

引用格式:杨威,王青竹,宋人杰,等. 三维图像联合加密和压缩算法 [J]. 微电子学与计算机,2020,37(7):78-81. [YANG W, WANG Q Z, SONG R J, et al. Joint encryption and compression method for three dimensional images [J]. Microelectronics & Computer,2020,37(7):78-81.]

三维图像联合加密和压缩算法

杨 威¹,王青竹²,宋人杰²,张元东²

(1 衢州光明电力投资集团有限公司 赋腾科技分公司,浙江 衢州 324000;

2 东北电力大学 计算机学院,吉林省 吉林 132012)

摘 要: 现有联合加密和压缩算法对三维图像序列可达到足够高的解密精度或压缩比,但却不能同时达到高的解密精度和压缩比,因为图像序列一般都被单独处理,所以通常忽略了它们之间的关系. 为解决上述问题,将张量压缩感知(TCS)联合加密和压缩的三维序列作为一个张量进行处理. 为进一步增强安全性,构建一个非自治洛伦兹系统来控制 TCS 的三个测量矩阵. 新算法保留了基于张量 3D 图像序列的内部结构,并实现了压缩比、解密精度和安全性之间的有效平衡. 实验结果验证了提出方案的有效性和可靠性.

关键词: 张量压缩感知;张量分解;三维图像;三维混沌密文

中图分类号: TN751

文献标识码: A

文章编号: 1000—7180(2020)07—0078—04

Joint encryption and compression method for three dimensional images

YANG Wei¹, WANG Qing-zhu², SONG Ren-jie², ZHANG Yuan-dong²

(1 Quzhou Futeng Information Technology Company Limited, Quzhou 324000, China;

2 School of Computer Science, Northeast Dianli University, Jilin 132012, China)

Abstract: Existing techniques for the simultaneous encryption and compression of three-dimensional (3D) image sequences may come with sufficient decryption accuracy or compression ratio, but do not inherently have both; the relationship between them is generally ignored because the images of a sequence are handled individually. To address this problem, we designed Tensor Compressive Sensing (TCS) to simultaneously encrypted compress a 3D sequence a tensor rather than sever a 2D images. The proposed method preserves the intrinsic structure of tensor-based 3D image sequences and achieves favorable balance of compression ratio, decryption accuracy, and security. Numerical simulation results verify the validity and the reliability of the TCS scheme.

Key words: tensor compressed sensing; tensor decomposition; three dimensional images; three dimensional chaotic ciphers

1 引言

近年来,网络多媒体发展迅速,且在现实生活中应用非常广泛. 多种加密技术已经应用于如彩色图像、视频序列和医学图像序列等多种 3D 图像序列,但大多数 3D 图像序列在加密过程中没有考虑到压缩. 快速和安全的图像传输过程要求减少数据量的

传输(压缩)并保护这些数据免受未经授权的访问(加密). 因此,针对 3D 图像的联合压缩和加密算法具有重要意义^[1].

本文在文献[2-14]的研究基础上,针对三维图像序列,如 CT 图像序列和灰度视频图像序列,提出一种基于改进 TCS 和 3D 洛伦兹并将加密和解密的 3D 图像作为张量的联合压缩和加密系统,同时

将交替最小二乘法(ALS)引入到基于 HOSVD 的 TCS 来对其进行优化,然后构建一个 3D 洛伦兹系统来控制三个测量矩阵.该算法主要有三个优势:(1)内在张量数据结构的保留减少了解密误差并提高了压缩比;(2)将传输数据注入到动态系统来指导非自主调制,有效增强了安全性;(3)由张量分解和 3D 洛伦兹生成的数据组成密钥.将 TCS 中张量积的顺序作为附加密钥以增加未经授权解密的难度.

2 改进的算法

本文提出的压缩和解压缩过程分别被嵌入在加密和解密中,具体过程如图 1 所示.

