基于全息加密与密集残差网络的图像隐写

doi:10.20269/j.cnki.1674-7100.2025.0007

王晓红　马春运　石明光

上海理工大学
出版学院
上海　200093

摘　要：为提高图像隐写容量、不可见性和安全性，提出基于全息加密与密集残差网络的图像隐写模型 CryptoStegoNet。该模型先将秘密信息转换为二维码，再经全息加密技术处理，嵌入载体图像中，生成高质量隐写图像，反之则提取秘密信息。DenseResidualGenerator 模块由跳跃连接、DenseBlock 和 DenseResBlock 组成。此外，通过引入 FID（Fréchet inception distance）损失来优化损失函数，以更好地引导网络训练，使生成的图像在视觉和统计上更接近载体图像。实验结果表明：与当前其他先进的隐写方法相比，本模型在视觉质量、隐写性能和安全性等多个指标上均实现了显著提升。

关键词：全息加密；密集残差网络；图像隐写；包装安全

中图分类号：TB489；TP309.7　　**文献标志码**：A

文章编号：1674-7100(2025)03-0046-09

引文格式：王晓红，马春运，石明光 . 基于全息加密与密集残差网络的图像隐写 [J]. 包装学报，2025，17(3)：46-54.

1　研究背景

图像隐写是一种通过在载体图像中隐藏秘密图像以进行隐蔽通信的技术，在信息安全、数据通信等领域起着至关重要的作用。通过图像隐写技术将隐写信息嵌入到包装中，可实现隐蔽的防伪标记，消费者或检查人员通过特定的软件提取这些标记信息，即可验证产品真伪。

图像隐写的发展经历了两个阶段：传统隐写方法和基于深度学习的隐写模型。在传统隐写方法的第一个阶段，研究人员通过特定的方式修改载体图像的像素值 [1-3]。例如，最低有效位（least significant bit，LSB）算法通过改变载体图像的像素值来嵌入秘密信息，但其嵌入容量有限，且易受到攻击。在传统隐写方法的第二阶段，为了解决这些问题，研究人员提出用自适应隐写模型（如 SUNIWARD[4]、WOW[5]、HUGO[6] 等），在图像的合适区域（如纹理复杂的区域）中自动识别进行隐写。然而，这些方法仍然无法在图像隐写中同时实现良好的隐蔽性、高容量和安全性。在传统隐写方法的第三阶段，张天骐等 [7] 提出了一个结合 DWT 和 DCT 的鲁棒水印算法。孙蕾等 [8] 提出了一种结合视觉密码与 DCT-SVD 技术的彩色图像水印算法。M. S. Subhedar 等 [9] 提出了使用帧分解和双对角 SVD 的隐写技术。总的来说，研究人员通过图像变换和精细的嵌入算法来增强图像隐写，尽管在隐蔽性、嵌入容量和安全性方面取得了显著进展，但简单嵌入操作的局限性制约了整体隐写效果。

由于深度学习具有强大的特征学习和数据处理能力，计算机视觉领域也取得了显著成果。深度学习在包装领域的应用也越来越广泛 [10]，如将深度学习

收稿日期：2024-10-18
基金项目：本研究成果受国家新闻出版署智能与绿色柔版印刷重点实验室招标课题资助（ZBKT202301）
作者简介：王晓红，女，教授，主要从事色彩学与色彩应用、印刷质量检测与控制、数字印刷技术研究，
E-mail：wang_keyan@163.com

用于图像隐写中，以增强隐写的隐蔽性。S. Baluja[11] 首次提出使用卷积神经网络（CNN）进行图像隐藏。之后，S. Baluja[12] 又试图通过深度隐写网络将两张彩色秘密图像隐藏在一张彩色载体图像中，并通过像素置换来提高安全性。A. Das 等 [13] 提出了一个类似的基于自动编码器的架构 MISDNN，用于实现多张彩色图像隐藏。基于 CNN 的隐写方法由于网络深度不足、结构简单，难以实现良好的隐写效果。J. Hayes 等 [14] 应用生成对抗网络（GAN）完成信息隐藏，结果表明对抗训练可以增强信息隐藏的安全性。Tang W. X. 等 [15] 构建了 ASDL-GAN，通过自动学习图像中的嵌入概率找到合适的隐藏点。Fu Z. J. 等 [16] 提出了隐写模型 HIGAN，将彩色秘密图像隐藏在另一张相同尺寸的彩色图像中，获得了比 CNN 更高的视觉质量和更强的安全性。王勇智 [17] 提出了基于伪随机数生成器的视频隐写模型，以提高视频隐写的安全性和隐蔽性，抵抗统计分析攻击。Zhang R.[18]、Chen B. J.[19]、Yao Y.[20] 等分别从 3 个方面探索了图像隐写方法：改变载体图像的色彩空间、使用条件约束控制载体图像、将载体图像从空间域转换到频率域。图像隐写隐蔽性在一定程度上得到了提升，但牺牲了嵌入容量和安全性。为了增强图像隐写网络的安全性，Huo L. 等 [21] 提出了一个将编码器－解码器架构与 GAN 相结合的创新框架 CHASE，用于将彩色秘密图像嵌入灰度图像。此外，它还结合了由 Logistic 混沌映射支持的图像置换算法，由于信息隐藏容量的扩展，隐写安全性显著增强。Zeng L. 等 [22] 采用了一种带有跳跃连接和 ExtractionBlock 的架构，该架构能够适应不同大小的特征，促进多尺度特征融合，从而实现高隐蔽性和隐写容量。这些研究仅对图像进行了基本和非复杂的模式转换，在不影响图像主要内容的情况下更改图像的某些属性，但不能在嵌入高容量秘密图像的同时，确保良好的隐蔽性和安全性。

