引用格式：HAN Si-min, ZHANG Wei, ZHANG Xiang, *et al*. Multiple Image Encryption Method Based on Light Field Imaging Theory and Chaotic System[J]. *Acta Photonica Sinica*, 2020, **49**(3):0310002
韩思敏,张薇,张翔,等.基于光场成像原理和混沌系统的多图像加密方法[J].光子学报,2020,**49**(3):0310002

基于光场成像原理和混沌系统的多图像加密方法

韩思敏,张薇,张翔,韦晓孝,万新军
(上海理工大学 光电信息与计算机工程学院,教育部光学仪器与系统工程研究中心,上海现代光学系统实验室,上海 200093)

摘　要:针对现有光学加密方法对加密系统要求高、受器件性能限制、加密效率低、解密图像易失真的局限性,提出一种基于光场成像原理和混沌系统的多图像加密方法.该方法利用混沌系统随机生成光场成像系统的个数与系统参数,并在计算机中构造出相应的多个光场成像系统;将多幅待加密图像拼接后置于光场成像系统中依次计算得到光场图像,通过提取光场图像的多幅子孔径图像并进行拼接,实现多幅图像的快速加密.解密过程为加密过程的逆过程.该方法将计算成像的方式引入加密过程,使加密不受硬件条件的限制,易于实现.实验结果表明,提出的算法密钥复杂度低,易于传输;对噪声有较好的鲁棒性,密钥空间大,密钥敏感度高,安全性好;加密效率高,解密图像无损失.在需要大量图像进行安全传输的领域具有广泛的应用前景.

关键词:信息光学;计算成像;光场成像;混沌系统;多图像加密
中图分类号:TP309.7　　**文献标识码**:A　　**doi**:10.3788/gzxb20204903.0310002

Multiple Image Encryption Method Based on Light Field Imaging Theory and Chaotic System

HAN Si-min, ZHANG Wei, ZHANG Xiang, WEI Xiao-xiao, WAN Xin-jun
(*Shanghai Key Lab of Modern Optical System, Engineering Research Center of Optical Instrument and System, Ministry of Education, School of Optical-Electrical and Computer Engineering, University of Shanghai for Science and Technology, Shanghai* 200093, *China*)

Abstract: In order to overcome the limitations of the existing optical encryption methods on high encryption system requirements, limited device performance, low encryption efficiency, and easy distortion of decrypted images, a multi-image encryption method based on the light field imaging principle and chaotic system was proposed. The method first generates random numbers through a chaotic system, and these numbers are used as the number of the light field imaging systems and the parameters of each system. Then multiple light field imaging systems are built according to the generated numbers in the computer. The images to be encrypted are spliced to a big image, and placed into the constructed light field imaging systems sequentially to obtain the corresponding light field images. By extracting and splicing the sub-aperture images of each light field image, the encryption of multiple images are achieved fast. The decryption process is the reverse of the encryption. The proposed method introduces the computing imaging technology into the encryption, which can avoid the limitation of real optical decives, and is easy to be achieved. The experimental results show that the proposed algorithm has low complexity

基金项目:国家重点研发计划(No.2016YFF0101402),国家自然科学基金(No.61205015)
第一作者:韩思敏(1995—),女,硕士研究生,主要研究方向为光场成像技术,光学加密技术等. Email:han_4min@163.com
导师(通讯作者):张薇(1978—),女,副教授,博士,主要研究方向为光场成像技术、光学系统设计、医用光学系统等. Email:wei_zhang@usst.edu.cn
收稿日期:2019-10-21;**录用日期**:2019-12-17

of secure keys which can be transmitted easily. And it has good robustness to noise, large key space and high sensitivity of keys, which can provide high security. It also has high efficiency. The proposed method has widely potential uses in the fields of requiring plenty of images transmission with security.

Key words: Information optics; Computational imaging; Light field imaging; Chaotic system; Multiple-image encryption

OCIS Codes: 100.4998; 070.4560; 110.1758; 110.1160; 100.6890

0 引言

网络技术的快速发展对图像加密技术的保密性能及加密效率有了越来越高的要求.基于光学原理的图像加密技术包括双随机相位编码技术[1-3]、分数阶傅里叶变换[4-5]、鬼成像加密技术[6-7]等,具有维度高、鲁棒性强等优势.但现有的光学加密方法大多对加密系统的要求较高,算法复杂,加密效率较低,无法高效完成大量图像的加密任务.因此,研究安全高效的多图像加密方法迫在眉睫.

针对多图像加密也有人提出了一些方法,如 ZHU Wei 等提出一种基于小波变换的算法[8],该算法避免了加性串扰,提高了系统容量.WU Jing-jing 等提出了一种基于不同衍射距离的计算成像的多图像加密算法[9],该方案密文不是复振幅,而是强度矢量,因此更便于记录和发送,但是会造成解密过程中图像的失真.TANG Zhen-jun 等提出了一种基于位平面分解和混沌的多图加密算法,该算法将四幅经过处理的图像分别作为便携式网络图形(Portable Network Graphics, PNG)格式图像的 R、G、B 和 Alpha 四个通道的分量,但一次仅可同时完成 4 幅图像的加密工作[10].ZHANG Xiao-qiang 等提出了一种基于混合图像元素和混沌的多图像加密算法[11];LI Yan-bin 等提出了一种基于级联分数傅里叶变换的算法[12],HU Ke-ya 等提出的基于圆柱衍射和相位截断的非对称式多图像加密系统[13],这两种算法抗攻击性极强;HU Yi-qun 等提出基于带参数的迭代 Arnold 变换和图像分解的量子多图像加密算法[14];MOSSO E 等提出基于线性调频 z 变换的非对称多图像加密系统[15]等.这些算法虽然改进了多幅图像加密技术,但在加密效率方面仍有欠缺.

