基于细粒度访问控制的密文域可逆信息隐藏

张敏情[1,2]，彭深[1,2]，姜超[1,2]，狄富强[1,2]，董钰峰[1,2]
（1. 武警工程大学密码工程学院，陕西 西安 710086；
2. 武警工程大学重点实验室，陕西 西安 710086）

摘　要：为提高云环境下密文域可逆信息隐藏算法的嵌入率和安全性，将密文策略属性基加密和密文域可逆信息隐藏有机结合，提出一种基于细粒度访问控制的密文域可逆信息隐藏算法。首先，根据预测误差范围对像素进行分类，利用参数二叉树对不同类别的像素进行标记；其次，基于密文策略属性基加密算法对图像加密密钥进行加密，将加密后的密钥和需要隐藏的信息嵌入密文图像中。实验结果表明，所提算法将不可嵌入像素分为自记录像素和不可记录像素后，辅助信息量减少，从而增大了嵌入容量。相较于现有最佳算法，所提算法平均嵌入率提高约 0.2 bit/pixel，同时能够实现对密文图像的细粒度访问控制，具有嵌入率大、安全性高、可逆性好等特点，实用性较强。

关键词：密文策略属性基加密；密文域；可逆信息隐藏；访问控制；参数二叉树标记
中图分类号：TP309.7
文献标志码：A
DOI：10.11959/j.issn.1000–436x.2025118

Reversible data hiding in encrypted domain based on fine-grained access control

ZHANG Minqing[1,2], PENG Shen[1,2], JIANG Chao[1,2], DI Fuqiang[1,2], DONG Yufeng[1,2]
1. College of Cryptography Engineering, Engineering University of PAP, Xi’an 710086, China
2. Key laboratory of CTC&IE (Engineering University of PAP), Ministry of Education, Xi’an 710086, China

Abstract: To improve the embedding rate and security of reversible data hiding algorithms in encrypted images for cloud environments, ciphertext-policy attribute-based encryption and reversible data hiding in encrypted images were organically integrated, and a reversible data hiding algorithm in encrypted images based on fine-grained access control was proposed. Firstly, pixels were classified according to the size of the prediction error value, and different categories of pixels were marked using a parametric binary tree. Secondly, the image encryption key was encrypted based on the ciphertext-policy attribute-based encryption algorithm, and the encrypted key, along with the information to be embedded, was embedded into the encrypted image. It was indicated by experimental results that categorizing the non-embeddable pixeled into self-recording pixels and non-recording pixels reduced the amount of auxiliary information, thus increasing the embedding capacity. Compared with state-of-the-art algorithms, the proposed algorithm achieves an average embedding rate improvement of approximately 0.2 bit/pixel while enabling fine-grained access control of the encrypted images. The algorithm demonstrates high embedding rate, strong security, and perfect reversibility, making it highly practical.

Keywords: ciphertext-policy attribute-based encryption, encrypted domain, reversible data hiding, access control, parametric binary tree labeling

收稿日期：2025–04–28；**修回日期：**2025–06–20
通信作者：彭深，18392602670@163. com
基金项目：国家自然科学基金资助项目（No.62272478）
Foundation Item：The National Natural Science Foundation of China (No.62272478)

0 引言

数字信息时代，随着社交媒体和智能拍照设备的广泛使用，用户将越来越多的图像上传到云服务器[1]。现实生活中用户为了保护个人隐私，通常会先将图像加密再上传到云服务器。如何在保护用户隐私安全的同时还能在密文图像中嵌入秘密信息，并且实现可逆提取秘密信息和无损恢复原始图像成为研究热点。因此，密文域可逆信息隐藏[2-3]（RDH-EI, reversible data hiding in encrypted image）得到快速发展，在远程医疗诊断、司法证据保全等对载体安全性与无失真重构均有严格要求的领域具有重要的应用价值。根据全局加密类算法所采用的加密系统类型，可将现有RDH-EI算法分为基于对称加密的RDH-EI算法和基于公钥加密的RDH-EI算法两大类[4]。

基于对称加密的RDH-EI算法[5-16]具有加解密速度快、嵌入容量大等优点，常用的加密方法包括AES加密[5,13]、流密码加密[7,11]和分块置乱加密[9,15]等。根据加密前是否对图像进行预处理，基于对称加密的RDH-EI算法有加密后生成冗余[5-6]（VRAE, vacating room after encryption）和加密前生成冗余[8,10]（VRBE, vacating room before encryption）这2种框架。在VRAE框架下，Puech等[5]最先提出利用AES加密后嵌入信息的算法，每个像素块可嵌入1 bit信息；随后，Zhang[6]提出利用流密码加密后生成冗余的算法，通过翻转像素的3 bit最低有效位嵌入1 bit信息。原始图像加密后破坏了像素之间的相关性，导致嵌入容量不高，同时存在可分离性差、载体恢复难度较大等缺点。为了充分利用原始图像像素间的相关性，基于VRBE的RDH-EI算法在图像加密前采用无损压缩[7,12]、像素预测[9,13]和编码[10-11]等技术进行预处理生成冗余，嵌入容量较大。Wu等[13]提出参数二叉树标记（PBTL, parametric binary tree labeling）的方法，首先根据选定的2个不同参数和预测误差范围，将密文图像中的像素分为参考像素、特殊像素、可嵌入像素和不可嵌入像素，然后在可嵌入像素的非标记位中嵌入信息。然而，基于对称加密的RDH-EI算法需要共享加密密钥，但密钥在传输过程中可能被中间人攻击截获，从而泄露密文图像内容，基于对称加密的RDH-EI在密钥传输过程中存在的问题如图1所示。

相较于对称加密，基于公钥加密的RDH-EI[4,17-25]算法具有不需要密钥共享、权限管理灵活等优点，常见的加密算法包括同态加密[17-22]、LWE加密[4,23-24]和NTRU加密[25]。基于公钥加密的RDH-EI算法有VRBE[19-20]和加密过程冗余[21-22]（VRIE,vacating redundancy in encryption）这2种框架。在VRBE框架下，Xiang等[20]在加密图像前首先通过自嵌入的方式腾出冗余空间，然后利用Paillier加密的同态和概率特性嵌入信息，可分离性较好；但预处理过程较为复杂，实际应用局限性较大。Ke等[4,23]首次提出基于VRIE的RDH-EI算法，利用R-LWE（ring-learning with error）加密后的密文冗余空间，通过量化分区和再编码实现多比特信息嵌入。Wu等[25]提出多项式编码和多项式调制在NTRU加密过程中嵌入信息的算法，计算效率较高。然而，基于公钥加密的RDH-EI算法存在计算开销较大、嵌入容量不高、密钥更新困难等问题。

