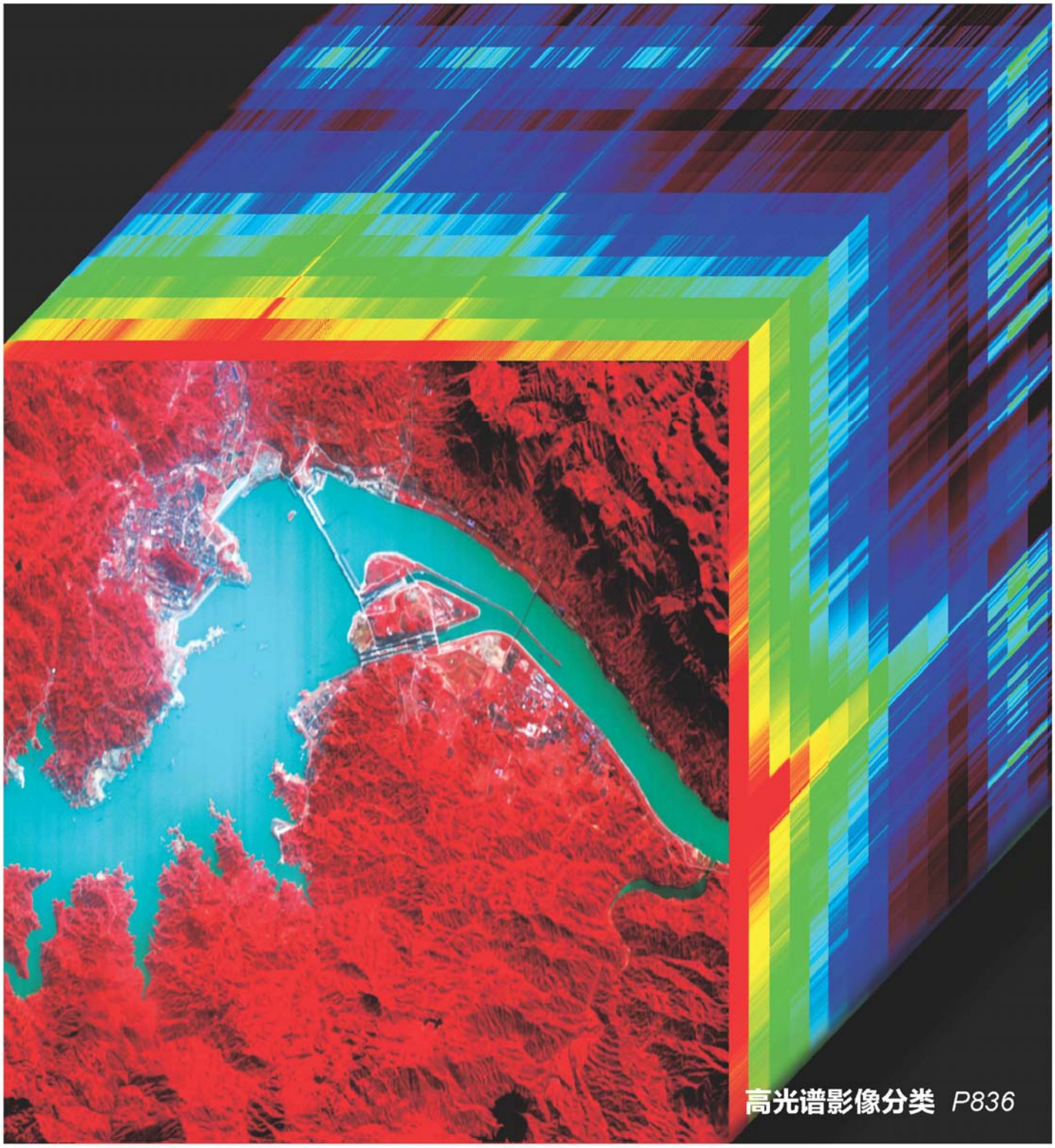
JOURNAL OF IMAGE AND GRAPHICS

主办：中国科学院遥感与数字地球研究所
中国图象图形学学会
北京应用物理与计算数学研究所

中国图象图形学报

2015
06
VOL.20

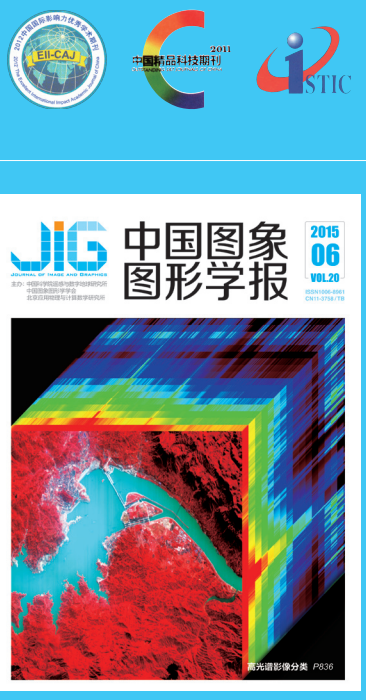
ISSN1006-8961
CN11-3758/TB



高光谱影像分类 P836

中国图象图形学报

刊名题字：宋健 | 月刊（1996年创刊）



第20卷第6期（总第230期）

2015年6月16日

中国精品科技期刊
中国国际影响力优秀学术期刊
中国科技核心期刊
中文核心期刊

主管单位 中国科学院
主办单位 中国科学院遥感与数字地球研究所
中国图象图形学学会
北京应用物理与计算数学研究所

主　　编 李小文
编辑出版 《中国图象图形学报》编辑出版委员会
邮政信箱 北京9718信箱
邮　　编 100101
电子信箱 jig@radi.ac.cn
电　　话 010-64807995
网　　址 www.cjig.cn

广告经营许可证 京朝工商广字第0361号
总 发 行 北京报刊发行局
订　　购 全国各地邮局
海外发行 中国国际图书贸易集团有限公司
（邮政信箱：北京399信箱　邮编：100048）
印刷装订 北京科信印刷有限公司

Journal of Image and Graphics

Title inscription: Song Jian | Monthly, Started in 1996

Superintended by Chinese Academy of Sciences
Sponsored by Institute of Remote Sensing and Digital Earth, CAS
China Society of Image and Graphics
Institute of Applied Physics and Computational Mathematics

Editor-in-Chief LI Xiaowen
Editor, Publisher Editorial and Publishing Board of Journal of Image and Graphics
P.O.Box 9718, Beijing, P.R.China
Zip code 100101
E-mail jig@radi.ac.cn
Telephone 010-64807995
Website www.cjig.cn

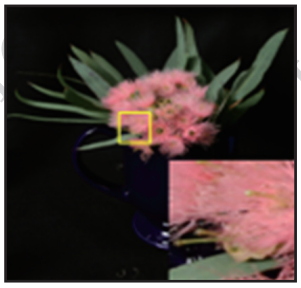
Distributed by Beijing Bureau for Distribution of Newspapers and Journals
Domestic All Local Post Offices in China
Overseas China International Book Trading Corporation
(P.O.Box 399, Beijing 100048,P.R.China))
Printed by Beijing Kexin Printing Co., Ltd.

