两个新的数字图像加密效果评价准则

张雪锋[1,2] 范九伦[2]
(西安电子科技大学电子工程学院 西安 710071)[1] (西安邮电学院信息与控制系 西安 710061)[2]

摘 要 图像信息熵和灰度变化平均值是两个常用的图像加密效果评价准则。分析指出,图像信息熵和灰度变化平均值受图像尺寸大小的影响较大,为此提出了两个新的图像加密效果评价准则:直方图均衡度和游程统计量。直方图均衡度可用于基于像素灰度值变换的加密过程的评价,游程统计量可用于图像坐标置换的加密过程的评价。新方法表达简单,计算便捷,其显著优点是与图像大小无关,不需要借助原图像。

关键词 图像加密,图像信息熵,灰度变化平均值,评价准则
中图法分类号 TP391 **文献标识码** A

Two New Digital Image Encryption Effect Evaluation Criterions

ZHANG Xue-feng[1,2] FAN Jiu-lun[2]
(School of Electronic Engineering, Xidian University, Xi'an 710071, China)[1]
(Department of Information and Control, Xi'an Institute of Posts and Telecommunications, Xi'an 710061, China)[2]

Abstract Image information entropy and gray modification average value are two familiar image encryption effect evaluation criterions. We pointed out that these two criterions are influenced obviously by the size of images, and two new image encryption effect evaluation criterions were presented, that is, histogram proportion degree and run statistic. Histogram proportion degree can be used in the effect evaluation of image encryption algorithm based on the image pixel gray values modification, and run statistic can be used in the effect evaluating of image encryption algorithm based on the image pixel coordinate permutation. The proposed criterions are simple on expression and convenient in computation, their main advantages are having litter effect on the size of images and the computing process are only related with the encrypted image.

Keywords Image encryption, Image information entropy, Gray modification average value, Evaluation criterion

1 引言

近年来,随着互联网和多媒体技术的飞速发展,基于数字图像的信息安全问题日益突出,数字图像的安全保密技术的研究越来越受到人们的关注。数字图像具有数据量大、相邻像素灰度值相关性强等特点,传统的基于文本的加密技术并不完全适用于加密图像数据。目前已经提出了很多图像加密技术[1-6],大体上分为图像灰度值变换[1]、图像坐标置换[2]以及图像坐标和灰度值同时变化[3,4]等技术。对图像灰度值的变换既可在空域上进行[1-4],也可在频域上进行[5,6]。

图像加密效果的好坏需要有一个评价依据,目前常用的两个评价准则是图像信息熵和灰度变化平均值[7,8]。图像信息熵准则不需要原图像的信息[7],而灰度变化平均值准则需要原图像的参与[8]。最近文献[9]给出了一种基于交叉熵的图像加密效果评价指标,该方法通过计算原图像与加密图像之间的交叉熵来对图像加密效果进行量化评价,但其缺点是交叉熵的计算过程需要原图像参与,影响了评价方法的实用性。

为了保证图像的加密效果和安全性,人们往往使用循环迭代的方式对图像进行多次加密。本文在分析加密迭代次数、图像尺寸大小对图像信息熵和灰度变化平均值影响的基础上,引入了两个新的图像加密效果评价准则:基于加密图像灰度直方图均衡程度的图像灰度值变换效果评价准则——直方图均衡度;基于游程统计思想的图像置乱效果评价准则——游程统计量。这两个评价准则的取值不仅受图像大小变化的 影响很小,而且计算过程不需要原始图像的参与。

2 Logistic 混沌映射与广义猫映射

采用混沌理论进行图像加密是目前常用的方式之一。混沌(chaos)是20世纪60年代发现的一种特殊的自然现象,是非线性确定系统由于内禀随机性而产生的外在复杂表现,是一种貌似随机的非随机现象。混沌系统表现为对初始值和系统参数的敏感性、白噪声的统计特性和混沌序列的遍历特性,其吸引子的维数是分维,有十分复杂的分形结构,具有不可预测性[10]。由于混沌序列具有如此优良的密码学特性,基于混沌的保密技术已经涉及到数据安全和通信保密等众多研究领

