基于密码反馈秘密共享的大容量密文域可逆隐藏

张敏情[1,2]，姜超[1,2]，狄富强[1,2]，蒋宗宝[1,2]，张雄[1,2]
（1. 武警工程大学密码工程学院，陕西 西安 710086；2. 中国人民武装警察部队密码与信息安全保密重点实验室，陕西 西安 710086）

摘 要：为提高分布式环境下密文域可逆信息隐藏算法的安全性、鲁棒性和嵌入率，提出了一种基于密码反馈秘密共享的多重嵌入算法。首先，利用秘密共享加密过程中产生的多项式冗余系数进行嵌入；其次，利用秘密共享的同态加性对秘密份额二次嵌入。实验结果表明，所提算法利用反馈机制提高了秘密共享的扩散特性从而增强了算法安全性和鲁棒性，在(3,4)和(3,5)门限下，嵌入率分别为 6.00 bpp 和 4.80 bpp。所提算法具有安全性高、完全可逆、嵌入率较大等特点；算法嵌入率不受载体图像影响，仅与算法参数选择有关。

关键词：信息隐藏；可逆；密文图像；秘密共享；密码反馈
中图分类号：TP309.7
文献标志码：A
DOI: 10.11959/j.issn.1000−436x.2023170

High capacity reversible hiding in encrypted domain based on cipher-feedback secret sharing

ZHANG Minqing[1,2], JIANG Chao [1,2], DI Fuqiang[1,2], JIANG Zongbao[1,2], ZHANG Xiong[1,2]
1. College of Cryptography Engineering, Engineering University of PAP, Xi'an 710086, China
2. Key Laboratory of PAP for Cryptology and Information Security, Xi'an 710086, China

Abstract: To improve the security, robustness and embedding rate of reversible hiding in encrypted domain in the distributed environment, a multiple embedding algorithm based on cipher-feedback secret sharing was proposed. Firstly, the additional data were embedded into the polynomial coefficients redundancy generated in the process of secret image sharing. Secondly, the extra secrets were embedded by using the additive homomorphism of secret sharing. Experimental results demonstrate that a better security and robustness has been obtained by improving the diffusion characteristic of secret sharing using the feedback mechanism. In the (3,4) and (3,5) threshold, the embedding rates can reach 6.00 bit per pixel and 4.80 bit per pixel respectively. The proposed algorithm can not only maintain the strong security and separability, but also obtain a better embedding capacity. Meanwhile, the embedding rate of the scheme is not affected by the carrier image and is only related to the selection of algorithm parameters.

Keywords: data hiding, reversible, encrypted image, secret sharing, cipher-feedback

0 引言

密文域可逆信息隐藏（RDH-ED, reversible data hiding in encrypted domain）[1]首先对载体加密，然后利用载体图像的冗余空间隐藏秘密，不仅可以隐蔽传输信息，还能可逆提取秘密信息和无失真恢复原始载体。RDH-ED 对于保护信息的安全性、准确性和完整性具有十分重要的作用。RDH-ED 的关键是生成冗余空间，目前主流的生成冗余方式可分为加密后生成冗余（VRAE, vacating room after en-

收稿日期：2023−05−22；**修回日期：**2023−08−14
通信作者：姜超，18740458410@163.com
基金项目：国家自然科学基金资助项目（No.62272478, No.62102450, No.61872384, No.62102451, No.62202496）
Foundation Item: The National Natural Science Foundation of China (No.62272478, No.62102450, No.61872384, No.62102451, No.62202496)

cryption）、加密前生成冗余（VRBE, vacating room before encryption）和加密中生成冗余（VRIE, vacating redundancy in encryption）。

基于 VRAE[2-10]的 RDH-ED 利用密文图像无损压缩或同态加密等技术生成冗余，通过修改密文比特实施嵌入，可实现无损提取和可逆恢复。由于加密过程破坏了数据之间的相关性，因此密文域冗余较少，嵌入率（ER, embedding rate）受限，同时存在载体难以恢复、可分离性差等缺点。基于 VRBE[11-20]的 RDH-ED 主要通过像素预测、压缩、编码等技术对原始图像预处理，利用像素间的相关性产生的冗余空间实施嵌入，其嵌入率通常较大，但其预处理过程过于烦琐，应用场景受限。

为解决以上问题，文献[21-22]首次提出基于 VRIE 的 RDH-ED 方案，将 LWE（learning with error）和 R-LWE（ring-learning with error）算法用于 RDH-ED，通过量化密文空间并利用密文扩展产生的冗余提升了嵌入率。Huang 等[23]在加密过程中预测像素，通过相应的误差修改密文像素以产生冗余，实现了可逆嵌入。相比于 VRAE 和 VRBE，VRIE[24]直接在加密过程中发掘并利用冗余，可以将信息隐藏和密码技术有机融合，提高 RDH-ED 的安全性、可逆性以及嵌入率，但是 VRIE 适用的密码算法有限，设计难度较大。

以上方案大多适于单一用户，针对当前云环境的普及应用，设计适于分布式场景的 RDH-ED 是当前亟待解决的重点问题。秘密共享（SS, secret sharing）[25]的门限效应使其具有较好的容灾性，适用于分布式场景。分布式场景下的秘密共享如图 1 所示，云服务器即秘密拥有者将秘密分割成多个秘密份额，分发至 n 个不同用户分布存储，收集任意大于或等于 k 个不同份额可以恢复秘密，否则无法恢复。

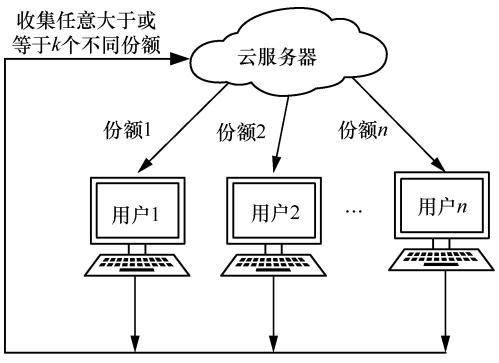


图 1　分布式场景下的秘密共享

Wu 等[26]首次提出基于秘密共享的 RDH-ED 算法，充分发挥了容灾作用。周能等[27-28]在秘密共享的基础上，同时利用同态加法嵌入和差值扩展嵌入，提升了嵌入率。Ke 等[29]和 Qin 等[30]基于中国剩余定理和秘密共享分别提出的 RDH-ED 具有较好的可分离性和解密图像质量。王泽曦等[31]利用秘密共享加密过程中产生的多项式冗余系数嵌入信息，进一步提高了嵌入率。Qin 等[32]基于秘密共享提出了 GF（Galois field）(p)和 GF(2^8)上的 RDH-ED，具有较低的失真率。为解决传统秘密共享方案不具扩散特性的缺点，Hua 等[33-34]基于密码反馈秘密共享（CFSS, cipher-feedback secret sharing）提出了 2 种 RDH-ED，通过对密文图像像素值预测编码，实现了较高的嵌入率和安全性。然而，随着分布式场景下越来越多载体被分发到云空间，由于分布式存储的脆弱性，图像拥有者希望在提供隐藏载体的同时，实现版权信息的嵌入以保护合法权益。针对此问题，张敏情等[35]利用多项式秘密共享实现了密文域多重嵌入，分别利用多项式嵌入和同态嵌入，进一步提高了嵌入率。将秘密共享应用于密文域可逆信息隐藏，可以提高算法的容灾性和嵌入率，能够适应分布式环境的需求。

