同态域 JPEG 可逆数据隐藏*

代 舒 辛 昕 钱振兴
(上海大学通信与信息工程学院 上海 200444)

摘 要：提出了两种基于同态加密的 JPEG 可逆数据隐藏方案，可分离方案和不可分离方案。在不可分离方案中，数据的提取是在明文中进行的，可以同时进行数据提取和图像恢复。在可分离方案中，数据提取是在密文中进行的，要先进行数据提取，再对图像密文解密并恢复图像。两种方案中数据提取的准确率均为 100%，同时针对同态加密算法时间成本较高的问题，两种方案在对 JPEG 图像的 DCT 系数加密之前，先进行整合，使多个系数合并为一个系数，从而节省了一定程度的时间成本。

关键词：不可分离数据隐藏；可分离数据隐藏；同态加密
中图分类号：TP391 **文献标识码**：A **国家标准学科分类代码**：510.4050

Reversible data hiding in JEPG image based on homomorphic encryption

Dai Shu Xin Xin Qian Zhenxing
(School of Communication and Information Engineering, Shanghai University, Shanghai 200444, China)

Abstract: This paper proposes two reversibledata hiding in JEPG imagebased on homomorphic encryptionschemes: inseparable and separablereversible data hiding. In the inseparable scheme, data extraction can only be done in the plain-text, and image recovery is performed simultaneously. In the separable scheme, the data can be extracted directly in the cipher-text, and the image recovery and decryption is conducted after data extraction. The accuracies ofthe extraction hidden data of the two schemesare both 100%. At the same time, for the higher time costs of homomorphic encryption, the two schemesmerge several factors into one before encryption to save the time to some degree.

Keywords: inseparable data hiding; separable data hiding; homomorphic encryption

1 引 言

随着多媒体技术与计算机网络迅速发展，通过网络进行数字数据传输变得非常普遍，数字图像因为直观、生动、形象的特点被广泛应用[1-2]。但是，在传输过程中，数字图像可能会被进行恶意的篡改、复制和非法传播等攻击[3]。因此，在通过图像进行数据传输的过程中，如何保证图像安全，特别是带有隐私数据机密的图像，成为了一个非常重要的问题。

近些年，有很多技术用于解决这个问题，其中数据隐藏与加密是两种非常重要的技术。很多研究往往只是采用一种技术，但是现实生活中有的应用需要将两种技术结合起来才可以解决。目前已有将两种技术结合起来进行数据传输的方案[4-7]，有的方案中数据隐藏和加密是分开进行的，即将图像分为两部分，一部分用来隐藏数据，一部分进行加密保护隐私数据[8-9]。Khan 等人[10]提出了基于离散余弦变换(DCT)的方案，选取重要的系数用来做加密，其余的系数用来嵌入数据。Abd-Eldayem 等人[11]提出了一种基于 DCT 变换的算法，该算法将数据嵌入到中频数据中，低频与高频数据用来做加密。有的方案是先将数据隐藏到明文图像中，然后再对图像进行加密。Bouslimi 等人[12]提出一种基于小波包变换和离散小波变换的算法。该算法是对载体进行小波包变换后，利用奇异值分解将数据嵌入到载体中，然后再对图像进行加密。还有一些方案，数据的嵌入是在密文中进行的，即先对图像进行加密，然后在密文中进行数据嵌入。在这种情况下，图像拥有者为了能够安全的共享自己的图像，可以在将图像发送出去之前对图像进行加密。当数据隐藏者需要隐藏额外的数据时，可以直接在密文图像中嵌入自己的数据，即使他不知道加密图像的内容。接收者得到图像后既可以恢复出图像，又可以提取隐藏的数据。Zhang[13]通过异或的方法对图像进行加密，然后将数据嵌入到图像的最低有效位上。Zhang[14]将密文图像的最低有效位进行压缩以生成稀疏空间用于嵌入数据。因为只有嵌入了数据的最低有效位改变了，直接解密得到的图

收稿日期：2016-03
* 基金项目：国家自然科学基金(61572308，U1536108)、上海市青年科技启明星人才计划基金(14QA1401900)资助项目

