基于二维码和信息隐藏的物流系统隐私保护方案

严文博，姚远志，张卫明，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：针对现有物流系统中的用户隐私信息容易泄露的问题，提出了一种基于二维码和信息隐藏的物流系统隐私保护方案。该方案使用信息隐藏技术将用户隐私信息嵌入快递面单上的二维码中，完成对隐私信息的访问权限控制。为了提升用户隐私信息的安全性，在该方案中设计了一种用于二维码的 JPEG 图像隐写算法。实验结果表明，该算法使在二维码图像中嵌入的用户隐私信息具有较高的抗检测性能，同时不影响载密二维码的正确扫描和解码。使用本文所提方案，在物流系统中具有访问权限的机构或个人才能够获取这些重要的隐私信息，既确保了快件的正确投递，也保障了用户的隐私安全。

关键词：二维码；信息隐藏；物流系统；隐私保护
中图分类号：TP309.2
文献标识码：A
doi: 10.11959/j.issn.2096-109x.2017.00210

Privacy-preserving scheme for logistics systems based on 2D code and information hiding

YAN Wen-bo, YAO Yuan-zhi, ZHANG Wei-ming, YU Neng-hai
(School of Information Science and Technology, University of Science and Technology of China, Hefei 230027, China)

Abstract: With regard to the user privacy leakage problem in existing logistics systems, a privacy-preserving scheme for logistics systems based on 2D code and information hiding was proposed. The information hiding technique was used in the proposed scheme to embed the user privacy information into the 2D code on the logistics waybill to achieve access control. To secure the user privacy information, a JPEG image stenographic algorithm for 2D code was designed. Experimental results demonstrate that this algorithm can guarantee the high undetectable performance and the stego 2D code can be correctly decoded. Using the proposed scheme, the institution or the person that has the access right can obtain the important privacy information so that the express can be delivered correctly and the user privacy can be preserved.

Key words: 2D code, information hiding, logistics system, privacy preservation

1　引言

随着互联网技术的成熟和其应用的深入，更多的行业在互联网技术下得到了成长和发展。其中，电子商务因其贴合大众生活等众多优点，在人们的生产生活中得到了迅猛和广泛发展。随着信息化的深入，电子商务在给人们提供廉价服务的同时，也令整个物流产业得到了高速前进的机会。据资料统计，2014 年全年中国快递行业总的业务受理量超过 140 亿件，第一次达到世界首位；2015 年更是突破 200 亿，达到人均 14 件[1]；2016 年中国快递行业业务量超过 300 亿件，同比增长约

收稿日期：2017-08-02；**修回日期**：2017-09-20。**通信作者**：俞能海，ynh@ustc.edu.cn
基金项目：国家自然科学基金资助项目（No.61371192, No.61572452, No.U1636201）
Foundation Item: The National Natural Science Foundation of China (No.61371192, No.61572452, No.U1636201)

50%；业务收入将近 4 000 亿人民币[2]。虽然各大物流公司推出各种多样化的配送服务，如“限时达”“次日达”和“夜间配”等。但是，物流行业在高速发展的同时也不可避免地产生了一些新的隐患，其中尤为引人注意的就是物流行业的快速发展带来用户隐私泄露问题[3]。

在物流系统中，一般通过在快件上粘贴面单的方式进行快件的流通，快递公司在快递面单中已经广泛使用条形码技术。二维码作为一种不同于传统码字的编码图形[4]，带来与以往不同的信息传递和存储的解决方案，它与其他编码方式相比具有高容量、高抗干扰、实用便捷等显著优点，一经面世就受到了广大信息领域专家学者的研究与关注。QR 码（quick response code）是一种广泛使用的二维码，在物流系统中主要存在于纸质订单和电子面单上。因此，现行快递面单上的条形码主要是 QR 码。

