# 基于高维张量奇异值分解的图像加密

李 勇[1],荀显超[2],王青竹[3]

(1. 吉林工程技术师范学院 信息工程学院,吉林 长春 130052;2. 空军航空大学 飞行基础训练基地基础部,吉林 长春;3. 东北电力大学 信息工程学院,吉林 吉林 132012)

**摘 要**:现有基于奇异值分解(SVD)的彩色信息加密系统提供了一种光学矩阵分解方案、安全的密文和敏感的密钥。高维张量奇异值分解(HOSVD)是 SVD 矩阵的自然线性延伸,提出了一种基于 HOSVD 的彩色图像加密算法。在加密过程中,HOSVD 比 SVD 提供了更多的密文乘法组合次序。这些乘法组合次序可以有效地增加未经授权的解密难度。在解密过程中,HOSVD 的重建精度比 SVD 更高。这些优点提高了准确性、安全性和鲁棒性。通过对 100 个图像测试数据集的计算机仿真验证了该算法的可行性。

**关键词**:高阶奇异值分解; 三维矩阵; GT 变换

**中图分类号**:TP309.7 **文献标志码**:A **文章编号**:1007-2276(2014)S-0243-05

# Image encryption based on higher-order singular value decomposition

Li Yong[1], Xun Xianchao[2], Wang Qingzhu[3]

(1. College of Information Engineering, Jilin Teathers' Institute of Engineering & Technology, Changchun 130052, China;
2. Basic Department of Basic Flight Traiming Base, Air Force Aviation University, Changchun 130022, China;
3. School of Information Engineering, Northeast Dianli University, Jilin 132012, China)

**Abstract**: The existing Singular Value Decomposition (SVD) based color information encryption system provided an optical matrix composition scheme, secure ciphertexts and very sensitive keys. As the Higher-order SVD (HOSVD) is a natural multi-linear extension of the matrix SVD, an HOSVD based color image encryption algorithm was proposed. In the encryption procedure, HOSVD can generate more multiplication orders of the ciphertexts (decomposition parts) than what SVD provides. These multiplication orders can be used as effective keys to make unauthorized decryption harder. In the decryption procedure, the reconstruction accuracy of HOSVD is higher than that of SVD. These advantages enhance the accuracy, security and robustness. Numerical simulations based on a test dataset of 100 images support the viability of the proposed algorithm.

**Key words**: higher-order dingular value decomposition; three dimensional matrix; gyrator transform

**收稿日期**:2014-04-26; **修订日期**:2014-04-15

**基金项目**:国家自然科学基金(61301257);吉林省科技发展计划(201201107)

**作者简介**:李勇(1970-),女,副教授,博士,主要从事数字图像处理方面的研究。Email:liyong8113@sina.com

## 0 引 言

光学加密技术因其提供的高速并行的不同维度(例如多自由度[1-2])而引起了人们的关注和显著的兴趣。其中一个重要的光学加密方法被称为“双随机相位编码(DRPE)”,即用随机相位扩散器将在输入和傅里叶域内的图像相乘[3]。随着该技术的应用,其他光学加密方法也相应提出[4-8]。

近年来,提出了一种基于奇异值分解(SVD)和 Arnold 变换的图像加密新算法[9]:原始图像首先通过分数傅里叶变换,然后通过 SVD 分解成三段。分数傅里叶变换(FFT)和它的扩展已经被研究并应用到光学信息处理中[10-13],这种变换属于一种线性标准变换(LCT),其中二次相位调制被加入到傅里叶域的光学实现系统中[14]。回转变换(GT)也是在图像处理领域研究的一种 LCT[15-16],与 FRT 不同的是,在 GT 的数学表达式中有 4 个交叉相位因子[17]。进一步,基于 SVD 和 GT 的彩色图像加密方法被提出[18-19],该系统具有以下优点:(1) 包括了 3 个非对称的加密密钥;(2) 提供了非常高的灵敏度参数,其中包括 GT 变换的角度、SVD 的 U、S、V 部分;(3) 对于任意错误的密钥,所有参数的均方误差(MSE)值都很高。

