一种密文图像安全性评价方案

韩 啸 熊礼治* 蒋鹏程 宋婷婷
(南京信息工程大学计算机与软件学院 江苏 南京 210044)

摘 要 在图像加密技术领域中,已存在多种图像加密方法,但很多图像加密方法因安全性不够而存在被破解的风险。现行的很多密文图像安全性评判方法,选择的参数较为单一,评价结果不够全面。对此,提出一种基于像素数量改变率、密钥空间大小、信息熵、相邻像素相关系数等多种指标参数的密文图像安全性评价方案。通过同一图像使用不同加密算法分别得到的多种指标参数横向比较,得出综合情况下安全性更好的算法。针对现阶段加密应用中使用较多的两类图像进行实验、分析和对比,结果表明方案非常有效、可靠、实用性强。

关键词 图像加密 指标参数 安全性分析

中图分类号 TP391 **文献标识码** A DOI: 10.3969/j.issn.1000-386x.2019.03.028

A CRYPTOGRAPHIC IMAGE SECURITY EVALUATION SCHEME

Han Xiao Xiong Lizhi* Jiang Pengcheng Song Tingting
(*School of Computer and Software, Nanjing University of Information Science and Technology, Nanjing 210044, Jiangsu, China*)

Abstract In the field of image encryption technology, there are many image encryption methods, but many image encryption methods are not secure enough and there is a risk of being cracked. Many existing cryptographic image security evaluation methods choose a single parameter, and the evaluation results are not comprehensive. To solve this problem, we proposed a cryptographic image security evaluation scheme based on pixel number change rate, key space size, information entropy, correlation coefficient of adjacent pixels and other index parameters. Through the horizontal comparison of various index parameters obtained by different encryption algorithms for the same image, it could be concluded which algorithm has better security under the comprehensive situation. Two kinds of images which are widely used in current encryption applications were experimented, analyzed and compared. The results show that the scheme is very effective, reliable and practical.

Keywords Image encryption Index parameter Security analysis

0 引 言

图像加密技术是目前为止主要的两种图像保护的方法之一,许多图像加密方案已被提出[1]。本文主要讨论的图像加密技术是根据图像的空间性、时间性、冗余度高、视觉可感知性等特性来设计加密算法[2]。但是密文图像仍存在着被破译的风险,这个时候就要减少被破解的可能性,所以需要提高算法的安全性[3]。由于图像加密算法种类越来越多,在选择使用哪种加密算法时,人们需要知道哪个算法相对其他算法的安全性更好,为此图像加密算法的安全性评价方法就被提出了。而目前对于加密算法安全性的评价,大多数都是对算法的单一指标参数进行比对,由于不同指标参数所针对的密文图像安全特性不同,单一的指标参数对于图像加密算法的安全性评价很有可能是片面的,不能全面地展示出密文图像的安全性能和适用场景。

为了能够综合比较不同加密算法的指标参数,本文提出一种基于多种指标参数横向比较的密文图像安全性评价方案,并设计和实现系统。本文先介绍采用的 5 种图像加密算法及其加解密步骤。然后介绍所采

收稿日期: 2018 - 09 - 16。南京信息工程大学大学生实践创新训练计划项目(201710300174)。韩啸,本科生,主研领域: 计算机软件设计。熊礼治,讲师。蒋鹏程,本科生。宋婷婷,本科生。

用算法的指标参数,如像素数量改变率、密钥空间大小、信息熵、相邻像素相关系数等,并对各个指标参数的可靠性进行分析比较。接着介绍通过 MATLAB 来实现本系统,并对文件照片和卫星地图照片这两类常用的"类图像"进行具体安全性分析。最后对全文进行总结。

1　图像加密算法

1.1　仿射变换加密

仿射变换是一种几何中常见的变换,该变换的公式如下:

$$\begin{cases} x' = ax + by + e \\ y' = cx + dy + f \end{cases} \quad \Delta = \begin{vmatrix} a & b \\ c & d \end{vmatrix} \neq 0 \tag{1}$$

