激光与光电子学进展 先进成像

运用同态加密的高分遥感影像交换密码水印算法

李玉[1,2,3]，张黎明[1,2,3*]，王昊[1,2,3]，王小龙[1,2,3]

[1]兰州交通大学测绘与地理信息学院，甘肃 兰州 730070；

[2]地理国情监测技术应用国家地方联合工程研究中心，甘肃 兰州 730070；

[3]甘肃省地理国情监测工程实验室，甘肃 兰州 730070

摘要 交换密码水印是一种新兴的加密技术与数字水印技术相结合的方法，具有数据安全传输和版权追踪双重保护能力，这类方法在多媒体数据安全领域得到了广泛的应用。然而已有算法没有顾及高分辨率遥感影像的敏感性和特殊性，无法为高分辨率遥感影像提供完全保护。为解决这一问题，运用同态加密技术提出了一种适用于高分辨率遥感影像的交换密码水印算法。首先对原始影像进行分块处理；然后运用整数小波变换提取每个子块的低频系数和高频系数；最后利用Paillier算法加密每个子块的低频系数和高频系数，同时基于Paillier算法的加法同态特性，将水印信息嵌入到低频系数。实验结果表明，所提算法实现了加密操作和水印操作之间的可交换性，在明文数据和密文数据中均能成功重构原始水印，并且具有较高的加密安全性和良好的水印鲁棒性。

关键词 遥感影像；交换密码水印；Paillier加密；安全分发；版权保护

中图分类号 TP309.7 **文献标志码** A **DOI**：10.3788/LOP202259.1815012

Commutative Encryption and Watermarking Algorithm for High-Resolution Remote Sensing Images Based on Homomorphic Encryption

Li Yu[1,2,3], Zhang Liming[1,2,3*], Wang Hao[1,2,3], Wang Xiaolong[1,2,3]

[1]*Faculty of Geomatics, Lanzhou Jiaotong University, Lanzhou* 730070, *Gansu, China*;

[2]*National-Local Joint Engineering Research Center of Technologies and Applications for National Geographic State Monitoring, Lanzhou* 730070, *Gansu, China*;

[3]*Gansu Provincial Engineering Laboratory for National Geographic State Monitoring, Lanzhou* 730070, *Gansu, China*

Abstract Commutative encryption and watermarking (CEW) is an emerging method that combines encryption technology with digital watermarking technology, which has double protection capabilities to achieve secure transmission and copyright tracking. In the field of multimedia data security, this method has been extensively used. However, existing algorithms have not considered the sensitivity and specificity of high-resolution remote sensing (HRRS) images; thus, they cannot completely protect HRRS images. This study proposes a CEW algorithm based on homomorphic encryption to solve this problem. First, partitioning is performed on the original image, and then integer wavelet transform is used to extract low- and high-frequency coefficients. Finally, the Paillier algorithm encrypts the low- and high-frequency coefficients of each sub-block, and the watermark is embedded in the low-frequency coefficient. The experimental results show that the proposed algorithm can achieve commutativity between encryption and watermarking and reconstruct the plaintext and ciphertext data's watermark. In addition, the proposed algorithm has high encryption security and strong watermark robustness.

Key words remote sensing image; commutative encryption and watermarking; Paillier encryption; secure transmission; copyright protection

收稿日期：2021-07-19；**修回日期**：2021-07-25；**录用日期**：2021-08-10

基金项目：国家自然科学基金(41761080)、甘肃高等学校产业支撑引导项目(2019C-04)、兰州交通大学优秀平台支持(201806)

通信作者：*zhang_lm@163.com

1 引 言

高分辨率遥感(HRRS)影像作为地球科学研究的基础,是国家基础测绘保障服务的数据源之一[1],广泛应用于地球科学领域[2-3]。然而,网络技术的迅速发展,使得生产成本昂贵且具有高价值的HRRS影像容易被黑客、盗版者及非授权用户窃取或分发,导致数据生产者或版权所有者的合法权益受损,迫切需要有效技术手段进行保护。

密码技术和数字水印技术作为保护遥感影像的两大关键技术[4],能够保护数据使用安全。前者是防止数据被非法截取或篡改的重要方法[5-6],可有效保证HRRS影像在存储和传输过程中数据内容不被泄露[7]。后者作为事后追责的关键技术[8],可用于HRRS影像的版权鉴定和盗版溯源[9-10]。因此,密码技术与数字水印技术相结合的多重保护机制成为保证HRRS影像安全的关键技术[11]。密码技术与数字水印技术的结合主要有两种方法:一是先加密后嵌入水印,二是先嵌入水印后加密[12]。然而,由于加密机制和水印机制会相互影响,直接结合存在操作次序要求高、安全性低、密钥易泄露等方面的不足[13]。

交换密码水印(CEW)作为密码技术与数字水印技术结合的新兴安全技术,可同时实现HRRS影像的安全分发和使用追踪[14]。其原理在于:允许对加密影像嵌入水印,或者是加密已嵌入水印的影像,且水印信息在密文数据和明文数据中均可提取,即加密操作和水印嵌入操作具有交换性,解密操作和水印提取操作亦具有交换性。现有CEW方案主要分为三类[15]。1) 基于不变特征的CEW方案,该方案主要利用置乱加密的原理,运用直方图平移[16]或者像素值修改的方式[17]将水印信息嵌入到不受加密影响的数据中,操作简单,但抗攻击性较差。2) 基于操作域独立的CEW方案,该方案的主要思路是分离加密操作区域和水印嵌入操作区域。其中,Cancellaro等[18]利用树结构Haar变换,对变换后的系数位平面进行操作域划分,在加密高位平面的同时将水印嵌入到低位平面中。Jiang等[19]设计了操作域独立的CEW方案,利用正交变换的特性将数据集划分成两个区域,分别进行加密操作和水印嵌入操作。由于加密和水印操作互不影响,因此该方案具有较好的可交换性、融合性及实用性,但水印操作区域不受加密保护,会降低数据在存储和传输过程中的安全性。3) 基于同态加密的CEW方案,该方案结合同态加密的特性,选择机理互不干扰的密码技术和数字水印技术进行结合,与基于不变特征或操作域独立的CEW方案相比,抗攻击性和安全性更佳。Jiang[20]利用Paillier加密的同态特性,结合Patchwork水印机制设计了基于图像的CEW模型。该方案为实现同一操作域的CEW提供了参考,但其中的水印嵌入操作在图像空间域完成,存在图像精度损失较大、水印鲁棒性差以及水印信息无法重构等不足。尽管HRRS影像与普通栅格图像具有相同的组织结构,但高度敏感和地物信息丰富等特性是HRRS影像区别于普通图像的重要特征,保证经加密和水印操作后HRRS影像的精度是基于HRRS影像的CEW算法的关键。因此,该CEW算法亦不适用于HRRS影像。

