arXiv:2305.05838v1 [cs.CV] 10 May 2023

生成式隐写流

Ping Wei、*Ge Luo*、*Qi Song*、*Xinpeng Zhang**、*Zhenxing Qian**、*Sheng Li*

复旦大学计算机科学技术学院，中国上海{pwei17, 18110240026, 19210240114, zhangxinpeng, zxqian, lisheng}@fudan.edu.cn

摘要

生成式隐写术（GS）是一种新型数据隐藏方式，其特点是直接根据秘密数据生成隐写媒体。现有 GS 方法通常因表现不佳而受到诟病。本文提出一种新颖的基于流的 GS 方法——生成式隐写流（GSF），无需封面图像即可直接生成隐写图像。我们将隐写图像生成和秘密数据恢复过程视为可逆变换，并在输入秘密数据与生成的隐写图像之间构建可逆双射映射。在正向映射中，秘密数据被隐藏在 Glow 模型的输入潜变量中，以生成隐写图像。通过逆向映射，可以从生成的隐写图像中精确提取隐藏数据。此外，我们提出一种新颖的潜变量优化策略，以提高隐写图像的保真度。实验结果表明，我们提出的 GSF 性能远超最先进的方法。

索引词— 隐写术、生成式隐写术、数据隐藏、归一化流

1. 引言

隐写术通常会对载体媒体进行轻微修改，以隐藏秘密数据[1]。早期基于图像的隐写算法通常将秘密数据隐藏在载体图像的最低有效位中。之后，人们提出了许多基于综合格编码（STC）的算法，以尽量减少嵌入数据后的失真[2]。随着深度学习（DL）的发展，许多基于深度学习的隐写方案也相继提出[3]。例如，Baluja[4]提出了一种神经网络，用于将秘密图像隐藏在载体图像中。然而，这些方法生成的隐写图像与载体图像之间存在不可忽视的差异，因此很容易被隐写分析算法检测出来[5, 6]。其中，隐写分析是用于检测图像是否包含秘密数据的对应技术。

近年来，一种名为生成式隐写术（GS）的新型隐写方式引起了研究人员的关注[7]。采用这种方法，可以将秘密数据直接转换为自然的隐写图像，即不再需要载体图像。

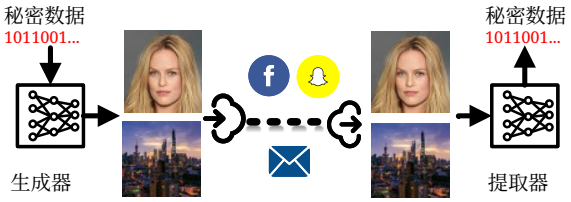


图 1。生成式隐写术流程图。二进制秘密数据经由图像生成器转换为隐写图像。随后，生成的隐写图像可通过社交网络、电子邮件或其他渠道传输。最后，使用数据提取器从接收到的隐写图像中恢复隐藏的秘密数据。

图 1 展示了 GS 的流程图。在早期，人们通常会合成某些特定类型的图像来隐藏秘密，例如纹理图像 [8] 和指纹图像[9]。然而，这类方法只能生成少数几种特殊类型的图像，而且图像内容不够自然，可能会引起监控者的怀疑。后来，一些研究人员[10, 11] 提出利用生成对抗网络（GANs）合成自然的隐写图像。对于这类方法，通常通过预先构建的映射字典，将 GANs 的输入变量用于表示秘密数据。通过分配相应的标签或噪声向量，利用 GANs 生成自然的隐写图像。然而，这些方法的性能较差，图像质量和隐藏容量都较低。

本文提出一种新颖的基于流的生成式隐写术方法，称为 GSF。不同于现有的生成式隐写术方法需要一个网络生成隐写图像、另一个网络提取隐藏的秘密数据，我们提出的 GSF 在一个网络上即可完成这两项任务。我们没有像大多数生成式隐写术方法那样使用映射字典，而是提出将秘密数据隐藏在 Glow 的二值化潜变量中，以获得更高的性能。我们构建了一种可逆双射映射，实现秘密数据与隐写图像之间的无损转换。我们的主要贡献如下：