本文研究整数域上的拟仿射变换。这种仿射变换一定存在逆变换,其积还是整数域上的拟仿射变换,且一一变换。它的定义是在 $\det\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \pm 1$ 时,将图像像素位置进行全局置乱,并在置乱的过程中选择性的舍入,从而实现加密的效果[4-5]。而对于仿射变换的解密过程即是对密文图像进行逆变换的过程[6]。

在这里,本文选取的密钥为:

$a = 9.484\ 911\ 376 \times 102$, $b = 1.332\ 291\ 989 \times 104$,
$c = 5.781\ 391\ 478 \times 103$, $d = 8.120\ 794\ 541 \times 104$,
$e = 1.615\ 675\ 500 \times 102$, $f = 2.275\ 588\ 209 \times 103$。

1.2　AES 加密

AES 加密算法是最常见的对称加密算法,同时属于分组加密算法,它将明文分成长度相同的几组数据。且根据 AES 加密的标准规范,分组长度只能是 128 位。而和分组长度不同,AES 加密算法的密钥长度有 3 中选择,根据 AES 密钥长度的不同,加密轮数也不同[7],如表 1 所示。

表 1　密钥长度与加密轮数

AES 类型	密钥长度(32 bits)	分组长度(32 bits)	加密轮数
AES_128	4	4	10
AES_192	6	4	12
AES_256	8	4	14

基于 AES 的图像加密需要将图像的灰度值转换为矩阵形式来计算: 以字节为单位对每一个 4×4 的矩阵按照从左上角至右上角的顺序,依次进行 AES 加密; 加密结束后再将分块按照加密时的顺序连接起来。得到的矩阵结果与原矩阵不同,即图像的灰度值产生了改变,得到置乱[8-9]。如果图像的灰度值不能正好转换成 4×4 矩阵的形式,就需要在缺少的矩阵的右下方补零,使图像的灰度值能够转换成 4×4 矩阵的形式[10]。

1.3　Tent 混沌映射加密

Yoshida 等分析研究了 Tent 映射在其不变密度和功率谱的混沌区间中的混沌行为(具有唯一最大值的分段线性连续映射)。他们发现随着最大高度的降低,在混沌区域中发生连续的波段分离过渡,并积累到过渡点进入非混沌区域,而且非周期性轨迹的时间相关函数及其功率谱在波段分离点处及其附近进行精确计算。由于 Tent 映射是拓扑共轭的,因此映射的行为在这个意义上是相同的。Tent 混沌映射计算公式如下:

$$x_{i+1} = f(x_i, \mu) \tag{2}$$

$$f(x_i, \mu) = \begin{cases} f_L(x_i, \mu) = \mu x_i & x \leqslant 0.5 \\ f_R(x_i, \mu) = \mu(1 - x_i) & x_i \geqslant 0.5 \end{cases} \tag{3}$$

1.4　混沌双重图像加密

混沌双重图像加密算法的整体原理如图 1 所示。

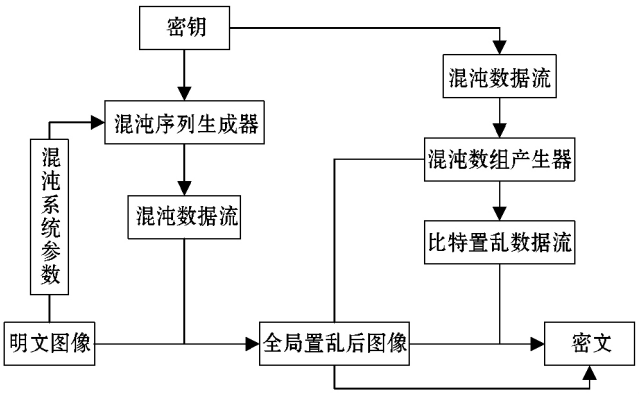

图 1　混沌双重图像加密算法的整体原理

本文的混沌双重置乱加密选取是性能优良的 Kent 映射,其表达式为:

$$F(x) = \begin{cases} \dfrac{x}{S} & x \in (0, S] \\ (1 - x)(1 - S) & x \in (S, 1) \end{cases} \tag{4}$$

当 $x \in (0,1)$、$S \in (0,1)$ 时。通过李雅普诺夫(Lyapunov)指数可以判断一个系统是否为混沌,若 Lyapunov 指数大于零,那就说明系统是混沌的。而 Kent 映射公式中就包含了一个正指数。其中初始 x_0 可以产生的任意序列,而 S 为控制参数。

