数字图像空域加密技术综述

黄林荃[1],刘 会[2],赵 波[2*]
(1.武汉软件工程职业学院 信息学院,湖北 武汉 430205;
2.武汉大学 国家网络安全学院,湖北 武汉 430079)

摘 要:数字图像包含了大量可视化的隐私信息,其在公共信道的安全传输和云环境下的可信存储难以得到充分的保障。数字图像加密技术作为一种重要的隐私保护手段被广泛应用于各个领域。数字图像空域加密指将图像看作二维矩阵,从灰度值和像素坐标两个方面对图像进行可逆变换。数字图像的空域加密结构包括置乱与扩散。置乱是指通过改变像素的坐标实现对像素位置信息的隐藏;扩散是指建立密文图像与明文图像之间的强关联,保证加密算法的错误传播无界特性。该文详细介绍了现阶段4类主流的数字图像空域加密方法,对比分析不同空域加密的优缺点,给出7种常用的数字图像加密技术安全性的评估方法,并指出未来可能的数字图像加密技术的研究方向,提供数字图像加密技术的整体概述。

关键词:数字图像;可信存储;可逆变换;空域加密;错误传播无界
中图分类号:TP309 **文献标识码**:A **文章编号**:1673-629X(2021)01-0137-05
doi:10.3969/j.issn.1673-629X.2021.01.025

Survey of Digital Image Spatial-domain Encryption Technology

HUANG Lin-quan[1],LIU Hui[2],ZHAO Bo[2*]
(1.School of Information,Wuhan Vocational College of Software and Engineering,Wuhan 430205,China;
2.School of Cyber Science and Engineering,Wuhan University,Wuhan 430079,China)

Abstract:Digital image contains a large amount of visual privacy information,which is difficult to be fully guaranteed in the secure transmission of public channels and trusted storage in the cloud environment. As an important means of privacy protection,digital image encryption technology has been widely used in various fields. The spatial-domain encryption of digital image refers to the reversible transformation of image from two aspects of gray-level value and pixel coordinates by treating the image as a two-dimensional matrix. The spatial-domain encryption structure includes scrambling and diffusion. Scrambling refers to the hiding of pixel position information by changing pixel coordinates. Diffusion refers to the establishment of strong correlation between cipher-image and plain-image to ensure the unbounded error propagation of the encryption algorithm. We introduce 4 kinds of digital image spatial-domain encryption methods in detail,and compare and analyze the advantages and disadvantages of these encryption algorithms. We give 7 kinds of security evaluation methods,point out possible future research direction of digital image encryption technology,and provide overall overview of the digital image encryption technology.

Key words:digital image;trusted storage;reversible transformation;spatial-domain encryption;unbounded error propagation

0 引 言

因其可视化特性,数字图像作为一种重要的信息载体被广泛应用于各个领域。在物联网移动终端(例如智能手机、监控设备等)的场景中,数字图像包含了大量的隐私信息,而移动终端在开放的环境下容易遭受窃取或丢失,从而使得数字图像面临严峻的隐私泄露的风险。随着云计算技术的成熟,大量数字图像信息通过云平台进行计算和存储。然而,由于云计算使得数字图像在物理侧脱离了用户的控制范围,用户对云计算服务可信性的怀疑正在加剧,从而限制了数字图像在云端的使用范围。同时,5G时代的到来将进一步促进数字图像的应用,图像的安全存储和传输显得尤为重要。加密技术是一种保障数据在不可信环境下的机密性的重要手段。现阶段有许多成熟的数字加密方案,例如以AES[1-2]为代表的国际加密标准和以SM2[3]为代表的国内自主设计的国密算法,能够有效

收稿日期:2020-01-10 **修回日期**:2020-05-13
基金项目:中央高校基本科研业务费专项资金项目(2042017kf024);武汉市应用基础前沿项目(2018010401011295)
作者简介:黄林荃(1991-),女,硕士,研究方向为计算机视觉、多媒体安全;赵 波,博士,教授,CCF高级会员(09009S),研究方向为信息安全、可信计算。

地保障数据的机密性。然而,由于图像的二维性、冗余性和相邻像素高的相关性,传统的加密技术无法为图像提供安全高效的保障。因此,安全高效的数字图像加密算法的设计显得尤为重要。