CN 11-3758/TB
ISSN 1006-8961
CODEN ZTTXFZ

国外发行代号 M1406
国内邮发代号 82-831
国内定价 50.00元

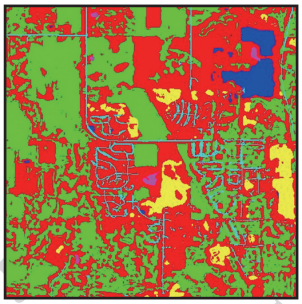
2015年6月 第20卷 第6期（总第230期）
中国图象图形学报
Zhongguo Tuxiang Tuxing Xuebao

目次



边缘结构保持的加权BDTV全光场图像超分辨率重建(第0733页)

基于超像素的多主体图像交互分割(第0764页)

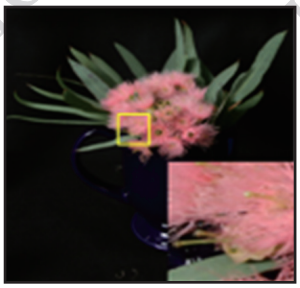


谐波分析光谱角制图高光谱影像分类(第0836页)

封面图片由中国科学院遥感与数字地球研究所高光谱遥感应用技术研究室张霞研究员提供

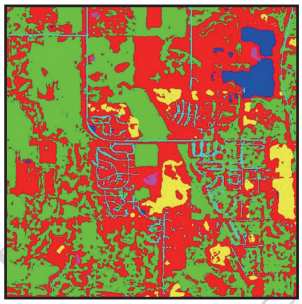
Volume 20, Number 6
Published June 16, 2015

CONTENTS
JOURNAL OF IMAGE AND GRAPHICS



Edge preserved light field image super-resolution based on weighted BDTV model (P0733)

Interactive multiphase image segmentation based on superpixels (P0764)



Classification algorithm of hyperspectral imagery by harmonic analysis and spectral angle mapping (P0836)

E-mail: jig@radi.ac.cn
Website: www.cjig.cn
Tel: 010-64807995

中国图象图形学报
JOURNAL OF IMAGE AND GRAPHICS

中图法分类号：TP309.7　　**文献标识码**：A　　**文章编号**：1006-8961(2015)06-0740-09

论文引用格式：Xu Y, Zhang S W. Encryption algorithm of image blocking and double adaptive diffusion with Arnold mapping[J]. Journal of Image and Graphics, 2015, 20(6): 0740-0748. [徐亚, 张绍武. 基于 Arnold 映射的分块双层自适应扩散图像加密算法[J]. 中国图象图形学报, 2015, 20(6): 0740-0748.] [DOI: 10.11834/jig.20150602]

基于 Arnold 映射的分块双层自适应扩散图像加密算法

徐亚，张绍武

西北工业大学自动化学院，信息融合技术教育部重点实验室，西安　710072

摘　要：**目的**　针对图像安全保障问题，提出一种基于 Arnold 映射的分块双层自适应扩散数字图像加密(BDAM)算法，提高图像加密效率及安全性。**方法**　首先利用 Logistic 映射、Tent 映射和 Sine 映射，进行两两组合构建 3 种新 1 维混沌映射，提取初始混沌序列；然后定义一个与明文图像矩阵大小相同的初始加密图像矩阵，对其进行分块，预处理 Arnold 映射参数，正反向联合映射将明文图像矩阵中随机位置像素值，存入初始加密矩阵随机块中的随机位置，并同时进行块内像素、块间自适应扩散，直至填满初始加密矩阵，完成加密。**结果**　针对多种类型灰度图像，通过仿真实验与性能对比分析表明：BDAM 算法在信息熵、密钥空间、相关性、敏感性等方面均优于其他加密算法，置乱效果好，对密钥及明文的敏感性高，可取得较好加密效果。**结论**　结合随机置乱的分块双层非线性自适应扩散 BDAM 算法可有效抵御多种攻击，安全性较高，适用于各种类型灰度图像加密，具有潜在应用价值。

关键词：Arnold 映射；分块；双层自适应扩散；图像加密

Encryption algorithm of image blocking and double adaptive diffusion with Arnold mapping

Xu Ya, Zhang Shaowu

Key Laboratory of Information Fusion Technology of Ministry of Education College of Automation, Northwest Polytechnical University, Xi'an　710072, China

Abstract: **Objective** With the rapid development and popularization of computer networks and information storage technologies, networks have become a mainstream tool for information transmission. This medium is used to transmit information, including text messages, audio, images, and other multimedia files. Thus, networks intuitively play an irreplaceable media-related role in the transmission of information flow security as the main carrier of network information. The security problem in the network transmission of image data must be solved effectively; therefore, an encryption algorithm of image blocking and double adaptive diffusion using Arnold maps (BDAM) was proposed in this paper to address image security issues. This algorithm can improve the efficiency and security of image encryption. **Method** BDAM first uses Logistic, Tent, and Sine maps to build three types of novel 1D chaotic maps according to the scheme of pairwise combination. This algo-

收稿日期：2014-09-17；**修回日期**：2015-02-12

基金项目：国家自然科学基金项目(61170134, 61473232, 91430111)

第一作者简介：徐亚(1988—)，女，西北工业大学控制理论与控制工程专业在读硕士研究生，主要从事图像压缩加密方面的研究。E-mail：xuya916@126.com

通信作者：张绍武，博士生导师，E-mail：zhangsw@nwpu.edu.cn

Supported by: National Natural Science Foundation of China (61170134, 61473232, 91430111)

rithm then extracts the initial chaotic sequence. Then, BDAM defines an initial encryption image matrix that is similar in size to the plain image matrix. The latter is divided into small blocks. The initial encryption image matrix pretreats the parameters of the Arnold map. The pixels in the random position of the plain image matrix are deposited at random positions within the random block of the initial encryption image matrix when ordinary and reverse maps are joined. At the same time, adaptive diffusion occurs among intra-block pixels and inter-blocks until the initial encryption matrix is filled. **Result** Scrambling and diffusion synchronization are initiated by combining forward and reverse Arnold mapping processes. The BDAM algorithm can equalize the access sequence of each pixel and the position of each storage sequence, enhance scrambling randomness, and overcome the drawbacks of conventional Arnold mapping from rules to the defects of random access. In addition, this algorithm can apply block and double adaptive diffusion in the scrambling process. The interactions among the ciphertext pixels and ciphertext pixels, plaintext pixels, and chaos random sequence spread the influence of each pixel to the image matrix of the entire site nonlinearly. Furthermore, these interactions continuously disturb chaotic systems during diffusion, initiate adaptive diffusion, and enhance the sensitivity of the encryption key, the ciphertext, and plaintext. The results of simulation and of performance comparison analysis show that the BDAM algorithm is superior to other encryption algorithms for many types of gray images in terms of information entropy, key space, correlation, and sensitivity, among other aspects. Scrambling randomness is favorable as well. Moreover, the algorithm displayed high sensitivity to the key and to the plaintext, thus improving encryption results. **Conclusion** Random scrambling that is combined with blocking and double nonlinear adaptive diffusion through the BDAM algorithm can resist various attacks effectively and exhibit high security. Therefore, this method is suitable for all types of gray-scale images and may be applied in this field.
Key words: Arnold mapping; blocking; double adaptive diffusion; image encryption