- 我们首次提出一种基于流的生成式隐写术解决方案，只需使用单个网络即可生成逼真的隐写图像并恢复隐藏的秘密数据。
- 我们构建了输入秘密数据与生成的隐写图像之间的可逆双射映射，借助该映射

[1]通讯作者为 Xinpeng Zhang 和 Zhenxing Qian。

秘密数据和隐写图像几乎可以在不丢失信息的情况下相互转换。

- 我们提出了一种新颖的潜变量优化策略，以提高隐写图像的质量。
- 与现有方法相比，我们提出的 GSF 取得了更优异的性能。我们方案的隐藏容量、提取准确率、含密图像质量和安全性均远高于当前最先进的方法。

2. 生成式隐写流程

所提出的 GSF 流程如图 2 所示，分为两个阶段：1. 潜变量优化阶段；2. 秘密信息隐藏与提取阶段。在第一阶段，对潜变量$\mathbf{Z}$ 进行优化，以提高生成的隐写图像的质量。如图 2 上方所示，采用质量评估器评估图像保真度，并根据每张输入图像的保真度输出评分。生成图像与真实图像之间的分数差异（差异）用作优化的反向损失；在第二阶段，建立从输入秘密数据到输出隐写图像的可逆双射映射，据此可将秘密数据转换为隐写图像，反之亦然。数据隐藏过程如图 2 下方所示。首先，将第一阶段得到的优化潜变量$\mathbf{Z}$ 编码为二进制序列，并将每个序列中的一些可隐藏位替换为输入秘密数据。其次，将这些修改后的序列转换为L个浮点张量，其尺寸与$\mathbf{Z}$中的张量相同，并将其命名为隐写潜变量$\mathbf{Z_s}$。最后，将$\mathbf{Z_s}$ 输入预训练 Glow 模型，以生成隐写图像。反过来，按照上述步骤的逆过程即可提取隐藏的秘密数据。

2.1. 模型训练

我们的方法基于流式生成模型 Glow[12], 构建，借助该模型，输入潜变量$\mathbf{Z}$ 与生成图像$\mathbf{I}$ 几乎可以在不造成信息损失的情况下相互转换，即 $Glow(\mathbf{I}) = \mathbf{Z}$ 且 $Glow^{-1}(\mathbf{Z}) = \mathbf{I}$。$Glow$ 由一系列可逆函数组成，$Glow = f_1 \times f_2 \cdots \times f_n$。Glow 的变换可表示为：$\mathbf{I} \xrightarrow{f_1} \mathbf{h_1} \xrightarrow{f_2} \mathbf{h_2} \cdots \xrightarrow{f_n} \mathbf{Z}$，$\mathbf{Z} \xrightarrow{f_n^{-1}} \mathbf{h_{n-1}} \cdots \xrightarrow{f_2^{-1}} \mathbf{h_1} \xrightarrow{f_1^{-1}} \mathbf{I}$，其中，$f_i$ 是一个可逆变换函数，$\mathbf{h_i}$ 是 f_i的输出。Glow 由三种模块组成，包括压缩模块、流模块和分割模块。压缩模块用于对特征图进行下采样，流模块用于特征处理。分割模块会将图像特

沿通道维度将特征分成两半，其中一半作为潜变量张量 $\mathbf{Z_i}$ 输出，其大小为：$(h_i, w_i, c_i) = \begin{cases} (\frac{H}{2^i}, \frac{W}{2^i}, 6 \times 2^i) & i = 0, \cdots, L-2 \\ (\frac{H}{2^i}, \frac{W}{2^i}, 12 \times 2^i) & i = L-1 \end{cases}$，其中