光场成像是近年来发展起来的一种能够获取三维图像的新方法[16-19],它可以同时获取目标在空间中的位置信息与方向信息,通过提取完整的四维光场信息并对其进行计算处理,可以获得目标在光场中不同维度的切片.完整光场信息的采集除现阶段采用的微透镜阵列外,相机与机械臂的组合使用同样可以完成该目的,利用机械臂的二维移动与转动可以对目标进行多个视角的成像[20],同样可以采用较小的透镜阵列和平板扫描仪完成对完整光场的采集[21],而可调相机阵列则通过使相机在水平和竖直方向的移动来完成对目标完整光场的采集[22].

本文基于光场成像原理结合混沌系统,提出一种新的多图像加密方法.利用混沌系统生成光场成像系统的个数和参数,通过构造多个光场成像系统并提取其子孔径图像,高效实现多幅图像同时加密,且解密过程无失真,并对该加密算法进行了性能评估.

1 光场成像系统基本原理

光场可以表征自由空间中的四维光线辐射,利用微透镜阵列实现的光场成像系统,能够记录光线的二维位置分布和二维方向分布.通过对采集到的光场信息进行重构,能够获得具有不同信息的新的图片,从而实现诸如三维成像、图像重聚焦等功能.

一种包含微透镜阵列的聚焦型光场成像系统的基本结构如图 1 所示[23].通常主镜头具有较大孔径,将物体成像于其焦平面上;微透镜阵列位于主透镜和图像传感器之间,其位置靠近但不在主透镜的焦平面上,每个微透镜都可看做独立的相机,能够对主镜头所成图像的一部分进行采集;探测器位于微透镜阵列后,主镜头焦平面位置与微透镜阵列间距离为 a,微透镜阵列与探测器之间距离为 b,它们与微透镜的焦距 f' 之间满足高斯成像公式

$$\frac{1}{b}+\frac{1}{a}=\frac{1}{f'} \tag{1}$$

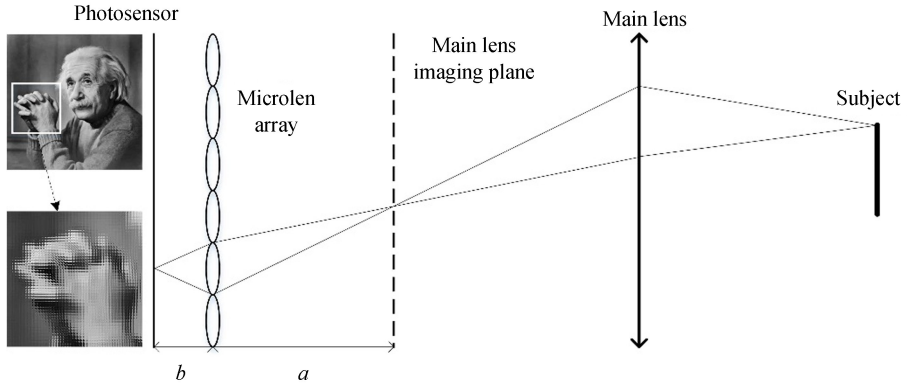


图 1　包含微透镜阵列的聚焦型光场成像系统的基本结构示意图

Fig.1　Basic structure diagram of a focused light field imaging system including a microlens array

在主镜头后方,光线经过微透镜阵列成像到探测器平面,每一个微透镜所对应的探测器上的成像区域形成一个宏像素,宏像素中的每一个像素点都与光场中一个位置与角度的采样相对应.在采集的光场图像中,每个宏像素中同一位置的像素与主镜头上相同位置的子孔径所成的像相对应.将这些像素按与微透镜顺序相对应的位置进行组合所得到的图像,定义为一幅子孔径图像,如图 2 所示.

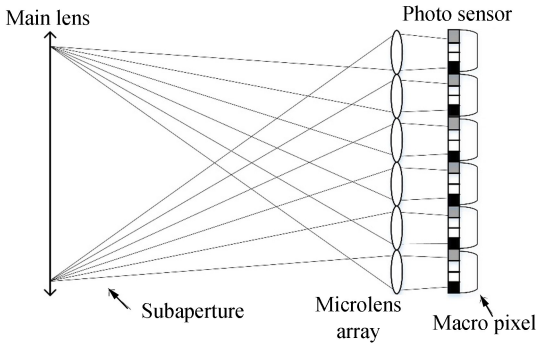


图 2　子孔径图像与宏像素示意图

Fig.2　Schematic of sub-aperture image and macro pixel

2　算法流程

2.1　加密步骤

提出的基于光场成像原理和混沌系统的多图像加密方法,其加密过程如图 3 所示,描述为:

1)将多幅待加密图像按任意顺序组合拼接为一幅图像.

其中待加密图像的数量为 $A\times A$,单幅待加密图像的像素数为 $B\times B$,则拼接完成的组合图像总像素数为 $A\times A\times B\times B$.

2) 由混沌系统 Logistic 映射生成加密用光场成像系统的个数及参数.