1 相关工作介绍

现阶段许多研究人员充分利用数字图像的特点设计复杂环境下图像加密的方案。按加密域的不同,数字图像加密可以分为频域加密和空域加密两类。频域加密是从频域空间对图像进行处理,利用离散余弦变换[4]、傅里叶变换[5-6]等频域变换方法实现图像加密。频域加密方案的特点是加密速度快,通常属于有损加密,即解密图像与明文图像存在少量差异。空域加密是指将数字图像作为二维矩阵,从空间的角度对二维矩阵进行可逆变换。常用的空域图像加密方案包括置乱和扩散两个阶段[7-8]。置乱是指对数字图像的像素坐标进行可逆变换,改变现有像素的空间信息以达到掩盖明文图像空间信息的目的。扩散是指从灰度值的角度建立像素值与整个密文图像的关联,使得当明文图像中任意像素遭到篡改后,密文图像以不可预测的方式改变,从而抵御选择明文攻击、差分攻击等先进的攻击手段。

近年来,基于混沌理论[9-11]的数字图像空域加密方案取得了飞速发展。混沌系统具有初始条件敏感性、遍历性和混合性等优点,符合密码学要求。基于混沌理论的图像加密算法通常利用混沌系统产生的伪随机序列对图像的像素值进行加密。Chai X 等人[9]利用四翼超混沌系统提供伪随机混沌序列,生成 DNA 编码和计算规则,实现基于动态 DNA 的图像加密算法。Akhshani A 等人[10]证明了最低次量子修正产生量子混沌映射,并首次将量子混沌映射运用于图像加密领域,取得了良好的加密效果。为进一步增强混沌映射结构的复杂性、提高混沌系统的混合性,朱和贵等人[11]提出了一种复合一维 Sine 和 Tent 混沌的二维超混沌系统,通过提升复合混沌系统的混沌性来增强图像加密算法的随机性。

Arnold 变换[12-13]是空域加密中非常重要的置换方法,旨在改变像素值在图像中的位置。通过将图像中所有像素的坐标带入 Arnold 变换中,计算出新的坐标,并将像素值置换至新坐标中,实现像素值空间位置的变换。为了改善传统二维离散 Arnold 变换的置乱和加密效果,吴成茂等人[12]提出了一种新的非线性图像置乱变换。该方法利用经典离散标准映射的构造思想,将经典二维离散 Arnold 变换中同余方程输出结果的非线性表达式嵌入到另一个二维离散 Arnold 变换的同余方程的输入项,并在离散 Arnold 变换的基础上构造了一种具有良好非线性特性的新变换,以快速提高灰度图像的置乱效果。针对 Arnold 变换周期性的问题,黄林荃等人[13]在 Arnold 置换的同时引入了非线性变换,消除 Arnold 变换周期性对图像加密算法安全性的影响。

以 DNA 计算[14-16]为代表的生物计算推动了数字图像在空域加密方面的发展。基于 DNA 计算的图像加密算法通过对图像像素值进行 DNA 编码、DNA 计算和 DNA 解码,实现像素值的修改,属于灰度加密范畴。为了提高密文图像的伪随机性,李桂珍等人[14]提出了一种基于 DNA 合成图像混沌映射的彩色图像加密算法,通过重复使用 DNA 的编码和计算规则提高加密算法的复杂性,使图像加密算法具备更高的伪随机性。针对遥感图像相邻像素相关性高的特点,Liu H 等人[15]利用置换过程不改变密文 DNA 碱基数量的特点,构建了图像与所有像素之间的关联,保障了图像加密算法的扩散性。Zhu C 等人[16]研究三维 DNA 计算的特性,提出了一种基于三维 DNA 水平置换和代换的图像加密算法,并模拟多种典型的攻击手段测试该算法的安全性和可用性。

S 盒(substitution-box)[17-18]是密码学中对称密钥加密算法执行替换计算的基本结构。基于 S 盒代换的图像加密算法利用显示查找表(look-up-table)构建明文图像与密文图像的映射关系。Zhang Y[17]改进了传统 S 盒代换结构简单的设计,提出了一种新的快速图像加密系统。该系统采用分段线性混沌映射和三维 S 盒生成具有良好统计特性的密钥流,设计出具有相同加/解密过程的图像加密算法,实际应用中仅需要部署一套算法就能同时实现图像加/解密过程。Silva V M 等人[18]考虑到静态 S 盒难以抵御代数攻击,利用混沌系统设计出高度非线性的动态 S 盒,实现了彩色图像的无损加密。实验表明该算法具备高度的随机性,能以稳健的方式对视频信息实时加密。

