DOI：10.19789/j.1004-9398.2026.04.010　　**Open Access**
文献引用：孙紫欣，马金铭，李煜玮，等．三元数哈特莱变换及其在图像加密中的应用[J]．首都师范大学学报（自然科学版），2026，47(4)：95-103. Sun Zixin，Ma Jinming，Li Yuwei，et al. Trinion Hartley transform and its application in image encryption[J]. Journal of Capital Normal University（Natural Science Edition），2026，47(4)：95-103.

三元数哈特莱变换及其在图像加密中的应用*

孙紫欣，马金铭**，李煜玮，张守岐

（首都师范大学信息工程学院，北京　100048）

摘要：本文提出三元数哈特莱变换（THT）并给出其所满足的常用性质，如线性性质、循环移位性质、卷积定理等。此外，推导THT与傅里叶变换之间的关系，并据此提出基于FFT的THT快速算法。最后，基于所提THT及其快速算法，提出适用于彩色图像的加密和解密方法，并通过实验验证所提方法的有效性。

关键词：三元数；哈特莱变换；快速算法；图像加密
中图分类号：TP309.7　　**文献标志码**：A

Trinion Hartley transform and its application in image encryption*

Sun Zixin，Ma Jinming**，Li Yuwei，Zhang Shouqi

（Information Engineering College，Capital Normal University，Beijing　100048）

Abstract：This paper proposes the trinion Hartley Transform（THT）and presents its commonly used properties，such as linearity，cyclic shift property，convolution theorem，and so on. In addition，the relationship between THT and Fourier Transform is derived，and a fast computation for THT based on FFT is proposed. Finally，based on the proposed THT and its fast computation，encryption and decryption methods suitable for color images are proposed，and the effectiveness of the proposed methods are verified by simulation results.

Keywords：trinion；Hartley transform；fast computation；image encryption
CLC：TP309.7　　**DC**：A

0　引　言

图像是人类社会活动中最常用的一种信息载体，也是人们获取、表达和传递信息主要的手段之一。随着信息技术的飞速发展，图像安全问题日益凸显。图像加密可将原始图像中的像素序列位置彻底打乱，以此掩盖图像原始信息，是保障信息安全的核心手段之一，已成为信号处理、计算机视觉和信息安全等领域的研究热点。传统的图像加密方法可基于混沌系统[1-3]、DNA编码[4-6]或光学[7-9]等时域方法实现，也可结合傅里叶变换、小波变换、正或余弦变换、希尔伯特变换、哈特莱变换等变换域方法实现[10-11]，其中变换域方法因具备更高的安全性和鲁棒性而被广泛适用。哈特莱变换[12-14]作为一种实值变换，在图像加密领域展现出独特的优势。然而，传统哈特莱变换方法多适用于处理灰度图像，在处理

收稿日期：2025-08-19
*国家自然科学基金青年科学基金项目（62201318）；北京市教育委员会科研计划一般项目（KM202410028012）
**通信作者：jinming_ma@cnu.edu.cn

彩色图像时只能简单地将红色(red,R)、绿色(green,G)和蓝色(blue,B)通道分别作为灰度图像各自进行处理,再对结果进行整合。这种方法的弊端在于忽视了各通道之间的关联性,难以达到好的加密效果。

近年来,三元数[15-16]、四元数[17-20]等超复数理论受到图像处理领域的广泛关注。三元数、四元数作为超复数,包含1个实部和多个虚部,利用此特性可将彩色图像的R、G、B通道作为三元数或四元数的1个实部和2个虚部。这种方法能够充分利用彩色图像各光谱通道间的内在关联性,为彩色图像提供了有效的一体化描述和处理方法,因而在彩色图像加密方面展现出独特价值。例如,离散三元数傅里叶变换与压缩感知相结合的图像加密方法通过在变换域引入稀疏表示与随机测量,可有效提升系统抵抗明文攻击与统计分析的能力[15]。此外,基于三元数离散余弦变换的图像加密方法能够在保视觉质量的前提下,实现高安全性图像加密[16]。

哈特莱变换作为一种经典的信号实值变换,其与三元数理论相结合,构建三元数哈特莱变换(trinion Hartley transform,THT),并系统研究其性质、快速算法及其在图像加密中的应用,具有重要的理论和应用价值。因此,本文研究THT以及相应的彩色RGB图像加密方法。通过将任意三元数信号分解为1个实部与2个虚部分量,并基于哈特莱变换,构造出THT,进而推导变换所满足的性质。所提THT可自然适配彩色图像的R、G、B通道耦合表示,兼具实值变换的运算效率。此外,本文基于THT,设计适用于彩色红绿蓝(red,green and blue,RGB)图像的加密与解密算法,并通过仿真实验验证所提算法的安全性与有效性。

1 预备知识

1.1 三元数

三元数是超复数的一种,可表示为[14]

$$q = a + \mathrm{i}b + \mathrm{j}c, \tag{1}$$

式中:a、b、c均为实数;i、j为虚数单位,满足以下规则

$$\mathrm{i}^2 = -1,\quad \mathrm{j}^2 = -1,\quad \mathrm{ij} = \mathrm{ji} = \mathrm{k},\quad \mathrm{k}^2 = 1。 \tag{2}$$

三元数之间的乘法遵循分配律。给定2个三元数$a = a_1 + a_2\mathrm{i} + a_3\mathrm{j}$和$b = b_1 + b_2\mathrm{i} + b_3\mathrm{j}$,它们的乘积$c = a \times b$可通过分配律和虚数单位规则(式(2))计算,即$c = (a_1b_1 - a_2b_2 - a_3b_3) + (a_1b_2 + a_2b_1)\mathrm{i} + (a_1b_3 + a_3b_1)\mathrm{j}$。

