基于图像多重隐写的区块链隐蔽通信方案

刘媛妮[①] 范 飞[①] 赵宇洋[①] 张建辉[②] 周由胜*[①]

[①](重庆邮电大学网络空间安全与信息法学院 重庆 400065)

[②](国家数字交换系统工程技术研究中心 郑州 450002)

摘 要：针对现有基于图像隐写的区块链隐蔽通信方案利用传统深度学习方法面临的抗隐写分析能力低、信息嵌入率低及信息泄露等问题，该文提出一种基于图像多重隐写嵌入的隐蔽通信方案。首先，构造基于隐写器的多重对抗网络，通过生成对抗网络和隐写分析对抗网络的对抗迭代训练，生成更适合信息隐写的载密图像；其次，利用基于位置图信息的密文域可逆信息隐藏方法，将隐蔽信息嵌入至载密图像，生成含完整隐蔽信息的载密密文图像；最后，将载密密文图像存储至IPFS文件返回唯一标识，利用地址映射的方法将该标识存储至区块链网络中实现隐蔽传输。理论及实验结果表明，相较于传统基于深度学习的区块链隐蔽通信方案，该方案具备更强的抗隐写检测攻击能力和更高的信息嵌入容量，同时减少了通信时延。

关键词：隐蔽通信；区块链；对抗网络；信息隐藏

中图分类号：TN918.91; TP309 **文献标识码**：A **文章编号**：1009-5896(2025)04-1126-14

DOI: 10.11999/JEIT240798

1 引言

隐蔽通信[1]是一种通过对通信内容进行编码、隐藏等方式保护通信信道传输的内容不被窃听，隐蔽信息安全传输的技术。现有隐蔽通信的实现方式包括认知无线电网络通信[2]、语义通信[3]、匿名通信、数字水印和隐写术等。其中，隐写术[4]作为隐蔽通信中的核心技术，通过将隐蔽信息嵌入载体生成载密图像，凭借其隐蔽性与抗攻击特性，广泛应用于数字水印、情报安全等领域。然而，攻击者可通过分析隐蔽信息的变化模式实施推断与破解，引发信息泄露风险。因此，研究面向隐蔽信息的安全通信机制，对于保障数据机密性、维护隐私安全具有重要理论与应用价值。

区块链[5]凭借去中心化、共识机制[6]、分布式存储、匿名性及不可篡改性等关键特性，为基于隐写术的隐蔽通信方案提供了更为可靠和安全的网络传输环境，并确保了通信双方身份的匿名性。即便区块链本身存在非授权端访问的风险，但是当前的隐蔽通信解决方案通过应用隐写术，将秘密信息嵌入到区块链交易中，通过在交易或数据流中嵌入看似无关紧要的信息片段，实现了发送方消息的有效隐藏。这种方法不仅增强了信息传递的隐蔽性和匿名性，还利用区块链的固有属性确保了数据的完整性和防篡改能力。然而，现有的基于区块链的隐蔽通信方案在安全性和传输效率方面仍面临挑战。在安全性方面，恶意用户可在新区块生成时通过交易信息分析引发安全威胁，或在载密载体上链前截获载体并分析特征以获取隐蔽信息；在传输效率方面，现有方案因依赖(Least Significant Bit, LSB)算法嵌入哈希串而产生大量账户交易地址，导致传输效率低下。文献[7,8]提出了通过优化信道接入和信息更新策略来提高传输的效率，但是信息的传输效率仍然会受到信息长度变化的影响，而利用星际文件系统[9](InterPlanetary File System, IPFS)将信息压缩成固定长度的标识传输，虽然可以有效地降低信息的传输开销，降低传输时延提高传输效率，但也增加了明文标识泄露的风险。

随着生成对抗网络[10](Generative Adversarial Networks, GAN)的发展，现有研究利用GAN生成与原始载体高度相似的载密图像，使攻击者难以区分是否含有隐蔽信息；进一步地，通过卷积神经网络[11–13](Convolutional Neural Network, CNN)检测载密图像，验证其抗隐写分析能力后上链传输。然而，上述方案在嵌入大量信息时易导致图像失真，增加隐蔽信息暴露风险；且当攻击者采用更精确的分类神经网络时，基于GAN生成的载密图像难以有效抵抗隐写分析攻击[14]。

本文针对区块链隐蔽通信中存在的隐写检测攻击、嵌入率低及传输开销大等问题，提出一种基于图像多重隐写的区块链隐蔽通信方案。本方案通过

收稿日期：2024-09-14；改回日期：2025-03-20；网络出版：2025-04-02

*通信作者： 周由胜 zhouys@cqupt.edu.cn

基金项目：国家重点研发计划(2023YFF0905300, 2023YFB3107405)，国家自然科学基金(62272076)

Foundation Items: The National Key Research and Development Program of China (2023YFF0905300, 2023YFB3107405), The National Natural Science Foundation of China (62272076)

多重对抗网络与密文域可逆信息隐藏算法生成高隐蔽性载密密文图像，并利用IPFS的唯一标识机制，结合区块链网络实现高效隐蔽传输。主要贡献如下：

(1)针对生成对抗网络生成载体易受隐写检测攻击的问题，本文提出一种基于隐写器的多重对抗网络，通过生成网络与判别网络的对抗迭代训练生成高相似度的载体图像，并利用隐写器嵌入隐蔽信息生成载密图像；同时利用隐写对抗网络检测载密图像的嵌密性，确保其具备抗隐写分析能力。

(2)针对传统隐写算法嵌入容量低且算法易被枚举的问题，本文提出一种基于位置图信息的密文域可逆信息隐藏方法，通过将位置图与隐蔽信息共同嵌入加密图像，实现载密图像的无损还原与高嵌入率，同时利用加密图像与载密密文图像的高度相似性，增强隐蔽信息的不可检测性。

(3)针对在区块链网络传输隐蔽信息传输效率低的问题，本文通过IPFS将载密密文图像压缩为唯一标识，采用字符映射方法将交易地址与标识映射生成序列，并嵌入交易后上传至区块链网络，有效防止恶意节点篡改信息。

(4)针对隐蔽消息长度变化导致的通信时延不稳定问题，本文通过IPFS将隐蔽消息处理为固定长度标识，利用字符索引关联交易与标识生成固定序列，嵌入交易后上传区块链网络，确保传输稳定性并显著降低时延。

实验结果表明，与现有方案相比，本方案不仅提高了载密图像的抗隐写分析能力，而且提高了隐蔽信息的嵌入容量，同时降低了传输过程的通信时延。

2　研究现状

现有隐蔽通信研究主要集中于利用区块链网络和神经网络模型生成载体进行数据传输。然而，现有方案普遍存在信息嵌入率低、载体图像易受隐写检测攻击及通信效率低等问题。

在区块链网络传输隐蔽信息方面，现有方法主要集中构建新的隐写算法，保证隐蔽信息的安全传输方面。针对传统隐蔽信道的抗干扰性及抗篡改性弱等问题，李彦峰等人[15]构建基于业务操作时间间隔的时间型区块链网络隐蔽信道，每间隔1次业务操作时间发送1次隐蔽信息，并通过区块的大小决定传输信息量，该传输信道具有较高的隐蔽性和安全性，但该信道不适用于其它传输模型。针对区块链网络传输信息的安全问题，Zhang等人[16]提出一种基于智能合约的隐蔽通信模型，通过将智能合约中的参数与隐蔽信息序列进行匹配，在调用智能合约的同时传输隐蔽信息，该模型具有防篡改和复杂度低的特点，但传输信息量有待增加。针对现有隐藏方法携带信息量低的问题，黄冬艳等人[17]设计了一种基于时间戳的密文传输方法，该方法将密文信息分片表示成区块时间戳间隔，并通过区块链进行传输，该方法提升了传输信息的效率，但易受到区块链内部节点的攻击且传输的开销较大。针对文本明文传输可能存在的安全问题，She等人[18]设计了一种基于IPFS的区块链传输方法，通过IPFS压缩了传输的信息量，并利用共识机制对区块链中的内部节点的身份进行认证，该方法保证了通信身份的匿名性，但嵌入信息量有限且难以抵抗隐写检测。

在利用神经网络模型传输隐蔽信息方面，现有方法主要集中于利用神经网络模型生成载体并嵌入隐蔽信息，但多数方案面临隐写检测攻击且信息嵌入容量较小。针对传统信息隐藏方法隐藏容量低、抗隐写分析能力弱等问题，张祯等人[19]提出一种基于文本无载体的隐藏方法，通过词语相似度计算方法选择同义词，并将该同义词嵌入不同的文本载体，该方法能够在隐藏信息的同时保持文本的语义连贯，但数据库的开销问题尚未解决。针对传统载体图像易被提取特征造成信息泄露等问题，Duan等人[20]提出一种基于卷积神经网络U-Net结构的隐写术方案，将秘密图像嵌入一张全尺寸图像，同时利用U-Net卷积神经网络判别载体是否嵌密，该方法能够提高隐蔽信息的嵌入容量，但载密图像易受到隐写检测攻击。针对图像嵌入率低的问题，Lu等人[21]提出一种用于图像隐写的大容量可逆隐写网络，引入单个可逆网络的前向和后向传播来进行隐蔽信息的嵌入和提取，该方法能够提高隐蔽信息嵌入和提取的效率，但图像存在有损压缩的问题。针对高频信息嵌入至低分辨率图像易丢失的问题，Guo等人[22]提出一种用于单图像隐写的缩放网络，缩放网络由编码器和解码器组成，编码器负责提取图像的特征表示，解码器负责将隐藏的秘密信息从特征表示中提取，该方法通过缩放网络能够准确识别图像的嵌入位置，但很难保证输出高质量的载密图像。针对GAN中生成图像质量差及抗隐写能力弱等问题，Song等人[23]提出一种基于隐写分析网络的对抗隐藏方法，通过将隐写分析器与GAN中的编码器结合，同时学习图像数据集样本和载密图像样本的特征，生成抗隐写能力强的载体图像，该方法能通过编码器生成合适的载体，但难以嵌入大量隐蔽信息。

