一种度量图像置乱加密程度的新算法

范延军 孙燮华
FAN Yan-jun,SUN Xie-hua

中国计量学院 计算机科学与技术系,杭州 310034
Department of Computer Science and Technology,China Institute of Metrology,Hangzhou 310034,China
E-mail:fanyanjun2002@yahoo.com.cn

FAN Yan-jun,SUN Xie-hua.New algorithm to measure scrambling degree of scrambling images.Computer Engineering and Applications,2007,43(29):93-94.

Abstract: In this paper,the methods to measure the scrambling degree of scrambling images are deeply discussed.Then,a new algorithm to measure the scrambling degree of scrambling images is proposed.The algorithm is as follows:first,devising the original image and the scrambling image to sub-block;second,calculating the distance of the according sub-block and get the result as the minimum value of eight valve situation.Finally,the definition of the scrambling degree is given.In order to evaluate the degree of the scrambling,we propose a new definition above it.The experiment results show that the scrambling degree is an efficient metrological method.

Key words: scrambling transformation;encryption;scrambling degree

摘 要:近年来,出现了许多有效的图像置乱加密算法,但却很难找到一种关于置乱加密效果的有效度量方法。对度量置乱加密效果的方法进行了深入的探讨,进而提出了"置乱加密度"的概念,能够客观地反映置乱算法的加密性能,同时兼顾人类的视觉特性,是一种有效的度量方法。算法的执行过程如下:首先,将原始图像和置乱加密后的图像按照同样的方法分割为许多子块;第二步,对于原始图像中的每一块,求出它与置乱加密后的图像各个子块的最小"距离";最后,给出了"置乱加密度"的定义,用来度量图像的置乱加密程度。实验结果证实了"置乱加密度"能有效地反映算法的置乱加密效果。

关键词:排列变换;加密;置乱加密度
文章编号:1002-8331(2007)29-0093-02 **文献标识码**:A **中图分类号**:TP391

1 引言

图像置乱(排列)变换是一种经典的基于内容的图像加密方法。如今图像置乱加密方法已有许多,如经典的 Arnold 变换、Hilbert 曲线变换、E 曲线变换[1]、几何变换[2]以及骑士巡游置乱变换[3]等等。虽然用这些方法置乱图像后的效果各不相同,但它们都具有一定的确定性,即在置乱过程中均只改变像素点的位置,而不改变其灰度值,所以置乱后的图像还是具有一定的规律性。文献[4]提出的基于混沌序列的加密算法,则既改变像素点的位置,又改变其灰度值。该算法属于空间域算法。尽管空间域的排列加密算法实现较为简单,计算量较少,不过,空间域的局部随机置乱效果不是很好。文献[5]中提出的算法是基于 DCT(Discret Cosine Transform)的频域算法。频域算法的优势是,在频域中每一点的变化对整个数据集合产生一定的影响,因此效率高。相对于空间域算法,频域算法的加密效率比较高,但计算量较大。

近年来出现了许多有效的置乱加密算法,但却很难找到一种关于置乱加密效果的有效度量方法。文献[6]中给出了一系列衡量图像置乱网络的性能指标,如不动点、k 阶距等等,但是文献[6]并没有给出度量的标准和算法。文献[4]中给出了"图像置乱度"的概念和算法。"图像置乱度"从人的主观感觉出发,是对图像内容(即灰度)置乱效果的一种主观评价,并未真正地反映置乱加密算法的效率。鉴于此,提出一种基于排列的"置乱加密度"的概念,能比较有效地反映置乱加密算法的效率,同时又能兼顾人类的视觉特征。

2 置乱加密程度的度量

图像置乱(排列)变换是一种经典的基于内容的图像加密方法。对于任一图像 I,设 I 的大小为 $n=M\times N$,且 I 中总共包含 k 种颜色,其中具有颜色 c_i 的像素个数为 n_i,$n_1+n_2+\cdots+n_k=n$,则 I 的直方图 H 可以看作是具有 k 个元素的多重集 $S=(n_1\cdot c_1,n_2\cdot c_2,\cdots,n_k\cdot c_k)$其基数为 n)。显然,S 上的任一个全排列 P_i 均对应一幅 $M\times N$ 图像 I_i,即与 I_i 存在一一对应关系。

