第42卷，第9期
2022年9月

光 谱 学 与 光 谱 分 析
Spectroscopy and Spectral Analysis

Vol 42，No. 9，pp2976-2982
September，2022

基于混沌与快速小波变换的多光谱图像压缩加密算法

徐冬冬[1]，于 欣[1*]，杜丽敏[1]，毕国玲[2]

1. 长春大学，吉林 长春 130022
2. 中国科学院长春光学精密机械与物理研究所，吉林 长春 130033

摘 要 针对多光谱图像存储和传输安全性问题，提出一种将混沌思想、小波变换和KL(karhunen-loeve)变换相结合的多光谱图像压缩加密算法。首先，采用K-means聚类方案将多光谱图像聚类为通用像素，通过选择合适的K值使算法的性能最优，同时便于后续处理；然后对通用像素进行二维离散9/7小波变换，对变换后的系数进行Arnold变换以及加密处理，消除多光谱图像大部分空间冗余，减少压缩过程中的块效应；之后对产生的小波系数进行改进的KL变换，消除残余空间冗余和光谱冗余；最后采用差分脉冲滤波器对系数进行编码，并采用Tent映射对码流进行混淆扩散加密。通过实验可知，本算法的信息熵达到11.794 3(选取12位多光谱图像)，信息熵更接近最大值12，优于现有算法，可以更好的隐藏原图特征；该算法的像素变化率(NPCR)和归一化平均变化强度(UACI)分别为99.81%和34.19，优于现有的其他算法，本算法可以更好的抵御差分攻击；输出比特流变化率保持在47.62%～47.71%之间，密文比特流变化率保持在47.45%～47.52%，本算法具有较好的密钥敏感性；在压缩比为4∶1～32∶1范围内，系统PSNR在42 dB以上，具有很高的压缩性能。在4∶1～32∶1范围内，本压缩算法达到很高的峰值信噪比，优于现有的压缩算法，在正常工作压缩比为16∶1时，比现有压缩算法的信噪比提高了0.64 dB以上。为进一步验证算法在高压缩比情况下的压缩性能，该研究测试了压缩比为128∶1时系统的信噪比为31.28，此时，重建后的图像较为清晰，优于现有算法1 dB以上。可见，该算法可行，且特别适合对压缩比要求较高的场合，并在频谱保真方面具有较好的效果。

关键词 KL变换；Arnold变换；NPCR；UACI；差分脉冲滤波器

中图分类号：TP309.7 **文献标识码**：A **DOI**：10.3964/j.issn.1000-0593(2022)09-2976-07

引 言

多光谱成像系统作为卫星的重要组成部分正朝着高分辨率、大视场角的方向发展。高分辨率可以得到更加详细和准确的信息，提高对地面和海洋目标的识别能力；大视场角可以使空间相机的覆盖范围更大，有效提高工作效率。而随着分辨率和视场角的提高，导致空间相机输出的数据量越来越大，这就对相关图像的压缩及解压算法提出了更高的要求。

此外，由于某些侦察监视工作不希望被其他国家或者组织破解，因此除了通信链路加密之外，非常有必要对多光谱图像进行加密，以确保数据的安全性。与此同时，地面对空间传回的数据量、数据质量以及安全性的需求越来越高，对算法的压缩效率、计算复杂度、稳定性、密钥空间以及敏感性提出了更高的要求，因此研制出压缩效率高、计算复杂度低、稳定性强、密钥空间大、对密钥和明文敏感高的加密算法是目前迫切需要解决的问题。

针对二维图像和多光谱图像，提出了很多压缩加密算法。郭家伟等提出了与联合图像专家组(joint photographic experts group，JPEG)压缩相结合的图像加密算法[1]，首先将像素点的RGB分量以8×8的子块为单位在行列方向上进行位置置乱，实现颜色分量重组，再进行JPEG压缩；完成离散余弦变换(discrete cosine transform，DCT)系数量化后，分别对DC系数和AC系数进行位置置乱，再对DCT系数的符号位进行随机修改。该算法加密效果好，密钥空间大，敏感性强，但压缩效率不足。Song等提出了基于熵编码和压缩感知的图像压缩加密方案，具有较好的压缩加密性能[2]，但在去冗余方面仍存在一定的不足。

收稿日期：2021-07-22，修订日期：2021-10-17

基金项目：国家自然科学基金项目(61801455)资助

作者简介：徐冬冬，1987年生，长春大学电子信息工程学院教师 e-mail：xudongdong611@aliyun.com

*通讯作者 e-mail：543204976@qq.com

(C)1994-2023 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

由于传统的多光谱数据传输和存储只是压缩，而没有考虑到“压缩—解压缩”过程引起的图像安全性问题。对于压缩域的多光谱遥感图像数据而言，其主要应用目的是对地物分类和目标识别，因此保留多光谱图像数据中的纹理信息是非常重要的。如何在保留用于分析的重要信息的前提下进行压缩域的多光谱图像数据加密是具有挑战性的工作，研究面向应用的压缩域多光谱遥感图像方法和技术，不仅能够对海量的多光谱数据进行有效的压缩，而且有利于保证多光谱图像链路传输时的安全。