像的质量比较理想。Qian 等人[15]提出了 JPEG 图像的密文中可逆数据隐藏[15]，利用图像的块效应进行数据提取。Zhang 等人[16]提出了基于同态加密的无损与可逆数据隐藏，提高了密文数据隐藏中加密算法的安全性，在无损方案中图像可以无损的恢复，且嵌入的数据可以直接在密文中提取。

本文结合同态加密算法提出了两种 JPEG 图像的可逆数据隐藏算法，不可分离方案和可分离方案。这两种方案均是对 JPEG 图像的 DCT 系数进行处理，然后进行加密与数据隐藏。在不可分离方案中，数据的提取是在明文中进行的，可以同时进行数据提取和图像恢复。在可分离方案中，数据的提取是在密文中进行的，要先进行数据提取，再将图像解密并恢复。同时，本文方案采用的加密算法为同态加密，针对其加密时间成本较高的问题，本文的两种方案在对图像加密之前，要先进行处理并整合，使多个系数合并为一个系数[17]，从而很大程度上节省了时间成本。

2　总体框架

本文一共提出了两个密文域可逆数据隐藏方案：不可分离方案与可分离方案，两个方案加密部分均是采用同态加密实现的。在不可分方案中，一共有 3 个参与方，加密者、数据隐藏者和接收者，数据的提取是在明文中进行，接收者可以同时进行数据提取和图像恢复，其总体方案如图 1 所示。

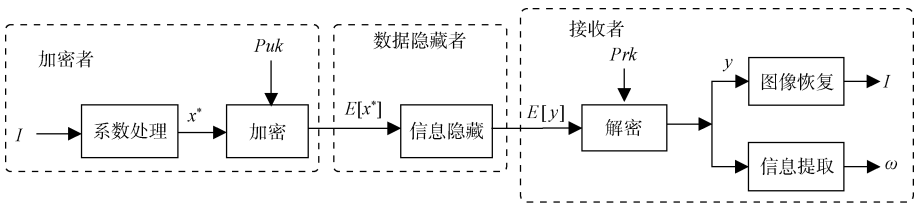

图 1　不可分离方案

加密者先将 JPEG 图像 I 的 AC 系数进行整合得到 $E[\boldsymbol{x}^*]$，然后将 $\boldsymbol{x}^*$ 用公钥 Puk 加密得到图像 DCT 系数的密文 $E[\boldsymbol{x}^*]$，最后将 $E[x^*]$ 发送给隐藏者；隐藏者接收到 $E[\boldsymbol{x}^*]$ 后，先用公钥 Puk 将需要嵌入的数据 $\boldsymbol{w}^*$ 进行加密得到 $E[\boldsymbol{w}^*]$，然后将其嵌入到 $E[\boldsymbol{x}^*]$ 中得到 $E[\boldsymbol{y}]$，最后数据嵌入者将 $E[\boldsymbol{y}]$ 发送给接收者；接收者接收到 $E[y]$ 后可以同时进行数据提取和图像恢复得到 $\boldsymbol{w}$ 和 I。

与不可分离方案相同，可分离方案中，一共有 3 个参与方，提供者、数据隐藏者和接收者，但是数据的提取是在密文中进行的，接收者需要先进行数据提取，然后再进行图像恢复。

3　系数处理与同态加密

3.1　系数处理

在本节的两个方案中，将系数加密之前首先要对 JPEG 图像的系数进行处理，将多个系数合并为一个系数。两个方案系数处理采用相同的方法，图像提供者将 JPEG 图像 I 的每一块分为 15 个子频带，即 $L_u=(l_1,l_2,\cdots,l_u)$，$u=(1,2,\cdots,15)$，如图 2 所示。将每个子频的非零系数进行修改，首先需要求出每个子频带 L_u 负系数的最大绝对值 l_{um}，然后将每个子频带的非零系数加上常数 a_u，$a_u=l_{um}+1$，得到 $X'_u=(x_1,x_2,\cdots,x_u)$，$X'_u\geqslant 0$ 恒成立。然后每个图像块选择 $s\times n$ 个修改后的 AC 系数，令 $X=(x_1,x_2,\cdots,x_{s\times n})$，用式(1)的方式[17]将 X 进行整合，每 s 个系数合并为一个系数。