3　隐蔽通信方案构造

本文提出一种基于图像多重隐写的区块链隐蔽通信方案，总体流程如图1所示。本方案的实体包括

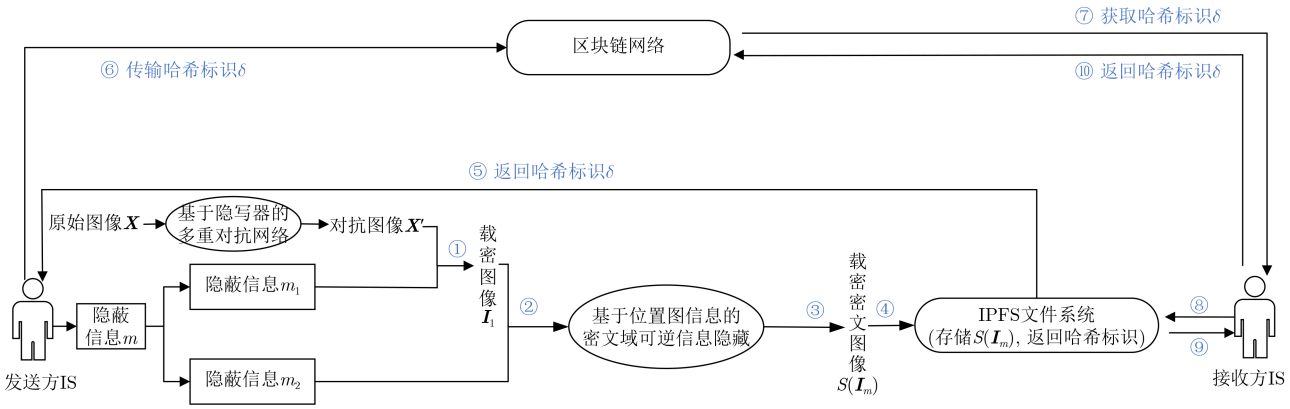

图 1 方案总体流程图

信息发送方、信息接收方以及区块链上的其它用户节点，以及区块链网络等，涉及到的图像及经处理后的图像均为灰度图像。在进行信息处理及传输前，发送方和接收方已协商好通信过程使用的嵌入方法、图像加密密钥和实体公钥等，需发送的隐蔽信息m分成m_1和m_2；首先，发送方将m_1隐写到基于隐写器的多重对抗网络的输出对抗图像$\boldsymbol{X}'$中，生成载密图像$\boldsymbol{I}_1$；其次，利用基于位置图信息的密文域可逆信息隐藏算法将隐蔽信息m_2嵌入至$\boldsymbol{I}_1$，生成载密密文图像$S(\boldsymbol{I}_m)$；随后，将$S(\boldsymbol{I}_m)$存储至IPFS文件系统，返回唯一的哈希标识δ，然后将δ存储到区块链网络中；最后，接收方从区块链交易信息获取δ，并将δ作为IPFS的输入，获取$S(\boldsymbol{I}_m)$。本文使用的具体符号变量如表1所示。

表 1 符号变量表

符号	描述
IS	信息发送方
IR	信息接收方
m_1	部分隐蔽信息
m_2	剩余隐蔽信息
m	隐蔽信息($m=m_1+m_2$)
$\boldsymbol{X}$	原始图像
$\boldsymbol{X}_{\mathrm{V}}$	对抗图像样本
$\boldsymbol{X}_{\mathrm{VM}}$	对抗隐写图像
$\boldsymbol{I}$	载体图像
$\boldsymbol{I}_1$	载密图像
$\boldsymbol{I}_e$	加密图像
$\boldsymbol{I}_{\mathrm{LM}}$	含位置图信息的加密图像
$\mathrm{IR}_{\mathrm{pub}}$	接收方公钥
$\mathrm{IR}_{\mathrm{pri}}$	接收方私钥
e	图像加密密钥(对称密钥)
$S(\boldsymbol{I}_m)$	载密密文图像
δ	IPFS返回的唯一哈希标识

3.1 基于隐写器的多重对抗网络构造

基于隐写器的多重对抗网络由4个模块组成，分别是生成器G、判别器D、隐写器SG和隐写对抗网络SDN。方案构造如图2所示，本文设计的多重对抗网络分为训练过程和嵌入过程，对抗网络的

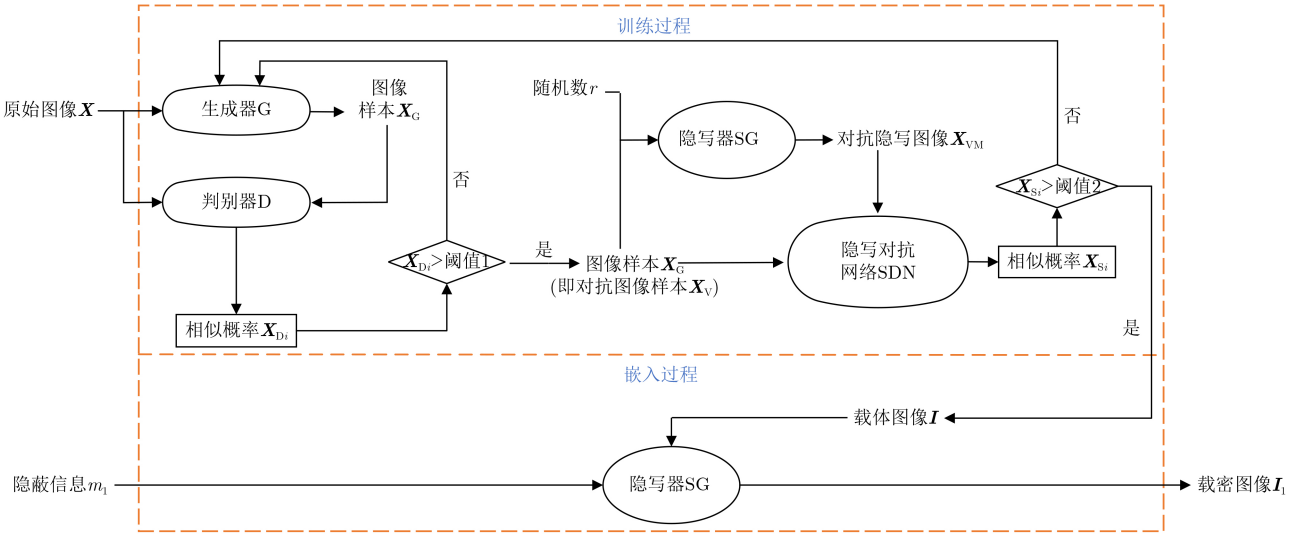

图 2 基于隐写器的多重对抗网络模型

输入为原始图像$\boldsymbol{X}$、隐蔽信息m_1，输出为载密图像$\boldsymbol{I}_1$。

在训练过程中，首先，将原始图像$\boldsymbol{X}$作为G的输入，生成图像样本$\boldsymbol{X}_{\mathrm{G}}$，并将$\boldsymbol{X}_{\mathrm{G}}$作为D的输入，输出$\boldsymbol{X}$和$\boldsymbol{X}_{\mathrm{G}}$的相似概率$\boldsymbol{X}_{\mathrm{D}i}$，若$\boldsymbol{X}_{\mathrm{D}i}$≤阈值1，则通过G生成图像样本继续训练判别器，否则将G训练生成的图像样本作为对抗图像样本$\boldsymbol{X}_{\mathrm{V}}$进行输出，且判别器结束训练；在判别器训练结束后，将随机数生成器RNG生成的32位随机数r和$\boldsymbol{X}_{\mathrm{V}}$作为SG的输入，生成对抗隐写图像$\boldsymbol{X}_{\mathrm{VM}}$，并将$\boldsymbol{X}_{\mathrm{V}}$和$\boldsymbol{X}_{\mathrm{VM}}$作为SDN的输入，输出$\boldsymbol{X}_{\mathrm{V}}$和$\boldsymbol{X}_{\mathrm{VM}}$的相似概率$\boldsymbol{X}_{\mathrm{S}i}$，若$\boldsymbol{X}_{\mathrm{S}i}$≤阈值2，则通过G生成图像样本重新训练判别器和隐写对抗网络，直到$\boldsymbol{X}_{\mathrm{D}i}$＞阈值1且$\boldsymbol{X}_{\mathrm{S}i}$＞阈值2。否则将G训练生成的对抗图像样本$\boldsymbol{X}_{\mathrm{V}}$作为最终的载体图像$\boldsymbol{I}$输出。在嵌入过程中，将训练过程中生成的载体图像$\boldsymbol{I}$和隐蔽信息$m_1$作为SG的输入，生成载密图像$\boldsymbol{I}_1$。

3.1.1 生成器构造

本文设计的生成器G用于训练学习生成与原始图像分布相似的图像。针对扰动噪声z分布不均导致的图像质量与抗隐写分析能力下降问题，采用上下采样方法解决：上采样通过反卷积层结合下采样信息生成高逼真对抗图像样本；下采样利用卷积层与池化层提取原始图像$\boldsymbol{X}$的低级特征，获取全局与局部环境信息。

生成器包含下采样编码、扩展路径和输出层3部分，共16组数据处理单元。首先，下采样编码由前8组单元构成，每组包含步长为2的3×3卷积层、批归一化层(Batch Normalization, BN)和修正线性单元(Rectified Linear Unit, ReLU)激活函数，用于特征提取与图像处理；其次，扩展路径由第9～15组单元组成，每组包含步长为2的5×5反卷积层、BN层和ReLU激活函数，通过上采样实现特征重建；最后，第16组单元为输出层，负责生成最终图像样本。