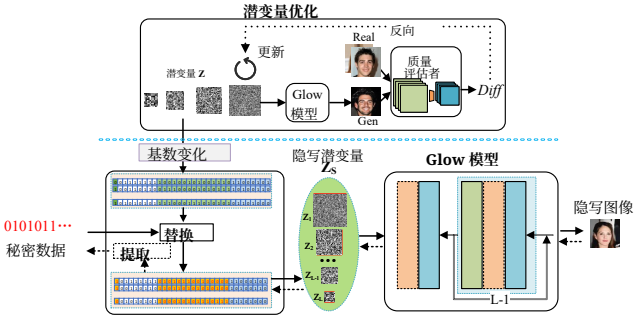


图 2。我们提出的 GSF 的整体结构。潜变量 $\mathbf{Z}$ 通过反向损失 差异循环更新，该损失由图像质量评估器计算。秘密数据隐藏在优化后的 $\mathbf{Z}$ 的二值化序列中。接下来，修改后的序列被转换为 $\mathbf{Z_s}$，然后发送到 Glow 模型以生成隐写图像。通过逆向执行隐藏过程，可以提取隐藏的秘密数据。

H/W 分别是生成图像的高度/宽度，L 是 $\mathbf{Z_i}$的数量。然后，将另一半特征送入压缩模块。在我们的方案中，$\mathbf{Z} = \sum_{i=1}^{L} \mathbf{Z_i}$ 被视为 Glow 的整体输入潜变量。Glow 模型的损失函数定义如下：

$$\log p_{\boldsymbol{\theta}}(\mathbf{I}) = \log p_{\boldsymbol{\theta}}(\mathbf{Z}) + \sum_{i=1}^{n-1} \log \left| \det \left(d\mathbf{h}_i / d\mathbf{h}_{i-1} \right) \right|, \quad (1)$$

其中，$\log \left| \det \left(d\mathbf{h}_i / d\mathbf{h}_{i-1} \right) \right|$ 表示雅可比矩阵 $d\mathbf{h}_i / d\mathbf{h}_{i-1}$行列式绝对值的对数。

2.2. 潜变量优化策略

Glow 的初始输入潜变量服从以下分布：$\mathbf{Z} \sim N(0, 1) \times \delta$, 但它只能生成低质量的生成图像。因此，我们提出了一种潜变量优化策略，以提升生成图像的质量。所提出的策略如图 2 顶部所示，并在算法 1 中进行了描述。我们没有使用随机正态分布，而是使用投影潜变量的平均值来初始化 $\mathbf{Z}$，其中，随机采样的 n 张真实图像 $\mathbf{I_n}$ 通过 Glow 模型转换为潜变量值，即 $\mathbf{Z} = \frac{1}{n} \sum Glow(\mathbf{I_n})$。接下来，使用反向损失 $Diff$循环更新初始化后的 $\mathbf{Z}$，以进一步提升图像质量。

在该策略中，我们使用质量评估器（QA）来评估图像的保真度。我们使用预训练分类器 Resnet50[13] 作为 QA，它在真实图像和 Glow 生成的生成图像上进行训练。对于真实输入图像，QA 会输出正评分；对于生成图像，则会输出负评分。 $Diff$ 是 QA 对n 张真实图像输出的平均评分与生成图像评分之间的差异，可按如下方式计算：

$$Diff = \left| \frac{1}{n} \sum_{1}^{n} score_{real}^{i} - score_{gen} \right|, \quad (2)$$

算法 1　　潜变量优化策略

输入：n 张随机采样的**真实图像**$\mathbf{I_n}$。

输出：优化潜变量$\mathbf{Z}$。

所需：　　一个预训练的 Glow 模型，以及一个预训练的 ResNet50 作为质量评估器（质量评估器）。

1：初始化潜变量，$\mathbf{Z} = \frac{1}{n}\sum Glow(\mathbf{I_n})$。

2：质量评估器为 i_{th} 图像 $\mathbf{I_n}$, $score^{i}_{real}$ 输出一个评分。

3: **for** 步骤在范围内（最大步数）**执行**

4:　　Glow 使用$\mathbf{Z}$生成图像（**Gen**）。

5:　　质量评估器为**Gen**输出评分，$score_{gen}$。

6:　　计算 $Diff = |\frac{1}{n}\sum_{1}^{n} score^{i}_{real} - score_{gen}|$。

7:　　使用梯度 $\nabla_{\mathbf{z}} Diff$ 更新$\mathbf{Z}$。

8:　　**如果** 差异 $<$ *thresh***那么**

9:　　保存优化潜变量$\mathbf{Z}$。

10:　　中断。

其中，$score^{i}_{real}$ 是 QA 对 i_{th} 张真实图像输出的评分，$score_{gen}$ 是生成图像的评分。每一步只生成一张图像。在每个优化步骤中，$\mathbf{Z}$ 按如下方式更新：

$$\mathbf{Z} := \mathbf{Z} - \varepsilon \cdot \nabla_{\mathbf{z}} Diff, \tag{3}$$

