台和图像接收方组成，其框架如图 1 所示。图像发送方一般是原始图像的采集者，首先对原始图像进行去隐私信息处理，并将去隐私信息的图像和加密后的隐私信息发送给云平台。云平台负责管理加密隐私信息，并根据加密隐私信息生成的统一资源定位符对去隐私信息的图像进行可逆可视水印嵌入。授权的图像接收方可以提取载密图像中嵌入的二维码，并根据二维码从云平台中得到加密隐私信息，最终获得融合隐私信息的原始图像。非授权的用户即使获得嵌入二维码的载密图像，也无法得到与图像关联的隐私信息。

图像发送方的工作流程为：对原始图像进行隐私信息提取，生成去隐私信息的图像和隐私信息（包括拍摄时间、拍摄地点和详细描述等，详细描述可以是原始图像采集者对图像的标注信息）；使用加密密钥对隐私信息进行加密；将去隐私信息的图像和加密隐私信息发送给云平台。

云平台的工作流程为：在存储服务器中管理接收到的加密隐私信息；生成能够链接到加密隐私信息的统一资源定位符；将统一资源定位符编码成二维码，并根据水印密钥将该二维码作为可视水印可逆地嵌入去隐私信息的图像中。

图像接收方的工作流程为：根据水印密钥提取载密图像中的二维码；根据解码二维码得到统一资源定位符，从存储服务器中查询加密隐私信息；使用加密密钥得到解密后的隐私信息，并进行隐私信息融合从而获得原始图像。

在上述的图像隐私保护方案中，根据加密密钥和水印密钥的拥有情况，可以分为 3 种隐私保护等级。同时拥有加密密钥和水印密钥的用户可以获得隐私信息和原始图像。仅拥有加密密钥的用户可以扫描载密图像中嵌入的二维码读取统一资源定位符，得到隐私信息。既没有加密密钥也没有水印密钥的用户，即使获得嵌入二维码的载密图像，也无法得到与图像关联的隐私信息。并且，嵌入的二维码无法从载密图像中提取。使用该图像隐私保护方案，可以在保障图像传输质量的同时降低隐私泄露的风险。

3.2　针对二维码的图像可逆可视水印算法

在本文提出的基于二维码和可逆可视水印的

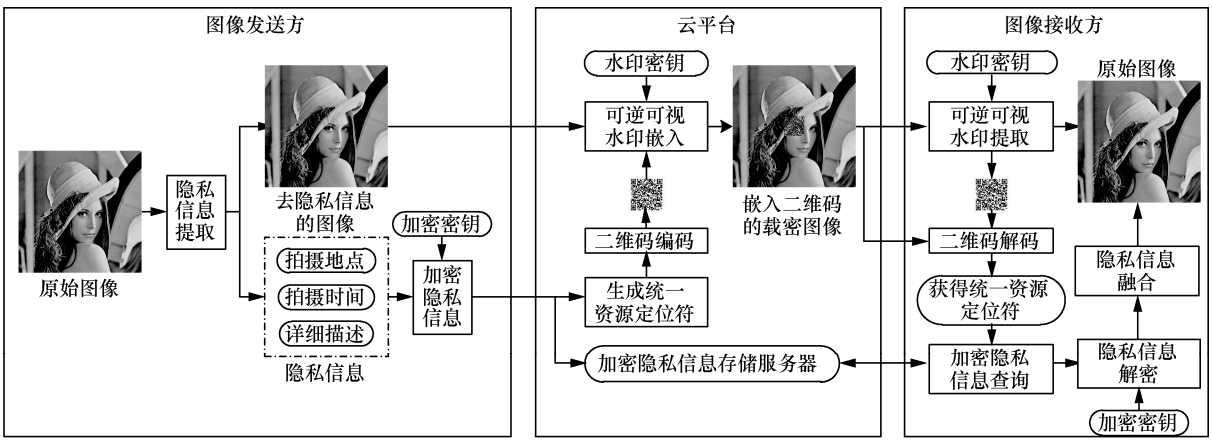


图 1　图像隐私保护方案框架

图像隐私保护方案中，嵌入的二维码的正确识别和解码是授权用户得到隐私信息的前提条件。同时，一般用户的体验效果受到载密图像视觉质量的影响。平衡水印的可视性和载密图像的视觉质量是本文提出方案解决的关键问题。

不失一般性，令 x 和 w 分别为 8 bit 的灰度载体图像像素和二值水印图像像素，则可视水印嵌入模型[17]可以表示为

$$y^{(x,w)}(\alpha)=(1-\alpha)x+\alpha w \tag{1}$$

其中，$y^{(x,w)}(\alpha)$ 是嵌入可视水印的载密图像像素，$\alpha\in[0,1]$ 是控制水印嵌入强度的嵌入参数。平衡水印的可视性和载密图像的视觉质量的本质是选择适合的嵌入参数 α，使嵌入二维码的载密图像在保证二维码能够被正确识别和解码的同时，还拥有较好的图像视觉质量。根据式(1)，可以得到在载密图像像素中的水印嵌入强度，如式(2)所示。

$$\alpha=\frac{y^{(x,w)}(\alpha)-x}{w-x} \tag{2}$$

在式(1)中，载密图像像素 $y^{(x,w)}(\alpha)$ 表示为载体图像像素 x 和二值水印图像像素 w 的线性组合。由于载体图像像素 x 的取值范围是 $[0,255]$，二值水印图像像素 w 的取值范围是 $\{0,255\}$，可以推断载密图像像素 $y^{(x,w)}(\alpha)$ 的取值范围是 $[0,255]$。水印嵌入强度 α 在很大程度上影响水印的可视性，本文使用视觉感知模型评估水印的可视性。