综上，本研究提出一种图像加密的 CryptoStegoNet 模型，旨在通过图像全息加密和改进隐写模型解决图像隐写所面临的嵌入容量、隐蔽性和安全性挑战。

2 CrypoStegoNet 网络模型设计

2.1 基本原理

为了提高图像隐写的图像质量和安全性，本研究将图像加密与隐写网络结合，设计了一个 CryptoStegoNet 框架，如图 1 所示。CryptoStegoNet 由秘密信息转换模块（secret message transformation module）、嵌入网络（embedder）、提取网络（extractor）和信息逆转换模块（message inverse transformation module）组成。嵌入网络和提取网络都使用了 GAN 作为基础结构，嵌入网络将秘密信息隐藏在载体图像中，以生成隐写图像，而提取网络从隐写图像中提取秘密信息。嵌入网络中，生成器（$G_{(Em)}$）采用编解码结构，判别器（$D_{(Em)}$）采用 XuNet[23] 结构。在提取网络中，生成器（$G_{(Ex)}$）采用编解码结构，判别器（$D_{(Ex)}$）采用 CNN 结构。

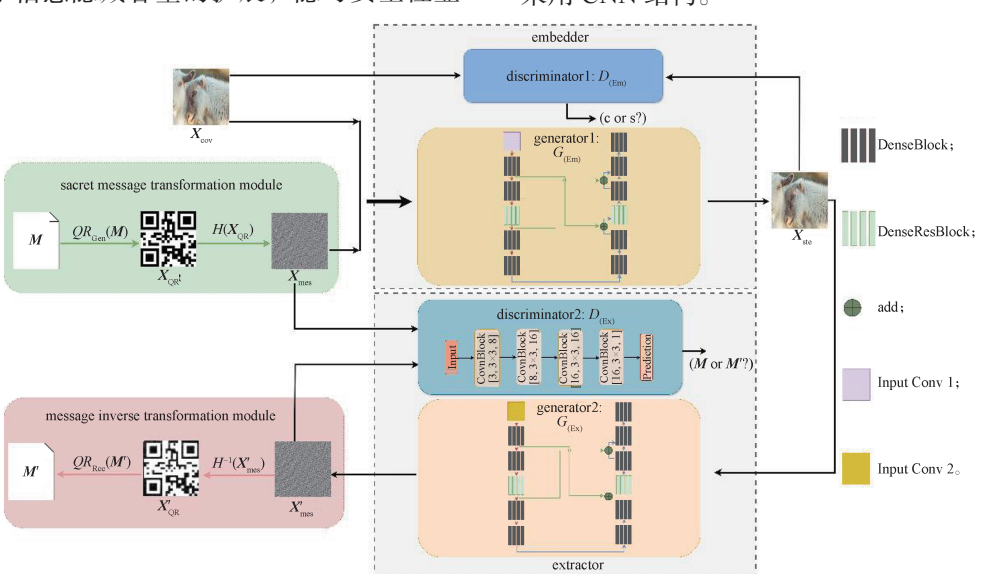

图 1　图像隐藏框架 CryptoStegoNet

Fig. 1　The image hiding framework CryptoStegoNet

使用二维码作为秘密信息（$\boldsymbol{M}$）的中间载体，因为二维码不仅可以存储文本，还可以是指向图像、视频或其他文件的超链接，从而实现多模态消息并支持大容量嵌入。秘密信息转换模块负责将秘密信息转换成二维码（$\boldsymbol{X}_{\mathrm{QR}}$），即

$$\boldsymbol{X}_{\mathrm{QR}}=QR_{\mathrm{Gen}}(\boldsymbol{M})。\tag{1}$$

为了提高隐写图像的质量和安全性，秘密信息转换模块进一步通过全息加密技术将二维码的独特斑块转换成均匀分布的全息图，该全息图作为嵌入网络的秘密图像（$\boldsymbol{X}_{\mathrm{mes}}$），即

$$\boldsymbol{X}_{\mathrm{mes}}=H(\boldsymbol{X}_{\mathrm{QR}})。\tag{2}$$

在嵌入过程中，将载体图像（$\boldsymbol{X}_{\mathrm{cov}}$）和秘密图像（$\boldsymbol{X}_{\mathrm{mes}}$）一起输入到嵌入网络的生成器 $G_{(\mathrm{Em})}$ 中，生成隐写图像（$\boldsymbol{X}_{\mathrm{ste}}$）。随后，判别器 $D_{(\mathrm{Em})}$ 确保 $\boldsymbol{X}_{\mathrm{ste}}$ 在视觉上类似于 $\boldsymbol{X}_{\mathrm{cov}}$。

$$\boldsymbol{X}_{\mathrm{ste}}=G_{(\mathrm{Em})}(\boldsymbol{X}_{\mathrm{cov}},\boldsymbol{X}_{\mathrm{mes}})。\tag{3}$$

在提取阶段，$\boldsymbol{X}_{\mathrm{ste}}$ 被输入到提取网络中的生成器 $G_{(\mathrm{Ex})}$ 中，提取秘密图像（$\boldsymbol{X}'_{\mathrm{mes}}$）。随后，判别器 $D_{(\mathrm{Ex})}$ 约束 $\boldsymbol{X}'_{\mathrm{mes}}$ 在视觉上接近 $\boldsymbol{X}_{\mathrm{mes}}$。

$$\boldsymbol{X}'_{\mathrm{mes}}=G_{(\mathrm{Ex})}(\boldsymbol{X}_{\mathrm{ste}})。\tag{4}$$

