doi :10.3969/j.issn.1671-1122.2021.04.008

基于同态加密的密文域可逆信息隐藏技术研究

林文兵[1,2]，张敏情[1,2]，周能[1,2]，孔咏骏[1,2]

（1. 武警工程大学密码工程学院，西安 710086；2. 网络与信息安全武警部队重点实验室，西安 710086）

摘　要：为了提高嵌入容量和实现解密与提取信息的可分离性，文章将希尔伯特曲线和同态加密的特性运用到密文域可逆信息隐藏中。首先，图像拥有者对原始图像进行预处理，并在加密后构造密文镜像点。然后，信息隐藏者通过同态加法对目标像素点进行秘密信息嵌入。最后，接收方不仅可以提取秘密信息，还可以无损地恢复原始图像。实验证明，文章方案不但能够实现解密与提取信息的可分离性，而且在保证图像质量的前提下，最大嵌入容量可达到 69120 bits。

关键词：可逆信息隐藏；同态加密；希尔伯特曲线；预测误差扩展

中图分类号：TP309　**文献标志码：**A　**文章编号：**1671-1122（2021）04-0073-08

中文引用格式：林文兵，张敏情，周能，等 . 基于同态加密的密文域可逆信息隐藏技术研究 [J]. 信息网络安全，2021，21（4）：73-80.

英文引用格式：LIN Wenbing, ZHANG Minqing, ZHOU Neng, et al. Research on Technology of Reversible Data Hiding in Encrypted Domain Based on Homomorphic Encryption[J]. Netinfo Security, 2021, 21(4): 73-80.

Research on Technology of Reversible Data Hiding in Encrypted Domain Based on Homomorphic Encryption

LIN Wenbing[1,2], ZHANG Minqing[1,2], ZHOU Neng[1,2], KONG Yongjun[1,2]

(1. *College of Cryptography Engineering, Engineering University of Chinese People Armed Police Force*(*PAP*), *Xi'an* 710086, *China*; 2. *Key Laboratory of Network and Information Security under PAP*, *Xi'an* 710086, *China*)

Abstract: In order to improve the embedding capacity and realize the separability of decryption and information extraction, the algorithm applies the characteristics of Hilbert curve and homomorphic encryption to reversible data hiding in the encrypted domain. First, the image owner preprocesses the original image and constructs the ciphertext mirror point (CMP) after encryption. Then, the data hider embeds the secret information on the target pixel through homomorphic addition. Finally, the receiver can not only extract the secret information, but also restore the original image lossless. Experiments have proved that this scheme can not only realize the separability of decryption and extraction of information, but also the maximum embedding capacity can reach 69120 bits under the guarantee of image quality.

Key words: reversible data hiding; homomorphic encryption; hilbert curve; prediction error expansion

收稿日期：2020-11-06

基金项目：国家自然科学基金 [61872384]

作者简介：林文兵（1993—），男，福建，硕士研究生，主要研究方向为信息隐藏；张敏情（1967—），女，陕西，教授，博士，主要研究方向为信息隐藏、密码学；周能（1993—），男，江苏，硕士研究生，主要研究方向为信息安全；孔咏骏（1990—），男，江苏，博士研究生，主要研究方向为密码学。

通信作者：张敏情 api_zmq@126.com

0 引言

信息隐藏技术[1]是信息安全领域的重要组成部分，用户可以将秘密信息嵌入到原始载体中，接收者可以从带有秘密信息的载体中提取秘密信息。但是，这种方法会对原始载体造成失真，并且在提取数据后无法完全地恢复原始载体。为了解决这一不足，可逆信息隐藏[2, 3]引起了学者们的关注。接收方可以在带有秘密信息的载体中提取秘密信息，并且在信息提取后，原始载体能无损地恢复。通常，典型的可逆信息隐藏算法有无损压缩[4,5]、差值扩展[6-8]和直方图平移[9,10]。为了提高数据安全性，用户通常使用加密算法将明文转换为密文，防止原始数据在不安全的通道或云服务器上公开。因此，密文域可逆信息隐藏成为研究的重点[11-14]。

