基于均匀置乱的图像位置置乱衡量方法

张 健,任洪娥,陈 宇
ZHANG Jian,REN Hong-e,CHEN Yu

东北林业大学 信息与计算机工程学院,哈尔滨 150040
Information and Computer Engineering College,Northeast Forestry University,Harbin 150040,China
E-mail:zhangjianok00@163.com

ZHANG Jian,REN Hong-e,CHEN Yu.Evaluation algorithm of image position scrambling based on even scrambling. Computer Engineering and Applications,2010,46(11):22-25.

Abstract: Image scrambling is evaluated from position and pixel value according to the kind of image encryption.Currently,the evaluation effect of pixel value depends on the original image which has limitation.The evaluation effect of position maybe bring huge difference according to different distance which has limitation too.From the scrambling essential,the concept of even scrambling is presented.At the same time,an evaluation algorithm of image position scrambling is put forward based on deviation and evenness.The experiment results show that the algorithm can accurately evaluate the image scrambling degree and keep uniformity with visual,and has feasibility and validity.

Key words: image encryption;position scrambling;even scrambling;evaluation

摘 要: 由于图像置乱分成位置和像素值置乱两类,图像置乱衡量也从这两方面进行分析。目前基于像素值的衡量效果依赖于原始图像,存在局限性;基于位置的衡量随着置乱距离的不同效果也有很大偏差,同样存在局限性。从图像位置置乱的实质出发,提出均匀置乱的概念,从偏离度和均匀度的角度对图像位置置乱效果进行衡量。通过对大量实验结果的分析得出,该衡量算法可以准确地衡量图像置乱程度,与人的视觉评价保持一致,具有可行性和有效性。

关键词: 图像加密;位置置乱;均匀置乱;衡量
DOI: 10.3778/j.issn.1002-8331.2010.11.007 **文章编号:** 1002-8331(2010)11-0022-04 **文献标识码:** A **中图分类号:** TP391

1 引言

尽管数字图像置乱算法被不断提出,但是却很少有文献去衡量评价图像置乱的效果。对图像保密而言,图像置乱的效果越好,其隐蔽性越好,抗破解能力越强[1]。因此,对置乱程度的研究有重要的理论和实际意义。

目前还没有统一的图像置乱衡量标准,基于图像置乱分为位置置乱和像素值置乱, 衡量方法也是从这两方面进行考虑。一类算法是从像素值的角度进行衡量,包括不动点、信息熵、灰度变化平均值[2];相邻灰度差置乱度[3];基于图像局部方差的图像置乱度定义[4]等。该类方法存在一定的合理性,但由于衡量是从像素值的角度考虑,所以衡量必然依赖于原始图像,即图像本身的像素值性质很大程度上决定了衡量的结果,这样使该类方法存在一定的局限性。

另一类是从位置变化的角度进行分析[5-6],这些方法的实质是计算图像置乱前后的位置移动距离, 位置移动距离越大,置乱效果越好。但该类方法存在一个重要的问题,如果把一幅图像的像素点进行对角线对调,此时各像素点移动的平均距离相对较大,导致置乱效果极差。也就是说,从图像置乱前后的位置移动距离来判断置乱效果同样存在着局限性。

从图像置乱的实质出发,提出均匀置乱的概念,进而提出一种基于均匀置乱的图像位置置乱衡量算法,并通过对经典的位置置乱算法进行实验分析,来验证算法的准确性和有效性。

2 均匀置乱

2.1 图像置乱的实质

图像是由若干像素点组成的,这些点放在一起才能表现出图像所包含的信息。如果单纯一个点,不能形成图像的任何信息。所以,图像可以看作是由若干个像素点集合所构成,每个像素点集合包含若干个像素点。或者说每个像素点都具有其确定的像素值,若干个像素点按照一定的位置关系集合在一起则形成图像信息。

之所以能分辨出不同图像或同一幅图像的不同部分,是由

基金项目: 国家自然科学基金(the National Natural Science Foundation of China under Grant No.30972314);中央高校基本科研业务费专项资金资助(No.DL09BB16)。