在利用三元数表征离散彩色图像$x(m,n)$时,可将R、G、B通道作为三元数的1个实部和2个虚部,即

$$x(m,n) = R(m,n) + \mathrm{i}G(m,n) + \mathrm{j}B(m,n), \tag{3}$$

其中彩色图像的R通道对应三元数的实部,G、B分别对应三元数的第1、第2虚部。

1.2 离散哈特莱变换

定义1 假设离散信号$x(n)$是长度为N的实信号,其哈特莱变换为[12]

$$X(k) = \sum_{n=0}^{N-1} x(k)\operatorname{cas}\left(\frac{2\pi nk}{N}\right)。 \tag{4}$$

2 THT的定义与性质

本节提出THT,给出该变换的定义,并推导其具备的一些常用性质。

2.1 THT定义

定义2 假设$x(n) = x_0(n) + \mathrm{i}x_1(n) + \mathrm{j}x_2(n)$是长度为$N$的三元数信号,其哈特莱变换为

$$X(k) = \boldsymbol{\mathcal{T}}[x](k) = \sum_{n=0}^{N-1} x(n)\operatorname{cas}\left(\frac{2\pi nk}{N}\right) = \sum_{n=0}^{N-1}\left[x_0(n)\operatorname{cas}\left(\frac{2\pi nk}{N}\right) + \mathrm{i}x_1(n)\operatorname{cas}\left(\frac{2\pi nk}{N}\right) + \mathrm{j}x_2(n)\operatorname{cas}\left(\frac{2\pi nk}{N}\right)\right], \tag{5}$$

式中$\boldsymbol{\mathcal{T}}$为THT算子。

二维信号$x(m,n)=x_0(m,n)+\mathrm{i}x_1(m,n)+\mathrm{j}x_2(m,n)$的THT可通过行列分离的方式实现。这是由于该变换具有线性性质,且二维运算在行与列维度上可分离。因此,完整的二维变换可分解为2个步骤:先对信号的每一行施加一维THT,再对所得结果的每一列施加一维THT。具体公式为

$$X(p,q) = \boldsymbol{\mathcal{T}}[x](p,q) = \sum_{m=0}^{M-1}\sum_{n=0}^{N-1} x(m,n)\operatorname{cas}\left(\frac{2\pi pm}{M}\right)\operatorname{cas}\left(\frac{2\pi qn}{N}\right)。 \tag{6}$$

定义3 THT的逆变换定义为

$$x(n) = \boldsymbol{\mathcal{T}}^{-1}[X](k) = \frac{1}{N}\sum_{k=0}^{N-1} X(k)\operatorname{cas}\left(\frac{2\pi nk}{N}\right)。 \tag{7}$$

证明 将定义2中的$X(k)$代入定义3的右端

$$\frac{1}{N}\sum_{k=0}^{N-1} X(k)\operatorname{cas}\left(\frac{2\pi nk}{N}\right) = \frac{1}{N}\sum_{k=0}^{N-1}\left(\sum_{m=0}^{N-1} x(m)\operatorname{cas}\left(\frac{2\pi mk}{N}\right)\right)\operatorname{cas}\left(\frac{2\pi nk}{N}\right) = \sum_{m=0}^{N-1} x(m)\left[\frac{1}{N}\sum_{k=0}^{N-1}\operatorname{cas}\left(\frac{2\pi mk}{N}\right)\operatorname{cas}\left(\frac{2\pi nk}{N}\right)\right]。 \tag{8}$$

由cas函数的正交性,可得

$$\frac{1}{N}\sum_{k=0}^{N-1}\mathrm{cas}\left(\frac{2\pi mk}{N}\right)\mathrm{cas}\left(\frac{2\pi nk}{N}\right)=\delta(m-n)=\begin{cases}1, m=n,\\0, m\neq n,\end{cases}\tag{9}$$

式中m、n = 0, 1, …, N–1。代入式(8)得

$$\frac{1}{N}\sum_{m=0}^{N-1}x\ (m)N\delta(m-n)=x(n)。\tag{10}$$

2.2　THT的性质

性质1(线性性质)　对任意三元数常数α、β及离散信号q、h,其线性组合的$\alpha x(n)+\beta y(n)$THT为

$$\mathcal{T}[z](k)=\alpha\mathcal{T}[x](k)+\beta\mathcal{T}[y](k)。\tag{11}$$

证明　由定义2可得,$\alpha x(n)+\beta y(n)$的THT为

$$\mathcal{T}[z](k)=\sum_{n=0}^{N-1}\big(\alpha x(n)+\beta y(n)\big)\mathrm{cas}\left(\frac{2\pi nk}{N}\right)=\alpha\sum_{n=0}^{N-1}x\ (n)\mathrm{cas}\left(\frac{2\pi nk}{N}\right)+\beta\sum_{n=0}^{N-1}y\ (n)\mathrm{cas}\left(\frac{2\pi nk}{N}\right)=\alpha T[x](k)+\beta T[y](k)。\tag{12}$$

性质2(实部虚部分离性)　设$x(n)=x_0(n)+\mathrm{i}x_1(n)+\mathrm{j}x_2(n)$,其THT$X(k)=X_R(k)+\mathrm{i}X_{I1}(k)+\mathrm{j}X_{I2}(k)$的分量可利用如下方式分离计算:

$$\begin{cases}X_R(k)=\sum_{n=0}^{N-1}x_0\ (n)\mathrm{cas}\left(\frac{2\pi nk}{N}\right),\\X_{I1}(k)=\sum_{n=0}^{N-1}x_1\ (n)\mathrm{cas}\left(\frac{2\pi nk}{N}\right),\\X_{I2}(k)=\sum_{n=0}^{N-1}x_2\ (n)\mathrm{cas}\left(\frac{2\pi nk}{N}\right),\end{cases}\tag{13}$$