作为矩阵 SVD 的天然多线性延伸,高阶张量奇异值分解(HOSVD)更适合于较高的三维图像(等于或大于三维)[20-21]。虽然 HOSVD 已经应用于图像降噪、水印、复原和压缩中[22-27],但到目前为止它并没有应用于彩色图像(三维图像)加密中。为了得到彩色图像加密系统的良好性能,文中提出了 HOSVD 方案及其框架。对于彩色图像的加密,HOSVD 相对 SVD 的主要优点如下:(1) HOSVD 可以生成更多的密文(分解部份)的乘法组合次序,正确组合次序可以用作一个有效的密钥,使未经授权的解密难度增加;(2) 基于 HOSVD 算法的解密误差比基于 SVD 算法小。

## 1 HOSVD 理论

为了便于区分标量、向量、矩阵和高维张量,文中用不同形式区分标量、一维向量、二维矩阵和三维张量(三维矩阵)。白体表示标量,如 $a$;小写黑体表示一维向量,如 $\mathbf{a}$;大写黑体表示二维矩阵,如 $\mathbf{A}$;花体表示三维张量,如 $\boldsymbol{\mathcal{A}}$。高维张量的展开模型是 HOSVD 的一个重要步骤。一个张量的矩阵展开也就是张量的矩阵表示,所有的列(或行)向量被逐次堆叠。对于三维张量 $\mathbf{I}_1\times\mathbf{I}_2\times\mathbf{I}_3$,其三维展开如图 1 所示,自上而下分别是 1 模式、2 模式和 3 模式的展开。

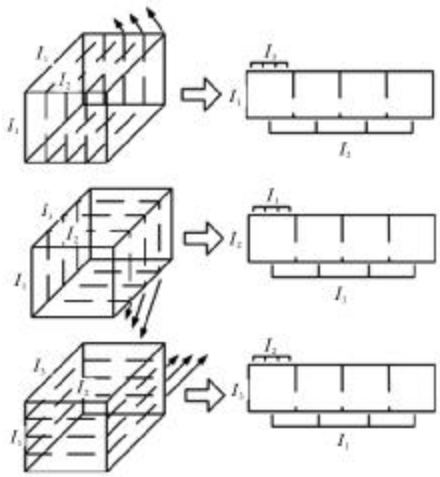


图 1 三维张量展开

Fig.1 Unfolding of 3D tensor

对于一个三维张量,其 HOSVD 分解与重建为:

$$\begin{cases}\boldsymbol{\mathcal{S}}=\boldsymbol{\mathcal{A}}\times_1\mathbf{U}^{(1)\mathrm{T}}\times_2\mathbf{U}^{(2)\mathrm{T}}\times_3\mathbf{U}^{(3)\mathrm{T}}\\ \boldsymbol{\mathcal{A}}=\boldsymbol{\mathcal{S}}\times_1\mathbf{U}^{(1)}\times_2\mathbf{U}^{(2)}\times_3\mathbf{U}^{(3)}\end{cases}\tag{1}$$

式中:$\boldsymbol{\mathcal{S}}$ 为奇异值张量;$\times_k$ 为 $k$ 模式乘法。通常情况下,公式(1)由公式(2)实现:

$$\begin{cases}\mathbf{S}_{(k)}=\mathbf{U}^{(k)\mathrm{T}}\cdot\mathbf{A}_{(k)}\cdot(\mathbf{U}^{(k+1)}\otimes\mathbf{U}^{(k+2)}\cdots\mathbf{U}^{(N)}\otimes\mathbf{U}^{(1)}\otimes\mathbf{U}^{(2)}\cdots\otimes\mathbf{U}^{(k-1)})\\ \mathbf{A}_{(k)}=\mathbf{U}^{(k)}\cdot\mathbf{S}_{(k)}\cdot(\mathbf{U}^{(k+1)}\otimes\mathbf{U}^{(k+2)}\cdots\mathbf{U}^{(N)}\otimes\mathbf{U}^{(1)}\otimes\mathbf{U}^{(2)}\cdots\otimes\mathbf{U}^{(k-1)})^{\mathrm{T}}\end{cases}\tag{2}$$