作者简介: 张健(1980-),男,博士,讲师,主要研究领域为信息安全;任洪娥(1962-),女,博士,教授,主要研究领域为图像处理;陈宇(1975-),男,博士,讲师,主要研究领域为信息安全,电容层析。

收稿日期: 2010-01-27 **修回日期:** 2010-02-28

于构成图像的若干集合所表现出的信息不同。然而,图像位置置乱的实质就是要降低像素点位置之间的相关性直至无关,从而破坏这些集合所表现出的信息,实现图像置乱的目的。

要降低集合中所有点的位置相关性,就是将该集合中的点分散开,即分散到其他集合中,实现彼此位置的变化,导致原像素集合发生变化而改变其表达的信息,达到加密的目的。如何实现分散,分散到什么程度是接下来要探讨的内容。

2.2　均匀置乱

将同一小集合中的像素称为"相邻像素点",为破坏相邻像素点之间的相关性,应该将相邻像素点相互之间分散到尽可能远的位置,实现原图像中相邻像素点在置乱后图像中相互之间距离最远,即"最近的点到最远"。由于图像中像素点总的个数是固定的,所以移走的像素点必须由其他位置处的像素来填充,那么将原最远位置处的点移过来效果更好。那么原图像中最远的两个点在置乱后图像中成为相邻像素点,即"最远的点到最近"。由此,最大限度地破坏原图像各个小集合所表现出的信息,达到置乱的目的。

为有效说明这种关系,首先提出"块"的概念。

定义:在大小为 $M\times N$ 的图像中,以 $f(i,j)(1\leqslant i\leqslant M,1\leqslant j\leqslant N)$像素点为中心的 $m\times n(0\leqslant m<M,0\leqslant n<N)$个相邻像素组成的一个邻域,称之为块。

根据块的定义,图像可以看作是由任意形状和数量的块集合所组成,为便于讨论问题,将图像及图像中的每个分块都规定为正方形;将块内像素点的距离定义为 0,将不同块中的像素点的距离定义为块间的距离。

理论上,图像的块其本身越小越好,因为块越小,相邻像素最近则越合理,前述定义的"块内像素点距离为 0"越趋近于理想。其实,块越小就相当于图像的块数越多,而块数越多,前述定义的"两块中像素点间距离为块间距离"才越合理,越趋近于理想。

图像分块涉及到置乱前后图像的分块数量以及两者的相互关系。如何才能实现最佳置乱效果,是必须要解决的问题。

如果将原始图像分成 A_1 块、每块含有 B_1 个点,将置乱后的图像分成 A_2 块、每块含有 B_2 个点。那么,要实现原始图像每块中像素点之间的相互距离由"最近"到"最远",就要保证该块中的所有像素点被分到置乱后图像的不同块中,则 $A_2\geqslant B_1$,否则该块中至少有 2 个像素被分在置乱后图像的同一块中,其距离还是 0,没有实现"最近"到"最远"。同理,要实现原始图像各块中像素点间的距离由"最远"到"最近",就必须保证在原始图像中所有块中各取一点,都能分到置乱后图像的同一块中,则 $B_2\geqslant A_1$。

因为 $A_2\geqslant B_1$、$B_2\geqslant A_1$,所以

$$A_2B_2\geqslant B_1B_2;B_1B_2\geqslant A_1B_1 \tag{1}$$

即:

$$A_2B_2\geqslant B_1B_2\geqslant A_1B_1 \tag{2}$$

由于置乱前后图像的像素点总数并没有发生变化,所以总的像素点个数 A_2B_2 应该与 A_1B_1 相等,所以

$$\begin{cases}A_2=B_1\\A_1=B_2\end{cases} \tag{3}$$

因此,原始图像的块数与置乱后图像每块中的像素点个数相同;原始图像每块中的像素点个数与置乱后图像的块数相同。

有了这一分块前提,那么原始图像各块的相邻像素在置乱后图像中如何分布才能保证最佳置乱效果,是需要进一步讨论的问题。为此,给出了均匀置乱的定义。

定义　原始图像中每块含有 $n\times n$ 个点,如果这些点分别出现在置乱后图像的 $n\times n$ 个块中,不管这些点在置乱后图像各块中出现的顺序如何,只要保证每块中各含有一个点,就称为均匀置乱。