在此，ε是控制变化程度的超参数，而$\nabla_{\mathbf{z}} Diff$是潜变量$\mathbf{Z}$的梯度。优化过程将持续进行，直到达到最大训练步，或 $Diff$ 的值低于阈值。

2.3. 秘密隐藏与提取

如图 2 和图 3 所示，秘密数据被隐藏在优化潜变量的二值化序列中。进制转换采用 IEEE 754 标准，通过该标准，$\mathbf{Z}$ 中的每个浮点数都被编码为一个 32 位二进制序列：

$$(n)_{10} = (-1)^{sign} \times 2^{(exponent)_{10}-127} \times (1 + (fraction)_{10}), \tag{4}$$

这里，$(n)_{10}$ 表示一个十进制浮点数。$sign$ 是符号位，其值为 0 或 1。$(exponent)_{10}$ 表示十进制指数乘数，在我们的方案中通常等于 125、126 或 127。$(fraction)_{10}$ 表示浮点数的小数部分。然后，$sign$ 位、$(exponent)_{10}$ 和 $(fraction)_{10}$ 的值依次转换为二进制数字，形成一个 32 位二进制序列。

图 3 展示了详细的数据隐藏过程。首先，使用公式 4 中定义的函数，将$\mathbf{Z}$ 中的所有浮点数编码为 32 位二进制序列。除会极大影响图像质量的指数位外，这些二值化序列中的 $Sign$ 位和小数部分（0_{th} 至 22_{th} 位）均可用于隐藏秘密数据，称为可隐藏位。其中，仅使用小数部分的 α_{th} 至 β_{th}（$0 \le \alpha \le \beta \le 22$，$[\alpha : \beta]$）位进行数据隐藏。在我们的方案中，我们改变 α 的值来传递不同的秘密载荷，同时将 β 固定为

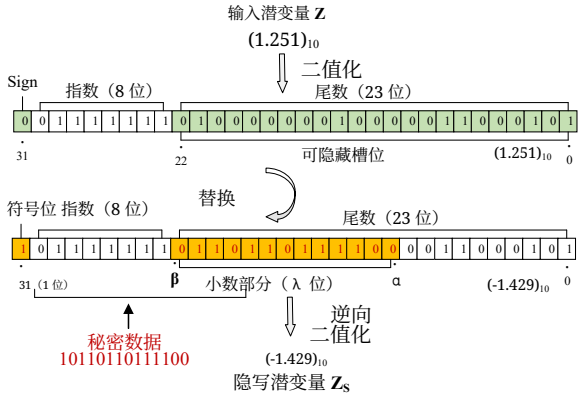


图 3：秘密数据隐藏示意图。将$\mathbf{Z}$ 转换为二值化序列后，输入的秘密数据将隐藏在这些序列的可隐藏位中。随后，将修改后的序列转换为名为$\mathbf{Z_s}$的浮点张量。

22。随后，将包含秘密数据的修改后序列重新转换为浮点数，再重构为隐写潜变量$\mathbf{Z_s}$。

我们可以逆转数据隐藏过程来提取秘密数据。首先，将接收到的隐写图像输入 Glow 模型，以恢复隐写潜变量。然后，将恢复的隐写潜变量$\mathbf{Z_s^*}$转换为二进制序列。最后，可以从这些序列的 $Sign$ 位和 $[\alpha : \beta]$ 位中取回隐藏的秘密数据。总之，秘密数据的隐藏与提取过程可描述如下：

$$\begin{aligned} \mathbf{Secret} &\rightarrow \mathbf{bin}(\mathbf{Z})[S, \alpha : \beta], \\ \mathbf{Secret}^* &\leftarrow \mathbf{bin}(\mathbf{Z_s^*})[S, \alpha : \beta], \end{aligned} \tag{5}$$