式中:$\mathbf{A}_{(k)}$ 为 $\boldsymbol{\mathcal{A}}$ $(k=1,2,3)$ 的第 $k$ 种展开模式;$\mathbf{U}^{(k)}$ 为其酉矩阵;$N$ 表示张量的维数;$\otimes$ 表示张量乘法(Kronecker 乘法)。上述所有参数在参考文献[20-21]中进行了详细的介绍,此处不再赘述。

## 2 提出的算法

文中提出的彩色图像加密方法是基于 GT 域内的 HOSVD 变换。

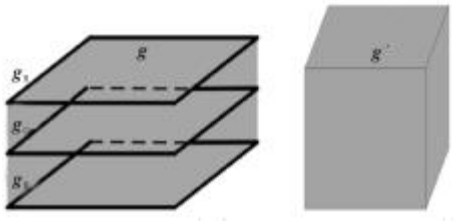
### 2.1 加 密

对于彩色图像 $\boldsymbol{\mathcal{A}}$,它的 3 个信道 $\mathbf{A}_R(x_i,y_i)$,$\mathbf{A}_G(x_i,$

$y_i)$,$A_B(x_i,y_i)$和随机相位掩模 $\exp[j\Phi_R(x_i,y_i)]$,$\exp[j\Phi_G(x_i,y_i)]$,$\exp[j\Phi_B(x_i,y_i)]$相乘,相应的随机图像经过 GT 变换,其变换角度分别为 $\alpha_R$,$\alpha_G$,$\alpha_B$。

$$\begin{cases} g_R(x_i,y_i)=\mathbf{G}^{\alpha_R}\{A_R(x_i,y_i)\exp[j\Phi_R(x_i,y_i)]\} \\ g_G(x_i,y_i)=\mathbf{G}^{\alpha_G}\{A_G x_i,y_i)\exp[j\Phi_G x_i,y_i)]\} \\ g_B(x_i,y_i)=\mathbf{G}^{\alpha_B}\{A_B(x_i,y_i)\exp[j\Phi_B(x_i,y_i)]\} \end{cases} \tag{3}$$

三维张量 g 是 $g_R$,$g_G$ 和 $g_B$ 的堆叠,如图 2(a)所示。因为 g 的长、宽、高维度不同,在解密过程中,各分解部分会因为维度特征而很容易地被区分。为了改善这个问题,g 首先变换成一个立方体三维张量 g′,如图 2(b)所示。



(a)　　(b)

图 2 三维张量变换

Fig.2 Transformation of 3D tensor

然后对张量 g′进行分解,公式(2)中的参数 $\mathbf{N}=3$,通过 g′三展开模式得到如下 3 个分解模型:

$$\begin{cases} g_{(1)}=U^{(1)}\cdot\mathbf{S}_{(1)}\cdot(U^{(2)}\otimes U^{(3)})^{\mathrm{T}} \\ g_{(2)}=U^{(2)}\cdot\mathbf{S}_{(2)}\cdot(U^{(3)}\otimes U^{(1)})^{\mathrm{T}} \\ g_{(3)}=U^{(3)}\cdot\mathbf{S}_{(3)}\cdot(U^{(1)}\otimes U^{(2)})^{\mathrm{T}} \end{cases} \tag{4}$$

展开模式 k 被用作一个附加的密钥。所有这些部分 $S_{(1)}$,$S_{(2)}$,$S_{(3)}$,$U^{(1)}$,$U^{(2)}$,$U^{(3)}$经过 GT 变换:

$$\begin{cases} \mathbf{E}_{s_{(k)}}(x_0,y_0)=\mathbf{G}^{\alpha_{s_{(k)}}}[S_{(k)}(x,y)] \\ \mathbf{E}_{U^{(k)}}(x_0,y_0)=\mathbf{G}^{\alpha_{U^{(k)}}}[U^{(k)}(x,y)] \end{cases} \tag{5}$$

式中:$\mathbf{E}_{s_{(1)}}$,$\mathbf{E}_{s_{(2)}}$,$\mathbf{E}_{s_{(3)}}$,$\mathbf{E}_{U^{(1)}}$,$\mathbf{E}_{U^{(2)}}$为密文。此外,由于它们具有相同维度而不能彼此识别。