为解决云环境中密钥传输困难的问题，Yang

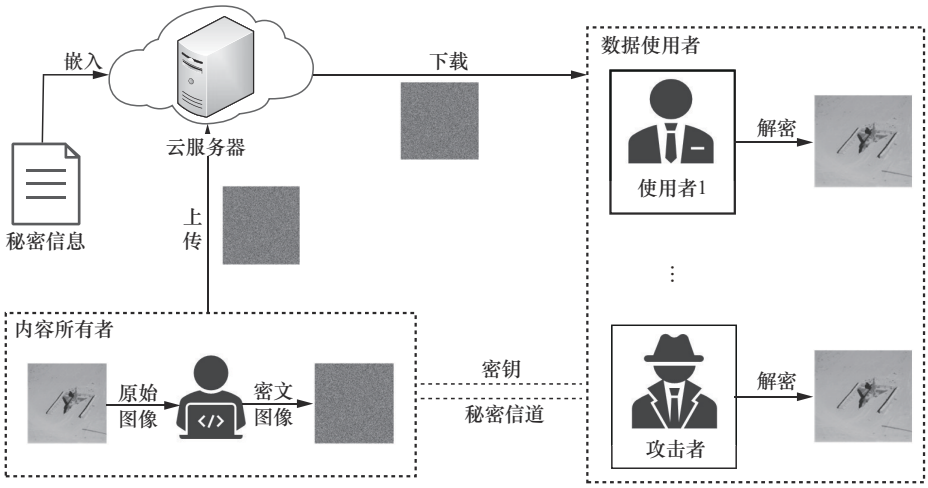


图1 基于对称加密的RDH-EI在密钥传输过程中存在的问题

等[26]提出一种混合加密方案，首先通过流密码加密原始图像，然后利用RSA加密对称密钥，在保证图像内容安全的同时，具有较高的嵌入率。但是在多用户应用场景中，该方案需要为每个用户单独维护独立密钥对，带来了密钥管理和更新困难的问题。而密文策略属性基加密[27-28]（CP-ABE,ciphertext-policy attribute-based encryption）方案能够确保云环境下多用户数据共享的安全性和灵活性。Bethencourt等[29]基于双线性映射首次提出CP-ABE加密方案，该方案将密钥与用户属性集合绑定，密文与访问控制策略关联，实现了对加密数据的细粒度访问控制。近年来，根据不同的应用场景需求，涌现出许多具有附加特性或功能的CP-ABE方案，如可追踪[30]、可撤销[31]以及去中心化[32]。Du等[32]将区块链技术与CP-ABE结合，解决了传统CP-ABE方案中存在的单点故障、隐私泄露和撤销效率低等问题。Zhang等[33]利用白盒追踪和二叉树技术，实现了高效用户追踪与短列表撤销。Chen等[34]提出结合CP-ABE的图像加密方案，对图像置乱加密后，利用CP-ABE对加密密钥进行二次加密，该方案有效解决了云环境中密钥管理困难的技术难题。

因此，为解决云环境多用户应用场景中的数据安全和密钥传输、管理以及更新困难的问题，本文将CP-ABE和RDH-EI有机结合，提出基于细粒度访问控制的参数二叉树标记的RDH-EI算法，主要研究工作如下。

1) 利用参数二叉树标记的方法在密文图像中嵌入和提取信息。在文献[13]的基础上，根据预测误差范围将不可嵌入像素进一步细分为自记录像素和不可记录像素两类，减少了辅助信息量，从而增大了嵌入容量。

2) 提出一种基于属性的密钥封装机制。首先通过AES-CTR算法加密原始图像，然后对加密密钥进行CP-ABE加密，并将加密后的密钥嵌入密文图像中，实现对密文图像的细粒度访问控制。

1　相关知识

1.1　双线性映射

设q是一大素数，G和G_T是2个阶为q的乘法循环群，g为群G的一个生成元，Z_q表示模q的整数集。G到G_T的双线性映射$e{:}G\times G\to G_T$，满足下面的性质。

1) 双线性：$\forall a,b\in Z_q, e\left(g^a,g^b\right)=e\left(g,g\right)^{ab}$。

2)非退化性：$e\left(g,g\right)\neq 1$。

3)可计算性：e是多项式时间可计算的。

1.2　访问结构

设$S=\left\{s_1,s_2,\cdots,s_n\right\}$表示属性空间，则其中一个非空的属性集合$A\subseteq 2^S/\{\varnothing\}$为访问结构。如果对$\forall B,C\subseteq S$,当$B\subseteq A$且$B\subseteq C$时,有$C\subseteq A$，则称$A$是一个单调的访问结构。对于$\forall M\in A$,称$M$为授权集合，反之称$M$为非授权集合。假设访问结构为$(B\wedge C)\vee \mathrm{D}$，那么授权集合为$\{B,C,D\}$、$\{B,C\}$和$\{D\}$,非授权集合为$\{B,D\}$和$\{C,D\}$。

1.3　二叉树数据结构

在二叉树BT中，每个叶节点分别对应一个用户。U表示用户集合，$|Y|$表示叶节点个数，RL表示撤销列表，则二叉树中节点个数为$2|Y|-1$。

采用广度遍历优先的方法对所有节点进行编号，利用KUNodes算法[35]实现用户撤销。令$\mathrm{path}(i)$表示从根节点到节点i的路径，$\mathrm{cover}(\mathrm{RL})$表示覆盖所有未被撤销用户的最小节点集合，如果用户$u\notin \mathrm{RL}$，那么有唯一的节点$j=\mathrm{cover}(\mathrm{RL})\cap \mathrm{path}(u)$。

二叉树BT示例如图2所示。撤销列表$\mathrm{RL}=\left\{u_1,u_4\right\}=\{7,10\}$，最小节点集合$\mathrm{cover}(\mathrm{RL})=\{2,8,9\}$。以$u_8$为例，$\mathrm{path}\left(u_8\right)=\mathrm{path}(14)=\{0,2,6,14\}$，则$\mathrm{path}\left(u_8\right)$与$\mathrm{cover}(\mathrm{RL})$相交的唯一节点$j=\{2\}$。

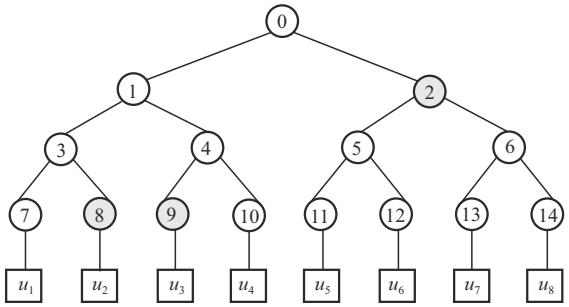


图2　二叉树BT示例

1.4　密文策略属性基加密方案

本文方案包括6个算法[36]，具体介绍如下。

$\mathrm{Setup}(\lambda,S,N)\to(\mathrm{PK},\mathrm{MSK},\mathrm{BT})$：系统初始化设置，由可信权威机构执行。输入安全参数λ、属性空间S和用户数量上限N，输出系统公钥PK、主密钥MSK和二叉树BT。

KeyGen(PK,MSK,u,P) → SK：用户私钥生成算法，由可信权威机构执行。输入系统公钥PK、主密钥MSK、用户身份u和属性集合P，输出相应用户私钥SK。

Encrypt(PK,T,RL,k_e) → CT：加密算法，由数据所有者执行。采用密钥封装的方式，先通过对称加密算法加密数据，而后利用PK和RL加密对称密钥。输入系统公钥PK、访问策略T、用户的撤销列表RL和对称密钥k_e，输出对应的密文CT。

Decrypt(PK,SK,CT,BT) → k_e 或 ⊥：解密算法，由数据使用者执行，解密得到对称密钥k_e后解密加密数据。输入系统公钥PK、用户私钥SK、密文CT和二叉树BT。如果与解密密钥SK相关联的属性集合P满足与CT相关联的访问策略，算法输出对称密钥k_e；反之，解密失败，输出⊥。

Revocation(RL,u,MSK,BT) → (RL′,BT′)：用户撤销算法，由可信权威机构执行。输入撤销列表RL、撤销用户u、系统主密钥MSK和原来的二叉树BT，输出新的撤销列表RL′和二叉树BT′。

CTUpdate(PK,RL′,CT) → CT′：密文更新算法，由数据所有者执行。输入系统公钥PK、新的撤销列表RL′和原来的密文CT，输出新的密文CT′

1.5 参数二叉树标记

对于一个8位的像素，可用7层完全二叉树表示，其中第i层有2^i个节点(i = 1,2,⋯,7)，完全二叉树中的二进制编码分布如图3所示。选定2个参数α和β（$1 \leqslant \alpha,\beta \leqslant 7$），将图像中的像素标记为可嵌入像素$C_1$和不可嵌入像素$C_2$这2个不同的类别，$\alpha$表示标记$C_1$所用编码位数，$\beta$表示标记$C_2$所用编码位数。标记方法如下：$C_2$中的所有像素用$\beta$位“0”（即第$\beta$层的第一个节点）进行标记；$C_1$中的像素利用式(1)可分为$n_\alpha$个不同子类，$\alpha$和$\beta$决定$n_\alpha$的值，计算式为

$$n_\alpha = \begin{cases} 2^\alpha - 1, \alpha \leqslant \beta \\ \left(2^\beta - 1\right) \times 2^{\alpha-\beta}, \alpha > \beta \end{cases} \tag{1}$$