随机选择初始值 $x_1^0\in(0,1)$,参数变量 $\mu_1\in(3.5699456,4)$,迭代 n_1(n_1 为任意正整数)次后得到混沌序列 $X_1=\{x_1^1,x_1^2,x_1^3,\cdots,x_1^{n1}\}$,将此序列的值归一化到$(0,K)$($K$ 为任意正整数)之间并向上取整,得到序列 $X_1'=\{x_1^1{}',x_1^2{}',x_1^3{}',\cdots,x_1^{n1}{}'\}$,取 $x_1^{n1}{}'=n$,并取 n 值作为光场系统的个数.求出 $A\times B$ 的所有因数并编号为 $a_1,a_2,a_3,\cdots a_s$,因 $a_1=1$,且为防止光场系统间的重复,仅选用 $a_2,a_3,\cdots a_{\frac{s}{2}-1}$.

随机选择初始值 $x_2^0\in(0,1)$,参数变量 $\mu_2\in(3.5699456,4)$,迭代 n_2($n_2=x_1^n{}'$)次后得到混沌序列 $X_2=\{x_2^1,x_2^2,x_2^3,\cdots,x_2^{n2}\}$,将此序列的值归一化到 $\left(0,\frac{s}{2}-1\right)$ 之间并向上取整,得到序列 $X_2'=\{x_2^1{}',x_2^2{}',x_2^3{}',\cdots,x_2^{n2}{}'\}$,将 $A\times B$ 的因数 $a_2,a_3,\ldots a_{\frac{s}{2}-1}$ 按照编号赋值给对应的 $x_2^i{}'(i=1,2,3,\cdots n_2)$,得到序列 $X_2''=\{x_2^1{}'',x_2^2{}'',x_2^3{}'',\cdots,x_2^{n2}{}''\}$,取该序列的值作为每个光场系统微透镜每行所覆盖的像素数 $M_1,M_2,M_3,\cdots M_n$ 的值.

3) 在计算机中构建 n 个基于微透镜阵列的光场成像系统.

每个构造的光场成像系统如图 1 所示.设主透镜焦距为 $f'_{n\mathrm{main}}$,微透镜个数为 $N_n\times N_n$,每个微透镜所覆盖的像素数为 $M_n\times M_n$,为了使探测器像素得到最大利用率,需要使每个微透镜采集到的光场信息无冗余,所以在选择密钥时需要满足 $A\times B\times A\times B=M_n\times N_n\times M_n\times N_n$.

4) 将拼接好的待加密图像依次置于构造出的 n 个光场成像系统中,得到光场图像 P,提取其相应的子孔径图像并进行拼接.

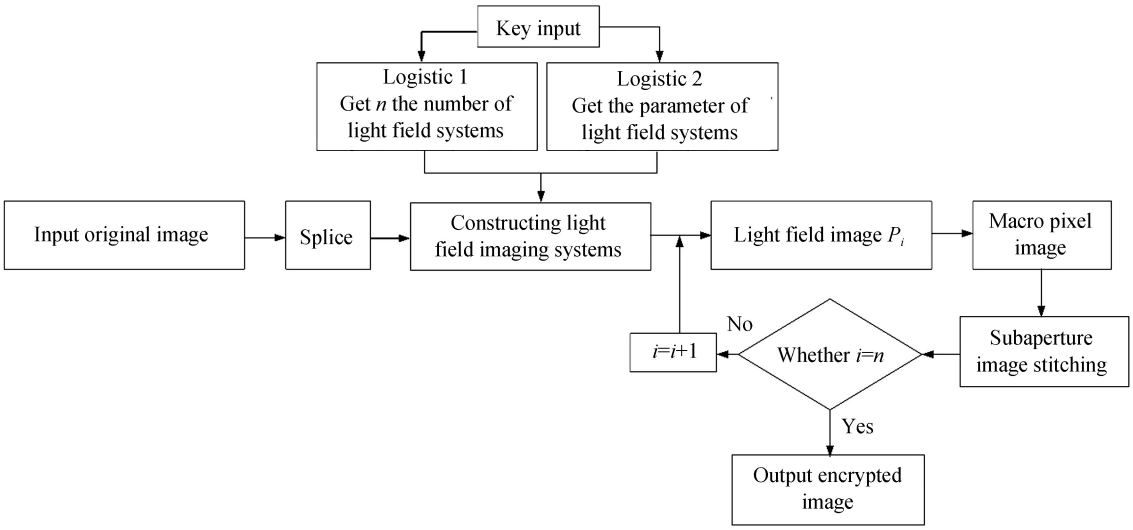


图 3 图像加密流程

Fig.3 Image encryption process

从光场图像中提取宏像素图像,对所有宏像素图像中的所有像素位置都进行子孔径图像提取,得到 $M_n\times M_n$ 个子孔径图像,每个子孔径图像包含 $N_n\times N_n$ 个像素.将所有子孔径图像按所对应的像素在宏像素图像中的位置顺序进行拼接,得到经过该光场成像系统的子孔径拼接图像.将得到的子孔径拼接图像作为初始图像,再经过下一个光场成像系统,做同样操作,直至依次经过 n 个光场成像系统后结束,最后得到的子孔径拼接图像即为加密图像.