虽然二维码具有较强的健壮性，可以很好地切合快递面单易受污损的特点，并且方便读取，可以很好地提高快递运输的准确性和效率。但是，在快递面单上直接使用二维码的后果是用户个人信息相当于直接以明文的方式显现在快递面单上，任何人只要通过二维码识别设备就可以轻易地获取二维码中蕴含的用户个人信息。在快递公司快件运输的业务流程中，如果用户的个人信息没有采取保护措施，会导致用户的个人隐私信息暴露在外，存在隐私泄露的隐患。据报道，某些不法分子将快递面单上的用户隐私信息用于商业交易以谋取利益，甚至利用用户隐私信息跟踪用户或对用户进行电话骚扰。这些不法行为严重地侵害了用户的合法权益。

根据以上分析，有必要对现行的物流信息系统进行改进，使快件在物流系统中高效运转的同时不会泄露用户的隐私信息。本文提出了一种基于二维码和信息隐藏的物流系统隐私保护方案，使用信息隐藏技术将用户隐私信息嵌入快递面单上的二维码中，完成对隐私信息的访问权限控制。为了保护用户隐私，需要对收件人信息进行分级处理，将其信息分为明文信息和密文信息。密文信息是包含收件人姓名、详细地址以及联系方式等的重要隐私信息，也是本物流系统隐私保护方案需要重点保护的信息。该方案将明文信息编码成载体 QR 码，并使用信息隐藏技术将密文信息嵌入载体QR码中生成载密 QR 码。使用该方案的物流系统包括订单提交模块、物流配送模块、物流中转模块和可信任云平台这 4 个模块，其中，配送工作人员和中转站根据扫描 QR 码得到的明文信息完成配送和中转任务。扫描载密QR码通知收件人取件的实际操作是由可信任云平台执行的。值得注意的是，在整个物流系统隐私保护方案中，只有可信任云平台才可以提取载密 QR 码中的收件人密文信息，收件人的隐私信息得到了很好的保护。

2　国内外研究现状

由于物流行业中的隐私泄露问题逐渐得到人们的关切和重视，国内外已有一些保护用户隐私的技术和方法。

目前，世界上的一些发达国家主要使用行业自律准则和颁布法律法规解决物流行业中的隐私泄露问题。英国邮政管理委员会规定，在物流运营商的许可证中必须明确关于邮政安全的相关条款，美国规定快递员在上岗前必须提供社会安全号[5]。上述通过法律法规或行业规范约束相关从业人员的做法的确可以解决一部分隐私泄露问题，但用户的个人隐私信息依然存在泄露的隐患。

目前，国内快递行业对于用户隐私泄露问题也给予了一定程度的重视。一些快递公司将用户个人信息封装于二维码再打印到快递面单中，只有获得相关的权限才可以扫描二维码获取用户个人信息。近年来，推出的隐私面单将用户个人信息用星号代替的方式，在隐私信息保护上取得了不小的进步。文献[3]提出一种采用分段加密技术对用户个人信息进行分层加密后转存到二维码的物流系统隐私保护方案。但以上的物流系统隐私保护方法只是设置了获取用户个人信息的访问权限，并没有掩盖用户个人信息存在的事实。如果出现服务器端的数据大规模泄露，容易引发用户隐私信息的严重泄露。

3　物流系统隐私保护方案

3.1　隐私保护方案框架

在本文提出的基于二维码和信息隐藏的物流系统隐私保护方案中，使用信息隐藏技术将用户

隐私信息嵌入快递面单上的二维码中，完成对隐私信息的访问权限控制。隐私保护方案框架如图 1 所示。使用该方案的物流系统包括订单提交模块、物流配送模块、物流中转模块和可信任云平台这 4 个模块。

在订单提交模块中，寄件人通过移动终端 App 在线提交订单时需要填写寄件人信息和收件人信息。在线提交订单的步骤如下。1) 对收件人信息进行分级处理，将其信息分为明文信息和密文信息。需要重点保护的密文信息是包含收件人姓名、详细地址以及联系方式的重要隐私信息。2) 将明文信息编码成载体 QR 码，并使用信息隐藏技术将密文信息嵌入载体 QR 码中生成载密 QR 码。3) 将寄件人信息和载密 QR 码上传至可信任云平台。生成载密 QR 码的示意如图 2 所示。