到稿日期:2009-03-31 返修日期:2009-06-18 本文受陕西省自然科学研究计划项目(SJ08F24)资助。
张雪锋(1975-),男,博士生,CCF会员,主要研究方向为数字图像保密技术,E-mail:zhangxuefeng3@163.com;范九伦(1964-),男,教授,博士生导师,主要研究方向为模式识别、信息安全。

域[11,12]。文献[13]给出了一种基于一维混沌系统和像素灰度值变换的图像加密算法，该算法对应用混沌映射生成的实数混沌序列进行简单的二值化处理，得到的二值序列再与图像灰度值对应的二值序列进行 XOR 运算，实现对图像的加密。文献[14]研究了一种广义的混沌映射，同时给出了基于坐标变换的图像加密方法，该方法通过广义混沌映射对图像的像素坐标进行循环迭代的置乱变换，以实现图像的加密过程。以上两种方法由于原理简单、实现效率高而被广泛应用。本文以文献[13]给出的基于像素灰度值变换的图像加密算法和文献[14]给出的基于坐标变换的图像加密算法为例，说明了加密效果与评价准则之间的变化关系。为此首先介绍用到的两种混沌映射——Logistic 混沌映射和广义猫映射。

2.1 Logistic 映射

Logistic 混沌系统由于其表达式简洁、计算简单，被广泛应用于加密算法、混沌优化等方面。Logistic 映射定义如下[10,13]：

$$a_{n+1}=F(a_n)=\mu\cdot a_n\cdot(1-a_n)\quad 0<a_n<1\quad n=1,2,\cdots \tag{1}$$

其中，$3.569946\cdots\leqslant\mu\leqslant 4$，Logistic 映射的输入和输出都分布在区间(0,1)上。

2.2 广义猫映射

二维猫映射定义如下[14]：

$$\begin{cases}x_{n+1}=(x_n+y_n)\bmod 1\\ y_{n+1}=(x_n+2y_n)\bmod 1\end{cases} \tag{2}$$

其中，mod 1 表示只取小数部分，即 $x \bmod 1=x-\lfloor x\rfloor$，因此 (x_n,y_n) 的相空间限制在单位正方形 $[0,1]\times[0,1]$ 内，将式(2)表示成矩阵形式为：

$$\begin{bmatrix}x_{n+1}\\ y_{n+1}\end{bmatrix}=\begin{bmatrix}1 & 1\\ 1 & 2\end{bmatrix}\cdot\begin{bmatrix}x_n\\ y_n\end{bmatrix}\bmod 1=C\begin{bmatrix}x_n\\ y_n\end{bmatrix}\bmod 1 \tag{3}$$

其中，伴随矩阵 $C=\begin{bmatrix}1 & 1\\ 1 & 2\end{bmatrix}$，可以发现式(3)中 C 的行列式 $|C|=1$，因此猫映射是一个保面积映射(没有吸引子)，同时也是一个一一映射，单位矩阵内的每一个点唯一地变换到单位矩阵内的另一点。

为了能够将以上定义的猫映射应用于图像加密，需要将猫映射扩展到 $N\times N$ 的矩阵内并进行离散化处理，相应的广义猫映射定义如下[14]：

$$\begin{bmatrix}x_{n+1}\\ y_{n+1}\end{bmatrix}=\begin{bmatrix}a & b\\ c & d\end{bmatrix}\cdot\begin{bmatrix}x_n\\ y_n\end{bmatrix}\bmod N=C\begin{bmatrix}x_n\\ y_n\end{bmatrix}\bmod N \tag{4}$$

其中，伴随矩阵 $C=\begin{bmatrix}a & b\\ c & d\end{bmatrix}$，要求矩阵 C 仍然满足行列式 $|C|=ad-bc=1$。式(4)定义的广义猫映射的相空间为 $\{0,1,2,\cdots,N-1\}\times\{0,1,2,\cdots,N-1\}$，其逆映射为：

$$\begin{bmatrix}x_n\\ y_n\end{bmatrix}=\begin{bmatrix}d & -b\\ -c & a\end{bmatrix}\cdot\begin{bmatrix}x_{n+1}\\ y_{n+1}\end{bmatrix}\bmod N \tag{5}$$