其中，$\mathbf{bin}(\cdot)$ 表示将潜变量张量中的浮点数转换为二进制序列。**秘密数据** 是输入的秘密数据，它隐藏在$\mathbf{bin(Z)}$的 $Sign$ 位和 α - β 位中，即 $[S, \alpha : \beta]$。**秘密数据*** 是从$\mathbf{bin(Z_s^*)}$的相同位置提取的秘密数据。

3. 实验结果

我们的方案在 CentOS 7 上使用 PyTorch 实现，硬件配备 4 张 Nvidia 1080Ti。使用 CelebA[14]评估模型性能。优化器为 Adam，学习率为 1e-3。训练 Glow 模型以生成 128×128图像，使用 $L = 5$。公式 3 中的参数 ε 设为 1e-3，公式 2 和算法 1 中的 n设为 3。算法 1 中的 $thresh$ 设为 0.1，而*max-step* 设为 100。

在隐写术中，位/像素是用于衡量隐写图像载荷的指标，位/像素 $= \frac{len(\text{秘密数据})}{H \times W}$ · 此处，~~位/像素~~表示每个像素所承载的秘密比特数（每像素比特数），$len(\cdot)$ 表示隐藏的秘密数据的长度，*H/W* 表示隐写图像的高度/宽度。准确率用于衡量秘密数据的提取准确率：准确率 $= \frac{\text{秘密数据}^* \odot \text{秘密数据}}{\text{len(秘密数据)}}$，



图 4。采用潜变量优化策略前后的结果图像（顶部 + 中左 / 底部 + 中右）。



图 5。潜变量优化过程中图像缓慢变化。

这里，**秘密数据*** 和**秘密数据**分别表示提取出的秘密数据和输入的秘密数据。 $\odot$ 表示 $XNOR$ 操作。隐写术的安全性通过指标 PE 进行评估，其定义如下：PE $=\min_{P_{FA}} \frac{1}{2}(P_{FA}+P_{MD})$，其中，$P_{FA}$和 P_{MD} 分别表示隐写图像的虚警率和漏检率。PE 的取值范围为 $[0, 1.0]$，其最优值为 0.5。此时，隐写分析器无法区分图像的来源，只能进行随机猜测。采用预训练的 ResNet50 作为质量评估器。该评估器使用 CelebA 数据集中的 20k 张真实图像和 Glow 生成的 20k 张生成图像进行训练。由未经修改的原始**Z**生成的图像称为普通图像，其中未隐藏任何秘密数据。由隐写潜变量$\mathbf{Z_S}$ 生成的图像称为隐写图像，其中包含秘密数据。

3.1. 潜变量优化策略的影响

所提出的潜变量优化策略有助于提高图像质量。图 4 对比了生成图像采用所提出策略前后的图像。顶行是原始生成图像，其保真度较低，内容中带有一些白线、马赛克和噪点。底行是采用所提出的潜变量优化策略后生成的图像。中间一行展示了细节图像。与未经优化的图像相比，可以发现，我们提出的优化策略能够显著提高图像质量。