### 2.2 解　密

在解密过程中,密文经过逆 GT 变换,分别为:

$$\begin{cases} \mathbf{D}_{s_{(k)}}(x,y)=\mathbf{G}^{-\alpha_{s_{(k)}}}[\mathbf{E}_{s_{(k)}}(x_0,y_0)] \\ \mathbf{D}_{U^{(k)}}(x,y)=\mathbf{G}^{-\alpha_{U^{(k)}}}[\mathbf{E}_{U^{(k)}}(x_0,y_0)] \end{cases} \tag{6}$$

然后 g′按公式(2)重建。g′的 3 种模式为:

$$\begin{cases} g_{(1)}=\mathbf{D}_{U^{(1)}}\cdot\mathbf{D}_S\cdot(\mathbf{D}_{U^{(2)}}\otimes\mathbf{D}_{U^{(3)}})^{\mathrm{T}} \\ g_{(2)}=\mathbf{D}_{U^{(2)}}\cdot\mathbf{D}_S\cdot(\mathbf{D}_{U^{(3)}}\otimes\mathbf{D}_{U^{(1)}})^{\mathrm{T}} \\ g_{(3)}=\mathbf{D}_{U^{(3)}}\cdot\mathbf{D}_S\cdot(\mathbf{D}_{U^{(1)}}\otimes\mathbf{D}_{U^{(2)}})^{\mathrm{T}} \end{cases} \tag{7}$$

最后,从 g′中恢复出 g。

## 3 计算机仿真结果

### 3.1 实验组

仿真实验使用 CPU 为 4 GB、RAM 为 2.8 GHz 的英特尔计算机和 Matlab R2011b。选择 10 幅彩色图像作为测试数据集。每种颜色的图像大小是 512×512×3。根据参考文献[18],GT 变换所用的变换角度如表 1 所示。

表1 所有参数的 GT 变换角度

Tab.1 Transformation angles of GT for all parameters

| | $\alpha_R$ | $\alpha_G$ | $\alpha_B$ | $\alpha_{S_{(1)}}$ | $\alpha_{S_{(2)}}$ | $\alpha_{S_{(3)}}$ | $\alpha_{U^{(1)}}$ | $\alpha_{U^{(2)}}$ | $\alpha_{U^{(3)}}$ |
|---|---|---|---|---|---|---|---|---|---|
| Angle/(°) | 0.45 | 0.55 | 0.65 | 0.10 | 0.20 | 0.30 | 0.40 | 0.50 | 0.60 |

### 3.2 结果与分析

基于 SVD 和 GT 的彩色信息验证系统的优点在参考文献[18]中进行了总结。HOSVD 相对 SVD 的优点陈述如下。

虽然 $\mathbf{D}_{s_{(k)}}$很容易与 $\mathbf{D}_{U^{(k)}}$区分,但密文仍然难以被解码,因为 $\mathbf{D}_{s_{(k)}}$有 3 种模式,所有 $\mathbf{D}_{s_{(k)}}$和 $\mathbf{D}_{U^{(k)}}$共有 18 种组合。公式(5)表明,只有 3 种组合是正确的,其他 15 种不正确的组合如下:

$$U^{(1)}\cdot\mathbf{S}_{(1)}\cdot(U^{(3)}\otimes U^{(2)})^{\mathrm{T}},\ U^{(2)}\cdot\mathbf{S}_{(1)}\cdot(U^{(1)}\otimes U^{(3)})^{\mathrm{T}},$$
$$U^{(2)}\cdot\mathbf{S}_{(1)}\cdot(U^{(3)}\otimes U^{(1)})^{\mathrm{T}},\ U^{(3)}\cdot\mathbf{S}_{(1)}\cdot(U^{(1)}\otimes U^{(2)})^{\mathrm{T}},$$
$$U^{(3)}\cdot\mathbf{S}_{(1)}\cdot(U^{(2)}\otimes U^{(1)})^{\mathrm{T}},\ U^{(1)}\cdot\mathbf{S}_{(2)}\cdot(U^{(2)}\otimes U^{(3)})^{\mathrm{T}},$$
$$U^{(1)}\cdot\mathbf{S}_{(2)}\cdot(U^{(3)}\otimes U^{(2)})^{\mathrm{T}},\ U^{(2)}\cdot\mathbf{S}_{(2)}\cdot(U^{(1)}\otimes U^{(3)})^{\mathrm{T}},$$
$$U^{(3)}\cdot\mathbf{S}_{(2)}\cdot(U^{(1)}\otimes U^{(2)})^{\mathrm{T}},\ U^{(3)}\cdot\mathbf{S}_{(2)}\cdot(U^{(2)}\otimes U^{(1)})^{\mathrm{T}},$$
$$U^{(1)}\cdot\mathbf{S}_{(3)}\cdot(U^{(2)}\otimes U^{(3)})^{\mathrm{T}},\ U^{(1)}\cdot\mathbf{S}_{(3)}\cdot(U^{(3)}\otimes U^{(2)})^{\mathrm{T}},$$
$$U^{(2)}\cdot\mathbf{S}_{(3)}\cdot(U^{(1)}\otimes U^{(3)})^{\mathrm{T}},\ U^{(2)}\cdot\mathbf{S}_{(3)}\cdot(U^{(3)}\otimes U^{(1)})^{\mathrm{T}},$$
$$U^{(3)}\cdot\mathbf{S}_{(3)}\cdot(U^{(2)}\otimes U^{(1)})^{\mathrm{T}}$$

通过均方误差(MSE)值[18]的计算来评估解码图像的质量。上述15 种组合的 MSE 如表 2 所示。

表 2 不正确组合的 MSE

Tab.2 MSE of incorrect combinations

| No. | Value | No. | Value | No. | Value |
|---|---|---|---|---|---|
| 1 | $7.371\,5\times10^{3}$ | 6 | $2.615\,1\times10^{4}$ | 11 | $2.612\,5\times10^{4}$ |
| 2 | $1.841\,3\times10^{4}$ | 7 | $2.638\,6\times10^{4}$ | 12 | $2.630\,8\times10^{4}$ |
| 3 | $1.852\,1\times10^{4}$ | 8 | $1.440\,6\times10^{4}$ | 13 | $1.410\,6\times10^{4}$ |
| 4 | $1.806\,0\times10^{4}$ | 9 | $1.472\,5\times10^{4}$ | 14 | $1.412\,2\times10^{4}$ |
| 5 | $1.807\,1\times10^{4}$ | 10 | $1.475\,6\times10^{4}$ | 15 | $1.442\,9\times10^{4}$ |

用对数曲线表示 HOSVD 和 SVD 的 MSE，如图 3 所示。图 3(a)为每一个测试图像的 MSE 原图，图 3(b)为(a)的局部放大图。100 个图像的平均 MSE 列于表 3。可以发现，无论选择哪一种展开模式，HOSVD 的解密错误都比 SVD 的小。

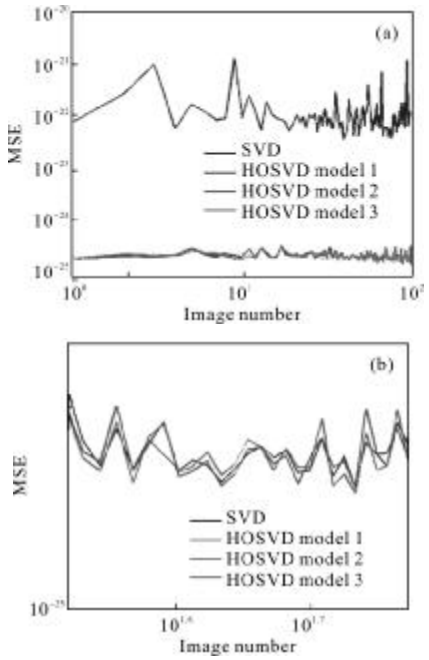



图 3 HOSVD 和SVD 的 MSE 对数曲线

Fig.3 MSE logistic curves of HOSVD and SVD

表 3 SVD 和 HOSVD 的 MSE

Tab.3 MSE of SVD and HOSVD

| | SVD | HOSVD mode 1 | HOSVD mode 2 | HOSVD mode 3 |
|---|---|---|---|---|
| MSE | $1.362\,7\times10^{-22}$ | $2.346\,8\times10^{-25}$ | $2.371\,1\times10^{-25}$ | $2.332\,1\times10^{-25}$ |