上述压缩加密算法对二维图像的压缩加密效果较好，对于多光谱图像的压缩加密效果欠佳；同时，针对多光谱图像的压缩加密算法，在压缩效率或加密效果方面存在不足。与普通图像相比，多光谱图像有两种冗余，即空间冗余和光谱冗余，因此压缩时只有兼顾这两部分冗余，才能使压缩性能最佳。有些算法，如 PCA 或独立成分分析，只通过降维实现压缩，忽略了空间相关性，因此，压缩效果一般。随后，兼顾空间相关性与光谱相关性的压缩算法应运而生，如 3D 多级树集合分裂（3D set partitioning in hierarchical trees，3D-SPIHT）以及 3D 小波嵌入零块编码算法（3D set partitioned embedded bloCK，3D-SPECK）。但这些算法都无法解决因数据量急剧增加所带来的存储和传输压力。现有的压缩加密算法，没有根据多光谱图像的特点选择相对应的算法，同时没有将压缩部分和加密部分紧密的结合在一起，因此压缩加密效果欠佳。针对多光谱图像的特点，在参考 KL 变换最新技术以及最新压缩、加密等算法[3-5]的基础上，本文提出一种基于混沌与快速小波变换的多光谱图像压缩加密算法，将压缩过程与加密过程紧密结合，在提高图像存储、传输效率的同时，保证图像的安全性，并实现了较高的压缩效率和较好的加密效果。

1　实验部分

1.1　多光谱图像压缩加密算法的设计

多光谱图像一般只有几个谱段，是由二维的空间几何信息和一维的光谱信息组成的三维立体图像。这种图像不仅存在空间相关性，而且还有谱间相关性。为了有效地去除空间相关性以及谱间相关性，同时保证多光谱信息的安全性，结合多光谱图像的光谱特性，本文提出了如图 1 所示的结构：

首先将多光谱图像聚类为通用像素；对通用像素进行二维离散 9/7 小波变换，在空间方向上将能量变换成一系列系数，消除多光谱图像大部分空间冗余，减少压缩过程中的块效应；然后对变换后的系数进行 Arnold 变换以及加密处理；之后对产生的小波系数进行基于不同基的 KL 变换，克服了单一 KL 变换基压缩性能有限的通病，有效地保护了多光谱信息，并实现了较高的压缩性能和压缩效率，消除残余空间冗余和光谱冗余；最后采用差分脉冲滤波器对系数进行编码，并采用 Tent 映射对码流进行混淆扩散加密，最后，通过解压解密算法重建多光谱图像。

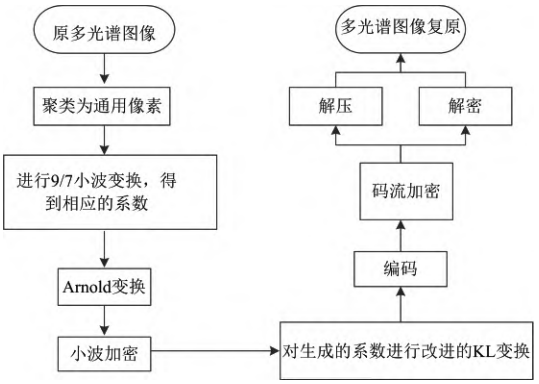

图 1　多光谱图像压缩加密算法流程图

Fig. 1　Flow chart of multispectral image compression and encryption algorithm

1.2　构造通用像素

超像素由一系列位置相邻且颜色、亮度、纹理等特征相似的像素点组成的小区域。这些小区域大多保留了进一步进行图像分割的有效信息，且一般不会破坏图像中物体的边界信息。通用像素由具有全局视图的高维图像空间中最相似的像素组成，跟超像素具有很多相似的属性，是超像素的扩展。不同之处在于，超像素位于相连的邻域中，通用像素不位于较小的局部区域。通用像素可以表示为

$$\forall\, i,\ j,\ a,\ b \begin{cases} I_{i,a} - I_{i,b} \leqslant D_a \\ I_{i,a} - I_{j,b} > D_a \\ I_i \cap I_j = \phi \\ I_i \cup I_j = I \end{cases} \tag{1}$$

式(1)中，I 是多光谱图像的像素集，$I_k = \{I_{k,1},\ I_{k,2},\ I_{k,3},\ \cdots,\ I_{k,n_k} (k = 1,\ 2,\ \cdots,\ K)\}$ 表示具有 n_k 个像素的第 k 个通用像素，K 是通用像素的数量，D_a 是通用像素中相似像素的阈值。通用像素中的像素数直接影响算法的性能，因此，选择合适的 K 值非常重要。