0 引　言

随着计算机网络和信息存储等技术迅速发展与普及,网络已经成为信息传输的主流工具。通过网络传输的信息包括文本信息、音频、图像等一些多媒体文件,其中,图像凭其直观性已成为网络信息的主要载体,在信息流安全传输中发挥不可替代的媒介作用。因此,网络传输中图像数据的安全问题十分重要,需发展有效的方法和途径解决。

传统加密算法,如国际数据加密算法 IDEA(international data encryption algorithm)、高级加密标准 AES(advanced encryption standard) 等都是针对 1 维数据流而设计,对图像数据加密效率不高,不适合图像数据加密,其原因在于图像类信息数据量大、数据之间相关性强、冗余度高。于是,近几年人们提出了一些数字图像加密算法,这些算法可归类为:空间域图像加密算法,如矩阵变换/像素置换图像加密算法[1-4]、基于信息熵的图像加密算法[5-6]; 变换域图像加密算法,如基于小波变换的图像压缩加密算法[7-8]、基于 EZW 的图像压缩加密算法[9]、基于 SPIHT 的图像压缩加密算法[10]等;基于混沌的图像加密算法,如超混沌图像加密算法[11-12]、结合 DNA 编码的图像加密算法[13]等。

矩阵变换/像素置换图像加密算法通过改变图像像素点的相互位置关系加密图像,常用置换方法有 Arnold 变换、幻方变换等,但这些变换算法经过有限次迭代后会出现回复现象,因而保密性不高。基于信息熵的图像加密算法应用一定加密规则替换图像像素值,使加密图像的直方图被平滑,信息熵增大到接近理论值来达到加密目的;但单纯采用此方法,会导致明密文中存在一定程度的线性计算关系,加密图像易被破解。变换域图像加密算法通过改变变换域中系数,使图像空间域中所有像素值发生改变来达到加密效果;该方法一般采用选择加密策略,即仅对变换域中少量重要系数进行加密,减少加密数据量,提高加密效率,但加密操作简单,攻击者可以通过忽略或替换被加密部分,窥探原始明文图像部分内容,因此易受选择明文攻击破解。混沌图像加密算法利用其类随机性、确定性、遍历性以及对系统参数和初始条件的高度敏感性等特点,结合像素置乱、替换和扩散等操作,可以设计出密钥空间大、加密流随机性高的图像加密算法,因此被应用于各种加密体制中,常用的混沌系统包括 Logistic 映射、Tent 映射、Lorenz 映射等,但现有的混沌加密技术大都基于 1 维或 2 维混沌系统,易受到相空间重构方法攻击。

近几年,基于混沌特性人们陆续提出了一些性能较好的图像加密算法[1,6,8],如 Zhang 等人[1]通过

双向利用2维混沌映射,采用非线性遍历明文方式替代传统线性遍历方法进行混淆、扩散,提出反向2维混沌映射算法,该算法可改善混淆效应,但对明文敏感性不够好。Zhou 等人[6]利用一些已有1维混沌系统构建新的1维混沌系统,提出新1维混沌加密算法,该算法混沌范围宽、混沌行为好,但仅通过旋转操作置乱图像,置乱随机性不高,具有周期性,置乱效果欠佳。罗玉玲等人[8]采用自适应扩散,提出量子混沌映射的小波域图像加密算法,该算法可增强加密算法敏感性,但将置乱和扩散分步进行,不适用加密数据量较大的图像。

基于上述分析,针对混沌图像加密算法中的明文敏感性不理想、置乱随机性不高问题,提出一种分块双层非线性自适应扩散的数字图像加密算法(BDAM),并通过图像仿真实验验证 BDAM 算法的有效性。

1 混沌系统模型

1.1 新1维混沌系统[6]

新混沌系统是由两个不同的已有1维混沌映射作为种子映射构造的非线性混沌系统,构造方程为

$$X_{n+1} = (F(a, X_n) + D(b, X_n)) \bmod 1 \quad (1)$$

式中,$F(a, X_n)$、$D(b, X_n)$为种子映射,a、b 分别为其控制参数。模操作为保证输出数据在区间(0,1)内,n 为迭代次数。

利用 Logistic、Tent 和 Sine 映射,两两组合作为种子映射,并按式(1)构造出3种新1维混沌映射系统[6]。动力学方程如下[6]:

Logistic-Tent 映射动力学方程

$$x_{n+1} = (L(\mu, x_n) + T((4-\mu), x_n)) \bmod 1 = \begin{cases} (\mu x_n(1-x_n) + (4-\mu)x_n/2) \bmod 1 & x_i < 0.5 \\ (\mu x_n(1-x_n) + (4-\mu)(1-x_n)/2) \bmod 1 & x_i \geqslant 0.5 \end{cases} \quad (2)$$

Logistic-Sine 映射动力学方程

$$x_{n+1} = (L(\mu, x_n) + S((4-\mu), x_n)) \bmod 1 = (\mu x_n(1-x_n) + (4-\mu)\sin(\pi x_n)/4) \bmod 1 \quad (3)$$

Tent-Sine 映射动力学方程

$$x_{n+1} = (T(\mu, x_n) + S((4-\mu), x_n)) \bmod 1 = \begin{cases} (\mu x_n/2 + (4-\mu)\sin(\pi x_n)/4) \bmod 1 & x_i < 0.5 \\ (\mu(1-x_n)/2 + (4-\mu)\sin(\pi x_n)/4) \bmod 1 & x_i \geqslant 0.5 \end{cases} \quad (4)$$

式中,L、T、S 分别表示 Logistic、Tent、Sine 映射,μ 为系统控制参数,$\mu \in (0,4)$。与种子混沌映射相比,新1维混沌系统具有更为复杂的混沌特性,它在 $\mu \in (0,4)$时处于混沌状态,可见,新1维混沌系统具有更宽混沌范围、更好混沌行为和混沌系统密度函数分布较一致等优点。

1.2 Arnold 映射

Arnold 映射动力学方程为[1]

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} 1 & p \\ q & pq+1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \bmod \begin{pmatrix} m \\ n \end{pmatrix} \quad (5)$$

式中,p、q 为控制参数。Arnold 映射一般用于图像置乱,是一种从规则位置到随机位置的映射,即由顺序位置(x,y)得到一个随机位置,并将(x,y)处像素值存入位置(x',y')。