然而，以上方案仍存在嵌入容量（EC, embedding capacity）受限，易遭受差分攻击、选择明文攻击等问题。为此，本文提出了一种基于 CFSS 的多重嵌入算法，首先对置乱后的载体图像分块，利用 CFSS 对图像块加密，并随机选取上一载体块的一个份额与下一载体块共同共享，同时利用多项式的冗余系数嵌入额外信息；然后利用秘密共享的同态加性，对分割后的秘密份额二次嵌入。实验结果表明，本文方案具有安全性高、完全可逆、嵌入率较大等特点。同时，算法嵌入率不受载体图像影响，仅与算法参数选择有关。

1　基础知识

1.1　秘密共享

Shamir[25]提出了基于 Lagrange 插值多项式的(r,n)秘密共享方案，秘密拥有者通过构建一元多项式将秘密分成 n 份，接收方收集任意大于或等于 r 个份额即可重构多项式恢复秘密。

定理 1　任选互不相同的 r 个(x_i,$w(x_i)$)，可由 Lagrange 插值公式唯一确定 r−1 次多项式，即

$$\Upsilon(x)=\sum_{i=1}^{r}w(x_i)\prod_{j=1,j\neq i}^{r}\frac{x-x_j}{x_i-x_j} \tag{1}$$

发送方构造 $r-1$ 次多项式如下

$$R(x)=\mathrm{se}+d_1x+d_2x^2+\cdots+d_{r-1}x^{r-1} \tag{2}$$

其中，se 为秘密，$d_1,d_2,\cdots,d_{r-1}$ 为随机数。发送方计算秘密份额 $s_i=R(i)$, $i=1,2,\cdots,n$，并将 s_i 分发至 n 个不同的用户 U_i。由定理 1 可知，收集任意 r 个互不相同的份额 s_i，即可重构 $R(x)$，相应地，秘密 se 即可被恢复。

1.2 基于输出反馈机制的秘密共享

由于秘密共享具有门限效应和同态效应，因此被广泛应用于云服务、远程通信等分布式场景。但是现有的秘密共享方案不具备扩散特性，不能有效抵抗差分攻击、选择明文攻击等。文献[33]提出的 CFSS 方案能够有效解决此类问题，其加密过程如图 2 所示，表达式为

$$R_i(x)=\begin{cases}R_0x^{r-1}+\sum_{l=0}^{r-2}d_lx^l, & i=1\\ R_{i-1}(j)x^{r-1}+\sum_{l=0}^{r-2}d_lx^l, & i\geqslant 2\end{cases} \tag{3}$$

其中，$R_i(x)$表示对第 i 块图像 CFSS 加密，其中，$d_0,d_1,\cdots,d_{r-2}$, $R(0)$为随机数，$R_{i-1}(j)$为第 $i-1$ 个共享的秘密份额中随机选取的第 j 个份额。对每块图像构建多项式加密时，都有一个系数来自上一块图像的共享份额，第 1 块中的 R_0 为随机数，采用这种反馈策略，当秘密图像中的一个比特被篡改时，其他份额都会产生较大的变化，可以有效抵抗差分攻击等多种攻击。因此 CFSS 方案可以有效解决传统方案的缺陷，具有较高的安全性和鲁棒性。

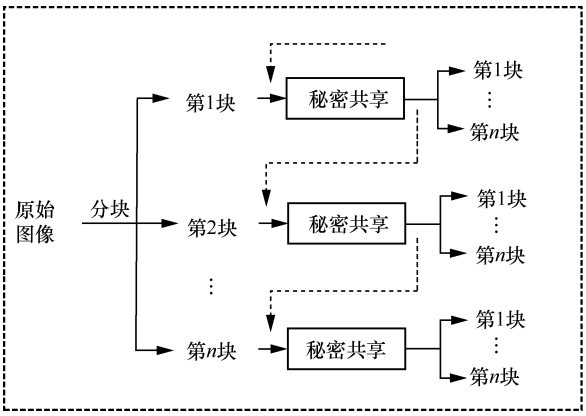


图 2 CFSS 方案加密过程

1.3 同态加性

对于 2 个门限为(r,n)的秘密共享方案，对其密文相加等效于对明文相加后再秘密共享，即秘密共享具有同态加性。假设构造 2 个多项式如下

$$R'(x)=\sum_{\mu=0}^{r-1}\lambda_\mu x^\mu,\ R''(x)=\sum_{\mu=0}^{r-1}\nu_\mu x^\mu \tag{4}$$

其中，$\lambda_\mu,\nu_\mu\in\mathrm{GF}(q^c)$，$\mu=(0,1,\cdots,r-1)$，其同态加性可表示为

$$R'(x)+R''(x)=\sum_{\mu=0}^{r-1}(\lambda_\mu+\nu_\mu)x^\mu \tag{5}$$

根据式(1)，可由 Lagrange 插值公式重构各项系数 $\lambda_\mu+\nu_\mu$。因为 λ_μ,ν_μ 均可取 0，所以当 $r_1\neq r_2$ 时，门限为(r_1,n)和(r_2,n)的秘密共享方案仍然满足同态加性。

2 算法设计

2.1 算法框架

云环境下的数据管理存在易被攻击的安全隐患，用户在传递信息过程中，不仅要求信息内容保密，还要保证信息传递行为不被泄露，所以将秘密信息隐藏在载体中传递。同时，部分图像拥有者也要求载体图像的机密性和完整性得到有效保护，需向其中添加相应的版权、身份标识等认证信息。针对以上问题，本文提出了多重嵌入算法，其框架如图 3 所示。首先，利用 CFSS 对载体图像加密，并在加密过程中利用多项式系数冗余实施嵌入，此处主要为图像拥有者嵌入相应的版权、认证信息等，并将含密图像分布存储于云服务器中；其次，信息隐藏者利用秘密共享的同态加性，直接向秘密份额中二次嵌入秘密信息。2 种嵌入方法均可实现秘密无损提取及载体图像可逆恢复。CFSS 将 VRIE 和 VRAE 这 2 种嵌入方法有机结合，可以保证较高的安全性和嵌入率。

2.2 算法步骤

2.2.1 图像预处理

为了保证图像的安全性，在对图像共享之前，首先对其进行 Baker 变换以破坏像素之间较强的相关性，Baker 变换式为

$$\varphi(m',n')=\begin{cases}\varphi\left(2m,\frac{n}{2}\right), & 0\leqslant m\leqslant\frac{1}{2}\\ \varphi\left(2m-1,\frac{n}{2}+\frac{1}{2}\right), & \frac{1}{2}<m\leqslant 1\end{cases} \tag{6}$$