混沌双重置换加密[11]的过程都是可逆的,那么说明其加密的逆操作即为解密。混沌双重置换加密是先进行全局置乱,然后对每个像素值进行替代加密[12]。而其解密就是先对密文进行反替代操作,然后根据混沌数组来计算中间密文。

1.5 频域加密

频域加密是通过将图像空域和频域进行转换来实现加密的,而它们之间的转换则是利用离散余弦变换(DCT)、快速傅里叶变换(FFT)以及小波变换(Wavelet)等实现[13]。其中相较于其他变换,离散余弦变换更好。因为它能够实现图像实时压缩、抗干扰能力强,且其算法比较简单,因此它的算法复杂度较低。所以通常优先选择离散余弦变换 DCT 的频域加密。

加密步骤如下:首先图像转化为灰度图像,将其转换成矩阵形式;然后将这个较大的矩阵划分成 8×8 的小矩阵方块,对每个小矩阵方块都进行 DCT 变换;最后量化非高频系数,以此减少需要计算的数据量,再将变换后的小矩阵方块拼起来就得到了密文图像。解密时,首先将密文图像的矩阵形式划分成小矩阵方块,然后对每个小矩阵方块进行 DCT 逆变换,最后将逆变换后的小矩阵方块拼起来就得到了原始图像。

2 密文图像安全性指标参数

2.1 像素数改变率和归一化平均改变强度

像素数量的改变率 NPCR 和归一化平均改变强度 UACI 都是衡量加密算法对明文敏感度的一个指标参数。由文献[14]可知,当 NPCR 接近 100%、UACI 接近 33%时,算法对明文更加敏感,算法的抵抗差分攻击性更好。

2.2 信息熵

在 Shanon 的信息论中,提出了信息熵的概念,它是用来反映一个信息的不确定性,并且该指标参数也可以用来反映图像信息中的不确定性,即图像的信息熵。它可以反映出图像中灰度值的分布。经分析得出:算法的信息熵的值越大,那么经过加密后得到的密文图像的灰度值分布的就越均匀,图像像素之间的关系越无法看出来,而图像信息也就不会被轻易破译。

2.3 相邻像素之间的相关系数

若已加密图像任意方向的相邻像素对的值之间都十分分散,且无关系可寻,那么它的相关系数就越接近 0,则密文图像就越难破解。

2.4 加密耗时

加密所消耗的时间长短决定了算法的时间复杂度的大小,而时间复杂度越小,那么算法的加密所需要的时间就越短,加密过程中需要承担的风险也就更小了,则该算法的安全性较好。而时间复杂度是通过一个函数公式精确地计算出算法进行加密时所需的时间。在本文中加密时间是通过记录原始图像从开始加密到生成密文图像的时间。

2.5 密钥空间大小

密钥空间的大小的单位是位,且密钥的位越长,其空间就越大[15-16]。一个好的加密算法,密钥空间应该足够大以抵抗穷举攻击。选取混沌迭代的初始值 x_0 和第二阶段所需的混沌系统的参数 S_2 作为计算密钥的参数。那么在 32 bit 计算机中双精度数据为 64 bit,则密钥空间为 $264\times264=2\ 128$。即便破译者一秒之内用数以亿计的密钥进行破译[17],也需要耗时一千多年才可以把整个密钥空间破译出来。

2.6 密钥敏感性

密钥敏感性意味着如果加密密钥不同,则会产生完全不同的密文图像;类似地,如果解密密钥不同,则基于相同密文的解密结果也将不同[18]。一个好的加密算法对密钥的敏感性是十分重要的,密钥敏感性表明算法的抗选择明文/密文攻击能力。密钥敏感性值越小,则算法的抗选择明文/密文攻击能力越好。