2 BDAM 算法及步骤

BDAM 算法方框图如图1所示,该算法主要包括混沌序列生成、分块双层自适应扩散两个过程。首先,利用 Logistic、Tent 和 Sine 映射构建新混沌系统,迭代产生混沌序列,预处理产生初始混沌序列。然后,设定一个与明文像素矩阵大小相同的初始加密矩阵,将其分块,预处理 Arnold 映射参数;正、反向联合映射,将明文图像中随机像素替换操作存入

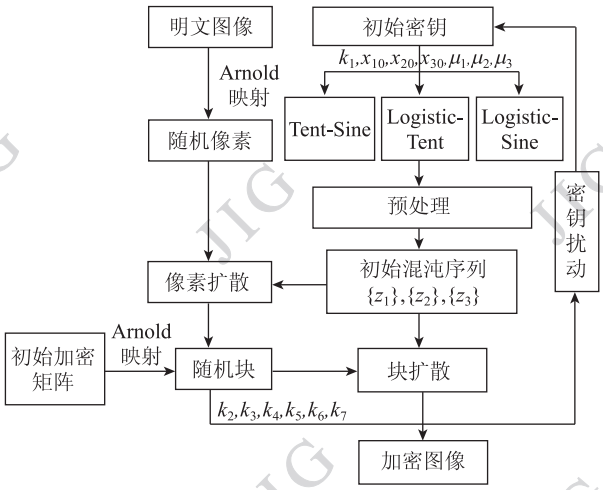


图1 BDAM 算法方框图

Fig. 1 The schematic diagram of BDAM algorithm

初始加密矩阵随机块中的随机位置，并同时进行块内像素、块间的自适应替换、扩散，使每个像素非线性地扩散到整幅图像矩阵中，直至填满初始加密矩阵，完成扩散加密。解密过程是加密的逆过程。

设明文图像为 $m\times n$ 的灰度图像 $\boldsymbol{I}$，BDAM 算法加密步骤如下：

1）定义初始加密矩阵。设初始加密矩阵 $\boldsymbol{E}$ 是元素全为 1 的 $m\times n$ 矩阵，并将其划分成大小为 $t\times t$ 的矩阵子块，共有 $(m/t)\times(n/t)$ 个子块（t 是 m、n 的公约数）。

2）混沌序列生成。给定初始密钥 $[k_1,x_{10},x_{20},x_{30},\mu_1,\mu_2,\mu_3]$，$x_{10}$，$x_{20}$，$x_{30}$，$\mu_1$，$\mu_2$，$\mu_3$ 分别为式(2)—(4)的初始值和初始参数。

(1)式(4)迭代 k 次，产生长度为 k 的混沌序列 $\{x'_{3,j}\}$，$j=1,2,\cdots,k$，舍弃前 k_1 项，按式(6)(7)处理余项，得序列 $\{x_{3,i}\}$，$\{y_{3,i}\}$。

$$\begin{aligned}y_{3,i}&=floor(x'_{3,i}\times 10^5-\\&floor(x'_{3,i}\times 10^5))\times 10^2 \bmod 8\\&i=1,2,\cdots,p\end{aligned}\tag{6}$$

$$x_{3,i}=floor(\boldsymbol{x}'_{3,i}\times 10^6-floor(\boldsymbol{x}'_{3,i}\times 10^6))\times 10^3 \bmod G,\ i=1,2,\cdots,p\tag{7}$$

式中，$p=t^2$，$k=k_1+p$，$floor(.)$ 表示向下取整，G 为图像灰度级。

(2)分别迭代式(2)(3)，取序列 $\{y_{3,i}\}$ 中前 $p-1$ 项作为采样间隔，对迭代产生的混沌序列从第 k_1+1 项开始进行抽样，生成序列 $\{x'_{1,i}\}$ 和 $\{x'_{2,i}\}$，并对其按照式(8)(9)处理，生成序列 $\{x_{1,i}\}$ 和 $\{x_{2,i}\}$。

$$x_{1,i}=floor(x'_{1,i}\times 10^6-floor(x'_{1,i}\times 10^6))\times 10^3 \bmod G,i=1,2,\cdots,p\tag{8}$$

$$x_{2,i}=floor(x'_{2,i}\times 10^6-floor(x'_{2,i}\times 10^6))\times 10^3 \bmod G,i=1,2,\cdots,p\tag{9}$$

(3)按照式(10)—(12)处理 $\{x_{1,i}\}$、$\{x_{2,i}\}$ 和 $\{x_{3,i}\}$ 序列生成混沌序列 $\{z_{1,i}\}$、$\{z_{2,i}\}$ 和 $\{z_{3,i}\}$，即

$$\{z_{1,i}\}=\{(x_{1,i}+x_{3,i})\bmod G\}\oplus x_{2,i}\tag{10}$$

$$\{z_{2,i}\}=\{(x_{2,i}+x_{3,i})\bmod G\}\oplus x_{1,i}\tag{11}$$

$$\{z_{3,i}\}=\{(z_{1,i}\times x_{3,i})\bmod G\}\oplus z_{2,i}\quad i=1,2,\cdots,p\tag{12}$$

式中，⊕为异或运算符号，$\{z_{1,i}\}$、$\{z_{2,i}\}$ 用于像素扩散，$\{z_{3,i}\}$ 用于块扩散，这样在扩散过程中每个像素的改变都与混沌序列 $\{x_{1,i}\}$、$\{x_{2,i}\}$、$\{x_{3,i}\}$ 均有关，同时也将影响扩散到别的像素中，即改变密钥 $[x_{10},x_{20},x_{30},\mu_1,\mu_2,\mu_3]$ 中任意一位，将导致所有像素发生变化，有一种牵一发动全军的效果。因此按照上面计算公式生成混沌序列的方式，会增加加密算法的密钥敏感性。

3）分块双层自适应扩散。此步骤通过结合 Arnold 正反向映射，不仅可以使每个像素的访问顺序及每个位置的存储顺序机会均等，增强置乱随机性，克服常规 Arnold 映射从规则到随机访问的缺陷，而且在置乱过程中采用分块双层自适应扩散，增加算法对密钥、明文的敏感性。其分块双层自适应扩散实现步骤如下：

给定密钥 $[k_1,k_2,\cdots,k_7,c_0]$。首先，对明文图像进行 Arnold 反向映射，利用式(13)获取明文图像矩阵中随机位置 (x',y') 处的明文像素值 $I(x',y')$。对初始加密矩阵进行 Arnold 正向映射，利用式(14)产生随机矩阵块位置 (g',h')，并对此随机矩阵块进行 Arnold 正向映射，利用式(15)产生此随机块中的随机位置 (k',l')。

$$\begin{pmatrix}x'\\y'\end{pmatrix}=\begin{pmatrix}1&p_1\\q_1&p_1q_1+1\end{pmatrix}\begin{pmatrix}x\\y\end{pmatrix}\bmod\begin{pmatrix}m\\n\end{pmatrix}\tag{13}$$

$$\begin{pmatrix}g'\\h'\end{pmatrix}=\begin{pmatrix}1&p_2\\q_2&p_2q_2+1\end{pmatrix}\begin{pmatrix}g\\h\end{pmatrix}\bmod\begin{pmatrix}m/t\\n/t\end{pmatrix}\tag{14}$$

$$\begin{pmatrix}k'\\l'\end{pmatrix}=\begin{pmatrix}1&p_3\\q_3&p_3q_3+1\end{pmatrix}\begin{pmatrix}k\\l\end{pmatrix}\bmod\begin{pmatrix}t\\t\end{pmatrix}\quad x=1,2,\cdots t;y=1,2,\cdots,t\tag{15}$$