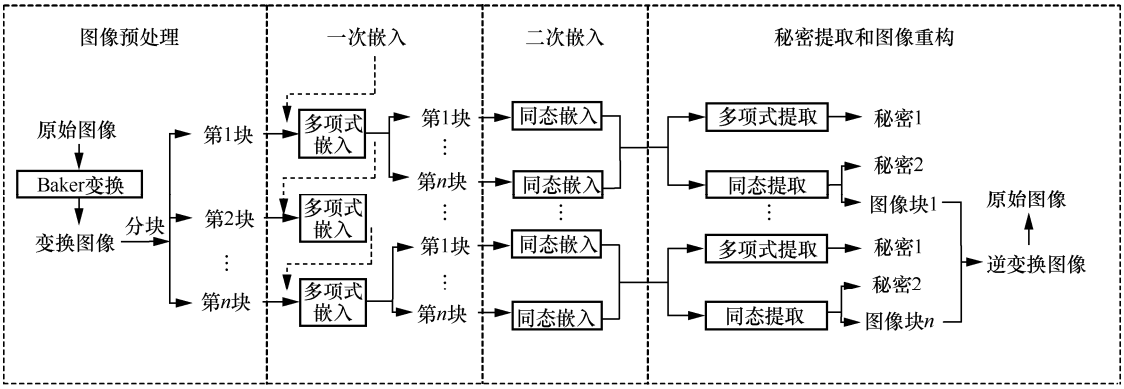


图 3　多重嵌入算法框架

假设图像大小为 $A\times A$，对其进行分割，得到 e 个小长方形，每个小长方形的高组成一个整数序列 $\{a_1,a_2,\cdots,a_e\}$，满足 $A=a_1+a_2+\cdots+a_e$，并定义 $A_0=0$，$A_i=a_1+a_2+\cdots+a_i$，则将原始图像的一个像素 (u,v)（$A_{i-1}\leqslant u< A_{i-1},0\leqslant v< A$）映射为

$$\begin{pmatrix}u'\\v'\end{pmatrix}=\begin{pmatrix}p_i(u-A_{i-1})+\mathrm{mod}(v,p_i)\\ \dfrac{v-\mathrm{mod}(v,p_i)}{p_i}+A_{i-1}\end{pmatrix} \tag{7}$$

其中，$p_i=\dfrac{A}{a_i}$，$1\leqslant i<e$，p_i 为整数。

2.2.2　信息嵌入

首先，在 CFSS 加密过程中进行多项式嵌入；然后，利用 CFSS 的同态加性对秘密份额二次嵌入，所有操作均在 GF(2^{16})上进行。

1) 多项式嵌入

多项式嵌入是指对变换图像加密时，利用构建的多项式系数冗余进行嵌入。传统的秘密共享如式(2)所示，将秘密设置为常数项系数，其余系数均采用随机数，由 se=R(0)可快速恢复常数项从而提取秘密。由于多项式的各项系数均可重构，因此可在其余系数上嵌入信息。首先，将变换图像分成大小相等的块，每个图像块中像素 P 的个数为 $2m$。下面以第 i 个图像块在 CFSS 加密过程中的多项式嵌入为例进行说明，选取的门限为(k,n)，其中 $2m\leqslant k\leqslant n$。

① 根据用户的身份号$\{i|i=1,2,\cdots,n\}$和种子密钥 h_i，利用伪随机数生成器生成 n 个互不相同的标识号 ID=$\{\mathrm{id}_1,\mathrm{id}_2,\cdots,\mathrm{id}_n\}$作为用户身份标识并通过秘密信道分发至用户。

② 将图像块中相邻的 2 个像素分别转化为二进制数后合并为一个 16 位二进制数，再将 16 位二进制数转换为十进制数得到 $p_{e1},p_{e2},\cdots,p_{em}$。嵌入者 1 将待嵌入的秘密 $S'=\{0,1\}^{\mathrm{T}}$ 以 16 位为单位转换为十进制数 $s_{e0},s_{e1},\cdots,s_{e(k-2m-1)}$。

③ 对第 i 块图像加密时，从第 i−1 个图像块共享的秘密份额中随机选取第 j 个份额 $f_{i-1}(j)$作为反馈份额，第一个图像块中的反馈份额 $f_0(j)$为随机数，并将 $f_{i-1}(j)$作为提取密钥 Key^1 通过秘密信道传送到信息提取方。

④ 利用 $p_{e1},p_{e2},\cdots,p_{em},s_{e0},s_{e1},\cdots,s_{e(k-2m-1)}$和 $f_{i-1}(j)$构建 k−1 次多项式如下

$$f_i(x)=s_{e0}+p_{e1}x+p_{e1}x^2+\cdots+p_{em}x^{2m-1}+p_{em}x^{2m}+s_{e1}x^{2m+1}+\cdots+(f_{i-1}(j)+s_{e(k-2m-1)})x^{k-1} \tag{8}$$

⑤ 将 ID=$\{\mathrm{id}_1,\mathrm{id}_2,\cdots,\mathrm{id}_n\}$作为自变量代入式(8)，计算秘密份额 $f_i(\mathrm{id}_1),f_i(\mathrm{id}_2),\cdots,f_i(\mathrm{id}_n)$并分发至用户。至此已完成对第 i 个图像块 CFSS 加密和多项式嵌入。

2) 同态嵌入

由 CFSS 的同态加性可知，对秘密份额实施嵌入等效于直接在相应的明文中实施嵌入，下面以第 i 个图像块生成秘密份额同态嵌入为例进行说明。

① 嵌入者 2 将待嵌入秘密 $S''=\{0,1\}^{\mathrm{T}}$ 以 16 位为单位转化为一个十进制数 $s_{c1},s_{c2},\cdots,s_{c(2m)}$。

② 利用 $s_{c1},s_{c2},\cdots,s_{c(2m)}$构建 $2m$ 次多项式如下

$$\gamma_i(x)=s_{c1}x+s_{c2}x^2+\cdots+s_{c(2m)}x^{2m} \tag{9}$$

③ 生成提取密钥 $\mathrm{Key}^2=\left\{\mathrm{Key}_1^2,\mathrm{Key}_2^2,\cdots,\mathrm{Key}_{2m}^2\right\}$。计算 $s_{c1}+s_{c2}$，将其转化为 16 位二进制数，将前 8 位转化为十进制数作为 Key_1^2，余下 8 位转化为十进制数作为 Key_2^2。同理，生成密钥 $\mathrm{Key}_3^2,\mathrm{Key}_4^2,\cdots,\mathrm{Key}_{2m}^2$，并通过安全信道传送到信息提取方。

④ 将 ID=$\{\mathrm{id}_1,\mathrm{id}_2,\cdots,\mathrm{id}_n\}$作为自变量代入式(9)，

计算秘密份额 $\gamma_i(\mathrm{id}_1),\gamma_i(\mathrm{id}_2),\cdots,\gamma_i(\mathrm{id}_n)$，再计算 $f_i(\mathrm{ID})+\gamma_i(\mathrm{ID})$，由式(5)可知，至此已将秘密 S''嵌入秘密份额。