若满足均匀置乱,则原始图像中任一块内的所有相邻像素被分布到置乱后图像的不同块中,满足"最近到最远"的原则;若不满足均匀置乱,则原始图像中有两个或更多的相邻像素分布在置乱后图像的同一个块中,那么原始图像中的若干个相邻像素在置乱后图像中仍然为相邻像素,他们是"最近到最近"、违背了"最近到最远"的原则。

同样,若满足均匀置乱,则在原始图像每一块中存在一点,这些点将被分布到置乱后图像同一块中,满足"最远到最近"的原则;若不满足均匀置乱,则在原始图像中有两块或更多块中的不相邻像素分布在置乱后图像不同块中,那么原始图像中的若干个不相邻像素在置乱后图像中仍然为不相邻像素,他们是"最远到最远"、违背了"最远到最近"的原则。

均匀置乱提供了一种进行图像位置置乱的思想,将图像分块并进行均匀置乱是实现图像位置置乱的一种有效途径。如果置乱过程中按块实现了均匀置乱,则就分块层面而言达到了"原图最近的像素在置乱图中最远,原图最远的像素在置乱图中最近"的效果,即像素间的相关性降到最低。但即使在前面讨论和提出的分块原则下进行图像分块,也可以有多种结果,即图像的分块数可以不同。每一种分块方法都相应存在着一种均匀置乱及其置乱效果。那么,需要探讨将图像分成多少块的均匀置乱才能实现最佳置乱效果。

如前所述,对于图像的块,其本身越小越好,但原图的块小,其中包含的像素点就少,按照前述的分块原则"原图每块中的像素点个数与置乱后图像的块数相同",那么置乱后图像的块数就少,块就大,这与理论上块越小越好相矛盾;反之,如果置乱后图像的块小,其中包含的像素点就少,按照分块原则"原图的块数与置乱后图像每块中的像素点个数相同",那么原图的块数就少,块就大,这同样与理论上块越小越好相矛盾。所以必须保证原始图像和置乱后图像的分块都很小才符合要求。一种均衡状态就是原始图像的分块数与置乱后图像的分块数相同,此时分块为最佳分块。按照上述原则,若对一幅由 $N\times N$ 个点组成的方形原始图像,将图像平均分成 $N/n\times N/n$ 块,则均衡状态的分块数应为 $\sqrt{N}\times\sqrt{N}$ 块。但对于不同大小的图像来说,这个值不一定为可以实现均匀分块的整数,所以可以将与这个值相近的两个数作为理想的分块数。

3　基于均匀置乱的图像位置置乱衡量算法

如果位置置乱的结果满足均匀置乱,那么可以将这个置乱效果作为最佳置乱状态。所以通过判断置乱结果是否满足均匀置乱,或者符合均匀置乱的程度,就可以判断置乱程度的优劣。那么衡量位置置乱程度的问题就成为如何衡量均匀置乱程度的问题。为此提出偏离度和均匀度的概念,作为衡量均匀置乱程度即位置置乱程度的参数。

3.1　偏离度

根据均匀置乱的定义,同时为了衡量置乱后图像中每块是否都含有原始图像任一块的一个点,提出"环"的概念。

定义　在置乱后图像中,把以图像中心点为中心的最近的 4 个块作为第一层(最内层)环,把第一层环外与其相邻的最近

的所有块作为第二层环,以此类推,直到确定最外层环,如图 1 所示。

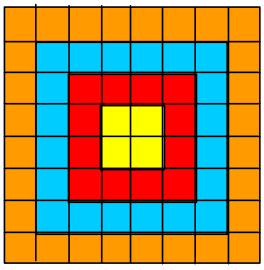


图 1　不同的环

经计算,如果原始图像的大小为 $N\times N$,分成 $M\times M$ 块,则置乱后图像环的个数为 $N/2M$。

在均匀置乱状态下,原始图像任一分块中的所有点在置乱后图像所有块中应该是每块有一个点。那么,每个环中的像素点个数可以用公式(4)表示:

$$\begin{cases} f(n)=4 & n=1 \\ f(n+1)=f(n)+8 & n>1 \end{cases} \tag{4}$$

式中:n 为由内至外的环,$f(n)$为第 n 个环所包含的原始图像任一块中的像素点个数。

设图像中心到第一个环的距离为 1,到第二个环的距离为 2,那么每个环的面积可以用式(5)表示:

$$\begin{cases} s(n)=(2\times n)^2 & n=1 \\ s(n)=4n^2-\sum_{i=1}^{n-1}s(i) & n>1 \end{cases} \tag{5}$$