视觉感知模型在很多实际应用场景发挥了重要作用，如数字水印[12]、图像质量评价[18]和图像/视频编码[19]等。人类视觉系统通常只能感知大于一定阈值的图像内容变化[20-22]。这个阈值被称为最小可察觉差值（JND, just noticeable difference）。根据 Wu 等[22]提出的 JND 模型，载体图像像素 x 的 JND 阈值 $T_{\mathrm{JND}}(x)$ 可以表示为

$$\begin{aligned}T_{\mathrm{JND}}(x)&=L_A(x)+M_S(x)-\\&\gamma\min\{L_A(x),M_S(x)\}\end{aligned} \tag{3}$$

其中，γ 是 JND 模型的参数；$L_A(x)$ 是亮度自适应可视性阈值；$M_S(x)$ 是空域掩模函数，该函数由类型掩模函数 $M_P(x)$ 和对比度掩模函数 $M_C(x)$ 共同决定，如式(4)所示。

$$M_S(x)=\max\{M_P(x),M_C(x)\} \tag{4}$$

在嵌入二值水印图像像素 w 时，载体图像像素 x 会发生变化。根据式(3)所示的 JND 模型，这个变化在一定范围内时，人类视觉系统无法感知。因此，载体图像像素 x 的不可视范围的上界和下界分别如式(5)和式(6)所示。

$$x_{\mathrm{upper}}=x+T_{\mathrm{JND}}(x) \tag{5}$$

$$x_{\mathrm{lower}}=x-T_{\mathrm{JND}}(x) \tag{6}$$

因此，由式(5)和式(6)决定的与载体图像像素 x 对应的不可视范围 $R(x)$ 可以表示为

$$R(x)=[x_{\mathrm{lower}},x_{\mathrm{upper}}] \tag{7}$$

根据式(2)和式(7)，可以讨论如图 2 所示的水印嵌入强度和水印可视性的关系。

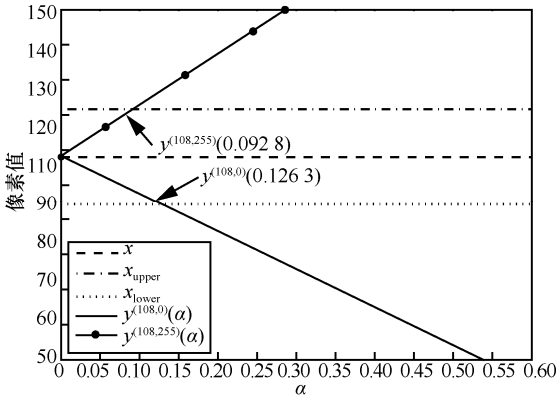


图 2 水印嵌入强度和水印可视性的关系

以标准测试图像 Lena 中位置为(478, 66)且像素值为 108 的 x 为例，该像素的 JND 阈值为 13.638 7。当嵌入的二值水印图像像素值为 255 时，在图 2 中定位载密图像像素值 $y^{(108,255)}(\alpha)$ 与不可视范围的上界的交点，即可得到使水印可视的最小水印嵌入强度 $\alpha_{\min}=0.092\,8$。同理，当嵌入的二值水印图像像素值为 0 时，在图 2 中定位载密图像像素值 $y^{(108,0)}(\alpha)$ 与不可视范围的下界的交点，即可得到使水印可视的最小水印嵌入强度 $\alpha_{\min}=0.126\,3$。由图 2 的分析可知，对于给定的载体图像像素和二值水印图像像素，在式(1)所示的可视水印嵌入模型下，存在最小的水印嵌入强度 $\alpha_{\min}$，使嵌入的水印可视。因此，水印可视范围可以表示为

$$\alpha\in[\alpha_{\min},1] \tag{8}$$

在建立了水印嵌入强度和水印可视性的关系之后，即可讨论针对二维码的图像可逆可视水印算法。在针对二维码的图像可逆可视水印算法中，需要根据二维码的结构和载体图像的 JND 阈值选择适合的水印嵌入强度。

如图 3 所示，二维码可以分为空白区域 I_{B}、位置探测区域 I_{D} 和其他区域 I_{R}。需要根据各个区域的特征和作用，选择不同的水印嵌入强度。令 $x_{i,j}$ 是第 (i,j) 个载体图像像素，$w_{i,j}$ 是第 (i,j) 个二值水印图像像素，$y_{i,j}$ 是第 (i,j) 个载密图像像素，$\alpha_{i,j}$ 是第 (i,j) 个载体图像像素 $x_{i,j}$ 的水印嵌入强度。对于二维码中的空白区域 I_{B}，可以直接令水印的嵌入强度 $\alpha_{i,j}$ 为 0，即 $\alpha_{i,j}=0$。此时，载密图像像素 $y_{i,j}$ 可以表示为

$$y_{i,j}=x_{i,j} \tag{9}$$

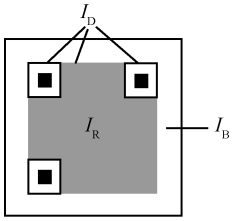


图 3　二维码分区示意

对于位置探测区域和其他区域，可以将可视水印嵌入建模为水印嵌入强度在水印可视范围内的最小化嵌入失真问题。基于式(1)所示的可视水印嵌入模型，载密图像像素 $y_{i,j}$ 的嵌入失真可以表示为

$$\rho_{i,j}(x_{i,j},y_{i,j})=(y_{i,j}-x_{i,j})^2=\alpha_{i,j}^2(w_{i,j}-x_{i,j})^2 \tag{10}$$

因此，水印嵌入强度在水印可视范围内的最小化嵌入失真问题可以表示为

$$\begin{aligned}&\min\ \rho_{i,j}(x_{i,j},y_{i,j})\\&\text{s.t.}\left|y_{i,j}-x_{i,j}\right|\geqslant T_{\mathrm{JND}}(x_{i,j})\\&y_{i,j}=(1-\alpha_{i,j})x_{i,j}+\alpha_{i,j}w_{i,j}\end{aligned} \tag{11}$$