2.2.3 信息提取和图像重构

信息提取者接收含密图像后，从含密份额中任意收集 k 份互不相同的份额，利用式(1)恢复多项式(10)，相应地各项系数即可恢复。

$$f_i(x)+\gamma_i(x)=s_{e0}+(p_{e1}+s_{c1})x+(p_{e1}+s_{c2})x^2+\cdots+(p_{em}+s_{c(2m)})x^{2m}+s_{e1}x^{2m+1}+\cdots+(f_{i-1}(j)+s_{e(k-2m-1)})x^{k-1} \tag{10}$$

信息提取者利用密钥 Key^1，通过计算 $(f_{i-1}(j)+s_{e(k-2m-1)})-\mathrm{Key}^1$ 可提取 $s_{e(k-2m-1)}$，即秘密 $S'=\{s_{e0}, s_{e1},\cdots, s_{e(k-2m-1)}\}$可全部提取。

信息提取者利用密钥 Key^2 分组提取像素值和秘密 S''，先将 $\mathrm{Key}_1^2, \mathrm{Key}_2^2,\cdots, \mathrm{Key}_{2m}^2$转化为二进制数，再将 Key_y^2两两分组。对于第一组密钥 Key_1^2和 Key_2^2，将 2 个 8 位的二进制数合并成一个 16 位二进制数后再转化为十进制 $\mathrm{Key}_{1\text{-}2}^2$，由此对于 p_{e1}、s_{c1} 和 s_{c2} 可得到三元一次方程式如下

$$\begin{cases} p_{e1}+s_{c1}=C_1 \\ p_{e1}+s_{c2}=C_2 \\ s_{c1}+s_{c2}=\mathrm{Key}_{1-2}^2 \end{cases} \tag{11}$$

因为 C_1、C_2、$\mathrm{Key}_{1\text{-}2}^2$均为已知量，所以 p_{e1}、s_{c1} 和 s_{c2} 均能求解。同理 $p_{e2}, p_{e3},\cdots, p_{em}, s_{c2}, s_{c3},\cdots, s_{c(2m)}$ 均可求解，即秘密 S''和像素 P 均可正确提取。

3 实验结果与分析

实验在 Windows 10 操作系统上进行，采用 MATLAB R2021b 编程，实验设备配置为 Intel(R) Core(TM) i7-11800H 2.30 GHz, 32GB。实验选取的测试数据为含有 10 000 张灰度图像的 BOSSbase 数据集，均为 512 像素×512 像素的灰度图像，但具有不同的纹理特征。

3.1 嵌入率

嵌入容量和嵌入率是评价 RDH-ED 性能的重要指标。嵌入容量是指在载体中嵌入的额外信息最大总比特数，嵌入率是指单位像素平均嵌入的额外信息比特数，两者之间的关系为

$$\mathrm{ER}=\frac{\mathrm{EC}}{N} \tag{12}$$

其中，N 为密文像素总数。本文算法嵌入容量由多项式嵌入容量 EC_1 和同态嵌入容量 EC_2 共同组成，算法的两次嵌入均与载体图像纹理无关，仅与载体图像大小及嵌入算法本身参数选择有关，两次嵌入容量为

$$\mathrm{EC}_1=16(k-2m),\ \mathrm{EC}_2=16\times 2m \tag{13}$$

其中，(k,n)为门限大小，m 为每块图像的像素数量，经过 CFSS 加密后密文像素量扩展为 $2mn$。因此，嵌入率可表示为

$$\mathrm{ER}=\frac{\mathrm{EC}_1+\mathrm{EC}_2}{2mn}=\frac{8k}{mn} \tag{14}$$

在数据集上随机选取 1 000 张图像计算其嵌入率平均值，并将本文算法与文献[31,35]算法对比，对比结果如表 1 所示。文献[31,35]和本文算法均利用秘密共享嵌入信息，文献[31]利用多项式系数冗余实施一次嵌入，文献[35]和本文算法同时进行了多项式嵌入和同态嵌入，更好地利用了秘密共享的冗余特征。由表 1 可知，当 k=n 时，本文算法嵌入率可达 8.00 bpp（bit per pixel），但此时方案不再具有容灾性，适用场景受限。几种算法嵌入率都随 k 值增大而提升，但要充分发挥秘密共享的容灾优势，(k,n)的取值不宜过大。当 m=1 时，对于常用门限(3,4)和(3,5)，本文算法嵌入率分别可达 6.00 bpp 和 4.80 bpp，比文献[31]算法高 2.00 bpp 和 1.60 bpp，比文献[35]算法高约 1.82 bpp 和 1.02 bpp，说明本文算法在嵌入能力和实用性方面更具优势。图 4 为不同算法在不同门限下的嵌入率对比。由图 4 可知，

表 1 不同算法嵌入率对比

算法	k=3			k=4			k=5			k=6		
	n=3	n=4	n=5	n=4	n=5	n=6	n=5	n=6	n=7	n=6	n=7	n=8
文献[31]算法	5.30	4.00	3.20	6.00	4.80	4.00	6.40	5.33	4.57	6.67	5.71	5.00
文献[35]算法	—	4.18	3.78	—	5.38	4.85	—	6.18	5.61	—	6.56	—
本文算法(m=2)	4.00	3.00	2.40	4.00	3.20	2.67	4.00	3.33	2.86	4.00	3.43	3.00
本文算法(m=1)	8.00	6.00	4.80	8.00	6.40	5.33	8.00	6.67	5.71	8.00	6.86	6.00

在不同门限下，本文算法相对于其他算法嵌入率均有不同幅度的提升。

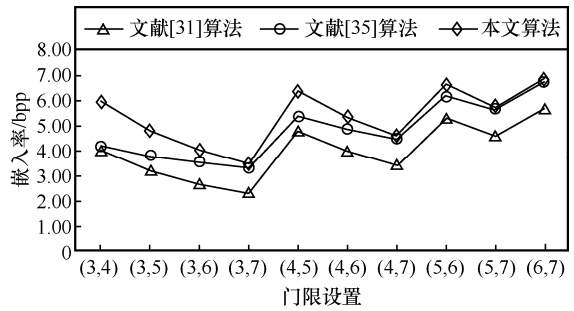


图 4　不同算法在不同门限下的嵌入率对比

为进一步证明本文算法的优越性，将本文算法与嵌入率较大的算法在多组载体图像下进行对比，对比结果如图 5 所示。文献[31,35]算法和本文算法的嵌入率均只与算法本身有关，不受载体图像纹理影响。文献[33-34]算法和本文算法均利用 CFSS 对载体图像加密，但文献[33-34]在加密后，对秘密份额进行像素预测以腾出空间嵌入额外信息，仅利用 CFSS 提高了安全性，没有充分发挥秘密共享的冗余优势，嵌入率受限，在(3,3)门限下，最大嵌入率比本文算法平均低约 5.26 bpp。文献[36]算法和本文算法均可同时适用于 VRIE 和 VRAE 框架，在(3,4)门限下，本文算法嵌入率较其平均高 3.12 bpp。