当$\alpha \leqslant \beta$时，在第α层从右往左依次选择$2^\alpha - 1$个节点来标记C_1中的n_α个不同子类；当$\alpha > \beta$时，在第α层从右往左依次选择$(2^\beta - 1) \times 2^{\alpha-\beta}$个节点来标记$C_1$中的$n_\alpha$个不同子类。同一子类的像素使用相同的$\alpha$位二进制编码标记；反之，则使用不同的$\alpha$位二进制编码标记。

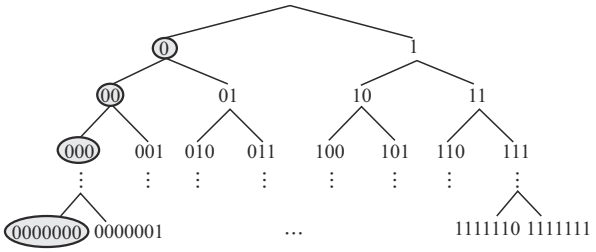


图3 完全二叉树中的二进制编码分布

以β = 2、α = 1~7为例，说明如何选择用于标记的二进制编码，如表1所示。当α = 2,β = 2时，C_2中的像素用“00”标记，C_1中的3个不同子类分别用“11”“10”和“01”标记。

表1 β = 2、α = 1~7时的标记位

β = 2	C_2	C_1	n_α
α = 1	00	1	1
α = 2	00	11,10,01	3
α = 3	00	111,110,101,100,011,010	6
α = 4	00	1111~0100	12
α = 5	00	11111~01000	24
α = 6	00	111111~010000	48
α = 7	00	1111111~0100000	96

2 算法设计

2.1 算法框架

基于细粒度访问控制的RDH-EI算法框架如图4所示，主要由密钥生成中心、云服务器、内容所有者和数据使用者4个实体部分组成。密钥生成中心生成系统公钥PK和主密钥MSK，并根据数据使用者的属性集合生成私钥SK。首先内容所有者利用中值预测器得到预测像素值；然后，采用AES-CTR算法加密原始图像，并利用系统公钥PK和撤销列表RL对加密密钥k_e进行加密，进而得到密文CT；接着，根据预测误差范围标记密文图像中的不同像素，将辅助信息和密文CT嵌入可嵌入像素中；最后，上传携密密文图像到云服务器。数据使用者从云服务器下载得到携密密文图像，首先从中提取出嵌入信息，然后利用私钥SK解密密文CT，只有满足要求的用户才能解密成功。

2.2 算法步骤

2.2.1 预测误差计算

为了充分利用原始图像像素之间的冗余，内容所有者在图像加密前会先进行预处理，通常采用中

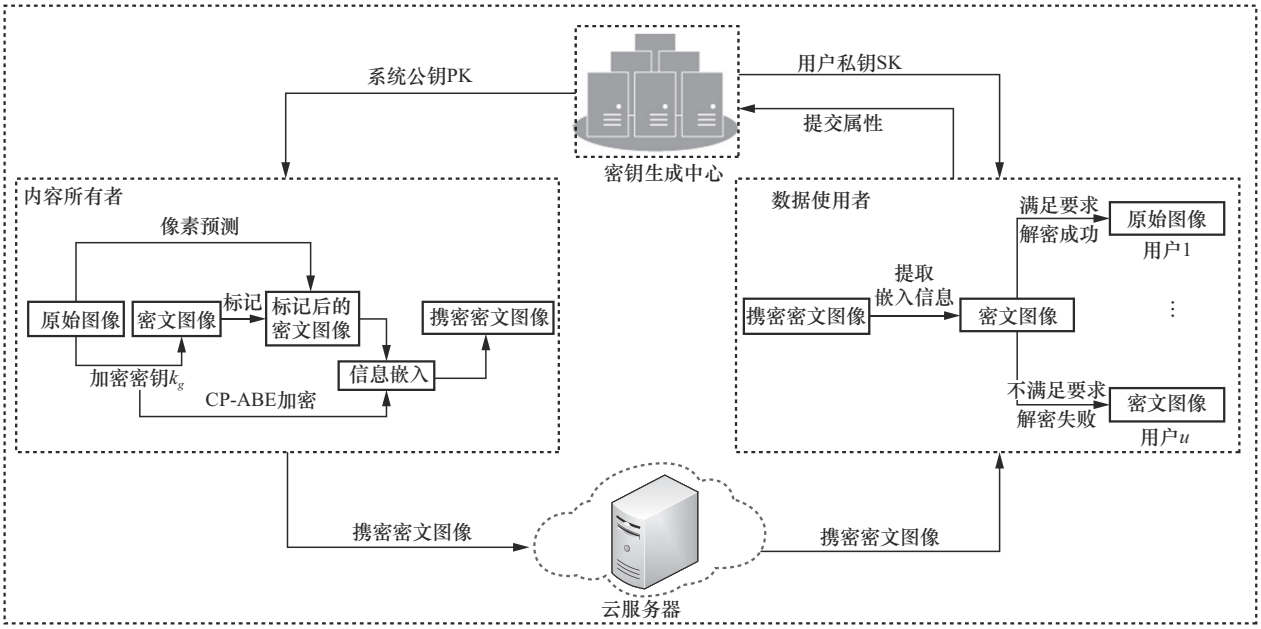


图4　基于细粒度访问控制的RDH-EI算法框架

值预测器来预测原始图像像素值。

对于尺寸为$m \times n$的灰度图像I，I中第一行和第一列为参考像素，$x(i,j)$表示I中任一像素值，其中$1 \leqslant i \leqslant m$，$1 \leqslant j \leqslant n$。中值预测器如图5所示，根据当前像素$x(i,j)$的上方、左上方和左侧3个相邻像素$a$、$c$、$b$来得到预测像素值$\hat{x}(i,j)$，预测像素值的计算式如式(2)所示。

$$\hat{x}(i,j)=\begin{cases}\max(a,b), c \leqslant \min(a,b)\\ \min(a,b), c \geqslant \max(a,b)\\ a+b-c, \text{其他}\end{cases} \tag{2}$$

c	a
b	$x(i,j)$

图5　中值预测器

预测误差$e(i,j)$的计算式为

$$e(i,j)=x(i,j)-\hat{x}(i,j) \tag{3}$$

2.2.2　图像加密

内容所有者计算得到原始图像的像素预测值和预测误差后，采用AES-CTR加密算法对原始图像进行加密。首先，图像所有者通过式(4)将原始图像中每个像素值转换为8位二进制序列，即

$$x^k(i,j)=\left\lfloor \frac{x(i,j)}{2^{k-1}} \right\rfloor \bmod 2, k=1,2,\cdots,8 \tag{4}$$