式中:n 为正整数,$s(n)$代表由内到外第 n 个环的面积。那么均匀置乱状态下,通过计算,$s(n)$与$f(n)$的关系曲线如图 2 所示,是一条斜率为 45°的直线。所以在衡量图像置乱程度时,可以通过判断各环中的像素点个数与均匀置乱状态下各环中的像素点个数差别,来对图像置乱程度进行衡量。如果图像置乱满足图 2 所示的均匀置乱,那么将该置乱程度作为满足均匀置乱的一个必要条件。

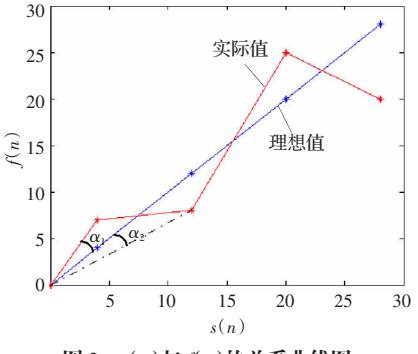


图 2　$s(n)$与$f(n)$的关系曲线图

当某一置乱程度得到的 $s(n)$与$f(n)$的关系曲线如图 2 所示的曲线,说明此时的置乱程度并没有达到均匀置乱,需要进一步判断其偏离程度。

为此,将图 2 中实际每个环的置乱程度$f(1)$与均匀置乱时的偏离角记为 α_1,将$f(2)$与均匀置乱状态直线的偏离角记为 α_2,其他同理。偏离角代表在对某种置乱程度进行衡量时,置乱后图像每个环中包含原始图像任一块像素点个数与均匀置乱的偏离程度。

将原始图像中的所有分块进行分析,计算每一块中各个环的偏离角,取所有环的平均偏离角,记为:$\overline{\alpha_1}=\sum_{i=1}^{M^2}\alpha_1/M^2$,$\overline{\alpha_2}=\sum_{i=1}^{M^2}\alpha_2/M^2,\cdots$。

平均偏离角代表在对某种置乱程度进行衡量时,置乱后图像每个环中包含原始图像所有块像素点个数与均匀置乱的偏离程度。

将所有环进行衡量分析,取所有平均偏离角的平均值,定义为偏离度 $\Delta\alpha$。

$$\Delta\alpha=\frac{\sum_{i=1}^{N/2M}\overline{\alpha_i}}{N/2M} \tag{6}$$

$\Delta\alpha$ 的取值范围是[0,33.685],$\Delta\alpha$ 代表通过判断置乱后图像每个环中包含原始图像任一块像素点个数与均匀置乱时的偏离程度,来进行衡量。$\Delta\alpha$ 越小说明图像置乱程度越接近于均匀置乱。

当图像没有置乱时,偏离度应该为最大值 45,而实际上图像没有置乱的值并不是 45。经实验计算得出,最大值为 33.685。

3.2　均匀度

前面提到如果图像置乱满足图 2 所示的均匀置乱,那么该置乱程度只能作为满足均匀置乱的一个必要条件。因为偏离度是从环的角度衡量图像置乱程度是否满足均匀置乱,而环中包含若干块,环中像素点满足均匀置乱并不能保证每个块都满足均匀置乱。如图 1 的最内层 4 个块中,至少有一个块没有原始图像某块中的像素点,有一块又多于原始图像某块中含有的一个像素点,但同时也满足最内层环有 4 个像素点。这时并没有实现均匀置乱,但用偏离度衡量却得出均匀置乱的结论。所以在用偏离度判断满足“均匀置乱”的基础上,需要再考虑另一个重要指标,即判断环中每块是否满足均匀置乱。