3.2　安全性分析

秘密共享将秘密分割成多个秘密份额，分发至不同用户分布存储，具有较强的容灾作用。算法在加密之前对载体图像进行 Baker 变换，破坏了像素之间较强的相关性，如图 6 所示，对图像 Baboon 进行一次变换达到了较强的视觉破坏效果，当变换 2 次时，就完全无法分析原始图像轮廓特征。图像加密过程采用的 CFSS 利用密码反馈策略，增强了秘密共享的扩散特性，当秘密图像中的一个比特被篡改时，其他份额都会产生较大的变化，能有效抵抗差分攻击、选择明文攻击等多种攻击，增强了算法的安全性和鲁棒性。

算法首次嵌入在加密过程中进行，二次嵌入是对密文进行操作，保证了嵌入过程不会影响载体的安全性。实验选取 k=3, n=4, m=1，图 7 为在未提取秘密时任选 k 个份额重构的图像及直方图，图 8 为算法主要阶段图像及直方图，图 8(a)为原始图像，图 8(b)为 Baker 变换 4 次后的置乱图像，图 8(c)为利用 CFSS 加密并首次嵌入信息的 4 份携密份额，图 8(d)为利用同态特性二次嵌入后的携密份额，图 8(e)和图 8(f)为重构密文图像和明文图像。从图 7 和图 8 可以看出，攻击者无法直接从秘密份额中得到任何涉及载体和秘密的相关信息，且收集任意多份携密份额，都无法从重构图像中获取有效信息。图 9 为提取的秘密信息和重构图像错误图，错误图是指将处理后的图像与原始图像进行逐比特比较，相等为 0，反之为 1。由图 9 可知，提取的秘密 S'、秘密 S''和重构图像的错误率均为 0，可证明本文算法能准确提取秘密和无损恢复图像。以上实验均可表明，本文算法能保证秘密及载体图像的安全性。

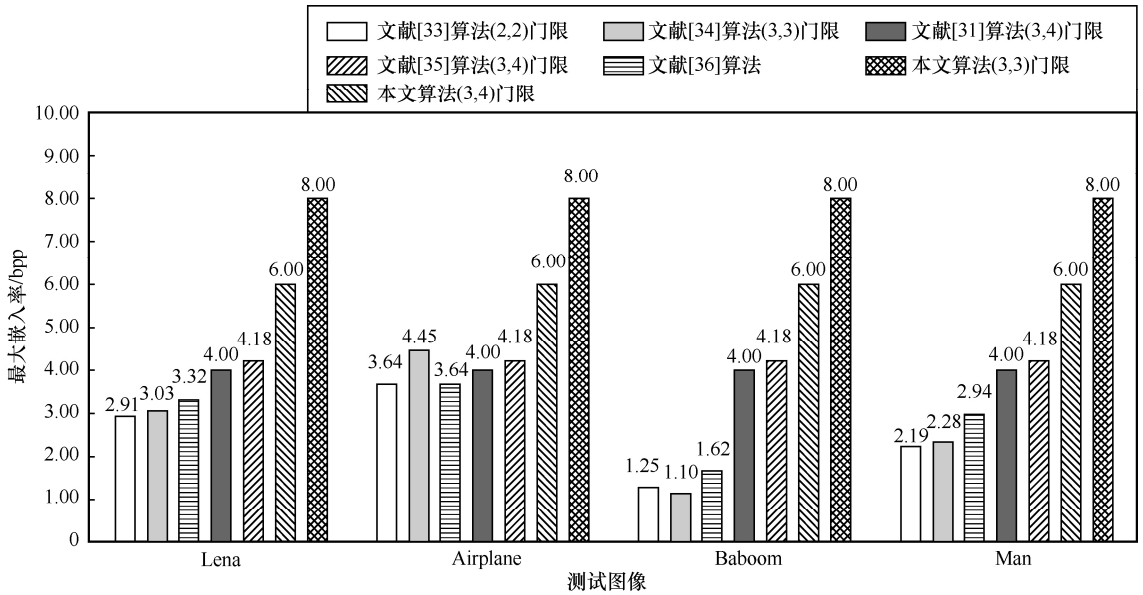


图 5　嵌入率对比

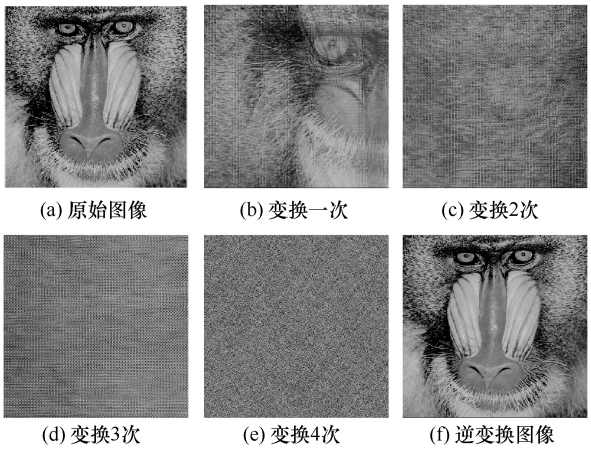


图 6　Baker 变换示例

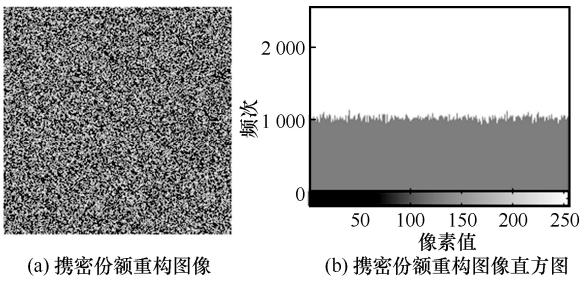


图 7　携密份额重构图像及直方图

3.3　可逆性

可逆性是指对载体图像加密和嵌入额外信息后，能否完全恢复原始图像以及无损提取额外信息，是衡量 RDH-ED 算法性能的重要指标。峰值信噪比（PSRN, peak signal to noise ratio）可用于评估 RDH-ED 重构图像的可逆恢复程度，其计算方法如下

$$\mathrm{PSNR}=10\lg\frac{2^8-1}{\frac{1}{XY}\sum_{i=0}^{X-1}\sum_{j=0}^{Y-1}\zeta(i,j)} \tag{15}$$

其中，$P(i,j)$为原始图像像素，$P'(i,j)$为重构图像像素，差值 $\zeta(i,j)=P(i,j)-P'(i,j)$。PSNR 值越大，图像失真程度越小，当 PSNR>35 dB 时，人眼无法察觉明显的失真，当 PSNR 趋于无穷大时，重构图像与原始图像相比无任何失真。由于本文算法采用 Lagrange 插值重构图像，其多项式系数均可无损恢复，即 PSNR 值为无穷大。且本文算法嵌入过程只与算法本身有关，与图像纹理特征无关，所以 PSNR 值不受嵌入率和载体图像影响。图 10 为本文算法与文献[14,24,27,28]算法在测试图像上的 PSNR 值随嵌入率变化对比。由图 10