2 空域加密方案分析

2.1 混沌理论

混沌[9-11]是指发生在确定性系统中看似随机的不规则运动。一个确定性理论描述的系统,其行为表现出不确定、不可重复和不可预测的特点,这种现象被称为混沌现象。由于初始值敏感性、参数敏感性、遍历性和伪随机性,混沌系统在数字图像空域加密领域得到了广泛的应用。常用的混沌系统包括四翼超混沌系统[9]、量子混沌系统[10]、Tent 混沌系统[11],以及这些经典混沌系统的变形和组合。然而,基于混沌理论的空域加密需要多次迭代混沌系统产生伪随机序列,并参与到图像加密的过程中,产生了大量的时间和空间

开销。而且,混沌系统的计算是链式计算结构,不支持并行计算,难以适用于需要高并行计算的场景。此外,图像加密算法的安全性并不等价于混沌系统的可靠性。攻击者通常不会尝试通过攻击混沌系统达到破译加密算法的目的,而是从混沌系统产生的伪随机序列与明文图像的结合中寻找攻击图像加密算法的线索,例如差分攻击、选择明文攻击等。因此,基于混沌理论的数字图像空域加密方案的安全性很大程度上依赖于混沌序列在加密过程中的运用和结合。

2.2　Arnold 变换

经典 Arnold 变换[12-13]通过计算图像的坐标实现对图像的快速置乱。由于 Arnold 变换是双射变换,所以多次迭代的 Arnold 变换也是双射变换。经典 Arnold 变换是一个二维可逆映射,其表达形式如下:

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = A \begin{bmatrix} x \\ y \end{bmatrix} (\mathrm{mod} N), A = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \quad (1)$$

其中,坐标 $(x,y)^{\mathrm{T}}$ 是 $N \times N$ 图像上的点,经 Arnold 变换后变成坐标 $(x',y')^{\mathrm{T}}$。在经典 Arnold 变换的基础上,研究人员相继提出了广义 Arnold 变换、三维 Arnold 变换、带密钥的 Arnold 变换等,这些变换改进了 Arnold 变换密钥空间不足、单次置乱效果不佳的缺陷,实现了在少数次迭代下良好的置乱效果。然而,经典 Arnold 变换具有两个严重缺陷,一是离散形式的 Arnold 变换具有周期性,二是只能对长和高相等的图像实现置换。在周期性方面,对于大小为 256×256 图像,其 Arnold 变换周期为 192,即攻击者只需要 192 次 Arnold 变换就能获取明文图像。Arnold 变化通常需要结合具有非周期性的非线性或线性变换解决这种周期性问题。对于等长图像的限制,加密算法需要对图像进行预处理,包括填充、分块等,以满足 Arnold 变换的计算特点。

2.3　DNA 计算

DNA 加密[14-16]是以 DNA 为信息载体,通过 DNA 计算实现的类生物加密方案。DNA 计算具有许多良好的特性,例如高平行、大存储和低能耗。DNA 代表着生物特征的遗传信息,是一种由四种核苷酸组成的分子结构,即腺嘌呤(A),胸腺嘧啶(T),胞嘧啶(C),鸟嘌呤(G)。两条单链 DNA 序列利用碱基互补配对规则通过氢键相互连接,其中,A 与 T 配对,C 与 G 配对。DNA 编码的 8 种组合方案如表 1 所示。

表 1　DNA 编码规则

规则	规则 1	规则 2	规则 3	规则 4	规则 5	规则 6	规则 7	规则 8
00	A	A	T	T	C	C	G	G
01	C	G	C	G	A	T	A	T
10	G	C	G	C	T	A	T	A
11	T	T	A	A	G	G	C	C

基于 DNA 计算的图像加密算法通过利用 DNA 编码的多样性实现对像素的灰度加密。对于 256 阶的单频道图像,每 8 位可以表示位长度为 4 的 DNA 序列。灰度值通过某种 DNA 编码规则编码,利用不同的规则解码并实现了图像灰度值加密。加密算法只需要掌握编码规则的选择即能控制图像加解密过程。基于 DNA 的数字图像空域加密算法的优点在于支持高并行计算,适用于遥感图像、医学影像等满足并行计算环境的场景。其缺点是加解密算法需要消耗大量的时间进行图像 DNA 编码和 DNA 计算。因此在不支持高并行计算的场景下,这类加密算法的加解密效率非常低。