密文域可逆信息隐藏是在加密图像中嵌入和提取信息，并且可以无损恢复原始图像。通常可分为加密前预留空间和加密后预留空间。加密前预留空间[15]可以提高嵌入容量，但是复杂的预处理增加了系统的运算负担。而加密后预留空间则是对加密图像进行预处理。在文献[16]中，ZHANG利用流密码对图像进行加密，然后通过翻转对应组中每个像素点的最低有效位，从而进行秘密信息的嵌入。在文献[17]中，HONG等人通过更好地利用空间相关性来改进ZHANG的方法。在文献[18]中，ZHANG提出一种可分离的密文域可逆信息隐藏，它可以直接在密文或明文上提取秘密信息。然而，以上算法都是通过对称密码进行加密。

2014年，CHEN[19]等人首次将公钥密码系统引进密文域可逆信息隐藏中。在文献[20]中，ZHANG等人利用Paillier算法对图像进行加密，并通过多层湿纸编码[21]将秘密信息嵌入加密图像中。在文献[22]中，XIANG等人运用同态的性质，提出一种基于镜像密文组的密文域可逆信息隐藏，其核心是通过加密前预留空间，并运用Paillier算法的同态特性，构造镜像密文组进行数据嵌入。

基于文献[22]的启发，为了提高可嵌像素点的利用率，本文将希尔伯特曲线和同态特性运用到密文域可逆信息隐藏。首先，图像拥有者将原始图像划分成3个部分：A，B和C，并运用希尔伯特曲线对图像A部分进行预处理。同时，为了预留嵌入空间，运用预测误差扩展算法，将A部分中参考像素的最低有效位和目标像素的所有位嵌入到B部分中，并在加密前将参考像素的最低有效位置零，目的是避免溢出。对图像进行加密后，将A部分中的所有目标像素替换为参考像素，以此构造密文镜像点。其次，信息隐藏者可以通过同态加法将加密的秘密信息嵌入到目标像素的最低有效位中，并且参考像素保持不变。最后，接收方通过构造的密文镜像点不仅可以实现可分离提取秘密信息，还能完全恢复原始图像。

1 相关知识

1.1 预测误差扩展

预测误差扩展[8]是将图像分成重叠的块，每个块由5个像素点组成。其中，中间像素点$p_{i,j}$用于数据嵌入，并且通过与其相邻的4个像素点计算出预测值。具体步骤如下：

1）数据嵌入处理

通过公式（1）对中间像素点$p_{i,j}$的4个相邻像素值求平均值，可以得到预测像素值$p'_{i,j}$。

$$p'_{i,j}=\left\lfloor \frac{p_{i,j-1}+p_{i,j+1}+p_{i-1,j}+p_{i+1,j}}{4} \right\rfloor \quad (1)$$

通过原始像素值减去预测像素值，可以得到预测误差值$e_{i,j}$，如公式（2）所示。

$$e_{i,j}=p_{i,j}-p'_{i,j} \quad (2)$$

通过差值扩展算法，将1 bit数据b嵌入到预测误差值中，可以得到嵌入信息后的预测误差值$e'_{i,j}$，如公式（3）所示。

$$e'_{i,j}=2\times e_{i,j}+b \quad (3)$$

当满足可嵌入条件时，每个块都可以嵌入秘密信息。嵌入信息后，可以得到嵌入信息后的像素值$P_{i,j}$，如公式（4）所示。

$$P_{i,j}=e'_{i,j}+p'_{i,j} \quad (4)$$

2）信息提取处理

在信息提取的处理中，由于相邻像素值保持不变，因此接收方可以通过计算获得与图像所有者相同的预测值。然后，根据接收到的嵌入信息后的像素值$P_{i,j}$，可以通过公式（5）计算出嵌入信息后的预测误差值。