以一幅测试图像为例，如图 4(a)所示。$U^{(1)}$，$U^{(2)}$，$U^{(3)}$ 和 $S_{(1)}$部分的编码图像分别如图 4(b)~(e)所示。用一个错误密钥($U^{(1)}\cdot S_{(1)}\cdot(U^{(3)}\otimes U^{(2)})$)解码的图像如图 4(f)所示；用两个错误密钥($U^{(2)}\cdot S_{(1)}\cdot(U^{(1)}\otimes U^{(3)})$)解码的图像如图 4(g)所示；用三个错误密钥($U^{(2)}\cdot S_{(1)}\cdot(U^{(3)}\otimes U^{(1)})$)解码的图像如图 4(h)所示。用错误 S($U^{(1)}\cdot S\cdot(U^{(2)}\otimes U^{(3)})$)解码的图像如图 4(i)所示。用所有正确密钥解密的图像如图 4(j)所示。

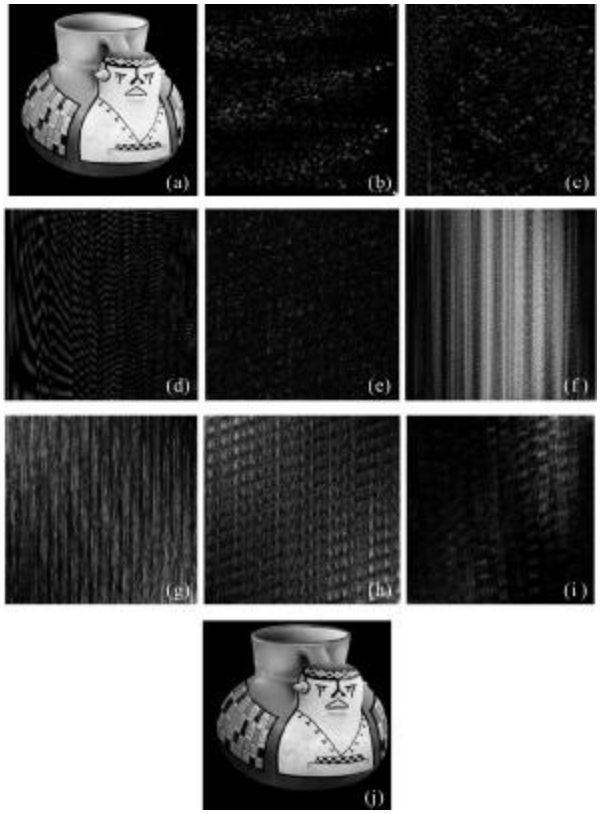



图 4 仿真结果

Fig.4 Simulation results

## 4 结 论

基于 HOSVD 的彩色图像加密算法是基于 SVD 的颜色信息验证系统在 GT 域的扩展[18-19]。此算法主要有两方面的改进：(1) 一种彩色图像 (三维张量) 有 3 种展开模式，并且每个展开模式包括 4 个分解部分。展开模式和乘法组合次序可以提供额外的密钥；(2) 对于彩色图像，HOSVD 的解密性能比 SVD 的更好。即用所有正确的密钥解密的 HOSVD 算法得到的 MSE 比 SVD 的要小得多。

然而，HOSVD 算法应用于对称密码系统中，即加密密钥和解密密钥相同。如何建立基于该算法的

非对称系统是今后工作的重点。

**参考文献:**


[1] Matoba O, Nomura T, Perez C E, et al. Optical techniques for information security [J]. Proceedings of IEEE, 2009, 97 (6): 1128-1148.

[2] Liu S, Guo C L, Sheridan J T. A review of optical image encryption techniques [J]. Optics and Laser Technology, 2014, 57: 327-342.

[3] Refregier P, Javidi B. Optical image encryption based on input plane and Fourier plane random encoding [J]. Optics Letters, 1995, 20(7): 767-769.

[4] Javidi B, Nomura T. Securing information by use of digital holography[J]. Optics Letters, 2000, 25(1): 28-30.