广义猫映射能够在 $N\times N$ 的二维空间内进行保面积映射，而且置换过程中各系数均为整数，所以整个运算过程中不会引入误差[14]。文献[14]建议在加密过程中采用选择密钥从 4 个矩阵 $\begin{bmatrix}1 & a\\ b & ab+1\end{bmatrix}$，$\begin{bmatrix}ab+1 & a\\ b & 1\end{bmatrix}$，$\begin{bmatrix}a & 1\\ ab-1 & b\end{bmatrix}$，$\begin{bmatrix}a & ab-1\\ 1 & b\end{bmatrix}$ 中选取一种形式作为伴随矩阵 C。需要说明的是，为了能够对图像的灰度矩阵进行充分置换，应用广义猫映射进行置乱加密时往往需要一定的迭代计算，但是该迭代过程并不能够增强置乱加密过程的安全性，因为：

$$\begin{bmatrix}x_{n+1}^m\\ y_{n+1}^m\end{bmatrix}=\prod_{i=1}^{m}C_i\begin{bmatrix}x_n^0\\ y_n^0\end{bmatrix}=B\begin{bmatrix}x_n^0\\ y_n^0\end{bmatrix}$$

说明进行多次迭代计算的结果等价于应用一个伴随矩阵 B 进行一次置乱计算。

3 图像加密效果评价准则

3.1 图像信息熵与灰度变化平均值

设原图像 Image 的大小为 $M\times N$，加密结果图像为 Enimage，则相应的图像加密效果评价标准定义如下：

(1) 图像信息熵[7]：信息熵可以度量图像灰度值的概率分布情况，灰度分布越均匀，图像信息熵越大。加密图像信息熵越大，说明加密图像中灰度分布越均匀，攻击者从加密图像的灰度分布中得到的原图像信息就越少，加密算法的安全性就越高。信息熵定义为：

$$H=-\sum_{i=1}^{L}p_i\log_2 p_i \tag{6}$$

其中，p_i 表示图像中灰度值为 i 的像素出现的概率，L 为图像的灰度等级。图像信息熵适用于对基于灰度值变换的图像加密算法的加密效果进行量化评价。

(2) 灰度变化平均值[8]：对于原图像和加密图像，灰度变化平均值定义为：

$$G=\frac{\sum_{i=1}^{M}\sum_{j=1}^{N}|\mathrm{Image}(i,j)-\mathrm{Enimage}(i,j)|}{M\times N} \tag{7}$$

通过计算原图像与加密图像之间的灰度变化平均值，可以对基于坐标变换的图像加密算法的加密效果进行量化评价。当然，该评价指标也适用于对基于灰度值变换的加密算法的效果进行评价。

3.2 直方图均衡度与游程统计量

为了更加有效地对加密图像对应的灰度直方图的统计信息进行量化评价，给出了一个新的图像加密效果评价指标：直方图均衡度。对于基于图像灰度值变换的加密方式，我们认为，一个好的图像加密评价准则，能够评价出加密后的图像是否以等可能的方式变换到灰度值取值范围中的每一个值，直方图均衡度通过计算灰度图像的灰度直方图的均匀程度来评价图像的加密效果。假设灰度图像的灰度取值范围为[0,255]，则相应的加密图像的灰度直方图均匀度定义为：

$$F=\frac{1}{M\times N}\sum_{i=0}^{255}\left(K(i)-\frac{M\times N}{256}\right)^2 \tag{8}$$

其中，$K(i)$ 表示灰度值为 i 的像素的个数。F 的取值范围为：$0\leqslant F<M\times N$。F 的值越小，说明图像的灰度直方图的均匀程度越好。

在图像编码中，游程是指一串相同的序列元素，其直接前驱元素和直接后继元素都与之不同[15]。例如，0111001 从一个“0”的 1 游程开始，接着是一个“1”的 3 游程和一个“0”的 2 游程，最后结束于一个“1”的 1 游程。“0”游程称为间隔(gap)，而“1”游程称为块组(block)。