$$e'_{i,j} = P_{i,j} - p'_{i,j} \tag{5}$$

根据所获得的预测误差值，可以计算出嵌入信息b，如公式（6）所示。

$$b = e'_{i,j} \bmod 2 \tag{6}$$

同时，还可以根据预测误差值来计算原始预测误差值$e'_{i,j}$，如公式（7）所示。

$$e_{i,j} = \left\lfloor \frac{e'_{i,j}}{2} \right\rfloor \tag{7}$$

最后，可以计算出原始像素值$p_{i,j}$，如公式（8）所示。

$$p_{i,j} = p'_{i,j} + e_{i,j} \tag{8}$$

3）防止溢出处理

使用预测误差扩展算法进行可逆信息嵌入可能会导致溢出问题。为了避免溢出问题，设置了一个阈值，如公式（9）所示。

$$\rho = \{0 \leqslant e_{i,j} + p_{i,j} \leqslant 254\} \tag{9}$$

在嵌入数据前，需要对原始图像进行预处理。如果遇到不满足阈值条件的像素点，则无法嵌入数据。同时，记录它们的相应位置。

1.2 Paillier 密码系统

Paillier密码系统[23]具有同态和概率性质，其安全性基于大型整数分解的困难性，并且已广泛用于安全计算。Paillier加密算法包括以下部分：

1）密钥生成

随机选择两个大质数p和q，计算$N=pq$和$\lambda=lcm(p-1,q-1)$。然后，选取$g\in Z^*_{N^2}$，使其满足$\gcd(L(g^\lambda \bmod N^2), N)=1$。其中，$L(x)=\frac{x-1}{N}$，$Z^*_{N^2}=\{1,2,\cdots,N^2-1\}$。最后，可得出公钥为$(N,g)$，私钥为$(p,q)$。

2）加密过程

对于给定信息$m\in Z^*_N$，信息隐藏者可以随机选择$r\in Z^*_N$，并通过公式（10）进行加密，得到密文c。

$$c = g^m r^N \bmod N^2 \tag{10}$$

3）解密过程

当接收方收到密文c时，可通过公式（11）得到明文m。

$$m = \frac{L(c^\lambda \bmod N^2)}{L(g^\lambda \bmod N^2)} \bmod N \tag{11}$$

2 算法设计

虽然文献[22]能够实现可分离提取信息，但是嵌入容量不是很高，导致在远程医疗、军事图像处理等领域中会有一定的局限性。因此，本文将希尔伯特曲线和同态特性运用到密文域可逆信息隐藏，提高了图像的嵌入容量、扩展了应用场景，其框架如图1所示。

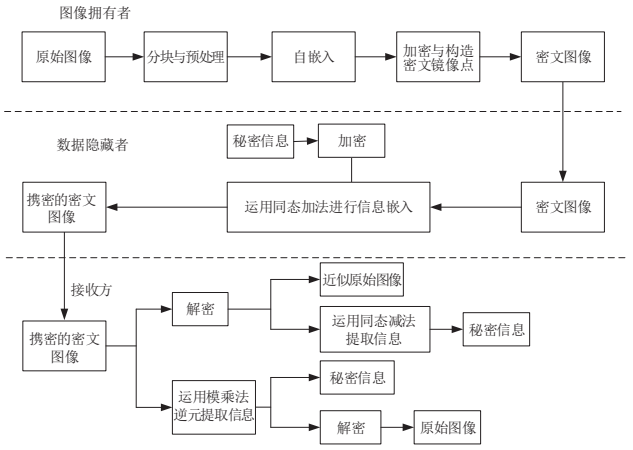


图 1 方案总体框架

2.1 图像加密

2.1.1 图像分块和希尔伯特曲线预处理

首先，图像拥有者将原始图像分为3个部分：A，B和C。同时，将图像A部分划分成尺寸大小为8×8且不重叠的各个分块。再运用三级希尔伯特曲线对图像A部分的各个分块进行预处理，并标记相应像素点的编号。如图2所示，以希尔伯特曲线对各个分块进行预处理，会得到一条固定的轨迹。同时，以16个像素点为一组，其中包括15个目标像素点和1个参考像素点。由于图像间具有相关性，因此参考像素点的编号为$P_r=8+16k$，k的取值为0，1，2，3。与文献[22]相比，本文算法一方面提高了参考像素点的隐蔽性，另一方