其中，k对应于二进制序列的位，$\lfloor * \rfloor$表示向下取整。然后根据加密密钥k_e生成与原始图像大小相等的伪随机矩阵$\boldsymbol{R}$，通过式(4)将$\boldsymbol{R}$中的像素$r(i,j)$转换为8位二进制序列，并按位异或得到密文图像I'，如式(5)所示。

$$x_e^k(i,j)=x^k(i,j) \oplus r^k(i,j), k=1,2,\cdots,8 \tag{5}$$

最后，计算密文图像像素值$x_e(i,j)$为

$$x_e(i,j)=\sum_{k=1}^{8} x_e^k(i,j) \times 2^{k-1}, k=1,2,\cdots,8 \tag{6}$$

以$m=4$、$n=4$为例，计算得到像素预测值、预测像素误差和密文图像像素值，如图6所示。

151	153	152	153
35	151	155	152
149	147	152	153
152	149	154	152

(a) 原始图像

151	153	152	153
35	37	151	155
149	151	151	152
152	150	152	154

(b) 像素预测值

151	153	152	153
35	114	4	−3
149	−4	1	1
152	−1	2	−2

(c) 预测像素误差

143	224	198	235
146	62	143	213
217	174	46	156
124	97	236	164

(d) 密文图像像素值

图6　预测像素误差和密文图像像素值

2.2.3 CP-ABE加密对称密钥

图像加密后，为了解决云环境多用户应用场景下的密钥传输、管理和更新困难的问题，内容所有者利用CP-ABE加密算法，使用密钥生成中心生成的系统公钥PK、访问策略T以及撤销列表RL对图像加密密钥k_e进行加密，产生的密文包括与访问策略T、撤销列表RL分别相关的2个部分，具体介绍如下。

1) 在访问策略T中，对任意一个节点$x \in T$,随机选择一个阶为$d_x = l_x - 1$的多项式q_x,其中l_x表示节点x的门限值。从根节点root开始，随机选择秘密值$s \in Z_q$，令$q_{\text{root}}(0) = s$，接着选择d_{root}个参数定义多项式q_{root}。对其他节点x，按照广度遍历优先的方式，令$q_x(0) = q_{\text{parent}(x)}(\text{index}(x))$，同样选择$d_x$个参数定义多项式$q_x$，其中$\text{parent}(x)$表示父节点，$\text{index}(x)$表示节点编号。

2) Y表示叶节点的集合，任取与q互素的2个素数$a,b \in Z_q$；对于所有节点$i \in Y$，任选$v_i \in Z_q$。计算$C = k_e e(g,g)^{sa}$，$C_0 = g^s$，与访问策略相关的密文部分为$CT_1 = \left\{C,C_0,\left\{C_{i,1},C_{i,2}\right\}\right\}$，其中，$C_{i,1} = g^{q_i(0)}$，$C_{i,2} = g^{v_{\text{attr}(i)}q_i(0)}$,$i \in Y$,$\text{attr}(i)$表示节点$i$的关联属性。

3) $\forall j \in \text{cover}(\text{RL})$，计算与撤销列表RL相关的密文部分$\text{CT}_2 = \left\{T_j = y_j^s\right\}$，$y_j = g^{x_j}$，产生的这部分密文用来防止已被撤销的用户仍能解密密文。

4) 最终得到密文$\text{CT} = \left\{\text{CT}_1,\text{CT}_2\right\}$。

2.2.4 像素标记和信息嵌入

在得到密文图像I'和密文CT后，图像所有者利用参数二叉树标记的方法在密文图像中嵌入辅助信息和密文CT。首先，图像所有者将参考像素P_{r}和特殊像素P_{s}分类出来后，在文献[13]的基础上，根据预测误差范围将密文图像I'中的剩余像素分为可嵌入像素P_{e}、自记录像素P_{ns}和不可记录像素P_{nn}。P_{r}为参考像素，在图像加密后的过程中像素值保持不变；P_{s}为图像右下角的单个像素，用于记录参数值α和β。剩余像素根据预测误差$e(i,j)$的范围，分为P_{e}、P_{ns}和P_{nn}。其中，可嵌入像素P_{e}的预测误差$e(i,j)$为

$$\left\lceil -\frac{n_\alpha}{2} \right\rceil \leqslant e(i,j) \leqslant \left\lfloor \frac{n_\alpha - 1}{2} \right\rfloor \tag{7}$$

对于自记录像素P_{ns}，其预测误差$e(i,j)$可以用$(8-\beta)$位表示。根据式(8)，可将自记录像素P_{ns}分为n_γ个子类别，n_γ的计算式为

$$n_\gamma = \begin{cases} 2^{8-\beta} - 2, 2 \leqslant \beta \leqslant 5 \\ 0, \text{其他} \end{cases} \tag{8}$$

P_{ns}中每个像素的前β位用β个“0”标记，剩下$(8-\beta)$位用于存储预测误差值$e(i,j)$，取值范围为$\left[\left\lceil \frac{-n_\alpha}{2} \right\rceil - \frac{n_\gamma}{2}, \left\lceil \frac{-n_\alpha}{2} \right\rceil\right) \cup \left(\left\lfloor \frac{n_\alpha - 1}{2} \right\rfloor, \left\lfloor \frac{n_\alpha - 1}{2} \right\rfloor + \frac{n_\gamma}{2}\right]$。

不可记录像素P_{nn}的预测误差$e(i,j)$不在上述2个范围内，用8个“0”二进制编码进行标记。

以$\alpha = 3$、$\beta = 2$为例，说明像素分类、像素标记和信息嵌入过程。标记位的编码如表2所示，图7为像素分类过程，其中，图7(b)为根据预测误差将图6(d)中像素分类后的情况。将参数α和β分别转换为二进制“0011”和“0010”，存储到特殊像素P_{s}中，P_{s}中原来的像素值作为辅助信息附加在秘密信息的前面。对于P_{e}和P_{ns}中的像素，在标记之前先进行位序反转，对像素标记分类后，再次进行位序反转操作。位序反转是为了防止因直接修改像素最高有效位导致原始图像内容泄露，像素标记过程如图8所示。

表2 $\alpha = 3$、$\beta = 2$时标记位的编码

像素	标记位	编码
P_{nn}	[−255,−35]∪[34,255]	00000000
P_{ns}	[−34,−4]∪[3,33]	00
P_{e}	−3	010
	−2	011
	−1	100
	0	101
	1	110
	2	111

P_{r}	P_{r}	P_{r}	P_{r}
P_{r}	P_{nn}	P_{ns}	P_{e}
P_{r}	P_{ns}	P_{e}	P_{e}
P_{r}	P_{e}	P_{e}	P_{S}

(a) 预测像素误差

151	149	152	153
153	114	4	−3
149	−4	1	1
152	−1	2	−2

(b) 分类后的像素

图7 像素分类过程

当$\alpha = 3$、$\beta = 2$时，对于一个8位的自记录像素P_{ns}，前2位标记为“00”，剩余6位用于记录预测误差。其中，6位中的最高位为符号位，如果误差值非负，则符号位为“1”；反之，则为“0”。其

余5位表示$e-e_{\max}(e\geqslant 0)$或$e-e_{\min}(e<0)$的值。由式(7)可知，$e_{\max}=2$，$e_{\min}=-3$。

10001111	11100000	11000110	11101011
10010010	00111110	10001111	11010101
11011001	10101110	00101110	10011100
01111100	01100001	11101100	10100100

(a) 密文图像的二进制表示

10001111	11100000	11000110	11101011
10010010	00111110	11110001	10101011
11011001	01110101	01110100	00111001
01111100	10000110	00110111	10100100

(b) P_e和P_{ns}像素位序反转

10001111	11100000	11000110	11101011
10010010	00000000	00100010	01001011
11011001	00000001	11010100	11011001
01111100	10000110	11110111	00110010

(c) 二进制编码标记像素

10001111	11100000	11000110	11101011
10010010	00000000	01000100	11010010
11011001	10000000	00101011	10011011
01111100	01100001	11101111	00110010

(d) 标记后的密文图像

图8　像素标记过程

图9为信息嵌入过程，“–”表示可嵌入像素P_e中嵌入信息的位置。像素标记后，将辅助信息、密文CT和需要嵌入的信息按照从左到右、自上而下的顺序嵌入密文图像中，最终得到携密密文图像I_e'。