由于二维码中的位置探测区域 I_{D} 对于定位二维码起到了至关重要的作用，使用式(11)进行最小化水印嵌入失真时，需要考虑的二值水印图像像素值范围为 $w_{i,j}\in\{0,255\}$。二维码中的其他区域 I_{R} 中包含二维码编码信息和纠错信息，使用式(11)进行最小化水印嵌入失真时，仅需考虑二值水印图像像素为黑色的情况，即 $w_{i,j}=0$。这是因为二维码中的其他区域 I_{R} 中的白色像素不用于承载二维码编码信息和纠错信息。

为了在提取嵌入的二维码之后可以无损恢复载体图像，需要将水印嵌入区域的载密图像和载体图像的像素差值构成重构数据分组 P，可以表示为

$$P=\left\{\delta_{i,j}\mid\delta_{i,j}=y_{i,j}-x_{i,j}\right\} \tag{12}$$

为了减小表达重构数据分组所需的比特数，在嵌入重构数据分组之前使用 JBIG（joint bi-level image expert group）压缩算法对重构数据分组进行压缩，以提高载密图像的视觉质量。令 $m_k\in\{0,1\}$ 为压缩后的重构数据分组中的比特，则长度为 L 的压缩后的重构数据分组可以表示为 $m=\{m_1,\cdots,m_L\}$。可以使用可逆信息隐藏算法将压缩后的重构数据分组嵌入水印嵌入区域以外的载密图像中，本文使用 Sachnev 等[23]提出的可逆信息隐藏算法进行压缩后的重构数据分组嵌入。首先，将水印嵌入区域以外的图像像素分为 2 类。其中第一类像素 $u_{i,j}$ 的位置满足 $\mathrm{mod}((i+j),2)=0$，第二类像素 $v_{i,j}$ 的位置满足 $\mathrm{mod}((i+j),2)=1$。数据可逆嵌入由 2 轮构成。在第一轮数据可逆嵌入中，使用第二类像素 $v_{i,j}$ 预测第一类像素 $u_{i,j}$，使用第一类像素 $u_{i,j}$ 嵌入数据。在第二轮数据可逆嵌入中，使用第一类像素 $u_{i,j}$ 预测第二类像素 $v_{i,j}$，使用第二类像素 $v_{i,j}$ 嵌入数据。以第一轮数据可逆嵌入为例，第一类像素 $u_{i,j}$ 的预测值 $u'_{i,j}$ 由其相邻的 4 个第二类像素预测得到，如式(13)所示。

$$u'_{i,j}=\left\lfloor\frac{v_{i,j-1}+v_{i+1,j}+v_{i,j+1}+v_{i-1,j}}{4}\right\rfloor \tag{13}$$

通过从原始像素 $u_{i,j}$ 中减去预测值 $u'_{i,j}$，可以得到预测误差 $d_{i,j}$，如式(14)所示。

$$d_{i,j}=u_{i,j}-u'_{i,j} \tag{14}$$

得到预测误差之后，使用预测误差扩展和直方图平移将压缩后的重构数据分组中的比特 m_k 嵌入预测误差 $d_{i,j}$ 中，如式(15)所示。

$$D_{i,j}=\begin{cases}2d_{i,j}+m_k, & d_{i,j}\in[T_n,T_p]\\ d_{i,j}+T_p+1, & d_{i,j}>T_p\geqslant 0\\ d_{i,j}+T_n, & d_{i,j}<T_n<0\end{cases} \tag{15}$$

其中，T_p 和 T_n 分别是控制预测误差扩展的正阈值和负阈值。在数据可逆嵌入之后，原始像素 $u_{i,j}$ 被修改为 $U_{i,j}$，如式(16)所示。

$$U_{i,j}=D_{i,j}+u'_{i,j} \tag{16}$$

在第二类像素中的数据可逆嵌入和在第一类像素中的数据可逆嵌入相似。数据可逆嵌入和提取

的细节描述可以参考文献[23]。为了防止水印恶意擦除，需要根据水印密钥使用流密码对压缩后的重构数据分组进行加密。图 4 描述了本文提出的针对二维码的图像可逆可视水印算法的原理。

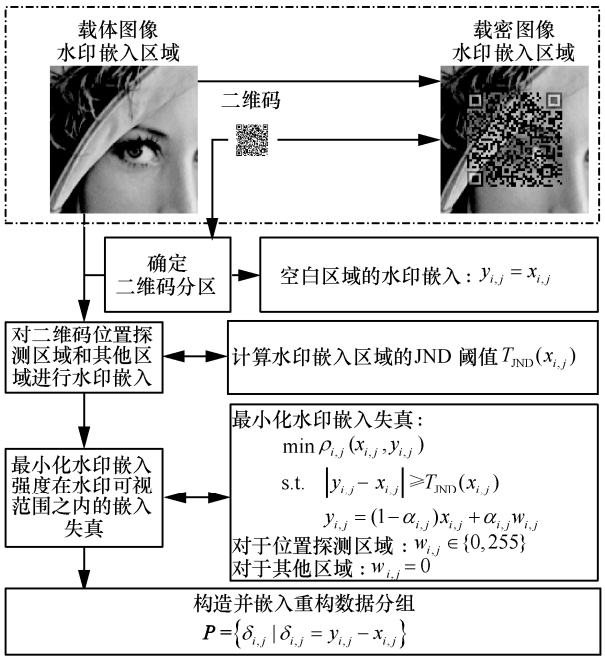


图 4 针对二维码的图像可逆可视水印算法的原理

4 实验设计与结果分析

4.1 实验设置

为了验证本文提出的基于二维码和可逆可视水印的图像隐私保护方案的有效性，在实验部分重点对针对二维码的图像可逆可视水印算法进行性能测试，并对所提图像隐私保护方案的安全性进行分析。