为解决以上问题,本文提出了一种适用于HRRS影像的CEW算法,从而为HRRS影像提供安全分发和版权追踪的双重保护能力。该算法有两个关键步骤:利用Paillier加密算法的加法同态性来实现明文数据水印嵌入和提取操作在密文数据上的映射,从而实现加密操作和水印操作在相同操作域中的可交换性,以及水印信息在明文数据和密文数据中的重构;考虑到HRRS影像的特征,所提算法在影像变换域中完成加密和水印操作,以此提高水印算法的鲁棒性和加密算法的安全性。

2 基于IWT的HRRS影像CEW算法

2.1 研究思路

与传统加密相比,同态加密允许不可信第三方在没有私钥的情况下直接对密文进行运算,避免了第三方在运算过程中需要解密密文而造成敏感信息泄漏的问题[21]。Paillier加密算法是一种典型的部分同态加密算法,通过公钥加密机制保证密文的安全性[22]。利用Paillier算法的加法同态特性,可以在数据不解密的情况下将水印信息嵌入密文影像后解密,得到的HRRS影像与直接对该影像嵌入水印的结果相同。因此利用该特性,可以将明文数据的水印嵌入和提取操作转换为对密文影像的操作,从而实现加密操作和水印操作交换。

HRRS影像与普通栅格图像的数据组织形式相同,设计HRRS影像CEW方法时可以借鉴普通图像CEW方法。但需要注意的是,与普通图像相比,HRRS影像具有纹理细节丰富、相邻区域内灰度值相关性更强、信息高度敏感等特点。因此,HRRS影像的加密和水印嵌入需要保证数据的精度不能出现严重损失,即不影响数据的后期使用,这是设计HRRS影像CEW算法的关键。整数小波变换(IWT)以提升小波为基础,不仅能打破HRRS影像的灰度值相关性,而且能够确保载体图像在分解和重建过程中不会出现数据丢失,相比传统的小波变换方法,运算速度更快[23]。因此,在整数小波变换域中进行加密和水印嵌入,不仅能增强加密扩散效果,保证密文安全性和水印不可感知性,而且能够降低加密和水印嵌入对HRRS影像的影响。

基于上述思想,本文基于IWT原理和Paillier算法的加法同态特性设计适用于HRRS影像的CEW算法,算法的流程如图1所示。该算法包括基于IWT的

HRRS影像加密算法和基于IWT和Paillier加法同态特性的水印算法两部分。首先对原始HRRS影像进行分块处理，以降低相邻像素相关性，进而提高加密安全性和水印鲁棒性；其次利用IWT对每个子块进行小波分解，并提取每个子块变换后的低频系数和高频系数；然后利用Paillier算法加密变换后的低频系数和高频系数，同时顾及HRRS影像对数据精度的要求，将水印信息嵌入到低频系数，其中明文HRRS影像的水印嵌入直接使用扩频加性嵌入机制完成，密文HRRS影像的水印嵌入则通过利用Paillier算法的加法同态特性对明文水印操作进行转换来完成；最后对完成加密和水印嵌入操作的子块进行数据合并，并实施逆IWT，得到原始HRRS影像的密文-水印载体影像。值得注意的是，解密和水印提取过程是加密和水印嵌入的逆过程。

2.2 基于IWT的HRRS影像加密算法

HRRS影像经IWT后的低频系数包含影像的轮廓信息，高频系数包含影像的细节和噪声。为保证加密后的HRRS影像具有不可读性，以及解密后的HRRS影像具有可用性，选择IWT后的低频系数和高频系数进行加密，一方面可以提升加密效率，另一方面可以通过逆变换增强加密扩散效果，保证密文安全性。此外，本文的CEW算法是基于同态加密特性实现的，因此加密算法选用比较成熟的Pailler加密算法。算法详细实现过程如下。

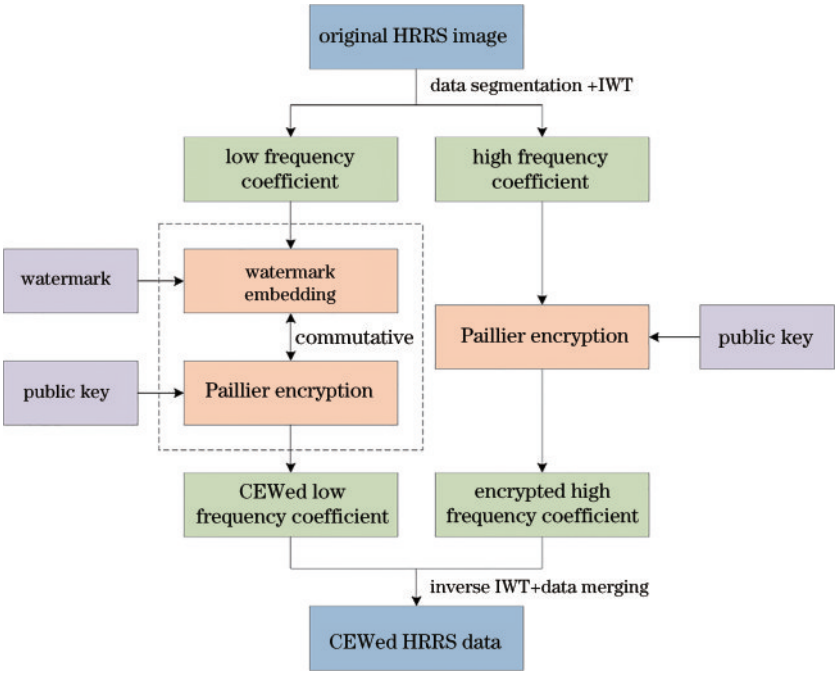

图1 HRRS影像的CEW算法模型

Fig. 1 CEW algorithm model for HRRS image

2.2.1 HRRS影像的加密

基于Paillier算法的HRRS影像加密算法的实现步骤如下。

1）影像预处理。HRRS影像具有较强的相邻像素相关性，为了降低相邻像素间的相关性，按图2所示影像划分方法将原始HRRS影像I划分成4个子块，每个子块的大小为$m \times n$。

2）整数小波分解。利用IWT对每个子块进行小波分解，并提取每个子块经过变换后的低频系数$D=\{d_{i,j}|0 \leqslant i<m, 0 \leqslant j<n\}$和高频系数$A=\{a_{i,j}|0 \leqslant i<m, 0 \leqslant j<n\}$。