在物流配送模块中，配送工作人员通过移动终端 App 收到快递任务消息时可以从可信任云平

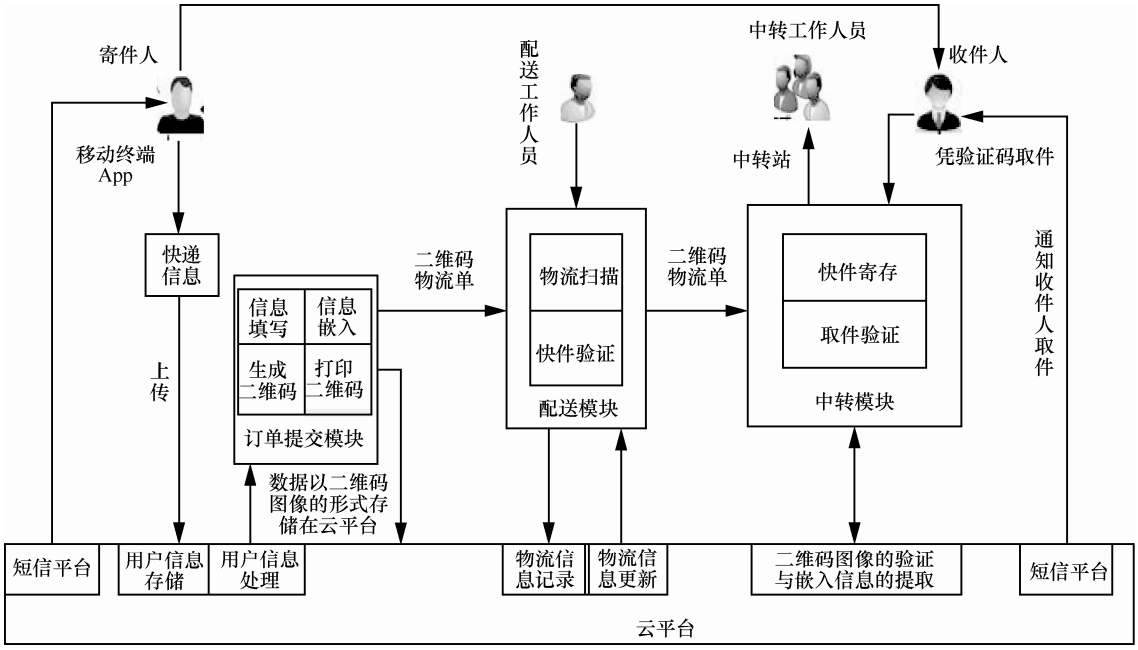


图 1　隐私保护方案框架

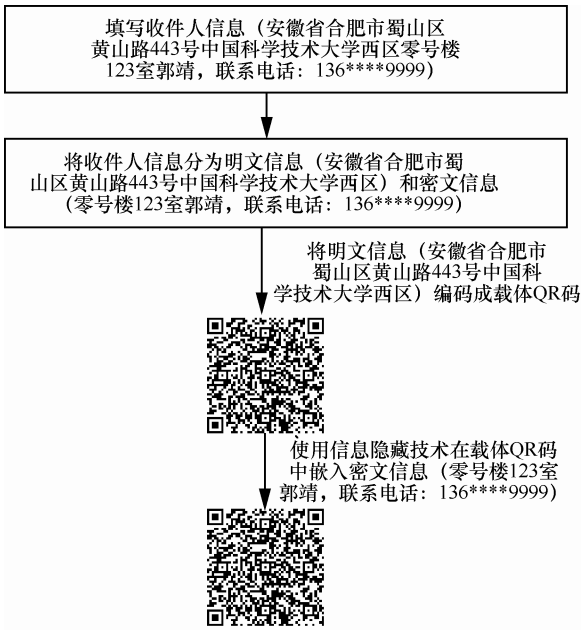


图 2　生成载密 QR 码的示意

台下载寄件人信息和载密 QR 码。配送工作人员联系寄件人接收快件并打印载密 QR 码至快递面单上，再根据扫描 QR 码获取的明文信息定位地址区域进行物流配送。当配送工作人员将快件配送至相应的中转站后，完成快件交接。