式中$X_R(k)$、$X_{I1}(k)$、$X_{I2}(k)$均为实值函数,每个分量独立计算,无耦合项。

证明　由定义2和性质1可得

$$X(k)=\sum_n\big[x_0(n)+\mathrm{i}x_1(n)+\mathrm{j}x_2(n)\big]\mathrm{cas}\left(\frac{2\pi nk}{N}\right),\tag{14}$$

直接得

$$\begin{cases}X_R(k)=\mathrm{Re}\{X(k)\}=\sum_n x_0\ (n)\mathrm{cas}\left(\frac{2\pi nk}{N}\right),\\X_{I1}(k)=\mathrm{Im_i}\{X(k)\}=\sum_n x_1\ (n)\mathrm{cas}\left(\frac{2\pi nk}{N}\right),\\X_{I2}(k)=\mathrm{Im_j}\{X(k)\}=\sum_n x_2\ (n)\mathrm{cas}\left(\frac{2\pi nk}{N}\right)。\end{cases}\tag{15}$$

这一性质表明,THT的实部和2个虚部(对应彩色RGB图像的3个通道)可以独立地进行计算,无需耦合。这一优势使其便于硬件并行实现,从而大幅提升大规模图像处理的效率。

性质3(循环移位性质)　长度为N的三元数信号$x(n)$循环移位d位后得到$x_d(n)=x((n-d)\bmod N)$其THT为

$$X_d(k)=X_R(k)\cos\left(\frac{2\pi dk}{N}\right)+X_{I1}(k)\sin\left(\frac{2\pi dk}{N}\right)+\mathrm{i}\left[X_{I1}(k)\cos\left(\frac{2\pi dk}{N}\right)-X_R(k)\sin\left(\frac{2\pi dk}{N}\right)\right]+\mathrm{j}X_{I2}(k),\tag{16}$$

式中$X(k)=X_R(k)+\mathrm{i}X_{I1}(k)+\mathrm{j}X_{I2}(k)$是原信号$x(n)$的THT,$X_R(k)$,$X_{I1}(k)$,$X_{I2}(k)$分别为$X(k)$的实部、第1个虚部和第2个虚部。

证明　由定义2可得,$x_d(n)$的THT为

$$X_d(k)=\sum_{n=0}^{N-1}x_d\ (n)\mathrm{cas}\left(\frac{2\pi nk}{N}\right)=\sum_{n=0}^{N-1}x\ ((n-d)\bmod N)\mathrm{cas}\left(\frac{2\pi nk}{N}\right),\tag{17}$$

令$m=n-d$,则$X_d(k)=\sum_{m=0}^{N-1}x\ (m)\mathrm{cas}\left(\frac{2\pi(m+d)k}{N}\right)$。展开cas函数

$$\mathrm{cas}\left(\frac{2\pi(m+d)k}{N}\right)=\cos\left(\frac{2\pi(m+d)k}{N}\right)+\sin\left(\frac{2\pi(m+d)k}{N}\right),\tag{18}$$

并应用三角恒等式

$$\begin{cases}\cos(A+B)=\cos A\cos B-\sin A\sin B,\\\sin(A+B)=\sin A\cos B+\cos A\sin B,\end{cases}\tag{19}$$

式中$A=\frac{2\pi mk}{N}$,$B=\frac{2\pi dk}{N}$,可得

$$X_d(k)=\sum_{m=0}^{N-1}x\ (m)\big[(\cos A\cos B-\sin A\sin B)+(\sin A\cos B+\cos A\sin B)\big]。\tag{20}$$

由性质2可得

$$\begin{cases}\sum_m^{N-1}x\ (m)\cos A=X_R(k)+\mathrm{i}X_{I1}(k)+\mathrm{j}X_{I2}(k),\\\sum_m^{N-1}x\ (m)\sin A=X_{I1}(k)+\mathrm{i}(-X_R(k))+\mathrm{j}0,\end{cases}\tag{21}$$

代入式(20)整理得

$$X_d(k)=\big[X_R(k)\cos B+X_{I1}(k)\sin B\big]+\mathrm{i}\big[X_{I1}(k)\cos B-X_R(k)\sin B\big]+\mathrm{j}X_{I2}(k),\tag{22}$$

即式(16)。

性质4(调制性质)　时域调制信号$x_m(n)=x(n)\mathrm{cas}\left(\frac{2\pi nk_0}{N}\right)$的THT为

$$X_m(k)=X_R(k-k_0)+X_{I1}(k+k_0)+\mathrm{i}\big[X_{I1}(k-k_0)-X_R(k+k_0)\big]+\mathrm{j}X_{I2}(k-k_0)。\tag{23}$$

证明 由定义2可得

$$X_m(k)=\sum_{n=0}^{N-1}x_m(n)\mathrm{cas}\left(\frac{2\pi nk}{N}\right)=\sum_{n=0}^{N-1}x(n)\mathrm{cas}\left(\frac{2\pi nk_0}{N}\right)\mathrm{cas}\left(\frac{2\pi nk}{N}\right)。\tag{24}$$

应用乘积恒等式

$$\mathrm{cas}(A)\mathrm{cas}(B)=\cos(A-B)+\sin(A+B),\tag{25}$$

式中$A=\frac{2\pi nk_0}{N}$, $B=\frac{2\pi nk}{N}$,可得

$$X_m(k)=\sum_{n=0}^{N-1}x(n)\left[\cos\left(\frac{2\pi n(k-k_0)}{N}\right)+\sin\left(\frac{2\pi n(k+k_0)}{N}\right)\right]。\tag{26}$$

由性质2和定义2可得第1项计算为

$$\sum_{n=0}^{N-1}x(n)\cos\left(\frac{2\pi n(k-k_0)}{N}\right)=X_R(k-k_0)+\mathrm{i}X_{I1}(k-k_0)+\mathrm{j}X_{I2}(k-k_0),\tag{27}$$