生成器的训练过程如下：首先，从初始原始图像$\boldsymbol{X}$和服从高斯分布的扰动噪声z生成图像样本$\boldsymbol{X}_{\mathrm{G}}$，将其与原始图像$\boldsymbol{X}$输入判别器D计算损失函数$L_{\mathrm{D}}$。当判别器无法区分$\boldsymbol{X}$与$\boldsymbol{X}_{\mathrm{G}}$时，将$\boldsymbol{X}_{\mathrm{G}}$作为对抗图像样本$\boldsymbol{X}_{\mathrm{V}}$输出，否则重复上述步骤；随后，将$\boldsymbol{X}_{\mathrm{V}}$与隐写器生成的对抗隐写图像$\boldsymbol{X}_{\mathrm{VM}}$输入隐写对抗网络SDN，计算损失函数$L_{\mathrm{SDN}}$，并根据式(1)计算生成器联合损失函数$L_{\mathrm{G}}$，通过反向传播[5]优化生成器参数。当判别器输出$\boldsymbol{X}$和$\boldsymbol{X}_{\mathrm{V}}$的相似概率$\boldsymbol{X}_{\mathrm{D}i}$＞阈值1且隐写对抗网络输出$\boldsymbol{X}_{\mathrm{V}}$和$\boldsymbol{X}_{\mathrm{VM}}$的相似概率$\boldsymbol{X}_{\mathrm{S}i}$＞阈值2时，表明$\boldsymbol{X}_{\mathrm{VM}}$无法被检测到含有秘密信息，此时$\boldsymbol{X}_{\mathrm{V}}$作为最终载体图像；否则重复训练过程

$$L_{\mathrm{G}}=\begin{cases}0, & i=0\\ -\alpha\cdot L_{\mathrm{D}}-\beta\cdot L_{\mathrm{SDN}}, & i\geq 1\end{cases} \tag{1}$$

其中，α,β为动态选择的权值参数，L_{D}为判别器损失，L_{SDN}为隐写对抗网络损失，i为当前训练迭代轮数。

3.1.2 判别器构造

本文设计的判别器D用于通过学习原始图像的分布来区分原始图像和图像样本，使得生成器G能生成适合信息嵌入的高质量对抗图像样本。由于传统判别器采用交叉熵损失函数易导致对异常样本过度敏感，故本文使用最小二乘损失函数，并在模型中引入归一化层BN，通过最大化原始图像与对抗样本间的差异来优化判别器训练。

判别器包含卷积特征提取和全连接层两部分。首先，在卷积特征提取部分，原始图像$\boldsymbol{X}$和生成图像$\boldsymbol{X}_{\mathrm{G}}$作为输入，由前8组数据处理单元进行特征提取，每组包含步长为3的3×3卷积层、批归一化层(BN)和泄漏修正线性单元(Leaky Rectified Linear Unit, Leaky-ReLU)激活函数。卷积层通过卷积操作捕捉局部特征，批归一化层增强模型鲁棒性，Leaky-ReLU通过引入负斜率解决神经元负载问题，处理后的数据传递至全连接层。然后，全连接层接收卷积特征输出，将特征映射到隐层节点，并通过Sigmoid激活函数输出0～1的概率值，用于判别输入图像的相似性。

判别器的训练过程如下：将原始图像$\boldsymbol{X}$和生成器生成的图像样本$\boldsymbol{X}_{\mathrm{G}}$输入判别器D，输出两者的相似概率，并根据式(2)计算损失函数L_{D}，通过反向传播[10]优化判别器参数以最小化L_{D}。当判别器输出$\boldsymbol{X}$和$\boldsymbol{X}_{\mathrm{G}}$的相似概率$\boldsymbol{X}_{\mathrm{D}i}$＞阈值1时，表明无法区分$\boldsymbol{X}$与对$\boldsymbol{X}_{\mathrm{G}}$，训练完成；否则重复上述过程

$$L_{\mathrm{D}}=-\sum_{i=1}^{2}\boldsymbol{x}_i'\ln(\boldsymbol{x}_i) \tag{2}$$

其中，$\boldsymbol{x}_1$, $\boldsymbol{x}_2$分别是原始图像和图像样本经判别器D本轮迭代输出的图像相似概率，$\boldsymbol{x}_1'$, $\boldsymbol{x}_2'$分别是原始图像和图像样本经判别器D上一轮迭代输出的图像相似概率。

3.1.3 隐写对抗网络构造

针对对抗图像样本$\boldsymbol{X}_{\mathrm{V}}$抗隐写分析检测能力低的问题，本文引入隐写对抗网络SDN，用于区分对抗图像样本$\boldsymbol{X}_{\mathrm{V}}$和对抗隐写图像$\boldsymbol{X}_{\mathrm{VM}}$，同时将隐写对抗网络SDN的损失函数记录为$L_{\mathrm{SDN}}$，并将$L_{\mathrm{SDN}}$作为生成器G损失函数的组成部分，使得生成器G生成更适合隐写的载体图像。本文选择SR-Net+Zhu-Net[10]作为隐写对抗网络SDN，并使用

SDN的损失函数进行优化，作为生成器损失的一部分。

隐写对抗网络的训练过程如下：将$\boldsymbol{X}_{\mathrm{V}}$和$\boldsymbol{X}_{\mathrm{VM}}$输入隐写对抗网络SDN，输出相似概率，并根据式(3)计算损失函数L_{SDN}，通过反向传播[5]优化网络参数以最小化L_{SDN}。当输出$\boldsymbol{X}_{\mathrm{V}}$和$\boldsymbol{X}_{\mathrm{VM}}$的相似概率$\boldsymbol{X}_{\mathrm{S}i}$>阈值2时，表明无法检测对抗隐写图像中的秘密信息，训练完成；否则，生成器重新生成图像样本并重复训练过程

$$L_{\mathrm{SDN}}=-\sum_{i=1}^{2}\boldsymbol{z}_i'\lg(\boldsymbol{z}_i) \tag{3}$$

其中，$\boldsymbol{z}_1$, $\boldsymbol{z}_2$分别是对抗图像样本和对抗隐写图像经隐写对抗网络SDN本轮迭代输出的图像相似概率，$\boldsymbol{z}_1'$, $\boldsymbol{z}_2'$分别是对抗图像样本和对抗隐写图像经隐写对抗网络SDN上一轮迭代输出的图像相似概率。

3.1.4 隐写器构造

针对生成对抗网络面临的隐写检测攻击问题，本文在多重对抗网络训练和嵌入的过程中引入隐写器，以生成不失真且抗检测的载体图像。

设图像载体$\boldsymbol{P}$大小为$n_1\times n_2$，$\boldsymbol{P}(i,j)$表示$\boldsymbol{P}$的所有像素，嵌入数据m_1后生成含密载体$\boldsymbol{P}_{m_1}$，该隐写器的嵌入步骤如下：

(1)计算图像载体$\boldsymbol{P}$水平方向、垂直、对角线方向的方向滤波器$\boldsymbol{K}^{(1)}$, $\boldsymbol{K}^{(2)}$, $\boldsymbol{K}^{(3)}$

$$\boldsymbol{K}^{(1)}=\boldsymbol{h}\cdot\boldsymbol{g}^{\mathrm{T}},\boldsymbol{K}^{(2)}=\boldsymbol{g}\cdot\boldsymbol{h}^{\mathrm{T}},\boldsymbol{K}^{(3)}=\boldsymbol{g}\cdot\boldsymbol{g}^{\mathrm{T}} \tag{4}$$

其中，$\boldsymbol{h}$为1维小波分解高通滤波器矩阵，$\boldsymbol{g}$为固定滤波器矩阵。

(2)计算图像载体$\boldsymbol{P}$的每个像素在这3个方向上的滤波变换

$$\boldsymbol{W}_{ij}^{(k)}=\boldsymbol{K}^{(k)}*\boldsymbol{P}(i,j),1\le i\le n_1,1\le j\le n_2,\quad 1\le k\le 3 \tag{5}$$

其中$*$表示卷积操作，图像载体$\boldsymbol{P}$经滤波变换后用$\boldsymbol{W}_{ij}^{(k)}(\boldsymbol{P})=(\boldsymbol{P}_1,\boldsymbol{P}_2,\cdots,\boldsymbol{P}_{n_1\times n_2})\in\{0,1\}^{n_1\times n_2}$表示。

(3)假设嵌入数据m_1后生成含密载体$\boldsymbol{P}_{m_1}$，$\boldsymbol{P}_{m_1}$经滤波变换后用$\boldsymbol{W}_{ij}^{(k)}(\boldsymbol{P}_{m_1})=(\boldsymbol{I}_1,I_2,\cdots,\boldsymbol{I}_{n_1\times n_2})\in\{0,1\}^{n_1\times n_2}$表示，那么该图像载体$\boldsymbol{P}$和含密载体$\boldsymbol{P}_{m_1}$的总体嵌入失真可表示为

$$D(\boldsymbol{W}_{ij}^{(k)}(\boldsymbol{P}),\boldsymbol{W}_{ij}^{(k)}(\boldsymbol{P}_{m_1}))=\sum_{k=1}^{3}\sum_{i=1}^{n_1}\sum_{j=1}^{n_2}\frac{|\boldsymbol{W}_{ij}^{(k)}(\boldsymbol{P})-\boldsymbol{W}_{ij}^{(k)}(\boldsymbol{P}_{m_1})|}{\sigma+|\boldsymbol{W}_{ij}^{(k)}(\boldsymbol{P})|} \tag{6}$$

(4)利用式(7)减少待隐藏的数据量(避免数据量过大引起图像失真)，求出使得总体嵌入失真$D(\boldsymbol{W}_{ij}^{(k)}(\boldsymbol{P}),\boldsymbol{W}_{ij}^{(k)}(\boldsymbol{P}_{m_1}))$最小的$\boldsymbol{W}_{ij}^{(k)}(\boldsymbol{P}_{m_1})$

$$\boldsymbol{W}_{ij}^{(k)}(\boldsymbol{P}_{m_1})=m_1\otimes\boldsymbol{H} \tag{7}$$

其中，$\otimes$为基于STC的滤波编码[12]操作；$\boldsymbol{H}$为校验矩阵(包含h行w列)；校验矩阵的宽度w与信息嵌入率α有关，选择$w=1/\alpha$；校验矩阵的长度h的取值为8。