式中，$p_1=z_1(1)$，$q_1=n/gcd(m,n)$，$p_2=z_2(1)$，$q_2=(n/t)/gcd(m/t,n/t)$，$p_3=z_3(1)$，$q_3=t/gcd(t,t)$，$gcd(m,n)$ 表示求 m,n 的最大公约数。

(1)块内随机像素扩散。将随机像素 $I(x',y')$ 按式(16)(17)进行像素替换、扩散处理，并存入大小为 $t\times t$ 过渡矩阵块 $\boldsymbol{C}$ 的 (k',l') 位置。

若 $k'\bmod 2=1$，则

$$C(k',l')=((I(x',y')+c)\bmod 256)\oplus z_1(t\times(k-1)+l)\tag{16}$$

否则

$$C(k',l')=((I(x',y')+c)\bmod 256)\oplus z_2(t\times(k-1)+l)\tag{17}$$

式中，c 为前一个处理过的随机像素。当 $x=1,y=1$ 时，$c=c_0$，直至填满矩阵块 $\boldsymbol{C}$。

(2)随机矩阵块扩散。为达到较佳置乱和扩散

效果,对已填满的过渡矩阵块 $\boldsymbol{C}$ 按式(18)进行块扩散处理,并存入加密矩阵 $\boldsymbol{E}$ 中(g',h')处的随机块内。

$$E(g',h') = ((\boldsymbol{C} + \boldsymbol{C}') \bmod 256) \oplus \boldsymbol{Z}_3 \tag{18}$$

式中,$\boldsymbol{C}'$为前一个随机加密矩阵块;当 $g=1, h=1$ 时,$\boldsymbol{C}' = \boldsymbol{C}_0$;$\boldsymbol{w} = (z_1 + z_2 + z_3) \bmod G$ 是长度为 p 的随机序列;$\boldsymbol{C}_0$ 是由 $\boldsymbol{w}$ 序列生成 $t \times t$ 矩阵块;$\boldsymbol{Z}_3$ 是混沌序列 z_3 转化的 $t \times t$ 矩阵块。

(3) 密钥扰动。将当前(g',h')处加密矩阵块中的像素作为扰动因子,按以下方式扰动混沌系统:

设 $M = \left(\sum_{i=1}^{t}\sum_{j=1}^{t} E_{i,j}\right) \bmod G$, $N = \bigoplus_{i=1}^{t}\bigoplus_{j=1}^{t} E_{i,j}$, 利用 M、N 产生 Logistic-Tent 映射、Logistic-Sine 映射及 Tent-Sine 映射混沌系统新的参数和初始值。

Logistic-Tent 映射

$$\begin{aligned} \mu_1 &= [k_2 + 2(M+N+1)/G]/2 \\ x_{10} &= (k_3 + MN)/256^2 \end{aligned} \tag{19}$$

Logistic-Sine 映射

$$\begin{aligned} \mu_2 &= [k_4 + 2(M+N+1)/G]/2 \\ x_{20} &= (k_5 + MN)/256^2 \end{aligned} \tag{20}$$

Tent-Sine 映射

$$\begin{aligned} \mu_3 &= [k_6 + 2(M+N+1)/G]/2 \\ x_{30} &= (k_7 + MN)/256^2 \end{aligned} \tag{21}$$

上述扰动密钥方式不仅可以使密文像素的影响扩散到整幅图像,从而增强加密图像对密钥、密文及明文的敏感性,而且 $k_1, k_2, \cdots, k_7, c_0$ 的引入可以增大密钥空间。

利用上述系统产生的参数和初始值,对混沌系统进行扰动,产生新的混沌序列 z_1、z_2、z_3,供下一个随机加密块生成使用。依此类推,直至把 $\boldsymbol{E}$ 填满,从而自适应完成加密,并生成加密图像矩阵 $\boldsymbol{E}$。

解密是加密的逆过程。

3 仿真结果与分析

基于 Matlab R2010b 平台,选取了大小为 512×512 像素的 baboon、Barb、Elaine、sailboat、peppers、gray-scale,及大小为 256×256 像素的 fingerprint、Lena 多幅标准测试图像进行加密仿真实验。

设加密密钥为 $[x_{10}, x_{20}, x_{30}, \mu_1, \mu_2, \mu_3]$ = [0.567 8, 0.432 1, 0.378 9, 2.134 5, 3.136 7, 1.122 1] $[k_1, k_2, k_3, k_4, k_5, k_6, k_7, c_0]$ = [123, 1.432, 0.123 4, 2.341, 1.234 5, 3.456, 2.345 6, 222],按照 BDAM 算法加密步骤对图像进行加密。图 2 为 4 种明文图像、BDAM 密文图像及其直方图。