10001111	11100000	11000110	11101011
10010010	00000000	01000100	-----010
11011001	10000000	-----011	-----011
01111100	-----001	-----111	00110010

(a) 标记后的密文图像

嵌入信息= 101001000011111101010110 (p_s | p_{nn} | CT)

10001111	11100000	11000110	11101011
10010010	00000000	01000100	10100010
11011001	10000000	10000011	11111011
01111100	01010001	10110111	00110010

(b) 携密密文图像

图9　信息嵌入过程

2.2.5　信息提取和图像恢复

数据使用者DU从云服务器中得到携密密文图像I_e'后，按照嵌入过程逆操作提取出嵌入信息。首先，保持参考像素P_r不变，数据使用者从右下角的特殊像素P_s中计算出参数α和β的值；然后，对像素的二进制序列进行位序反转，通过标记位对像素进行分类；最后，按照从左至右、自上而下的顺序，从可嵌入像素P_e的前$(8-\alpha)$位中提取出辅助信息和密文CT，实现嵌入信息的可逆提取。提取出嵌入信息后，只有当DU的属性集合P满足访问策略T的要求时，才能够解密CT得到加密密钥k_e。

密钥生成中心根据DU的属性集合P和撤销列表RL生成私钥SK。SK分为两部分，其中一部分与用户属性相关：$\forall r,t,\varepsilon\in Z_q$，$\forall\sigma\in P$，设置哈希函数$H_1:\{0,1\}\rightarrow G$，计算$D=g^{\frac{(a+bt)}{\varepsilon}}H_1(u)^r$，$D_{\sigma,1}=H_1(u)^{\varepsilon r}g^{v_\sigma r}$，$D_2=g^r$；另一部分与撤销列表相关，计算$K_u=g^{\frac{bt}{x_{i_u}}}$，$i_u$表示BT中与DU相关的叶子节点。DU得到$\mathrm{SK}=\left\{D,D_{\sigma,1},D_2,K_u,\{x_i\}_{i\in \mathrm{path}(i_u)},\varepsilon\right\}$后进行解密操作，过程如下。

1) 令$\theta=\dfrac{x_{i_u}}{x_j}$，计算$M$为

$$M=e\left(K_u,T_j\right)^\theta=e\left(g^{\frac{bt}{x_{i_u}}},y_j^s\right)^\theta=e(g,g)^{bts}\tag{9}$$

2) 定义$\mathrm{DecryptNode}(\mathrm{CT},\mathrm{SK},x)$，$x$为叶节点，令$\sigma=\mathrm{attr}(x)$，计算过程为

$$\mathrm{DecryptNode}(\mathrm{CT},\mathrm{SK},x)=\frac{e\left(D_{\sigma,1},C_{x,1}\right)}{e\left(D_{\sigma,1},C_{x,1}\right)}=$$

$$\frac{e\left(H_1(u)^{\varepsilon r}g^{v_\sigma r},g^{q_x(0)}\right)}{e\left(g^r,g^{v_{\mathrm{attr}(x)}q_x(0)}\right)}=$$

$$\frac{e\left(H_1(u),g\right)^{\varepsilon r q_x(0)}e\left(g,g\right)^{r v_\sigma q_x(0)}}{e(g,g)^{r v_\sigma q_x(0)}}=e\left(H_1(u),g\right)^{r q_x(0)}\tag{10}$$

3) 根据式(10)，计算解密结果W_{root}为

$$W_{\mathrm{root}}=\mathrm{DecryptNode}(\mathrm{CT},\mathrm{SK},\mathrm{RL})=$$

$$e\left(H_1(u),g\right)^{\varepsilon r q_{\mathrm{root}}(0)}=e\left(H_1(u),g\right)^{\varepsilon r s}\tag{11}$$

4) 计算得到对称密钥k_e为

$$\frac{CW_{\mathrm{root}}M}{e\left(C_0,D\right)^\varepsilon}=\frac{k_e e\left(g,g\right)^{sa}e\left(H_1(u),g\right)^{\varepsilon r s}e\left(g,g\right)^{bts}}{e\left(g^s,g^{(a+bt)/\varepsilon}H_1(u)^r\right)^\varepsilon}=$$

$$\frac{k_e e\left(g,g\right)^{sa}e\left(H_1(u),g\right)^{\varepsilon r s}e\left(g,g\right)^{bts}}{e\left(g,g\right)^{sa}e\left(H_1(u),g\right)^{\varepsilon r s}e\left(g,g\right)^{bts}}=k_e\tag{12}$$

若DU满足解密要求，在得到密钥k_e后，首先恢复出参考像素P_r，然后根据标记位和自记录像素标记方法确定预测误差，最后通过式(13)计算得到

原始图像的像素值，进而恢复出原始图像。

$$x(i,j)=e(i,j)+\hat{x}(i,j) \tag{13}$$

相反，若属性不满足解密要求，则无法获取原始图像的内容。由于上面的每一步都是可逆的，因此实现了可逆提取嵌入信息和无损恢复原始图像。

3　实验结果与分析

为了评估本文算法的性能，本节对嵌入率、安全性、可逆性、运行时间和适用性进行实验。实验环境为：主机配置CPU AMD Ryzen 5-4 600H 3.00 GHz，Windows 10操作系统，内存16 GB。在MATLAB R2021a编程实现图像加密和信息隐藏，使用Charm-Crypto库[37]在Python 3.8的环境下利用CP-ABE对图像加密密钥k_e进行加密，选择超奇异对称椭圆曲线群（“ss512”），选用的4幅测试图像如图10所示。

(a) Jetplane　(b) Baboon　(c) Lena　(d) Man

图10　测试图像

3.1　嵌入率

本文算法嵌入率与可嵌入像素数N_{P_e}、特殊像素数N_{P_s}、不可记录像素数$N_{P_{nn}}$和密钥加密后的大小N_{CT}有关。嵌入容量EC等于总嵌入容量与总辅助信息量之差，计算式为

$$EC=(8-\alpha)\times N_{P_e}-8\times\left(N_{P_{nn}}+N_{P_s}+N_{CT}\right) \tag{14}$$

其中，α表示单个像素中用于标记的二进制编码位数，总辅助信息量为$N_{P_{nn}}$、N_{P_s}和N_{CT}三者的比特数之和。嵌入率ER表示平均每个像素嵌入的比特数，单位是bit/pixel。对于大小为$m\times n$的灰度图像，嵌入率的计算式为

$$ER=\frac{(8-\alpha)\times N_{P_e}-8\times\left(N_{P_{nn}}+N_{P_s}+N_{CT}\right)}{m\times n} \tag{15}$$

当数据使用者的属性个数等于3时，图像所有者利用CP-ABE加密16 B对称密钥k_e后的N_{CT}为1 088 B。为了验证本文算法的嵌入性能，以图10中的4幅测试图像为例，对比文献[13]中的最大嵌入率，结果如表3所示，其中，“—”表示无法嵌入信息。分析表3中数据可以得到：当$\alpha=1$时，由于总嵌入容量少于辅助信息量，因此2种算法在标记后的密文图像中均无法嵌入信息；当$2\leqslant\alpha\leqslant5$时，本文算法的嵌入率均高于文献[13]。由表3可知，测试图像Jetplane、Baboon、Lena和Man的最大嵌入率分别为3.308 1 bit/pixel、1.479 5 bit/pixel、3.067 0 bit/pixel和2.835 6 bit/pixel，比文献[13]的最大嵌入率分别高0.283 1 bit/pixel、0.239 3 bit/pixel、0.380 3 bit/pixel和0.356 6 bit/pixel；当$6\leqslant\alpha\leqslant7$时，虽然许多像素被标记为可嵌入像素，但是对于可嵌入像素而言，标记位的二进制编码位数增多，导致可嵌入位减少，另外，此时相较于文献[13]，本文算法的不可记录像素产生的辅助信息量较大，导致嵌入容量相对较低。