最后，信息逆转换模块负责将提取出的 $\boldsymbol{X}'_{\mathrm{mes}}$ 进行全息逆变换生成 $\boldsymbol{X}'_{\mathrm{QR}}$，再转换为秘密信息（$\boldsymbol{M}'$）。

$$\boldsymbol{X}'_{\mathrm{QR}}=H^{-1}(\boldsymbol{X}'_{\mathrm{mes}}),\tag{5}$$

$$\boldsymbol{M}'=QR_{\mathrm{Rec}}(\boldsymbol{X}'_{\mathrm{QR}})。\tag{6}$$

2.2 DenseResidualGnerator 模块

为了实现高容量的信息隐藏，设计了与任务高度匹配的深度隐写网络，称为 DenseResidualGenerator。它由跳跃连接、DenseBlock 和 DenseResBlock 组成。密集连接和残差连接结合能够增加特征的传递和复用，从而提升图像隐写的隐秘性和图像质量。跳跃连接将编码器和解码器连接起来，能够增强特征传递并减少梯度消失问题，从而提高隐写网络中图像生成的学习能力和稳定性。

嵌入网络的生成器 $G_{(\mathrm{Em})}$ 和提取网络的生成器 $G_{(\mathrm{Ex})}$ 都使用 DenseResidualGenerator 结构，但在卷积层的输入通道数量上有所不同。图 2 显示了 $G_{(\mathrm{Em})}$ 的网络架构。编码器由 6 个子层组成：enc1 为 ConvBlock，enc4 为 DenseResBlock，其他子层则为 DenseBlock。ConvBlock 的输入通道数为 7。为了加快收敛，6 个子层都使用了批归一化（batch normalization，BN）。从 enc1 到 enc5 的输入和输出通道数都设置为 32，enc6 的输入通道数为 32，输出通道数为 3。解码器也由 6 个子层组成：dec3 为 DenseResBlock，其余子层均为 DenseBlock。除了 dec1 和 dec6，从 dec2 到 dec5，输入和输出通道均为 32。

在嵌入过程中，$\boldsymbol{X}_{\mathrm{cov}}$ 和 $\boldsymbol{X}_{\mathrm{mes}}$ 通过编码器的 6 个子层表达式如下：

$$\Gamma_1=enc_1(\boldsymbol{X}_{\mathrm{cov}},\boldsymbol{X}_{\mathrm{mes}}),\tag{7}$$

$$\Gamma_i=enc_i(\Gamma_{i-1}),\ i=2,3,\cdots,6。\tag{8}$$

$\boldsymbol{X}_{\mathrm{cov}}$ 和 $\boldsymbol{X}_{\mathrm{mes}}$ 通过解码器的 6 个子层表达式如下：

$$\vartheta_1=dec_1(\Gamma_6),\tag{9}$$

$$\vartheta_i=dec_i(\Gamma_{i-1})。\tag{10}$$

在提取过程中，$\boldsymbol{X}_{\mathrm{ste}}$ 通过编码器的 6 个子层表达式如下：

$$\partial_1=enc_1(\boldsymbol{X}_{\mathrm{ste}}),\tag{11}$$

$$\partial_i=enc_i(\partial_{i-1})。\tag{12}$$

$\boldsymbol{X}_{\mathrm{ste}}$ 通过解码器的 6 个子层表达式如下：

$$\forall_1=dec_1(\partial_6),\tag{13}$$

$$\forall_i=dec_i(\forall_{i-1})。\tag{14}$$

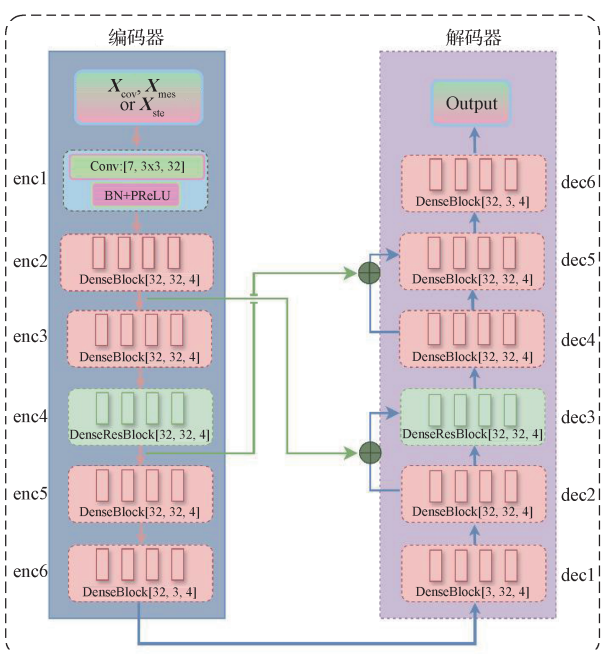

图 2 DenseResidualGenerator 模块结构

Fig. 2 The architecture of DenseResidualGenerator

2.3 DenseBlock 模块

DenseBlock 模块设计借鉴了 DenseNet 的密集连接结构。DenseBlock 有 4 个卷积层，所有前置层的信息直接传递给后续层，从而实现更有效的信息传递和共享。此外，梯度更有效地向早期层反向传播。相比于一些传统的全连接网络，此模块加快了模型的收敛速度。图 3 展示了 DenseBlock 模块的详细结构。