以 256×256 图像为例进行说明,把置乱后图像分成 8×8=64 块,如图 1 所示。如果满足均匀置乱,原始图像中任取一块的所有像素点,共 64 个像素点应该均匀置乱在置乱后图像的 64 个块中,即每块含有一个像素点。在置乱程度衡量时,原始图像任一块的 64 个点,如果出现在置乱后图像的某个块中,不管该块中包含这 64 个像素点中的几个,都将该块记为 $p_k=1/64$,如果某个块没有出现这 64 个点中任何一个点,将该块记为 $p_k=0$。那么,均匀置乱状态下,置乱后图像的 64 块应该满足公式(7):

$$\sum_{k=1}^{64}p_k=1 \tag{7}$$

写成一般形式,假设原始图像的大小为 $N\times N$,分成 $M\times M$ 块,则均匀置乱状态下原始图像中任取一块 A,将置乱后图像各块含有 A 块中的点记为 $p_k=M^2/N^2$,不含有记为 0,则

$$\sum_{k=1}^{N^2/M^2}p_k=1 \tag{8}$$

在实际衡量时,为了计算的方便,当置乱后图像各块中含有原始图像任取一块 A 中的点记为 1(含有多于一个点也记为 1),没有点记为 0。有点的块数总和记为 n_k,那么定义原始图像中块 A 的均匀度 P_A 如式(9)所示:

$$\Delta P=\frac{n_k}{N^2/M^2} \tag{9}$$

块 A 的均匀度 P_A 代表在对某种置乱程度进行衡量时,原

始图像中块 A 中所有点置乱后符合均匀置乱的程度。

对原始图像所有块进行衡量分析,取所有块均匀度的平均值,定义为偏离度 ΔP。

$$\Delta P=\frac{\sum_{i=1}^{N\times M}P_i}{M\times M} \tag{10}$$

ΔP 的取值范围是[0,1],ΔP 代表通过判断原始图像中块 A 所有点置乱后满足均匀置乱程度的方式进行置乱程度衡量时,置乱程度与均匀置乱的偏离程度。ΔP 越大说明图像置乱程度越接近于均匀置乱。

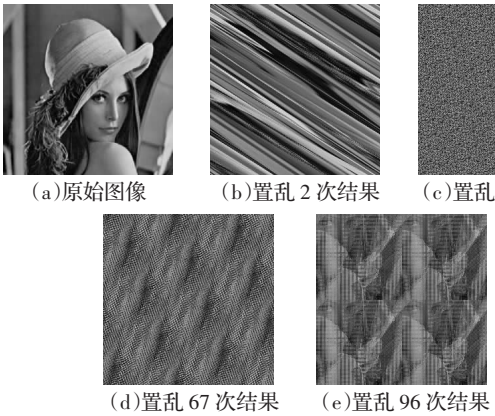
在实际图像置乱程度衡量时,先进行偏离度 $\Delta\alpha$ 的衡量,如果偏离度 $\Delta\alpha$ 很小,再判断是否满足均匀度;如果偏离度 $\Delta\alpha$ 很大,说明其不具备满足均匀置乱的条件,无需再判断均匀度。如果两个指标都达到了比较理想的状态,就可以判定该置乱程度是比较理想的。

4　实验及分析

实验图像从著名的美国南加州大学 USI-SIPI image database(http://sipi.usc.edu/services/database/index.html)和美国麻省 media 实验室图像库(http://vismod.media.mit.edu/)中选择的。通过对大量图像进行实验分析,均得到了一致的结果,现选取最经典的 lena 图像进行说明,图像大小为 256×256,如图 3(a)所示,用最经典的图像位置置乱算法 Arnold cat 变换进行图像置乱,Arnold cat 变换的参数 a=2,b=2。置乱 2 次、27 次、67 次、96 次的效果分别如图 3(b)~(e)所示。

从视觉上看,置乱 27 次和 67 次的效果要明显好于 2 次和 96 次;27 次要好于 67 次;96 次表现出了原始图像的信息,应该是效果最差。接下来从是否满足均匀置乱的角度,利用提出的偏离度和均匀度进行衡量,来验证该算法与视觉的吻合程度。