3）密钥生成。基于Paillier算法原理，首先随机选择两个大质数p和q，再分别计算两个质数的乘积N和最小公倍数λ，表达式分别为

$$N=p \cdot q, \tag{1}$$

$$\lambda=\mathrm{lcm}(p-1, q-1)。 \tag{2}$$

然后选择随机整数g，$g \in Z_{N^2}^{*}=\{x|0<x<N^2, \gcd(x, N)=1\}$，并且$\mu=\left[L\left(g^{\lambda} \bmod N^2\right)\right]^{-1} \bmod N$在$Z_{N^2}^{*}$中存在，其中$L(x)=\dfrac{x-1}{N}$，则Paillier公钥$p_k$为$(N, g)$，私钥$s_k$为$(\lambda, \mu)$。

4）数据加密。根据Paillier算法原理，使用公钥p_k和随机数$r(r \in Z_{N^2}^{*})$，加密每个子块的低频系数和高频系数，得到加密后的低频系数$d_{i,j}^{E}$和高频系数$a_{i,j}^{E}$：

$$\begin{cases} d_{i,j}^{E}=E\left[d_{i,j}, N, g\right]=g^{d_{i,j}} \cdot r^{N} \bmod N^2 \\ a_{i,j}^{E}=E\left[a_{i,j}, N, g\right]=g^{a_{i,j}} \cdot r^{N} \bmod N^2 \end{cases}。 \tag{3}$$

5）密文影像数据的生成。将每个子块经小波分解得到的原始低频系数$d_{i,j}$和高频系数$a_{i,j}$替换为加密后的低频系数$d_{i,j}^{E}$和高频系数$a_{i,j}^{E}$，并进行逆IWT，得到加密后的子块数据；对所有子块均完成加密操作后，通过子块合并，得到加密后的影像数据（E-ed）。

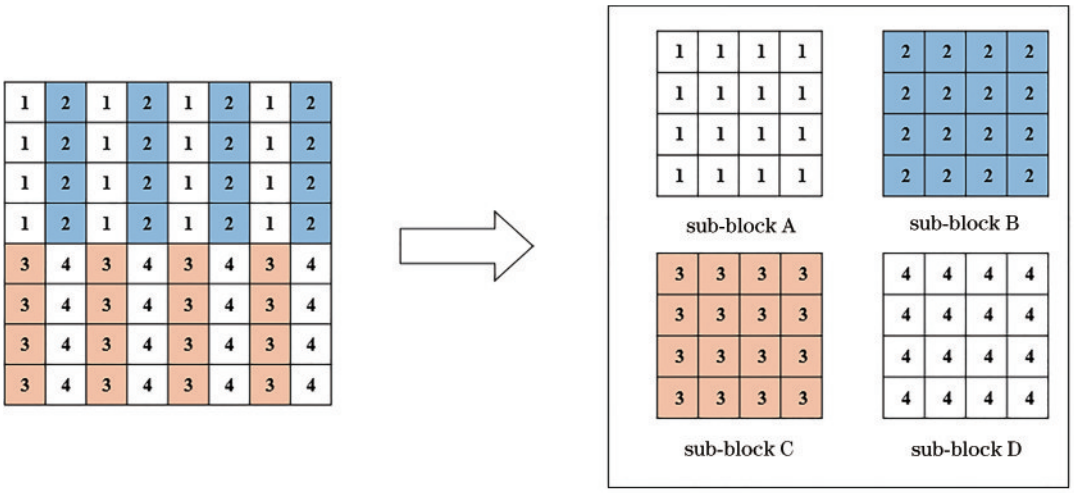

图 2　HRRS影像划分

Fig. 2　Division of HRRS image

6) 密钥管理者通过某种特定的安全方式将解密密钥s_k发送至合法用户。

2.2.2　HRRS影像的解密

解密过程是加密的逆过程。首先,对加密后的影像数据(E-ed)进行子块划分得到加密子块,然后对加密子块进行整数小波分解,提取密文低频系数$d_{i,j}^{E}$和密文高频系数$a_{i,j}^{E}$。然后利用从密钥管理者处获取的解密密钥s_k,分别对每个子块的密文低频系数$d_{i,j}^{E}$和密文高频系数$a_{i,j}^{E}$进行解密,得到解密后的低频系数$d'_{i,j}$和高频系数$a'_{i,j}$:

$$\begin{cases} d'_{i,j}=L\left[\left(d_{i,j}^{E}\right)^{\lambda} \bmod N^2\right]\cdot\mu \bmod N \\ a'_{i,j}=L\left[\left(a_{i,j}^{E}\right)^{\lambda} \bmod N^2\right]\cdot\mu \bmod N \end{cases}。\tag{4}$$

最后,将每个子块经过IWT得到的密文低频系数$d_{i,j}^{E}$和密文高频系数$a_{i,j}^{E}$替换为解密后的低频系数$d'_{i,j}$和高频系数$a'_{i,j}$,并进行逆IWT和数据合并,得到解密后的影像数据(D-ed)。

2.3　利用Paillier加法同态特性的HRRS影像水印算法

HRRS影像经IWT后的低频系数包含影像的轮廓信息,不涉及HRRS影像的细节特征,具有稳定性。因此,选择低频系数嵌入水印信息,一方面能很好地保证水印信息的不可感知性和水印算法的鲁棒性[24],另一方面可以降低水印嵌入对HRRS影像精度的影响。此外,利用Paillier算法的加法同态特性,可以将明文数据的水印操作映射到密文数据上,从而通过明文域水印算法和密文域水印算法共同实现水印操作和加密操作之间的交换。需要指出的是,对于明文数据形式的HRRS影像,水印嵌入和提取操作可根据正常的运算规则来设计,不需要利用同态特性;而对于密文数据形式的HRRS影像,水印嵌入和提取操作是基于同态特性将明文数据的水印嵌入和提取操作转换为对密文影像的操作。

2.3.1　水印嵌入

HRRS影像的水印嵌入过程包含5个步骤。

1) 数据预处理。为了保证水印算法的鲁棒性,按图2所示影像划分方法将原始HRRS影像I划分成4个子块,每个子块的大小为$m\times n$。

2) 整数小波分解。利用IWT对每个子块进行小波分解,并提取每个子块经过变换后的低频系数$D=\left\{d_{i,j}\middle|0\leqslant i<m,0\leqslant j<n\right\}$。