DenseBlock 的过程描述如下：

$$C_1=layer_1(\boldsymbol{X}), \tag{15}$$

$$C_i=layer_i(C_1+C_2+\cdots+C_{i-1}),\ i=2,3,4。 \tag{16}$$

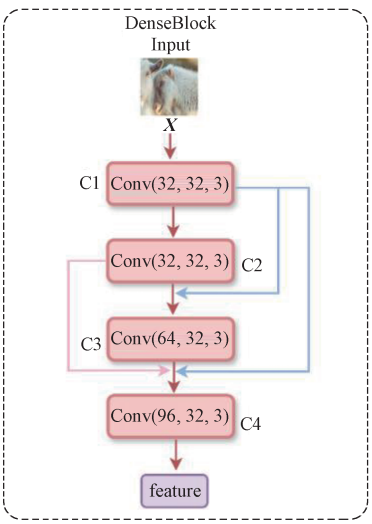

图 3　DenseBlock 模块结构

Fig. 3　The architecture of DenseBlock module

2.4　DenseResBlock 模块

残差结构可以保留更多的图像特征信息，提升图像质量。故在 DenseBlock 中引入残差连接，设计 DenseResBlock 模块，以平衡图像隐写的隐匿性和安全性。在安全性方面，残差连接的引入使得网络能够更好地抵抗隐写分析攻击。通过增强特征的传递和复用，网络能够在不显著改变图像统计特征的情况下嵌入秘密信息，从而降低被检测的风险。图 4 展示了 DenseResBlock 模块的详细结构。

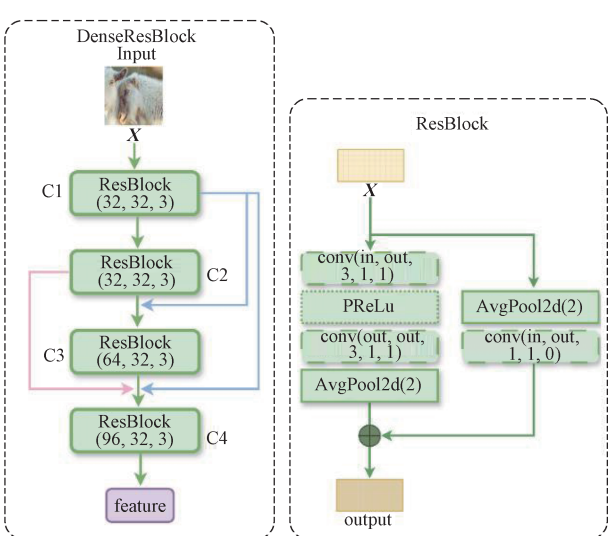

图 4　DenseResBlock 模块结构

Fig. 4　The architecture of our DenseResBlock module

2.5　损失函数

嵌入网络接收载体图像和秘密图像作为输入，生成隐写图像。使用均方误差（mean square error，MSE）计算载体图像与隐写图像之间的相似度，即

$$L_{\mathrm{MSE}}=\left\|\boldsymbol{X}_{\mathrm{ste}}-\boldsymbol{X}_{\mathrm{cov}}\right\|_2^2。 \tag{17}$$

为确保隐写图像的隐蔽性和增强图像隐写的安全性，引入 FID 作为损失函数，评估载体图像与隐写图像的相似性。

$$L=\left\|\boldsymbol{\mu}_{\mathrm{cov}}-\boldsymbol{\mu}_{\mathrm{ste}}\right\|^2+Tr\left(\boldsymbol{C}_{\mathrm{cov}}-\boldsymbol{C}_{\mathrm{ste}}-2\left(\boldsymbol{C}_{\mathrm{cov}}\boldsymbol{C}_{\mathrm{ste}}\right)^{0.5}\right), \tag{18}$$

式中：$\boldsymbol{\mu}_{\mathrm{cov}}$、$\boldsymbol{\mu}_{\mathrm{cov}}$ 分别为载体图像与隐写图像的均值向量；$\boldsymbol{C}_{\mathrm{cov}}$、$\boldsymbol{C}_{\mathrm{cov}}$ 分别为载体图像与隐写图像的协方差矩阵。

对抗损失是生成对抗网络中用于训练判别器的关键技术，目的是通过对抗训练生成逼真的数据。具体来说，判别器 $D_{(\mathrm{Em})}$ 试图区分载体图像和隐写图像，而生成器 $G_{(\mathrm{Em})}$ 则试图生成能欺骗判别器的隐写图像。对抗损失为

$$L_{\mathrm{A}}^{G_{(\mathrm{Em})}}=-\frac{1}{N}\sum_{i=1}^{N}\log D_{(\mathrm{Em})}\left(G_{(\mathrm{Em})}\left(\boldsymbol{X}_{\mathrm{cov}},\boldsymbol{X}_{\mathrm{ste}}\right)\right), \tag{19}$$

式中，N 为载体图像和隐写图像对数量。

通过 $G_{(\mathrm{Ex})}$ 提取的秘密图像与实际秘密图像之间的 MSE 可以用来优化 $G_{(\mathrm{Em})}$，即

$$L_{\mathrm{E}}^{G_{(\mathrm{Em})}}=\left\|\boldsymbol{X}_{\mathrm{mes}}-\boldsymbol{X}'_{\mathrm{mes}}\right\|_2^2。 \tag{20}$$

因此，嵌入网络的累积损失为

$$L_{\mathrm{sum}}^{G_{(\mathrm{Em})}}=L+\alpha\times L_{A}^{G_{(\mathrm{Em})}}+\gamma\times L_{\mathrm{E}}^{G_{(\mathrm{Em})}}, \tag{21}$$