考虑到灰度图像的加密图像仍然是灰度图像，对应的灰度矩阵并不是二值矩阵，为了对灰度图像进行相应的游程统计，首先应计算灰度图像 Image 对应的像素灰度平均值 ave，像素灰度平均值定义为：

$$ave=\frac{1}{M\times N}\sum_{i=1}^{M}\sum_{j=1}^{N}\text{Image}(i,j) \tag{9}$$

根据图像 Image 的像素灰度平均值 ave 来定义灰度图像的“游程”。灰度图像的“游程”是指一串与像素灰度平均值保持相同大小关系的像素序列，其直接前驱和直接后继像素的灰度值均与图像的 ave 满足不同的大小关系，我们称这种灰度序列对应的“游程”为灰度游程。

设序列为 $L=(78,134,65,82,234,156,221,178)$，首先计算其平均灰度值：

$$ave=\frac{1}{8}\times(78+134+65+82+234+156+221+178)$$
$$=143.5$$

根据灰度平均值 $ave=143.5$ 可知，灰度序列 L 包含两个灰度游程，其中灰度游程 1 由灰度序列(78,134,65,82)组成，游程长度为 4，灰度游程 2 由灰度序列(234,156,221,178)组成，游程长度为 4。灰度序列 L 对应的灰度游程总数为 2。

对于大小为 $M\times N$ 的灰度图像 Image，设其对应的灰度矩阵为 $\text{Image}=[a_{i,j}]_{M\times N}$。将灰度矩阵看作是由 M 个灰度值行向量构成的序列 $\text{Image}=[A_1,A_2,\cdots,A_M]^T$，行向量中每一个元素 A_i 都对应一个灰度序列。现在应用评价序列随机性的游程测试方法对行向量序列 $\text{Image}=[A_1,A_2,\cdots,A_M]^T$ 进行分析。

图像信息具有较强的相关性，位于相同邻域之间的像素灰度值之间具有较强的关联性。基于像素坐标变换进行加密的出发点是通过置乱变换使相同邻域像素之间的相关性减弱。当对灰度图像进行基于像素坐标置乱变换的加密后，加密图像相邻像素之间的灰度值相关性减弱，相应的灰度取值反差会增大，导致对应的灰度值行向量序列 $\text{Image}=[A_1,A_2,\cdots,A_M]^T$ 中所有元素 A_i 包含的灰度游程总个数会相应地增加。

根据以上分析，将加密图像对应的灰度矩阵 $\text{Image}=[A_1,A_2,\cdots,A_M]^T$ 中的第 k 行 A_k 包含的灰度游程个数记为 num_k，则灰度图像 Image 的灰度游程总数满足：$num=\sum_{i=1}^{M}num_i$。对于灰度图像 Image，根据 num 定义相应的游程统计量：

$$R=\frac{1}{M\times N}\times num=\frac{1}{M\times N}\times\sum_{i=1}^{M}num_i \tag{10}$$

由式(10)可知，对于任意的灰度图像 Image，游程统计量的值满足条件：$1/N\leqslant R\leqslant 1$。当游程统计量的值增大时，说明灰度图像灰度游程总数 num 在增大，相应的灰度图像中相邻像素之间灰度取值变化也就越剧烈，图像混乱程度在增加。

4 实验结果

4.1 基于灰度值变换的图像加密效果评价

以文献[13]给出的基于灰度值变换的数字图像加密算法为例，通过实验仿真，分析两个评价准则：图像信息熵和直方图均衡度与图像加密迭代次数、图像大小之间的变化关系。其中 Logistic 映射的初始条件为：$a_0=0.3141$，$u=4$。图 1—图 4 和表 1 分别给出了迭代加密的结果图像及其灰度直方图、不同迭代次数的加密结果图像相应的评价准则取值与加密次数之间的变化关系。其中图像 1 大小为 1024×1024，图像 2 大小为 256×256。