本文采用 K-means 聚类方案来构建通用像素。K-means 算法按照样本之间距离大小，将样本分为 K 个簇，使簇间的距离尽量大，簇内的点的距离尽量小。多光谱图像像素之间的距离公式为

$$\mathrm{Dis}(I_b,\ I_a) = \left\| \frac{I_b}{\| I_b \|_2} - \frac{I_a}{\| I_a \|_2} \right\|_2 + \alpha \times (\| I_b \|_2 - \| I_a \|_2) \tag{2}$$

式(2)中，I_b，I_a 是多光谱图像中任意两个像素，$\| \cdot \|_2$ 表示向量的 2 范数，$\mathrm{Dis}(I_a,\ I_b)$ 表示两个像素之间的距离。α 是修正范数差异的平衡参数。通过迭代的方法，使目标的平方误差最小，即

$$E = \sum_{i=1}^{k} \sum_{x \in C_i} \| x - \mu_i \|_2^2 \tag{3}$$

式(3)中，μ_i 是簇 C_i 的均值向量。

1.3　小波加密算法

本加密算法由生成子密钥、小波系数置乱和数据流加密 3 部分构成。

(C)1994-2023 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net

1.3.1 生成子密钥

本文采用的混沌系统为改进的 Logistic 映射和 Tent 映射，改进后的映射方程为

$$x_{n+1}=[\mu_0+(4-\mu_0)\times\cos((10^{-6}+x_n)\times\pi/2)]\times x_n\times(1-x_n/n) \tag{4}$$

$$x_{n+1}=\begin{cases}\dfrac{x_n}{p} & 0<x_n<p\\ \dfrac{1-x_n}{1-p} & \text{其他}\end{cases} \tag{5}$$

其中，$p\in(0,1)$，$x_n\in[0,1]$，μ_0 为3.569 945 673，放大因子 $1/n\in(0,1)$。当 $\mu\in(3.569\ 945\ 673,4]$时，Logistic 映射生成的序列处于混沌状态，且当其取值为 4 时，系统处于最佳混沌状态，但此时的加密效果较差。因此本文采用一个无限接近 4 的表达式代替 4，以达到预期的混沌特性以及安全性。

我们把通过 Logistic 映射构造散列函数生成的散列值分为 5 组，记 f_1，f_2，f_3，f_4 和 f_5。由式(6)生成子密钥，作为 Logistic 映射的初始值。

$$x_0^m=\mathrm{mod}\Big(\sum_{i=1}^{5}f_i/2^{32},1\Big) \tag{6}$$

式(6)中，mod 表示模运算。给定初始密钥 x_0，x_1 和 x_2，由式(7)扰动初始密钥生成子密钥，并分别作为 Tent 映射的初始值、控制参数和初始密文块。

$$\begin{cases}x'_0=\mathrm{mod}(x_0+(f_1\oplus f_2)/2^{32},1)\\ x'_1=\mathrm{mod}(x_1+(f_3\oplus f_4)/2^{32},1)\\ x'_2=x_2\oplus f_5\end{cases} \tag{7}$$

1.3.2 小波系数置乱

构造完通用像素后，为了减少压缩过程中的块效应，保护图像的真实信息，需对像素进行小波变换。小波变换是在傅里叶变换的基础上提出的一种新的变换方法，在延续了短时傅里叶变换局部化优点的同时，克服了傅里叶变换的一系列缺点。下面将给出小波变换的基本概念。

如果函数满足容许性条件

$$C_\Psi=\int_{-\infty}^{+\infty}|\hat{\Psi}(\omega)|^2|\omega|^{-1}\mathrm{d}\omega<+\infty \tag{8}$$

式(8)中，$\int_{-\infty}^{+\infty}|\Psi(t)|^2\mathrm{d}t<+\infty$，$\hat{\Psi}(\omega)$ 是 $\Psi(\omega)$ 的傅里叶变换，则称 $\Psi(t)$ 为母小波或基小波。

二维小波函数可由一维小波的张量积构造，二维连续小波变换为

$$W_\Psi f(a,b,c)=\iint f(x,y)\Psi_{a,b,c}(x,y)\mathrm{d}x\mathrm{d}y \tag{9}$$

式(9)中，$a\in R^+$，b，$c\in R$，$\Psi(x,y)$ 为二维小波函数。$\Psi_{a,b,c}(x,y)=|a|^{-1}\Psi\Big(\dfrac{x-b}{a},\dfrac{y-c}{a}\Big)$。

二维离散小波变换是在二维连续小波的基础上进行参数量化，即：$a=2^{-j}$，$b=i_1 2^{-j}$，$c=i_2 2^{-j}$，j，i_1，$i_2\in Z$，$\Psi_{j,i_1,i_2}(m,n)=2^j\Psi(2^j m-i_1,2^j n-i_2)$，可得信号的二维离散小波变换为

$$f(m,n)=\langle f(m,n),\widetilde{\Psi}_{j,i_1,i_2}(m,n)\rangle\Psi_{j,i_1,i_2}(m,n) \tag{10}$$