2.2 解密步骤

解密过程为加密过程的逆过程,描述为:

1)将解密密钥 x_1^0,μ_1,n_1,K 输入 Logistic1 映射,得到加密光场系统的数量 n.将解密密钥 x_2^0,μ_2 输入 Logistic2 映射,得到每个加密光场成像系统中每个微透镜所覆盖的像素数 M_1,M_2,M_3,…,M_n.

2) 根据 n、M_1,M_2,M_3,…,M_n 构造多个光场成像系统.

3) 将加密图像依次置于构造的光场成像系统中,计算得到光场图像.

在一个光场成像系统中,根据微透镜参数将加密图像分割成 $M_n\times M_n$ 个子孔径图像,每个子孔径图像包含 $N_n\times N_n$ 个像素,将每个子孔径图像中的相同位置的像素按照其在子孔径图像集中的排列顺序进行排列,得到一个宏像素图像;对 $M_n\times M_n$ 个子孔径图像做同样的操作,得到 $N_n\times N_n$ 个宏像素图像.将这些宏像素图像按照该宏像素对应的微透镜在阵列中的位置顺序进行拼接,即得到该光场成像系统下的光场图像.

将该光场图像作为初始图像,再经过下一个光场成像系统,做同样操作,直至按逆序依次经过 n 个光场成像系统后结束,最后得到的光场图像即为原始加密图像的拼接图像.

4)将最终得到的拼接图像按照图像数量进行分割,得到解密了的原始图像.

3 实验与安全性分析

3.1 实验

为了测试所提出的加密方法的有效性,用 9 幅尺寸为 150×150 像素的灰度图像来进行模拟仿真,原始图片如图 4 所示,为说明方便,不失一般性地将主镜头放大率取为 1,仅将微透镜阵列及探测器的参数作为

密钥.在实际应用中，当主镜头放大率不为 1 时，密钥空间将进一步扩大.

当主镜头放大率为 1 时，图像经过单次光场加密过程像素位置的变化公式为

$$\begin{cases} s'(x',y')=s(x,y) \\ x'=M\times\left[x-1-N\times\mathrm{floor}\left(\dfrac{2x}{2N+1}\right)\right]+\mathrm{floor}\left(\dfrac{2x}{2N+1}\right)+1 \\ y'=M\times\left[y-1-N\times\mathrm{floor}\left(\dfrac{2y}{2N+1}\right)\right]+\mathrm{floor}\left(\dfrac{2y}{2N+1}\right)+1 \end{cases} \tag{2}$$

式中，$s(x,y)$ 为输入光场系统前图像在坐标 (x,y) 的像素值，$s'(x',y')$ 为经过单次光场加密后图像在坐标 (x',y') 的像素值.(x,y) 为输入光场系统前图像坐标系中的坐标值，(x',y') 为经过单次光场加密后图像坐标系中的坐标值，且 $1\leqslant x\leqslant M\times N$，$1\leqslant y\leqslant M\times N$，$1\leqslant x'\leqslant M\times N$，$1\leqslant y'\leqslant M\times N$.$N$ 为微透镜的数量，M 为微透镜的像素数，floor 表示向下取整操作.当经过多次光场加密时，将不同光场系统的参数依次带入公式中进行计算即可.

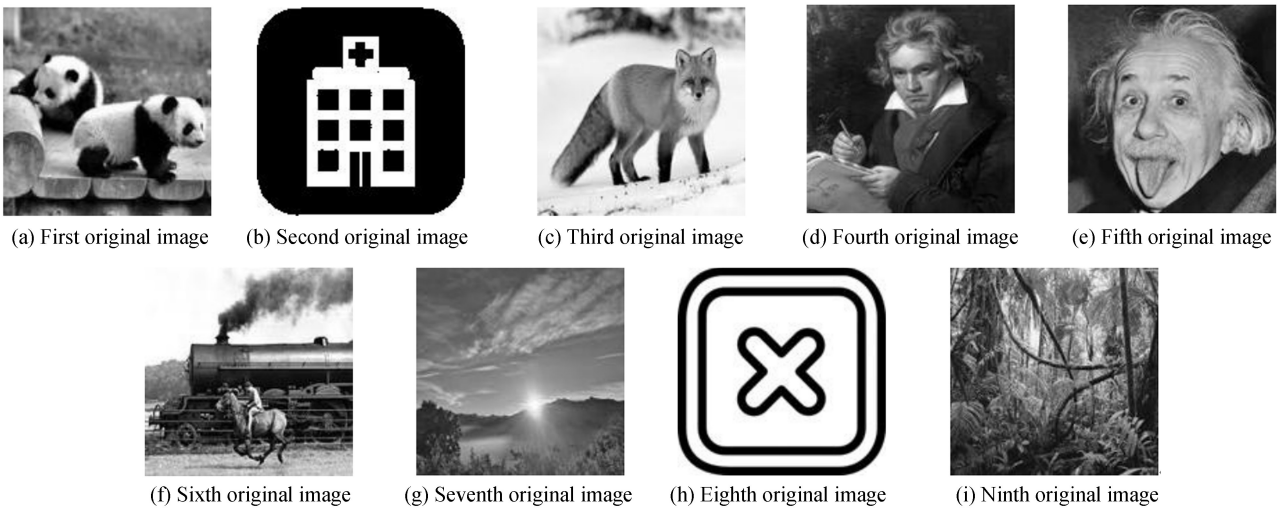


图 4　原始图像

Fig.4　Original images

实验中取 $x_1^0=0.78$，$\mu_1=3.45$，$n_1=5$，$K=10$，$x_2^0=0.75$，$\mu_2=3.45$，得到的加密图像如图 5 所示，尺寸为 450×450 像素.解密过程即为加密过程的逆过程，将密钥和加密图像输入后得到解密图像如图 6 所示，解密图像与原始图像完全一致，提出的加密方法对图像质量无损失.