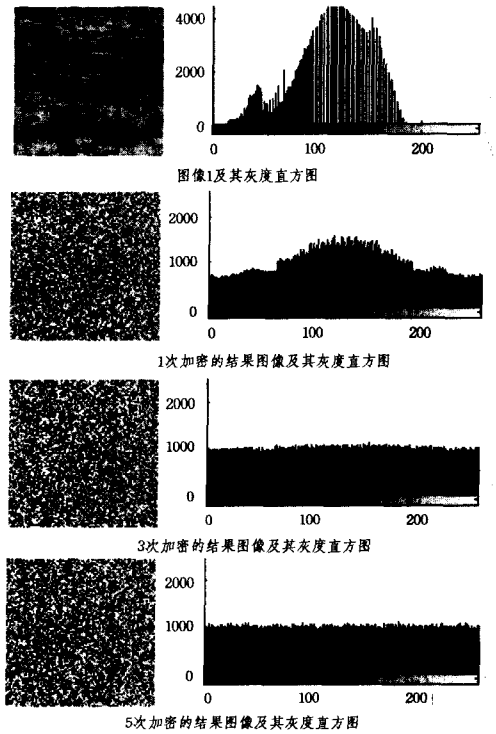

图 1 循环迭代加密结果图像及其灰度直方图

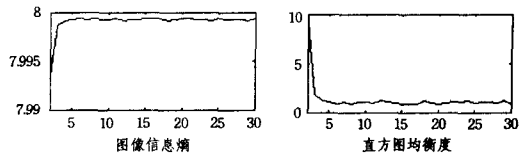

图 2 评价准则与加密次数变化关系

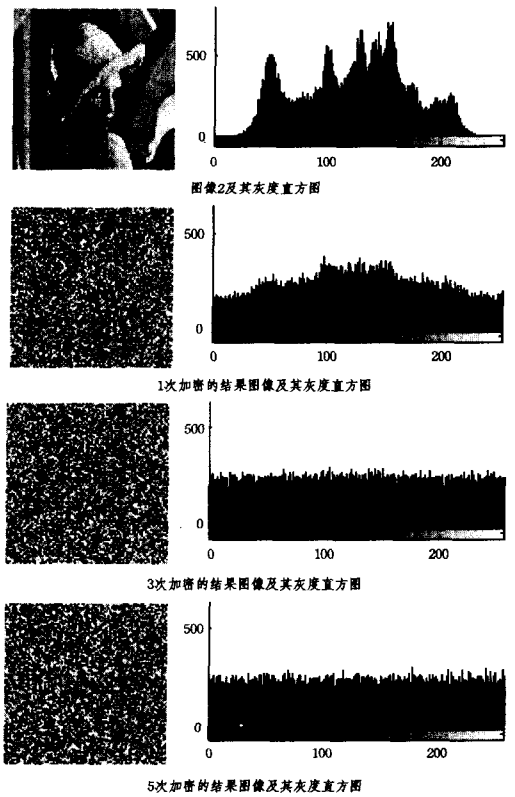

图 3 循环迭代加密结果图像及其灰度直方图

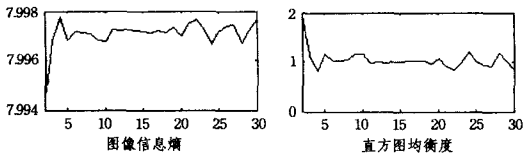

图 4　评价指标与加密次数变化关系

表 1　加密次数与加密效果评价指标之间的关系

迭代加密次数	图像信息熵 H		直方图均衡度 F	
	图像 1	图像 2	图像 1	图像 2
1	7.9431	7.9642	82.2553	12.7162
2	7.9935	7.9945	9.3037	1.9661
3	7.9986	7.9968	1.9240	1.1285
4	7.9992	7.9978	1.1477	0.8030
5	7.9993	7.9968	1.0575	1.1393
6	7.9994	7.9971	0.9058	1.0159
7	7.9993	7.9971	1.0505	1.0195
8	7.9994	7.9971	0.9010	1.0379
9	7.9993	7.9968	1.0584	1.1537
10	7.9993	7.9967	1.0468	1.1573

通过图 1 和图 3 的实验结果可知，随着加密次数的增加，相应的加密图像灰度直方图反映出的原图像灰度统计信息越来越少，说明加密效果越来越好。图 2 和图 4 给出了随着加密迭代次数的增加，相应的加密图像对应的评价准则：图像信息熵、直方图均衡度与图像加密迭代次数之间的变化关系。实验结果表明，以上两种评价指标取值与主观评价结果基本一致。

为了揭示评价准则与图像大小之间的关系，下面分别对 20 幅不同大小的灰度图像进行了 10 次迭代加密，每一次加密后计算相应的评价准则取值，其中图像大小从 128×128 到 1024×1024 不等。