$$x_i^*=\sum_{k=1}^{k=s-1} b^{s-k-1}\cdot x_{s\times i-(s-k)} \tag{1}$$

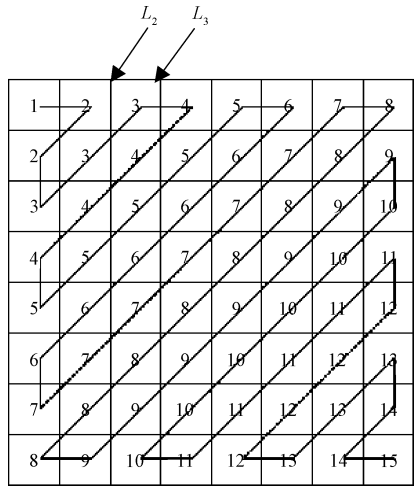

图 2　图像块子频带示意图

式中：$i=1,2,\cdots,n$，b 为固定常数，$b>2\,|x_i|_{\max}$。

3.2　同态加密系统

假设一个加密系统的同态操作是“$*$”，如果存在一个操作 $f(,;,)$，则任意 x_1 和 x_2，可以得到：

$$(f(E[x_1],E[x_2])=x_1*x_2 \tag{2}$$

其中 $D[]$、$E[]$ 表示解密、加密操作。显而易见，由式(2)可以得到一个加法同态加密映射了一个在明文域的加法到一个密文域的操作[18](通常是乘法)。给定两个明 x_1 和 x_2，下列等式成立：

$$D[E[x_1],E[x_2]]=x_1+x_2 \tag{3}$$

从而可得：

$$D[E[x]^{\beta}]=\beta x \tag{4}$$

具有同态性质的公钥密码体制有很多,常见的有 Paillier、RSA、ECC 等,本文所提方案的加密是依靠 Pillier 算法实现的。Paillier 算法[18]的密钥生成及加解密操作具体步骤如下。

1)生成密钥:选择两个大素数 p 和 q,计算 $n=pq$,$\varphi(n)=lcm(p-1,q-1)$,其中 lcm 为最小公倍数。G 为模 n^2 的乘法群,即 $G=\{x \mid x \in Z_{n^2}\}$ 随机选择 $g \in G$,使得 g 满足 $gcd=(L(g^{\varphi} mod\ n^2),n)=1$,其中 gcd 为最大公约数。则该加密系统的公钥为 (g,n),私钥为 $\varphi(n)$,明文 h 取值域为 Z_n,即范围为 $h<n$。设要加密的数据为 $h \in Z_n$,随机选择数 $r \in Z_n^*$,h 对应的密文为 e,一般情况下素数 p 和 q 要大于 2^{256} 才能保证 Paillier 算法的安全性。

2)加密:

$$e=g^h r^n mod\ n^2 \tag{5}$$

3)解密:

$$h=\frac{L(e^{\varphi} mod\ n^2)}{L(g^{\varphi} mod\ n^2)} mod\ n \tag{6}$$

4　数据隐藏

在本文的两种方案中,数据嵌入者收到 $E[x_i^*]$ 后,首先将系数 x_i^* 扩大到 $2x_i^*$,由 Paliier 算法的加同态性质得密文中 x_j^* 的扩展如下:

$$E[2x_i^*]=E[x_i^*]^2 \tag{7}$$

但是,两种方案选择扩展的系数不同。

4.1　不可分离方案

在不可分离方案中,是将所有的密文系数进行扩展,然后生成需要嵌入的数据,为二进制数据 $W=(w_1,w_2,\cdots,w_{s\times n})$,$w_j \in \{0,1\}$,$j=(1,2,\cdots,s\times n)$;生成数据后,数据隐藏者把相邻的 s 个数据 w_j 整合为一个数,得集合 $W^*=\{w_1^*,w_2^*,\cdots w_n^*\}$,合并方式如式(1)所示。求得 w_i^* 后,用 Puk 对 w_i^* 进行加密得 $E[w_i^*]$,然后嵌入到 $E[x_i^*]$ 中得 $E[y_i]$,嵌入方式如下:

$$E[y_i]=E[2x_i^*]\times E[w_i^*] \tag{8}$$

求得 $E[y_i]$ 后,数据隐藏者将 $E[y_i]$ 发送给接收者。

4.2　可分离方案

在可分离方案中,是选择 m 个高频系数 x_i^* 进行扩展,将 x_i^* 扩大到 $2x_i^*$,密文中 x_j^* 的扩展如式(7)所示。然后,令 $\boldsymbol{V}^*=(v_1^*,v_2^*\cdots,v_m^*)$,表示扩展后的系数,如图 3 所示,将所有的 $E[v_i^*]$ 转换为二进制流,用 t_i 表示二进制流的最低有效位,然后将 t_i 嵌入到 $E[v_{i+1}^*]$ 中,求得 $E[y_i^*]$,数据嵌入的方式如式(8)所示,具体步骤如下所示:

1)令 $E[y_1^*]=E[v_1^*]$,记 $E[y_1]$ 的最低有效位为 t_1,并用 Puk 将其加密得 $E[t_1]$,然后将 t_1 嵌入到 $E[y_2]$ 中得到 $E[y_2^*]$。

2)记 $E[y_2]$ 的最低有效位为 t_2,并用 Puk 将其加密得 $E[t_2]$,然后将 t_2 嵌入到 $E[y_3]$ 中,得到 $E[y_3^*]$。

3)依次类推,记 $E[y_{j-1}]$ 的最低有效位为 t_{j-1},并用

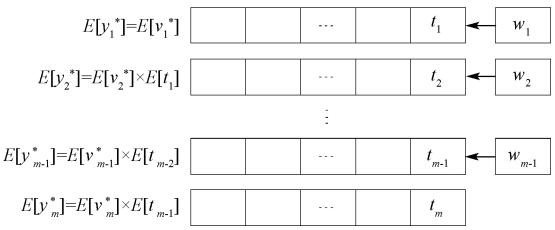

图 3　可分离方案数据嵌入过程

Puk 将其加密得 $E[t_{j-1}]$,然后将 t_{j-1} 嵌入到 $E[y_j]$ 中求得 $E[y_j^*]$,$j=1,2,\cdots,m-1$。

4)最后,记 $E[y_{m-1}]$ 的最低有效位为 t_{m-1},然后将 t_{m-1} 嵌入到 $E[y_m]$ 中得到 $E[y_m^*]$。

需要隐的数据为二进制数据,设为 $W=(w_1,w_2,\cdots,w_{m-1})$,$w_j \in \{0,1\}$,$j=1,2,\cdots,s\times n$。求得 $E[y_i^*]$ 后,数据嵌入分为两种情况:$i=1,2,\cdots,m-1$。时,用 w_j 代替 $E[y_{i-1}^*]$ 的最低有效位得 $E[y_{i-1}]$;当 $i=m$ 时,$E[y_i]=E[y_i^*]$。求得 $E[y_i]$ 后,数据隐藏者将 $E[y_i]$ 与未改变的图像数据一起发送给接收者。

5　数据提取与图像恢复

5.1　不可分离方案

接收到 $E[y_i]$ 后,接收者首先用 Prk 对 $E[y_i]$ 进行解密得 y_i,解密方法如式(6)所示,由 Paillier 的性质可得解密后 $y_i=2x_i^*+w_i^*$,如式(9)所示。求得 y_i 后,数据提取和系数拆分同时进行,嵌入的数据 w_j 可由式(10)和(11)求得,系数拆分可由式(12)和(13)求得。