3) 水印信息生成。为降低原始水印图像的相邻像素相关性和增加水印安全性,首先应用Arnold变换对大小为$h\times w$的原始二值水印图像进行置乱;然后,按照每个子块经过IWT后的低频子带D的大小对置乱后的水印图像进行扩展,得到扩频后的水印信息$w_{i,j}=\{0,1\}\left(i=1,2,\cdots,\lfloor m/h\rfloor;j=1,2,\cdots,\lfloor n/w\rfloor\right)$,其中$\lfloor\cdot\rfloor$表示向下取整函数;最后,对扩频水印信息$w_{i,j}$进行映射处理,得到新的水印信息$w'_{i,j}$,

$$w'_{i,j}=\begin{cases}1, & w_{i,j}=1\\ -1, & w_{i,j}=0\end{cases}。\tag{5}$$

4) 水印信息嵌入。运用扩频加性嵌入的方式将水印信息嵌入到HRRS影像每个子块的低频系数$d_{i,j}$。嵌入水印后的低频系数可以表示为

$$d_{i,j}^{W}=d_{i,j}+\theta\cdot w'_{i,j},\tag{6}$$

式中:θ表示嵌入强度。根据Paillier算法的加法同态特性,

$$E\left[m_1\right]\cdot E\left[m_2\right]=g^{m_1}r_1^{N}\cdot g^{m_2}r_2^{N} \bmod N^2=$$
$$g^{m_1+m_2}\left(r_1\cdot r_2\right)^{N} \bmod N^2=E\left[m_1+m_2\right],\tag{7}$$

将式(6)明文数据的水印嵌入操作映射至密文数据,因此HRRS影像密文数据的水印嵌入方法为

$$d_{i,j}^{EW}=\begin{cases}d_{i,j}^{E}\cdot E\left[\theta\right] \bmod N^2, & w'_{i,j}=1\\ d_{i,j}^{E}\cdot E\left[-\theta+N\right] \bmod N^2, & w'_{i,j}=-1\end{cases},\tag{8}$$

式中：m_1和m_2分别表示两个明文数据；r_1和r_2分别是加密m_1和m_2时选择的随机数；$E[\cdot]$表示Paillier加密函数，值得注意的是，在Paillier加密系统中，负整数$E[-m_1]$可以用$E[-m_1+N]$；$d_{i,j}^{\mathrm{E}}$表示每个子块的低频系数$d_{i,j}$的密文数据；$d_{i,j}^{\mathrm{EW}}$表示加密后嵌入水印的密文-水印数据。

5）含水印影像数据的生成。将每个子块经过小波分解得到的原始低频系数$d_{i,j}$替换为嵌入水印后的低频系数$d_{i,j}^{\mathrm{W}}$或$d_{i,j}^{\mathrm{EW}}$，并进行逆IWT，得到含水印的子块数据；对所有子块均完成水印嵌入操作后，通过子块数据合并，得到含水印的影像数据（W-ed）或密文-水印影像数据（CEWed）。

值得注意的是，假设明文数据为m_1，水印信息为1，根据式（7），$E[m_1]\cdot E[1]=E[m_1+1]$，由此可知，加密和水印嵌入操作的先后顺序不影响最终的CEW结果。因此，加密操作和水印嵌入操作具有可交换性。

2.3.2　水印提取

水印提取过程是水印嵌入的逆过程，水印提取的详细步骤如下。

1）对含水印的影像数据（W-ed）或密文-水印影像数据（CEWed）进行子块划分，然后按块进行整数小波分解，并提取低频系数$d_{i,j}^{\mathrm{W}}$或$d_{i,j}^{\mathrm{EW}}$。

2）从每个子块的低频系数中提取水印，对于明文数据形式的低频系数$d_{i,j}^{\mathrm{W}}$，水印提取方法为

$$w'_{i,j}=\begin{cases}1, & d_{i,j}^{\mathrm{W}}-d_{i,j}\geqslant 0\\ 0, & d_{i,j}^{\mathrm{W}}-d_{i,j}<0\end{cases},\tag{9}$$

式中：$d_{i,j}$表示原始HRRS影像的低频数据；$w'_{i,j}$表示提取的水印信息。对于密文数据形式的低频系数$d_{i,j}^{\mathrm{EW}}$，需根据Paillier算法的加法同态特性，

$$D\left[E[m_1]\cdot E[m_2]\right]=(m_1+m_2)\bmod N,\tag{10}$$

将式（9）明文数据的水印提取操作映射至密文数据，以此实现密文域水印信息的提取。密文数据中水印提取方法为

$$w'_{i,j}=\begin{cases}1, & D\left[d_{i,j}^{\mathrm{EW}}\cdot E[-d_{i,j}+N]\times\%\times N^2\right]\geqslant N/2\\ 0, & D\left[d_{i,j}^{\mathrm{EW}}\cdot E[-d_{i,j}+N]\times\%\times N^2\right]<N/2\end{cases},\tag{11}$$

式中：$D[\cdot]$表示Paillier解密函数。

3）对提取的水印信息$w'_{i,j}$按照原始二值水印大小进行解扩处理，并进行逆Arnold变换，以此重构原始水印信息。

同样地，假设明文数据为m_1，水印信息为1，根据式（10），$D\left[E[m_1]\cdot E[1]\right]=(m_1+1)\bmod N$，由于$N$表示能加密的明文的最大值，因此$D\left[E[m_1]\cdot E[1]\right]=(m_1+1)\bmod N=m_1+1$，即可提取出所嵌入的水印信息为1。因此，解密操作与水印提取操作亦具有交换性。

3　实验分析

为验证所提算法的有效性和通用性，实验使用Python 3.7编码实现。实验环境是：处理器为Intel（R）Core（TM）i5-10500，CPU为3.10 GHz，运行内存RAM为8GB，操作系统为64位的Windows系统。从DOTA[25] HRRS数据集中选择3幅影像作为实验数据，如图3所示，影像大小分别为512×512、1024×1024和2048×2048。DOTA数据集由三个数据源组成：Google Earth、GF-2、JL-1。Google Earth影像的分辨率为0.5 m，GF-2影像的分辨率为0.8 m，JL-1影像的分辨率为0.72 m。本实验以HRRS影像的单波段数据为例，进行CEW算法测试。考虑到选用的HRRS影像的像素位深度为8位，实验中Paillier加密过程中选用素数$p=89$，$q=97$，其能加密的明文的上限值$N=p\times q=8633$；水印嵌入过程中，水印嵌入强度$\theta=1$，所用的二值水印图像的大小为64×64。图4（a）、（b）分别为原始水印信息、Arnold置乱后的水印。

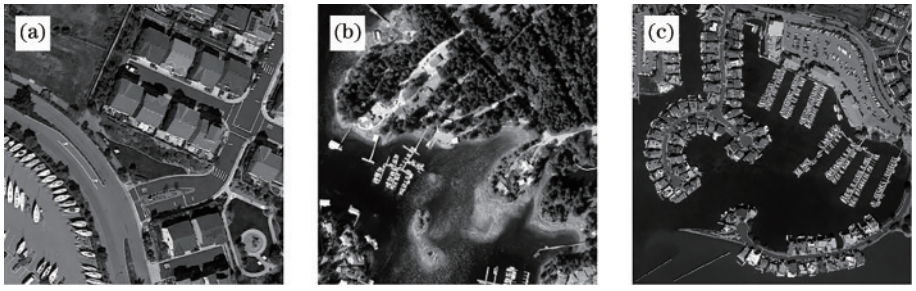

图3　原始影像。（a）影像A；（b）影像B；（c）影像C

Fig. 3　Original images. (a) Image A; (b) image B; (c) image C

3.1　实验结果可视化

对3幅原始HRRS影像（A、B、C）进行CEW测试，实验结果如图5所示。图5（a）～（c）分别是使用加密密钥$p_{\mathrm{k1}}=(8633, 8634)$经CEW操作后得到的CEWed影像（A1、B1、C1），图5（d）～（f）分别是使用正确解密密钥$s_{\mathrm{k1}}=(8448, 8493)$解密CEWed影像得到的解密-水印载体（D-Wed）影像（A2、B2、C2）。从图5可以看出，原始HRRS影像在经过CEW操作后，影像的内容完全发生