2.4　S 盒代换

在图像加密领域,S 盒代换作为一种高度非线性变化常常用于图像的混淆,即使得明文与密文、密钥与密文之间的统计相关性尽可能小,以抵御统计分析攻击。许多加密算法中的非线性变换仅由 S 盒提供,因此图像加密算法的安全性很大程度上依赖于 S 盒的性能。对于包含 2^8 色阶的图像,S 盒通常将 8 位明文像素值分为高 4 位和低 4 位,然后根据显示查找表得到代换后的值,作为密文保存。

S 盒代换利用显示查找表建立明文图像与密文图像的非线性映射关系,使明文与密文、密文与密钥之间的关系更加复杂,从而提升了加密算法抵御统计分析攻击的能力。进一步,S 盒代换支持高并行计算,且 S 盒代换及其逆变换运用同一套运算体系,因此在某些场景下基于 S 盒代换的图像加密算法在时间和空间方面可以进一步优化。然而,传统密码学采用代数方式构建 S 盒,虽然可以获得高度的非线性,但由于结构简单,难以抵御差分-代数攻击。因此在 S 盒构建中,通常需要引入混沌理论、动态特性等,使 S 盒代换更为安全可靠,但也产生了一定的时间空间开销,从而降低了图像加密算法的运算效率。

3　加密系统安全评估方法

3.1　直方图分析

直方图[19]直观地反映了图像中各个灰度值的分布情况。明文图像的直方图表现出明显的统计规律,

针对统计规律的攻击方案被称为统计分析攻击。统计分析攻击是指攻击者通过分析密文和明文的统计规律来破译密码。攻击者对截获的密文图像进行统计分析,总结出其间的统计规律,并与明文的统计规律进行比较,从中提取明文图像和密文图像之间的变换关系,以达到攻击加密方案的目的。因此,加密算法应尽可能掩盖密文图像的统计信息,使密文图像的像素直方图趋近于一致,增加攻击者构建明文图像与密文图像变换关系的难度。直方图的方差能有效量化加密算法抵御统计分析攻击能力,其计算方法如下:

$$\mathrm{var}(Z)=\frac{1}{256^2}\sum_{i=1}^{256}\sum_{j=1}^{256}\frac{1}{2}(z_i-z_j)^2 \tag{2}$$

其中,$Z=\{z_1,z_2,\cdots,z_{256}\}$,$z_i$ 和 z_j 表示像素值分别等于 i 和 j 的数量。直方图方差能够准确量化图像中的像素分布情况。方差越小,说明像素分布越均匀,图像显示的统计信息就越少,图像加密方案就越安全。

3.2 相关性分析

相关性分析[19-20]是指对两个或多个具备相关性的变量元素进行分析,从而衡量变量之间的相关密切程度。由于图像相邻像素之间的相关性非常高,攻击者可以利用该特性推理预测出下一个像素的灰度值,从而实现对整个明文图像的恢复。为了抵御类似攻击,加密算法应保证密文图像尽可能少地显示相邻像素的相关性。考虑到图像的二维特性,像素的相邻关系应该至少包括水平相关、竖直相关和对角线相关。对应的相关性分析包括相邻像素的水平相关性、竖直相关性和对角线相关性。相邻像素相关性计算方法如下:

$$\begin{cases}E=\dfrac{1}{N}\sum_{i=1}^{N}x_i\\ D(x)=\dfrac{1}{N}\sum_{i=1}^{N}(x_i-E(x))^2\\ \mathrm{Cov}(x,y)=\dfrac{1}{N}\sum_{i=1}^{N}(x_i-E(x))(y_i-E(y))\\ r_{xy}=\dfrac{\mathrm{Cov}(x,y)}{\sqrt{D(x)}\ \sqrt{D(y)}}\end{cases} \tag{3}$$

其中,x_i、y_i 分别表示相邻两像素的像素值,r_{xy} 即为两相邻像素的相关性。通常,明文图像相邻像素的相关性接近 1,而密文图像相邻像素的相关性应该接近于 0。