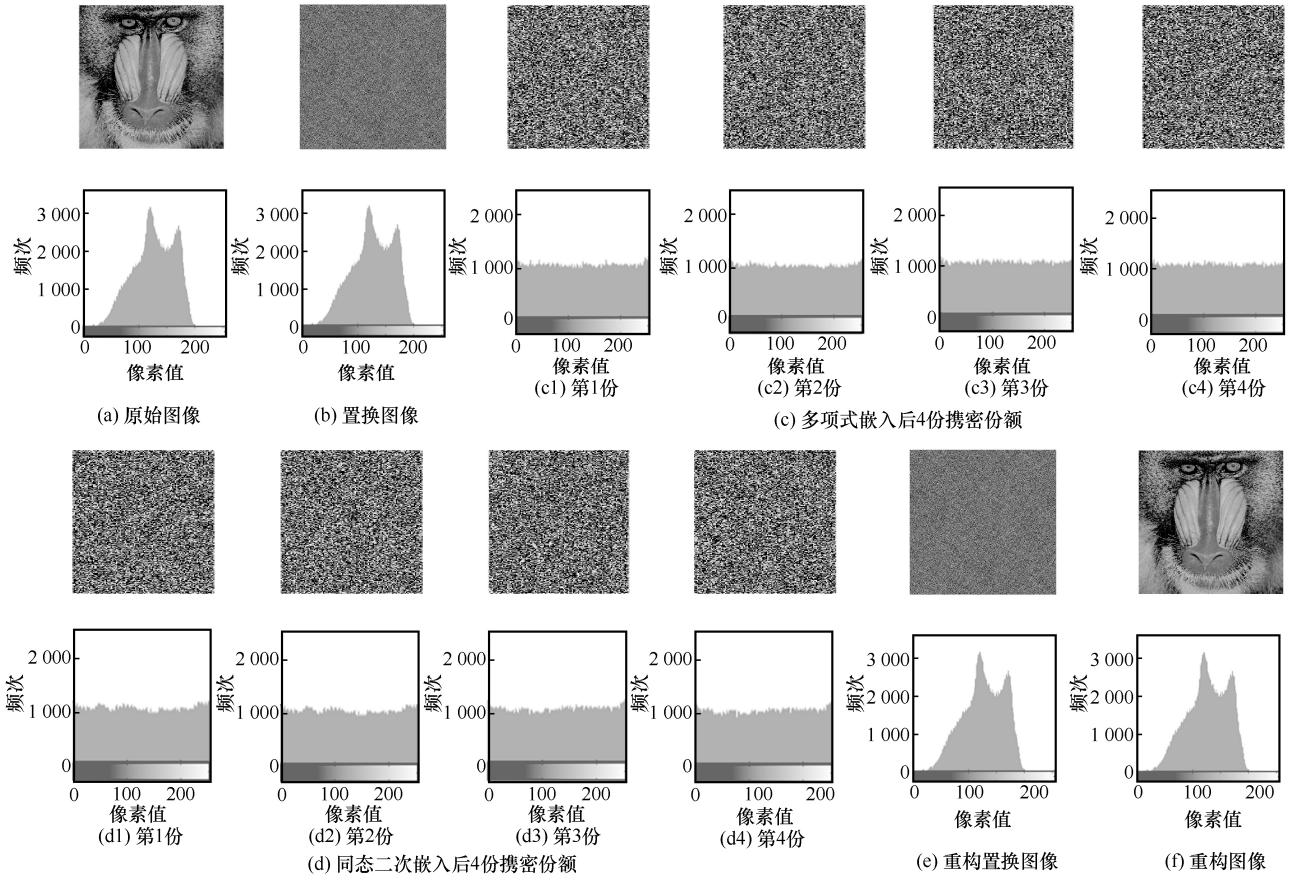


图 8　算法主要阶段图像及直方图

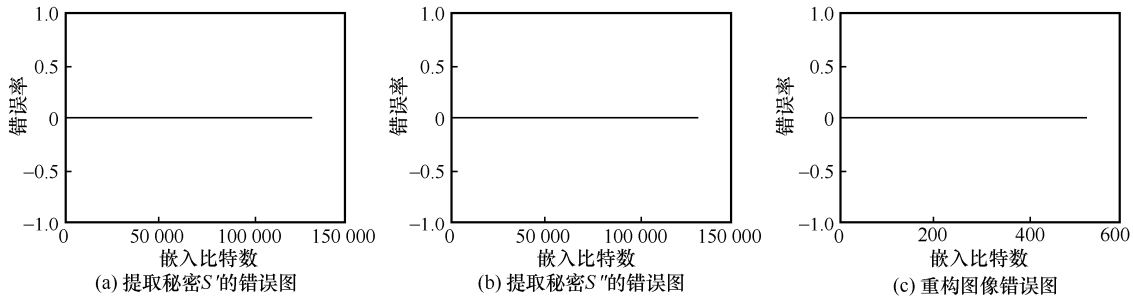


图 9　秘密提取及图像重构错误图

可知，本文算法在不同的嵌入率下，其峰值信噪比均趋于+∞，具有完全可逆性。

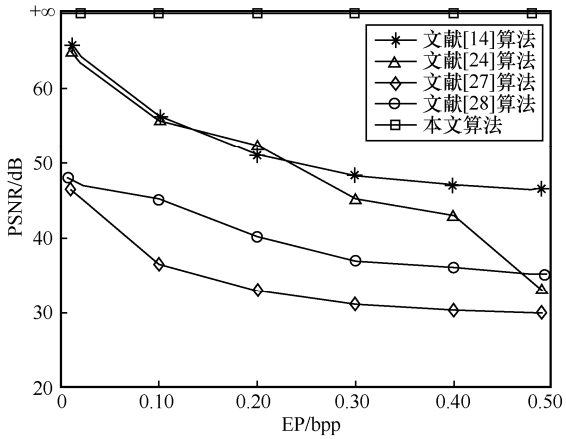


图 10　不同算法峰值信噪比对比

3.4　数据扩展

数据扩展是指密文图像大小大于原始图像大小。数据扩展率 R_{DE} 是指密文图像大小 S_{IE} 与原始图像大小 S_{IO} 之间的比值，是衡量数据扩展程度的重要指标，其计算方法如式(16)所示。相对扩展率指单个嵌入者实施嵌入产生的扩展率。

$$R_{\mathrm{DE}}=\frac{S_{\mathrm{IE}}}{S_{\mathrm{IO}}} \tag{16}$$

本文算法生成冗余的方式为 VRIE 和 VRAE，这里选取的对比算法为不同加密方式的 VRIE 算法或 VRAE 算法，对比结果如表 2 所示。文献[24,31]算法均为 VRIE 类算法。文献[24]算法采用同态加密，产生了较大数据扩展。文献[31-32,34]以及本文算法均为利用秘密共享生成秘密份额，采用秘密共享生成的秘密份额大小和原始图像大小相等。文献[32,34]算法利用秘密共享加密，然后在加密图像中嵌入额外信息，虽然密文图像总大小为原始图像的 n 倍，但对于每个分布式存储器而言，其数据扩展率为 1。文献[31]算法只在秘密共享加密过程中单次嵌入信息，然后将携密信息分布式存储，其相对密文扩展率为 1。本文算法分别在加密过程和加密过后进行两次嵌入，对于单个嵌入者而言，两次嵌入的扩展率均为 1。利用秘密共享加密，其总扩展率取决于门限大小，但对每个嵌入者而言，没有产生数据扩展。在门限相同的情况下，本文算法与文献[31-32,34]算法的数据扩展率相等，均在合理范围内。