面增加了可嵌像素点的利用率。

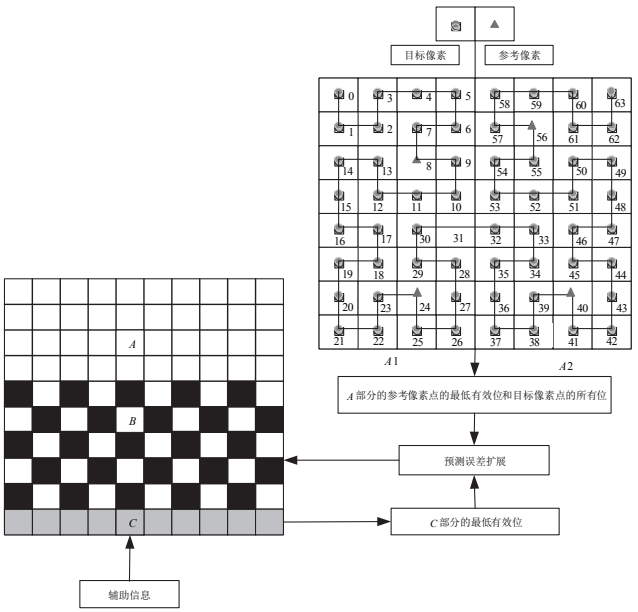


图 2 图像分块与自嵌入

2.1.2 自嵌入和预留空间

将A部分中参考像素点的最低有效位和目标像素的所有位嵌入到B部分之前，图像拥有者需要对B部分进行防溢出处理，并标记相应的位置L_m。如图2所示，为了腾出嵌入信息的空间，通过预测误差扩展算法，将A部分中参考像素点的最低有效位和目标像素的所有位，以及C部分的最低有效位嵌入到B部分。然后，将位置图L_m和参考像素点的编号嵌入到C部分的最低有效位中作为辅助信息，从而获得修改后的图像。

2.1.3 加密和构造镜像密文点

将参考像素点的最低有效位重置为零，目的是避免嵌入信息时造成溢出。然后，图像拥有者运用Paillier算法对修改后的图像进行加密，并在密文域中构建镜像密文点，即将同一组中所有目标像素替换为参考像素，保证信息提取的可逆性。

2.2 数据嵌入

为了增强安全性，数据隐藏者选择一个随机整数$r_{s_w}(r_{s_w}<n)$，并运用Paillier算法对秘密信息进行加密，从而获得加密的秘密信息C_{S_w}，如公式（12）所示。

$$C_{S_w}=g^{S_w}r_{s_w}{}^{N}\bmod N^2 \tag{12}$$

与图像拥有者一样，密文图像分为3个部分：A_E，B_E和C_E。数据隐藏者将加密的秘密信息嵌入到A_E部分中目标像素点的最低有效位，通过公式（13）可获得带有秘密信息的加密图像I_{S_w}。然后，将加密密钥和信息隐藏密钥嵌入C部分中，作为辅助信息。

$$I_{S_w}=g^{I'+S_w}(rr_{s_w})^N \bmod N^2 \tag{13}$$

2.3 信息提取与图像还原

2.3.1 密文域中提取秘密信息

接收方采用和图像拥有者相同的方式对携密的密文图像进行分块后，利用希尔伯特曲线进行遍历并标记相应位置。然后，根据C部分的辅助信息，利用公式（14）对秘密信息进行提取。

$$\Theta\cdot y=1\bmod z \tag{14}$$

其中，y和z是互素整数，且$y<z$；Θ是y的模乘法逆元。

2.3.2 明文域中提取秘密信息

接收方通过私钥直接对带有秘密信息的加密图像进行解密，并以图像拥有者相同的方式对携密的密文图像进行分块。然后，利用希尔伯特曲线构造的镜像密文点，实现在明文域中运用同态减法来获取秘密信息，如公式（15）所示。

$$S_w=P''_h-P''_r \tag{15}$$

2.3.3 图像还原

提取完秘密信息后，根据提取出的辅助信息，运用预测误差扩展方法对A部分和C部分中相关的像素值进行还原，从而无损地恢复原始图像。

3 实验结果与分析

为了测试本文算法性能，选用USC-SIPI图像库中大小为512×512的256级灰度图像进行实验。实验环境为Windows10操作系统，CPU型号为Intel(R) Core(TM) i7-8550U，内存大小为16GB，实验仿真软件为MATLAB R2018a。同时，从4个方面进行分析：参数选取、可逆性、安全性和性能比较。

3.1 参数选取

为了测量处理后的图像质量，通常采用峰值信噪

比（*PSNR*）来进行客观评估，如公式（16）所示。

$$PSNR = 10 \times \log_{10} \frac{255^2}{MSE} \quad (16)$$

其中，*MSE* 是原始图像和已处理图像之间差异的平方的期望值，由公式（17）可以计算出。

$$MSE = \frac{1}{M \times N} \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} \left[p(i,j) - c(i,j) \right]^2 \quad (17)$$