第2项计算为

$$\sum_{n=0}^{N-1}x(n)\sin\left(\frac{2\pi n(k+k_0)}{N}\right)=X_{I1}(k+k_0)-\mathrm{i}X_R(k+k_0),\tag{28}$$

将2项相加并分离实部、虚部1、虚部2,可得

$$X_m(k)=\left[X_R(k-k_0)+X_{I1}(k+k_0)\right]+\mathrm{i}\left[X_{I1}(k-k_0)-X_R(k+k_0)\right]+\mathrm{j}X_{I2}(k-k_0),\tag{29}$$

此即式(23)。

性质5(卷积定理) 假设三元数信号$x(n)$与$h(n)$的循环卷积为

$$(x*h)(n)=\sum_{m=0}^{N-1}x(m)h((n-m)\bmod N),$$

其THT为

$$\begin{aligned}\mathcal{T}\{(x*h)(n)\}=&[X_R(k)H_R(k)-X_{I1}(k)H_{I1}(k)]+\\&\mathrm{i}[X_R(k)H_{I1}(k)+X_{I1}(k)H_R(k)]+\\&\mathrm{j}[X_{I2}(k)H_R(k)+X_R(k)H_{I2}(k)-\\&X_{I1}(k)H_{I2}(k)+X_{I2}(k)H_{I1}(k)],\end{aligned}\tag{30}$$

式中$H(k)=H_R(k)+\mathrm{i}H_{I1}(k)+\mathrm{j}H_{I2}(k)$是$h(n)$的THT。

证明 循环卷积的THT为

$$Y(k)=\mathcal{T}\{(x*h)(n)\}=\sum_{n=0}^{N-1}(x*h)(n)\mathrm{cas}\left(\frac{2\pi nk}{N}\right)=\sum_{n=0}^{N-1}\sum_{m=0}^{M-1}x(m)h((n-m)\bmod N)\mathrm{cas}\left(\frac{2\pi nk}{N}\right),\tag{31}$$

交换求和次序(令$l=n-m$),可得

$$Y(k)=\sum_m x(m)\sum_l h(l)\mathrm{cas}\left(\frac{2\pi(l+m)k}{N}\right),\tag{32}$$

其中内层求和为移位信号的THT

$$\sum_l h(l)\mathrm{cas}\left(\frac{2\pi(l+m)k}{N}\right)=[H_R\cos\theta_m+H_{I1}\sin\theta_m]+\mathrm{i}[H_{I1}\cos\theta_m-H_R\sin\theta_m]+\mathrm{j}H_{I2},\tag{33}$$

式中$\theta_m=\frac{2\pi mk}{N}$。代入式(32)得

$$Y(k)=\sum_m x(m)H_m(k)。\tag{34}$$

将$x(m)=x_0(m)+\mathrm{i}x_1(m)+\mathrm{j}x_2(m)$和$H_m(k)$展开,由式(2)逐项计算三元数乘法

$$x(m)H_m(k)=\begin{bmatrix}x_0A-x_1B-x_2H_{I2}\\+\mathrm{i}(x_0B+x_1A)\\+\mathrm{j}(x_0H_{I2}+x_2A)\end{bmatrix},\tag{35}$$

式中$A=H_R\cos\theta_m+H_{I1}\sin\theta_m$, $B=H_{I1}\cos\theta_m-H_R\sin\theta_m$。对$m$求和后,由性质2可得

$$\begin{cases}\sum_m x_0\cos\theta_m=X_R(k),\ \sum_m x_0\sin\theta_m=X_{I1}(k),\\ \sum_m x_1\cos\theta_m=X_{I1}(k),\ \sum_m x_1\sin\theta_m=-X_R(k),\\ \sum_m x_2\cos\theta_m=X_{I2}(k),\ \sum_m x_2\sin\theta_m=X_{I2}(k),\end{cases}\tag{36}$$

代入整理即得式(30)。

性质6(Parseval定理) 信号$x(n)$及其THT$X(k)$遵循能量守恒定律

$$\sum_{n=0}^{N-1}|x(n)|^2=\frac{1}{N}\sum_{k=0}^{N-1}|X(k)|^2。\tag{37}$$

证明 由模定义和信号分解可得

$$|x(n)|^2=x_0^2(n)+x_1^2(n)+x_2^2(n),\tag{38}$$

根据实信号离散哈特莱变换的Parseval定理

$$\begin{cases}\sum_{n=0}^{N-1}x_0^2(n)=\frac{1}{N}\sum_{k=0}^{N-1}X_R^2(k),\\ \sum_{n=0}^{N-1}x_1^2(n)=\frac{1}{N}\sum_{k=0}^{N-1}X_{I1}^2(k),\\ \sum_{n=0}^{N-1}x_2^2(n)=\frac{1}{N}\sum_{k=0}^{N-1}X_{I2}^2(k),\end{cases}\tag{39}$$

3个公式相加,可得

$$\sum_{n=0}^{N-1}\left(x_0^2(n)+x_1^2(n)+x_2^2(n)\right)=\frac{1}{N}\sum_{k=0}^{N-1}\left(X_R^2(k)+X_{I1}^2(k)+X_{I2}^2(k)\right)。\tag{40}$$