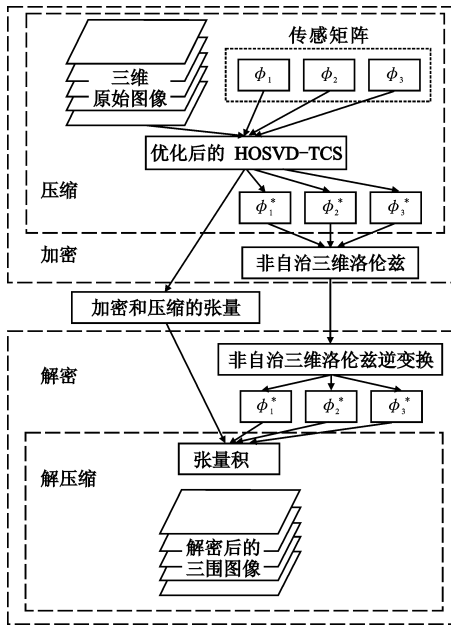


图 1 算法流程图

2.1 加密

受交替最小二乘法(ALS)的启发,对 $\Phi_1 \Phi_2 \Phi_3$ 进行了优化,对于初始的 3D 图像 $A \in R^{M_1 \times M_2 \times M_3}$,加密过程包含如下步骤:

(1) 随机初始化这三个高斯传感矩阵 $\Phi_i^{(0)} \in R^{M_i \times m_i}$ ($m_i < M_i, i = 1, 2, 3$).为了精确的解密 A ,优化的 Φ_i^* 应该满足:

$$\{\Phi_1^*, \Phi_2^*, \Phi_3^*\} = \underset{\Phi_1, \Phi_2, \Phi_3}{\operatorname{argmin}} \|A - W \times_1 \Phi_1 \times_2 \Phi_2 \times_3 \Phi_3\|_F^2 \quad (1)$$

这个问题可转换为如下式子^[15]:

$$\{\Phi_1^*, \Phi_2^*, \Phi_3^*\} = \underset{\Phi_1, \Phi_2, \Phi_3}{\operatorname{argmax}} \|A \times_1 \Phi_1^T \times_2 \Phi_2^T \times_3 \Phi_3^T\|_F^2 \quad (2)$$

为了解决这个问题,找到满足 $\Phi_i^T \Phi_i = I$ 的 Φ_i 就够了.为进一步增强重构算法的精确度,使用 ALS 算法对公式(2)进行改进.

(2) 当 $k = 0$ 时,迭代公式(3)至公式(6),直到 Φ_i 收敛或达到最大迭代次数.

$$Z^{(1)} = A \times_2 \Phi_2^{(k)T} \times_3 \Phi_3^{(k)T} \quad (3)$$

$$Z^{(2)} = A \times_1 \Phi_1^{(k)T} \times_3 \Phi_3^{(k)T} \quad (3)$$

$$Z^{(3)} = A \times_1 \Phi_1^{(k)T} \times_2 \Phi_2^{(k)T} \quad (3)$$

$$Z_i = (Z^{(i)})_{(i)} \quad (4)$$

$$Z_i \approx U_{i, m_i} \sum_{i, m_i} V_{i, m_i}^T \quad (5)$$

式中, $\sum_{m_i} = \operatorname{diag}\{\sigma_1, \dots, \sigma_{m_i}\}$ 代表一个 Z_i 中包含第 m_i 个最大奇异值的对角矩阵,其中 $\sigma_1 \geq \sigma_2 \geq \dots \geq \sigma_{m_i}$. U_{m_i} 和 V_{m_i} 分别代表以列作为 Z_i 前导的 m_i 左奇异向量和右奇异向量的矩阵.令

$$\Phi_i^{(k+1)} = U_{i, m_i} \quad (6)$$

公式(3)和(4)在修正三个测量矩阵中的两个测量矩阵的同时,更新另外一个测量矩阵.公式(5)计算 Z_i 中第 m_i 个截尾 SVD,然后获得优化的 Φ_1, Φ_2 和 Φ_3 .在文献[15]中可查阅更多有关 ALS 的计算过程.

(3) 计算压缩核心张量:

$$W = A \times_1 \Phi_1^T \times_2 \Phi_2^T \times_3 \Phi_3^T \quad (7)$$

(4) 将 W 展开到其第 n 个模式 $W_{(n)}$.其中,模式 n 代表有 1, 2, 3 三个可能取值的私钥.