与此同时，图像内容可能会在优化过程中逐渐变化。从图 5 可以观察到，面部表情、发型和性别都在平滑地变化。同时，这些图像也变得更加清晰。

3.2. 所提出 GSF 的性能

根据隐写图像是否经过舍入操作后保存，我们提出了两种生成隐写图像的策略。其中，秘密数据被隐藏在潜变量**Z**编码二进制序列的不同位位置中。

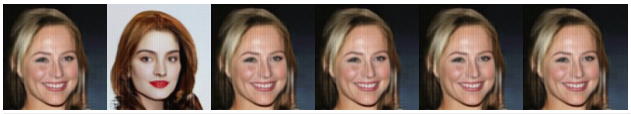
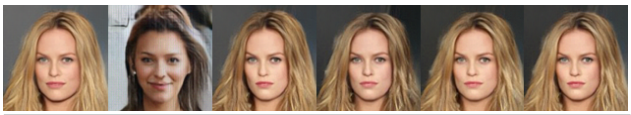
在第一种情况下，生成的隐写图像会被四舍五入为 $[0, 255]$ 之间的整数，并保存为 PNG 和未压缩 JPEG 等图像格式。由于舍入操作不可逆，且图像保存过程中会有大量像素被裁剪，秘密数据的提取准确率会降低。如表 1 所示，最左侧一列是生成的普通图像（0 位/像素，即不含秘密数据的图像），这些图像由未修改的潜变量生成。其余各列展示了不同载荷下生成的隐写图像的性能。 $[S, \alpha: \beta]$ 表示用于数据隐藏的 $Sign$位以及从 α_{th} 到 β_{th} 的各位。将 β 固定为 22，改变 α的值即可获得不同的载荷。准确率是秘密数据平均提取准确率。随着载荷增加，准确率缓慢下降，因为像素裁剪和舍入操作会使序号较小的位更难提取。本方案的最大载荷为 72 位/像素，准确率为 51.84%。载荷为 3 位/像素时，准确率相对较高，达到 92.44%。实际上，使用纠错码即可达到 100%。生成的隐写图像看起来与普通图像截然不同，因为修改 $Sign$ 位会反转像素值，并对图像内容造成显著影响。不过，生成的隐写图像整体质量较低，这可能

表1。我们方案在 PNG 隐写图像上的性能。

0 位/像素	3 位/像素	6 位/像素	9 位/像素	36 位/像素	72 位/像素
$[S, \alpha: \beta]$	S	S, 22:22	S, 21:22	S, 12:22	S, 0:22
准确率 (%)	92.44	74.09	64.65	54.19	51.84



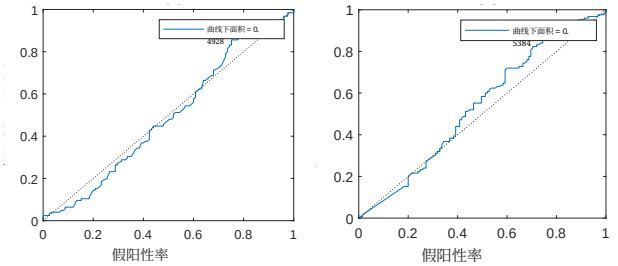
表2。该方案在 TIFF 隐写图像上的性能。

0 位/像素	3 位/像素	3 位/像素	27 位/像素	48 位/像素	69 位/像素
$[S, \alpha: \beta]$	S	22:22	14:22	7:22	0:22
准确率 (%)	99.99	99.95	98.53	85.61	74.71
					
准确率 (%)	100	99.98	99.26	89.47	77.32
					

引起第三方的怀疑。

在第二种情况下，生成的隐写图像以浮点数据类型保存，不执行舍入操作，即图像可以以 float32 数据类型保存为 TIFF 格式。因此，保存时不会引入信息损失。事实上，浮点 TIFF 格式广泛用于要求高精度的场景，例如航空图像。我们在此采用所提出的潜变量优化策略，以提高 TIFF 隐写图像的质量。表中，随机潜变量（$\mathbf{Z} \sim N(0,1) \times \delta$）和优化潜变量（$\mathbf{Z}$ 优化后）均用于生成 TIFF 隐写图像，结果列于表2。可以看出，所提出的潜变量优化策略能够生成质量更高的隐写图像，但修改 $Sign\,(S)$ 位会降低图像质量。为保持隐写图像的保真度，我们只修改二值化序列的尾数 $\alpha_{th} - \beta_{th}$ 位来隐藏秘密数据。表中，准确率随着载荷增加而逐渐下降。我们的 GSF 实现了最高 69 位/像素的载荷，准确率为 77.32%。当载荷低于 27 位/像素时，准确率均高于 99%。

我们提出的 GSF 的安全性通过四种先进的隐写分析方法进行测试：SCRMQ1[5], Ye-net[15], SR- net[6] 和孪生卷积神经网络[16]。SCRMQ1 是一种用于彩色隐写图像的传统特征提取器，其结果



(a) 3 位/像素 PNG 隐写图像　(b) 27 位/像素 TIFF 隐写图像

图6。在 SCRMQ1 上测试我们的隐写图像所得的受试者工作特征曲线。

表 3。生成的隐写图像的 PE值

图像格式 位/像素		SCRMQ1	Ye-net	SR-net	孪生网络
PNG	3	0.4780	0.500	0.493	0.473
TIFF	18	0.4998	0.458	0.470	0.304
	27	0.4824	0.416	0.404	0.252