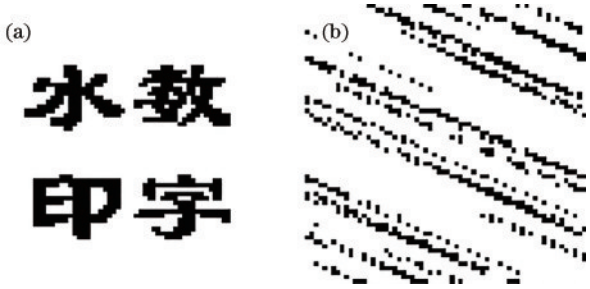

图 4　水印图像。(a)原始水印;(b)置乱水印

Fig. 4　Watermark images. (a) Original watermark; (b) shuffled watermark

改变,解密后的影像与原始影像在视觉上并无差别。

3.2　加密安全性分析

3.2.1　密钥长度分析

密钥长度是密钥安全性的重要评价指标。为了算法能具有较强的抗穷举攻击能力,密钥空间应该足够大,且密钥长度应大于标准要求,即密钥空间不小于2^{100}。所提算法是基于Paillier算法进行设计的,密钥空间大小取决于Paillier算法本身。传统的AES加密算法的密钥长度最高可达256 bit,Paillier算法的密钥长度达2048 bit。因此所提算法的密钥空间大小为2^{2048},充分表明所提算法具有较强的抗穷举攻击能力。

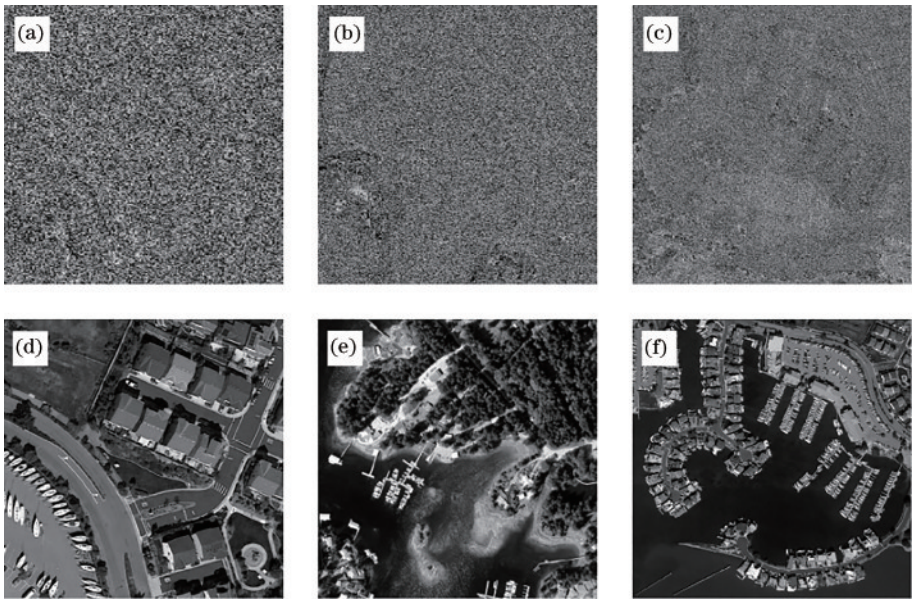

图 5　CEW 实验结果。(a)~(c) CEWed 影像(A1、B1、C1);(d)~(f) D-Wed 影像(A2、B2、C2)

Fig. 5　CEW experiment results. (a)-(c) CEWed image (A1, B1, C1); (d)-(f) D-Wed image (A2, B2, C2)

3.2.2　密钥敏感度分析

密钥的敏感度指当密钥发生轻微变化,加密数据或解密数据将与用初始密钥得到的数据之间有极大差异。密钥越敏感,密文就更加不易被理解,安全性更高。为了分析不同密钥对加密结果的影响,使用修改后的公钥p_{k2}=(8631, 8632)对原始影像(A、B、C)进行加密,得到CEWed影像(A3、B3、C3),如图6(a)~(c)所示。同时,为了分析不同密钥对解密结果的影响,使用修改后的私钥s_{k2}=(8447, 1346)对使用公钥p_{k1}加密得到的CEWed影像(A1、B1、C1)进行解密,得到D-Wed影像(A4、B4、C4),如图6(d)~(f)所示。

为了进一步评估密钥的敏感性,引入平均绝对误差(MAE)来衡量两幅影像之间的差异。一般来说,MAE的值为0时,表明两幅影像之间没有差异;MAE越大,意味着两幅影像之间的差异越大。MAE定义为

$$M_{\mathrm{AE}}=\frac{1}{M\times N}\sum_{i=1}^{M}\sum_{j=1}^{N}\left[Q(i,j)-Q'(i,j)\right]^2,\quad(12)$$

式中:$Q(i,j)$与$Q'(i,j)$为原始影像与加密影像在位置(i,j)处的像素值;$M\times N$为影像尺寸。根据式(12),分别计算了使用公钥p_{k1}得到的CEWed影像(A1、B1、C1)与使用公钥p_{k2}得到的CEWed影像(A3、B3、C3)之间的MAE、使用私钥s_{k1}得到的D-Wed影像(A2、B2、C2)与使用私钥s_{k2}得到的D-Wed影像(A4、B4、C4)之间的MAE,计算结果如表1所示。由图6和表1可以发现,使用不同密钥得到的加密影像之间存在极大差异。同时,当解密密钥发生变化,即使是轻微改变,也无法对密文数据进行解密,这表明所提算法具有较强的密钥敏感性,只有使用正确密钥才能对加密影像正确解密,解密密钥一旦发生修改,密文数据则无法正确解密。

3.2.3　抗统计攻击分析

相邻像素具有很强的相关性是HRRS影像的重要数据特征之一。为了避免攻击者利用该特性推理周围像素的灰度值,从而实现对整个明文数据的恢复,需打破加密影像相邻像素间的相关性来确保密文的安全性。为了更好分析原始影像和加密影像相邻像素间的相关性,引入二维相关系数来分析像素的相关性。二维相关系数的定义为