(5) Φ_1, Φ_2, Φ_3 通过下面提出的 3D 洛伦兹系统同时构建,受非自治 3D 洛伦兹系统可同时加密两个数据集的启发^[16],本文设计一种将三个测量矩阵嵌入到三个状态变量的 3D 洛伦兹系统.令 $\varphi_d = \operatorname{vec}(\Phi_d) = \{\varphi_d^k\}, d = 1, 2, 3, k = 1, \dots, m_d \times M_d$.矩阵 Φ_d 的向量化 $\operatorname{vec}(\cdot)$ 表示为, φ_d 其通过连接 Φ_d 的每个列向量组成. φ_d^k 代表向量 φ_d 的第 k 个元素.这三个测量矩阵 Φ_1, Φ_2, Φ_3 分别被插入到三个状态变量中:

$$\begin{cases} U_{k+1} = g_1((V_k - U_k)A + \varphi_1^k) + U_k \\ V_{k+1} = g_2((BU_k - V_k - 20U_k W_k) + \varphi_2^k) + V_k \\ W_{k+1} = g_3((5U_k V_k - CW_k) + \varphi_3^k) + W_k \end{cases} \quad (8)$$

式中, U_0, V_0, W_0 代表在发射端和接收端作为密钥一部分的初始值.为 $W_{(n)}$ 发射信号, U 为状态变量,其中 $U \in R^{M_1 \times m_1}, W_{(n)} \in R^{m_1 \times m_2 \times m_3}$.因此压缩比可表示为:

$$\gamma = \frac{m_1 m_2 m_3 + m_1 M_1}{M_1 M_2 M_3} \approx \frac{m_1 m_2 m_3}{M_1 M_2 M_3} \quad (9)$$

2.2 解密

因为发射的加密信号是一个单状态变量,所以在解密过程中需要进行迭代,但迭代过程传了三个数据值.这里给出一个包含三个状态变量和无穷

解的方程,在发射端的发生器进行三次加密,产生了包含三个未知数的三个方程,若其他参数已知,则产生一个唯一解。

在这种情况下, U_{k+1} 仅传送 φ_1^k . 在接收器端,为了计算 φ_1^k ,在第一个公式中的所有变量包括 U_{k+1} 是已知的. 由于 U_{k+1} 是第一个接收信号, φ_1^k 可以通过如下式子计算:

$$\tilde{\varphi}_1^k = \frac{1}{g_1}(U_{k+1} - U_k) - A(V_k - U_k) \quad (10)$$

然而,为了更新接收器的状态变量,所有的 φ_1^k 、 φ_2^k 、 φ_3^k 必须是已知的,考虑使用下列公式进行计算:

$$\tilde{V}_{k+1} = \frac{1}{A}(\frac{(U_{k+2} - U_{k+1})}{g_1} - \tilde{\varphi}_1^{k+1}) + U_{k+1} \quad (11)$$

$$\tilde{\varphi}_2^k = \frac{1}{g_2}(\tilde{V}_{k+1} - V_k) - (BU_k - V_k - 20U_k W_k) \quad (12)$$

$$\tilde{W}_{k+1} = -\frac{(\frac{(V_{k+2} - V_{k+1})}{g_2} + V_k - BU_k - \tilde{\varphi}_2^{k+1})}{20U_k} \quad (13)$$

$$\tilde{\varphi}_3^k = \frac{1}{g_3}(\tilde{W}_{k+1} - W_k) - (5U_k V_k - CW_k) \quad (14)$$

式中, $\tilde{\varphi}_1^{k+1} = \tilde{\varphi}_1^k$, $\tilde{\varphi}_2^{k+1} = \tilde{\varphi}_2^k$.

解密过程如下:

(1) 由所有解密元素 $\tilde{\varphi}_d^k$ 构成解密测量矩阵 D_{Φ} .

(2) $W_{(n)}$ 和得到的 D_{Φ_i} 以正确的顺序相乘来恢复 A' ,有以下三种可行的方法来实现:

$$A'_{(n)} = \begin{cases} D_{\Phi_1} \cdot S_{(1)} \cdot (D_{\Phi_2} \otimes D_{\Phi_3})^T \\ D_{\Phi_2} \cdot S_{(2)} \cdot (D_{\Phi_3} \otimes D_{\Phi_1})^T \\ D_{\Phi_3} \cdot S_{(3)} \cdot (D_{\Phi_1} \otimes D_{\Phi_2})^T \end{cases} \quad (15)$$

式中“ $\otimes$ ”代表克罗内克积. 实际处理过程中, $A'_{(n)}$ 的计算要根据 n 值而定. n 取 1、2、3 时,分别对应第 1、2、3 种计算方法.