3 方案实现

本文提出的基于多种指标参数横向比较的密文图像安全性评价方案,首先需要将选取的图像内容,按照 5 种不同的图像加密算法进行加密,然后由得到的密文图像计算各指标参数,并将各个指标参数与期望值对比,根据各指标参数的可靠性,判断该算法安全性。实验选取的图像内容为目前加密应用中常使用的两类“类图像”——文件照片和卫星地图照片。由于这两种图像的图像特征(颜色特征、纹理特征、形状特征和空间关系特征)和安全特性具有代表性,对其进行安全性分析得出的结论更能体现出本文方案的实用性。

3.1 图像加密

实现了 Tent 混沌映射加密、AES 加密、混沌双重置乱加密、仿射变换加密和频域加密这 5 种图像加密算法以及它们各自的解密功能。

3.2 指标参数计算

实现计算像素数改变率(NPCR)、归一化平均变化强度(UACI)、信息熵、加密时间、相邻像素之间相关系数、密钥空间大小和密钥敏感性。下面介绍部分指标参数计算方法,并由此分析各指标参数在该方案中的可靠性。

(1) NPCR 与 UACI:假设两个原始图像仅存在一个像素不同时,设它们的密文图像中第 (i,j) 点的像素值分别为 $C_1(i,j)$ 和 $C_2(i,j)$。若 $C_1(i,j)=C_2(i,j)$,定义 $D(i,j)=0$;若 $C_1(i,j)\neq C_2(i,j)$,定义 $D(i,j)=1$。则 NPCR 与 UACI 的计算公式分别为:

$$NPCR = \frac{1}{M \times N}\sum_{i=1}^{M}\sum_{j=1}^{N} D(i,j) \times 100\% \quad (5)$$

$$UACI = \frac{1}{M \times N}\sum_{i=1}^{M}\sum_{j=1}^{N} \frac{|C_1(i,j) - C_2(i,j)|}{255} \times 100\% \quad (6)$$

式中: M 和 N 是原始图像像素转换的矩阵的行数与列数。

由于 NPCR 与 UACI 是衡量加密算法对明文敏感度的一个指标参数,对于加密算法的安全性评判是可靠的,因此将其作为主要参数进行分析。

(2) 信息熵: 设 $Q = (q_{ij})_{M \times N}$ 是一个灰度级为 L 的图像,x_i 表示第 i 个灰度,$p(x_i)$ 表示第 i 个灰度在 Q 中的比例,其中 $\sum_{i=1}^{n} p(x_i) = 1$,图像的信息熵定义为:

$$H(Q) = -\sum_{i=1}^{L} p(x_i)\log_2 p(x_i) \quad (7)$$

信息熵反映图像信息的不确定性,即灰度值分布的不确定性。该参数能够直接反映密文图像的安全性,是可靠的。若某加密算法的信息熵过小,则可以判断该方法是不安全的。

(3) 相邻像素之间的相关系数: 首先选择 N 组任意图像中任意方向(水平或垂直或对角方向)的相邻像素,再通过以下公式计算相邻像素之间的相关系数:

$$\bar{x} = \frac{1}{N}\sum_{i=1}^{N} x_i \quad (8)$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N} (x_i - \bar{x})^2 \quad (9)$$

$$Conv(x,y) = \frac{1}{N}\sum_{i=1}^{N} (x_i - \bar{x})(y_i - \bar{y}) \quad (10)$$

$$\gamma_{xy} = \frac{Conv(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \quad (11)$$

(4) 加密耗时: 在本文中加密时间是指原始图像从开始加密到生成密文图像的时间。该参数主要用于判断加密过程的速度,而不直接反映安全性,因此优先级较低。

(5) 密钥空间大小: 这里以本文的混沌双重置乱加密为例,当密钥长度为 r 时,密钥空间有 2^r 个元素。密钥空间足够大时可以抵抗穷举攻击,因此是可靠的。

(6) 密钥敏感性: 为了更加清晰明确地反映其中密文图像的不同,通过计算不同密钥对应的密文图像与原始图像的 NPCR 和 UACI 来比较。密钥敏感性表明算法的抗选择明文/密文攻击能力,最能体现方法安全性。

综上所述,得到指标参数优先级排序。为了让评判更加全面,本文将主要参数设为: 密钥敏感性、信息熵、NPCR 与 UACI。其余参数在使用的加密方法满足主要参数评判的安全性后,作为参考进一步比较方法的安全性。