为了说明本文算法嵌入容量较大，将本文算法最大嵌入率与文献[13-15]算法最大嵌入率进行对比，结果如图11所示。实验结果表明，相较于现有最佳算法[15]，本文算法在4幅测试图像中的平均嵌入率提高约0.2 bit/pixel。

为了说明本文算法的嵌入率不受测试图像随机性的影响，从BOSSbase[38]、BOWS-2[39]和UCID[40]这3个数据集中各取100幅测试图像进行实验并取平均值，比较本文算法与文献[13-15]算法的平均嵌

表3　$\beta=2$、$\alpha=1$～7时嵌入率对比

测试图像	算法	(1,2)	(2,2)	(3,2)	(4,2)	(5,2)	(6,2)	(7,2)
Jetplane	文献[13]	—	1.539 5	2.609 8	3.025 0	2.672 6	1.922 3	0.992 5
	本文算法	—	1.771 2	3.240 1	**3.308 1**	2.751 9	1.905 0	0.940 3
Baboon	文献[13]	—	—	—	0.203 9	0.969 2	1.240 2	0.861 5
	本文算法	—	0.067 6	0.687 8	1.178 7	**1.479 5**	1.280 2	0.595 1
Lena	文献[13]	—	0.393 3	1.660 9	2.686 7	2.644 7	1.928 5	0.991 9
	本文算法	—	1.161 8	2.538 5	**3.067 0**	2.727 6	1.906 2	0.940 5
Man	文献[13]	—	—	0.817 3	2.002 4	2.479 0	1.909 4	0.989 4
	本文算法	—	—	2.422 1	**2.835 6**	2.567 5	1.841 3	0.906 6

入率，结果如图12所示。结果表明，本文算法的平均嵌入率均高于现有算法。

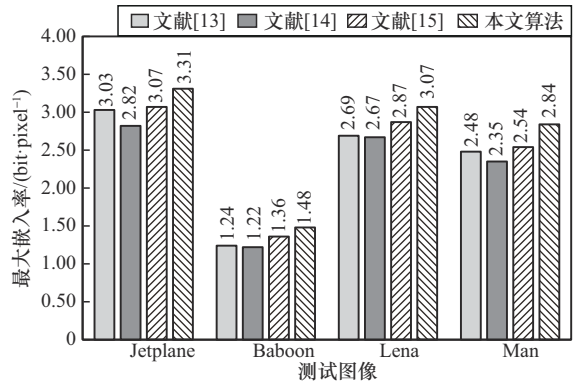


图11　最大嵌入率对比

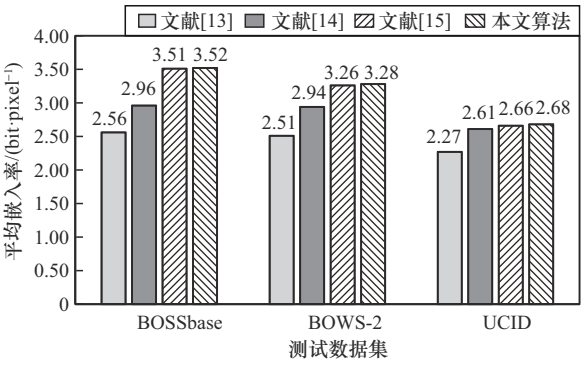


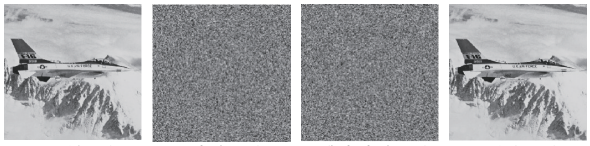
图12　本文算法与现有算法的平均嵌入率对比

3.2　安全性分析

直方图和信息熵是评估算法安全性的关键指标。本节直方图以测试图像Jetplane为例，说明原始图像在不同阶段的实验结果，并计算图10中4幅测试图像在不同阶段的信息熵。

3.2.1　直方图

图13和图14分别为本文算法在不同阶段生成图像的实验结果和直方图。从图14的直方图可知，图13(a)和图13(d)中的像素分布一致，说明本文算法能够实现无损恢复原始图像；图13(b)和图13(c)的像素分布均匀，而与图13(a)差异较大，说明本文算法可以保证原始图像的内容安全。



(a) 原始图像　(b) 密文图像　(c) 携密密文图像　(d) 恢复图像

图13　本文算法在不同阶段的实验结果

3.2.2　信息熵

为了进一步验证本文算法的安全性，计算信息熵$H(s)$来说明不同阶段生成图像的像素随机性。信息熵$H(s)$可通过式(16)计算得到，其中，s表示

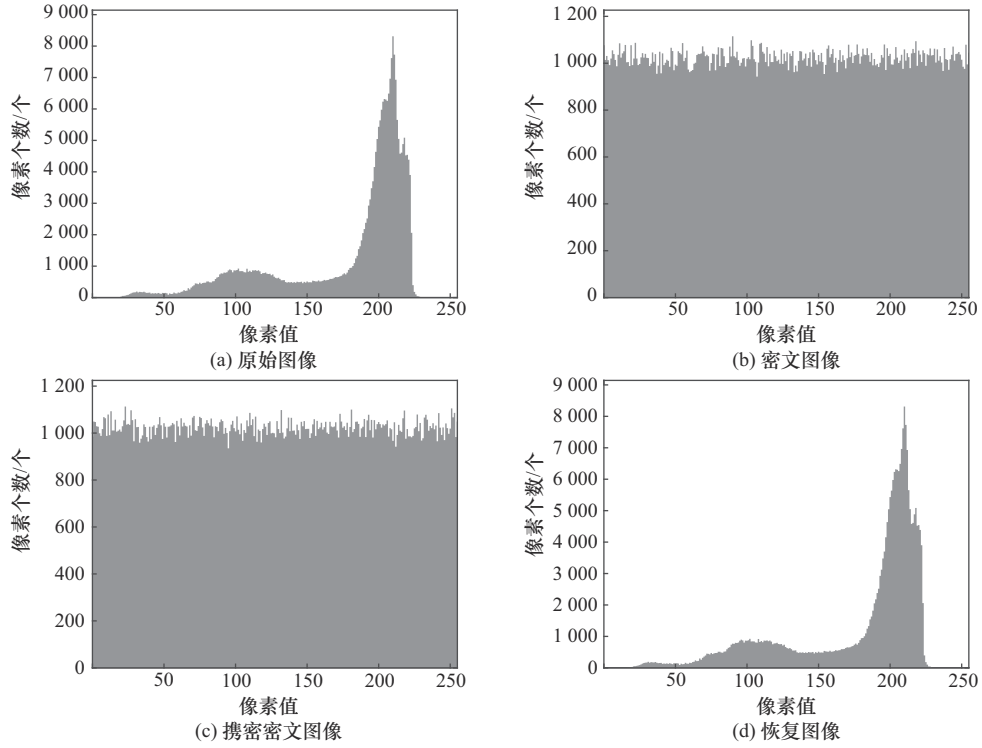


图14　本文算法在不同阶段图像的直方图

图像像素的灰度级，$p(s_i)$表示图像中特定灰度级s_i的相对概率，2^8表示灰度级的总数。

$$H(s)=-\sum_{i=0}^{2^8-1}p(s_i)\mathrm{lb}\left(p(s_i)\right) \tag{16}$$

对图10中4幅测试图像的不同阶段分别计算其信息熵，结果如表4所示。理论上信息熵最大值为8，值越接近8，像素随机性越好。结果表明，本文算法满足安全性要求。

表4 测试图像在不同阶段的信息熵

测试图像	原始图像	密文图像	携密密文图像
Jetplane	6.702 5	7.999 3	7.991 3
Baboon	7.358 3	7.999 2	7.998 1
Lena	7.445 1	7.999 3	7.993 4
Man	7.523 7	7.999 8	7.996 3