在物流中转模块中，当有新快件到达时，中转工作人员会扫描载密 QR 码，触发可信任云平台通知收件人取件，并向中转工作人员和收件人发送验证码。当收件人收到取件通知时，即可前往相应的中转站取件。取件时中转工作人员与收件人核对各自持有的验证码是否一致，若二者一致则完成取件。

在上述的隐私保护方案中，只有可信任云平台才可以提取载密 QR 码中的收件人密文信息，从而通知收件人取件。因此，配送工作人员、中转工作人员和其他人员无法获取收件人密文信息，收件人的隐私信息得到了有效保护。

3.2　用于二维码的 JPEG 图像隐写算法

在本文提出的基于二维码和信息隐藏的物流系统隐私保护方案中，QR 码图像是以 JPEG 格式存储的。为了提升嵌入密文信息的抗检测性能，需要设计高安全性的用于二维码的 JPEG 图像隐写算法。

通过观察 QR 码图像可以发现其中的黑色方块和白色方块的交界处具有丰富的纹理信息，属于自适应隐写中优先嵌入消息的区域。为了丰富载体图像的纹理区域，增加嵌入信息量，在嵌入秘密消息之前，可以对 QR 码图像进行纹理增强。纹理增强采用的方法是将 QR 码图像和具有较丰富纹理的自然图像进行融合。假设 QR 码图像的 (i,j) 位置处的像素值为 $I(i,j)$，自然图像的 (i,j) 位置处的像素值为 $J(i,j)$，则纹理增强的 QR 码图像的 (i,j) 位置处的像素值 $S(i,j)$ 的计算方法如下。

$$S(i,j)=\alpha\cdot I(i,j)+\beta\cdot J(i,j) \tag{1}$$

在式(1)中，参数 α 取值为 0.6，参数 β 取值为 0.4。

对 QR 码图像进行纹理增强处理的优势如下。第一，丰富了载体图像的纹理信息，提升了嵌入秘密消息的抗检测性能；第二，不影响 QR 码的正确扫描和识别；第三，用于纹理增强的自然图像可以是快件包裹（或信封）的快照，方便寄件人、收件人和工作人员辨识包裹（或者信封），提高物流效率。

最小化嵌入失真隐写模型[6]是目前设计高安全性隐写算法的理论基础。在最小化嵌入失真隐写模型中，可以假设消息嵌入时的载体序列为 $x=(x_1,x_2,\cdots,x_n)$，待嵌入的秘密消息序列为 $m=(m_1,m_2,\cdots,m_q)$。在载体中嵌入秘密消息 m 后，生成的载密序列为 $y=(y_1,y_2,\cdots,y_n)$。假设秘密消息嵌入过程中修改各个载体元素引入的嵌入失真是相互独立的，则嵌入秘密消息后对载体引入的总体嵌入失真为

$$D(x,y)=\sum_{i=1}^{n}\rho_i(x_i,y_i) \tag{2}$$

在式(2)中定义的嵌入失真称为加性失真，其中 $\rho_i(x_i,y_i)$ 满足 $0\leqslant\rho_i(x_i,y_i)\leqslant+\infty$，表示载体元素 x_i 因嵌入秘密消息变成 y_i 后对载体元素引入的嵌入失真。在本算法中，秘密消息嵌入可以看成是如下的嵌入给定秘密消息 m 时，使总体嵌入失真最小化的优化问题。

$$\begin{aligned}&\min_{\pi}E_{\pi}(D)=\sum_{y\in\mathbb{Y}}\pi(y)D(x,y)\\&\text{subject to } H(\pi)=-\sum_{y\in\mathbb{Y}}\pi(y)\log\pi(y)=q\end{aligned} \tag{3}$$