4　实验结果

4.1　卫星地图照片

图 2 为一张卫星地图照片,灰度化处理后,对其依次进行 Tent 混沌映射加密、AES 加密、混沌双重置乱加密、仿射变换加密和频域加密,得到如图 3 – 图 7 所示的加密效果。

图 2　原图 1

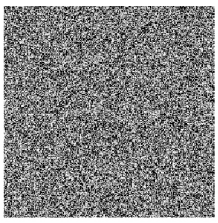

图 3　Tent 混沌映射加密 1

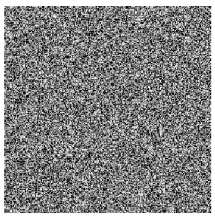

图 4　AES 加密 1

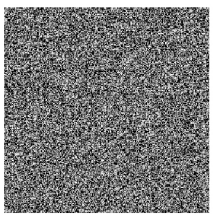

图 5　混沌双重置乱加密 1

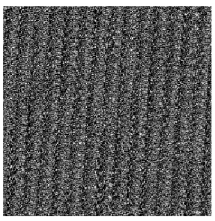

图 6　仿射变换加密 1

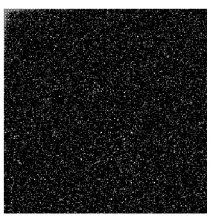

图 7　频域加密 1

通过对比,可以看出 Tent 混沌映射加密和 AES 加密的效果较好,混沌双重置乱其次。而由此得到的指标参数如表 2、表 3 所示。由指标参数综合分析得到的结论与上文是一致的。

表 2　信息熵等指标参数分析 1

加密方法	指标参数			
	1-NPCR	信息熵	UACI	相邻像素相关系数
Tent 混沌异或加密	0.003 906	7.997 5	0.307 69	0.012 322
AES 加密	0.004 059	7.997 1	0.308 43	-0.003 062
混沌双重置乱加密	0.004 303	7.947 3	0.288 23	0.005 762
仿射变换加密	0.006 058	7.623 3	0.224 62	0.060 273
频域加密	0.003 037	4.606 3	0.306 17	0.004 917

表 3 密钥敏感性等指标参数分析 1

加密方法	指标参数		
	加密用时/s	密钥敏感性	密钥空间大小
Tent 混沌异或加密	0.141	1.00E－16	8.11E＋31
AES 加密	27.218	2.94E－39	3.40E＋38
混沌双重置乱加密	9.390	1.00E－10	3.40E＋38
仿射变换加密	0.121	2.33E－10	6.28E＋57
频域加密	0.197	2.33E－10	4.29E＋09

通过对指标参数的分析，我们已知的结论有：

（1）像素的改变率期望值为 100%，为了方便，本文使用的是 1-NPCR，所以该值越接近 0，算法安全性越高。

（2）归一化平均改变强度的期望值为 33%，所以算法的归一化平均改变强度越接近 33%，该算法安全性越高。

（3）信息熵反映加密后图像复杂程度即图像的灰度分布情况，算法的信息熵越接近 8，该算法安全性越高。

（4）相邻像素之间的相关系数越接近 0，算法安全性越高。

（5）算法加密耗时越短，安全性越高。

（6）密钥空间大小反映系统抗穷举攻击能力，其值越大，算法越安全。

（7）密钥敏感性表明系统抗选择明文/密文攻击能力，其值越小，算法越安全。

以上述为前提，选取相应样本，五种加密算法的指标参数的横向比较结论如下：

加密耗时：仿射变换最快，其次是 Tent 混沌异或加密、频域加密、混沌双重置乱，AES 最慢。

信息熵：Tent 最好，其次是 AES、混沌双重置乱、仿射变换加密，频域加密最差。

密钥空间大小：仿射变换加密最好，其次是 AES 和混沌双重置乱、Tent、频域加密。

密钥敏感性：AES 最好，其次是 Tent、混沌双重置乱和仿射变换、频域加密。

1－像素数改变率：频域加密较好、其次是 Tent、AES、混沌双重置乱、仿射。

归一化平均改变强度：AES 最好，其次是 Tent、频域加密、混沌双重置乱、仿射。

相邻像素的相关系数：AES 最好，其次是频域、混沌双重置乱、Tent、仿射。

综上所述，根据主要指标参数和参考其他参数可以得出，卫星地图照片加密中，不考虑加密耗时的情况下，AES 最好；综合情况下 Tent 和 AES 都具有较高的安全性。