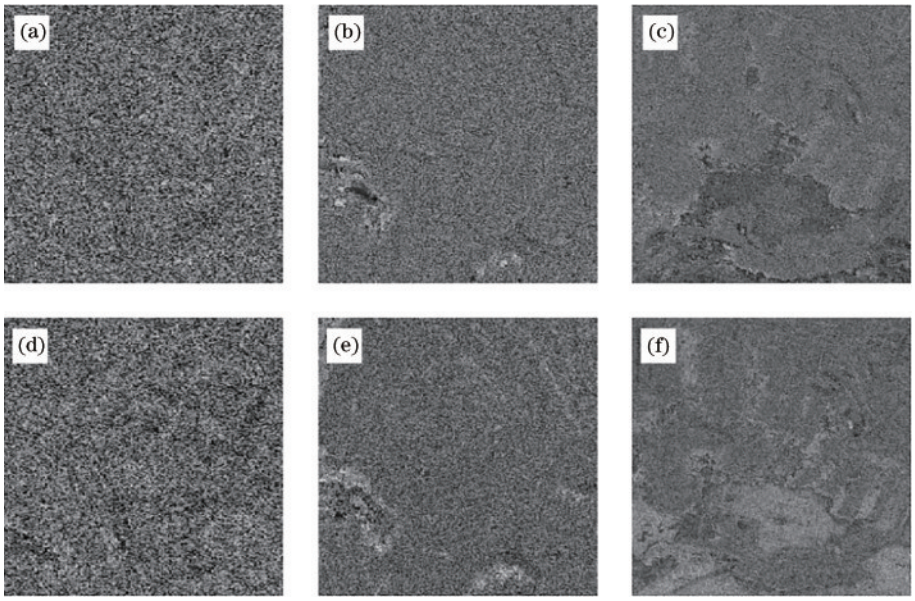

图 6　密钥敏感度分析结果。(a)~(c)公钥 p_{k2} 加密影像(A3、B3、C3);(d)~(f)密钥 s_{k2} 解密影像(A4、B4、C4)

Fig. 6　Analysis result of key sensitivity. (a)-(c) CEWed image (A3, B3, C3) with the key p_{k2}; (d)-(f) D-Wed image (A4, B4, C4) with s_{k2}

表 1　使用不同密钥得到的 CEWed/D-Wed 影像之间的 MAE

Table 1　MAE of CEWed/D-Wed images using different secret keys

HRRS image	MAE between CEWed images	MAE between D-Wed images
A	9.58×10^{14}	2.55×10^{7}
B	9.39×10^{14}	2.39×10^{7}
C	9.06×10^{14}	2.01×10^{7}

$$r=\frac{\sum_{i=1}^{M}\sum_{j=1}^{N}\left[Q(i,j)-\bar{Q}\right]\left[Q'(i,j)-\overline{Q'}\right]}{\sqrt{\sum_{i=1}^{M}\sum_{j=1}^{N}\left[Q(i,j)-\bar{Q}\right]^{2}\times\sum_{i=1}^{M}\sum_{j=1}^{N}\left[Q'(i,j)-\overline{Q'}\right]^{2}}},\tag{13}$$

式中:$\bar{Q}$ 和 $\overline{Q'}$ 分别为原始影像和加密影像的像素平均值。

根据式(13),随机选择 10000 对像素值,分别从水平、垂直和对角线 3 个方向计算原始影像(A、B、C)和 CEWed 影像(A1、B1、C1)的像素相关性,结果如表 2 所示。

由表 2 可知,3 幅加密影像在水平、垂直和对角方向上的相关性均趋向 0,与原始影像相比,相邻像素相关性极小,表明所提算法具有良好的抗统计分析能力。

表 2　原始影像和加密影像相邻像素间的相关性

Table 2　Adjacent pixel correlation between original images and encrypted images

Direction	Original image			CEWed image		
	A	B	C	A1	B1	C1
Horizontal	0.9685	0.9657	0.9479	0.0065	0.0118	0.0521
Vertical	0.9755	0.9723	0.9274	0.0809	0.0991	0.0855
Diagonal	0.9506	0.9462	0.8936	−0.0038	0.0072	0.0311

3.3　水印安全性分析

1) 不可感知性

不可感知性是指原始影像与 D-Wed 影像之间的差异。对于 HRRS 影像而言,水印信息嵌入到原始影像中应不影响数据的使用。本研究通过峰值信噪比(PSNR)衡量水印的不可感知性,定义如下:

$$R_{\mathrm{PSN}}=10\times\lg\frac{(M\times N)\times\left[\max\left(Q'\right)-\min\left(Q'\right)\right]}{\sum_{i=1}^{M}\sum_{i=1}^{N}\left[Q(i,j)-Q'(i,j)\right]^{2}},\tag{14}$$

式中:Q 和 Q' 分别为原始影像和 D-Wed 影像;$Q(i,j)$ 与 $Q'(i,j)$ 为原始影像与 D-Wed 影像在位置 (i,j) 处的像素值;max(•)和 min(•)分别表示影像的最大像素值和最小像素值。

理想情况下,当两幅图像之间的 PSNR 大于 30 dB,人眼很难分辨出它们之间的差异,表明图像质量较好。同时,PSNR 值越高,水印的不可感知性越好。根据式(14),计算不同嵌入强度下 D-Wed 影像(A2、B2、C2)的 PSNR,计算结果如表 3 所示。由表 3 可知,所提算法得到的 D-Wed 影像的 PSNR 远大于

表 3　不同嵌入强度下 D-Wed 影像的 PSNR

Table 3　PSNR of D-Wed images with different embedding intensities

Embedding strength	A2	B2	C2
1	48.0967	47.2722	48.0991
2	42.0769	41.2517	42.0784
3	38.5568	37.7299	38.5599

30 dB，但随着嵌入强度的增大，D-Wed影像的PSNR逐渐减小。显然，当水印嵌入强度为1时，所提算法的水印不可感知性更佳，解密后含水印的HRRS影像的图像质量无明显下降。

2）水印鲁棒性

根据HRRS影像的实际应用，D-Wed影像应能抵抗噪声、平滑、裁剪等常规攻击。引入归一化相关系数（NC）作为水印鲁棒性的评价标准，定义为

$$N_{\mathrm{C}}=\frac{\sum_{i=1}^{M}\sum_{j=1}^{N}Q(i,j)-Q'(i,j)}{\sum_{i=1}^{M}\sum_{j=1}^{N}Q(i,j)^{2}}。\tag{15}$$

原则上提取水印与原始水印越相似，NC值越接近于1。为了检测所提算法的鲁棒性，对D-Wed影像（A2、B2、C2）进行了常规攻击，如加噪、平滑、裁剪等操作。在不同的攻击方式下，水印提取结果如表4所示。