(3) 根据私钥 n 将 $A'_{(n)}$ 还原为 A' .

除了测量矩阵的密钥外,模式 n 展开(张量积的顺序)也可以作为附加密钥.

3 实验结果分析

数值模拟实验在 CPU 为 Intel Core i7, RAM 为 32GB, 仿真环境为 Matlab2011 的主机上进行. <http://imaging.cancer.gov/programsandresources/InformationSystems/LIDC> 网站肺部图像数据库联盟(LIDC)提供的肺部 CT 图像.

本文将提出算法与其它算法(包括 DCT、Wavelet、CS、TCS)进行对比突出提出算法的优越性. 如文献[9,10]所述,在 FrMT 域基于二维 CS 的

加密算法(这里将该算法定义为算法 1. 其具有有效性强、鲁棒性高和安全的加密性能. 在该算法中,二维 CS 是基于测量矩阵由混沌映射和二维 NSL₀ 组成的二维小波变换. 在 FrFT 域基于 HOSVD-TCS 的加密算法[11]应用也很广泛,这里将该算法定义为算法 2. 如文献[2]所述,与先前的加密和压缩算法相比,基于谱融合和 DCT 的加密算法会产生更佳的 PSNR 值,这里将该算法定义为算法 3.

肺部 CT 视频序列的每一帧预处理成 512×512 大小,并选取 512 帧,则视频序列作为一个整体由 $512 \times 512 \times 512$ 个张量表示,且共有 134 217 728 个体素. 针对每个模式随机构造的高斯测量矩阵大小为 $512 \times m_i$ ($i=1,2,3$),所以采样率(压缩比)由以下式子计算得出:

$$\gamma = \frac{m_1 m_2 m_3}{512 \times 512 \times 512} \quad (16)$$

解密误差通过峰值信噪比 PSNR 来定量测量, PSNR 是由解密数据和原数据间的均方根误差(RMSE)得到,可由如下式子表示:

$$\text{PSNR} = 20 \log_{10} \frac{255}{\text{RMSE}} \quad (17)$$

图 2 是不同算法的图像压缩比与峰值信噪比的关系曲线,表 1 是算法的运行时间. 同时由实验结果可看出,随着压缩比的增加,提出算法相较于其它算法的优势更大. 体现最明显的如算法 3,在提高压缩比的情况下需要消耗大量帧,此时随着帧数的增加, PSNR 值迅速下降,因此该算法在处理超过一定数量帧时其效果也会下降.

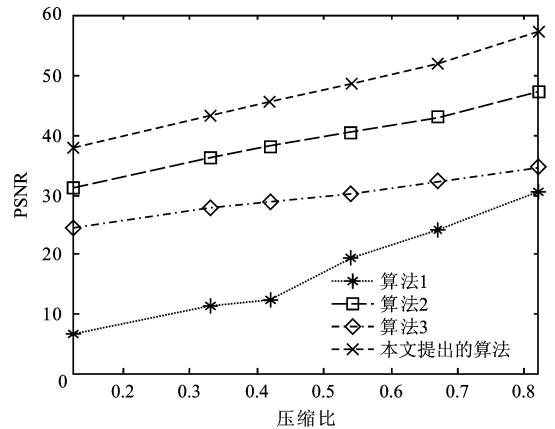


图 2 不同算法的图像压缩比与峰值信噪比

本文也比较了每种情况的计算时间(在所有采样比和噪声水平下实验的平均计算时间). 由表 1 比较发现,算法 3 的计算时间更快,而提出算法的迭代方式比算法 1 和算法 2 更简单.

表 1 算法运行时间

方法	运行时间/s
算法 1	896
算法 2	185
算法 3	160
本文提出算法	230

提出算法的密钥由 3D 洛伦兹控制的三个测量矩阵和核心张量 W 的模式 n 展开生成的数据构成. 使用 3D 洛伦兹控制的 Φ_i 上的密钥是 U_0, V_0, W_0 , 参数 A, B, C 以及每个状态方程的 g_i 值的状态变量的初始值. 这里使用 64 位双精度 (10^{-15} 精度等级), 所以三个测量矩阵的密钥空间为 $10^{15 \times 9} = 10^{135}$ 大小. 同时张量积的顺序可以作为附加密钥, 其共有 18 种组合. 提出算法的总的密钥空间大于 $10^{353} \cdot 18 \gg 2^{30}$, 即提出算法足以阻挡更强的破译攻击.