$$y_i=(2x_{2i-1}+w_{2i-1})+b\times(2x_{2i}+w_{2i}) \tag{9}$$

$$w_{j+k-1}=mod((mod(y_i,b^k)-mod(y_i,b^{k-1})),2) \tag{10}$$

$$w_{j+s-1}=mod(floor(\frac{y_i}{b^{s-1}}),2) \tag{11}$$

$$x_{j+k-1}=floor((mod(y_i,b^k)-mod(y_i,b^{k-1}))/b^{k-1}) \tag{12}$$

$$x_{j+s-1}=floor(y_i/b^{s-1}) \tag{13}$$

式中:$j=1,2,\cdots,s\times(n-1)+1$;$k=1,2,\cdots,s-1$;$i=1,2,\cdots,n$,函数 $floor(\cdot)$ 表示向下取整;$j=s\times(i-1)+1$。求得系数后,接收者对其进行系数修改的逆操作。将 $X=(x_1,x_2,\cdots,x_{s\times n})$ 重新划分到子频带中,对每个系数按子频带进行整合前修改的逆操作。每个子频带中令 $g=(1,2,\cdots,u)$,若 $x_g>1$,则 $l_g=x_g-a_u$;否则,$l_g=x_g$,从而可以无损的恢复出原始图像。

5.2　可分离方案

接收者得到密文图像数据后,首先要对 $E[y_i]$,$i=1,2,\cdots,m$ 进行数据提取,将所有 $E[y_i]$ 转化为二进制流,由于 $E[y_i]$ 中只有 $i=(1,2,\cdots,m-1)$ 时,y_i 的最低有效位中嵌入了数据,令 $E[y_j]$,$j=1,2,\cdots,m-1$ 表示含数据信

息，所以数据提取只需要判断 $E[y_j]$ 即可。数据的提取通过判断 $E[y_j]$ 的最低有效位来实现，若 $E[y_j]$ 的最低有效位为 1，则 $w_j=1$；若 $E[y_j]$ 的最低有效位为 0，则 $w_j=0$。最后可得嵌入的数据 $W=w_1,w_2,\cdots,w_{m-1}$。

解密分为两部分，嵌入数据部分 $E[y_j]$，$i=1,2,\cdots,m-1$ 和未嵌入数据部分 $E[x^*]$。对于未嵌入数据部分 $E[x^*]$，是直接用 Prk 解密 $E[x^*]$ 得到 x^*。对于嵌入数据部分的密文系数 $E[y_j]$，首先是进行数据提取，提取数据后，用 Prk 对 $E[y_j]$ 进行解密，解密的过程如下所示。

1)对 $E[y_m]$ 进行解密，得 $y_m=2x_m^*+t_{m-1}$，并用式(14)求 t_{m-1}。

$$t_{m-1}=mod(2x_m^*,2) \tag{14}$$

2)用 t_{m-1} 替换 $E[y_{m-1}]$ 的最低有效位，然后对其进行解密得 y_{m-1}，并用式(14)求得 t_{m-2}。

3)以此类推，用 t_{m-j} 替换 $E[y_{m-j}]$ 的最低有效位，然后解密得到 y_{m-j}，$j=1,2,\cdots,m-1$。

解密后，得到的整合系数分为两种情况。嵌入了 t_j 的集合 $\boldsymbol{Y}=(y_1,y_2,\cdots,y_m)$ 和未做修改的系数集合 $\boldsymbol{X}^*=(x_1^*,\ x_2^*,\cdots\ x_{s\times n-m}^*)$。令 $Z=X^*\cup Y$，$Z=(z_1,z_2,\cdots,z_{s\times n})$，若接收者不对被扩展的系数进行收缩，直接进行图像恢复，则系数的拆分方法如式(15)和(16)所示。