对图像进行一次小波变换，将产生四个子带，分别为低频子带(LL)，水平方向高频子带(LH)，垂直方向高频子带(HL)，对角线方向高频子带(HH)。二次变换是在低频子带(LL)的基础上重复类似的划分。针对不同的子带系数进行不同的处理，以达到更好的研究效果。

本文采用 Arnold 变换对小波变换后的系数进行置乱。根据 Arnold 变换周期表，选择合适的次数对目标像素进行变换置乱，得到变换置乱图。

1.3.3 KL 变换

KLT 可用于主成分分析(principal component analysis，PCA)，是一种具有去相关性能的线性可逆变换。原算法计算过程如下：

首先，将含有 N 谱段的多光谱图像矩阵采用行堆叠的方法整合成二维矩阵 $\boldsymbol{Y}$，计算向量 $\boldsymbol{Y}$ 的平均值，计算过程如式(11)所示。

$$m=\boldsymbol{E}\{\boldsymbol{Y}\}\approx\frac{1}{N}\sum_{i=1}^{N}Y_i \tag{11}$$

其次，求向量 $\boldsymbol{Y}$ 的协方差矩阵 $\boldsymbol{C}$，计算过程如式(12)所示。

$$\boldsymbol{C}=\boldsymbol{E}\{(\boldsymbol{Y}-\boldsymbol{m})(\boldsymbol{Y}-\boldsymbol{m})^{\mathrm{T}}\}=\frac{1}{N}\sum_{i=1}^{N}\boldsymbol{Y}_i\boldsymbol{Y}_i^{\mathrm{T}}-\boldsymbol{m}\boldsymbol{m}^{\mathrm{T}} \tag{12}$$

最后，求协方差矩阵 $\boldsymbol{C}$ 的特征值和特征向量。可得 KL 变换表达式如式(13)所示。

$$\boldsymbol{Y}=\boldsymbol{A}^{\mathrm{T}}(\boldsymbol{Y}-\boldsymbol{m}) \tag{13}$$

该算法所需运算量巨大，其中计算 $M\times N$ 大小的谱段需要$(M\times N-1)$次加法和 1 次除法，计算 H 需要$(M\times N)$次减法，而其他步骤的运算所需的运算复杂度更高，针对此问题，将作如下改进。

首先，计算协方差时并不使用全部光谱向量，而是随机地选取光谱向量的一个子集，适当选取该子集大小，在保证图像质量的前提下尽量降低计算复杂度。通过实验可得，在采样后的尺寸为传统方法的 1/100 时，压缩性能最好，计算复杂度也较低，综合考虑压缩性能与计算时间，本文选用此值作为采样比估算协方差。

然后，求对称矩阵特征值与特征向量时常采用 Jacobi 算法，然而，利用 Jacobi 算法求特征值不仅要选取主元素，而且还要同时进行行与列的旋转变换，使得整个计算的过程十分复杂，难于并行实现。

为计算对称矩阵 $\boldsymbol{M}$ 的特征值，将采用一系列变换将矩阵 $\boldsymbol{M}$ 变为各列两两正交的方阵 $\boldsymbol{T}$，即 $\boldsymbol{M}\boldsymbol{V}_1\cdots\boldsymbol{V}_k=\boldsymbol{T}$，因此 $\boldsymbol{T}^{\mathrm{T}}\boldsymbol{T}=\boldsymbol{V}_k^{\mathrm{T}}\cdots\boldsymbol{V}_1^{\mathrm{T}}\boldsymbol{M}^{\mathrm{T}}\boldsymbol{M}\boldsymbol{V}_1\cdots\boldsymbol{V}_k$，我们可以根据矩阵 $\boldsymbol{T}$ 与 $\boldsymbol{T}^{\mathrm{T}}\boldsymbol{T}$ 的关系得出方阵 $\boldsymbol{T}$ 各列的谱范数即为所求对称阵特征值的绝对值，其正负可由特征值与特征向量的关系式 $Mb_i=\lambda_i b_i$ 中 Mb_i 与 b_i 的符号是否相同来判断，若相同，则 λ_i 为正，否则为负。

最后，计算特征向量矩阵。代替经典 KLT 中的矩阵乘法(均值×特征向量)，采用提升方案。将特征向量矩阵分解为 $\boldsymbol{A}^{\mathrm{T}}=\boldsymbol{PLUS}$，其中 $\boldsymbol{P}$ 为置换矩阵，$\boldsymbol{L}$ 为单位下三角矩阵，$\boldsymbol{U}$ 为单位上三角矩阵，$\boldsymbol{S}$ 为对角矩阵。为了保持无浮点输出，在每个阶段之后，对输出元素进行舍入。改进后的 KL 表达式如式(14)所示。