由性质2代入得

$$\sum_{n=0}^{N-1}|x(n)|^2=\frac{1}{N}\sum_{k=0}^{N-1}|X(k)|^2,\tag{41}$$

即式(37)。

3　THT的快速算法

本节基于FFT给出THT的快速算法,并分析其计算复杂度。

引理1　设实信号$x(n)$的傅里叶变换为$F(k)=F_R(k)+\mathrm{j}F_I(k)$,则其离散哈特莱变换$X(k)$与其傅里叶变换$F(k)$之间的关系为

$$X(k)=F_R(k)-F_I(k)。\tag{42}$$

证明　由离散傅里叶变换定义可知

$$F(k)=\sum_{n=0}^{N-1}x(n)\mathrm{e}^{-\mathrm{j}2\pi kn/N},\tag{43}$$

利用欧拉公式$\mathrm{e}^{-\mathrm{j}\theta}=\cos\theta-\mathrm{j}\sin\theta$展开

$$F(k)=\sum_{n=0}^{N-1}x(n)\left[\cos\left(\frac{2\pi kn}{N}\right)-\mathrm{j}\sin\left(\frac{2\pi kn}{N}\right)\right]。\tag{44}$$

分离实部与虚部

$$F_R(k)=\sum_{n=0}^{N-1}x(n)\cos\theta_{kn},\quad F_I(k)=-\sum_{n=0}^{N-1}x(n)\sin\theta_{kn},\tag{45}$$

式中$\theta_{kn}=\dfrac{2\pi kn}{N}$。由哈特莱变换定义可得

$$X(k)=\sum_{n=0}^{N-1}x(n)\mathrm{cas}(\theta_{kn})=\sum_{n=0}^{N-1}x(n)\left[\cos\theta_{kn}+\sin\theta_{kn}\right]=F_R(k)-F_I(k)。\tag{46}$$

定理1　设$x(n)=x_0(n)+\mathrm{i}x_1(n)+\mathrm{j}x_2(n)$为三元数信号,其THT为

$$X(k)=X_R(k)+\mathrm{i}X_{I1}(k)+\mathrm{j}X_{I2}(k)。\tag{47}$$

与此同时,信号的3个实分量$x_p(n),p=0,1,2$的傅里叶变换分别为$F_p(k)$,则THT的3个分量的计算式为:

$$\begin{cases}X_R(k)=\mathrm{Re}(F_0(k))-\mathrm{Im}(F_0(k)),\\ X_{I1}(k)=\mathrm{Re}(F_1(k))-\mathrm{Im}(F_1(k)),\\ X_{I2}(k)=\mathrm{Re}(F_2(k))-\mathrm{Im}(F_2(k))。\end{cases}\tag{48}$$

考虑到傅里叶变换具有FFT快速算法,因此在实际计算过程中,可基于傅里叶变换与THT之间的关系,利用FFT计算THT。具体方法为:首先,对三元数信号的3个实分量分别进行FFT,得到相应的傅里叶变换结果;其次,依据式(48)将各分量的频谱合成为THT的3个分量;最后,将这些分量组合为完整的THT结果。

在计算复杂度方面,假设信号$x(n)$长度为$N=2^s$,式(48)3次FFT所需的复数乘法次数为$\dfrac{3N}{2}\log_2N$,相当于$6N\log_2N$次实数乘法,复数加法次数为$3N\log_2N$,相当于$6N\log_2N$次实数加法。此外,式(47)所描述的线性组合操作还需进行$3N$次实数。综上所述,本文算法的总体乘法复杂度为$6N\log_2N$,加法复杂度为$6N\log_2N+3N$。

注意到,对R、G、B通道分别进行传统哈特莱变换的传统方法也需进行3次FFT运算(分别利用FFT求取三通道的哈特莱变换)。因此,本文所提方法的计算复杂度与传统方法相当。但所提方法能够利用三元数理论实现彩色图像的整体化处理,保留了通道间的关联性,因而能够在彩色图像加密中提供更优的性能。

4　基于THT的图像加密方法

4.1　图像加密

本文所提的基于THT的图像加密系统流程如图1所示,具体步骤如下。

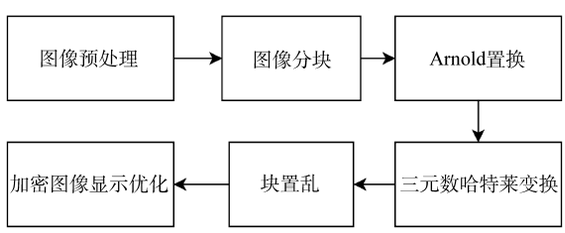


图1　加密流程

Figure 1　flowchart of the encryption process

(1)读取原始图像,将其大小调整为250×250像素;把该图像均匀分割为4个125×125像素的子块,分别为左上、右上、左下、右下子块,为后续的加密处理做准备。

(2)针对分割后的每个子块,进行分块加密(Arnold变换和THT)操作。

(a)空间域置乱,对每个子块分别进行Arnold变换,并利用3次标准Arnold猫映射$(x,y)\to(x+y,x+2y)$打乱像素位置(实验表明,少于3次迭代时置乱不充分,部分图像结构可能保留,而多于3次迭代时计算开销显著增加,而图像安全性提升有限)。

(b)颜色空间变换,首先将彩色RGB图像转换为三元数形式,并进行三元数旋转变换,以增强颜色分量间的耦合性。在像素值处理方面:先进行归一化,pixel/255;接下来,采用幂次变换进行非线性映射,映射方式为$p^{\frac{1}{s}}$,式中p表示归一化后的像素

值,s为加密密钥参数,由$s = 0.97 + 0.03 \times rand(\cdot)$生成,该幂次变换可有效改变像素值的统计分布,增强加密系统的非线性特性;最后对变换结果进行范围调整,恢复至标准像素值范围。

(c)频域变换中,基于子块的R、G、B通道构建三元数,对其进行二维THT并提取变换后的R、G、B分量。

(3)块置乱与重组,生成随机的置乱序列$\mathrm{perm}_{\mathrm{order}}$,依据该序列对经过加密处理的4个子块进行重新排列。完成置乱后,将4个子块再次组合,形成一幅完整的加密图像。

(4)加密图像显示效果优化。首先抑制其频谱中心的直流分量,减少低频信号的影响;然后对频谱进行对数增强,拓宽图像灰度级的动态范围;最后采用自适应直方图均衡技术,让图像的对比度得到进一步增强,使类噪声加密图像看起来更清晰、对比更分明。