3.3 可逆性

峰值信噪比（PSNR, peak signal to noise ratio）和结构相似性（SSIM, structural similarity index measure）是2个用于评估算法可逆性的重要指标。其中，PSNR值的高低能够说明处理后的图像与原始图像的接近程度，值越高，接近程度越大，PSNR的单位是dB；当PSNR< 35 dB时，此时处理后的图像无法被人眼识别。SSIM通过评估感知图像质量的结构变化，以此来对比处理后的图像和原始图像的差异；SSIM值越接近于1，说明处理后的图像与原始图像越相似。

表5~表8分别给出了$\alpha=3$、$\beta=2$时，密文图像、标记后的密文图像、携密密文图像、恢复图像与原始图像的PSNR和SSIM的实验结果。可以看出，表5~表7中每个阶段图像的PSNR值较低且SSIM值接近0，说明与原始图像存在很大差异；表8中PSNR值均为+∞，SSIM值均为1，说明本文算法具有完全可逆性。

表5 密文图像与原始图像的PSNR和SSIM

测试图像	PSNR	SSIM
Jetplane	8.007 7	0.034 6
Baboon	9.510 8	0.029 9
Lena	9.225 5	0.038 5
Man	7.993 7	0.068 1

表6 标记后的密文图像与原始图像的PSNR和SSIM

测试图像	PSNR	SSIM
Jetplane	8.128 9	0.041 3
Baboon	9.199 7	0.004 5
Lena	9.671 9	0.038 8
Man	8.427 4	0.064 0

表7 携密密文图像与原始图像的PSNR和SSIM

测试图像	PSNR	SSIM
Jetplane	8.144 9	0.040 7
Baboon	9.201 6	0.005 8
Lena	9.684 9	0.038 5
Man	8.426 9	0.065 9

表8 恢复图像与原始图像的PSNR和SSIM

测试图像	PSNR	SSIM
Jetplane	+∞	1
Baboon	+∞	1
Lena	+∞	1
Man	+∞	1

3.4 运行时间分析

本文算法包括像素预测、图像加密、CP-ABE加密、像素标记、信息嵌入、信息提取和图像恢复7个步骤。其中前5个步骤由内容所有者完成，运行时间的长短会直接影响用户体验，后2个步骤由数据使用者完成，提取出嵌入信息后，利用私钥SK解密得到图像加密密钥k_e，进而恢复原始图像。在图像加密密钥k_e大小不变的前提下，内容所有者利用CP-ABE算法对k_e进行加密的时间开销如图15所示，实验结果取运行10次的平均值。由于文献[34]算法需要对4组对称密钥进行CP-ABE加密，所需加密时间较长。从图15中可以看出，属性个数越多，加密时间越长，二者呈正相关关系。

假设数据使用者DU的属性个数为3，比较本文和现有算法内容所有者的时间开销，取3个数据集中不同大小的图像运行10次的平均时间，结果如表9所示。可以看出，文献[13]中的内容所有者使用PBTL算法，在像素预测后对图像加密并利用二进制编码对密文图像中的像素进行标记，而后嵌

入辅助信息，所需时间最短。文献[14]算法需要内容所有者对具有稀疏特征的位置图进行算术编码，所需时间最长。文献[15]中的内容所有者利用Huffman编码对预测误差进行编码和标记，所需时间较长。相较于现有算法，本文算法时间开销较小。与文献[13]的主要区别是：本文增加了自记录像素分类以及利用CP-ABE对图像加密密钥k_e进行加密，并将加密结果嵌入密文图像中，运行时间相对较长。

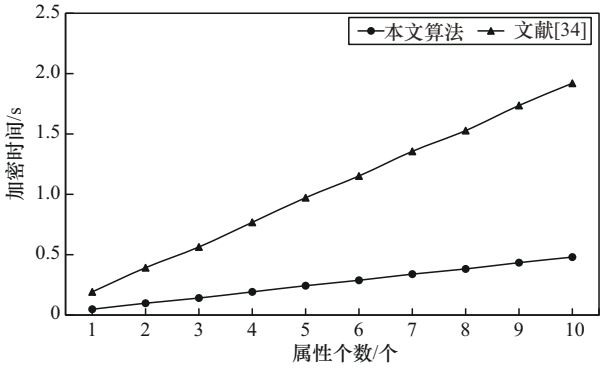


图15　CP-ABE加密时间

表9　　内容所有者的运行时间对比

图像大小	运行时间/s			
	文献[13]	文献[14]	文献[15]	本文算法
512像素 × 384像素	9.59	15.48	13.22	9.80
384像素 × 512像素	9.58	15.47	13.23	9.78
512像素 × 512像素	13.66	23.09	21.24	13.87

3.5　适用性

计算复杂度和嵌入率是衡量算法适用性的重要指标。在云计算多用户应用场景中，实现对加密数据的细粒度访问控制同样重要。文献[20-21]基于同态加密构造RDH-EI算法，运算量较大，且存在数据扩展的问题，实际应用受限。文献[4,24]基于R-LWE和LWE构造RDH-EI算法，安全性高，但运算效率较低。本文提出基于属性的密钥封装机制，解决了云环境多用户应用场景中密钥分发、管理和更新困难的问题，实现了对密文图像的细粒度访问控制，具有嵌入容量大、计算复杂度小的优点，表10为本文算法与其他算法的性能对比。

表10　　不同算法的性能对比

算法	加密方式	计算复杂度	嵌入率	访问控制
文献[4]	R-LWE	$O(N^2)$	低	否
文献[20]	Paillier	$O(N^3)$	低	否
文献[21]	全同态加密	$O(N^3)$	低	否
文献[24]	LWE	$O(N^2)$	低	否
本文算法	流密码	$O(N)$	高	是

4　结束语

本文将密文策略属性基加密与密文域可逆信息隐藏相结合，针对当前云环境多用户应用场景中密钥分发、管理和更新困难的问题，提出一种基于属性的密钥封装机制，利用CP-ABE对图像加密密钥进行加密，并将加密后的密钥作为秘密信息嵌入密文图像中，实现对密文图像的细粒度访问控制。同时，针对现有PBTL算法嵌入容量不高的问题，在根据预测误差对像素进行分类时，将不可嵌入像素细分为自记录像素和不可记录像素2类，从而减少了辅助信息量，增大了嵌入容量。后续将从以下两方面进行深入研究，一是选择其他预测误差的方法，使更多的像素能够被标记为可嵌入像素，并优化参数选择来提高嵌入率；二是针对云环境中可能存在滥用解密权限的恶意用户，增加CP-ABE的身份追踪功能。

参考文献：

[1] ABDULKAREEM N M, ZEEBAREE S R M, SADEEQ M A M, et al. IoT and cloud computing issues, challenges and opportunities: a review[J]. Qubahan Academic Journal, 2021, 1(2): 1-7.

[2] QI K L, ZHANG M Q, DI F Q, et al. High capacity reversible data hiding algorithm in encrypted images based on image adaptive MSB prediction and secret sharing[J]. Tsinghua Science and Technology, 2025, 30(3): 1139-1156.

[3] LI M Y, ZHU Y T, DU R Z, et al. Verifiable en- crypted image retrieval with reversible data hiding in cloud environment[J]. IEEE Transactions on Cloud Computing, 2025, 13(1): 397-410. D

[4] 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.

[5] PUECH W, CHAUMONT M, STRAUSS O. A reversible data hiding method for encrypted images[C]//Conference on Security, Forensics, Steganography, and Watermarking of Multimedia Contents. Bellingham: SPIE Press, 2008: 534-542

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

[7] 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): 219-230.
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 on Communications, 2022, 43(8): 219-230.