4 结束语

本文提出一种针对 3D 图像序列的联合压缩和加密算法. 该方法保留了 TCS 和 3D 洛伦兹的优点, 并实现了在高压缩比下的高精度解密, 提出算法的安全性也满足加密技术标准的要求. 同时, 张量积的展开模式特征可作为附加密钥使未授权的解密更具挑战性.

参考文献:

[1] 杨鹏. 基于混沌 Gyrator 变换与压缩感知的光学图像加密算法[J]. 计算机测量与控制, 2018, 238(7): 260-264.

[2] ALFALOU A, BROSSEAU C, ABDALLAH N. Simultaneous compression and encryption of color video images [J]. Optics Communications, 2015 (338): 371-379.

[3] TONG X J, WANG Z, ZHANG M, et al. A new algorithm of the combination of image compression and encryption technology based on cross chaotic map[J]. Nonlinear Dynamics, 2013, 72(1/2):229-241.

[4] TONG X J, ZHANG M, WANG Z, et al. A joint color image encryption and compression scheme based on hyper-chaotic system[J]. Nonlinear Dynamics, 2016, 84(4):2333-2356.

[5] YANG H Q, LIAO X F, WONG KW, et al. SPIHT-based joint image compression and encryption[J]. Acta Physica Sinica Chinese Edition, 2012, 61(4):40505.

[6] CAMBARERI V, MANGIA M, PARESCHIF, et al. On Known-Plaintext Attacks to a Compressed Sensing-Based Encryption: A Quantitative Analysis[J]. IEEE

Transactions on Information Forensics and Security, 2015, 10(10):2182-2195.

[7] 王厚林,李智. 一种基于压缩感知与混沌系统的比特级图像加密方法[J]. 软件导刊,2017(4):188-121.

[8] ZHAO S, WANG L, LIANG W, et al. High performance optical encryption based on computational ghost imaging with QR code and compressive sensing technique[J]. Optics Communications, 2015 (353): 90-95.

[9] ZHOU N, LI H, WANG D, et al. Image compression and encryption scheme based on 2D compressive sensing and fractional Mellin transform[J]. Optics Communications, 2015(343):10-21.

[10] ZHOU N, PAN S, CHENG S, et al. Image compression-encryption scheme based on hyper-chaotic system and 2D compressive sensing[J]. Optics & Laser Technology, 2016(82):121-133.

[11] CAIAFA C F, CICHOCKI A. Stable, Robust and Super Fast Reconstruction of Tensors Using Multi-Way Projections[J]. IEEE Transactions on Signal Processing, 2014, 63(3):780-793.

[12] DUARTE M F, BARANIUK R G. Kronecker compressive sensing[J]. IEEE Transactions on Image Processing A Publication of the IEEE Signal Processing Society, 2012, 21(2):494-504.

[13] SIDIROPOULOS N D, KYRILLIDIS A. Multi-Way Compressed Sensing for Sparse Low-Rank Tensors [J]. IEEE Signal Processing Letters, 2012, 19(11):757-760.

[14] HAROUN M F, GULLIVER T A. A new 3D chaotic cipher for encrypting two data streams simultaneously [J]. Nonlinear Dynamics, 2015, 81(3):1053-1066.

[15] SHEEHAN B N, SAAD Y. Higher order orthogonal iteration of tensors (HOOT) and its relation to PCA and GLRAM[J]. 2007: 355-365. DOI: 10.1137/1.9781611972771.32

[16] HAROUN M F, GULLIVER T A. A new 3D chaotic cipher for encrypting two data streams simultaneously [J]. Nonlinear Dynamics, 2015, 81(3):1053-1066.

作者简介:

杨威 男,(1981-),硕士,高级工程师,企业一级人力资源师.研究方向为科技信息化在电力系统的应用、智能电网.

王青竹 女,(1984-),博士,副教授.研究方向为多维信号处理、智能控制.

宋人杰 女,(1966-),硕士,教授.研究方向为智能信息处理及电力应用、多媒体技术应用.

张元东(通讯作者) 男,(1993-),硕士研究生.研究方向为视频编解码. E-mail:1406632033@qq.com.