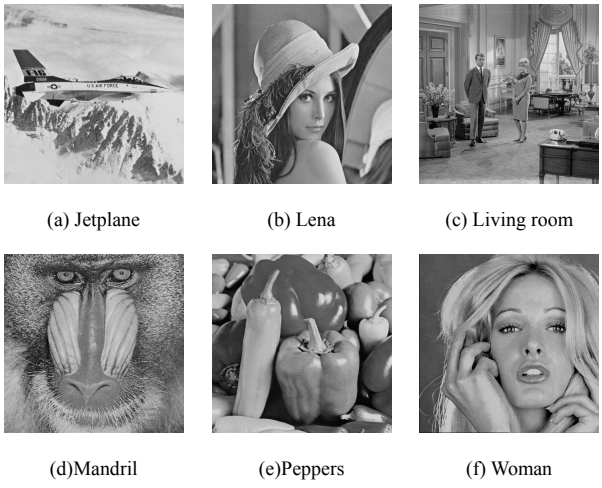
将针对二维码的图像可逆可视水印算法在 Matlab R2016a 中实现，并选取 Huang 等[16]提出的图像可逆可视水印算法（以下简称 Huang 等算法）、Mohammad 等[13]提出的图像可逆可视水印算法（以下简称 Mohammad 等算法）和 Yao 等[15]提出的图像可逆可视水印算法（以下简称 Yao 等算法）作为对比方案。这里使用二维码开源开发库 ZXing.Net 实现二维码的编码和解码。为了便于验证二维码能否正确识别和解码，实验中作为可视水印的二维码的编码信息为“University of Science and Technology of China”，尺寸分别为 128 像素×128 像素和 256 像素×256 像素，如图 5 所示。选取标准测试图像库中的 6 幅图像作为载体图像，如图 6 所示。实验中使用峰值信噪比（PSNR, peak signal-to-noise ratio）（单位为 dB）和结构化相似度（SSIM, structural similarity）[24]评价载密图像相对于载体图像的视觉质量。

4.2 参数选择

在本文提出的针对二维码的图像可逆可视水印算法中，控制水印嵌入强度的嵌入参数 $\alpha_{i,j}$ 是平衡水印的可视性和载密图像的视觉质量的重要参数。本文在讨论可视水印嵌入模型以及水印嵌入强度和水印可视性的关系的基础上，建立了如式(11)所示的水印嵌入强度在水印可视范围内的最小化嵌入失真模型。使用该模型进行可视水印嵌入时，可以适配载体图像和二值水印图像的内容选择相应的嵌入参数 $\alpha_{i,j}$，以平衡水印的可视性和载密图像的视觉质量。

(a) 尺寸为 128 像素×128 像素的二维码　(b) 尺寸为 256 像素×256 像素的二维码

图 5 作为可视水印的二维码



(a) Jetplane　(b) Lena　(c) Living room

(d)Mandril　(e)Peppers　(f) Woman

图 6 实验中使用的载体图像

以标准测试图像 Lena 中位置为(478, 66)且像素值为 108 的像素为例，讨论嵌入参数 $\alpha_{i,j}$ 对载密图像像素嵌入失真 $\rho_{i,j}(x_{i,j},y_{i,j})$ 的影响，如表 1 所示。随着嵌入参数 $\alpha_{i,j}$ 的增加，载密图像像素的失真增大，同时水印的嵌入强度增大。

选取载体图像为 Lena 且嵌入的二维码的尺寸为 128 像素×128 像素，讨论嵌入参数的选择方法，具体步骤如下。

表 1　　**不同嵌入参数时载密图像像素的嵌入失真**

图像像素	嵌入参数 $\alpha_{i,j}$										
	0.0	0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8	0.9	1.0
水印像素 $w_{i,j}=255$	0	216	864	1 945	3 457	5 402	7 779	10 588	13 830	17 503	21 609
水印像素 $w_{i,j}=0$	0	117	467	1 050	1 866	2 916	4 199	5 715	7 465	9 448	11 664

步骤 1　依次遍历得到载体图像中水印嵌入区域的像素 $x_{i,j}$。

步骤 2　根据二值水印图像像素 $w_{i,j}$，使用式(11)对载体图像像素 $x_{i,j}$ 进行水印嵌入。

步骤 3　得到与载密图像像素 $y_{i,j}$ 对应的嵌入参数 $\alpha_{i,j}$。

通过步骤 1~步骤 3，可以得到如图 7 所示的控制水印嵌入强度的嵌入参数 $\alpha_{i,j}$ 的统计直方图。使用载体图像 Jetplane、Living room、Mandril、Peppers 和 Woman 进行水印嵌入，使用的嵌入参数同样可以根据式(11)计算得到。

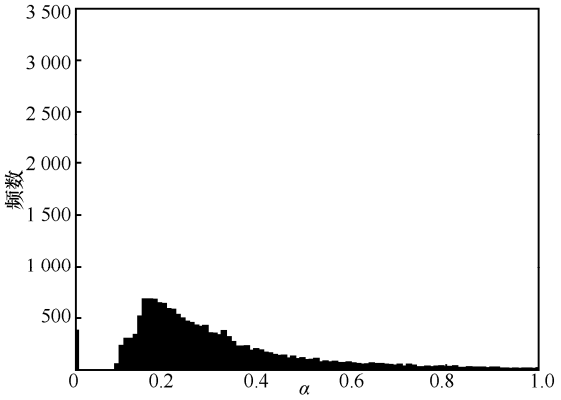
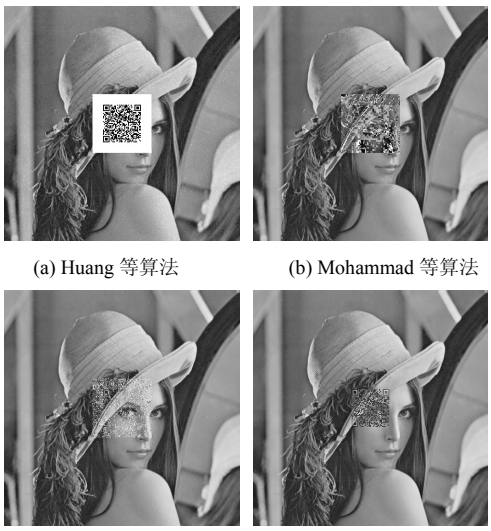