其中，$M \times N$ 表示图像的大小；$p(i,j)$ 表示原始图像的像素值；$c(i,j)$ 表示处理后图像的像素值。表 1 是在不同图像中不同参数 n 的嵌入容量和 *PSNR* 值列表，可以看出，在相同的嵌入量下，随着不同图像中参数 n 的变化，峰值信噪比也随之变化。其中，n 表示的是目标像素中用来嵌入秘密信息的最低有效位的个数。因此，在相同的嵌入容量下，随着不同图像中参数 n 的增加，峰值信噪比也相应增加。但是，当 n=4 时，在构造镜像密文点时引入了更多的失真，从而导致图像的峰值信噪比减小。因此，当参数 n=3 时，图像的峰值信噪比最好。表 2 表示的是在参数 n=3 的条件下，三级希尔伯特曲线中由不同个数的像素点组成，随着嵌入容量的增加，峰值信噪比也会相应变化。由表 2 得到，当遍历 16 个像素点并将其组成一个组时，图像的峰值信噪比最好。

综上所述，当 n=3、m=16 时，嵌入信息后图像的性能最好。

3.2 可逆性分析

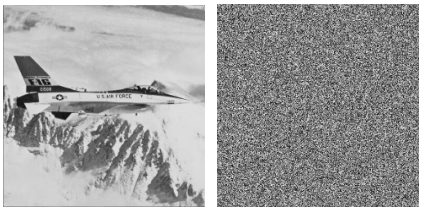
可逆性是可逆信息隐藏的基本要求，实验测试以标准图像 Plane 作为实验载体。同时，将秘密信息转化为二进制字符串，其长度为 69120 bits。本文算法可逆性示意如图 3 所示，a）表示图像尺寸大小为 512×512 的原始图像 ；b）表示嵌入秘密信息后的携密密文图像 ；c）表示直接解密的携密图像，其图像的峰值信噪比是 35.288 dB ；d）表示正确提取嵌入信息后的恢复图像。经过数据对比，恢复图像与原始图像一致。实验表明，本文算法不仅能够正确提取出嵌入信息，还能无损地恢复原始图像。

表 1 不同图像中嵌入容量和 *PSNR* 值对比

PSNR/dB								
图像	n	嵌入容量 /bpp						
		0.015	0.029	0.044	0.059	0.073	0.088	0.103
Lena	1	48.40	45.07	42.22	40.10	38.44	37.19	36.21
	2	54.27	51.39	48.54	46.15	45.31	43.87	42.64
	3	54.92	51.98	49.12	47.59	45.64	44.40	43.65
	4	52.11	49.31	47.45	45.21	44.27	42.47	41.16
Hill	1	51.60	45.65	41.36	38.50	36.44	34.98	34.24
	2	52.42	51.34	48.03	45.52	43.18	41.27	39.77
	3	53.18	52.04	50.65	47.44	46.54	45.31	43.56
	4	52.74	51.50	49.09	46.80	45.51	44.85	42.82
Plane	1	42.66	41.04	39.33	37.51	36.08	35.33	34.78
	2	46.65	42.65	41.88	41.01	40.21	39.31	38.16
	3	47.55	45.28	42.50	41.85	41.66	40.88	40.21
	4	47.37	44.63	41.59	40.88	39.22	39.03	38.64
Man	1	43.79	40.92	39.53	38.28	37.29	36.47	35.84
	2	45.73	43.80	41.88	40.08	39.50	38.68	37.54
	3	46.57	44.22	42.68	40.83	40.05	39.25	38.33
	4	46.28	43.03	41.72	39.90	38.95	38.01	37.83

表 2 希尔伯特曲线中不同参数 m 的 *PSNR* 值（n=3）

嵌入容量 / bits	*PSNR*/ dB			
	m = 4	m = 8	m = 16	m = 32
3 840	38.780	54.179	54.922	54.053
7 680	35.901	51.160	51.984	50.774
11 520	33.623	46.931	49.118	46.691
15 360	32.483	45.934	46.587	45.670
19 200	31.648	45.141	45.636	44.997
23 040	30.715	43.991	44.401	43.148
26 880	30.093	43.285	43.651	42.539
30 720	29.569	42.569	42.872	41.869
46 080	27.709	39.654	39.731	38.732
69 120	25.956	36.329	36.899	35.903