(C)1994-2023 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

$$\boldsymbol{Y} = \text{round}(\text{round}(\text{round}(\boldsymbol{XS})\boldsymbol{U})\boldsymbol{L})\boldsymbol{P} \tag{14}$$

式(14)中，round 表示四舍五入。乘以 $\boldsymbol{P}$ 就是元素交换，其中乘法仅由 1 和 0 进行。因此，置换并不是计算密集型的，因为它只需要循环遍历向量就可以交换某些元素。$\boldsymbol{S}$ 矩阵是稀疏的下三角矩阵；因此，通过将零校验技术应用于乘法运算，可以需要更少的元素乘法运算。

变换后效果图见图 2，对一幅多光谱图像(含 4 个谱段)的前三个谱段(a，b，c)分别作 KLT，得到三幅变换后的图像(d，e，f)，消除了大部分谱间冗余，能量主要集中在前两个谱段。

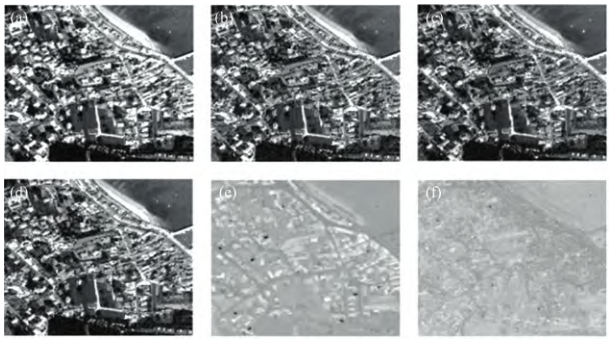

图 2　各个谱段 KL 变换效果图

Fig. 2　KL transformation effect diagram of each spectrum

1.3.4　数据流加密

为了进一步压缩，需要将原始信号转换为新的整数流，并将整数流转换为二进制编码流，并采用霍夫曼编码。但是，如果这些整数通过霍夫曼编码直接转换为二进制比特流，则也将需要太多的存储空间。因此，采用 DPCM 滤波器将原始信号转换为新的整数数组。

首先，用量化器对非零系数统一进行量化。然后，为了节约存储空间，进一步压缩非零系数，我们将处理得到的系数，使原始信号转换为新的整数数组。最后，将整数流转换成二进制编码流，实现图像的高效编码。

采用 Tent 映射对压缩后码流进行混淆扩散加密。假设明文压缩后的数据流为 R，Tent 映射初值和控制参数分别为 x'_0，x'_1，初始密文块为 x'_2。数据流加密过程如下。

首先，将 R 分成 n 个长度为 32 的子块 m。

然后，以 x'_0，x'_1 为初值和控制参数，迭代 n 次，迭代过程如式(15)所示。

$$y_q = \text{mod}(\text{round}(x'_q \times 10^{16}), 2^{32}) \tag{15}$$

最后，以 x'_2 为初始密文块，通过式(16)得到加密序列。其中，$SR[e, f]$ 表示将 e 右移 f 位，L_5 表示取序列的低 5 位。

$$x_i = SR[(\text{mod}((r_i \oplus m_q + x_{i-1}), 2^{32}), L_5(m_{(1+\text{mod}(x'_{i-1}, n))})] \tag{16}$$

2　结果与讨论

2.1　加密性能分析

2.1.1　抗攻击性分析

根据香农定理，熵可以反映信息量的大小。加密效果越好，信息越混乱，与此同时，图像中所含的信息越少，信息熵越大。信息熵的计算公式如式(17)

$$E = \sum_{i \in I} p_i \times \log(p_i) \tag{17}$$

式(17)中，p_i 为像素 i 出现的概率。表 1 显示了几种加密算法的信息熵差异。

表 1　信息熵对比

Table 1　Information entropy comparison

算法	信息熵
约瑟夫环算法	10.185 7
AES 算法	10.758 4
改进的 LOGISTIC 算法	11.135 1
本算法	11.794 3

从表 1 中可以看出，本算法的信息熵更接近理想值(12)，具有更好的抗攻击性。

像素变化率(the number of pixels change rate，NPCR)和归一化平均变化强度(the unified average changing intensity，UACI)是有效分析抗差分攻击的重要指标。其中 NPCR 表示不同密文图像在相同位置上灰度值互不相同的比率，UACI 表示不同密文图像之间的平均变化密度。其公式如式(18)和式(19)所示。

$$\text{NPCR} = \frac{\sum_{i,j} D(i, j)}{m \times n} \times 100\% \tag{18}$$

$$\text{UACI} = \frac{1}{m \times n} \sum_{i,j} \left| \frac{C_1(i, j) - C_2(i, j)}{255} \right| \times 100\% \tag{19}$$

其中，m 和 n 分别表示图像的行和列，当 $C_1(i, j) = C_2(i, j)$ 时 $D(i, j) = 0$，反之，$D(i, j) = 1$。表 2 列出了本算法与其他几种算法的 NPCR 和 UACI 的测试结果。