从图 5 的结果可见，当迭代次数小于 5 时，图像信息熵和直方图均衡度这两个评价指标的取值变化较大，当迭代次数大于 5 时，以上指标的取值情况变化逐渐平稳。图 5 的实验结果也表明，随着加密迭代次数的增加，图像信息熵取值趋势比较稳定，但具体取值不仅取决于加密迭代次数，而且与图像大小有关，这意味着对不同大小的图像加密效果进行客观评价时，图像信息熵的取值在不同图像之间不具有可比性。而本文给出的直方图均衡度的取值趋势也比较稳定，且直方图均衡度的取值主要取决于图像加密迭代次数，基本不受图像大小变化的影响，其取值范围介于 1 附近，该性质保证了对不同大小图像的加密效果能够进行相互比较。

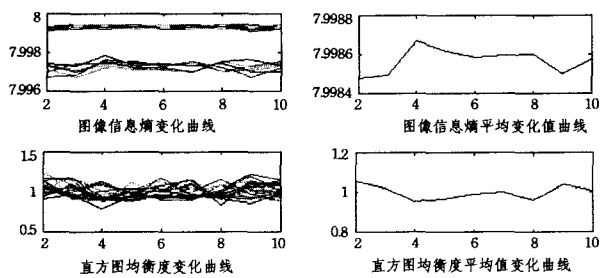

图 5　多幅图像加密次数与加密效果评价指标之间的变化关系

4.2　基于坐标变换的图像加密效果评价

以文献[14]给出的基于图像坐标变换的数字图像加密算法为例，分析灰度变化平均值、游程统计量与图像加密迭代次数、图像大小之间的变化关系。加密算法采用式(4)定义的广义猫映射作为置乱变换的混沌映射，图像 1 对应的灰度均值 $ave=106.3934$，图像 2 对应的灰度均值 $ave=123.6022$。对于每一次置乱变换的结果图像，由于置乱变换不会改变图像灰度值的统计特性，因此加密图像和原图像将具有相同的灰度直方图和灰度均值。接下来的实验中，根据图像对应的灰度均值，分别计算其灰度变化平均值和游程统计量，相应的实验结果如表 2 所列。

表 2　加密次数与加密效果评价准则之间的关系

迭代加密次数	灰度变化平均值 G		游程统计量 R	
	图像 1	图像 2	图像 1	图像 2
1	39.6981	55.6852	0.1559	0.0695
2	40.2595	55.4767	0.2499	0.1231
3	40.5224	55.2822	0.3429	0.2235
4	39.7736	54.9627	0.4327	0.3804
5	39.7421	54.6813	0.5187	0.4501
6	39.6638	54.7439	0.5180	0.5841
7	39.6992	54.6562	0.5088	0.5030
8	39.7108	54.6991	0.4910	0.5682
9	39.7401	54.7017	0.4603	0.5191
10	39.7228	54.8998	0.4984	0.5421

由图 6 和图 8 的实验结果可知，随着加密次数的增加，置乱加密的效果越来越好，当次数大于 5 时，加密图像完全隐藏了原图像的内容信息。图 7 和图 9 分别给出了对应图 6 和图 8 的加密过程中随着加密迭代次数的增加，灰度变化平均值、游程统计量与图像加密迭代次数之间的变化关系。结果表明，随着加密迭代次数的增加，灰度变化平均值的取值总体上趋于稳定，但是其取值与主观评价结果一致性较差，尤其是对应图像 2 的实验结果，当加密迭代次数小于 5 时，随着加密次数的增加，图像的加密效果越来越好，但加密图像的灰度变化平均值却随着加密次数的增加而减小，不能准确反映出加密效果与迭代次数之间的关系。而游程统计量的取值随着加密迭代次数的增加也趋于稳定，且取值能够较准确地反映加密迭代次数和加密效果之间的变化关系。同时，灰度变化平均值的计算过程依赖于原图像和加密结果图像的灰度直方图。而游程统计量的计算过程仅仅依赖于加密结果图像的灰度平均值，便于实际应用。