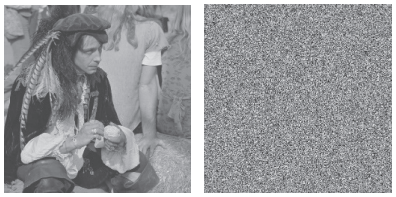
a）原始图像　　b）携密密文图像

c）直接解密的图像　　d）恢复图像

图 3 本文算法可逆性示意

3.3 安全性分析

本文利用Paillier算法对图像进行加密，并运用同态的性质进行秘密信息的嵌入，使其具有同态和概率性质。因此，如果没有私钥，是很难破解的。为了验证Paillier算法加密的安全性和抗攻击能力，通过实验分析了加密图像的直方图和相关性。原始图像和加密图像如图4所示。

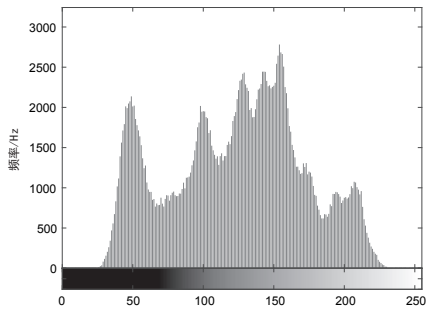


a）原始图像　　b）加密图像

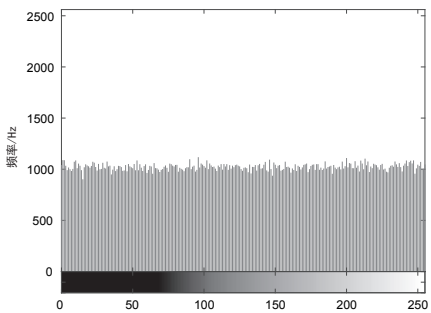
图 4 原始图像与加密图像

与原始图像不同，加密图像的直方图均匀分布，并利用 $hist_i(i=0,1,\cdots,255)$ 来表示图像的直方图。运用公式（18）可得到原始图像和加密图像的直方图分布，如图5所示。

$$S=\frac{1}{256}\sum_{i=0}^{255}(hist_i-\frac{1}{256}\sum_{i=0}^{255}hist_i) \tag{18}$$



a）原始图像



b）加密图像

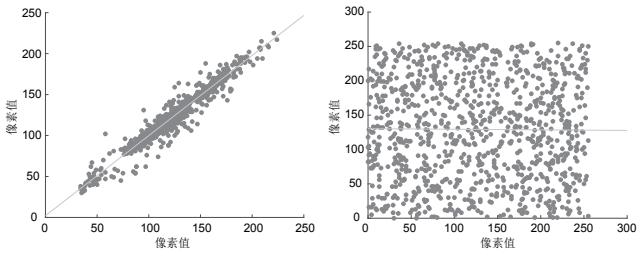
图 5 原始图像和加密图像的直方图分布

如图5所示，一般情况下，原始图像的直方图分布具有较大的波动性。但是，加密图像的直方图分布是均匀的、一致的。因此，原始图像经过加密后得到的加密图像是安全的。

通常原始图像之间存在一定的相关性，而加密图像的相关系数在理论上是等于0。其相关系数值可通过公式（19）得到。

$$\rho_{XY}=\frac{\mathrm{Cov}(X,Y)}{\sqrt{D(X)}\sqrt{D(Y)}} \tag{19}$$

其中，X 表示原始图像，Y 表示加密图像，Cov 表示协方差，D 表示方差。通过实验，原始图像与加密图像的相关性如图 6 所示。



a）原始图像　　b）加密图像

图 6 原始图像与加密图像的相关性

如图6所示，原始图像的分布具有一定的规律性，而加密图像则是随机分布，不会发生信息泄露。

3.4 性能比较

本节主要对本文算法与相关文献的主要性能进行比较，如表3所示。在文献[20]中，ZHANG等人使用多层湿纸编码将秘密信息嵌入到加密图像中，该算法的计算复杂度为 $O(k^3)$，其中 k 是秘密信息的数量。在文献[22]中，XIANG等人使用同态加法将秘密信息嵌入密文图像。而本文的方案中，镜像密文点是在加密之后构造的，并通过同态加法将秘密信息嵌入到密文图像中。与文献[22]相比，本文算法不仅提高了参考像素点的隐蔽性，而且增加了可嵌像素点的利用率。同时，本文算法和文献[22]的计算复杂度一致。