3.3 信息熵

信息论之父克劳德·香农给出的信息熵的三个性质:单调性,发生概率越高的事件其携带的信息量越低;非负性,信息熵作为一种广度量,非负性是一种合理的必然;累加性,多随机事件同时发生存在的总不确定性的量度是可以表示为各事件不确定性的量度之和。在图形图像处理领域,信息熵[17,21]用来量化图像所包含的信息量的多少,其计算方法如下:

$$H(s)=-\sum_{i=0}^{2^n-1}p(s_i)\log_2 p(s_i) \tag{4}$$

其中,$p(s_i)$ 是信号 s_i 出现的概率。对于 256 阶的灰度图像,密文图像理想的信息熵为 8。密文图像的信息熵越接近于 8,说明其包含的信息量越少,攻击者难以从密文图像中获取有用的信息,因此加密算法安全性越高。

3.4 差分攻击

差分攻击[22-23]是指攻击者对大小为 $M\times N$ 的图像 P 做少量改动得到 P',分别利用相同的安全密钥加密 P 和 P' 得到 C 和 C',比较 C 和 C' 的区别以找到攻击图像加密方案的线索。当 C 和 C' 表现出较大差异时,攻击者就难以实施差分攻击。在图像加密领域,衡量两张图像的差异有两个非常重要的变量:像素改变率(number of pixels change rate,NPCR)和一致平均改变强度(unified average changing intensity,UACI),其计算方式如下:

$$\begin{cases}D(i,j)=\begin{cases}0, C(i,j)=C'(i,j)\\ 1, C(i,j)\neq C'(i,j)\end{cases}\\ \mathrm{NPCR}=\dfrac{\sum_{i,j}D(i,j)}{M\times N}\times 100\%\end{cases} \tag{5}$$

$$\mathrm{UACI}=\frac{1}{M\times N}\left[\sum_{i,j}\frac{|C(i,j)-C'(i,j)|}{255}\right]\times 100\% \tag{6}$$

像素改变率 NPCR 反映了两张图像相同位置不相等的像素的个数占图像所有像素个数的比例;一直平均改变强度 UACI 反映了两张图像相同位置像素灰度值的差异。假设两张图像的像素值完全随机,NPCR = 99.609 4%,UACI = 33.463 5%。

3.5 密钥敏感度测试

密钥敏感度测试[24]是为了检测加密算法对安全密钥的灵敏程度。当攻击者对密钥做少量改动(哪怕只修改 1 位),如果加密算法以不可预测的方式生成完全不同的密文图像,则说明该加密算法对安全密钥的敏感度高。密钥敏感度测试可以通过修改安全密钥 K 中的某一位得到 K',利用 K 和 K' 加密同一张图像得到 C 和 C',采用像素改变率 NPCR 和一直平均改变强度 UACI 量化两张密文图像的差别。NPCR 和 UACI 越接近理想值,说明加密算法对安全密钥的敏感度越强,加密算法越安全。

3.6 密钥空间分析

密钥空间的大小取决于安全密钥的长度。对于长度为 L 的二进制安全密钥,其密钥空间大小为 2^L,即攻击者想要通过暴力攻击的手段攻击加密系统,理论

上需要计算 2^L 次才能保证一定能攻击成功。以现阶段计算机的计算能力来看,当安全密钥长度 $L=128$,即密钥空间大小为 2^{128} 时,加密算法能抵御任何形式的暴力攻击[20,25]。

3.7　时间和空间开销分析

加密算法的时间和空间开销是衡量加密算法性能的重要指标之一[9,26-27]。特别是在物联网环境下,移动终端难以提供充足的计算能力和存储资源,加密算法的时间和空间开销分析显得尤为重要。时间开销分析通常包括加/解密算法的时间复杂度分析和模拟平台测试的真实的加/解密运行速度,通过对算法的时间复杂度的分析从理论上证明图像加密算法在效率上的可行性,同时将该加密算法部署在测试平台,给出实际加/解密效率的结果。空间开销分析是指分析图像加密算法在加/解密过程中占用的最大内存单元,给出模拟平台下需要的最大内存资源。