4.2 文件照片

图 8 为一张文件照片，步骤同 4.1，得到如图 9－图 13 所示的加密效果。

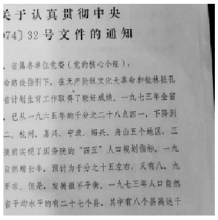
关于认真贯彻中央
[74] 32 号文件的通知

图 8 原图 2

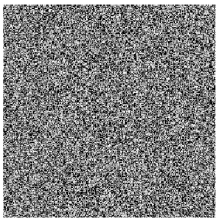

图 9 Tent 混沌映射加密 2

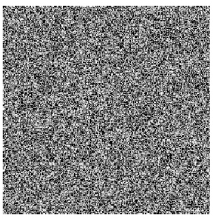

图 10 AES 加密 2

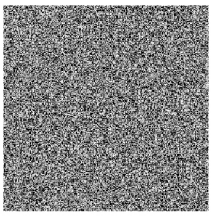

图 11 混沌双重置乱加密 2

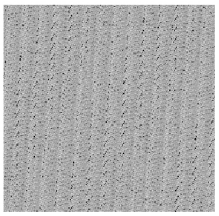

图 12 仿射变换加密 2

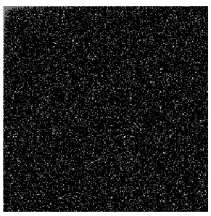

图 13 频域加密 2

可以看出 Tent、AES、混沌双重置乱的加密效果相近。而由此得到的指标参数如表 4、表 5 所示。

表 4 信息熵等指标参数分析 2

加密方法	指标参数			
	1-NPCR	信息熵	UACI	相邻像素相关系数
Tent 混沌异或加密	0.003 906	7.997 5	0.276 31	－0.001 225
AES 加密	0.003 891	7.997 3	0.278 62	－0.008 210
混沌双重置乱加密	0.005 066	7.866 6	0.252 64	－0.005 682
仿射变换加密	0.017 700	6.381 2	0.107 64	0.064 865
频域加密	0.000 488	4.608 7	0.513 84	0.005 008

表 5 密钥敏感性等指标参数分析 2

加密方法	指标参数		
	加密用时/s	密钥敏感性	密钥空间大小
Tent 混沌异或加密	0.167	1.00E－16	8.11E＋31
AES 加密	27.461	2.94E－39	3.40E＋38
混沌双重置乱加密	9.364	1.00E－10	3.40E＋38
仿射变换加密	0.116	2.33E－10	6.28E＋57
频域加密	0.287	2.33E－10	4.29E＋09

由主要指标参数的横向比较得出的结论如下:

信息熵: Tent 最好,其次是 AES、混沌双重置乱、仿射变换加密,频域加密最差。

密钥敏感性: AES 最好,其次是 Tent、混沌双重置乱和仿射变换、频域加密。

1 - 像素数改变率: 频域加密较好、其次是 AES、Tent、混沌双重置乱、仿射。

归一化平均改变强度: AES 最好,其次是 Tent、混沌双重置乱、频域加密、仿射。

综上所述,根据主要指标参数和参考其他参数可以得出,文件照片加密中,AES 具有安全性最高,Tent 其次。

5 结　语

本文对五种密文图像进行基于多种指标参数的安全性评价,并由选取的两种图像样本得出相应结论: 虽然两次实验结果相近(即 Tent 综合情况下安全性高,AES 加密耗时长而安全性最高) ,但具有不同图像特征和安全特性的图像,根据各指标参数分析而得到的安全性评价是不同的。本文提出的密文图像安全性评价方案,在根据需求选取不同种类的样本时,能够得出特定情况下安全性最高的图像加密算法,从而使实际应用中,选取更安全的图像加密算法,得到更好的密文图像。

本文存在的不足是在对指标参数优先级划分时,不够客观细致。下一步工作将用具体的权重划分方法,更客观全面地评判图像加密方法安全性。

参 考 文 献

[1] 冯媛媛,刘莹,赵丽. 基于余弦变换和混沌映射的图像加密方案 [J]. 控制工程,2018,25(6): 1103-1107.