4.2 图像解密

图像解密系统流程图如图2所示,具体步骤如下。

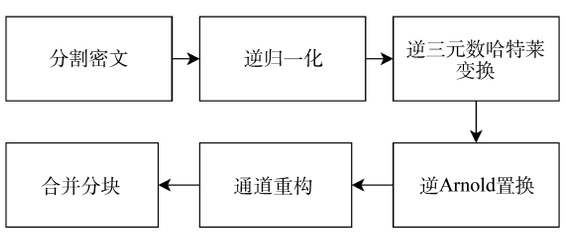


图2 解密流程

Figure 2 flowchart of the decryption process

(1)加密块解密过程。解密过程中使用的密钥包括Arnold变换的迭代次数、幂次变换的指数γ、置乱序列S等。所有参数需与加密过程一致方可正确解密。首先对每个加密块进行解密操作,在定位原始块时,通过使用之前用于置乱的$\mathrm{perm}_{\mathrm{order}}$序列,精准找到当前加密块在原始图像中对应的位置;其次进行逆THT,先依据提取的R、G、B分量构建三元数,应用逆THT操作,提取R、G、B分量;随后是逆非线性变换环节,先将像素值通过除以$\mathrm{secret}_{\mathrm{scale}}$进行范围还原;再次利用逆幂次变换$p^{1/s}$恢复像素值,通过乘以255进行反归一化;最后是逆Arnold置换,对每个通道分别进行3次逆Arnold变换,使用逆映射$(x, y) \rightarrow (2xy, x + y)$恢复图像的原始空间位置。

(2)解密图像重构。将经过上述解密步骤后的各个块,按照原始位置重新进行组合。为了消除可能存在的块边界效应,对重组后的图像应用轻微的高斯滤波,设置滤波参数σ为0.8,使图像更加平滑自然。

(3)解密图像质量评估。为衡量解密图像的质量,采用峰值信噪比(peak signal-to-noise ratio,PSNR)和结构相似性指数(structural similarity index measure,SSIM)这2个指标。计算PSNR评估图像的失真程度,数值越高表示图像失真越小;计算SSIM评估图像的结构相似性,数值越接近1表示图像结构与原始图像越相似。

5 实验结果

本节选用标准测试图像库中的叶片、辣椒、足球和花朵作为测试图像,对所提方法进行验证。具体测试内容包括加密图像视觉效果、指标特性、噪声攻击、统计直方图以及信息熵分析。

5.1 视觉效果

原始图像以及加密、解密结果如图3所示。通过加密操作,原始图像的像素关联性显著降低,内容被隐藏,呈现类噪声的无序纹理;解密结果借助密钥逆向还原,与原始图像视觉一致性高,能精准复现原图细节,验证了所提方法在隐藏与恢复图像信息上的有效性,满足图像保密传输与存储需求。

5.2 指标特性

表1展示了图像解密后的PSNR和SSIM指标。其中:PSNR反映图像失真程度,4组图像平均值均>35dB,说明解密图像与原始图像能量差异小;SSIM衡量结构匹配度,平均值均>0.96,表明解密图像保留了原始图像的纹理与结构特征。2类指标说明加密、解密过程对图像信息的损伤处于低水平,满足实用化的质量要求,验证了算法在还原图像质量上的可靠性。

5.3 噪声攻击检测

为验证加密算法的鲁棒性,对加密图像施加方差为0.05的高斯噪声攻击,并测试解密效果。图4展示了加噪后的加密图像与解密图像,尽管加密图像受噪声污染,解密后仍能有效恢复原始图像的主体内容与纹理特征,表明所提方法在高斯噪声攻击下具备良好的鲁棒性,可保障图像信息的可靠还原。

5.4 统计直方图

以叶片图为例,原始图像和加密图像的统计直方图如图5所示。从每幅原始图像的统计直方图中

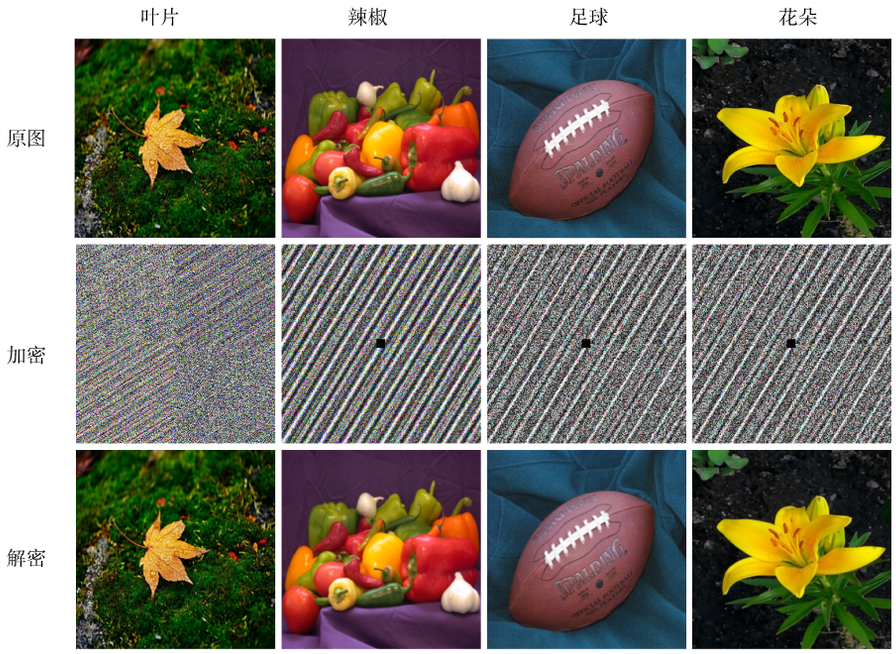


图3　不同图像加密、解密效果展示

Figure 3　display of encryption and decryption effects for different images

表1　不同图像指标

Table 1　different feature indicators

指标	叶片				辣椒				足球				花朵			
	R	G	B	平均	R	G	B	平均	R	G	B	平均	R	G	B	平均
PSNR	34.48	34.70	37.16	35.45	42.19	42.49	43.09	42.59	38.93	38.90	38.89	38.91	37.72	37.62	39.77	38.37
SSIM	0.98	0.98	0.97	0.98	0.99	0.99	0.99	0.99	0.97	0.97	0.99	0.97	0.98	0.98	0.98	0.98