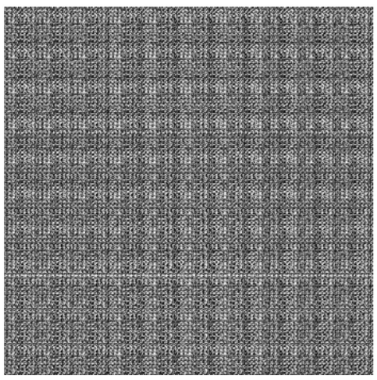


图 5　加密图像

Fig.5　Encrypted image

图 6　解密图像

Fig.6　Decrypted image

3.2　安全性分析

为验证加密算法的有效性和安全性，通常从相邻像素相关性、密钥空间、密钥敏感度、信息熵、鲁棒性等方面对加密方法进行分析，并根据所得参数对加密方法进行综合评估[24].

3.2.1 相邻像素相关度

通常在原始待加密图像中相邻像素之间水平、垂直、对角线方向的相关性都很高，意味着相邻像素的灰度值非常接近，攻击者能够利用相邻像素值来推测原始图像，因此，一个合格的加密算法需要尽可能降低相邻像素的相关性.

相邻像素相关性的值的公式为

$$R_{xy}=\frac{E[(x-\mu_x)(y-\mu_y)]}{\sigma_x\sigma_y} \tag{3}$$

式中，μ_x 和 μ_y 是 x 和 y 的平均值，σ_x 和 σ_y 表示 x 和 y 的标准差，$E[]$表示期望函数.当相关性的值越接近1，表示相关性越强，相关性的值越接近0，则表示相关性越弱.

本实验中，在水平、垂直、对角线方向上分别取1 000对相邻像素点，表1是9幅原始图像和加密像图在水平、垂直、对角线三个方向的相邻像素相关性值，图7是原始图像拼接后图像的水平方向相邻像素分布，图8是加密图像的水平方向相邻像素分布.可以看出，加密后相邻像素的像素值几乎充满整个图像，图像的相关性已经丢失，说明提出的加密方法能够有效地去除原始图像的相关性.

表1 原始图像和加密图像的相邻像素相关度

Table 1 Adjacent pixel correlation of original image and encrypted image

Image	Horizontal	Vertical	Diagonal
Fig.4(a)	0.958 1	0.951 5	0.914 6
Fig.4(b)	0.917 2	0.910 5	0.849 6
Fig.4(c)	0.955 6	0.961 6	0.919 5
Fig.4(d)	0.956 2	0.952 5	0.916 2
Fig.4(e)	0.960 3	0.967 3	0.940 7
Fig.4(f)	0.962 2	0.939 8	0.912 4
Fig.4(g)	0.964 6	0.940 9	0.916 6
Fig.4(h)	0.879 3	0.881 3	0.809 3
Fig.4(i)	0.793 6	0.848 2	0.729 5
Stitched image	0.931 9	0.935 4	0.882 1
Encrypted image	0.077 9	0.028 0	0.046 2

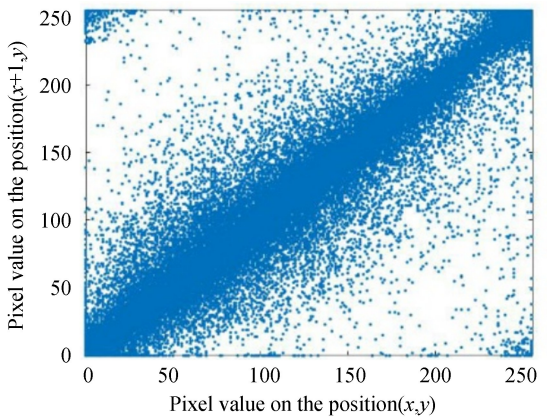


图7 原始图像拼接后图像的水平方向相邻像素相关性

Fig.7 Horizontal pixel adjacent pixel correlation of original images after stitching