通过集成分类器进行分类。Ye-net、SR-net和孪生卷积神经网络是三种最先进的基于深度学习的隐写分析算法。在检测中，生成的普通图像（0 位/像素）被用作载体数据集，而生成的隐写图像则被用作含密数据集。我们生成的隐写图像的ROC曲线如图6所示。它们的曲线下面积值都接近0.5（最优值）。详细的检测PE值列于表3中。正如我们所看到的，大多数PE值都接近理想值0.5，这表明我们的方法非常安全。这意味着现有的隐写分析方法几乎无法将我们生成的隐写图像与载体图像区分开来。

3.3. 结果比较

我们将 GSF 与表 4 所列的最先进方法进行了比较。Zhang[10] 和 Hu[11] 是两种基于生成对抗网络的最先进生成式隐写网络，它们利用生成对抗网络的语义标签和噪声向量来隐藏秘密数据。我们在 CelebA 数据集上按照默认设置和网络结构重新实现了这两种方法，并将我们的方案与它们的最佳结果进行比较。需要注意的是，Zhang 和 Hu 的准确率数值是根据浮点TIFF图像得出的。图 7 展示了不同方法生成的隐写图像。为评估图像质量，我们在方案中采用无参考评价器自然图像质量评价器[17]。自然图像质量评价器评分越低，图像质量越好。我们使用隐写分析器 Ye-net[15]通过指标 PE 评估所有算法的安全性。在检测中，我们将生成的普通图像（不含秘密数据）和隐写图像（含随机二进制秘密数据）分别作为载体数据集和含密数据集。从结果可以看出，我们提出的 GSF 在几乎所有指标上都显著优于另外两种方法。GSF 的隐藏容量是其他方法的 40 多倍。同时，我们的方案还实现了更高的秘密信息提取准确率、更好的含密图像质量和更高的安全级别。

表 4。所提出的 GSF 与最先进方法的比较。

方法	位/像素 ↑	准确率 (%) ↑	自然图像质量评价器 ↓	PE → 0.5
Zhang([10])	1.22e-3	71.85	56.60	0.48
胡（[11]）	7.32e-2	90.50	14.13	0.49
GSF PNG	**3**	**92.44**	**14.01**	**0.50**
GSF TIFF	**24**	**99.53**	**12.96**	0.44

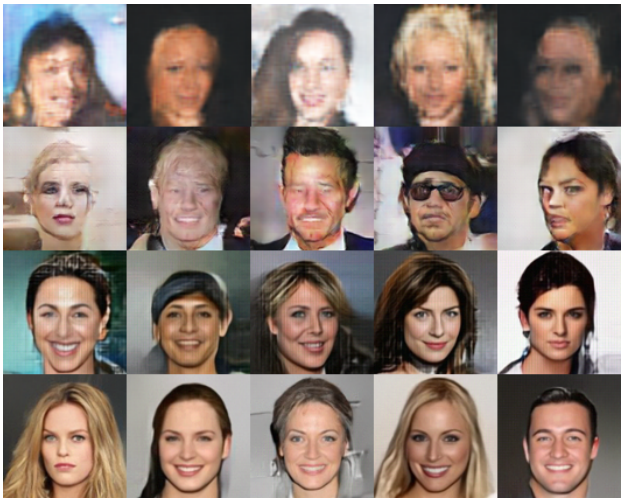


图 7。生成的隐写图像的视觉比较。前两行是 Zhang [10]（载荷：5 位/图像）和 Hu[11]（300 位/图像）生成的隐写图像；后两行是我们的 GSF 生成的 128×128 PNG 和 TIFF 隐写图像，其载荷分别为 3 位/像素（49,152 位/图像）和 24 位/像素（393,216 位/图像）。

4. 结论

本研究提出了一种新颖的基于流的生成式隐写术方案，该方案能够通过单个网络生成逼真的隐写图像，并恢复隐藏的秘密数据。我们首先构建一种可逆双射映射，将秘密数据转换为隐写图像，并通过反向映射准确恢复隐藏的秘密数据。此外，我们还开发了一种新颖的潜变量优化策略，以提升生成隐写图像的保真度。与现有方法相比，我们提出的 GSF 性能更优，在隐藏容量、提取准确率、图像质量和安全性方面均有提升。