式中，α 和 γ 为权重系数。

嵌入网络整体训练目标为

$$L_{\mathrm{obj}}^{G_{(\mathrm{Em})}}=\min_{G_{(\mathrm{Em})}}\max_{D_{(\mathrm{Em})}}V\left(G_{(\mathrm{Em})},D_{(\mathrm{Em})}\right)+L_{\mathrm{MSE}}+\gamma\times L_{\mathrm{E}}^{G_{(\mathrm{Em})}}。 \tag{22}$$

式中，$V(G_{(\mathrm{Ex})},D_{(\mathrm{Ex})})$ 为一个衡量生成器和判别器博弈结果的函数。

通过 $V(G_{(\mathrm{Ex})},D_{(\mathrm{Ex})})$，生成器和判别器不断竞争，最终达到一个平衡的状态，使得生成的隐写图像和载体图像难以区分。提取网络的损失函数与嵌入网络的相同。

3　实验结果与分析

3.1　实验设置

使用二维码生成程序将一串数字序列生成二维码图像，再通过 Matlab 软件中全息变换算法将

二维码图像转换为全息图像，即得秘密图像，共得 800 张秘密图像；使用 800 张秘密图像和随机选取的 800 张来自 Div2K 数据集 [24] 的载体图像训练 CryptoStegoNet。训练图像的分辨率为 256×256，总迭代次数为 2500。测试数据集是从 Div2K、LFW[25]、Pascal VOC[26] 数据集各选取 800 张图像。

为了评估模型优越性，将本模型与传统的图像隐藏算法 4bit-LSB 以及其他基于深度学习的方法进行比较，如文献 [11]、T-PAMI-19[12]、StegGAN[27]、HiDDeN[28]、文献 [29]、DeepMIH[30]、DGANS[31]、文献 [32]、ISGAN[33]、文献 [34]、AISU[35] 和文献 [36]。

为了评估隐写图像的不可感知性，采用 5 个评价指标：峰值信噪比（peak signal-to-noise ratio，PSNR）、结构相似性（structural similarity，SSIM）、MSE、感知损失和 FID。PSNR 和 SSIM 值越大，MSE、感知损失和 FID 值越小，表明图像质量越高。

用识别率（R）表示恢复秘密图像的效果。通过提取网络获得 800 张秘密图像，再通过全息逆变换将其转换为二维码，最后使用自动识别算法得到秘密信息。识别率为

$$R=\frac{T}{800}\times 100\%, \tag{23}$$

式中，T 为正确识别的秘密信息数量。

为了验证抗检测性能，用 SRNet[37] 进行隐写分析。检测准确率用于表示抗隐写分析能力，即

$$A=\frac{TP+TN}{TP+TN+FP+FN}\times 100\%, \tag{24}$$

式中：TP 和 TN 分别为正确识别为正例、负例的样本数；FP 和 FN 分别为错误识别为正例、负例的样本数。

A_{ac} 越小，表示抵抗隐写分析能力越强。A_{ac} 为

$$A_{ac}=\left|A-50\%\right|。 \tag{25}$$

3.2 消融实验

为了验证全息图像加密方法的有效性，在 Div2K 数据集上使用不同秘密图像评估 CryptoStegoNet 的图像隐写质量，如表 1 所示。由表 1 可知，全息秘密图像的隐写质量更高；在安全性方面，图像隐写分析的检测正确率提升了 7.75%。这证明了全息图像加密方法提升了隐写的图像质量和安全性。

为了验证 DenseBlock 模块和 DenseResBlock 模块的有效性，比较了不同组合模型对全息秘密图像进行隐写的质量和安全性，如表 2 所示。由表 2 可知，与普通卷积模型（Basic）相比，添加 DenseBlock 模块后，载体 / 隐写图像对的 PSNR 提高，检测准确率下降，这说明隐写图像质量和安全性得到提升。与添加 DenseResBlock 模块相比，DenseBlock 和 DenseResBlock 模块组合使用，PSNR 提升 2.9 dB，SSIM 提升 0.0022，而隐写分析结果稍有提升，这表明图像隐写质量和安全性之间存在博弈。

表 1 在 Div2K 数据集上使用不同秘密图像的 CryptoStegoNet 消融研究

Table 1 Ablation study of CryptoStegoNet with different secret images on the Div2K dataset

图像类型	PSNR/dB	SSIM	FID	A/%
普通秘密图像	32.49	0.9812	20.41	67.44
全息秘密图像	37.31	0.9963	8.77	59.69

表 2 不同组件组合的图像隐写质量

Table 2 Image steganography quality of different component combinations

模 型	PSNR/dB	SSIM	FID	A/%
Basic	37.98	0.9931	23.25	58.56
Basic+DenseBlock	41.86	0.9975	**10.51**	**52.81**
Basic+DenseBlock+DenseResBlock	**44.76**	**0.9997**	11.08	54.75

注：加粗字体表示各列最优结果。

3.3 隐写质量分析

本研究用 CryptoStegoNet 与其他模型在 Div2K、LFW 和 Pascal VOC 数据集上的载体 / 隐写图像对结果进行详细比较，如表 3 所示。表中，“↑”表示值越高越好。