令集合 $X=\{1,2,\cdots,n\}$,则 X 的一个置换是指 X 到其自身的一个双射 $p:X\to X$。定义两个置换 p_1 和 p_2 的乘法运算为 $p_1\cdot p_2:X\to X$,$p_1\cdot p_2(x)=p_1(p_2(x))$,$x\in X$,则由 X 的所有置换组成的集合在该乘法运算下构成一个群,记为 S_n,称之为 X 上的对称

作者简介:范延军(1977-),讲师,主要研究方向为计算机图形学,数字水印,图像置乱,分形几何等;孙燮华(1945-),教授,主要研究方向为计算机图形学,图像处理,算法分析和应用数学等。

群[7]。置换 p 就是将 X 的一个排列变成另一个排列。由于图像与排列之间有一一对应关系。可将集合 X 的元素看作是图像 I 中各元素顺序排列时的下标，则任何一个置换 p 都可看作是 I 到 $p(I)$的一个图像变换。因此，可利用排列变换对图像进行加密。

2.1 “距离”的定义

设 $\boldsymbol{I}=\begin{Bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{Bmatrix}$ 为一自然序矩阵，置乱后的序列矩阵为 $\boldsymbol{Q}=\begin{Bmatrix} b_{11} & b_{12} & \cdots & b_{1n} \\ b_{21} & b_{22} & \cdots & b_{2n} \\ \vdots & \vdots & & \vdots \\ b_{m1} & b_{m2} & \cdots & b_{mn} \end{Bmatrix}$，其中 $\boldsymbol{I}$ 是自然数序列(1,2,…,$m\times n$)按照行-列优先顺序填入而得到的矩阵；$\boldsymbol{Q}$ 是置乱序列(序列值取值范围为[1,$m\times n$])按照行-列优先顺序填入而得到的矩阵。

将 $\boldsymbol{I}$ 分割成个可相互重叠的子块 I_i,i=1,2,…,k，设每块的尺寸为 $2^R\times 2^R$。具体的分割方法如下：先在 $\boldsymbol{I}$ 的左上角取出第一个子块 $\boldsymbol{I}_1$；以 $\boldsymbol{I}_1$ 为种子块，水平向左移一个步长 Δ(用户自定义大小，一般 $\Delta\leqslant R$)取得子块 $\boldsymbol{I}_2$，重复向左平移 Δ，并取得相应子块，直到达到矩阵最右端；此时，将 $\boldsymbol{I}_1$ 垂直向下移 Δ 得到新的种子块，并以 Δ 为步长水平向左移，得到相应子块；重复上述过程直到整个 I 分割完毕。

以同样的方法将 $\boldsymbol{Q}$ 分割成个可相互重叠的子块 $\boldsymbol{Q}_j$,j=1,2,…,k，每块的尺寸为 $2^R\times 2^R$。设

$$\boldsymbol{I}_i=\begin{Bmatrix} a_{xy} & a_{x(y+1)} & \cdots & a_{x(y+2^R-1)} \\ a_{(x+1)y} & a_{(x+1)(y+1)} & \cdots & a_{(x+1)(y+2^R-1)} \\ \vdots & \vdots & & \vdots \\ a_{(x+2^R-1)y} & a_{(x+2^R-1)(y+1)} & \cdots & a_{(x+2^R-1)(y+2^R-1)} \end{Bmatrix}$$ 和

$$\boldsymbol{Q}_j=\begin{Bmatrix} b_{uv} & b_{u(v+1)} & \cdots & b_{u(v+2^R-1)} \\ b_{(u+1)v} & b_{(u+1)(v+1)} & \cdots & b_{(u+1)(v+2^R-1)} \\ \vdots & \vdots & & \vdots \\ b_{(u+2^R-1)v} & b_{(u+2^R-1)(v+1)} & \cdots & b_{(u+2^R-1)(v+2^R-1)} \end{Bmatrix}$$ 为两子块，定义他们之间的距离为：

$$D(I_i,Q_j)=\sqrt{\sum_{s=0}^{2^R-1}\sum_{t=0}^{2^R-1}(a_{(x+s)(y+t)}-b_{(u+s)(y+t)})^2} \tag{1}$$