[5] Taajahuerce E, Javidi B. Encrypting three-dimensional information with digital holography [J]. Applied Optics, 2000, 39(35): 6595-6601.

[6] Haw J W, Park C S, Ryu D H. Optical image encryption based on XOR operations[J]. Optical Engineering, 1999, 38 (1): 47-54.

[7] Chen L F, Zhao D M. Optical color image encryption by wavelength multiplexing and lensless Fresnel transform holograms[J]. Optics Express, 2006, 14(19): 8552-8560.

[8] Unnikrishnan G, Joseph J, Singh K. Optics encryption by double-random phase encoding in the fractional Fourier domain[J]. Optics Letters, 2000, 25: 887-889.

[9] Chen L F, Zhao D M, Ge F. Image encryption based on singular value decomposition and arnold transform in fractional domain [J]. Optics Communications, 2013, 291: 98-103.

[10] Liu Z, Liu S. Random fractional Fourier transform[J]. Optics Letters, 2007, 32: 2088-2090.

[11] Hennelly B M, Sheridan J T. Generalizing, optimizing, and inventing numerical algorithms for the fractional Fourier, Fresnel, and linear canonical transforms [J]. Journal of the Optical Society of America A, 2005, 22(5): 917-927.

[12] Liu S, Sheridan J T. Optical encryption by combining image scrambling techniques in fractional fourier domains [J]. Optics Communications, 2013, 287(10): 73-80.

[13] Tao R, Lang J, Wang Y. Optical image encryption based on the multiple parameter fractional Fourier transform[J]. Optics Letters, 2008, 33: 581-583.

[14] Alieva T, Bastiaans J. Alternative representation of the linear canonical integral transform [J]. Optics Letters, 2005, 30 (24): 3302-3304.

[15] Rodrigo J A, Alieva T. Calvo M L. Applications of gyrator transform for image processing [J]. Optics Communications, 2007, 278(2): 279-284.

[16] Rodrigo J A, Alieva T, Calvo M L. Experimental implementation of the gyrator transform [J]. Journal of Optical Society of America A, 2007, 24(10): 3135-3139.

[17] Liu Z J, Chen D Z, Ma J P. Fast algorithm of discrete gyrator transform based on convolution operation [J]. Optik, 2011, 122: 864-867.

[18] Muhammad R A. An asymmetric color image cryptosystem based on schur decomposition in gyrator transform domain [J]. Optics and Lasers in Engineering, 2014, 58: 39-47.

[19] Muhammad R A. Color information verification system based on singular value decomposition in gyrator transform domains [J]. Optics and Lasers in Engineering, 2014, 57: 13-19.

[20] Lieven D L. A multilinear singular value decomposition[J]. Siam Journal on Matrix Analysis and Application, 2000, 21 (4): 1253-1278.

[21] Vannieuwenhoven N. A new truncation strategy for the higher-order singular value decomposition [J]. Siam Journal on Scientific Computing, 2012, 34(2): 1027-1052.

[22] Rajwade A, Rangarajan A, Banerjee A. Image denosing using the higher order singular value decomposition [J]. IEEE Transactions on Pattern Analysis and Machine Intelligence, 2013, 35(4): 849-862.

[23] Xiao H S, Wang Z L, Fan Z G. Optical distortion Evaluation of an aerodynamically heated window, based on the higher-order singular value decomposition with the influence of elasto-optical effect excluded [J]. Applied Optics, 2012, 51(16): 3269-3278.

[24] Jussi S, Andreas R, Visa K. Sequential unfolding SVD for tensors with applications in array signal processing[J]. IEEE Transactions on Signal Processing, 2009, 57(12): 4719-4733.

[25] Chen Y L, Hsu C T. Multilinear graph embedding: representation and regularization for images [J]. IEEE Transactions on Image Processing, 2014, 23(2): 741-754.

[26] Li Q, Shi X Q, Schonfeld D. Robust HOSVD-based higher-order data indexing and retrieval[J]. IEEE Signal Processing Letters, 2013, 20(10): 984-987.

[27] Fan D S, Meng X F, Wang Y R. Optical information encoding and image watermarking scheme based on phase-shifting interferometry and singular value decomposition[J]. Journal of Modern Optics, 2013, 60(9): 749-756.