图 7　控制水印嵌入强度的嵌入参数的统计直方图

4.3　载密图像视觉质量

为了测试水印的可视性，分别使用 Huang 等算法、Mohammad 等算法、Yao 等算法和本文提出的针对二维码的图像可逆可视水印算法进行水印嵌入。图 8 描述了对载体图像 Lena 使用不同可逆可视水印算法生成的载密图像，其中水印嵌入区域为载体图像的中心，嵌入的二维码的尺寸为 128 像素×128 像素。图 9 描述了对载体图像 Peppers 使用不同可逆可视水印算法生成的载密图像，其中水印嵌入区域为载体图像的中心，嵌入的二维码的尺寸为 256 像素×256 像素。

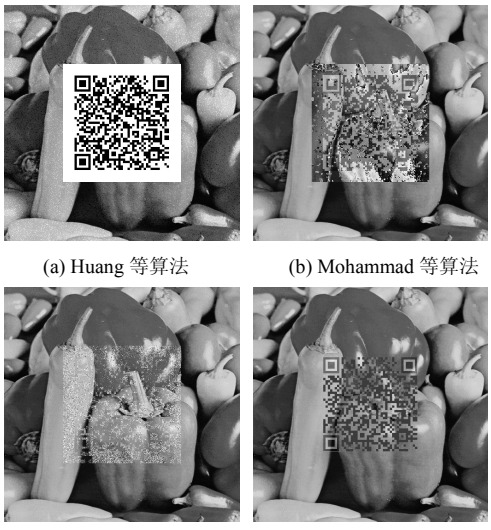
由图 8 和图 9 可知，使用 Mohammad 等算法和 Yao 等算法在载体图像中嵌入二维码后，无法识别嵌入的二维码。在使用 Huang 等算法生成的载密图像中，嵌入的二维码虽然可以被正确识别，但是嵌入的二维码完全掩盖了水印嵌入区域的图像内容。本文提出的算法致力于解决水印的可视性和载密图像的视觉质量之间的均衡分析问题，嵌入的二维码既可以被正确识别，也不会完全掩盖水印嵌入区域的图像内容，可以较好地兼顾水印的可视性和载密图像的视觉质量，为授权用户得到隐私信息提供必要的前提条件。



(a) Huang 等算法　　(b) Mohammad 等算法

(c) Yao 等算法　　(d) 本文提出的算法

图 8　对载体图像 Lena 使用可逆可视水印算法生成的载密图像



(a) Huang 等算法　　(b) Mohammad 等算法

(c) Yao 等算法　　(d) 本文提出的算法

图 9　对载体图像 Peppers 使用可逆可视水印算法生成的载密图像

为了客观评价载密图像的视觉质量，分别使用 Huang 等算法、Mohammad 等算法、Yao 等算法和本文提出的针对二维码的图像可逆可视水印算法进行水印嵌入。表 2 描述了嵌入的二维码的尺寸为 128 像素×128 像素时使用不同可逆可视水印算法生成载密图像的客观质量。表 3 描述了嵌入的二维码的尺寸为 256 像素×256 像素时使用不同可逆可视水印算法生成载密图像的客观质量。在使用本文提出的算法进行水印嵌入时，需要根据式(11)对图像水印嵌入区域中每个像素选择适合的嵌入参数。表 4 描述了嵌入的二维码的尺寸为 128 像素×128 像素时本文提出的算法中嵌入参数的均值和标准差。表 5 描述了嵌入的二维码的尺寸为 256 像素×256 像素时本文提出的算法中嵌入参数的均值和标准差。

表 2 和表 3 中的粗体数字表示相应的图像可逆可视水印算法可以取得最好的载密图像客观质量。从表 2 和表 3 可以看出，本文提出的针对二维码的图像可逆可视水印算法在大多数情况下可以取得最好的载密图像视觉质量。然而，有些情况下本文提出的算法在载密图像客观质量上不如 Yao 等算法。这是由于，实验中选用的载体图像为自然图像，自然图像具有较强的空间相关性。Yao 等算法在嵌入水印前先对载体图像分块，为每个图像块中的像素选择相同的嵌入参数，有利于保护图像的空间相关性。但是，本文提出的算法对图像水印嵌入区域中每个像素选择适合的嵌入参数，对图像的空间相关性造成一定程度的影响。与表 2 相比，表 3 中嵌入的二维码的尺寸为 256 像素×256 像素，水印嵌入区域更大，因此使用本文提出的算法对图像空间相关性的影响会更大。在本文提出的图像隐私保护方案中，二维码的正确识别和解码是授权用户得到隐私信息的前提条件。为了使嵌入的二维码可以被正确识别，本文提出的针对二维码的图像可逆可视水印算法需要对水印嵌入区域中每个像素选择适合的嵌入参数。

表 2　嵌入的二维码的尺寸为 128 像素×128 像素时使用不同可逆可视水印算法生成载密图像的客观质量

载体图像	Huang 等算法		Mohammad 等算法		Yao 等算法		本文提出的算法	
	PSNR	SSIM	PSNR	SSIM	PSNR	SSIM	PSNR	SSIM
Jetplane	18.445	0.793 1	23.201	0.943 6	**27.401**	0.954 3	26.750	**0.976 5**
Lena	17.146	0.755 0	22.493	0.941 2	25.746	0.944 7	**27.903**	**0.974 5**
Living room	17.482	0.795 7	21.500	0.935 2	25.892	0.945 6	**29.692**	**0.975 1**
Mandril	18.939	0.867 5	21.827	0.934 0	28.159	0.945 1	**29.008**	**0.973 7**
Peppers	17.325	0.746 2	21.810	0.940 3	26.791	0.944 3	**28.755**	**0.973 7**
Woman	17.400	0.800 8	21.471	0.935 4	26.069	0.938 1	**28.269**	**0.972 5**
均值	17.790	0.793 1	22.050	0.938 3	26.676	0.945 4	**28.396**	**0.974 3**
标准差	0.725	0.043 0	0.673	0.003 9	0.958	0.005 2	1.015	0.001 4