表 2　　数据扩展率对比

算法	类型	加密方法	相对扩展率	总扩展率
文献[24]算法	VRIE	同态加密	256	256
文献[31]算法	VRIE	秘密共享	1	n
文献[32]算法	VRAE	秘密共享	1	n
文献[33]算法	VRAE	秘密共享	$\frac{1}{r-1}$	$\frac{n}{r-1}$
文献[34]算法	VRAE	秘密共享	1	n
本文算法	VRIE+VRAE	秘密共享	1	n

3.5　适用性分析

算法复杂度、嵌入率和可逆性可以用来衡量 RDH-ED 算法的适用性。算法复杂度是指算法运行过程中消耗的各种资源的总和。文献[13,24]是基于同态加密构造的 RDH-ED 算法，同态加密后的密文大小相比原始明文更大，对密文执行计算的时间比对明文执行计算时间更多，运算量较大，在实际运用过程中受到一定限制。文献[21-2]是基于 LWE 和 R-LWE 的算法，其算法复杂度等价于格上的一般性困难问题，基于格的算法具有较强的抗攻击安全性，但是其运算效率低。本文算法与文献[31,35]的计算方式均为多项式运算，算法复杂度较低。由于本文算法同时进行了多项式嵌入和同态嵌入，充分利用了秘密共享的冗余特性，因此嵌入率较高，且两次嵌入均只与算法参数选择有关，与图像纹理特征无关，可实现完全可逆。表 3 为本文算法与其他

算法的性能定性对比结果，本文算法在保证低复杂度和完全可逆的基础上，嵌入率更高，且嵌入能力不受载体图像影响，仅与算法参数选择有关，适用性更强。

表 3 算法性能定性对比

算法	加密方式	计算复杂度	嵌入率	可逆性
文献[13]算法	同态加密	高	低	强
文献[21]算法	LWE	高	低	强
文献[22]算法	R-LWE	高	低	强
文献[24]算法	同态加密	高	低	强
文献[31]算法	秘密共享	低	高	强
文献[35]算法	秘密共享	低	高	强
本文算法	秘密共享	低	非常高	强

4 结束语

本文基于 CFSS 提出一种多重嵌入方案，为提高算法的安全性，首先对原始图像 Baker 变换，以破坏像素之间的相关性，然后利用 CFSS 对载体图像加密，增强了算法的安全性和鲁棒性；为提高算法嵌入率，首先在加密过程中利用产生的多项式冗余系数嵌入秘密，然后利用秘密共享的同态特性对生成的秘密份额二次嵌入，进一步提升了算法的嵌入率。实验结果表明，本文算法具有较高的安全性和鲁棒性，能实现信息完全可逆提取和图像无损恢复，最大嵌入率可达 8.00 bpp，在门限(3,4)和(3,5)下，本文算法嵌入率比文献[35]分别提高了 1.82 bpp 和 1.02 bpp，且嵌入率与载体图像无关，仅与算法参数选择有关，适用性更强。

参考文献：

[1] SHI Y Q, LI X L, ZHANG X P, et al. Reversible data hiding: advances in the past two decades[J]. IEEE Access, 2016, 4: 3210-3237.

[2] PUECH W, CHAUMONT M, STRAUSS O. A reversible data hiding method for encrypted images[C]//Proceedings of the International Society for Optical Engineering. Bellingham: SPIE Press, 2008, 6819: 534-542.

[3] ZHOU J T, SUN W W, DONG L, et al. Secure reversible image data hiding over encrypted domain via key modulation[J]. IEEE Transactions on Circuits and Systems for Video Technology, 2016, 26(3): 441-452.

[4] ZHANG X P. Reversible data hiding in encrypted image[J]. IEEE Signal Processing Letters, 2011, 18(4): 255-258.

[5] ZHANG X P. Separable reversible data hiding in encrypted image[J]. IEEE Transactions on Information Forensics and Security, 2012, 7(2): 826-832.

[6] CHEN Y C, SHIU C W, HORNG G. Encrypted signal-based reversible data hiding with public key cryptosystem[J]. Journal of Visual Communication & Image Representation, 2014, 25(5):1164-1170.

[7] ZHANG X P, LONG J, WANG Z C, et al. Lossless and reversible data hiding in encrypted images with public-key cryptography[J]. IEEE Transactions on Circuits and Systems for Video Technology, 2016, 26(9): 1622-1631.

[8] 王继军, 孙泽锐, 李国祥. 图像抛物线插值空间大容量可逆信息隐藏算法[J]. 电子学报, 2019, 47(1): 8.
WANG J J, SUN Z R, LI G X. High capacity reversible data hiding algorithm based on parabolic interpolation space[J]. Acta Electronica Sinica, 2019, 47(1): 8.

[9] YU C Q, ZHANG X Q, ZHANG X P, et al. Reversible data hiding with hierarchical embedding for encrypted images[J]. IEEE Transactions on Circuits and Systems for Video Technology, 2021, 32(2): 451-466.

[10] YANG Y L, HE H J, CHEN F, et al. Reversible data hiding in encrypted images based on time-varying Huffman coding table[J]. IEEE Transactions on Multimedia, 2023, PP(99): 1-12.

[11] MA K D, ZHANG W M, ZHAO X F, et al. Reversible data hiding in encrypted images by reserving room before encryption[J]. IEEE Transactions on Information Forensics and Security, 2013, 8(3): 553-562.

[12] 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, 13(7): 1670-1681.

[13] XIANG S J, LUO X R. Reversible data hiding in homomorphic encrypted domain by mirroring ciphertext group[J]. IEEE Transactions on Circuits and Systems for Video Technology, 2018, 28(11): 3099-3110.

[14] 李天雪, 张敏情, 狄富强, 等. 基于位平面分割的密文域可逆信息隐藏算法[J]. 计算机应用研究, 2018, 35(9): 6.
LI T X, ZHANG M Q, DI F Q, et al. Cryptographic domain reversible data hiding algorithm based on bit plane segmentation[J]. Application Research of Computers, 2018, 35(9): 6.