$$x'_{j+k-1}=floor\{[mod(z_i,c^k)-mod(z_i,c^{k-1})]/c^{k-1}\} \tag{15}$$

$$x'_{j+s-1}=floor(z_i/c^{s-1}) \tag{16}$$

式中：$j=s\times(i-1)+1$；$i=1,2,\cdots,n$；$j=1,2,\cdots,s\times(n-1)+1$。系数拆分后，将 $\boldsymbol{X}'=(x'_1,x'_2,\cdots x'_{s\times n})$ 重新划分到子频带中，对每个系数按子频带进行整合前修改的逆操作。每个子频带中令 $g=1,2,\cdots,u$，若 $x'_g>1$，则 $l'_g=x'_g-a_u$；否则，$l'_g=x'_g$。每个子频带的系数恢复后，接收者可以恢复出原始图像，但是由于被扩展的系数没有被收缩，所以恢复出的图像质量下降。若接收者对扩展的系数进行收缩，则系数拆分分为两种情况进行：集合 $\boldsymbol{Y}=(y_1,y_2,\cdots,y_m)$ 的拆分方法如式(12)和(13)所示；集合 $\boldsymbol{X}^*=(x_1^*,x_2^*,\cdots,x_{s\times n-m}^*)$ 中系数的拆分如式(15)和(16)所示。这种方法求得系数后可以无损的恢复出原始图像。

6　实验结果

实验过程中，4 幅大小为 512×512 的 JPEG 图像 Pepper、Lena、Tiffany 和 Boats 用来验证图像质量与数据提取准确率，图 3.5 表示原始图像。本章提出的两种方案均是采用 JPEG 图像量化的系数来进行数据嵌入，且同态加密实验中生成的素数 p 和 q 都是大于 $2^{1\,024}$ 的大数，由于 Paillier 算法只能加密正数，所以两种方案都在对系数整合之前先将要加密的系数进行处理。将要加密的系数修改为正整数，然后再对系数进行整合，将多个系数合并为一个系数。在两个方案中，系数的修改都是将 JPEG 图像的每个图像块的系数分为 15 个子频带，对每个子频带的非零系数分别进行修改，每个子频带加的值不同。

系数修改后，将 s 个系数整合为一个数，然后将整合的系数进行加密发送给数据隐藏者。但是在不可分离方案中，数据隐藏者是将所有密文系数进行扩展，用于数据嵌入。由 5.1 节所示，图像解密后可无损的恢复出原始图像，而且数据提取的准确率为 100%。令 c 表示嵌入量，由于每个系数都可以嵌入 1 Byte 数据，所以一个图像块最多可以嵌入 64 Byte 数据。对一幅 512×512 的图像嵌入数据，Zhang 在文献[16]中提出的不可分离方案的最大嵌入率为 1/2，即最多嵌入 131 072 Byte 数据；本文提出的方案，最大嵌入率可达到 1，即最多嵌入 262 144 Byte 数据，提高了嵌入容量。

图 4　原始图像

图 5　直接恢复图像(Q=70)

同时,文献[16]中提出的方法,需要对所有的像素进行加密,由于同态加密算法的加密与解密过程计算量很大,在相同嵌入量下,本章方案只需加密合并后的系数,很大程度上减少了计算量。由表 1 可以看出,对于一幅大小为 512×512 的图像,相同嵌入量的情况下,文献[16]的方法需要加密的数据量远远大于本章所提出的方案。其中 c 表示嵌入量,k 表示最少需要加密的数据量。而且,本章方案中相同嵌入量下,s 越大,需要加密的数据量越少。可分离方案的系数修改与合并与不可分离方案相同,但是隐藏者只选择 m 个合并后的高频系数进行扩展并用于数据嵌入。隐藏者接收到密文系数后,选择 m 个高频系数进行扩展与数据嵌入。接收者在密文中提取数据,准确率为 100%。解密后,如果在系数拆分时,对扩展的系数进行收缩,则可以无损的恢复出原始图像。

表 1　相同嵌入量下不同方案需要加密的数据量

	c/bit		32 768	65 536	98 304	131 072
	文献[16]		262 144	262 144	262 144	262 144
k	本文	$s=2$	16 384	32 768	49 512	65 536
	方案	$s=4$	8 192	16 384	24 576	32 768