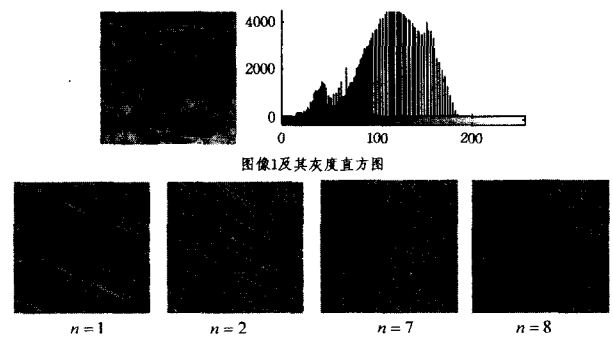

图 6　不同迭代加密次数 n 对应的加密效果

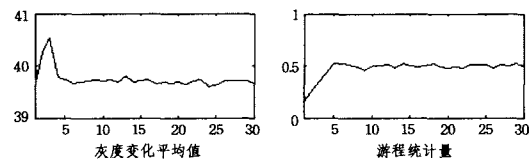

图 7　评价准则与加密次数的变化关系

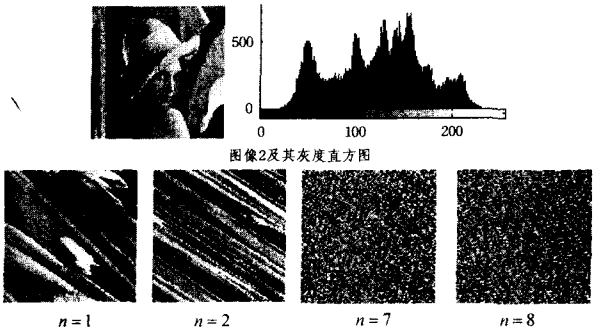

图 8　不同迭代加密次数 n 对应的加密效果

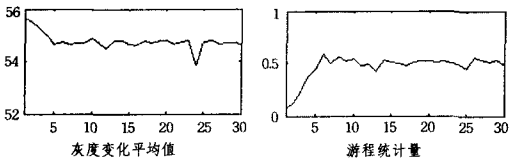

图 9　评价准则与加密次数的变化关系

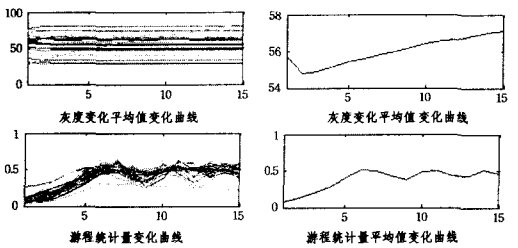

图 10　多幅图像加密次数与加密效果评价准则之间的变化关系

为了揭示评价准则与图像大小之间的关系，下面对 20 幅不同大小的灰度图像分别进行了 15 次迭代加密，每一次加密后计算相应的评价指标取值，其中图像大小从 128×128 到 1024×1024 不等。图 10 给出了多幅图像加密次数与评价指标——灰度变化平均值和游程统计量之间的变化关系。结果表明，灰度变化平均值不仅与迭代次数紧密相关，而且对于不同大小的图像，其加密图像的灰度变化平均值取值差异较大，这意味着在对不同大小的图像加密效果进行客观评价时，灰度变化平均值的取值在不同图像之间不具有可比性。此外，其平均值变化曲线与主观评价结果一致性也较差。而本文定义的游程统计量取值对不同大小图像虽然也会有变化，但是在经过多次迭代加密以后，其取值范围介于 0.3～0.6 之间，取值范围跨度较小。该性质能保证在对不同大小图像加密效果进行比较时评价效果的有效性，而且游程统计量的平均值变化曲线与主观评价结果也基本一致。

结束语　本文给出了两个新的图像加密效果评价方法：直方图均衡度和游程统计量。这两种评价准则的计算仅与加密的结果图像有关，不依赖于原始图像信息，便于实际应用。实验结果表明，这两个评价指标的取值与主观评价结果一致性较好，受图像大小变化的影响较小，更适合于对不同大小图像的加密效果进行客观评价。

参 考 文 献

[1] Behnia S, Akhshani A, Mahmodi H, et al. A novel algorithm for image encryption based on mixture of chaotic maps[J]. Chaos solitons & fractals, 2008, 35: 408-419