从表 3 可以看出，CryptoStegoNet 在载体 / 隐写图像对的表现上都显著优于其他方法。具体来说，在 PSNR 方面，本模型比 DeepMIH、AISU 及文献 [34] 模型分别在 Div2K、LFW 和 Pascal VOC 数据集上的结果提升了 1.24, 6.45, 12.22 dB。在 SSIM 方面，本模型有显著优势，SSIM 值在 99% 以上。这表明 CryptoStegoNet 取得了最优的隐写质量。尽管模型仅在 Div2K 数据集上训练，但在 LFW 和 Pascal VOC 数据集上也表现出色，这表明本模型具有很强的泛化能力。

图 5 为本模型在不同数据集上的隐写与恢复秘密图像效果图。从图 5 可以看出，载体图像与隐写图像在视觉质量上几乎完全一致，体现了本模型具有较好的隐写效果。

表 3　不同隐写方法在不同数据集上的性能表现

Table 3　Performance of different steganography methods on different Image Net datasets

数据集	模型	PSNR/dB ↑	SSIM ↑	数据集	模型	PSNR/dB ↑	SSIM ↑
Div2K	文献 [11]	36.77	0.9645	LFW	ISGAN[33]	34.12	0.9660
	T-PAMI-19[12]	25.52	0.8405		文献 [34]	38.97	0.9658
	4bit-LSB	33.19	0.9453		AISU[35]	39.39	0.9894
	StegGAN[27]	34.39	0.9744		本模型	**45.84**	**0.9995**
	HiDDeN[28]	35.21	0.9691	Pascal VOC	文献 [32]	33.70	0.9600
	文献 [29]	39.75	0.9765		ISGAN[33]	34.44	0.9635
	DeepMIH[30]	43.72	0.9895		文献 [36]	36.59	0.9661
	本模型	**44.96**	**0.9979**		文献 [34]	37.05	0.9689
LFW	DGANS[31]	24.00	0.9072		本模型	**49.27**	**0.9945**
	文献 [32]	33.70	0.9500				

注：加粗字体表示各组数据最优结果。

图 5　本模型在不同数据集下的视觉质量分析

Fig. 5　Visual quality analysis across different datasets

表 4 展示了本模型在 3 个数据集上 800 对载体 / 隐写图像对的 MSE、感知损失和 FID。表中，“↓”表示值越低越好。从表 4 可知，不同数据集下载体 / 隐写图像对的 MSE、感知损失和 FID 都较小，表明隐写过程对载体图像的影响非常小，秘密图像的不可见性好。从隐写图像提取的二维码识别率可达 96% 以上，表明本模型恢复秘密图像的效果也较好。

表 4　本模型在不同数据集上的性能表现

Table 4　Performance of this model on different datasets

数据集	MSE ↓	感知损失 ↓	FID ↓	*R*/%
Div2K	0.000 23	0.049 84	6.41	99.13
LFW	0.003 88	0.115 76	14.95	96.63
Pascal VOC	0.000 25	0.138 23	11.88	98.00

3.4　安全性分析

抗隐写分析能力是衡量图像隐写安全性的重要因素[38]。较多研究人员利用 SRNet 作为隐写分析工具来评估模型的安全性。因此，本实验也采用 SRNet 评估本模型的抗隐写分析能力。从 Div2K 数据集选用 6000 对载体 / 隐写图像对训练 SRNet，训练代数为 150，再用 SRNet 测试本模型生成的 800 对载体 / 隐写图像对。表 5 为不同隐写模型的检测准确率（A）和 A_{ac} 值。与其他方法相比，本模型的检测准确率为 52.81%，A_{ac} 达到了 2.81%，这表明本模型具有强大的抗隐写分析能力。网络的复杂性和深度为秘密信息的高容量嵌入提供了必要条件。此外，图像加密方法进一步增强了隐写术的安全性，因为全息反变换具有较高的复杂性。

表 5　不同方法的安全性分析对比结果

Table 5　Comparison of safety analysis results for different methods

隐写模型	A/%	A_{ac}/%
文献 [11]	99.80	49.80
HiDDeN[28]	80.84	30.84
文献 [29]	77.43	27.43
DeepMIH[30]	75.54	25.54
LSB [39]	99.13	49.13
MSIDNN[40]	99.56	49.56
ISN[41]	75.69	25.69
SteganoGAN[42]	65.35	15.35
DUIANet[43]	46.80	3.20
HiNet[44]	55.86	5.86
本模型	**52.81**	**2.81**

注：加粗字体表示各列最优结果。

3.5　嵌入容量分析

嵌入容量是指在不显著影响图像质量和隐蔽性的前提下，在载体图像中嵌入的秘密信息量。不同隐写模型的嵌入容量对比结果如表 6 所示。由表 6 可知，与文献 [11]、文献 [36] 和 GSN[45] 对比，本模型的隐写容量得到显著提升。与 ISGAN[33] 和 AISU[35] 相比，本模型在达到相同隐写容量的同时，实现了较高的图像质量，PSNR 和 SSIM 得到大幅提升。本模型将二维码作为秘密信息的中间载体，实现了多模态信息隐写，能存储大容量信息如图像、视频等媒体信息。

表 6　嵌入容量对比结果

Table 6　Comparison results of steganographic capacities

隐写模型	隐写容量 /(bit • 像素 $^{-1}$)	PSNR/dB ↑	SSIM ↑	FID ↓
文献 [11]	1~4	36.77	0.9645	
ISGAN[33]	8	34.44	0.9660	
AISU[35]	8	39.39	0.9894	
文献 [36]	1			
GSN[45]	2			
本模型	8	**41.86**	**0.9910**	**10.51**

注：加粗字体表示各列最优结果。

4　结语

本研究提出一种基于全息加密和密集残差网络的图像隐写策略，旨在解决图像隐写术的三大挑战：确保隐写信息的隐蔽性、提升隐写过程的安全性及增加隐写信息的嵌入容量。实验结果表明，本模型在视觉质量、安全性和容量方面均优于现有方法。在未来的工作中，将继续深入探索隐写网络的优化策略，并进一步研究如何将图像加密技术与隐写术更紧密地结合，以期达到更高的安全标准和更优的隐写效果，并将图像隐写应用到包装防伪中。

参考文献：

[1] RÉMI C，ZITZMANN C，FILLATRE L，et al. A Cover Image Model for Reliable Steganalysis[C]//13th International Conference. Prague：Springer，2011：178−192.