[8] 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, 2022, 32(2): 451-466.

[9] 杨尧林, 和红杰, 陈帆, 等. 基于预测误差自适应编码的图像加密可逆数据隐藏[J]. 计算机研究与发展, 2021, 58(6): 1340-1350.
YANG Y L, HE H J, CHEN F, et al. Reversible data hiding of image encryption based on prediction error adaptive coding[J]. Journal of Computer Research and Development, 2021, 58(6): 1340-1350.

[10] 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.

[11] 蒋宗宝, 张敏情, 董炜娜, 等. 基于自适应中值预测和霍夫曼编码的密文域可逆信息隐藏算法[J]. 科学技术与工程, 2024, 24(27): 11752-11762.
JIANG Z B, ZHANG M Q, DONG W N, et al. Reversible data hiding algorithm in encrypted images based on adaptive Median edge detection and huffman coding[J]. Science Technology and Engineering, 2024, 24(27): 11752-11762.

[12] ZHANG X M, ZHANG X Q, YU C Q, et al. Re- versible data hiding in encrypted images using prediction error modification and basic block compression[J]. Signal Processing, 2025, 231: 109896.

[13] WU Y Q, XIANG Y Z, GUO Y T, et al. An im- proved reversible data hiding in encrypted images using parametric binary tree labeling[J]. IEEE Transactions on Multimedia, 2020, 22(8): 1929-1938.

[14] 陈佳妮, 徐达文. 利用可变预测的密文域可逆信息隐藏[J]. 中国图象图形学报, 2024, 29(1): 95-110.
CHEN J N, XU D W. Reversible data hiding in en- crypted images using variable prediction[J]. Journal of Image and Graphics, 2024, 29(1): 95-110.

[15] 王玉, 孔祥婷, 吴媛媛. 基于像素调制自适应编码密文域的可逆信息隐藏算法[J]. 湖北大学学报(自然科学版), 2025, 47(1): 109-117.
WANG Y, KONG X T, WU Y Y. Reversible data hiding algorithm with pixel modulation adaptive coding in encrypted domain[J]. Journal of Hubei University (Natural Science), 2025, 47(1): 109-117.

[16] ANKUR, KUMAR R, SHARMA A K. Reversible data hiding in encrypted image using bit-plane based label-map encoding with optimal block size[J]. Journal of Information Security and Applications, 2025, 90: 104005.

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

[18] 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.

[19] WU H T, CHEUNG Y M, YANG Z Y, et al. A high-capacity reversible data hiding method for homomorphic encrypted images[J]. Journal of Visual Communication and Image Representation, 2019, 62: 87-96.

[20] 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.

[21] 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.

[22] WU H T, CHEUNG Y M, ZHUANG Z W, et al. Lossless data hiding in encrypted images compatible with homomorphic processing[J]. IEEE Transactions on Cybernetics, 2023, 53(6): 3688-3701.

[23] KE Y, ZHANG M Q, LIU J, et al. A multilevel re- versible data hiding scheme in encrypted domain based on LWE[J]. Journal of Visual Communication and Image Representation, 2018, 54: 133-144.

[24] KE Y, LIU J, HAN Y L. Two-stage reversible data hiding in encrypted domain with public key embedding mechanism[J]. Signal Processing, 2025, 233: 109918.

[25] WU H T, CHEUNG Y M, TIAN Z H, et al. Lossless data hiding in NTRU cryptosystem by polynomial encoding and modulation[J]. IEEE Transactions on Information Forensics and Security, 2024, 19: 3719-3732.

[26] YANG Y L, HE H J, FENG Z, et al. Cloud-based privacy-preserving medical images storage scheme with low consumption[J]. IEEE Transactions on Multimedia, 2025, 27: 3556-3570.

[27] ZHANG L, OU Z R, HU C H, et al. Data sharing in the metaverse with key abuse resistance based on decentralized CP-ABE[J]. IEEE Transactions on Computers, 2025, 74(3): 901-914.

[28] LI J G, ZHANG E F, HAN J G, et al. PH-MG-ABE: a flexible policy-hidden multigroup attribute-based encryption scheme for secure cloud storage[J]. IEEE Internet of Things Journal, 2025, 12(2): 2146-2157.

[29] BETHENCOURT J, SAHAI A, WATERS B. Ci- phertext-policy attribute-based encryption[C]//Proceedings of the 2007 IEEE Symposium on Security and Privacy (SP '07). Piscataway: IEEE Press, 2007: 321-334.

[30] 宁建廷, 黄欣沂, 魏立斐, 等. 支持恶意用户追踪的属性基云数据共享方案[J]. 计算机学报, 2022, 45(7): 1431-1445.
NING J T, HUANG X Y, WEI L F, et al. Tracing malicious insider in attribute-based cloud data sharing[J]. Chinese Journal of Computers, 2022, 45(7): 1431-1445.

[31] 姜美羡, 高军涛, 裴焘. 格上高效且可撤销的密文策略属性基加密方案[J]. 系统工程与电子技术, 2025, 47(4): 1364-1373.
JIANG M X, GAO J T, PEI T. Efficient and revo- cable ciphertext-policy attribute-based encryption scheme on lattice[J]. Systems Engineering and Electronics, 2025, 47(4): 1364-1373.

[32] 杜瑞忠, 张添赫, 石朋亮. 基于区块链且支持数据共享的密文策略隐藏访问控制方案[J]. 通信学报, 2022, 43(6): 168-178.
DU R Z, ZHANG T H, SHI P L. Ciphertext policy hidden access control scheme based on blockchain and supporting data sharing[J]. Journal on Communications, 2022, 43(6): 168-178.

[33] 张嘉伟, 马建峰, 马卓, 等. 云计算中基于时间和隐私保护的可撤销可追踪的数据共享方案[J]. 通信学报, 2021, 42(10): 81-94.
ZHANG J W, MA J F, MA Z, et al. Time-based and privacy protection revocable and traceable data sharing scheme in cloud computing[J]. Journal on Communications, 2021, 42(10): 81-94.

[34] CHEN T Y, LIU Y, CHEN X J. Image-oriented ci- phertext-policy attribute-based encryption system[C]//Proceedings of the 2022 18th International Conference on Computational Intelligence and Security (CIS). Piscataway: IEEE Press, 2022: 366-370.

[35] NAOR D, NAOR M, LOTSPIECH J. Revocation and tracing schemes for stateless receivers[C]//Advances in Cryptology — CRYPTO 2001. Berlin: Springer, 2001: 41-62.

[36] 王经纬. 云环境下属性基加密方案数据可控性与可用性研究[D]. 扬州: 扬州大学, 2023.
WANG J W. Research on data controllability and data availability of attribute-based encryption for the cloud environment[D]. Yangzhou: Yangzhou University, 2023.

[37] AKINYELE J A, GARMAN C, MIERS I, et al. Charm: a framework for rapidly prototyping cryptosystems[J]. Journal of Cryptographic Engineering, 2013, 3(2): 111-128.

[38] BAS P, FILLER T, PEVNÝ T. Break our steganographic system: the ins and outs of organizing BOSS[C]//International Workshop on Information Hiding. Berlin: Springer, 2011: 59-70.

[39] BAS P, FURON T. Image database of BOWS-2[R]. 2017.

[40] SCHAEFER G, STICH M. UCID: an uncompressed colour image database[C]//Storage and Retrieval Methods and Applications for Multimedia. Bellingham: SPIE Press, 2003: 472-480.

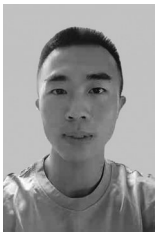
[作者简介]

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。

彭深（2000– ），男，湖南株洲人，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。

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

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、深度学习等。



董钰峰（1998– ），男，云南昆明人，武警工程大学硕士生，主要研究方向为信息安全、深度学习。