(5)对$\boldsymbol{W}_{ij}^{(k)}(\boldsymbol{P}_{m_1})$进行逆滤波变换，得到中间图像$\boldsymbol{P}_{m_1}'$

$$\boldsymbol{P}_{m_1}'(i,j)=\boldsymbol{W}_{ij}^{(k)}(\boldsymbol{P}_{m_1})(/*)\boldsymbol{K}^{(k)} \tag{8}$$

其中$/*$为反卷积操作。

(6)将m_1的二进制序列B_{m_1}(每8位二进制组成一个十进制像素值$p_{m_1}(i,j)$)嵌入至中间图像$\boldsymbol{P}_{m_1}'(i,j)$中像素值为0的像素位置，生成含密载体$\boldsymbol{P}_{m_1}$，嵌入过程为

$$p(i,j)=\begin{cases}p(i,j), & p(i,j)\ne 0\\ p_{m_1}(i,j), & p(i,j)=0\end{cases} \tag{9}$$

其中$p(i,j)$为中间图像$\boldsymbol{P}_{m_1}'$的像素。

3.2 基于位置图信息的密文域可逆信息隐藏

基于位置图信息的密文域可逆信息隐藏如图3所示。首先，载密图像$\boldsymbol{I}_1$经像素预测模块生成预测图像$\boldsymbol{I}_1'$；其次，标记$\boldsymbol{I}_1$和$\boldsymbol{I}_1'$像素的相同比特位置，通过概率分布计算哈夫曼编码，生成位置图信息LM；随后，通过图像加密模块对预测图像$\boldsymbol{I}_1'$进行加密，生成加密图像$\boldsymbol{I}_e$；并将LM隐藏至$\boldsymbol{I}_e$的像素空间，生成含位置图信息的加密图像$\boldsymbol{I}_{\mathrm{LM}}$；最后，将隐蔽信息$m_2$隐藏至$\boldsymbol{I}_{\mathrm{LM}}$剩余的像素空间，生成载密密文图像$S(\boldsymbol{I}_m)$。

本文利用预测图像和载体图像中标记值的概率分布分配不同的编码序列，生成位置图信息并采用

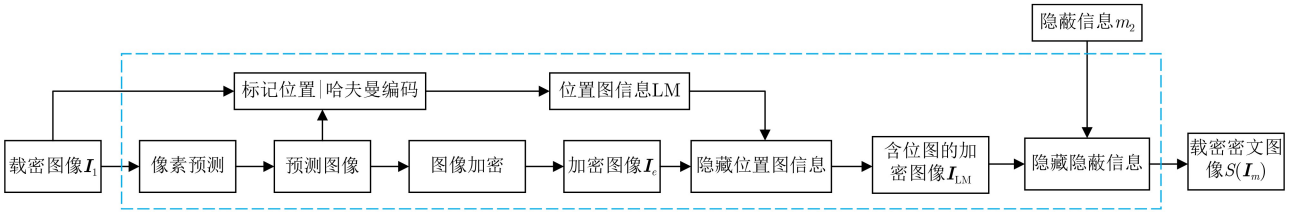

图 3 基于位置图信息的密文域可逆信息隐藏

自适应编码压缩位置图信息，与剩余隐蔽信息m_2记录至加密图像的像素空间，提高了信息的嵌入率。

3.2.1 像素预测

生成预测图像$\boldsymbol{I}_1^{'}$。将载密图像$\boldsymbol{I}_1$像素的第1行和第1列像素作为固定像素(像素值保持不变)，其它非固定像素经式(10)进行像素预测得到预测像素值，进而生成预测图像$\boldsymbol{I}_1^{'}$

$$\widehat{p}=\begin{cases}\min(a,b), & c\geq\max(a,b)\\ \max(a,b), & c\leq\min(a,b)\\ a+b-c, & \text{其他}\end{cases}\tag{10}$$

其中，非固定像素p经像素预测成$\widehat{p}$，a为像素p左相邻像素原始值，b为像素p上边相邻像素原始值，c为像素b左相邻像素原始值。

3.2.2 标记位置

(1)获取标记位置值：将载密图像$\boldsymbol{I}_1$和预测图像$\boldsymbol{I}_1^{'}$对应的非固定像素转为8位二进制表示，如式(11)所示，从最高有效位到最低有效位逐一比较直到某比特位不同，相同的比特位数即为该像素的标记位置值，固定像素的像素值定为–1

$$\boldsymbol{I}_{(1)}^{k}(i,j)=\left\lfloor \boldsymbol{I}_{(1)}(i,j)/2^{k-1}\right\rfloor \bmod 2,k=1,2,\cdots,8\tag{11}$$

其中，$\boldsymbol{I}_{(1)}(i,j)$表示载密图像$\boldsymbol{I}_1$及预测图像$\boldsymbol{I}_1^{'}$的十进制表示，$\boldsymbol{I}_{(1)}^{k}(i,j)$表示$\boldsymbol{I}_1$和$\boldsymbol{I}_1^{'}$的8位二进制表示。

(2)生成哈夫曼编码序列L_{bs}：在求出所有像素标记位置值后，统计每一个位置值出现的概率，构造哈夫曼树，根据左0右1的规则求出每个位置值对应的编码，编码序列对应的编码序列L_{bs}为

$$L_{\text{bs}}=\sum_{t=0}^{8}(g_t\times\lambda_t)\tag{12}$$

其中，g_t表示标记位置值的个数，λ_t表示标记位置值对应的编码长度。以8×8图像像素标记值为例，表2给出了对应的概率分布及编码序列。

3.2.3 生成位置图信息LM

在生成哈夫曼编码序列L_{bs}后，需要生成位置图信息，该位置图信息的作用是还原载密图像$\boldsymbol{I}_1$。位置图信息LM由编码序列L_{bs}和附加信息组成，附加信息包括位置值对应编码长度的二进制表示C、编码序列与标记位置值的对应关系H、载密图像$\boldsymbol{I}_1$中固定像素的二进制表示$B(p^{'})$、除L_{bs}的位置图长度的二进制表示$B(\text{Len})$，位置图信息组成如图4所示。

表 2　像素标记值对应的编码序列

像素标记值	个数统计	概率分布	编码长度	编码序列
2	2	0.040 8	4	0010
3	11	0.224 5	2	01
5	3	0.061 2	3	000
6	31	0.632 7	1	1
8	2	0.040 8	4	0011

3.2.4 图像加密

预测图像$\boldsymbol{I}_1^{'}$加密。利用随机数生成器(Random Number Generator, RNG)生成与图像加密密钥e长度相同的随机数，并将该随机数以$\boldsymbol{I}_1^{'}$的维度大小转化为矩阵$\boldsymbol{R}$(若e长度为n bit，则将随机数分为$n/8$个字节，并将其排列为$n/8$行的矩阵)，通过矩阵$\boldsymbol{R}$对$\boldsymbol{I}_1^{'}$各个位置的像素值相互进行异或操作，得到加密图像$\boldsymbol{I}_e$，如式(13)所示

$$\boldsymbol{I}_e^{k}(i,j)=\boldsymbol{I}^{k}(i,j)\oplus r^{k}(i,j),k=1,2,\cdots,8\tag{13}$$

其中，$\boldsymbol{I}_e^{k}(i,j)$为预测图像$\boldsymbol{I}_1^{'}$的二进制形式；$r^{k}(i,j)$为矩阵$\boldsymbol{R}$中元素的二进制表示；$\oplus$为异或操作。

3.2.5 位置图信息隐藏

隐藏位置图信息至加密图像$\boldsymbol{I}_e$。在加密图像$\boldsymbol{I}_e$中选取第1行和第1列作为固定像素，将位置图信息LM中标记位置值对应编码长度的二进制表示C、编码序列与位置值的关系编码H、载密图像$\boldsymbol{I}_1$中固定像素的二进制表示$B(p^{'})$、除L_{bs}的位置图长度的二进制表示$B(\text{Len})$记录到固定像素中，生成含位图的加密图像$\boldsymbol{I}_{\text{LM}}$，如式(14)所示

$$\begin{aligned}p_{kv}^{'}(i,j)\ &=p_{kv}(i,j)\text{^}(C\sim H\sim B(p^{'})\sim B(\text{Len})),\\ &k=1||v=1\end{aligned}\tag{14}$$

其中，k,v分别表示$\boldsymbol{I}_e$图像矩阵的行数和列数；^为替换操作；～为二进制累加操作；$p_{kv}(u,v)$为$\boldsymbol{I}_e$对应各个位置的像素值；$p_{kv}^{'}(u,v)$为替换后$\boldsymbol{I}_{\text{LM}}$对应各个位置的像素值。

3.2.6 隐蔽信息隐藏

在非固定像素中，将编码序列L_{bs}对应的每一个像素编码从左至右、从上至下依次嵌入至对应的非固定像素中，如式(15)所示

$$\boldsymbol{I}_e^{'}(i,j)=\begin{cases}\boldsymbol{I}_e(i,j)\ \bmod\ 2^{7-t}+\sum_{s=0}^{t}(b_s\times 2^{7-s}), & 0\leq t\leq 6\\ \sum_{s=1}^{8}(b_s\times 2^{8-s}), & 7\leq t\leq 8\end{cases},s=\begin{cases}t+1, & 0\leq t\leq 7\\ t, & t=8\end{cases}\tag{15}$$

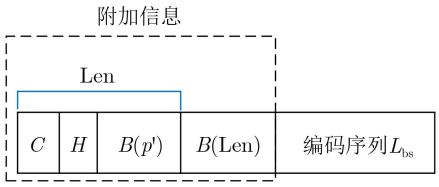

图 4 位置图信息组成

其中，$\boldsymbol{I}_e^{'}(i,j)$为载密密文图像$S(\boldsymbol{I}_m)$的像素值，$b_s$为编码序列对应$\boldsymbol{I}_{\mathrm{LM}}$像素的编码，$t$为标记位置值；当$t$小于等于7时，$\boldsymbol{I}_e$中的像素可嵌入$B(p^{'})$的空间为$t+1$位，否则没有隐藏空间。