[15] PUTEAUX P, PUECH W. A recursive reversible data hiding in encrypted images method with a very high payload[J]. IEEE Transactions on Multimedia, 2021, 23: 636-650.

[16] 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.
WU Y Q, GUO Y T, TANG J, et al. Reversible data hiding in encrypted images using adaptive Huffman encoding strategy[J]. Chinese Journal of Computers, 2021, 44(4): 846-858.

[17] WANG Y M, CAI Z C, HE W G. High capacity reversible data hiding in encrypted image based on intra-block lossless compression[J]. IEEE Transactions on Multimedia, 2021, 23: 1466-1473.

[18] 吴友情, 马文静, 殷赵霞, 等. 基于预测误差位平面压缩的密文图像可逆信息隐藏[J]. 通信学报, 2022, 43(8): 12.
WU Y Q, MA W J, YIN Z X, et al. Reversible data hiding in encrypted image based on bit-plane compression of prediction error[J]. Journal of Communications, 2022, 43 (8): 12.

[19] 马文静, 吴友情, 殷赵霞. 自适应编码的高容量密文可逆信息隐藏算法[J]. 软件学报, 2022, 33(12): 4746-4757.
MA W J, WU Y Q, YIN Z X. High-capacity reversible data hiding in encrypted images using adaptive encoding[J]. Journal of Software, 2022, 33(12): 4746-4757.

[20] ZOU H, CHEN G. Reversible data hiding in encrypted image with

local-correlation-based classification and adaptive encoding strategy[J]. Signal Processing, 2023, 205: 1108847.

[21] 张敏情, 柯彦, 苏婷婷. 基于LWE的密文域可逆信息隐藏[J]. 电子与信息学报, 2016, 38(2): 7.
ZHANG M Q, KE Y, SU T T. Reversible steganography in encrypted domain based on LWE[J]. Journal of Electronics & Information Technology, 2016, 38(2): 7.

[22] 柯彦, 张敏情, 苏婷婷. 基于 R-LWE 的密文域多比特可逆信息隐藏算法[J]. 计算机研究与发展, 2016, 53(10): 2307-2322.
KE Y, ZHANG M Q, SU T T. A novel multiple bits reversible data hiding in encrypted domain based on R-LWE[J]. Journal of Computer Research and Development, 2016, 53(10): 2307-2322.

[23] HUANG D, WANG J. High-capacity reversible data hiding in encrypted image based on specific encryption process[J]. Signal Processing Image Communication, 2019, 80:115632.

[24] KE Y, ZHANG M Q, LIU J, et al. Fully homomorphic encryption encapsulated difference expansion for reversible data hiding in encrypted domain[J]. IEEE Transactions on Circuits and Systems for Video Technology, 2020, 30(8): 2353-2365.

[25] SHAMIR A . How to share a secret[J]. Communications of the ACM, 1979, 22(11): 612-613.

[26] WU X T, WENG J, YAN W Q. Adopting secret sharing for reversible data hiding in encrypted images[J]. Signal Processing, 2018, 143: 269-281.

[27] 周能, 张敏情, 林文兵. 基于秘密共享的可分离密文域可逆信息隐藏算法[J]. 计算机工程, 2020, 46(10): 112-119.
ZHOU N, ZHANG M Q, LIN W B. Separable reversible information hiding algorithm in encrypted domain based on secret sharing[J]. Computer Engineering, 2020, 46(10): 112-119.

[28] 周能, 张敏情, 刘蒙蒙. 基于秘密共享的同态加密图像可逆信息隐藏算法[J]. 科学技术与工程, 2020, 20(19): 7.
ZHOU N, ZHANG M Q, LIU M M. Reversible data hiding algorithm in homomorphic encrypted image based on secret sharing[J]. Science Technology and Engineering, 2020, 20(19): 7.

[29] KE Y, ZHANG M Q, ZHANG X P, et al. A reversible data hiding scheme in encrypted domain for secret image sharing based on Chinese remainder theorem[J]. IEEE Transactions on Circuits and Systems for Video Technology, 2022, 32(4): 2469-2481.

[30] QIN C, GAO S Y, JIANG C Y, et al. Reversible data hiding in encrypted images based on Chinese remainder theorem and secret sharing mechanism[C]//Proceedings of the 2021 3rd International Conference on Big-data Service and Intelligent Computation. New York: ACM Press, 2021: 23-32.

[31] 王泽曦, 张敏情, 柯彦, 等. 基于图像秘密共享的密文域可逆信息隐藏算法[J]. 计算机应用, 2022, 42(5): 1480-1489.
WANG Z X, ZHANG M Q, KE Y, et al. Reversible data hiding algorithm in encrypted domain based on secret image sharing[J]. Journal of Computer Applications, 2022, 42(5): 1480-1489.

[32] QIN C, CHANYU J, MO Q, et al. Reversible data hiding in encrypted image via secret sharing based on GF(p) and GF(2^8)[J]. IEEE Transactions on Circuits and Systems for Video Technology, 2022, 32(4): 1928-1941.

[33] HUA Z Y, WANG Y X, YI S, et al. Reversible data hiding in encrypted images using cipher-feedback secret sharing[J]. IEEE Transactions on Circuits and Systems for Video Technology, 2022, 32(8): 4968-4982.

[34] HUA Z Y, WANG Y X, YI S, et al. Matrix-based secret sharing for reversible data hiding in encrypted images[J]. IEEE Transactions on Dependable and Secure Computing, 2023, 20(5): 3669-3686.

[35] 张敏情, 王泽曦, 柯彦, 等. 基于多项式秘密共享的图像密文域可逆信息隐藏[J]. 电子与信息学报, 2022, 44(12): 4337-4347.
ZHANG M Q, WANG Z X, KE Y, et al. Reversible data hiding in encrypted images based on polynomial secret sharing[J]. Journal of Electronics & Information Technology, 2022, 44(12): 4337-4347.

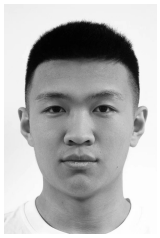
[36] QIU Y Q, YING Q C, YANG Y Y, et al. High-capacity framework for reversible data hiding in encrypted image using pixel prediction and entropy encoding[J]. IEEE Transactions on Circuits and Systems for Video Technology, 2022, 32(9): 5874-5887.

[作者简介]

张敏情（1967− ），女，陕西西安人，博士，武警工程大学教授、博士生导师，主要研究方向为密码学、信息隐藏等。

姜超（1997− ），男，安徽安庆人，武警工程大学硕士生，主要研究方向为信息安全、密文域可逆信息隐藏。

狄富强（1990− ），男，山东莱芜人，博士，武警工程大学副教授，主要研究方向为信息安全、深度学习。



蒋宗宝（1999− ），男，山东德州人，武警工程大学硕士生，主要研究方向为信息安全、密文域可逆信息隐藏。

张雄（1995− ），男，湖北仙桃人，武警工程大学硕士生，主要研究方向为信息隐藏、深度学习。