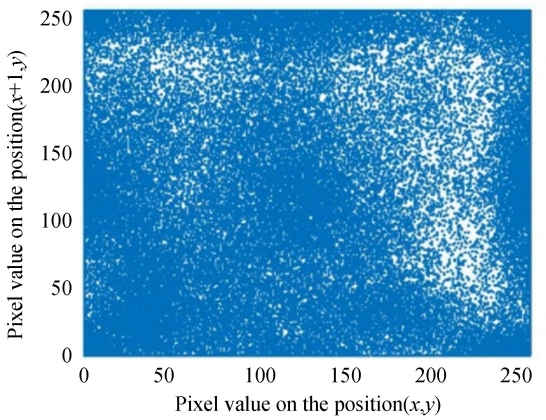


图8 加密图像的水平方向相邻像素相关性

Fig.8 Horizontal pixel adjacent pixel correlation of encrypted images

3.2.2 密钥空间

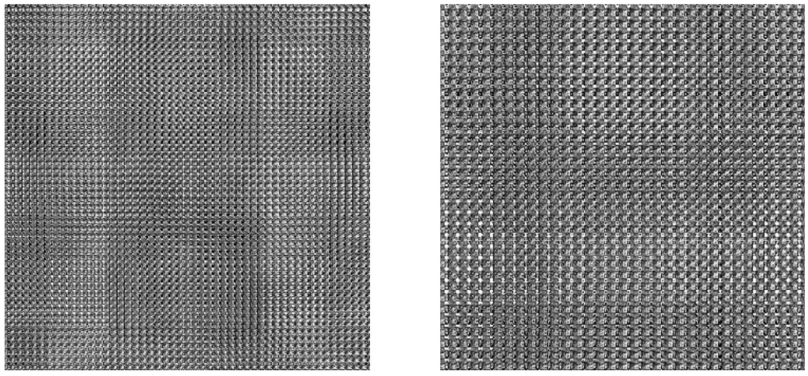
为确保加密算法的安全性，密钥空间必须足够大才能抵御攻击者的破解.

实验中假设计算机的计算精度为 10^{-15}，则混沌序列 X_1 和混沌序列 X_2 的密钥空间为 $(10^{15})^4$；为保证加密效率，参数密钥 P 和 n_1 取值均设定为 $(1,10^4)$，则本文算法的密钥空间为 $(10^{15})^4\times10^4\times10^4=10^{68}$，表明本文算法的密钥空间足够大.

3.2.3 密钥敏感度

有效的加密方案对安全密钥的变化非常敏感,当加密秘钥和解密密钥之间存在微小差别时,接收者就无法获得正确的解密图像.

当改变混沌序列 X_1 的密钥时,光场系统的个数和光场系统的参数均会发生改变,如将 x_1^0 的 0.78 改为 0.779,用该参数得到的解密图像如图 9(a)所示.当改变混沌序列 X_2 的密钥时,会导致光场系统参数发生改变,如将 μ_2 的 3.45 改为 3.451,得到的解密图像如图 9(b)所示.从解密图像中可以看出,当密钥参数发生微小改变时,从解密图像中完全无法识别出原始图像,表明本算法具有很高的密钥灵敏度.



(a) Decrypted image when x_1^0 is changed (b) Decrypted image when μ_2 is changed

图 9 算法的密钥敏感度测试

Fig.9 Key sensitivity test of the algorithm

3.2.4 信息熵

图像中包含信息的不确定性可以用信息熵来评估,信息熵的值越大,图像的不确定性越高,当信息熵等于 8 时,每个灰度出现的概率相同,因此,图像的信息熵越接近 8,图像的灰度分布越均匀,攻击者从灰度分布中得到的图像信息就越少,原始图像就越不容易被泄露.信息熵可以表示为

$$H(m)=-\sum_{i=0}^{255}p(m_i)\log_2 p(m_i) \tag{4}$$

表 2 为原始图像和加密图像的信息熵,可见经过加密后图像的信息熵已经非常接近理论值,本算法能够有效地将图像灰度均匀化.

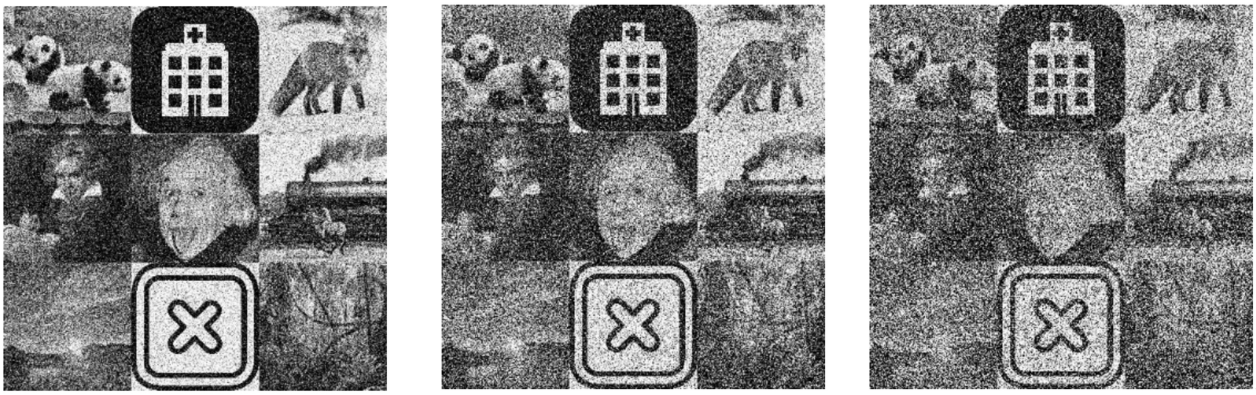
表 2 原始图像和加密图像的信息熵

Table 2 Information entropy of original image and encrypted image

Image	Information entropy
Fig.4(a)	7.681 6
Fig.4(b)	1.960 3
Fig.4(c)	7.249 2
Fig.4(d)	7.136 7
Fig.4(e)	7.509 8
Fig.4(f)	7.517 3
Fig.4(g)	7.142 5
Fig.4(h)	2.609 0
Fig.4(i)	7.592 4
Stitched image	7.378 1
Encrypted image	7.875 4

3.2.5 鲁棒性

为了测试算法的鲁棒性,对加密图像进行噪声攻击.图 10 为在加密图像中加入方差 $\sigma=0.1$、0.3 和 0.5 的高斯噪声后的解密图像.可以看出,在加密图像遭受噪声攻击时,解密图像依旧能够被辨认出.这表明本算法对噪声攻击有较好的鲁棒性.