在每个像素的额外空间上依次记录载密图像中固定像素的二进制表示$B(p^{'})$。当编码序列L_{bs}和$B(p^{'})$嵌入完成后，基于RSA非对称加密[4]对隐蔽信息m_2进行加密，如式(16)所示

$$e_m = \mathrm{Unicode}(m_2)^{\mathrm{IR_{pub}}} \bmod pq \tag{16}$$

其中，Unicode为编码方式；p和q为大素数；e_m为加密后的密文信息。

隐藏e_2至$\boldsymbol{I}_{\mathrm{LM}}$剩余的像素空间，生成最终的载密密文图像$S(\boldsymbol{I}_m)$，隐藏过程如式(17)所示

$$\boldsymbol{I}_{\mathrm{LM}}^{'}(i,j) = \boldsymbol{I}_{\mathrm{LM}}(i,j)\text{^}(e_m) \tag{17}$$

其中，^为替换操作；$\boldsymbol{I}_{\mathrm{LM}}(i,j)$ 为$\boldsymbol{I}_{\mathrm{LM}}$对应各个位置的像素值；$\boldsymbol{I}_{\mathrm{LM}}^{'}(i,j)$为替换后$S(\boldsymbol{I}_m)$对应各个位置的像素值。

3.3 隐蔽信息传输及提取

3.3.1 隐蔽信息传输

在通过智能合约上传数据至链上的过程中，将载密密文图像通过IPFS生成唯一标识δ；将δ和交易地址对应的字符进行映射，生成映射序列，最后将该序列嵌入至交易中，对交易及所在区块验证后上链存储。传输过程如图5所示。

(1)生成重复数字序列$\delta(c)$：δ的字符序列为$\delta<\delta_1,\delta_2,\cdots,\delta_n>$，字符索引序列为$\delta^{'}<J_1,J_2,\cdots,J_n>$；若$\delta$中出现重复字符$c$，那么重复数字序列$\delta(c)$可表示为式(18)

$$\delta(c)=\begin{cases}<c,(J_1,J_2,\cdots,J_k)>, & \delta_{J_1}=\delta_{J_2}=\cdots=\delta_{J_k}\\ <c,(J_1)>, & \delta_{J_1}\neq\delta_{J_2}\neq\cdots\neq\delta_{J_k}\end{cases} \tag{18}$$

其中，$J_1,J_2,\cdots,J_k$为$\delta_1,\delta_2,\cdots,\delta_k$中对应的数字索引序列。

(2)生成映射序列$J(\delta_1)$：发送方向区块链网络任一节点转账生成交易TX_1，TX_1的交易地址是随机产生的哈希序列$h<s_1,s_2,\cdots,s_m>$，h对应的索引序列为$h^{'}<x_1,x_2,\cdots,x_n>$。若$\delta^{'}(c)$中的字符$c$与哈希序列中的$c^{'}$字符相同，那么字符$c^{'}$对应的哈希索引为$x_c$，构造映射信息$J(c)$如式(19)所示

$$\begin{aligned}J(c)=&<x_c,(J_1,J_2,\cdots,J_k)>,\\ &\delta_{J_1}=\delta_{J_2}=\cdots=\delta_{J_k}=h_{x_c}\end{aligned} \tag{19}$$

其中，$\delta_{J_1},\delta_{J_2},\delta_{J_3}$ 为不同索引的相同字符。当所有用于构造$J(c)$的地址序列字符遍历完后，将得到需要上链的映射部分序列$J(\delta_1)$，将$J(\delta_1)$嵌入交易TX_1中的extraData信息中。

若此时δ的字符序列仍没完全嵌入，则发送方继续向区块链网络中的节点转账生成交易TX_2，进而生成映射部分序列$J(\delta_2)$，重复以上步骤，直到生成完整的映射序列$J(\delta)$。当区块链中其他节点验证生成交易后，由记账节点打包为区块并上链存储。

3.3.2 隐蔽信息提取

接收方提取隐蔽信息的过程可分为载密密文图像获取及隐蔽信息提取。

(1)载密密文图像获取：接收方首先从公开的区块中寻找来自发送方转账产生的交易$\mathrm{TX}_1,\mathrm{TX}_2,\cdots,\mathrm{TX}_n$，并从这些交易中的extraData信息映射序列获取$J(\delta)$；由于$J(\delta)$由该交易的哈希序列$h<s_1,s_2,\cdots,s_m>$、哈希索引序列为$h^{'}<x_1,x_2,\cdots,x_n>$及重复数字序列$\delta(c)$组成，接着

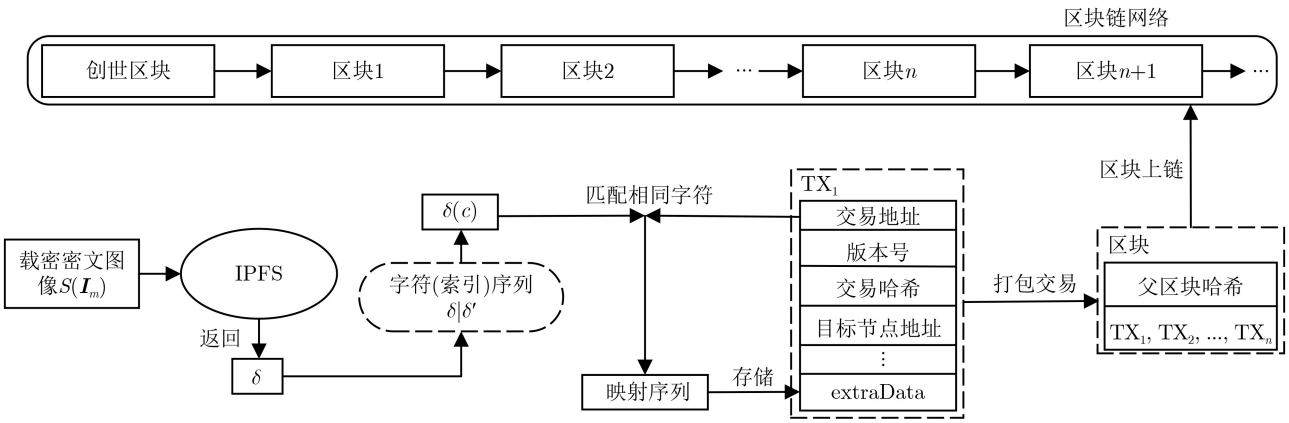

图 5 隐蔽信息传输过程

从$\delta(c)$中获取组成δ的相关字符序列，并根据$\delta(c)$和哈希索引序列h'按顺序进行组合，得到δ；最后，将δ作为IPFS文件系统的输入，获取载密密文图像$S(\boldsymbol{I}_m)$。

(2)隐蔽信息提取：接收方首先从$S(\boldsymbol{I}_m)$中第1行和第1列固定像素中获取位置图信息LM中位置值对应编码长度的二进制表示C、编码序列与位置值的对应关系H、位置图长度的二进制表示$B(\text{Len})$，接着从非固定像素中获取像素的编码序列、载密图像$\boldsymbol{I}_1$中固定像素的二进制表示$B(p')$以及密文信息e_m。利用式(20)对e_m解密，获取隐蔽信息m_2，同时将$B(p')$放回固定像素第1行和第1列，得到中间图像$\boldsymbol{I}_e'$

$$\delta = \text{DE\_Unicode}(\delta_e^{\text{IR}_{\text{pri}}} \bmod pq) \tag{20}$$

其中，DE_Unicode为反编码方式；p和q为大素数。

载密图像$\boldsymbol{I}_1$恢复的过程为：利用图像加密密钥e_1生成矩阵对中间图像$\boldsymbol{I}_e'$每一个像素进行异或操作，得到不含位置图信息的图像$\boldsymbol{I}''$。在图像$\boldsymbol{I}''$中每一个非固定像素的前t位或者$t+1$位与载密图像$\boldsymbol{I}_1$像素不同，若$t \le 7$，则载密图像$\boldsymbol{I}_1$像素值的$t+1$位与图像$\boldsymbol{I}''$像素值相反，载密图像$\boldsymbol{I}_1$像素值第$t+2$至第8位与图像$\boldsymbol{I}''$像素值相同，最终还原载密图像$\boldsymbol{I}_1$的非固定像素，得到载密图像$\boldsymbol{I}_1$，还原过程如式(21)所示

$$\boldsymbol{I}_1(i,j) = \begin{cases} \boldsymbol{I}''(i,j)^{\text{tMSE}} + (\boldsymbol{I}''(i,j)^{t+1} \oplus 1) \times 2^{7-t} + \boldsymbol{I}''(i,j) \bmod 2^{7-t}, & 0 \le t \le 7 \\ \boldsymbol{I}''(i,j), & t = 8 \end{cases} \tag{21}$$

其中，$\boldsymbol{I}''(i,j)^{\text{tMSE}}$表示图像$\boldsymbol{I}''$高$t$位的值，$\boldsymbol{I}''(i,j)^{t+1}$表示图像$I''$第$t+1$位的值，$\boldsymbol{I}''(i,j)^{t+1} \oplus 1$表示对图像$\boldsymbol{I}''$第$t+1$位的值做异或取反操作。

最后，在得到载密图像$\boldsymbol{I}_1$后，根据载密图像$\boldsymbol{I}_1$可以求出经滤波变换后的$W_{uv}^{(k)}(I_1)$，利用式(8)即可获取隐蔽信息m_1，进而提取完整的隐蔽信息m。

4　实验结果与分析

4.1　仿真实验设计

4.1.1　实验环境

本实验深度学习所使用的硬件环境为8核32G的云服务器，软件环境为conda；隐写算法所使用的软件环境为matlab 2021；区块链的仿真环境为CentOS 7系统，通过Geth搭建以太坊模拟区块链环境。