[2] THAI T H，COGRANNE R，RETRAINT F. Statistical Model of Quantized DCT Coefficients: Application in the Steganalysis of Jsteg Algorithm[J]. IEEE Transactions on Image Processing，2014，23(5)：1980−1993.

[3] THAI T H，COGRANNE R，RETRAINT F. Optimal Detection of Outguess Using an Accurate Model of DCT Coefficients[C]//Processing of IEEE International Workshop on Information Forensics & Security. GA：IEEE，2014：179−184.

[4] HOLUB V，FRIDRICH J，DENEMARK T. Universal Distortion Function for Steganography in an Arbitrary Domain[J]. EURASIP Journal on Information Security，2014，2014(1)：1−13.

[5] HOLUB V，FRIDRICH J. Designing Steganographic

Distortion Using Directional Filters[C]//2012 IEEE International Workshop on Information Forensics and Security (WIFS). Costa Adeje：IEEE，2012：234−239.

[6] PEVNÝ T，FILLER T，BAS P. Using High-Dimensional Image Models to Perform Highly Undetectable Steganography[C]//Information Hiding. Berlin：Springer，2010：161−177.

[7] 张天骐，马焜然，邹 涵，等 . DWT-DCT 结合 SURF 与 PSO 的优化鲁棒水印算法 [J]. 信号处理，2024，40(6)：1148−1159.

[8] 孙 蕾，王洪君，刘鑫淇 . 基于视觉密码和 DCT-SVD 彩色图像水印技术 [J]. 智能计算机与应用，2024，14(3)：154−158.

[9] SUBHEDAR M S，MANKAR V H. Secure Image Steganography Using Framelet Transform and Bidiagonal SVD[J]. Multimedia Tools and Applications，2020，79(3)：1865−1886.

[10] 郝发义，刘伟丽 . 人工智能在包装领域的应用及研究进展 [J]. 包装学报，2024，16(4)：81−88.

[11] BALUJA S. Hiding Images in Plain Sight: Deep Steganography[C]//Proceedings of the 31st International Conference on Neural Information Processing Systems. New York：Curran Associates Inc.，2017：1−11.

[12] BALUJA S. Hiding Images Within Images[J]. IEEE Transactions on Pattern Analysis and Machine Intelligence，2020(7)：1685−1697.

[13] DAS A，WAHI J S，ANAND M，et al. Multi-Image Steganography Using Deep Neural Networks[J/OL]. 2021. https://arxiv.org/abs/2101.00350.

[14] HAYES J，DANEZIS G. Generating Steganographic Images via Adversarial Training[J/OL]. 2017. https://arxiv.org/abs/1703.00371.

[15] TANG W X，TAN S Q，LI B，et al. Automatic Steganographic Distortion Learning Using a Generative Adversarial Network[J]. IEEE Signal Processing Letters，2017，24(10)：1547−1551.

[16] FU Z J，WANG F，CHENG X. The Secure Steganography for Hiding Images via GAN[J]. EURASIP Journal on Image and Video Processing，2020，2020(1)：1−18.

[17] 王勇智 . 基于伪随机数生成器的视频隐写模型 [J]. 包装学报，2024，16(5)：58−62.

[18] ZHANG R，DONG S，LIU J. Invisible Steganography via Generative Adversarial Networks[J]. Multimedia Tools and Application，2019(7)：8559−8575.

[19] CHEN B J，WANG J X，CHEN Y Y，et al. High-Capacity Robust Image Steganography via Adversarial Network[J]. KSII Transactions on Internet & Information Systems，2020，14(1)：366−381.

[20] YAO Y，WANG J，CHANG Q，et al. High Invisibility Image Steganography with Wavelet Transform and Generative Adversarial Network[J]. Expert Systems with Applications，2024，249：123540.

[21] HUO L，CHEN R，WEI J，et al. A High-Capacity and High-Security Image Steganography Network Based on Chaotic Map and Generative Adversarial Networks[J]. Applied Sciences，2024，14(3)：1225.

[22] ZENG L，YANG N，LI X，et al. Advanced Image Steganography Using a U-Net-Based Architecture with Multi-Scale Fusion and Perceptual Loss[J]. Electronics，2023，12(18)：3808.

[23] XU G S，WU H，SHI Y. Structural Design of Convolutional Neural Networks for Steganalysis[J]. IEEE Signal Processing Letters，2022，23：708−712.

[24] AGUSTSSON E，TIMOFTE R. NTIRE 2017 Challenge on Single Image Super-Resolution: Dataset and Study[C]//IEEE Conference on Computer Vision and Pattern Recognition Workshops. HI：IEEE，2017：126−135.

[25] HUANG G B，MATTAR M，BERG T，et al. Labeled Faces in the Wild: A Database forStudying Face Recognition in Unconstrained Environments[C]//Processdings of Workshop on Faces in Real-Life Images: Detection, Alignment, and Recognition. California：Hans Publishers，2008：1−15.