表 2　NPCR 和 UACI 的测试结果

Table 2　Test results of NPCR and UACI

算法	微小明文改变(像素值)	NPCR/%	UACI/%
算法 1[6]	1	99.60	33.50
算法 2[7]	1	99.62	31.59
本算法	1	99.81	34.19

NPCR 和 UACI 的值越大代表算法的抗差分攻击能力越强。由表 2 可知，本算法的 NPCR 和 UACI 优于现有算法，因此，与同类算法相比，本算法可以更好的抵御差分攻击。

为进一步验证本算法加密效果，选取多幅具有三个波段的多光谱图像进行加密前后的水平、垂直以及对角线方向的相关系数进行测试，测试结果(均值)见表 3。

由表 3 可知，经加密后，图像的相关系数明显降低。

本算法共 5 个初始密钥，每个密钥产生的精度空间接近 10^{16}。加密的过程中，密钥随着明文的变化而不断变化。因此，该算法具有较大的密钥空间，能有效抵抗已知明文攻击和穷举攻击。

(C)1994-2023 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net

表 3 加密前后相关性

Table 3 Correlation before and after encryption

波段	水平	垂直	对角
波段 1 原始图像	0.939 6	0.867 9	0.859 1
波段 1 加密图像	0.415 7	−0.004 7	−0.354 3
波段 2 原始图像	0.925 4	0.860 3	0.822 7
波段 2 加密图像	−0.003 2	−0.006 1	−0.253 8
波段 3 原始图像	0.941 6	0.924 3	0.847 8
波段 3 加密图像	−0.020 4	−0.000 7	0.318 1

2.1.2 加密敏感性分析

为了验证算法对密钥的敏感性，采用具有微小差异的密钥对原图像加密，比较码流的变化率。通过实验可得，输出比特流变化率保持在 47.62%～47.71%之间，具有较好的密钥敏感性。

保持密钥不变，随机改变图像中某一像素值，通过加密后的比特流变化评价本算法对明文的敏感性。对具有不同特征的特定压缩比的 QuickBird 进行 100 次仿真实验，通过实验可知，密文比特流变化率保持在 47.45%～47.52%。由此可知，本算法对明文图像很敏感，可有效抵抗差分攻击。

为方便观察实验结果，利用该算法对多光谱图像的某谱段进行加密，加密效果如图 3 所示。由图 3 可以看出，本算法具有较好的加密效果，有效地保护了多光谱图像的有用信息。

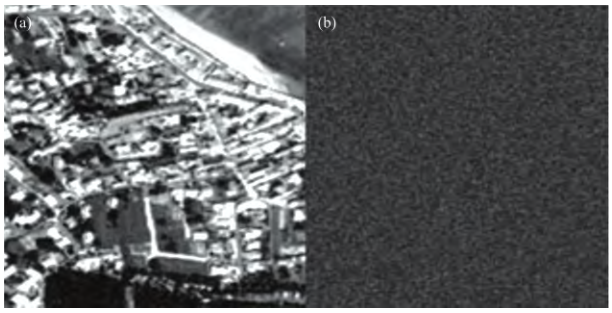

图 3 某谱段图像与加密图像

Fig. 3 Image of a certain spectrum and encrypted image

同时，本算法对多幅多光谱图像的不同谱段分别进行了测试，均有较好的加密效果。

2.2 压缩性能分析

为方便验证算法的可行性，测试图像选用具有三个谱段的多光谱图像。整个算法在计算机上用 Matlab R2012b 进行仿真。像素深度为 8 bit/pixel(b/p)，压缩比为 16∶1，实验结果如图 4 所示，其中 a 为原始图像，b 为重建后图像。

由图 4 可知，在码率比较高的情况下，本算法的 PSNR 特别高，重构后的图像与原图像差别不大。图像经 DWT 与 KLT 后，大部分像素值位于 1 bit，可见，光谱冗余被消除掉了。

为进一步验证压缩后图像的质量，选择 4 组具有不同特征的 QuickBird 多光谱图像进行测试，每组 20 幅，并用最近提出的多光谱图像压缩算法进行比较。测试结果见表 4。

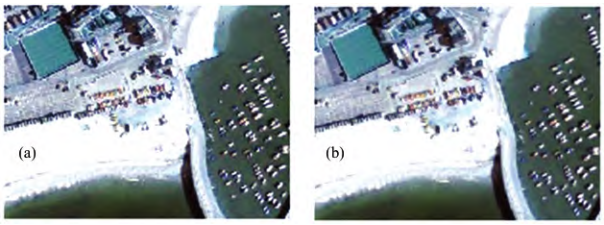

图 4 原始图像与压缩重构图像对比图

Fig. 4 Comparison of original image and compressed reconstructed image

表 4 压缩系统测试结果

Table 4 Test results of compression system

Methods	4∶1	8∶1	16∶1	32∶1
SA-DCT[8]	48.94	48.02	43.60	39.83
DWT-Tucker[9]	53.11	50.22	46.85	41.78
ATS[10]	50.17	45.87	43.36	41.23
JPEG2000[11]	49.45	48.11	45.07	40.31
Ours	54.15	50.98	47.49	42.40