4　结束语

在互联共享的时代,数字图像安全在公共信道的传输和不可信第三方的存储过程中难以得到保障,使得个人隐私面临严峻的隐私泄露的风险。图像加密是一种常用的保护数据机密性的重要技术手段。数字图像空域加密方案充分利用了数字图像的二维性、冗余性等,从像素坐标和灰度值两个方面构建置乱+扩散的加密模型,保障数字图像的机密性。基于不同理论的图像加密算法具备各自的优势,通过对比各种理论基础的空域图像加密算法可以为用户根据自身场景下选择合适的图像加密方案。该文还列举了重要的分析图像安全性的指标,提供了详尽的安全性评估方法。

未来的研究中,考虑到感知层计算能力的局限性和图像信号的稀疏结构,结合压缩感知技术的图像加密方案将是一个重要的研究方向。压缩感知技术能够充分利用数字图像的冗余性寻找欠定线性系统的稀疏解,在获取和重构稀疏或可压缩信号的同时利用图像加密技术保障感知层图像采集和传输的机密性。此外,由于数字图像加密的安全性测试无法穷尽所有可能的攻击方法,因此数字图像加密的可证明安全也是一个重要的研究方向,为数字图像加密方案提供数学上的保证。

参考文献:

[1] BANIK S, BOGDANOV A, REGAZZONI F. Compact circuits for combined AES encryption/decryption[J]. Journal of Cryptographic Engineering, 2019, 9(1): 69-83.

[2] NOOR S M, JOHN E B. Resource shared Galois field computation for energy efficient AES/CRC in IoT applications [J]. IEEE Transactions on Sustainable Computing, 2019, 4(4): 340-348.

[3] 韩在峰,赵丽敏. 一种安全 RTU 的设计与实现[J]. 电子技术应用,2018,44(7):72-75.

[4] SHAHEEN A M, SHELTAMI T R, AL-KHAROUBI T M, et al. Digital image encryption techniques for wireless sensor networks using image transformation methods: DCT and DWT[J]. Journal of Ambient Intelligence and Humanized Computing, 2019, 10(12): 4733-4750.

[5] SUI Liansheng, ZHANG Xiao, HUANG Chongtian, et al. Silhouette-free interference-based multiple-image encryption using cascaded fractional Fourier transforms[J]. Optics and Lasers in Engineering, 2019, 113: 29-37.

[6] GONDIM M A A, DE OLIVEIRA NETO J R, LIMA J B. Steerable Fourier number transform with application to image encryption[J]. Signal Processing: Image Communication, 2019, 74: 89-95.

[7] CHEN J, ZHU Z L, ZHANG L B. Exploiting self-adaptive permutation-diffusion and DNA random encoding for secure and efficient image encryption[J]. Signal Processing, 2018, 142: 340-353.

[8] NKAPKOP J D D, EFFA J, BORDA M. Chaotic encryption scheme based on a fast permutation and diffusion structure [J]. International Arab Journal of Information Technology, 2017, 14(6): 812-819.

[9] CHAI X, FU X, GAN Z, et al. A color image cryptosystem based on dynamic DNA encryption and chaos[J]. Signal Processing, 2019, 155: 44-62.

[10] AKHSHANI A, AKHAVAN A, MOBARAKI A, et al. Pseudo random number generator based on quantum chaotic map [J]. Communications in Nonlinear Science and Numerical Simulation, 2014, 19(1): 101-111.

[11] 朱和贵,蒲宝明,朱志良,等. 二维 Sine-Tent 超混沌映射及其在图像加密中的应用[J]. 小型微型计算机系统,2019,40(7):1510-1518.

[12] 吴成茂. 离散 Arnold 变换改进及其在图像置乱加密中的应用[J]. 物理学报,2014(9):090504-1-090504-20.

[13] 黄林荃,刘　会,张　牧. 改进 Arnold 变换与量子混沌的图像加密系统[J]. 小型微型计算机系统,2019,40(9):1897-1902.

[14] 李桂珍,任晓芳. 基于 DNA 合成图像和混沌映射的图像加密算法[J]. 控制工程,2018,25(7):1278-1284.

[15] LIU H, ZHAO B, HUANG L. A remote-sensing image encryption scheme using DNA bases probability and two-dimensional Logistic map[J]. IEEE Access, 2019, 7: 65450-65459.

[16] ZHU C, GAN Z, LU Y, et al. An image encryption algorithm based on 3-D DNA level permutation and substitution scheme[J]. Multimedia Tools and Applications, 2020, 79: 7227-7258.

(下转第 148 页)