若 $D(I_i,Q_j)$=0，即 $I_i=Q_j$，则说明 I_i 在置乱算法完成之后块内数据并没有被打乱，说明该置乱加密算法并不理想。

2.2 “置乱加密度”定义

考虑子块的几何旋转情形：一个正方形子块的几何旋转有 8 种方式，即旋转 0°,90°,180°,270°和垂直中线反射、水平中线反射和对角线反射。设 I_i 是一子块，设 a_{xy}(其中 x,y=1,2,…,2^R)是 I_i 中的任意一个元素，定义“反射-旋转”操作符 L_p：

L_1: $a_{xy}=a_{xy}$ 旋转 0°

L_2: $a_{xy}=a_{y(2^R-x+1)}$ 旋转 90°

L_3: $a_{xy}=a_{(2^R-x+1)(2^R-y+1)}$ 旋转 180°

L_4: $a_{xy}=a_{(2^R-y+1)x}$ 旋转 270°

L_5: $a_{xy}=a_{x(2^R-y+1)}$ 垂直中线反射

L_6: $a_{xy}=a_{(2^R-x+1)y}$ 水平中线反射

L_7: $a_{xy}=a_{yx}$ 对角线 $x=y$ 反射

L_8: $a_{xy}=a_{(2^R-y+1)(2^R-x+1)}$ 对角线 $x+y=2^R+1$ 反射

如果 I 中的一个子块 I_i 经过反射-旋转操作符作用后等于 Q 中的一个子块 Q_j，即 $L_p(I_i)=Q_j$，则说明经过置乱算法作用后，子块 I_i 只是经过了简单的几何旋转或反射，其块内信息并没有被打乱，不能有效的加密和隐藏图像信息。

对于子块 I_i，定义距离 D_i：

$$D_i=\min\{D(L_p(I_i),Q_j),p=1,2,\cdots,8\},\ \forall\, Q_j\in Q \tag{2}$$

如果 $\exists\, I_i\in I$，使得 D_i=0，则表明改算法的置乱加密效果并不理想；如果 $\forall\, D_i\neq 0$，则定义置乱加密度 η：

$$\eta=\frac{\sum_{i=1}^{k}D_i}{k} \tag{3}$$

其中 k 为分割后得到的子块总数。η 越大，则表明算法的置乱加密程度越大，加密效果越好；反之，加密效果越差。在实际应用中，考虑到人类的视觉特性，分割子块的大小应适中，一般取 R=2 或 3。

3 实验结果与结论

利用 Matlab 工具实现了“置乱加密度”计算的算法，取原始图像 Lenna.bmp(图 1)，分别对其进行 Arnold 变换置乱和混沌置乱，得到置乱后的图像(图 2-图 5)，并计算“置乱加密度”，计算结果如表 1 所示。

从实验结果可以看出：利用 Arnold 变换进行图像置乱，当变换次数达到 3 次以上时，置乱后的图像给人的主观感觉都是比较乱的，根本看不出原始图像的残留痕迹，人的肉眼根本无法分辨出 3 次、4 次、5 次 Arnold 变换置乱后的图像哪一个的置乱效果更好。而通过计算“置乱加密度”，可以清楚地看到，随着 Arnold 变换次数的增加，计算出的 η 值也随之增大，说明 5 次 Arnold 变换的置乱加密效果好于 4 次和 3 次 Arnold 变换。通过进一步实验，计算出混沌置乱图像(图 5)的“置乱加密度”，从计算结果看出，计算出 η 的值远小于 Arnold 变换的 η 值，这说明在“置乱加密度”的客观评价意义下，图 5 的置乱效果不如图 2-图 4。但是，从人的主观感觉上看，图 5 似乎更“乱”一些，这是由于混沌映射产生的混沌序列是非周期、不收敛的，

图 1 Lenna 原图像

图 2 用 Arnold 变换的置乱图像(变换次数为 3 次)

图 3 用 Arnold 变换的置乱图像(变换次数为 4 次)

图 4 用 Arnold 变换的置乱图像(变换次数为 5 次)

图 5 混沌置乱图像(初始密钥为 0.750 000 001)

(下转 97 页)