由表 4 可知，在 4∶1～32∶1 范围内，本压缩算法达到很高的峰值信噪比，优于现有的压缩算法，在正常工作压缩比为 16∶1 时，比现有压缩算法的信噪比提高了 0.64 dB 以上。为进一步测试本算法的性能，进行了极高压缩比条件下的测试。在压缩比 64∶1 和 128∶1 的情况下，系统的 PSNR 可分别达到 35.03 和 31.28，优于现有算法 1 dB 以上。可见，本算法可行，且特别适合对压缩比要求较高的场合。

表 5 数据处理速度比较结果

Table 5 Comparison result of data processing speed

方法	吞吐率/(Mpixels·s^{-1})	频率/MHz
JPEG2000[11]	5.52	88
KLT[12]	9.77	88
DWT-Tucker[9]	11.26	88
3DSPIHT[13]	16.04	88
Ours	5.05	88

表 5 列出了本算法与现有的一些算法的数据处理速度比较结果。由表 5 可知，本文提出的压缩算法数据吞吐率低于现有压缩算法，与 JPEG2000 相比处理速度相当，但压缩比要远远高于 JPEG2000 以及其他压缩算法。本算法吞吐率略低的一部分原因是因为与其他压缩算法相比，算法中加入了加密算法，提高了算法的复杂度。随着硬件方案的不断完善，该算法的处理速度会不断提升，与此同时算法的高峰值信噪比优势将更加明显。

为验证算法的去冗余效果，测试图像选用 JPL 实验室的 AVIRIS 多光谱图像序列。多光谱图像经二维离散 9/7 小波变换后，大部分空间冗余被消除了，子带 HL 像素深度由 8 bit 减少到 0～6 bit，大部分像素值为 5 bit 左右。经 KL 变换后，大部分像素位于 0.9 bit 左右。对图像采用信息熵进行比较，经 9/7 小波变换后的图像信息熵为 6.864 9，KL 变换后

(C)1994-2023 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

图像的信息熵为 3.015 8。可见，多光谱图像经小波变换和 KL 变换后，空间冗余和光谱冗余大部分被消除了，图像的压缩比得到了极大的提升。

与多光谱图像相比，高光谱图像以及超光谱图像拥有更多的波段，同时波段更加连续，相邻波段高度相关，因此其数据量更大、冗余信息更多，压缩加密的难度会有所提升，但其冗余的特性相似。本算法基于光谱图像的谱间冗余以及空间冗余特性进行压缩以及加密，因此，本算法同样适用于高光谱图像以及超光谱图像的压缩加密，同时，在此基础上进行了大量的测试，测试效果较为理想。

原始像素和重建像素之间的光谱失真常用于测量保真度，而光谱角距离(SAD)是评价多光谱图像的最常用的标准之一。较小的 SAD 意味着压缩具有较少的信息损失，并且重构的多光谱图像对于后续应用更为可靠。为方便起见，我们采用均值 SAD 来揭示多光谱图像的平均光谱失真。关于不同方法的均值 SAD 的结果如图 5 所示。从图中我们可以看到，该方法在最大比特率下实现了较小的平均 SAD，这表明该方法的平均频谱失真小于其他方法。因此，所提出的方法具有良好的频谱保真度。

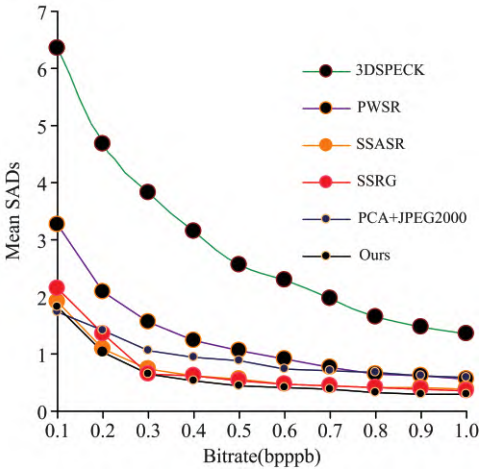

图 5　均值 SAD

Fig. 5　Mean SAD

3　结　论

多光谱图像在提供了关于地物更细致的光谱信息的同时，其数据量急剧增加，给机载和星载数据传输和存储带来困难。此外，由于某些侦察监视工作不希望被其他国家或者组织破解，因此除了通信链路加密之外，非常有必要对多光谱图像进行加密，以确保数据的安全性。在此基础上，本文提出一种将混沌思想、小波变换和 KL 变换相结合的多光谱图像压缩加密算法。该算法充分利用多光谱图像的冗余特性，弥补了传统算法的不足。实验结果表明，该方法信噪比高、运算时间短、密钥空间大，同时对密钥和明文敏感，并在频谱保真方面具有较好的效果。