4.1.2　数据集和评价指标

(1)数据集：本文选用BOSSBase, BOWS-2数据集的10 000张灰度图像和UCID数据集的1 388张灰度图像作为实验数据，涵盖自然图像、人物图像及复杂图像等多种类型，以反映实际场景。训练集和验证集分别设置为9 000张和3 888张。隐写器嵌入率大小为0.5，同时设置生成器的学习率=0.000 05, beta_1=0.5, beta_2=0.99。

(2)评价指标：本文对抗隐写能力、隐蔽性和嵌入容量分析时，分别使用P_{E}、峰值信噪比(Peak Signal-to-Noise Ratio, PSNR)和结构相似性指数(Structural Similarity Index Measure, SSIM)、bpp作为评价指标。

(a)P_{E}：隐写检测正确率。$P_{\text{E}} = T_{\text{P}}/(T_{\text{P}}+F_{\text{P}})$，其中$T_{\text{P}}$为正确检测为对抗图像样本数，$F_{\text{P}}$为未检测为对抗图像样本数。若$P_{\text{E}}$越接近0.5，说明判别器难以区分对抗图像样本和对抗隐写图像，进一步说明抗隐写能力越强。

(b)PSNR：峰值信噪比$\text{PSNR} = 10\lg(255^2/\sum_{i=1}^{M}\sum_{j=1}^{N}(\boldsymbol{I}(i,j)-\boldsymbol{I}'(i,j))^2/(M\times N))$，其中$\boldsymbol{I}(i,j)$与$\boldsymbol{I}'(i,j)$分别为两个比较图像的像素，$M \times N$为图像的分辨率。当PSNR高于40 dB时，说明加工后的图像质量极好，非常接近原始图像。

(c)SSIM：结构相似度$\text{SSIM}(\boldsymbol{I},\boldsymbol{I}') = (2\mu_{\boldsymbol{I}}\mu_{\boldsymbol{I}'} + c_1)(2\sigma_{\boldsymbol{I}\boldsymbol{I}'} + c_2)/(\mu_{\boldsymbol{I}}^2 + \mu_{\boldsymbol{I}'}^2 + c_1)(\sigma_{\boldsymbol{I}}^2 + \sigma_{\boldsymbol{I}'}^2 + c_2)$，其中$\mu_{\boldsymbol{I}}$和$\mu_{\boldsymbol{I}'}$分别为图像$\mu_{\boldsymbol{I}}$和图像$\mu_{\boldsymbol{I}'}$与高斯核匹配的平均值，$\sigma_{\boldsymbol{I}}$和$\sigma_{\boldsymbol{I}'}$分别为两图像匹配的方差，$\sigma_{\boldsymbol{I}\boldsymbol{I}'}$为两图像的协方差，$c_1$和$c_2$则为常数。当SSIM的值为1时，表示加工后的图像与原始图像完全相同；SSIM值越小，表明加工后的图像与原始图像的相似度越低。

(d)bpp：嵌入率bpp=嵌入的总比特数/图像像素总数。当嵌入率越高，则图像能嵌入的信息越多。

4.2　结果分析

为验证方案的有效性，从抗隐写能力、隐蔽性、嵌入容量、通信时延四个方面对实验结果进行分析。

4.2.1　抗隐写分析

图6展示了判别器损失函数值随迭代次数的变化。当迭代次数小于等于4 500时，损失值为负，表明假图像分布较多；当迭代次数约4 600时，真图像分布逐渐增多；当迭代次数约8 000时，损失值趋近于0，表明真假图像分布趋于均衡，判别模型难以区分。

表3显示了消融实验结果，隐写图像检测表示隐写分析优化网络识别隐写图像的准确率，对抗样本隐写检测表示隐写对抗网络识别对抗样本隐写图

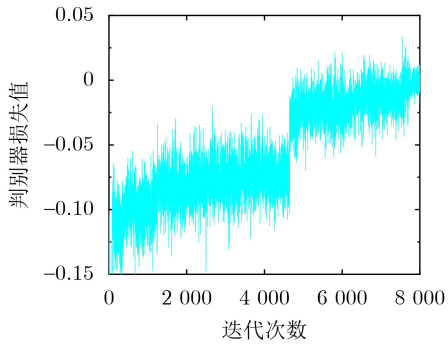

图 6 判别器损失变化

像的准确率，最优结果应为0.5，表明隐写对抗网络无法区分载体图像是否为隐写图像；同时，对抗样本隐写检测结果表明本文方案能够抵抗图像篡改和压缩攻击。当对抗样本$\boldsymbol{X}_{\mathrm{V}}$隐写检测和隐写图像$\boldsymbol{X}_{\mathrm{VM}}$检测概率越低，那么生成载体图像$\boldsymbol{I}$的安全性更高。综上，选择SRNet与Zhu-Net进行训练，可实现隐写安全和图像质量之间的平衡。

针对生成器总损失，表4展示了不同α和β设置下，最优的PSNR与SSIM值以及4种隐写分析网络的分类准确率。由表4可知，当$\alpha=0.1$，$\beta=0.9$时，生成载体图像的PSNR为39.123 6、SSIM为0.963 0，4种隐写分析网络的准确率分别达到49.3%, 50.3%, 50.2%和49.6%，此时生成载体图像质量最优，且抗隐写分析能力也较强。综上所述，本文生成器总损失选择的参数分别为$\alpha=0.1$, $\beta=0.9$。

本文分别测试多重对抗网络使用的隐写器、基于小波变换的权重隐写算法(Wavelet Obtained Weights, WOW)算法和高通-低通-低通滤波隐写算法(HIgh-pass, Low-pass, and Low-pass, HILL)算法的抗隐写能力，将嵌入率设置为0.1～0.5 bpp。为了评估抗隐写分析指标，选择测试集的总分类错误概率P_{E}，测试结果如图7所示。随着嵌入率的不断增加，误差概率越来越小，判别器模型则以较高置信度正确判别隐写图像，同时本文隐写器相比WOW算法和HILL算法更能以较高置信度错误判别隐写图像，说明有着更强的抗隐写分析能力。

4.2.2 隐蔽性分析

表5、表6、表7分别给出了Scenry, Building, Lena, Steamship和Cat 5张图像中的载密图像与加密图像、载密图像与载密密文图像、载密密文图像与还原后的载密图像的PSNR, SSIM值。其中载密图像与加密图像、载密密文图像的PSNR值都非常低，而SSIM值接近0；原始图像与还原后载密图像的PSNR值接近无穷，SSIM值为1。

以上实验数据表明，基于位置图和空域的密文域可逆数据隐藏方法隐蔽性高，能有效保护图像内容并实现无损恢复。

4.2.3 嵌入容量分析

本文隐写器针对Scenry图像最终实现了每像素平均嵌入0.5 bpp的比特数，总计可嵌入131 072 bit信息。表8展示了文献[24]对Scenry图像的编码过程，而表9呈现了本文隐藏方法对Scenry图像的编码过程。由两表对比分析可知，本文方案的图像净嵌入容量高于文献[24]。

在图8中，针对5张对抗网络生成的测试图像进行分析，比较了本文提出的隐写算法与其他隐写算法的最大嵌入率。实验结果表明，当测试Lena图像时，本文算法的最大嵌入率约为2.617 bpp，略低

表 3 隐写分析对抗网络消融实验结果

隐写分析对抗网络	平均PSNR (dB)	平均SSIM	对抗样本隐写检测(%)	隐写图像检测(%)	训练时间(min)
SRNet	45.325	0.979 2	52.3	88.9	962
Xu-Net	46.296	0.982 3	48.6	89.6	1 038
Zhu-Net+Xu-Net	42.539	0.956 3	51.2	87.8	1 369
SRNet+Zhu-Net+Xu-Net	39.689	0.862 4	49.6	86.4	1 738
Zhu-Net	44.569	0.991 4	51.4	89.2	965
SRNet+Zhu-Net	43.647	0.963 2	50.3	86.3	1 345

表 4 判别器和隐写对抗网络损失权重对比

隐写对抗损失权重组合	平均PSNR (dB)	平均SSIM	SRNet (%)	Xu-Net (%)	Zhu-Net (%)	Ye-Net (%)
$\alpha=0.6,\beta=0.4$	38.637 9	0.954 8	50.6	50.1	50.1	49.7
$\alpha=0.3,\beta=0.7$	39.107 5	0.961 9	50.2	49.6	49.3	50.2
$\alpha=0.1,\beta=0.9$	39.123 6	0.963 0	49.3	50.3	50.2	49.6
$\alpha=0.2,\beta=0.8$	39.123 6	0.961 3	50.3	49.7	50.4	50.3
$\alpha=0.5,\beta=0.5$	38.864 7	0.954 7	49.3	50.6	50.1	50.8

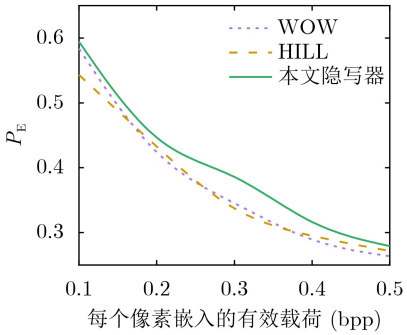

图 7 不同对抗网络隐写器判别误差变化

表 6　载密图像与载密密文图像的PSNR和SSIM值

载密图像/载密密文图像	PSNR (dB)	SSIM
Scenry	7.813 3	0.059 2
Building	8.117 3	0.056 6
Lena	10.078 8	0.021 2
Steamship	7.256 4	0.053 1
Cat	8.330 4	0.058 3

表 5　载密图像与加密图像的PSNR和SSIM值

载密图像/加密图像	PSNR (dB)	SSIM
Scenry	7.782 2	0.055 4
Building	8.670 3	0.060 0
Lena	10.072 9	0.021 9
Steamship	7.321 3	0.052 0
Cat	8.375 7	0.056 7

表 7　载密图像与还原后载密图像的PSNR和SSIM值

载密图像/还原后的载密图像	PSNR (dB)	SSIM
Scenry	$+\infty$	1
Building	$+\infty$	1
Lena	$+\infty$	1
Steamship	$+\infty$	1
Cat	$+\infty$	1