在可分离方案中,如果接收者不对扩展的系数进行收缩,直接进行图像恢复,则图像质量有所下降。取 $s=2$,$m=2$,每个图像块选择 zigzag 扫描的第 2～33 个系数进行合并,此时 $n=15$,每个图像块都选择 x_{15}^{*} 和 x_{16}^{*} 进行数据嵌入,一幅 512×512 的图像可以嵌入 4096 比特数据。图 5 表示的是直接恢复得到的图像(质量因子 $Q=70$)。图 6 表示不同质量因子的 JPEG 图像,直接恢复得到图像的峰值信噪比(peak signal-to-noiseratio, PSNR),因为数据是嵌入在高频系数上,所以随着质量因子增大,高频系数中负数的绝对值较大,非零系数的个数增加,被修改的系数增加且修改程度增大,因此图像峰值信噪比随着质量因子先增加后下降。

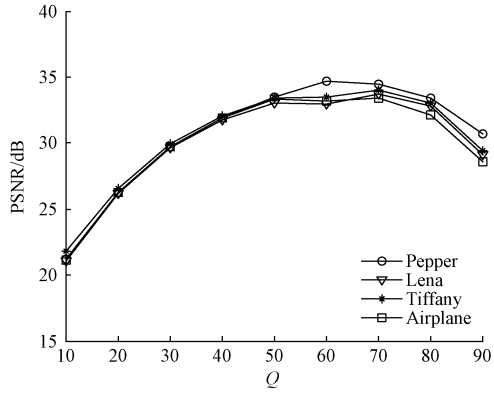

图 6　直接恢复的图像在不同质量因子下的 PSNR

图 7 表示 $Q=70$,$s=2$ 时,m 取不同值时,即嵌入量 c 不同时,直接恢复图像与原始图像的峰值信噪比的关系,m 与嵌入量 c 的关系如表 2 所示。由图可以看出,相同情况下随着 m 的增大,嵌入量就越大,被扩展的系数越多,从而被修改的系数越多,所以直接恢复的图像 PSNR 下降。

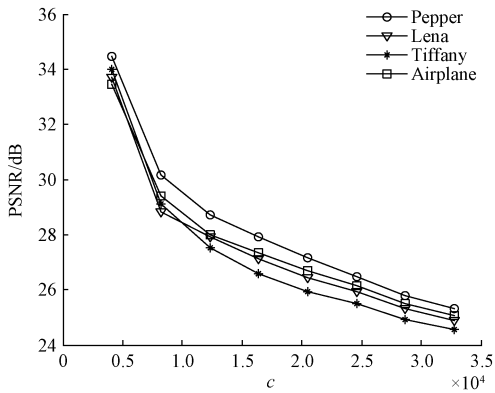

图 7　嵌入量不同时直接恢复图像的 PSNR

表 2　未授权图像未被篡改情况下实验数据

m	2	3	4	5	6	7	8	9
c/bit	4 096	8 192	12 288	16 384	20 480	24 576	28 672	32 768

图 8 表示的是令 $Q=70$,$m=2$,当 s 取不同的值时,直接恢复的图像与原始图像的峰值信噪比的关系,由图可以看出虽然嵌入量相同,但是 s 越大,被扩展的系数越多,从而被修改的系数越多,所以相同嵌入量下,随着 s 增大,直接恢复的图像 PSNR 下降。

6　结　论

本文提出了两种基于同态加密的 JPEG 可逆数据隐藏算法,不可分离方案和可分离方案。这两种方案均是对 JPEG 图像的 DCT 系数进行合并,然后再进行加密与数据嵌入。将多个系数合并为一个系数,一定程度解决同态加密算法耗时较长的问题,节省了时间成本。不可分离方案,需要先将含数据的密文信息进行解密,然后再进行数据提取和图像恢复。可分离方案,是先在密文中提取数据,然后再对图像解密并恢复。同时,可分离方案中,若接收者对扩展的系数不进行收缩,直接恢复图像,则图像的质量变差;若接收者对扩展的系数先进行收缩,再恢复图像,则也可以无损的恢复出原始图像。