注:PSNR为峰值信噪比;SSIM为结构相似性指数;R、G、B分别为红色、绿色、蓝色通道。

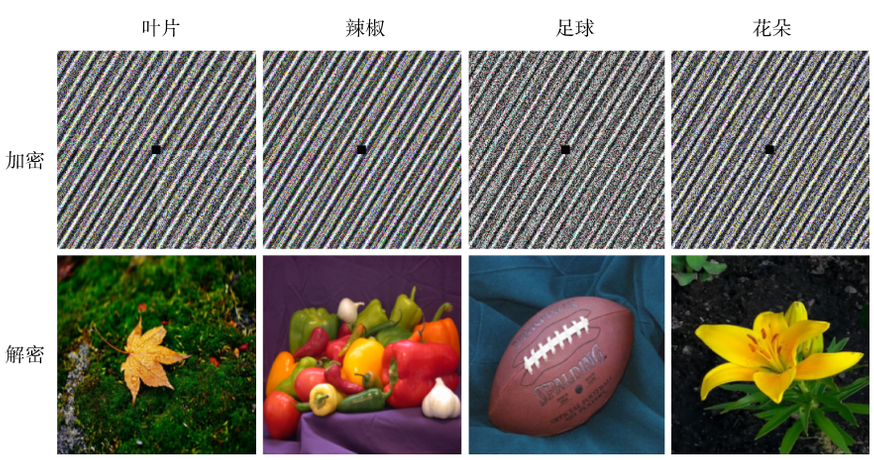


图4　受方差为0.05的高斯噪声攻击后的图像

Figure 4　encrypted and decrypted images after Gaussian noise attack with variance 0.05

可以看到,像素值之间存在明显的分布特征。而加密图像的统计直方图则呈现出较为均匀的分布,这表明加密算法有效地破坏了原始图像的统计特性,从而增强了抗统计分析攻击的能力。

6　结束语

本文系统研究了THT理论及其在彩色图像加密中的应用。具体而言,本文定义了THT,并推导

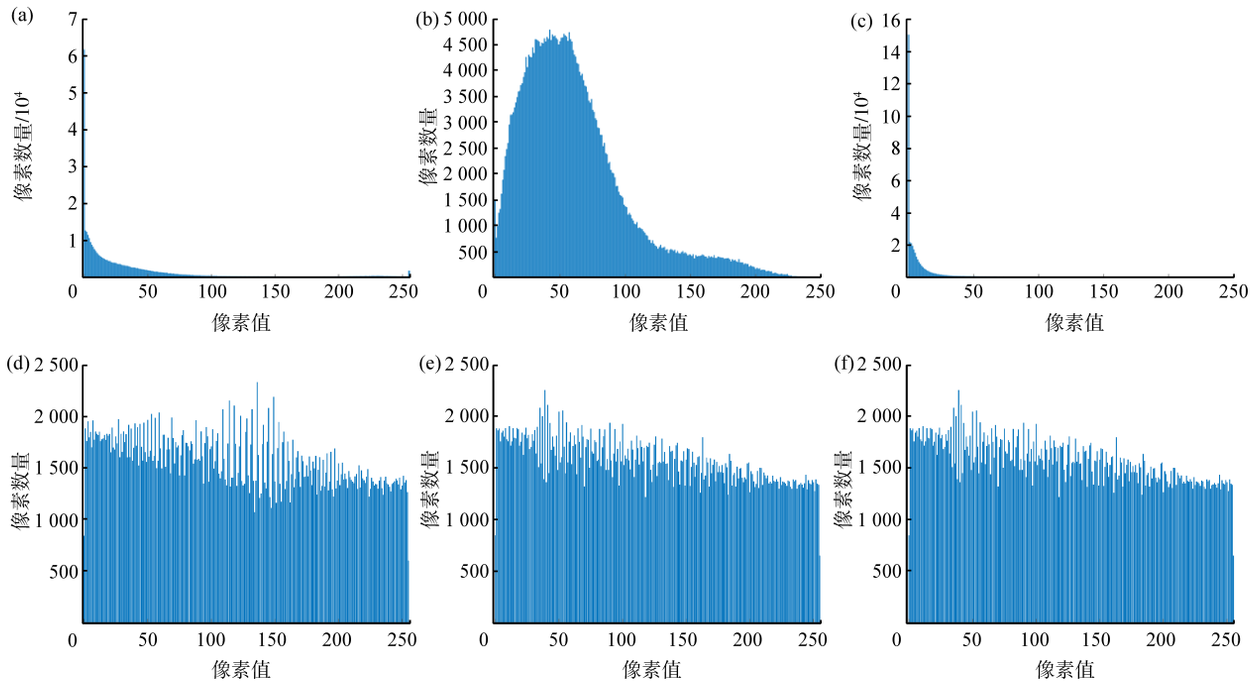


图5　原始图像和加密图像的统计直方图

(a~c)红色、绿色、蓝色原始图像;(d~f)红色、绿色、蓝色加密图像

Figure 5　statistical histograms of plaintext images and ciphertext images

(a-c)plaintext images of red, green and blue; (d-f)ciphertext images of red, green and blue

了其所满足的常用性质。此外,提出了THT的快速算法,该算法可基于所提变换与傅里叶变换之间的关系,利用FFT实现快速计算。最后,基于THT提出了适用于彩色RGB图像的加密和解密方法。实验结果体现了良好的性能,验证了所提方法的有效性。

©The editorial department of Journal of Capital Normal University (Natural Science Edition) 2025. This is an open access article under the CC BY-NC-ND 4.0 license (https://creativecommons.org/licenses/by-nc-nd/4.0/).