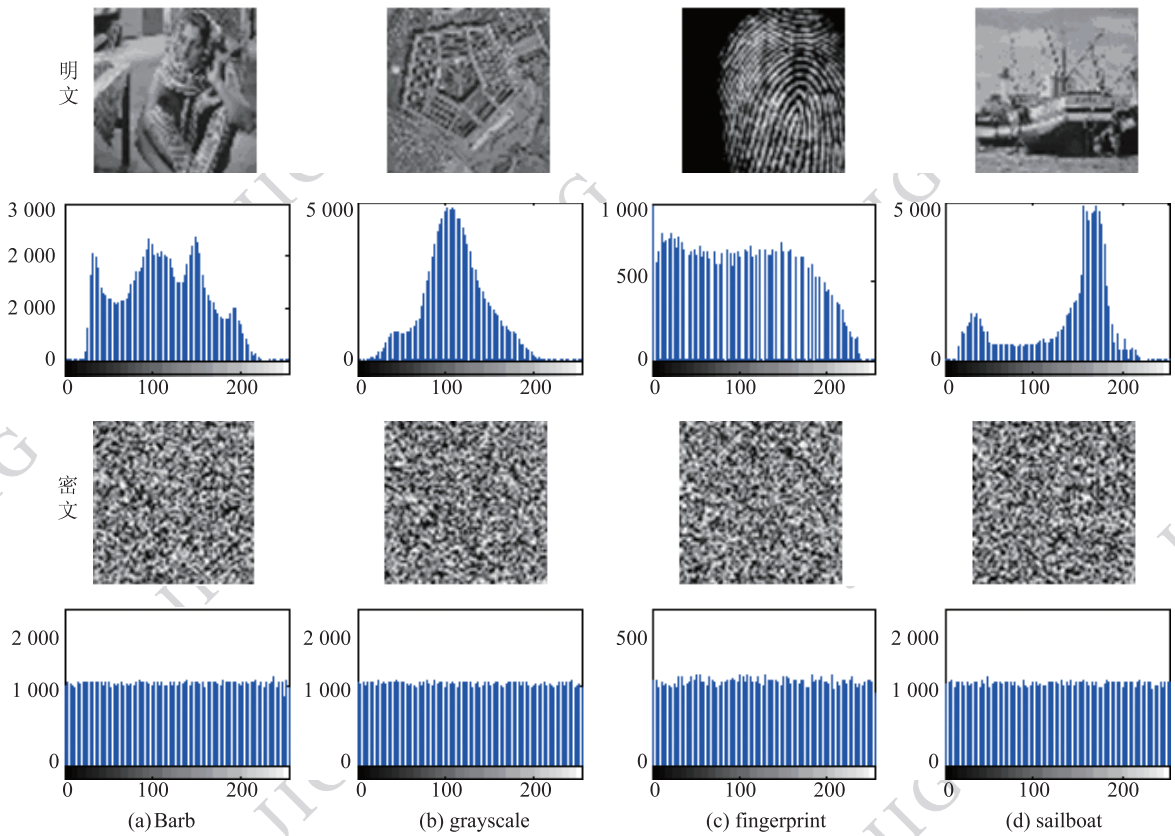


图 2 4 种测试图像的明文、BDAM 密文图像及其直方图

Fig. 2 Plain images, encryption images with BDAM algorithm, and their corresponding histograms for four test images

由图 2 可知，图像加密前后的直方图差别较大，加密后图像矩阵的直方图呈均匀分布，说明各像素出现频率非常接近，可较好地掩盖明文图像分布规律。图 2 结果表明 BDAM 算法能够有效抵御统计分析攻击和已知密文攻击。

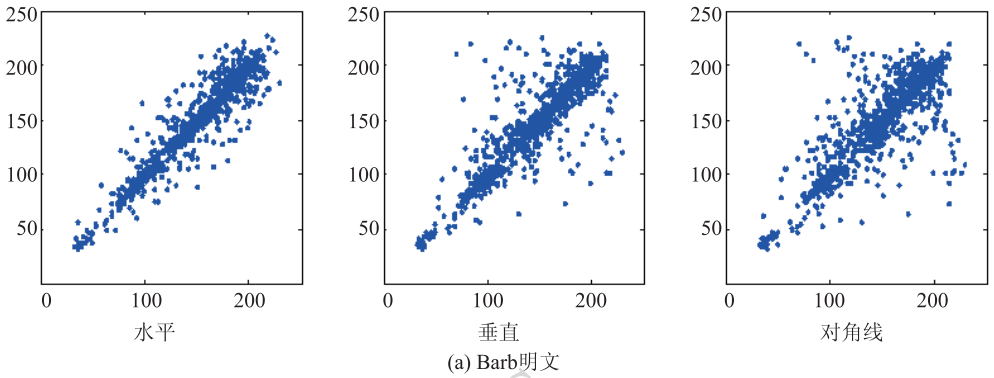
3.1　明文图像和密文图像相邻像素相关性分析

为了进一步研究 BDAM 算法抵御统计攻击性能，选用 Barb、baboon 和 peppers 3 幅图像，与文献[1,6,8]进行对比研究。随机在 Barb 和 baboon 明文图像和密文图像中分别选择 2 000 对像素点，在 peppers 明文图像和密文图像中选择 10 000 对像素点，然后计算它们水平、垂直、对角方向相邻像素之间的相关系数[8]。表 1 为文献[1,6,8]及 BDAM 4 种算法的密文图像相邻像素相关系数对比结果，图 3为 Barb 明文图像及 BDAM 算法密文图像在水平、垂直、对角方向上相邻像素分布图。

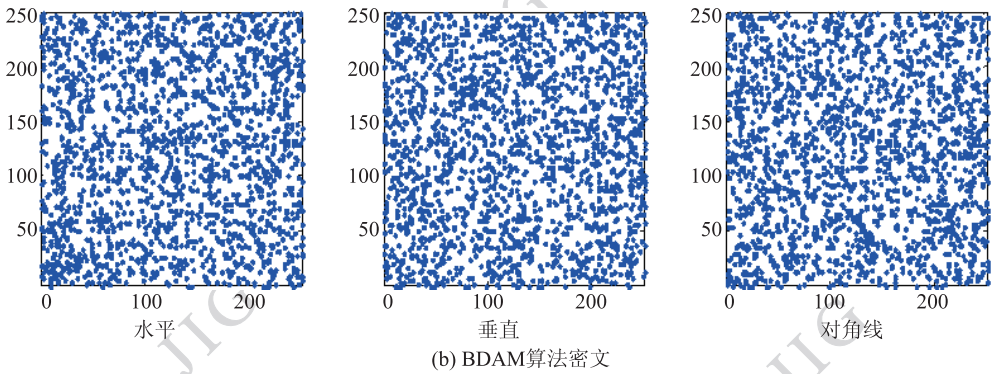
表 1　4 种算法明/密文图像相邻像素相关系数

Table 1　Correlation coefficients between two adjacent pixels in plain/cipher images with four algorithms

测试图像	算法	水平方向	垂直方向	对角线方向
baboon	明文	0.866 40	0.749 63	0.708 43
	BDAM	$-1.056\,3\times10^{-4}$	$-4.966\,8\times10^{-5}$	$8.448\,0\times10^{-5}$
	文献[1]	0.002 747	0.002 014	−0.001 647
	文献[6]	$-4.188\,7\times10^{-4}$	$-8.295\,1\times10^{-4}$	$1.096\,9\times10^{-4}$
Barb	明文	0.860 6	0.959 8	0.877 4
	BDAM	$-1.369\,5\times10^{-4}$	$-1.228\,7\times10^{-4}$	$6.163\,8\times10^{-4}$
	文献[1]	$9.149\,1\times10^{-4}$	−0.002 561	0.001 464
	文献[6]	$3.334\,4\times10^{-4}$	$-9.892\,8\times10^{-4}$	−0.002 428
peppers	明文	0.968 05	0.970 30	0.927 48
	BDAM	$-2.614\,2\times10^{-4}$	$-9.481\,1\times10^{-5}$	-3×10^{-4}
	文献[8]	−0.009 13	−0.001 88	0.001 08



(a) Barb明文



(b) BDAM算法密文

图 3　Barb 明文图像及其 BDAM 算法密文图像在水平、垂直和对角方向上的相邻像素分布

Fig. 3　Distribution of adjacent pixels in horizontal, vertical and diagonal directions in plain/cipher images of Barb image