表4　鲁棒性实验结果

Table 4　Experimental results of robustness

Parameter		No attack	Salt-and-pepper noise	Gaussian noise	Median filtering	Upper part cut	Arbitrary cut	Arbitrary cut
			0.01	0.003	3×3	1/2	1/8	1/4
NC	A2	1.0	0.9803	0.9848	0.8793	1.0	1.0	0.9675
	B2	1.0	0.9805	0.9839	0.8971	1.0	1.0	0.9838
	C2	1.0	0. 9805	0.9843	0.9266	1.0	1.0	1.0

由表4可以看出，对D-Wed影像进行一系列常规的图像攻击后，所提算法仍能成功提取水印信息，且提取水印的NC值保持在0.8以上，尤其对裁剪攻击具有较好的抵抗能力。

3.4　算法效率

所提算法利用公钥机制进行设计，不仅需要保证加密算法和水印算法各自的安全性，两者结合的算法效率也是所提算法的重要评价指标。因此，为验证所提CEW算法的时间效率，对实验所用的3幅HRRS影像（A、B、C）经过加密和水印嵌入操作、解密和水印提取操作的时间分别进行计算，并与文献[26]提出的CEW算法进行对比，结果如表5所示。

表5　算法运行时间的比较

Table 5　Comparison of algorithm running time　　unit: s

Procedure	Proposed CEW algorithm			CEW algorithm in Ref. [26]		
	A	B	C	A	B	C
Encryption and watermark embedding	2.2	8.9	35.7	8.7	45.6	98.6
Decryption and watermark extraction	3.2	13.5	55.4	10.5	49.2	105.9

由表5可知，随着影像尺寸的增大，所提算法的效率也会增加。总体而言，所提算法的效率优于文献[26]所提出的CEW算法，能够在满足加密和水印安全性的前提下，保证算法的效率。

3.5　HRRS影像精度分析

相比普通图像，HRRS影像对解密后含水印影像有更高的精度要求。为保证所提算法能够满足HRRS影像的精度要求，利用非监督分类对原始影像（A、B、C）和D-Wed影像（A2、B2、C2）进行精度评价。对于影像分类，采用相同的分类方法和参数，分类方法为K-Means，分类数量为5，最大迭代15次。为进一步验证D-Wed影像的数据精度，利用混淆矩阵对分类结果进行精度评价，评价结果如表6所示。需要指出的是，本研究只是为了验证D-Wed影像的数据精度，因此并没有进行具体的地物分类。

表6　精度评价结果

Table 6　Result of accuracy evaluation

Parameter	D-Wed image A2	D-Wed image B2	D-Wed image C2
OA /%	99.4835	99.1806	99.2253
Kappa coefficient	0.9933	0.9896	0.9898

由表6可知，对原始HRRS影像和解密-水印载体影像进行非监督分类，所提算法的总体精度（OA）均大于90%，且Kappa系数在0.9以上，说明所提算法对原始HRRS影像的影响较小，HRRS影像的数据精度能很好地得到控制，不影响HRRS影像后期的使用。

3.6　与现有算法的对比分析

为了进一步分析所提算法的有效性，从水印不可感知性和水印鲁棒性两方面，对所提算法与文献[2]、[9]、[27]提出的水印算法以及文献[26]提出的CEW算法进行比较，结果如图7和图8所示。

从图7可以看出，随着影像大小的增加，所提算法得到的D-Wed影像的PSNR比文献[26]中的算法低，但与文献[2]、[9]、[27]相比，PSNR总体较高，不可感知性更好。图8为以D-Wed影像B2为例，所提算法与文献[2]、[9]、[27]中的算法在水印鲁棒性方面的对比结果。显然，除中值滤波攻击，所提算法在其他常规攻击和裁剪攻击方面保持着较稳定的

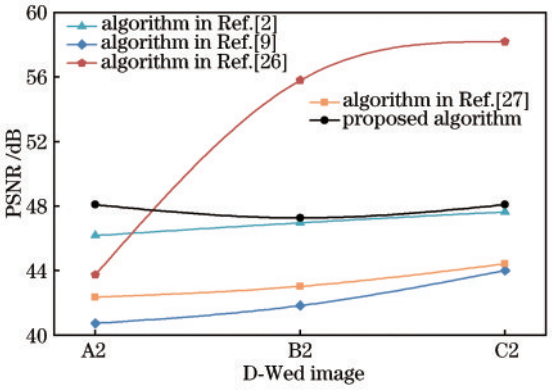

图 7　不可感知性对比结果

Fig. 7　Comparison result of imperceptibility

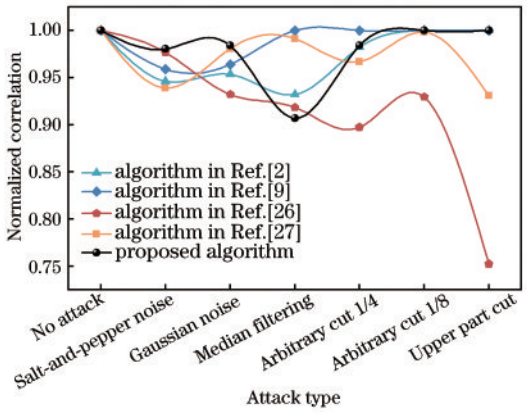

图 8　鲁棒性对比结果

Fig. 8　Comparison result of robustness

鲁棒性，且 NC 值基本上高于对比算法。总体而言，所提算法在水印不可感知性和鲁棒性方面均满足要求，表明所提算法具有良好的水印不可感知性和鲁棒性。

4　结　　论

提出了一种适用于 HRRS 影像的 CEW 算法，旨在使数据生产者或版权所有者实现对 HRRS 影像的安全分发和版权追踪。该算法利用 Paillier 算法的同态性，将明文数据的水印嵌入和提取操作映射至密文数据，从而实现了加密算法和水印算法在相同操作域内的交换，以及水印信息在密文数据和明文数据中的重构。此外，结合 HRRS 影像的数据特征，基于分块和 IWT 原理，在变换域完成 CEW 操作，提高了加密算法的安全性和水印算法的鲁棒性，且算法本身对 HRRS 特征及后期应用影响不大。作为 CEW 在 HRRS 影像上的针对性应用，所提算法的适用性并不局限于 HRRS 影像，对普通光学图像亦具有适用性。然而，尽管所提算法可以很好地抵抗一系列常规攻击及裁剪攻击，但在抵抗旋转、缩放和平移攻击方面鲁棒性较差，还有待改进。

参　考　文　献

[1] Ding K M, Yang Z D, Wang Y Y, et al. An improved perceptual Hash algorithm based on U-net for the authentication of high-resolution remote sensing image[J]. Applied Sciences, 2019, 9(15): 2972.