[26] EVERINGHAM M，GOOL L V，WILLIAMS C K I，et al. The Pascal Visual Object Classes (VOC) Challenge[J]. International Journal of Computer Vision，2010，88(2)：303−338.

[27] SINGH B，SHARMA P K，HUDDEDAR S A，et al. StegGAN: Hiding Image Within Image Using Conditional Generative Adversarial Networks[J]. Multimedia Tools and Applications，2022，81(28)：40511−40533.

[28] ZHU J R，KAPLAN R，JOHNSON J，et al. HiDDeN: Hiding Data With Deep Networks[C]//European Conference on Computer Vision. Munich：Springer，2018：682−697.

[29] WENG X Y，LI Y Z，CHI L，et al. High-Capacity Convolutional Video Steganography with Temporal Residual Modeling[C]//Proceedings of the 2019 on International Conference on Multimedia Retrieval. Ottawa：ACM，2019：87−95.

[30] GUAN Z Y，JING J P，DENG X，et al. DeepMIH: Deep Invertible Network for Multiple Image Hiding[J]. IEEE Transactions on Pattern Analysis and Machine Intelligence，2022，45(1)：372−390.

[31] 竺乐庆，郭 钰，莫凌强，等 . DGANS: 基于双重生成式对抗网络的稳健图像隐写模型 [J]. 通信学报，2020，41(1)：125−133.

[32] REHMAN A U，RAHIM R，NADEEM M S，et al. End-to-End Trained CNN Encode-Decoder Networks for Image Steganography[EB/OL]. [2024−7−26]. https://arxiv.org/abs/1711.07201.

[33] ZHANG R，DONG S，LIU J. Invisible Steganography via Generative Adversarial Networks[J]. Multimedia Tools and Applications，2019，78(7)：8559−8575.
[34] CHEN B，WANG J，CHEN Y，et al. High-Capacity Robust Image Steganography via Adversarial Network[J]. KSII Transactions on Internet & Information Systems，2020，14(1)：366−381.
[35] ZENG L，YANG N，LI X，et al. Advanced Image Steganography Using a U-Net-Based Architecture with Multi-Scale Fusion and Perceptual Loss[J]. Electronics，2023，12(18)：12183808.
[36] DUAN X T，KAI J，LI B X，et al. Reversible Image Steganography Scheme Based on a U-Net Structure[J]. IEEE Access，2019，7：9314−9323.
[37] BOROUMAND M，CHEN M，FRIDRICH J. Deep Residual Network for Steganalysis of Digital Images[J]. IEEE Transactions on Information Forensics and Security，2018，14(5)：1181−1193.
[38] MENG R，CUI Q，YUAN C. A Survey of Image Information Hiding Algorithms Based on Deep Learning[J]. Computer Modeling in Engineering & Sciences，2018，117(3)：425−454.
[39] TAMIMI A A，ABDALLA A M，ALALLAF O. Hiding an Image Inside Another Image Using Variable-Rate Steganography[J]. International Journal of Advanced Computer Science and Applications，2013，4(10)：18−21.
[40] DAS A，WAHI J S，ANAND M，et al. Multi-Image Steganography Using Deep Neural Networks[EB/OL]. [2024−05−19]. https://arxiv.org/abs/2101.00350v1.
[41] LU S P，WANG R，ZHONG T，et al. Large-Capacity Image Steganography Based on Invertible Neural Networks[C]//2021 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR). TN：IEEE，2021：10816−10825.
[42] ZHANG K A，CUESTA-INFANTE A，XU L，et al. SteganoGAN: High Capacity Image Steganography with GANs[EB/OL]. [2024−05−21]. https://arxiv.org/abs/1901.03892v2.
[43] DUAN X，WU G M，LI C，et al. DUIANet: a Double Layer U-Net Image Hiding Method Based on Improved Inception Module and Attention Mechanism[J]. Journal of Visual Communication and Image Representation，2024，98：104035.
[44] JING J P，DENG X，XU M，et al. HiNet: Deep Image Hiding by Invertible Network[C]//International Conference On Computer Vision. [S. l.]：IEEE，2021：4733−4742.
[45] WEI P，LI S，ZHANG X，et al. Generative Steganography Network[C]//Proceedings of the 30th ACM International Conference on Multimedia. [S. l.]：ACM，2022：1621−1629.

（责任编辑：邓　彬）

Research on Packaging Security Steganography Based on Holographic Encryption and Dense Residual Networks

WANG Xiaohong，MA Chunyun，SHI Mingguang

（School of Communication and Art Design，University of Shanghai for Science and Technology，Shanghai 200093，China）

Abstract：To enhance the capacity, invisibility, and security of image steganography, an image steganography model named CryptoStegoNet based on holographic encryption and dense residual networks is proposed. The model first converts the secret information into a QR code, then processes it with holographic encryption technology, and embeds it into the cover image to generate a high-quality steganographic image. The secret information can be extracted in the reverse process. The DenseResidualGenerator module, which consists of skip connections, DenseBlock, and DenseResBlock, is a key component of this model. Additionally, by introducing the FID (Fréchet inception distance) loss, the loss function is optimized to better guide the network training, making the generated images visually and statistically closer to the cover images. Experimental results demonstrate that compared with other state-of-the-art steganography methods, the model achieves significant improvements in visual quality, steganographic performance, and security.

Keywords：holographic encryption；dense residual network；image steganography；packaging security