(a) Decrypted image with σ=0.1 Gaussian noise (b) Decrypted image with σ=0.3 Gaussian noise (c) Decrypted image with σ=0.5 Gaussian noise

图 10 受到噪声攻击后的解密图像

Fig.10 Decrypted images with noise attack

3.2.6 算法性能比较

为了验证本文算法的性能，选择一种多图像加密算法，即 TANG 所提出的基于位平面分解和混沌的多图像加密算法[10]与本文方法进行比较.

从单次能够加密的图像数量方面看，TANG 的加密算法中，是将 4 幅经过处理的图像分别作为 PNG 格式图像的 R、G、B 和 Alpha 四个通道的分量，所以该算法单次只能同时加密 4 幅图像.而本文所提出的加密算法，理论上对单次能够处理的图像数量没有限制.

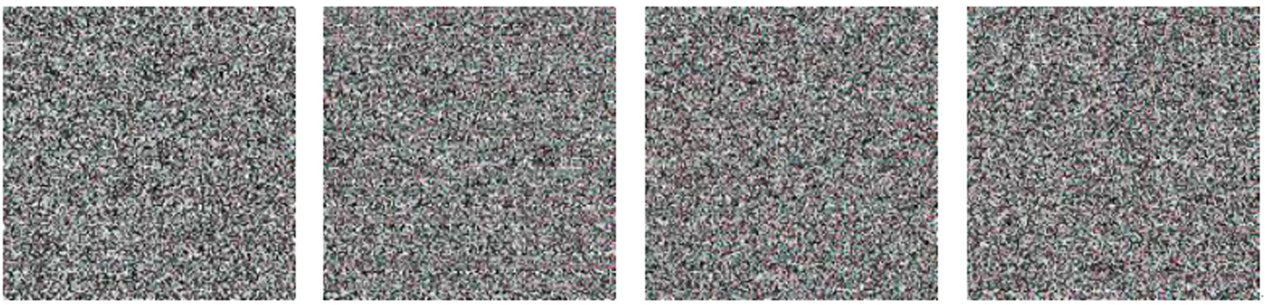
从计算复杂度方面看，TANG 的算法中，主要的计算复杂度包括将 4 幅原始图像进行位平面分解、不同位平面间的位块交换、将位平面图像转换为灰度图和异或运算等；而本文所提出的加密算法，主要计算复杂度仅在于根据光场系统参数进行的图像像素间的置乱.

实验选取 16 幅灰度图像作为原始图像，如图 11 所示，大小均为 150×150 像素，分别使用两种加密方法在同一台 CPU 为 i7-7700HQ，内存为 16G 的笔记本电脑上，利用 Matlab R2017b 编程进行测试.

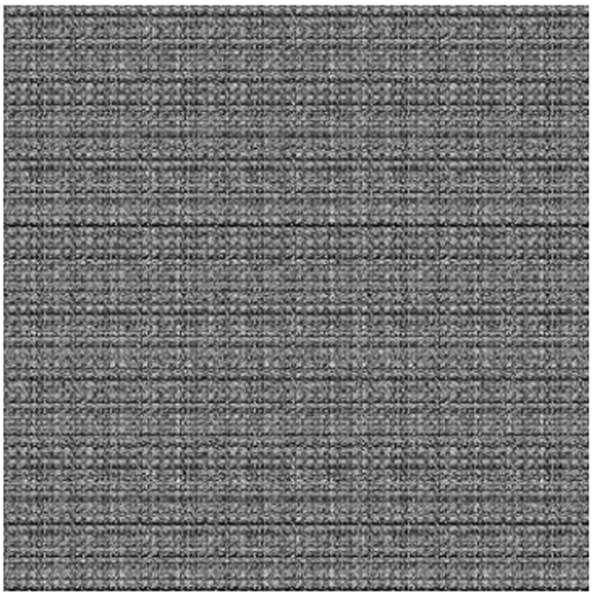
图 11 算法对比实验中的原始图像

Fig.11 Original image in algorithm comparison experiment

TANG的算法得到的加密图像如图12(a)所示，为4幅大小为150×150像素的彩色图像.本文算法得



(a) Encrypted image of TANG's algorithm



(b) Encrypted image of the proposed algorithm

图 12　使用两种算法得到的加密图像

Fig.12　Encrypted images using two algorithms

表 3　两种算法的计算时间

Table 3　The calculation time of two algorithms

Algorithms	Calculation time/s
TANG	17.288
Proposed	1.853

到的加密图像如图 12(b)所示，为 1 幅大小为 600×600 像素的灰度图像.加密所用的计算时间如表 3 所示，可以看出本文算法在加密效率上具有明显优势.

4　结论

本文提出了一种基于光场成像原理和混沌系统的多幅图像加密算法.该方法利用混沌系统生成随机的用于加密的光场成像系统的个数和参数，并在计算机中构造出相应的多个不同参数的光场成像系统；然后将多幅待加密图像拼接后依次置于多个光场系统中成像；从获得的光场图像中提取相应的子孔径图像，并将多幅子孔径图像重组得到加密图像.实验结果表明，该算法安全有效，有较好的鲁棒性、密钥空间大、密钥敏感度高，且加密过程简单，加密效率高.

参考文献

[1] SINGH M, KUMAR A, SINGH K. Encryption by using matrix-added, or matrix-multiplied input images placed in the input plane of a double random phase encoding geometry[J]. *Optics and Lasers in Engineering*, 2009, **47**: 1293-1300.