表 3　嵌入的二维码的尺寸为 256 像素×256 像素时使用不同可逆可视水印算法生成载密图像的客观质量

载体图像	Huang 等算法		Mohammad 等算法		Yao 等算法		本文提出的算法	
	PSNR	SSIM	PSNR	SSIM	PSNR	SSIM	PSNR	SSIM
Jetplane	11.736	0.554 3	17.990	0.786 8	**21.734**	0.818 8	18.102	**0.857 6**
Lena	11.062	0.435 1	17.099	0.773 9	20.132	0.795 1	**20.456**	**0.853 9**
Living room	11.460	0.560 5	16.787	0.774 6	20.770	0.808 4	**21.069**	**0.858 8**
Mandril	11.644	0.647 1	16.591	0.753 5	**21.486**	0.804 8	19.389	**0.851 8**
Peppers	11.657	0.471 1	16.411	0.774 3	**21.510**	0.783 5	21.034	**0.853 9**
Woman	12.103	0.539 9	16.711	0.766 9	**21.597**	0.783 8	20.686	**0.854 6**
均值	11.610	0.534 7	16.932	0.771 7	**21.205**	0.799 1	20.123	**0.855 1**
标准差	0.342	0.074 4	0.567	0.011 0	0.624	0.014 1	1.164	0.002 6

表 4　嵌入的二维码的尺寸为 128 像素×128 像素时本文提出的算法中嵌入参数的均值和标准差

载体图像	均值	标准差
Jetplane	0.313	0.244
Lena	0.243	0.195
Living room	0.211	0.185
Mandril	0.304	0.254
Peppers	0.25	0.218
Woman	0.217	0.175

表 5　嵌入的二维码的尺寸为 256 像素×256 像素时本文提出的算法中嵌入参数的均值和标准差

载体图像	均值	标准差
Jetplane	0.258	0.234
Lena	0.216	0.21
Living room	0.19	0.197
Mandril	0.224	0.221
Peppers	0.197	0.192
Woman	0.214	0.194

在表 2 和表 3 中使用均值和标准差这 2 个统计量评价图像可逆可视水印算法在客观质量上的综合性能。对于给定的图像可逆可视水印算法，相应的图像客观质量的均值越大说明该算法综合性能越好。在表 2 中，本文提出的算法在 PSNR 和 SSIM 上均取得了最好的综合性能。在表 3 中，Yao 等算法在 PSNR 上取得了最好的综合性能，本文提出的算法在 SSIM 上取得了最好的综合性能。PSNR 的标准差越大，说明图像可逆可视水印算法的对图像的自适应能力越强。

4.4　图像隐私保护方案的安全性分析

图像隐私保护方案的安全性包括加密安全性和可视水印安全性。

4.4.1　加密安全性

通过云平台传输数据时存在隐私泄露风险。在本文提出的基于二维码和可逆可视水印的图像隐私保护方案中，构建了图像发送方、云平台和图像接收方之间的数据安全流转通道，有效降低了隐私泄露的风险。对于图像发送方，需要对原始图像进行去隐私信息处理，并根据加密密钥对隐私信息进行加密，降低了与云平台通信过程中的隐私泄露。对于云平台，隐私信息处于加密状态，云平台在没有加密密钥的情况下无法得到解密的隐私信息。对于非授权用户，由于没有正确的加密密钥，即使获得嵌入二维码的载密图像，也无法得到与图像关联的隐私信息。

在本文提出的针对二维码的图像可逆可视水印算法中，用于载体图像无损恢复的压缩后的重构数据分组的长度为 L。使用流密码加密压缩后的重构数据分组时产生 L 种可能的伪随机序列[25]，在没有水印密钥的情况下得到压缩后的重构数据分组的概率为 $\frac{1}{L}$。因此，在没有水印密钥的情况下，非授权用户几乎无法提取嵌入的二维码。

然而，有时候存在授权用户恶意泄露隐私信息加密密钥和水印密钥的情况，从而导致图像隐私保护方案遭受攻击。此时可以采用基于 Shamir 秘密共享的密钥分发及其改进算法[26]提升图像隐私保护方案的加密安全性。对于隐私信息加密密钥，秘密分发者为图像发送方；对于水印密钥，秘密分发者为云平台。

在秘密共享的初始化阶段，秘密分发者需要根据 n 个不同的非零元素 $x_1,x_2,\cdots,x_n$ 标识每个影子秘密拥有者 $U_r\in\{U_1,U_2,\cdots,U_n\}$，并公开 x_r 以及相应的 U_r。

在秘密分发阶段，假设需要分发的秘密为 s，则需要在有限域 GF(p) 中任意选择 $(t-1)$ 个元素构成多项式，如式(17)所示。

$$f(x)=(a_0+\sum_{i=1}^{t-1}a_i x^i)\bmod p \tag{17}$$

其中，大素数 $p>s$，待分发的秘密 $s=f(0)=a_0$。秘密分发者为每个影子秘密拥有者 U_r（$r=1,2,\cdots,n$）生成的影子秘密可以表示为

$$s_r=f(x_r)=(a_0+\sum_{i=1}^{t-1}a_i x_r^i)\bmod p \tag{18}$$

在生成影子秘密之后，秘密分发者可以将 s_r 安全地发送给相应的影子秘密拥有者 U_r。

在秘密恢复阶段，任何 t 个影子秘密拥有者可以使用如式(19)所示的拉格朗日插值公式恢复秘密 s，这里的秘密 s 可以是隐私信息加密密钥或水印密钥。

$$s=\sum_{i=1}^{t}f(x_i)\prod_{j=1,j\neq i}^{t}\frac{-x_j}{x_i-x_j}\bmod p \tag{19}$$