表 8　针对Scenry图像文献[24]的编码过程

标记值	标记值个数	概率分布	编码序列	嵌入容量	编码序列长度	净嵌入容量
–1	985	–	–	–	–	–
0	9 736	0.043	11010	1	5	–4
1	13 082	0.058	1100	2	4	–2
2	10 093	0.045	11011	3	5	–2
3	27 952	0.125	100	4	3	1
4	26 893	0.121	011	5	3	2
5	44 509	0.198	00	6	2	4
6	30 836	0.137	101	7	3	4
7	36 437	0.162	111	8	3	5
8	24 963	0.111	010	8	3	4
合计	224 501	1.000	–	1 286 558	706 697	579 861

表 9　针对Scenry图像本文隐藏方法的编码过程

标记值	标记值个数	概率分布	编码序列	嵌入容量	编码序列长度	净嵌入容量
–1	985	–	–	–	–	–
0	9736	0.043	0100	1	4	–3
1	14 823	0.066	1110	2	4	–2
2	13 693	0.062	0101	3	4	–1
3	25 961	0.116	011	4	3	1
4	28 469	0.126	100	5	3	2
5	43 259	0.192	00	6	2	4
6	30 836	0.138	101	7	3	4
7	35 123	0.156	110	8	3	5
8	22 601	0.101	1111	8	4	4
合计	224 501	1	–	1 263 848	691 097	572 751(+131 072)

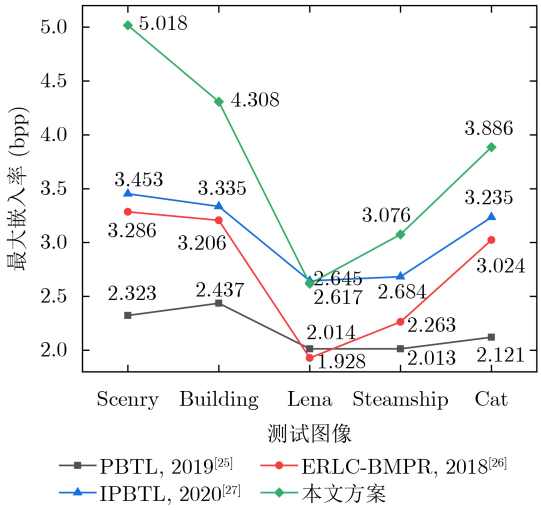

图 8 不同隐写算法在测试图像的最大嵌入率

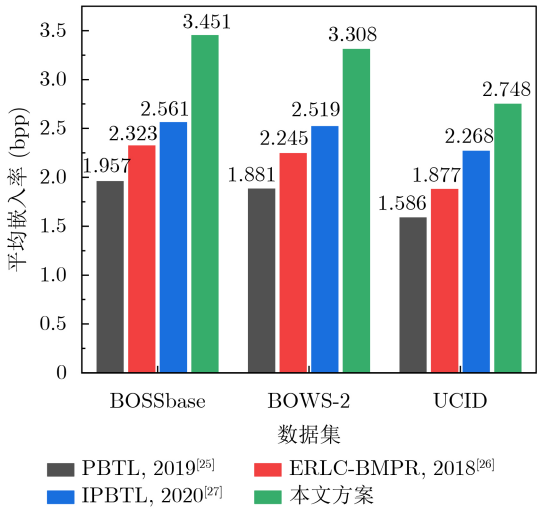

图 9 不同隐写算法在3种数据集的平均嵌入率

于文献[27]中的最大嵌入率2.645 bpp；当测试其他图像时，与其他同类算法相比，本文算法均展现出较高的最大嵌入率。

在图9中，针对BOSSbase, BOWS-2和UCID 3种图像数据集进行分析，BOSSbase因其灰度处理及未压缩格式的高质量图像，嵌入率高于其他数据集。同时，将本文提出的隐写算法与其它算法的平均嵌入率进行对比，实验结果表明，本文算法在这3种数据集上分别达到了3.451 bpp, 3.308 bpp和2.748 bpp的平均嵌入率，明显高于文献[25]、文献[26]和文献[27]算法的平均嵌入率，进一步说明本文算法具有更高的平均嵌入率。

4.2.4 通信时延分析

图10分析了传输100～500长度隐蔽信息的通信时延，并与其他方案对比。随着隐蔽消息长度增加，文献[28]、文献[29]和文献[30]中的通信时延都是先增加后趋于稳定，而本文方案相较于这些文献显示出了更低的通信时延。本文方案的通信时延在1 000～1 200 s之间浮动，隐蔽消息长度为300时达到最低时延，由于隐蔽消息经过IPFS处理后得到的字符串可能存在相同的字符比较多，采用字符匹配的方法可以识别并去除重复的数据进而减少了区块的使用，降低了通信时延。这是由于本文所提方案中，通信传输的数据是经IPFS处理后的固定长度标识，交易存储的也是长度相同标识的字符索引。因此，不论隐蔽消息长度如何变化，通信时延都会在固定的区间浮动。

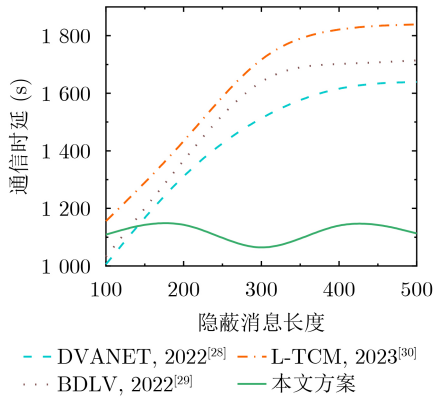

图 10 不同通信方案的通信时延对比

5 结束语

本文提出了一种基于图像多重隐写嵌入的区块链隐蔽通信方案，使用多重对抗网络生成高质量且具有抗隐写检测能力的载密图像；此外，采用基于位置图信息的密文域可逆信息隐藏方法将隐蔽信息嵌入载密图像，提高了隐蔽信息的嵌入率；最后，利用IPFS和加密签名算法将载密密文图像通过区块链网络传输，减少信息传输开销的同时保证了隐蔽信息不被恶意获取。实验表明，该方案在抗隐写分析、隐蔽性、嵌入率和通信时延方面表现优异。未来研究将引入同态加密与身份认证机制，确保仅授权用户可解密访问隐蔽信息，进一步提升安全性。

参 考 文 献

[1] ZHENG Tongxing, WANG Huiming, NG D W K, *et al*. Multi-antenna covert communications in random wireless networks[J]. *IEEE Transactions on Wireless Communications*, 2019, 18(3): 1974–1987. doi: 10.1109/TWC.2019.2900915.

[2] HU Jinsong, LI Hongwei, CHEN Youjia, *et al*. Covert communication in cognitive radio networks with poisson distributed jammers[J]. *IEEE Transactions on Wireless Communications*, 2024, 23(10): 13095–13109. doi: 10.1109/TWC.2024.3398651.

[3] HU Jinsong, YE Longjie, CHEN Youjia, *et al*. Covert

communications for text semantic with finite blocklength[J]. *IEEE Wireless Communications Letters*, 2024, 13(10): 2842–2846. doi: 10.1109/LWC.2024.3448614.

[4] RATHORE M S, POONGODI M, SAURABH P, *et al*. A novel trust-based security and privacy model for internet of vehicles using encryption and steganography[J]. *Computers and Electrical Engineering*, 2022, 102: 108–205. doi: 10.1016/j.compeleceng.2022.108205.

[5] YANG Qinglin, ZHAO Yetong, HUANG Huawei, *et al*. Fusing blockchain and AI with metaverse: A survey[J]. *IEEE Open Journal of the Computer Society*, 2022, 3: 122–136. doi: 10.1109/OJCS.2022.3188249.

[6] LIU Yuanni, PAN Ling, and CHEN Shanzhi. A hierarchical blockchain-enabled security-threat assessment architecture for IoV[J]. *Digital Communications and Networks*, 2024, 10(4): 1035–1047. doi: 10.1016/j.dcan.2022.12.019.

[7] WANG Lei, FAN Rongfei, HU Han, *et al*. Age of information minimization for opportunistic channel access[J]. *IEEE Transactions on Communications*, 2024, 72(12): 7449–7465. doi: 10.1109/TCOMM.2024.3415608.

[8] MA Yue, MA Ruiqian, LIN Zhi, *et al*. Improving age of information for covert communication with time-modulated arrays[J]. *IEEE Internet of Things Journal*, 2025, 12(2): 1718–1731. doi: 10.1109/JIOT.2024.3466855.

[9] KUMAR R, TRIPATHI R, MARCHANG N, *et al*. A secured distributed detection system based on IPFS and blockchain for industrial image and video data security[J]. *Journal of Parallel and Distributed Computing*, 2021, 152: 128–143. doi: 10.1016/j.jpdc.2021.02.022.

[10] ZHANG Ru, ZHU Feng, LIU Jianyi, *et al*. Depth-wise separable convolutions and multi-level pooling for an efficient spatial CNN-based steganalysis[J]. *IEEE Transactions on Information Forensics and Security*, 2020, 15: 1138–1150. doi: 10.1109/TIFS.2019.2936913.

[11] 李敬轩, 胡润文, 阮观奇, 等. 基于手工特征提取与结果融合的CNN音频隐写分析算法[J]. 计算机学报, 2021, 44(10): 2061–2075. doi: 10.11897/SP.J.1016.2021.02061.
LI Jingxuan, HU Runwen, RUAN Guanqi, *et al*. A CNN based audio steganalysis algorithm by manual feature extraction and result merging[J]. *Chinese Journal of Computers*, 2021, 44(10): 2061–2075. doi: 10.11897/SP.J.1016.2021.02061.

[12] REINEL T S, RAUL R P, and GUSTAVO I. Deep learning applied to steganalysis of digital images: A systematic review[J]. *IEEE Access*, 2019, 7: 68970–68990. doi: 10.1109/ACCESS.2019.2918086.