[2] KISHK R, JAVIDI B. Information hiding technique with double phase encoding[J]. *Applied Optics*, 2002, **41**(26): 5462-5470.

[3] QIN Yi, ZHENG Chang-bo. Color image encryption technology based on double random phase encoding[J]. *Acta Photonica Sinica*, 2012,**41**(3):326-329.
秦怡，郑长波. 基于双随机相位编码的彩色图像加密技术[J].光子学报，2012，**41**(3):326-329.

[4] UNNIKRISHNAN G, JOSEPH J, SINGH K. Optical encryption by double-random phaseencoding in the fractional Fourier domain[J]. *Optics Letters*, 2000, **125**(12): 887-889.

[5] HENNELLY B, SHERIDAN T. Optical image encryption by random shiftingin fractional Fourier domains[J]. *Optics Letters*, 2003, **28**(4): 269-271.

[6] ZHU Ji-nan. Research on image encryption method based on computational ghost imaging[D]. Jinan: Shandong University, 2019.
朱吉男. 基于计算鬼成像的图像加密方法的研究[D]. 济南：山东大学，2019.

[7] XUE Yu-lang, WAN Ren-gang, FENG Fei, *et al*. Experimental study on lensless ghost imaging with three different

structures[J]. *Acta Photonica Sinica*, 2014, **43**(8): 0823006.
薛玉郎,万仁刚,冯飞,等.三种不同结构的无透镜鬼成像实验研究[J].光子学报, 2014, **43**(8): 0823006.

[8] ZHU Wei, YANG Geng, CHEN Lei, *et al*. Multi-image encryption algorithm based on wavelet transform and improved double random phase encoding[J]. *Journal of Nanjing University of Posts and Telecommunications*, 2014, **34**(5): 87-92.
朱薇, 杨庚, 陈蕾, 等. 基于小波变换和改进双随机相位编码的多图像加密算法[J]. 南京邮电大学学报, 2014, **34**(5): 87-92.

[9] WU Jing-jing,XIE Zhen-wei, LIU Zheng-jun, *et al*. Multiple-image encryption based on computational ghost imaging[J]. *Optics Communications*, 2016, **359**: 38-43.

[10] TANG Zhen-jun, SONG Juan, ZHANG Xian-quan, *et al*. Multiple-image encryption with bit-plane decomposition and chaotic maps[J]. *Optics and Lasers in Engineering*, 2016, **80**: 1-11.

[11] ZHANG Xiao-qiang, WANG Xue-song. Multiple-image encryption algorithm based on mixed imageelement and chaos [J].*Computers and Electrical Engineering*, 2017, **62**: 401-413.

[12] LI Yan-bin, ZHANG Feng, LI Yuan-chao, *et al*. Asymmetric multiple-image encryption based on the cascadedfractional Fourier transform[J]. *Optics and Lasers in Engineering*, 2015, **72**: 18-25.

[13] HU Ke-ya, WU Chao, WANG Ying, *et al*. An asymmetric multi-image cryptosystem based on cylindrical diffraction and phase truncation[J]. *Optics Communications*, 2019, **449**:100-109.

[14] HU Yi-qun, XIE Xin-wen, LIU Xing-bin, *et al*. Quantum multi-image encryption based on iteration arnold transform with parameters and image correlation decomposition[J]. *International Journal of Theoretical Physics*, 2017, **56**(7): 2192-2250.

[15] MOSSO E, SUAREZ O, BOLOGNINI N. Asymmetric multiple-image encryption system based on a chirp z-transform [J]. *Applied Optics*, 2019, **58**(21): 5674-5680.

[16] REN N. Digital light field photography[C]. Stanford: Leland Stanford Junior University, 2006.

[17] LEVOY M, REN N, ADAMS A,*et al*. Light Field microscopy[J]. *ACM Trans Graph*, 2006, **25** (3): 924-934.

[18] LUMSDAINE A, GEORGIEV T. The focused plenoptic camera[C]. San Franciscan: IEEE International Computational Photography, 2009: 1-8.

[19] GEORGIEV T, ZHAN Yu, LUMSDAINE A, *et al*. Lytro camera technology: theory, algorithms, performance analysis[C]. SPIE, 2013,**8667**: 86671J.

[20] LEVOY M, HANRAHAM P. Light filed rendering. Proccedings of the 23rd annual conference on Computer graphies and interactive techniques[C]. New York: ACM, 1996, **237199**: 31-43.

[21] YANG J C, MCMILLAN L, SMITH A C. A light field camera for image based rendering [D]. Cambridge: Massachusetts Institute of Technology, 2000.

[22] YANG J C, EVERETT M, BUEHLER C, *et al*.A real-time distributed light field camers. Proceedings of the 13th Eurographics workshop on Rangering[C]. Aire-la-Ville: Eurographics Association, 2002:77-86.

[23] GEORGIEV T, LUMSDAINE A. Focused plenoptic camera and rendering[J]. *Journal of Electron Imaging*, 2010, **19** (2):1-11.

[24] ZHAN Xin-sheng. Image encryption scrambling performance analysis [D]. Zhengzhou: Zhengzhou University,2005.
詹新生. 图像加密置乱性能分析[D]. 郑州:郑州大学,2005.

Foundation item: The National Key Research and Development Program of China (No.2016YFF0101402), the National Natural Science Foundation of China (No.61205015)