将原始图像分成 16×16 块,则原图像每块有 16×16 个像素点,置乱后的图像分为 16×16 块。根据公式(6)计算偏离度 $\Delta\alpha$,其数据如表 1 所示。图 4 为 Arnold cat 变换置乱 2 次,27 次,67 次,96 次的置乱程度与均匀置乱的偏离度比较图。



(a)原始图像　(b)置乱 2 次结果　(c)置乱 27 次结果

(d)置乱 67 次结果　(e)置乱 96 次结果

图 3　原始图像与置乱后的图像

表 1　偏离度 $\Delta\alpha$

置乱次数	2	27	67	96
偏离度	16.805 9	0.705 4	5.491 4	21.107 5

通过表 1 和图 4 可以很清楚地看到,置乱效果优劣依次为 27 次、67 次、96 次和 2 次。这与视觉评价完全吻合,这说明将原始图像分成 16×16 块进行衡量的准确性,符合前面在均匀置乱探讨时得出的结论。

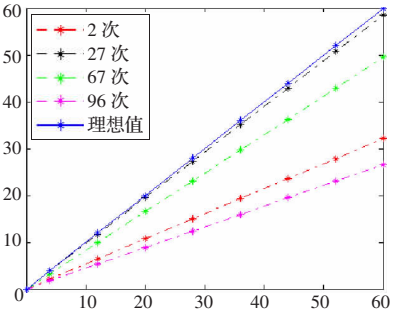


图 4　置乱程度与均匀置乱的偏离度比较图

在这 4 次置乱中,置乱 27 次和 67 次的效果相对最好,也就是说用偏离度进行衡量得出的结论是:置乱 27 次和 67 次的效果都接近于均匀置乱。对两个都接近均匀置乱的不同置乱次数,可以通过均匀度进一步验证。根据公式(10)计算均匀度,其数据如表 2 所示。

表 2　均匀度 ΔP

置乱次数	27	67
16×16 块	0.726 6	0.164 1

通过表 2 可以看出,置乱 27 次要明显好于 67 次,与视觉评价一致,再一次验证了该算法的准确性和有效性。

针对其他的经典位置置乱算法面包师变换、Hilbert 曲线变换以及 Zigzag 曲线变换,从偏离度和均匀度两个方面进行了大量的实验,由于篇幅有限,不能一一列举,但均得到如下结论:

(1)衡量效果与人的视觉评价完全吻合;

(2)衡量算法是从位置的角度进行分析,不依赖于原始图像;

(3)对 256×256 的原始图像,分块为 16×16 衡量最准确;对 512×512 的原始图像,分块为 16×16 和 32×32 都可以很好地衡量置乱程度与均匀置乱的偏离程度。这也符合前面提到的均匀置乱分块原则。

5　结论

从图像位置置乱的实质出发,提出了均匀置乱的概念,进而提出了可以通过计算偏离度和均匀度来衡量图像置乱效果的优劣。从大量实验结果中得出该算法衡量效果与人的视觉评价相吻合,具有可行性和有效性。

参考文献:

[1] 任洪娥,尚振伟,张健.适用于矩形图像的新二维映射图像加密算法[J].光学精密工程,2008(8):1483-1489.

[2] 王迤冉,朱维军,詹新生.基于图像加密的置乱性能分析研究[J].计算机工程与设计,2006,27(24):4729-4731.

[3] 向德生,熊岳山.基于约瑟夫遍历的数字图像置乱算法[J].计算机工程与应用,2005,41(10):44-46.

[4] 张小华,刘芳,焦李成.一种基于混沌序列的图象加密技术[J].中国图象图形学报,2003,8(4):374-378.

[5] Kwok H S,Tang W K S.A fast image encryption system based on chaotic maps with finite precision representation[J].Chaos,Solitons & Fractals,2007,32(4):1518-1529.

[6] Kingston A,Svalbe I.Generalised finite radon transform for $N\times N$ images[J].Image and Vision Computing,2007:1620-1630.