在式(3)中，$\pi(y)$ 是将载体序列 x 修改为载密序列 y 的概率。STC 编码（syndrome-trellis code）[7]可以在嵌入给定秘密消息的过程中最小化总体嵌入失真，是设计高安全性隐写算法的强有力工具[8,9]。

因此，设计隐写方法的关键在于如何定义失真函数 $\rho_i(x_i,y_i)$。J-UNIWARD 算法[10,11]是目前抗检测性能较强的 JPEG 图像隐写算法。因此，可以将 J-UNIWARD 算法用于纹理增强的 QR 码图像隐写。在 J-UNIWARD 算法中，首先将需要嵌入消息的载体 JPEG 图像解码为空域图像 X。对载体 JPEG 图像中的某个量化 DCT 系数 x_i 定义嵌入失真时，首先对该量化 DCT 系数 x_i 进行加 1 或减 1 操作，然后将修改后的 JPEG 图像解码为空域图像 Y。通过 3 个不同方向的线性小波滤波器分别对空域图像 X 和空域图像 Y 滤波，得到 3 个不同方向滤波后的频域系数矩阵 $\boldsymbol{W}^{(k)}(X)$ 和

$\boldsymbol{W}^{(k)}(Y)$，其中 $k \in \{1,2,3\}$。

那么，总体嵌入失真可以按如下方式定义。

$$D(X,Y)=\sum_{k=1}^{3}\sum_{u,v}\frac{|\boldsymbol{W}_{u,v}^{(k)}(X)-\boldsymbol{W}_{u,v}^{(k)}(Y)|}{\varepsilon+|\boldsymbol{W}_{u,v}^{(k)}(X)|} \tag{4}$$

在式(4)中，u,v 是量化 DCT 系数的坐标，参数 ε 是用于平滑的常数，这里取 $\varepsilon=10^{-15}$。在物流系统隐私保护方案中，纹理增强的 QR 码图像实际是 JPEG 图像，具有丰富的纹理信息。因此，J-UNIWARD 算法可以自然地用于高安全性的二维码图像隐写。为了进一步提升安全性，在秘密消息嵌入之前使用密钥 key 对秘密消息加密，生成加密的秘密消息，然后使用高安全性的二维码图像隐写算法进行消息嵌入。

4　实验设计与结果分析

4.1　实验设置

为了验证本文设计的用于二维码的 JPEG 图像隐写算法的性能，将用于二维码的 JPEG 图像隐写算法在 Matlab R2016b 中实现，这里使用 QR 码开源开发库 ZXing[12]实现 QR 码图像的编码和解码。

4.2　载密图像质量

首先使用标准测试图像 Lena[13]作为纹理增强的自然图像，生成如图 3(a)所示的纹理增强的 QR 码图像，该图像为载体图像。对图 3(a)中的纹理增强的载体 QR 码图像进行消息嵌入时，经过编码该 QR 码含有的明文信息“安徽省合肥市黄山路 443 号中国科学技术大学”，嵌入的密文信息为“科技实验楼”，得到如图 3(b)所示的含有密文信息的载密 QR 码图像。

使用客观图像质量评价指标 *PSNR* 对图 3 中的含有密文信息的载密 QR 码图像进行质量评价。*PSNR* 的计算方法如式(5)所示。

$$PSNR=10\lg\frac{(2^n-1)^2}{MSE} \tag{5}$$

在式(5)中，*MSE* 是载密图像和载体图像之间像素的均方误差，n 是图像的比特位深度，这里取 $n=8$。实验中测得的 *PSNR* 值为 71.538 9 dB，说明用于二维码的 JPEG 图像隐写算法生成的载密 QR 码图像具有较高的图像质量。图 3(a)的纹理增强的 QR 码图像和图 3(b)的含有密文信息的载密 QR 码图像均可正确扫描和解码。