[13] REINEL T S, BRAYAN A A H, ALEJANDRO B O M, *et al*. GBRAS-Net: A convolutional neural network architecture for spatial image steganalysis[J]. *IEEE Access*, 2021, 9: 14340–14350. doi: 10.1109/ACCESS.2021.3052494.

[14] 李梦涵, 陈可江, 张卫明, 等. 基于合成语音的计算安全隐写方法[J]. 网络与信息安全学报, 2022, 8(3): 134–141. doi: 10.11959/j.issn.2096-109x.2022025.
LI Menghan, CHEN Kejiang, ZHANG Weiming, *et al*. Computationally secure steganography based on speech synthesis[J]. *Chinese Journal of Network and Information Security*, 2022, 8(3): 134–141. doi: 10.11959/j.issn.2096-109x.2022025.

[15] 李彦峰, 丁丽萍, 吴敬征, 等. 区块链环境下的新型网络隐蔽信道模型研究[J]. 通信学报, 2019, 40(5): 67–78. doi: 10.11959/j.issn.1000-436x.2019111.
LI Yanfeng, DING Liping, WU Jingzheng, *et al*. Research on a new network covert channel model in blockchain environment[J]. *Journal on Communications*, 2019, 40(5): 67–78. doi: 10.11959/j.issn.1000-436x.2019111.

[16] ZHANG Lejun, ZHANG Zhijie, WANG Weizheng, *et al*. Research on a covert communication model realized by using smart contracts in blockchain environment[J]. *IEEE Systems Journal*, 2022, 16(2): 2822–2833. doi: 10.1109/JSYST.2021.3057333.

[17] 黄冬艳, 李琨. 多地址的时间型区块链隐蔽通信方法研究[J]. 通信学报, 2023, 44(2): 148–159. doi: 10.11959/j.issn.1000-436x.2023026.
HUANG Dongyan and LI Kun. Research on multi-address time-based blockchain covert communication method[J]. *Journal on Communications*, 2023, 44(2): 148–159. doi: 10.11959/j.issn.1000-436x.2023026.

[18] SHE W, HUO L J, TIAN Z, *et al*. A double steganography model combining blockchain and interplanetary file system[J]. *Peer-to-Peer Networking and Applications*, 2021, 14(5): 3029–3042. doi: 10.1007/s12083-021-01143-0.

[19] 张祯, 倪嘉铭, 姚晔, 等. 基于同义词扩展和标签传递机制的文本无载体信息隐藏方法[J]. 通信学报, 2021, 42(9): 173–183. doi: 10.11959/j.issn.1000-436x.2021139.
ZHANG Zhen, NI Jiaming, YAO Ye, *et al*. Text coverless information hiding method based on synonyms expansion and label delivery mechanism[J]. *Journal on Communications*, 2021, 42(9): 173–183. doi: 10.11959/j.issn.1000-436x.2021139.

[20] DUAN Xintao, JIA Kai, LI Baoxia, *et al*. Reversible image steganography scheme based on a U-Net structure[J]. *IEEE Access*, 2019, 7: 9314–9323. doi: 10.1109/ACCESS.2019.2891247.

[21] LU Shaoping, WANG Rong, ZHONG Tao, *et al*. Large-capacity image steganography based on invertible neural networks[C]. 2021 IEEE/CVF Conference on Computer Vision and Pattern Recognition, Nashville, USA, 2021: 10811–10820. doi: 10.1109/CVPR46437.2021.01067.

[22] GUO Mengxi, ZHAO Shijie, LI Yue, *et al*. Invertible single image rescaling via steganography[C]. 2021 IEEE International Conference on Multimedia and Expo (ICME), Taipei, China, 2022: 1–6. doi: 10.1109/ICME52920.2022.9859915.

[23] SONG Yalin, ZHONG Yuhao, GAN Zhihua, *et al*. Generative adversarial networks-based image steganography with multiscale features integration[J]. *Journal of Electronic Imaging*, 2022, 31(5): 053028. doi: 10.1117/1.JEI.31.5.053028.

[24] 吴友情, 郭玉堂, 汤进, 等. 基于自适应哈夫曼编码的密文可逆信息隐藏算法[J]. 计算机学报, 2021, 44(4): 846–858. doi: 10.11897/SP.J.1016.2021.00846.

WU Youqing, GUO Yutang, TANG Jin, *et al*. Reversible data hiding in encrypted images using adaptive huffman encoding strategy[J]. *Chinese Journal of Computers*, 2021, 44(4): 846–858. doi: 10.11897/SP.J.1016.2021.00846.

[25] YI Shuang and ZHOU Yicong. Separable and reversible data hiding in encrypted images using parametric binary tree labeling[J]. *IEEE Transactions on Multimedia*, 2019, 21(1): 51–64. doi: 10.1109/TMM.2018.2844679.

[26] CHEN Kaimeng and CHANG C C. High-capacity reversible data hiding in encrypted images based on extended run-length coding and block-based MSB plane rearrangement[J]. *Journal of Visual Communication and Image Representation*, 2019, 58: 334–344. doi: 10.1016/j.jvcir.2018.12.023.

[27] WU Youqing, XIANG Youzhi, GUO Yutang, *et al*. An improved reversible data hiding in encrypted images using parametric binary tree labeling[J]. *IEEE Transactions on Multimedia*, 2020, 22(8): 1929–1938. doi: 10.1109/TMM.2019.2952979.

[28] CHEN Jianguo, LI Kenli, and YU P S. Privacy-preserving deep learning model for decentralized VANETs using fully homomorphic encryption and blockchain[J]. *IEEE Transactions on Intelligent Transportation Systems*, 2022, 23(8): 11633–11642. doi: 10.1109/TITS.2021.3105682.

[29] WANG Shujuan, HU Yingnan, and QI Guanqiu. Blockchain and deep learning based trust management for Internet of Vehicles[J]. *Simulation Modelling Practice and Theory*, 2022, 120: 102627. doi: 10.1016/j.simpat.2022.102627.

[30] XU Yan, LIU Xinyan, CUI Jie, *et al*. L-TCM: A lightweight privacy-preserving traffic condition monitoring scheme with source authentication in cloud-assisted VANETs[J]. *IEEE Systems Journal*, 2023, 17(4): 6138–6147. doi: 10.1109/JSYST.2023.3279620.

刘媛妮：女，教授，博士，研究方向为物联网安全，车联网安全，身份认证等.

范 飞：男，硕士生，研究方向为数据隐蔽通信.

赵宇洋：男，硕士生，研究方向为数据隐蔽通信.

张建辉：男，研究员，博士，研究方向为路由和交换设计、路由协议、资源调度、网络安全和未来网络等.

周由胜：男，教授，博士，研究方向为数据安全、认证与密钥协商等.

责任编辑：余 蓉

A Convert Communication Scheme of Blockchain Based on Image Multilevel Steganography Embedding

LIU Yuanni[①] FAN Fei[①] ZHAO Yuyang[①] ZHANG Jianhui[②] ZHOU Yousheng[①]

[①](*College of Cyberspace Security and Information Law, Chongqing University of Posts and Telecommunications, Chongqing* 400065, *China*)

[②](*National Digital Switching System Engineering and Technological Research and Development Center, Zhengzhou* 450002, *China*)

Abstract:

Objective With the advancement of information technology, information security concerns have become increasingly significant, making covert communication technology a critical area of focus. Existing schemes face limitations regarding embedding rate, anti-detection, and communication efficiency. To address these issues, steganographic embedding methods based on Generative Adversarial Networks (GANs) have gained considerable attention. This study utilizes the iterative training of GAN and steganalysis adversarial networks to generate stego-images with enhanced anti-detection capabilities. This approach aims to meet the concealment requirements for secure information transmission, while also improving the communication efficiency and security of the information exchange.

Methods This study proposes a blockchain-based covert communication scheme utilizing image multilevel

steganography. First, a multiple adversarial network for steganography is constructed, generating stego-images with enhanced anti-detection capabilities through the adversarial iterative training of GAN and steganalysis adversarial networks. Next, a reversible data hiding method in the ciphertext domain, based on location map information, is employed to embed the hidden data into the stego-images, resulting in a stego-images that contains the complete hidden information. Finally, the ciphertext image is stored in the InterPlanetary File System (IPFS) to assign it a unique identity, and then mapped to an address in the blockchain to enable covert transmission.

Results and Discussions To evaluate the effectiveness of the proposed scheme in terms of anti-steganography capability, invisibility, embedding capacity, and communication delay, simulation experiments are conducted. Regarding anti-steganography capability, the stego-images generated by the proposed scheme demonstrate strong anti-detection performance, outperforming the WOW and HILL algorithms (Fig. 7). In terms of concealment, the reversible data hiding method in the ciphertext domain, based on location map and spatial domain information, offers high concealment, effectively protecting the image content while enabling lossless restoration (Table 5, Table 6, Table 7). Concerning embedding capacity, the steganography algorithm in this scheme exhibits a high embedding capacity, with an average embedding rate exceeding that of the PBTL, IPBTL, and ERLC-BMPR algorithms (Fig. 9). Finally, in terms of communication delay, the proposed scheme results in low covert communication delay, outperforming the DVANET, BDLV, and L-TCM algorithms (Fig. 10).

Conclusions This paper proposes a blockchain-based covert communication scheme utilizing image multilevel steganography. Simulation experiments validate its advantages in information embedding rate, anti-steganography detection capability, concealment, and communication delay. The results demonstrate the following: 1. In terms of anti-steganography ability, the anti-detection performance of stego-images generated by SRNet+Zhu-Net significantly exceeds that of the WOW and HILL methods; 2. Regarding invisibility and embedding capacity, the proposed reversible data hiding method in the encrypted domain, based on location map and spatial domain information, achieves a high embedding rate and lossless recovery, outperforming the PBTL, IPBTL, and ERLC-BMPR methods; 3. In terms of communication efficiency, this scheme significantly reduces communication delay by combining blockchain and IPFS. Future research will focus on homomorphic encryption and identity authentication mechanisms to further enhance the security of on-chain data.

Key words: Covert communication; Blockchain; Adversarial network; Information hiding