由表 1 可知,3 幅明文图像相邻像素之间均存在着较大的相关性,4 种算法的密文图像相邻像素之间相关性远小于明文图像。但 BDAM 算法的密文图像相邻像素相关系数绝对值比文献[1]算法的相关系数绝对值小 1 ～2 个数量级,比文献[6]算法的相关系数绝对值约小 1 个数量级,比文献[8]的相关系数绝对值小 1 ～2 个数量级。由此可知,BDAM 算法中采用将 Arnold 双向映射结合,并对初始加密矩阵分块,将明文图像中随机像素存入随机块内随机位置的这种置乱方法,其置乱效果优于文献[1,6,8]中的置乱方法。

从图 3 可看出,明文图像在 3 个方向上的相邻像素几乎分布在一条直线上,而 BDAM 算法的密文图像在 3 个方向上的相邻像素杂乱无章均匀分布于整个像素空间,进一步表明 BDAM 算法的置乱效果好。因此, BDAM 算法有较强的抵抗统计分析能力。

3.2 信息熵分析

信息熵描述信息不确定度,反映图像中的灰度分布情况[1]。理论上,对于 8 位二进制表示的灰度图像,理想情况下密文图像的信息熵应该等于 8。为了研究 BDAM 算法抵御熵攻击性能,选用 Barb、peppers 和 Elaine 3 幅测试图像,计算它们的 BDAM 算法加密图像信息熵,并与文献[1,6,8]进行对比研究。结果如表 2 所示。

表 2 4 种算法的密文图像信息熵

Table 2 Information entropy of cipher-image by the four schemes

测试图像	文献[1]算法	文献[6]算法	文献[8]算法	BDAM 算法
Barb	—	7.991 41	—	7.999 30
peppers	—	7.991 63	7.997 30	7.999 34
Elaine	7.999 22	7.991 80	—	7.999 26

由表 2 可知,BDAM 算法所测密文图像的信息熵非常接近于理论值 8,且大于文献[1,6,8]中信息熵,可见,本文的 BDAM 算法具更强抵御熵攻击的能力。

3.3 密钥空间分析

BDAM 算法的密钥包括 $[x_{10}, x_{20}, x_{30}, \mu_1, \mu_2, \mu_3, k_1, k_2, k_3, k_4, k_5, k_6, k_7, c_0]$,$k_1$、$c_0$ 为 8 位二进制数,其余均为双精度型,且 $[x_{10}, x_{20}, x_{30}] \in (0,1)$、$[\mu_1, \mu_2, \mu_3, k_2, k_4, k_6] \in (0,4)$、$[k_3, k_5, k_7] \in (0,256)$。BDAM 算法对每个密钥敏感性不同,由实验得出该算法对密钥 x_{10}、x_{20}、x_{30}、k_3 的敏感度均为 10^{-16},对密钥 μ_1、μ_2、μ_3、k_2、k_4、k_5、k_6、k_7 的敏感度均为 10^{-15}。算法每个密钥的密钥空间等于其取值范围与其敏感度的比值,而总密钥空间为所有相互独立密钥空间的乘积,因此,BDAM 算法的密钥空间为 $V = 2^{8\times 2} \times 256 \times \left(\frac{1}{10^{-16}}\right)^4 \times 4^6 \times 256^2 \times \left(\frac{1}{10^{-15}}\right)^8 > 10^{199}$。BDAM 算法与文献[1,6,8]算法的密钥空间对比结果如表 3 所示。

表 3 4 种算法的密钥空间对比

Table 3 Comparison of key space with four algorithms

	BDAM	文献[1]	文献[6]	文献[8]
密钥空间	$>10^{199}$	10^{128}	10^{84}	10^{79}

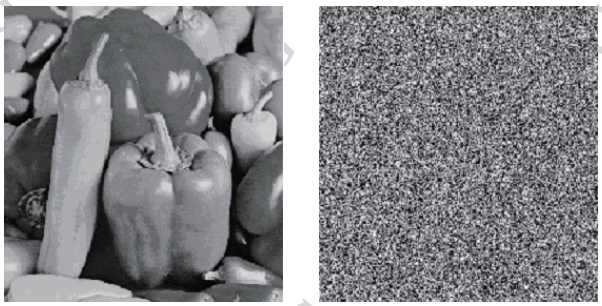
由表 3 可知 BDAM 算法的密钥空间大于文献[1,6,8]算法的密钥空间,因此,BDAM 算法可以更好地抵御穷举法的攻击。

3.4 密钥敏感性分析

为分析 BDAM 算法的密钥敏感性,选取 peppers 图像进行解密测试,图 4(a)为正确解密得到的图像,图 4(b)为在其他解密密钥保持不变,只有解密密钥 $x_{10} = 0.567\,8$ 改为 $x_{10} = 0.567\,8 + 10^{-16}$ 时所获得的解密图像。由此可见,当密钥仅发生 10^{-16} 微小变化时,也不能正确解密,从而表明 BDAM 算法密钥敏感性较高。

3.5 抗差分攻击能力分析

为研究 BDAM 算法的抗差分攻击性能,选用



(a) 正确解密图像　　(b) 错误解密图像

图 4 解密图像

Fig. 4 The decryption image

Barb 和 Lena 两幅图像，与文献[1,6,8]进行对比研究。如果加密算法对明文的敏感性越强，其抵抗差分攻击的能力也就越强，因而采用像素数改变率(NPCR)[8]和归一化像素值平均改变强度(UACI)[8]度量加密算法对明文的敏感性。本文实验中，将 Barb、Lena 图像(1,1)处的像素值分别加 1，得到新的明文图像，分别利用加密算法对改变前后的两组明文图像用相同密钥加密，得到相应的两组密文图像，然后计算它们的 NPCR 值与 UACI 值。文献[1,6,8]和 BDAM 4 种算法的 NPCR 值与 UACI 值如表 4 所示。

表 4　4 种算法的 NPCR 与 UACI 值

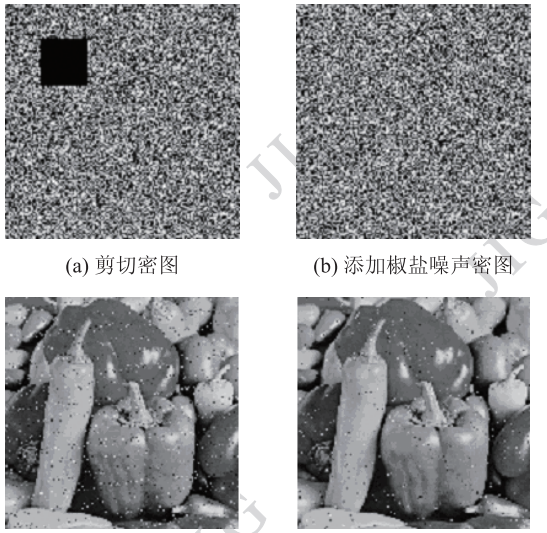
Table 4　The NPCR and UACI value with four algorithms

算法	NPCR/%		UACI/%	
	Barb	Lena	Barb	Lena
文献[1]	99.58	—	33.42	—
文献[6]	99.58	99.62	33.39	33.41
文献[8]	—	99.50	—	33.38
BDAM	99.60	99.61	33.42	33.43