(a) 纹理增强的载体 QR 码图像

(b) 含有密文信息的载密 QR 码图像

图 3　纹理增强的载体 QR 码图像和含有密文信息的载密 QR 码图像

4.3　抗检测性能

1) 图像库构建

为了测试用于二维码的 JPEG 图像隐写算法的抗检测性能，首先使用 QR 码开源开发库 ZXing[12]随机生成 1 000 张 QR 码图像，并使用 BOSSbase 1.01[14]图像库中的 1 000 张图像作为用于纹理增强的自然图像，最后生成 1 000 张纹理增强的 QR 码图像。

2) 特征选择

使用经典的 JPEG 图像隐写分析方法 CHEN486[15]、CCPEV548[16]和 DCTR[17]提取特征，这 3 种方法提取的特征维度分别为 486、548 和 8 000。

3) 训练与分类

在隐写分析实验中使用分类器 Ensemble Classifier[18]。秘密消息嵌入率使用平均每个交流 DCT 系数嵌入的比特数衡量。秘密消息的嵌入率

分别设置为 0.05 bpac、0.1 bpac、0.2 bpac、0.3 bpac、0.4 bpac 和 0.5 bpac。使用最小平均错误检测概率 P_E 衡量抗检测性能，如式(6)所示。一般认为，若最小平均错误检测率大于 0.4，则该信息隐藏方法的抗检测性能满足要求。

$$P_E = \min_{P_{FA}} \frac{P_{FA} + P_{MD}(P_{FA})}{2} \tag{6}$$

在式(6)中，P_{FA} 和 P_{MD} 分别是虚警率和漏检率。表 1 描述了用于二维码的 JPEG 图像隐写算法的抗检测性能。如果分辨率为 512×512 的纹理增强的载体 QR 码图像经过编码含有明文信息“安徽省合肥市黄山路 443 号中国科学技术大学”，嵌入的密文信息为“科技实验楼”。此时载体图像中的交流量化 DCT 系数数目为 258 048，嵌入的密文信息“科技实验楼”所需比特数为 80，那么实际的秘密消息的嵌入率约为 0.000 3 bpac。根据表 1 中的抗检测性能比较，当秘密消息的嵌入率为 0.000 3 bpac 时，在 3 种隐写分析方法检测下的最小平均错误检测率均高于 0.4，具有较高的抗检测性能，满足保护用户隐私的需求。如果选取嵌入率为 0.1 bpac，那么实际的嵌入的密文信息所需比特数为 25 804，约 1 600 个中文汉字，可以满足快递面单中信息的长度要求，同时具有较高的抗检测性能。

表 1　　抗检测性能比较

嵌入率/bpac	抗检测性能		
	CHEN486	CCPEV548	DCTR
0.05	0.467 0	0.473 0	0.434 0
0.1	0.440 0	0.451 0	0.361 0
0.2	0.352 0	0.370 0	0.242 0
0.3	0.254 0	0.274 0	0.164 0
0.4	0.187 0	0.227 0	0.108 0
0.5	0.128 0	0.161 0	0.065 0

5　结束语

引发现行物流系统中用户隐私信息泄露的主要原因在于用户隐私信息通常以明文的方式呈现在快递面单上，一旦不法分子得到快递面单，即可获取这些重要隐私信息。本文提出了一种基于二维码和信息隐藏的物流系统隐私保护方案。该方案使用信息隐藏技术将用户隐私信息嵌入快递面单上的二维码中，完成对隐私信息的访问权限控制。为了提升用户隐私信息的安全性，在该方案中设计了一种用于二维码的 JPEG 图像隐写算法。实验结果表明，该算法使在二维码图像中嵌入的用户隐私信息具有较高的抗检测性能，同时不影响载密二维码的正确扫描和解码。使用本文提出的方案，在物流系统中具有访问权限的机构或个人才能够获取这些重要的隐私信息，既确保了快件的正确投递，也保障了用户的隐私安全。

参考文献：

[1] 中华人民共和国国家邮政局. 2016 年中国快递发展指数报告[M]. 2016.
State Post Bureau of The People’s Republic of China. China express development index report in 2016[R]. 2016.