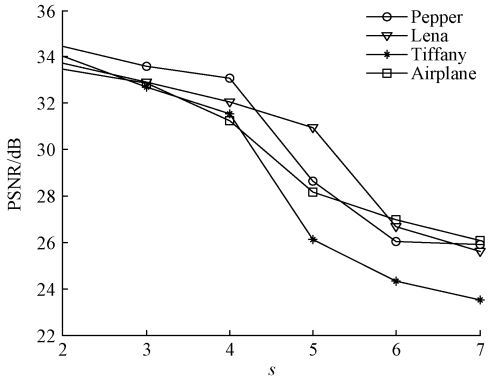

图 8　s 取值不同时直接恢复图像的 PSNR

参考文献

[1] 张国刚，徐向辉. 基于加权纹理特征的 SAR 图像目标识别算法[J]. 国外电子测量与技术，2015，34(9)：22-25.

[2] 高强，阳武，李倩. DBN 层次趋势研究及其在航拍图像故障识别中的应用[J]. 仪器仪表学报，2015，36(6)：1267-1274.

[3] 吴一全，史骏鹏，陶飞翔. 基于 SIFT 和 NMF-SVD 的 NSCT 域抗几何攻击水印算法[J]. 电子测量与仪器学报，2015，29(7)：961-969.

[4] 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.

[5] BIANCHI T，PIVA A，BAENI M. On the implementation of the discretefouriertransform in the encrypted domain [J]. IEEE Transactions on Information Forensics and Security，2009，4(1)：86-97.

[6] BIANCHI T，PIVA A，BAENI M. Composite signal representation for fast and storage-efficient processing of encrypted signals [J]. IEEE Transactions on Information Forensics and Security，2010，5(1)：180-187.

[7] ZHENG P，HUANG J. Discrete wavelet transform and data expansion reduction in homomorphic encrypted domain[J]. IEEE Transactions on Image Processing，2013，22(6)：2455-2468.

[8] ZHANGX P. Commutative reversible data hiding and encryption [J]. Security and Communication Networks，2013，11(6)：1396-1403.

[9] CANCELLARO M，BATTISTI F，ARLI M. A commutative digital image watermarking and encryption method in the tree structured haartransform domain[J]. Signal Processing：Image Communication，2011，26(1)：1-12.

[10] KHAN M I，JEOTI V，MALIKA S. A joint watermarking and encryption scheme for DCT based codecs[C]. Asia-Pacific Conference on Communications (APCC)，IEEE，2011，10(1)：816-820.

[11] ABD-ELDAYEM M. A proposed security technique based on watermarking and encryption for digital imaging and communications in medicine [J]. Egyptian Informatics Journal，2013，14(1)：1-13.

[12] BOUSLIMI D，COATRIEUX G，ROUX C. A joint encryption/watermarking algorithm for verifying the reliability of medical images：Application to ethographicimages [J]. Computer Methods and Programs in Biomedicine，2011，106(1)：47-54.

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

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

[15] QIAN Z X，ZHANG X P，WANG S Z. Reversible data hiding in encrypted JPEG bitstream[J]. IEEE Transactions on Multimedia，2014，16(5)：1486-1491.

[16] ZHANG X P，LONG J，WANG Z C. Lossless and reversible data hiding in encrypted images with public key cryptography[J]. IEEE Transactions on Circuits and Systems for Video Technology，2015，14(5)：1-10.

[17] BIANCHI T，PIVA A，BAENI M. Composite signal representation for fast andstorage-efficient processing of encrypted signals [J]. IEEE Transactionson Information Forensicsand Security，2010，5(1)：180-187.

[18] BIANCHI T，PIVA A. Secure watermarking for multimedia content protection：A review of its benefits and open issues[J]. IEEE Signal Processing Magazine，2013，30(2)：87-96.

作者简介

代舒，1992 年出生，上海大学通信与信息工程学院，工学硕士，从事数字图像处理工作。

辛昕，1990 年出生，上海大学通信与信息工程学院，工学硕士，从事数字图像处理工作。

钱振兴(通讯作者)，1981 年出生，上海大学通信与信息工程学院，副研究员，从事数字图像处理工作。

E-mail：zxqian@shu.edu.cn