参 考 文 献

[1] Yan S H, Zhang J D, Lu R. Multistability discrete chaotic map and its application of image encryption[J]. Physica Scripta, 2025, 100(8): 085207. DOI: 10.1088/1402-4896/adee66.

[2] Ramar R, Sambas A, Kaçar S, et al. Design of new chaotic system with hyperbolic sine function based on pseudo-random number generation for medical image encryption [J]. Journal of Nonlinear Mathematical Physics, 2025, 32(1): 52. DOI: 10.1007/s44198-025-00308-2.

[3] Nabil H, Tayeb H. Fractional-order supply chain finance system with conformable derivative: Chaotic dynamics, complexity analysis, and RGB color image encryption [J]. Journal of Computational and Applied Mathematics, 2026, 476: 117105. DOI: 10.1016/j.cam.2025.117105.

[4] Zhao C F, Zhai Z B, Zeng B. Delayed chaotic image encryption algorithm using cross-layer and DNA coding techniques[J]. Computer Standards & Interfaces, 2025, 93: 103974. DOI: 10.1016/j.csi.2025.103974.

[5] Yan X P, Hu Q, Teng L. A novel color image encryption method based on new three-dimensional chaotic mapping and DNA coding [J]. Nonlinear Dynamics, 2025, 113(2): 1799-1826. DOI: 10.1007/s11071-024-10277-8.

[6] Feng S J, Zhao M C, Liu Z B, et al. A novel image encryption algorithm based on new one-dimensional chaos and DNA coding [J]. Multimedia Tools and Applications, 2024, 83(36): 84275-84297. DOI: 10.1007/s11042-024-19090-2.

[7] Lang J, Zhang F. Optical image encryption based on 3D double-phase encoding algorithm in the gyrator transform domain[J]. Multimedia Tools and Applications, 2024, 83(38): 85963-85985. DOI: 10.1007/s11042-024-20176-0.

[8] Rao S K, Nishchal N K, AlFalou A. Optical asymmetric image encryption using vectorial light field encoding[J].

Optics Communications, 2024, 554: 130097. DOI: 10.1016/j.optcom.2023.130097.

[9] Zhou Q M, Wang X G, Jin M X, et al. Optical image encryption based on two-channel detection and deep learning[J]. Optics and Lasers in Engineering, 2023, 162:107415. DOI:10.1016/j.optlaseng.2022.107415.

[10] Liu Y J, Sham W C, Zhang F Q, et al. Visually meaningful asymmetric image encryption based on a random devil's Vortex phase mask in the gyrator transform domain[J]. Optics and Lasers in Engineering, 2025, 194: 109121. DOI: 10.1016/j. optlaseng. 2025.109121.

[11] Singh H. Double-phase image encryption using interference concept, devil's fractional Vortex Fresnel lens phase masks, and the gyrator transform[J]. Optik, 2025,327:172289. DOI:10.1016/j.ijleo.2025.172289.

[12] Yadav A K, Singh P, Saini I, et al. Asymmetric encryption algorithm for colour images based on fractional Hartley transform [J]. Journal of Modern Optics, 2019, 66(6): 629-642. DOI: 10.1080/09500340. 2018.1559951.

[13] Abdul-Kareem A A, Al-Jawher W A M. An image encryption algorithm using hybrid sea lion optimization and chaos theory in the hartley domain[J]. International Journal of Computers and Applications, 2024, 46(5): 324-337. DOI:10.1080/1206212X.2024.2313300.

[14] Polyakova M, Cariow A, Sklyar J. Fast algorithms for short-length odd-time and odd-frequency discrete hartley transforms [J]. Electronics, 2025, 14 (5): 996. DOI: 10.3390/electronics14050996.

[15] Wang X, Shao Z H, Li B C, et al. Color image encryption based on discrete trinion Fourier transform and compressive sensing [J]. Multimedia Tools and Applications, 2024, 83 (26): 67701-67722. DOI: 10. 1007/s11042-024-18184-1.

[16] Shao Z H, Wang X, Tang Y D, et al. Trinion discrete cosine transform with application to color image encryption [J]. Multimedia Tools and Applications, 2023, 82(10): 14633-14659. DOI: 10.1007/s11042-022-13898-6.

[17] El-Khanchouli K, Joudar N E, Sayyouri M. Proposal of a novel quaternionic integer reversible Racah transform and a hyperchaotic system for secure encryption of colored medical images [J]. Expert Systems with Applications, 2025, 287: 128024. DOI: 10.1016/j. eswa. 2025.128024.

[18] Li X Y, Song C Q. QGI algorithm for solving quaternion equation arising in image encryption[J]. Mathematical Methods in the Applied Sciences, 2025, 48(12): 12514-12527. DOI:10.1002/mma.11042.

[19] Li X Y, Song C Q, Liu H J. QMGI algorithm for solving quaternion equation and its application in color image encryption [J]. Numerical Algorithms, 2025, 99 (3): 1429-1462. DOI:10.1007/s11075-024-01920-x.

[20] El-khanchouli K, Mansouri H, Bencherqui A, et al. Proposed quaternion fractional dual-Hahn moments for color image reconstruction and encryption [J]. Knowledge-Based Systems, 2025, 329: 114467. DOI: 10.1016/j.knosys.2025.114467.

(责任编辑:马田田)