由表 4 可知，与文献[1,6,8]算法相比，BDAM 算法的 NPCR 值与 UACI 值更接近理论值 99.6%、33.46%。说明 BDAM 算法采用的分块双层自适应扩散方法，可提高明文的敏感性，能有效抵抗差分攻击。

3.6　抗恶意攻击分析

实际应用中，图像在传输过程避免不了发生数据剪切或者噪声干扰等恶意攻击。为研究 BDAM 算法抗恶意攻击能力，选 peppers 的 BDAM 密文作为测试图像，分别用剪切图中任意 100×100 大小的块和在图中添加 1% 椒盐噪声对其进行攻击，并用本文解密算法恢复，结果如图 5 所示。



(a) 剪切密图　(b) 添加椒盐噪声密图

(c) 剪切密图解密图　(d) 添加椒盐噪声密图解密图

图 5　剪切和噪声攻击分析

Fig. 5　Data loss and noise attacks analysis

由图 5 可知，密文图像受剪切和噪声攻击后，恢复结果虽然受到一些噪声颗粒的影响，但仍然能较好的反映原图内容，可以获知需要了解的信息。因此，BDAM 算法对剪切、噪声等恶意攻击具有较强的鲁棒性。

3.7　时间复杂度分析

为分析 BDAM 算法的时间复杂度，选用 Lena 作为测试图像，在 Intel(R) core(TM) i5-2400 CPU @ 3.10 GHz、4 GB 内存的计算机上，将文献[6,8]中算法和本文 BDAM 算法在 Matlab R2010b 平台的加密运行时间作比较，结果如表 5 所示。

表 5　算法加密时间比较

Table 5　Comparison of the encryption time of different algorithms

	文献[6]	文献[8]	BDAM
加密时间/s	0.352	1.615	1.498

从表 5 可以看出，本文 BDAM 算法加密过程较文献[8]算法快，但是较文献[6]算法慢。这是由于本文为改善加密算法对密钥、明文的敏感性以及置乱随机性以达到较好的加密效果，采用分块双层自适应扩散方式，增加了算法时间复杂度。虽然文献[8]算法也有自适应扩散，但文献[8]将置乱扩散分开进行，因而速度较慢；而文献[6]未采用自适应扩散方式，加快了加密速率，但是对密钥的敏感性、置乱随机性相对较低。因此，本文以牺牲时间复杂度来换取较高的加密安全性。

4　结　论

本文提出一种基于 Arnold 映射的分块双层自适应扩散图像加密算法，该算法有效利用已有 1 维混沌系统产生新 1 维混沌系统，使其具有较宽的混沌范围和较好的混沌行为。通过结合 Arnold 正反

向映射,将置乱与扩散同步进行,不仅可以使每个像素的访问顺序及每个位置的存储顺序机会均等,增强置乱随机性,克服常规 Arnold 映射从规则到随机访问的缺陷,而且在置乱过程中采用分块双层自适应扩散,利用密文像素与密文像素、明文像素及混沌随机序列间的相互作用,将每个像素影响非线性地扩散到整幅图像矩阵中,并在扩散过程中不断扰动混沌系统,形成自适应扩散过程,增强加密图像对密钥、密文及明文的敏感性。实验结果及分析表明,本文加密方案适用各种类型灰度图像,密钥空间大,抵御穷举攻击能力强,对密钥及明文度敏感性高,可有效抵御选择密文攻击和选择明文攻击,密文图像相邻像素相关性小,密文图像像素分布均匀,可有效抵御统计攻击。因此,本文算法具有较高的安全性和潜在应用价值。

参考文献(References)

[1] Zhang W, Wong K W, Yu H, et al. An image encryption scheme using reverse 2-dimensional chaotic map and dependent diffusion[J]. Communications in Nonlinear Science and Numerical Simulation, 2013, 18(8): 2066-2080.

[2] Wena C, Wanga Q, Liub X, et al. An image encryption algorithm based on scrambling and chaos [J]. Joumal of Information & Computational Science, 2013, 17(10):5725-5733.

[3] Pareek N K, Patidar V, Sud K K. Diffusion-substitution based gray image encryption scheme[J]. Digital Signal Processing, 2013, 23(3): 894-901.

[4] Eslami Z, Bakhshandeh A. An improvement over an image encryption method based on total shuffling[J]. Optics Communications, 2013, 286: 51-55.

[5] Zhang L Y, Hu X, Liu Y, et al. A chaotic image encryption scheme owning temp-value feedback [J]. Communications in Nonlinear Science and Numerical Simulation, 2014, 19(10): 3653-3659.

[6] Zhou Y, Bao L, Chen C. A new 1D chaotic system for image encryption[J]. Signal Processing, 2014, 97: 172-182.

[7] Li Y Y, Zhang S W. Image compression and encryption with discrete wavelet transform and SHA-1[J]. Journal of Image and Graphics, 2013, 18(4): 376-381. [李园园, 张绍武. 小波变换和 SHA-1 相结合的图像压缩加密[J]. 中国图象图形学报, 2013, 18(4): 376-381.][DOI:10.11834/jig.20130403]

[8] Luo Y L, Du M H. Wavelet domain image encryption algorithm based on quantum Logistic mapping[J]. Journal of South China University of Technology: Natural Science Edition, 2013, (6): 53-62. [罗玉玲, 杜明辉. 基于量子 Logistic 映射的小波域图像加密算法[J]. 华南理工大学学报: 自然科学版, 2013, (6): 53-62.]

[9] Deng H T, Deng J X, Deng X M. Image compression and tree encryption synchronization algorithm based on EZW[J]. Journal of physics, 2013, 62(11): 110701(1-8). [邓海涛, 邓家先, 邓小梅. 基于 EZW 的图像压缩和树形加密同步算法[J]. 物理学报, 2013, 62(11): 110701(1-8).]

[10] Yang H Q, Liao X F, Wo Wong K, et al. Image encrption and compression algorithm based on SPIHT[J]. Journal of Physics, 2012, 61(4): 29-36. [杨华千, 廖晓峰, Wo Wong K, et al. 基于 SPIHT 的图像加密与压缩关联算法[J]. 物理学报, 2012, 61(4): 29-36.]

[11] Ye G, Wong K W. An image encryption scheme based on time-delay and hyperchaotic system[J]. Nonlinear Dynamics, 2013, 71(1-2): 259-267.

[12] Wang J, Jiang G P. Image scrambling and mixing encryption algorithm based on hyper-chaotic system[C]//Proceedings of the 32nd Chinese Control Conference. Xi′an: IEEE, 2013: 459-464.

[13] Peng J, Jin S, Lei L, et al. Research on a novel image encryption algorithm based on the hybrid of chaotic maps and DNA encoding[C]// Proceedings of the 12th IEEE International Conference on Cognitive Informatics & Cognitive Computing. New York: IEEE, 2013: 403-408.