致谢： 本工作得到国家自然科学基金项目 U20B2051、62072114、U20A20178 和 U1936214 的资助。

5. 参考文献

[1] Jessica Fridrich,《数字媒体中的隐写术：原理、算法与应用》，剑桥大学出版社，2009年。[2] Mehdi Hussain、Ainuddin Wahid Abdul Wahab、Yamani Idna Bin Idris、Anthony TS Ho 和 Ki-Hyun Jung，《空间域图像隐写术：综述》，《信号处理：图像通信》，第65卷，第46–66页，2018年。[3] Inas Jawad Kadhim、Prashan Premaratne、Peter James Vial 和 Brendan Halloran，《图像隐写术综合综述：技术、评估与未来研究趋势》，《神经计算》，第335卷，第299–326页，2019年。[4] Shumeet Baluja，《在图像中隐藏图像》，《*IEEE*模式分析与机器智能汇刊》，第42卷，第7期，第1685–1697页，2020年。[5] Miroslav Goljan、Jessica Fridrich 和 R´emi Cogranne，《彩色图像隐写分析的富模型》，载于*2014*年*IEEE*国际信息取证与安全研讨会（*WIFS*）。IEEE，2014年，第185–190页。[6] Mehdi Boroumand、Mo Chen 和 Jessica Fridrich，《用于数字图像隐写分析的深度残差网络》，《*IEEE*信息取证与安全汇刊》，第14卷，第5期，第1181–1193页，2018年。[7] Jiaohua Qin、Yuanjing Luo、Xuyu Xiang、Yun Tan 和 Huajun Huang，《无载体图像隐写术：综述》，《*IEEE*开放获取》，第7卷，第171372–171394页，2019年。[8] K Wu 和 C Wang，《使用可逆纹理合成的隐写术》，《*IEEE*图像处理汇刊》，第24卷，第1期，第130–139页，2014年。[9] Sheng Li 和 Xinpeng Zhang，《迈向基于构造的数据隐藏：从秘密数据到指纹图像》，《*IEEE*图像处理汇刊》，第28卷，第3期，第1482–1497页，2018年。[10] Zhuo Zhang、Guangyuan Fu、Rongrong Ni、Jia Liu 和 Xiaoyuan Yang，《一种利用辅助语义通过载体合成实现隐写术的生成方法》，《清华大学学报（英文版）》，第25卷，第4期，第516–527页，2020年。[11] Donghui Hu、Liang Wang、Wenjie Jiang、Shuli Zheng 和 Bin Li，《一种基于深度卷积生成对抗网络的新型图像隐写方法》，《*IEEE*开放获取》，第6卷，第38303–38314页，2018年。[12] Diederik P Kingma 和 Prafulla Dhariwal，《Glow：具有可逆1×1卷积的生成流》，2018年。[13] Kaiming He、Xiangyu Zhang、Shaoqing Ren 和 Jian Sun，《用于图像识别的深度残差学习》，载于*IEEE*计算机视觉与模式识别会议论文集，2016年，第770–778页。[14] Ziwei Liu、Ping Luo、Xiaogang Wang 和 Xiaoou Tang，《野外人脸属性的深度学习》，载于国际计算机视觉会议（*ICCV*）论文集，2015年12月。[15]Jian Ye、Jiangqun Ni 和 Yang Yi，《用于图像隐写分析的层次化表征深度学习》，《*IEEE*信息取证与安全汇刊》，第12卷，第11期，第2545–2557页，2017年。[16] Weike You、Hong Zhang 和 Xianfeng Zhao，《用于图像隐写分析的孪生卷积神经网络》，《*IEEE*信息取证与安全汇刊》，第16卷，第291–306页，2020年。[17] Anish Mittal、Rajiv Soundararajan 和 Alan C Bovik，《构建“完全盲”的图像质量分析器》，《*IEEE*信号处理快报》，第20卷，第3期，第209–212页，2012年。