基于 Shamir 秘密共享的密钥分发中，任意不少于 t 个影子秘密能够恢复出分发的秘密，并且少于 t 个影子秘密不能获得关于分发的秘密的任何信息，提

升了图像隐私保护方案的加密安全性。

4.4.2 可视水印安全性

水印的稳健性是十分重要的性质。在本文提出的图像隐私保护方案中，水印的稳健性可以保证在嵌入二维码的载密图像遭受恶意攻击时，授权用户仍然可以提取嵌入的二维码，从而得到与图像关联的隐私信息。由于图像经常在异构网络中传输，图像传输会面临网络带宽的变化。JPEG 图像压缩是常用的且有效的针对图像水印的攻击手段。

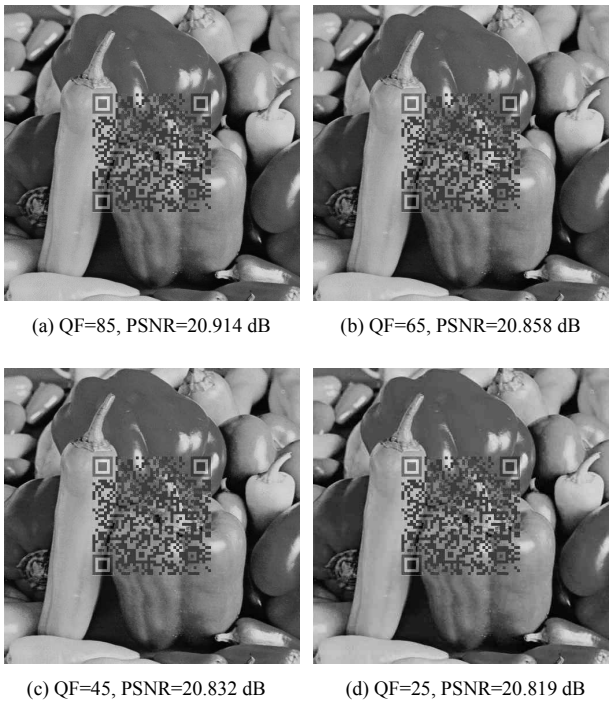
为了验证本文提出的针对二维码的图像可逆可视水印算法的稳健性，图 10 描述了当载体图像为 Lena 且嵌入的二维码的尺寸为 128 像素×128 像素时生成的载密图像抵抗 JPEG 图像压缩攻击的稳健性，图 11 描述了当载体图像为 Peppers 且嵌入的二维码的尺寸为 256 像素×256 像素时生成的载密图像抵抗 JPEG 图像压缩攻击的稳健性。JPEG 图像压缩中选取的质量因子（QF, quality factor）分别为 85、65、45 和 25。选取的质量因子越低，对载密图像的压缩程度越高，相应的载密图像视觉质量越低。从图 10 和图 11 的稳健性分析实验可以看出，即使当质量因子为 25 时，载密图像中嵌入的二维码仍然可以被正确识别。

(a) QF=85, PSNR=27.589 dB (b) QF=65, PSNR=27.376 dB

(c) QF=45, PSNR=27.213 dB (d) QF=25, PSNR=26.967 dB

图 10 载密图像 Lena 抵抗 JPEG 图像压缩攻击的稳健性
（二维码尺寸为 128 像素×128 像素，可识别）

在图 10 中，与质量因子为 85、65、45 和 25 的载密图像对应的 PSNR 分别为 27.589 dB、27.376 dB、27.213 dB 和 26.967 dB。在图 11 中，与质量因子为 85、65、45 和 25 的载密图像对应的 PSNR 分别为 20.914 dB、20.858 dB、20.832 dB 和 20.819 dB。稳健性分析实验表明，本文提出的图像隐私保护方案具有抵抗 JPEG 图像压缩的稳健性，在一定程度的恶意攻击环境下仍然可以发挥作用。



(a) QF=85, PSNR=20.914 dB (b) QF=65, PSNR=20.858 dB

(c) QF=45, PSNR=20.832 dB (d) QF=25, PSNR=20.819 dB

图 11 载密图像 Peppers 抵抗 JPEG 图像压缩攻击的稳健性
（二维码尺寸为 256 像素×256 像素，可识别）

5 结束语

本文针对图像在网络传输中的隐私信息泄露问题，提出了一种基于二维码和可逆可视水印的图像隐私保护方案。在该方案中，图像发送方为了保护图像拍摄时间、拍摄地点和详细描述等隐私信息，首先将这类隐私信息加密后存储在云平台，并由云平台生成能够链接到加密隐私信息的统一资源定位符。云平台将统一资源定位符编码成二维码，并将该二维码作为可视水印可逆地嵌入图像中，实现对隐私信息的访问权限控制。为了平衡水印的可视性和载密图像的视觉质量，在该方案中使用视觉感知模型选择适合的水印嵌入参数。实验结果表明，使用该方案进行可视水印嵌入能够保证载密图像具有良好的视觉质量，同时不影响二维码的正确识别和解码。该方案既保障了图像的传输质量也降低了隐私泄露风险。

参考文献：

[1] 李凤华, 李晖, 贾焰, 等. 隐私计算研究范畴及发展趋势[J]. 通信学报, 2016, 37(4): 1-11.
LI F H, LI H, JIA Y, et al. Privacy computing: concept, connotation and its research trend[J]. Journal on Communications, 2016, 37(4): 1-11.

[2] 中国互联网信息中心. 第 43 次中国互联网发展状况统计报告[R]. (2019-02-28)[2019-07-08].
China Internet Network Information Center. The 43rd China statistical report on internet development[R]. (2019-02-28)[2019-07-08].