[2] 陈刚，赵晓宇，李均利. 一种自适应的图像加密算法[J]. 软件学报，2005，16(11)：1975-1982

[3] Wong K-W, Kwok B S-H, Law W-S. A fast image encryption scheme based on chaotic standard map[J]. Physics letters A, 2008, 372: 2645-2652

[4] 张翌维，王育民，沈绪榜. 基于混沌映射的一种交替结构图像加密算法[J]. 中国科学(E辑)，2007，37(2)：183-190

[5] Liu Zhengjun, Liu Shutian. Double image encryption based on ite-rative fractional Fourier transform[J]. Optics communications, 2007, 275: 324-329

[6] 侯启槟，杨小帆，王阳生，等. 一种基于小波变换和骑士巡游的图像置乱算法[J]. 计算机研究与发展，2004，41(2)：369-375

[7] 柏森，胡中豫，吴乐华，等. 通信信息隐匿技术[M]. 北京：国防工业出版社，2005

[8] 徐江峰，杨有. 加密图像置乱性能分析[J]. 计算机科学，2006，33(3)：110-113

[9] 陈燕梅，张胜元. 基于交叉熵的数字图像置乱程度评价方法[J]. 中国图象图形学报，2007，12(6)：997-1001

[10] Ausloos M, Dirickx M. The logistic map and the route to chaos [M]. Springer, 2006

[11] Alvarez G, Montoya F, Romera M, et al. Breaking two secure communication systems based on chaotic masking[J]. IEEE transactions on circuits and systems-II, 2004, 51(10): 505-506

[12] Parker A T, Short K M. Reconstructing the keystream from a chaotic encryption scheme[J]. IEEE transactions on circuits and systems-I Fundamental theory and applications, 2001, 48(5): 624-630

[13] Habutsu T, Nishio Y, Sasase I, et al. A secret cryptosystem by iterating a chaotic map[A] // Advances in Cryptology EURCRYPT'91[C]. Berlin: Springer-Verlag, 1991: 127-140

[14] 马在光，丘水生. 基于广义猫映射的一种图像加密系统[J]. 通信学报，2003，24(2)：51-57

[15] Mao Wenbo. Modern Cryptography: Theory and Practice[M]. Prentice Hall, 2003

(上接第 263 页)

[4] Lucht R, Knopp M V, Brix G. Elastic matching of dynamic MR mammographic images[J]. Magnetic Resonance in Medicine, 2000, 43: 9-16

[5] Martel A L, Froh M S, Brock K K, et al. Evaluating an optical-flow-based registration algorithm for contrast-enhanced magnetic resonance imaging of the breast[J]. Physics in Medicine and Biology, 2007, 52: 3803-3816

[6] Mainardi L, Passera K M, Lucesoli A, et al. A Nonrigid Regi-stration of MR Breast Images Using Complex-valued Wavelet Transform[J]. Journal of Digital Imaging, 2008, 21(1): 27-36

[7] Thirion J P. Image matching as a diffusion process: an analogy with Maxwell's demons[J]. Medical. Image Analysis, 1998, 2: 243-260

[8] Pennec X, Cachier P, Ayache N. Understanding the "Demon's Algorithm": 3D Non-Rigid registration by Gradient Descent [C] // 2nd Int. Conf. on Medical Image Computing and Computer-Assisted Intervention-MICCQAI, 99. 1999: 597-605

[9] Wang He, Dong Lei, O'Daniel J, et al. Validation of an accelerated 'demons' algorithm for deformable image registration in radiation therapy[J]. Physics in Medicine and Biology, 2005, 50: 2887-2905

[10] Hayton P, Brady M, Tarassenko L, et al. Analysis of dynamic MR breast images using a model of contrast enhancement[J]. Med. Image Anal., 1997, 1: 207-224

[11] Kuhl C K, Mielcareck P, Klaschik S, et al. Dynamic breast MR imaging: are signal intensity time course data useful for differential diagnosis of enhancing lesions? [J]. Radiology, 1999, 211: 101-110

[12] Roche A, Malandain G, Ayache N, et al. Toward a better comprehension of similarity measures used in medical image registration[C] // Proc. 2nd Int. Conf. Medical Image Computing and Computer-Assisted Intervention (MICCAI'99). vol. 1679, Oct. 1999: 555-566