当参数 n=3时，不同图像在不同嵌入量下的峰值信噪比如表4所示。其中，n 表示的是目标像素中用来嵌入秘密信息的最低有效位的个数。

表 3 不同文献的性能比较

文献	性能特征			
	是否可逆	是否可分离	计算复杂度	信息嵌入保护机制
文献 [20]	是	是	$O(k^3)$	多层湿纸编码
文献 [22]	是	是	$O(k)$	Paillier 的同态特性
本文算法	是	是	$O(k)$	Paillier 的同态特性

表 4 在 n=3 下的嵌入容量和 *PSNR*

嵌入容量 / bits	*PSNR*/ dB			
	Lena	Hill	Man	Plane
3840	54.922	53.179	46.566	47.549
7680	51.984	52.038	44.221	45.280
11520	49.118	50.647	42.683	42.502
15360	46.587	47.444	40.833	41.851
19200	45.636	46.538	40.051	41.655
23040	44.401	45.310	39.246	40.883
26880	43.651	43.555	38.326	40.214
30720	42.872	42.558	37.616	39.924
46080	39.731	38.759	35.176	37.536
69120	36.899	35.107	33.114	35.288

从表4可知，随着嵌入容量的增加，图像的峰值信噪比也随之下降。在保证图像质量的前提下，最大嵌入容量为69120 bits秘密信息。

图7以Lena图像为例，表示本文算法与文献[20]和文献[22]在不同嵌入容量下峰值信噪比的比较。

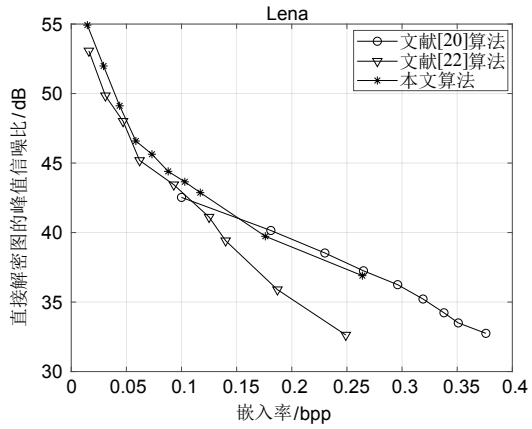


图 7 不同嵌入容量下的峰值信噪比比较

文献[20]通过在加密前缩小图像直方图来预留嵌入空间，这样会引入失真。同时，该方案将秘密信息嵌入到像素的最低有效位中，可能存在像素值被替换的风险。文献[22]在构造镜像密文组时，随着自嵌入量的增加，直方图移位的数量也增加，从而导致更大的失真。从图7中可以看出，运用希尔伯特曲线预处理后，在嵌入容量较高时，本文算法要优于文献[22]。同时，与文献[20]相比，本文算法通过同态加法嵌入数据，因此不存在像素被替换的风险。

4 结束语

本文算法通过希尔伯特曲线进行预处理，一方面使参考像素点的隐蔽性更好，另一方面使可嵌的像素点增加，从而提高了最大嵌入容量。同时，运用Paillier算法进行加密，不但能够构造镜像密文点将秘密信息嵌入到加密图像中，实现了可分离提取秘密信息，而且在理论上确保加密算法的安全性。此外，未来可以在运用同态加密时，在减少密文的扩张和降低计算复杂度上进一步研究，提高加密算法的时效性。