[3] 李维皓, 曹进, 李晖. 基于位置服务隐私自关联的隐私保护方案[J]. 通信学报, 2019, 40(5): 57-66.
LI W H, CAO J, LI H. Privacy self-correlation privacy-preserving scheme in LBS[J]. Journal on Communications, 2019, 40(5): 57-66.

[4] 王新宇, 牛犇, 李凤华, 等. APP 隐私泄露风险评估与保护方案[J]. 通信学报, 2019, 40(5): 13-23.
WANG X Y, NIU B, LI F H, et al. Risk assessing and privacy-preserving scheme for privacy leakage in APP[J]. Journal on Communications, 2019, 40(5): 13-23.

[5] 严文博, 姚远志, 张卫明, 等. 基于二维码和信息隐藏的物流系统隐私保护方案[J]. 网络与信息安全学报, 2017, 3(11): 22-28.
YAN W B, YAO Y Z, ZHANG W M, et al. Privacy-preserving scheme for logistics systems based on 2D code and information hiding[J]. Chinese Journal of Network and Information Security, 2017, 3(11): 22-28.

[6] MOHANTY S P, RAMAKRISHNAN K R, KANKANHALLI M S. A DCT domain visible watermarking technique for images[C]//International Conference on Multimedia and Expo. IEEE, 2000: 1029-1032.

[7] SHI Y Q, LI X, ZHANG X, et al. Reversible data hiding: advances in the past two decades[J]. IEEE Access, 2016, 4: 3210-3237.

[8] HU Y, JEON B. Reversible visible watermarking and lossless recovery of original images[J]. IEEE Transactions on Circuits and Systems for Video Technology, 2006, 16(11): 1423-1429.

[9] YIP S K, AU O C, HO C W, et al. Lossless visible watermarking[C]//International Conference on Multimedia and Expo. IEEE, 2006: 853-856.

[10] TSAI H M, Chang L W. A high secure reversible visible watermarking scheme[C]//International Conference on Multimedia and Expo. IEEE, 2007: 2106-2109.

[11] LIU T Y, TSAI W H. Generic lossless visible watermarking—a new approach[J]. IEEE Transactions on Image Processing, 2010, 19(5): 1224-1235.

[12] YANG Y, SUN X, YANG H, et al. A contrast-sensitive reversible visible image watermarking technique[J]. IEEE Transactions on Circuits and Systems for Video Technology, 2009, 19(5): 656-667.

[13] MOHAMMAD N, SUN X, YANG H, et al. Lossless visible watermarking based on adaptive circular shift operation for BTC-compressed images[J]. Multimedia Tools and Applications, 2017, 76(11): 13301-13313.

[14] LIN Y K, YANG C H, TSAI J T. More secure lossless visible watermarking by DCT[J]. Multimedia Tools and Applications, 2018, 77(7): 8579-8601.

[15] YAO Y, ZHANG W, WANG H, et al. Content-adaptive reversible visible watermarking in encrypted images[J]. Signal Processing, 2019, 164: 386-401.

[16] HUANG H C, CHANG F C, FANG W C. Reversible data hiding with histogram-based difference expansion for QR code applications[J]. IEEE Transactions on Consumer Electronics, 2011, 57(2): 779-787.

[17] FRAGOSO-NAVARRO E, CEDILLO-HERNÁNDEZ M, NAKANO-MIYATAKE M, et al. Visible watermarking assessment metrics based on just noticeable distortion[J]. IEEE Access, 2018, 6: 75767-75788.

[18] GAO X, LU W, TAO D, et al. Image quality assessment based on multiscale geometric analysis[J]. IEEE Transactions on Image Processing, 2009, 18(7): 1409-1423.

[19] WU H R, REIBMAN A R, LIN W, et al. Perceptual visual signal compression and transmission[J]. Proceedings of the IEEE, 2013, 101(9): 2025-2043.

[20] LIU A, LIN W, PAUL M, et al. Just noticeable difference for images with decomposition model for separating edge and textured regions[J]. IEEE Transactions on Circuits and Systems for Video Technology, 2010, 20(11): 1648-1652.

[21] WU J, LIN W, SHI G, et al. Pattern masking estimation in image with structural uncertainty[J]. IEEE Transactions on Image Processing, 2013, 22(12): 4892-4904.

[22] WU J, LI L, DONG W, et al. Enhanced just noticeable difference model for images with pattern complexity[J]. IEEE Transactions on Image Processing, 2017, 26(6): 2682-2693.

[23] SACHNEV V, KIM H J, NAM J, et al. Reversible watermarking algorithm using sorting and prediction[J]. IEEE Transactions on Circuits and Systems for Video Technology, 2009, 19(7): 989-999.

[24] WANG Z, BOVIK A C, SHEIKH H R, et al. Image quality assessment: from error visibility to structural similarity[J]. IEEE Transactions on Image Processing, 2004, 13(4): 600-612.

[25] MENEZES A J, VAN OORSCHOT P C, VANSTONE S A. Handbook of applied cryptography[M]. CRC Press, 1996.

[26] 荣辉桂, 莫进侠, 常炳国, 等. 基于 Shamir 秘密共享的密钥分发与恢复算法[J]. 通信学报, 2015, 36(3): 265-274.
RONG H G, MO J X, CHANG B G, et al. Key distribution and recovery algorithm based on Shamir's secret sharing[J]. Journal on Communications, 2015, 36(3): 265-274.

[作者简介]

姚远志（1989− ），男，安徽望江人，博士，中国科学技术大学副研究员，主要研究方向为信息隐藏和视频编码。

王锋（1996− ），男，安徽潜山人，中国科学技术大学硕士生，主要研究方向为信息隐藏和隐私保护。

严文博（1991− ），男，安徽寿县人，中国科学技术大学博士生，主要研究方向为信息隐藏和隐私保护。

俞能海（1964− ），男，安徽无为人，博士，中国科学技术大学教授、博士生导师，主要研究方向为图像视频处理与分析、计算机视觉与模式识别、信息隐藏与媒体内容安全、信息检索与数据挖掘。