[2] 孙力,梁立. 基于位置换的混沌对称图像加密算法 [J]. 计算机应用与软件,2015,32(7): 305-309.

[3] 孙婧. 可视媒体内容加密的视觉安全性研究 [D]. 武汉: 武汉大学,2013.

[4] 李银华,叶瑞松. 一种基于仿射变换的图像置乱预处理的水印算法 [J]. 汕头大学学报(自然科学版) ,2014,29(1): 9-16.

[5] 李银华. 基于仿射变换及伴随分形插值曲面混沌系统的图像加密算法 [D]. 汕头: 汕头大学,2014.

[6] 朱桂斌,曹长修,胡中豫,等. 基于仿射变换的数字图像置乱加密算法 [J]. 计算机辅助设计与图形学学报,2003,15(6): 711-715.

[7] 李倩倩. 基于 FPGA 图像加密技术的研究与设计 [D]. 天津: 河北工业大学,2014.

[8] 李雷波. 几个国际标准分组密码算法的安全性分析 [D]. 济南: 山东大学,2014.

[9] 龙长贵,马秀荣,白媛,等. 基于外部密钥的多混沌系统图像加密算法 [J]. 计算机应用与软件,2014,31(7): 320-323,327.

[10] 班昊. 对称密钥算法加密机使用中的安全控制 [J]. 计算机应用与软件,2012,29(8): 280-281,300.

[11] 曹建秋,肖华荣,蓝章礼. 基于变参混沌系统的图像双重置换加密 [J]. 计算机工程与应用,2011,47(32): 101-104.

[12] Patidar V, Pareek N, Sud K. A new substitution-diffusion based image cipher using chaotic standard and logistic maps [J]. Communications in Nonlinear Science and Numerical Simulation, 2009, 14(7): 3056-3075.

[13] 梁锐,郑梁君. 浅谈电子档案中数字图像加密技术 [J]. 中国科技博览,2012(24): 285-285.

[14] 邓晓衡,廖春龙,朱从旭,等. 像素位置与比特双重置乱的图像混沌加密算法 [J]. 通信学报,2014,35(3): 216-223.

[15] Sempere V, Albero T, Silvestre J. Analysis of communication alternatives in a heterogeneous network for a supervision and control system [J]. Computer Communications, 2006, 29(8): 1133-1145.

[16] Wang X Y, Lei Y. A novel chaotic image encryption algorithm based on water wave motion and water drop diffusion models [J]. Optics Communications, 2012, 285(20): 4033-4042.

[17] 周浩. 基于同态加密机制的密文域图像可逆信息隐藏算法研究 [D]. 兰州: 兰州理工大学,2016.

[18] 田玉萍. 基于离散分数阶 Fourier 变换本征矢量分解的图像加密算法 [J]. 计算机应用与软件,2016,33(2): 318-321,333.

(上接第 115 页)

[3] 王淼. 美国图书馆“读者决策采购”的兴起、特点与发展趋势分析 [J]. 图书与情报,2015(2): 42-45.

[4] 王显燕. 基于读者决策采购的高校图书馆资源建设策略研究 [J]. 情报探索,2013(10): 68-71.

[5] 李燕. 灰色预测模型的研究及其应用 [D]. 杭州: 浙江理工大学,2012.

[6] 南敬昌,桑百行,高明明. 新颖的神经网络逆建模方法及其应用 [J]. 计算机应用与软件. 2016,33(1): 147-150,194.

[7] 顾兆军,王蕊莉,王帅卿. 基于 GMM 改进的信息系统安全态势实时预测研究 [J]. 计算机应用与软件. 2017,34(2): 272-279.

[8] 郭云开,朱禄宏,熊旭平,等. 灰色模型结合神经网络预测高速公路路基沉降 [J]. 长沙理工大学学报. 2016,13(3): 19-23.

[9] 杜淼. 两类层次分析法的转换及在应用中的比较 [J]. 计算机工程与应用,2012,48(9): 114-119.