参考文献：

[1] WANG Lina, ZHANG Huanguo, YE Dengpan, et al. Information Hiding Technology and Application[M]. Wuhan: Wuhan University Press, 2012.
王丽娜，张焕国，叶登攀，等. 信息隐藏技术与应用 [M]. 武汉 : 武汉大学出版社，2012.
[2] SHI Yunqing, LI Xiaolong, ZHANG Xinpeng, et al. Reversible Data Hiding: Advances in The Past Two Decades[J]. IEEE Access, 2016, 4(5): 3210−3237.
[3] LI Xiaolong, LI Bin, YANG Bin, et al. General Framework to Histogram Shifting Based Reversible Data Hiding[J]. IEEE Trans on Image Processing, 2013, 22(6): 2181−2191.
[4] FRIDRICH J, GOLJAN M, DU R. Lossless Data Embedding New Paradigm in Digital Watermarking[J]. EURASIP Journal on Advances in Signal Processing, 2002, 2002(2): 185−196.
[5] CELIK M U, SHARMA G, TEKALP A M, et al. Lossless Generalized LSB Data Embedding[J]. IEEE Trans on Image Processing, 2005, 14(2): 253−266.
[6] TIAN Jun. Reversible Data Embedding Using a Difference Expansion[J]. IEEE Trans on Circuits and Systems for Video Technology, 2003, 13(8): 890−896.
[7] SUBBURAM S, SELVAKUMAR S, GEETHA S. High Performance Reversible Data Hiding Scheme Through Multilevel Histogram Modification in Lifting Integer Wavelet Transform[J]. Multimedia Tools and Applications, 2018, 77(6): 7071−7095.
[8] QIU Yingqiang, QIAN Zhenxing, YU Lun. Adaptive Reversible Data Hiding by Extending The Generalized Integer Transformation[J]. IEEE Signal Processing Letters, 2016, 23(1): 130−134.

[9] PAN Zhibin, HU Sen, MA Xiaoxiao, et al. Reversible Data Hiding Based on Local Histogram Shifting with Multilayer Embedding[J]. Journal of Visual Communication and Image Representation, 2015, 31(8): 64–74.
[10] LI Xiaolong, ZHANG Weiming, GUI Xinlu, et al. Efficient Reversible Data Hiding Based on Multiple Histograms Modification[J]. IEEE Transactions on Information Forensics and Security, 2017, 10(9): 2016–2027.
[11] GE Haoli, CHEN Yan, QIAN Zhenxing, et al. A High Capacity Multi-level Approach for Reversible Data Hiding in Encrypted Images[J]. IEEE Transactions on Circuits and Systems for Video Technology, 2019, 29(8): 2285–2295.
[12] YIN Zhaoxia, XIANG Youzhi, ZHANG Xinpeng, et al. Reversible Data Hiding in Encrypted Images Based on Multi-MSB Prediction and Huffman Coding[J]. IEEE Transactions on Multimedia, 2020, 22(4): 874–884.
[13] YI Shuang, 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.
[14] MALIK A, WANG Hongxia, CHEN Yanli, et al. A Reversible Data Hiding in Encrypted Image Based on Prediction-error Estimation and Location Map[J]. Multimedia Tools and Applications, 2020, 79(1): 11591–11614.
[15] PUTEAUX P, PUECH W. An Efficient MSB Prediction-based Method for High-capacity Reversible Data Hiding in Encrypted Images[J]. IEEE Transactions on Information Forensics and Security, 2018, 18(6): 1–12.
[16] ZHANG Xinpeng. Reversible Data Hiding in Encrypted Image[J]. IEEE Signal Processing Letters, 2011, 18(4): 255–258.
[17] HONG Wen, CHEN Tingshou, WU Hanyan. An Improved Reversible Data Hiding in Encrypted Images Using Side Match[J]. IEEE Signal Processing Letters, 2012, 19(4): 199–202.
[18] ZHANG Xinpeng. Separable Reversible Data Hiding in Encrypted Image[J]. IEEE Trans on Information Forensics and Security, 2012, 7(2): 526–532.
[19] CHEN Yuchi, SHI Chihei, HORNG Gwoboa. Encrypted Signal-based Reversible Data Hiding with Public Key Cryptosystem[J]. Journal of Visual Communication and Image Representation, 2014, 25(5): 1164–1170.
[20] ZHANG Xinpeng, LONG Jing, WANG Zichi, et al. Lossless and Reversible Data Hiding in Encrypted Images with Public Key Cryptography[J]. IEEE Trans on Circuits and Systems for Video Technology, 2016, 26(9): 1622–1631.
[21] FRIDRICH J, GOLJAN M, LISONEK P, et al. Writing on Wet Paper[J]. IEEE Trans on Signal Processing, 2005, 53(10): 3923–3935.
[22] XIANG Shijun, LUO Xinrong. Reversible Data Hiding in Homomorphic Encrypted Domain by Mirroring Ciphertext Group[J]. IEEE Trans on Circuits and Systems for Video Technology, 2018, 28(11): 3099–3110.
[23] PAILLIER P. Public-key Cryptosystems Based on Composite Degree Residuosity Classes[J]. Proceeding of the Advances Cryptology, 1999, 92(4), 223–238.