[2] 中华人民共和国国家邮政局. 2016 年邮政行业发展统计公报[R]. 2016.
State Post Bureau of The People’s Republic of China. Statistics report of the postal industry in 2016[R]. 2016.

[3] ZHANG X, LI H, YANG Y, et al. LIPPS: logistics information privacy protection system based on encrypted QR code[C]//IEEE Trustcom/BigDataSE/ISPA. 2016: 996-1000.

[4] QR Code 二维码技术与应用[M]. 北京: 中国标准出版社, 2002.
QR Code technique and application[M]. Beijing: Standards Press of China, 2002.

[5] BERGHEL H. Identity theft, social security numbers, and the Web[J]. Communications of the ACM, 2000, 43(2): 17-21.

[6] FILLER T, FRIDRICH J. Gibbs construction in steganography[J]. IEEE Transactions on Information Forensics and Security, 2010, 5(4): 705-720.

[7] FILLER T, JUDAS J, FRIDRICH J. Minimizing additive distortion in steganography using syndrome-trellis codes[J]. IEEE Transactions on Information Forensics and Security, 2011, 6(3): 920-935.

[8] LI B, WANG M, LI X, et al. A strategy of clustering modification directions in spatial image steganography[J]. IEEE Transactions on Information Forensics and Security, 2015, 10(9): 1905-1917.

[9] SEDIGHI V, COGRANNE R, FRIDRICH J. Content-adaptive steganography by minimizing statistical detectability[J]. IEEE Transactions on Information Forensics and Security, 2016, 11(2): 221-234.

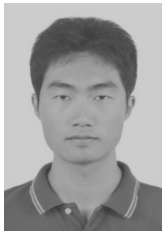
[10] HOLUB V, FRIDRICH J. Digital image steganography using universal distortion[C]//The first ACM Workshop on Information Hiding and Multimedia Security. 2013: 59-68.

[11] HOLUB V, FRIDRICH J, DENEMARK T. Universal distortion function for steganography in an arbitrary domain[J]. EURASIP Journal on Information Security, 2014, (1): 1-13.

[12] ZXing.Net[EB/OL]. http://zxingnet.codeplex.com/.
[13] Standard test images[EB/OL]. http://www.ece.rice.edu/~wakin/ images/.
[14] BAS P, FILLER T, PEVNY T. Break our steganographic system: the ins and outs of organizing BOSS[C]//Information Hiding. 2011: 59-70.
[15] CHEN C, SHI Y Q. JPEG image steganalysis utilizing both intrablock and interblock correlations[C]//IEEE International Symposium on Circuits and Systems. 2008: 3029-3032.
[16] PEVNY T, FRIDRICH J. Merging Markov and DCT features for multi-class JPEG steganalysis[C]//SPIE Electronic Imaging. 2007.
[17] HOLUB V, FRIDRICH J. Low-complexity features for JPEG steganalysis using undecimated DCT[J]. IEEE Transactions on Information Forensics and Security, 2015, 10(2): 219-228.
[18] KODOVSKT J, FRIDRICH J, HOLUB V. Ensemble classifiers for steganalysis of digital media[J]. IEEE Transactions on Information Forensics and Security, 2012, 7(2): 432-444.

作者简介：

严文博（1991-），男，安徽寿县人，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。



姚远志（1989-），男，安徽望江人，博士，主要研究方向为多媒体信号处理。

张卫明（1976-），男，河北定州人，博士，中国科学技术大学教授、博士生导师，主要研究方向为信息隐藏、密码学和媒体内容安全。

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。