[2] 侯翔, 闵连权. 基于 SURF 特征区域的鲁棒水印算法[J]. 武汉大学学报·信息科学版, 2017, 42(3): 421-426.
Hou X, Min L Q. A robust watermarking algorithm using SURF feature regions[J]. Geomatics and Information Science of Wuhan University, 2017, 42(3): 421-426.

[3] Zhang X G, Yan H W, Zhang L M, et al. High-resolution remote sensing image integrity authentication method considering both global and local features[J]. ISPRS International Journal of Geo-Information, 2020, 9(4): 254.

[4] 朱长青. 地理数据数字水印和加密控制技术研究进展[J]. 测绘学报, 2017, 46(10): 1609-1619.
Zhu C Q. Research progresses in digital watermarking and encryption control for geographical data[J]. Acta Geodaetica et Cartographica Sinica, 2017, 46(10): 1609-1619.

[5] Kaur M, Kumar V. A comprehensive review on image encryption techniques[J]. Archives of Computational Methods in Engineering, 2020, 27(1): 15-43.

[6] 李云坤, 蒲涛, 郑吉林, 等. 基于并联强度调制的量子噪声随机加密实现方案研究[J]. 中国激光, 2021, 48(17): 1706002.
Li Y K, Pu T, Zheng J L, et al. Realization scheme of quantum noise randomized cypher based on parallel intensity modulation[J]. Chinese Journal of Lasers, 2021, 48(17): 1706002.

[7] Geng W H, Zhang J, Chen L, et al. Hybrid domain encryption method of hyperspectral remote sensing image [M]//Zeng B, Huang Q M, Saddik A E, et al. Advances in multimedia information processing-PCM 2017. Lecture notes in computer science. Cham: Springer, 2018, 10736: 890-899.

[8] 吴德阳, 赵静, 汪国平, 等. 一种基于改进奇异值和子块映射的图像零水印技术[J]. 光学学报, 2020, 40(20): 2010002.
Wu D Y, Zhao J, Wang G P, et al. An image zero watermarking technology based on ameliorated singular value and subblock mapping[J]. Acta Optica Sinica, 2020, 40(20): 2010002.

[9] 王潇, 任娜, 朱长青, 等. 基于 QR 码和量化 DCT 的遥感影像数字水印算法[J]. 地理与地理信息科学, 2017, 33(6): 19-24.
Wang X, Ren N, Zhu C Q, et al. A digital watermarking algorithm based on QR code and quantization DCT for remote sensing image[J]. Geography and Geo-Information Science, 2017, 33(6): 19-24.

[10] 刘颖, 杨星, 朱婷鸽. 基于结构森林边缘和 SIFT 的鲁棒水印算法[J]. 激光与光电子学进展, 2021, 58(6): 0615006.
Liu Y, Yang X, Zhu T G. Robust watermarking algorithm based on structured forests edge and SIFT[J].

Laser & Optoelectronics Progress, 2021, 58(6): 0615006.

[11] Benrhouma O, Mannai O, Hermassi H. Digital images watermarking and partial encryption based on DWT transformation and chaotic maps[C]//2015 IEEE 12th International Multi-Conference on Systems, Signals & Devices, March 16-19, 2015, Mahdia, Tunisia. New York: IEEE Press, 2015: 15651794.

[12] Li M, Xiao D, Zhu Y, et al. Commutative fragile zero-watermarking and encryption for image integrity protection[J]. Multimedia Tools and Applications, 2019, 78(16): 22727-22742.

[13] Ren N, Zhu C Q, Tong D Y, et al. Commutative encryption and watermarking algorithm based on feature invariants for secure vector map[J]. IEEE Access, 2020, 8: 221481-221493.

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

[15] Schmitz R. Use of SHDM in commutative watermarking encryption[J]. EURASIP Journal on Information Security, 2021, 2021: 1-12.

[16] Schmitz R, Li S J, Grecos C, et al. Towards robust invariant commutative watermarking-encryption based on image histograms[J]. International Journal of Multimedia Data Engineering and Management, 2014, 5(4): 36-52.

[17] Schmitz R, Li S J, Grecos C, et al. A new approach to commutative watermarking-encryption[M]//de Decker B, Chadwick D W. Communications and multimedia security. Lecture notes in computer science. Heidelberg: Springer, 2012, 7394: 117-130.

[18] Cancellaro M, Battisti F, Carli M, et al. A commutative digital image watermarking and encryption method in the tree structured Haar transform domain[J]. Signal Processing: Image Communication, 2011, 26(1): 1-12.

[19] Jiang L, Xu Z Q, Xu Y Y. Commutative encryption and watermarking based on orthogonal decomposition[J]. Multimedia Tools and Applications, 2014, 70(3): 1617-1635.

[20] Jiang L. The identical operands commutative encryption and watermarking based on homomorphism[J]. Multimedia Tools and Applications, 2018, 77(23): 30575-30594.

[21] 杨亚涛, 赵阳, 张卷美, 等. 同态密码理论与应用进展[J]. 电子与信息学报, 2021, 43(2): 475-487.
Yang Y T, Zhao Y, Zhang J M, et al. Recent development of theory and application on homomorphic encryption[J]. Journal of Electronics & Information Technology, 2021, 43(2): 475-487.

[22] Alloghani M, Alani M M, Al-Jumeily D, et al. A systematic review on the status and progress of homomorphic encryption technologies[J]. Journal of Information Security and Applications, 2019, 48: 102362.

[23] Meng L Z, Liu L S, Tian G, et al. An adaptive reversible watermarking in IWT domain[J]. Multimedia Tools and Applications, 2021, 80(1): 711-735.

[24] Makbol N M, Khoo B E, Rassem T H, et al. A new reliable optimized image watermarking scheme based on the integer wavelet transform and singular value decomposition for copyright protection[J]. Information Sciences, 2017, 417: 381-400.

[25] Xia G S, Bai X, Ding J, et al. DOTA: a large-scale dataset for object detection in aerial images[C]//2018 IEEE/CVF Conference on Computer Vision and Pattern Recognition, June 18-23, 2018, Salt Lake City, UT, USA. New York: IEEE Press, 2018: 3974-3983.

[26] Zope-Chaudhari S, Venkatachalam P, Buddhiraju K M. Secure dissemination and protection of multispectral images using crypto-watermarking[J]. IEEE Journal of Selected Topics in Applied Earth Observations and Remote Sensing, 2015, 8(11): 5388-5394.

[27] Li Y M, Wei D Y, Zhang L N. Double-encrypted watermarking algorithm based on cosine transform and fractional Fourier transform in invariant wavelet domain [J]. Information Sciences, 2021, 551: 205-227.