References

[1] GUO Jia-wei, ZHANG Da-xing, YANG Shan-shan, et al(郭家伟，张大兴，杨姗姗，等). Computer Applications and Software(计算机应用与软件), 2019, (5): 178.
[2] Song Y J, Zhu Z L, Zhang W, et al. Nonlinear Dynamics, 2019, 95(3): 2235.
[3] Hu Z, Huang X, Yang Z, et al. Light: Science & Applications, 2021, 10: 140.
[4] Xiong J, Wu S T. eLight 2021, 1: 3.
[5] Zhang W, Song H, He X, et al. Light: Science & Applications, 2021, 10: 108.
[6] GUO Yi, SHAO Li-ping, YANG Lu(郭　毅，邵利平，杨　璐). Application Research of Computers(计算机应用研究), 2015, (4): 1131.
[7] ZHAO Xiao-long, LI Bo, JIA Peng, et al(赵晓龙，李　博，贾　芃，等). Chinese Journal of Electron Devices(电子器件), 2021, (1): 125.
[8] Jiao L C, Wang L, Wu J L, et al. IEEE Geoscience and Remote Sensing Letters, 2011, 8(2): 326.
[9] LI Jin, JIN Long-xu, LI Guo-ning(李　进，金龙旭，李国宁). Journal of Electronics & Information Technology(电子与信息学报), 2013, (2): 489.
[10] Ulug B. IEEE Transactions on Circuits and Systems for Video Technology, 2011, 21(7): 983.
[11] Gonzalez C, J, Bartrina R J, Serra S J. IEEE Geoscience and Remote Sensing Letters, 2010, 72(2): 251.
[12] Ian B, Joan S S. IEEE Tranctions on Geoscience and Remote Sensing, 2010, 48(7): 2854.
[13] Khelifi F, Bouridane A, Kurugollu F. IEEE Transactions on Multimedia, 2008, 10(3): 316.

(C)1994-2023 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net

Multispectral Image Compression and Encryption Algorithm Based on Chaos and Fast Wavelet Transform

XU Dong-dong[1], YU Xin[1]*, DU Li-min[1], BI Guo-ling[2]

1. Changchun University, Changchun 130022, China

2. Changchun Institute of Optics, Fine Mechanics and Physics, Chinese Academy of Sciences, Changchun 130033, China

Abstract A multispectral image compression and encryption algorithm that combines chaos, wavelet transform and KL transform is proposed for solving the security problem of multi-spectral image compression and transmission. Firstly, the K-means clustering scheme is used to cluster multi-spectral images into common pixels, and the performance of the algorithm is optimized by selecting the appropriate K value, and it is convenient for subsequent processing. Secondly, the multispectral image is clustered into general pixels, we will perform a two-dimensional discrete 9/7 wavelet transform on the general pixels, and then perform Arnold transform and encryption processing on the transformed coefficients to eliminate most of the spatial redundancy of the multispectral image and reduce the block effect of the compression process. Next, to eliminate residual spatial redundancy and spectral redundancy, the generated wavelet coefficients are performed by KL transform. Finally, differential pulse filters are used to encode the coefficients, and Tent mapping is used to implement confusion diffusion encryption on the code stream. Through experiments, it can be known that the information entropy of this algorithm reaches 11.794 3 (selecting 12-bit multispectral images), and the information entropy is closer to the maximum value of 12, which is better than the existing algorithm and can better hide the original image features. The NPCR and UACI are respectively 99.81% and 34.19, which are better than the existing other algorithms, which can better resist differential attacks. The output bit-stream change rate is maintained between 47.62%～47.71%, and the ciphertext bitstream change rate is maintained between 47.45%～47.52%, so this algorithm has good key sensitivity; In the range of 4∶1～32∶1, the system PSNR is above 42 dB, which has high compression performance. Within the range of 4∶1～32∶1, this compression algorithm achieves a very high peak signal-to-noise ratio, which is better than the existing compression algorithm. When the normal working compression ratio is 16∶1, it is better than the existing compression algorithm. The ratio is improved by more than 0.64 dB. In order to further verify the compression performance of the algorithm in the case of a high compression ratio, this paper tested the system's signal-to-noise ratio of 31.28 when the compression ratio is 128∶1. The reconstructed image is clearer at this time, which is more than 1dB better than the existing algorithm. It can be seen that this algorithm is feasible and particularly suitable for occasions which require a high compression ratio and has a good effect in terms of spectrum fidelity.

Keywords KL transform; Arnold transform; NPCR; UACI; Differential pulse filter

(Received Jul. 22, 2021; accepted Oct. 17, 2021)

* Corresponding author

(C)1994-2023 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net