一种新的基于概率距离的图像置乱评价方法

刘建华[1]，韩纯洁[2]，范九伦[1]，袁岁维[1]
（1. 西安邮电学院 信息与控制系，西安 710061；2. 西北电子设备研究所，西安 710065）

摘　要：通过对图像的分块处理，提出一种评价图像置乱效果的方法。将原图像与加密图像进行相同的分块处理后，计算分块变换前后概率分布差异的 Bhattacharyya 系数，并以所有分块 Bhattacharyya 系数的平均值作为图像在置乱变换下具有的置乱程度。该方法计算简单、意义明确；实验结果表明，该方法可以有效地反映出图像在不同置乱变换下具有的置乱程度。

关键词：置乱变换；分块处理；Bhattacharyya 系数；置乱程度
中图分类号：TP391　　**文献标志码**：A　　**文章编号**：1001-3695(2010)03-1083-03
doi:10.3969/j.issn.1001-3695.2010.03.076

New image scrambling evaluation method based on probability distance

LIU Jian-hua[1], HAN Chun-jie[2], FAN Jiu-lun[1], YUAN Sui-wei[1]
(1. *Dept. of Information & Control, Xi'an University of Post & Telecommunications, Xi'an* 710061, *China*; 2. *Northwest Electronics Equipment Institute, Xi'an* 710065, *China*)

Abstract: This paper proposed a method for evaluating image scrambling effect through the way of block processing. After processing the initial and encrypted images with the same block size, Bhattacharyya coefficients between the initial and encrypted image probability distributions were calculated, and then treating the average value of all blocks as the scrambling degree of the scrambling transformation. New method was simple and the meaning was clean. Experimental results show that the method can reflect the scrambling degree under different scrambling transformation.

Key words: scrambling transformation; block processing; Bhattacharyya coefficient; scrambling degree

0　引言

网络技术的迅速发展给人们的生活带来了极大的便利，人们通过网络传递所需的信息。而网络的开放性也使非法用户有机会截取他人的敏感信息，因此如何保证网络数据的安全传输成为一个热点研究问题。数字图像作为网络信息的一种重要载体，针对其安全传输，目前主要采用信息隐藏与伪装技术，包括数字图像置乱技术、数字图像分存技术、数字图像隐藏技术和数字水印技术等。通过这些技术可以将嵌有秘密信息的图像变得杂乱无章，以降低图像在传输过程中遭受攻击的可能性。

一般而言，图像置乱加密的效果越好，将秘密信息隐藏在其内的隐蔽性就越好，即秘密信息具有越高的抗检测攻击能力，可以更加安全地进行传输。因此，图像信息在传输之前的加密处理可以极大地提高信息安全传输的能力。而采用不同的加密算法处理图像，可以得到不同的加密结果图像，导致了隐藏在图像内的秘密信息被检测出来的可能性也不相同。因此，有必要寻求一种能够客观评价不同图像置乱变换具有的置乱程度的方法，以指导人们寻找置乱性能更好的图像置乱算法。

目前已有很多评价图像置乱效果的方法。文献[1]提出了利用不动点、自然率、k 阶位置因子、k 阶矩、置乱矩阵的相关性等方法度量图像的置乱程度。文献[2]充分考虑了图像置乱前后像素点位置的变化情形，提出了基于距离思想的置乱程度评价方法及其改进的方法。引进图像分块，依据图像变换前后任意一个灰度值在每一个小分块中所占的比例与其在整幅图像中所占的比例相同为最佳变换，提出了基于 Walsh 变换的图像置乱程度的定义。文献[3]将交叉熵的思想引入图像置乱度的评价中，与图像的最优分块相结合，对各分块交叉熵值进行统计平均，得到置乱算法的置乱程度。文献[4]提出以图像分块信息熵和整体信息熵的比值作为置乱程度的判决标准，同时利用各分块中互为相邻的像素差值的平均值作为加权系数进行加权平均，得出了基于信息熵的图像置乱度评价方法。

本文在已有的图像置乱程度评价算法的基础上，利用 Bhattacharyya 系数[5]提出一种新的图像置乱程度的评价方法。以信息论中度量两个概率分布相似程度的 Bhattacharyya 系数为出发点，在对图像进行自主分块的基础上，通过统计图像变换前后所有分块像素值的概率分布，计算图像变换前后概率分布变化的 Bhattacharyya 系数，以得到的系数平均值作为该变换具有的置乱程度。

1　数字图像的置乱变换

为了说明本文提出的置乱程度评价算法的原理，本文选用常用的 Arnold 变换和 Fibonacci 变换对测试图像进行变换得到

收稿日期：2009-06-11；**修回日期**：2009-08-31

作者简介：刘建华(1963-)，男，河北易县人，高级工程师，主要研究方向为信息安全；韩纯洁(1972-)，男，陕西人，高级工程师，硕士，主要研究方向为机床数控系统维护；范九伦(1964-)，男，陕西西安人，教授，博导，主要研究方向为模式识别、信息安全、图像处理；袁岁维(1985-)，女，陕西咸阳人，硕士研究生，主要研究方向为图像处理(qu_yuan_5@163.com)。

加密图像,以测试本文方法的性能。

由文献[2]可知,对于一幅给定的数字图像 A,可以将其视为二维矩阵 $A=[a(i,j)]_{m\times n}$,二维矩阵在(i,j)处的值即为图像在(i,j)处的像素值,设变换 T 为 A 到其自身的一一映射,即满足:

$$\begin{pmatrix} x_1 \\ y_1 \end{pmatrix} = T\begin{pmatrix} x \\ y \end{pmatrix} \tag{1}$$

式(1)表示将图像 A 中(x,y)处的像素值在变换 T 的作用下变换至(x_1,y_1)处。用相同的方法可以遍历图像的所有像素点,得到图像 B,则称变换 T 是图像 A 的置乱变换。当 $T=\begin{pmatrix} a & b \\ c & d \end{pmatrix}$,且 $ad-bc=\pm 1$ 时,称变换 T 为几何变换。特别地,当 $a=b=c=1,d=2$ 时,即为 Arnold 变换;$a=b=c=1,d=0$ 时,即为Fibonacci变换。本文选用这两种变换的离散形式对图像进行变换处理,将图像中的点进行离散化处理,引入模运算。图 1 给出了实验中用到的测试图像 Lena 和 people,大小均为 256×256。

图 1　测试图像

Arnold 变换是一种具有周期性的置乱变换,变换周期与图像大小具有一定的关系;Fibonacci 变换与 Arnold 变换同属于几何变换,两者仅是参数存在一定的差异。以下通过实验对测试图像在这两种变换下具有的置乱程度进行比较。

图 2 和 3 分别给出了测试图像 Lena 在两种变换下经过不同加密次数得到的加密结果图像。从整体上看,在相同加密次数下,Arnold 变换的加密效果优于 Fibonacci 变换的加密效果。

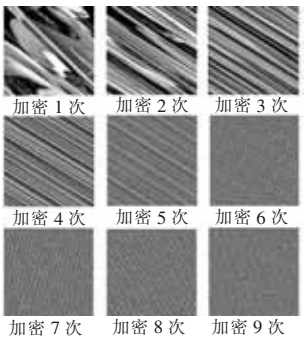

图 2　Lena 在 Arnold 变换下的加密结果图像

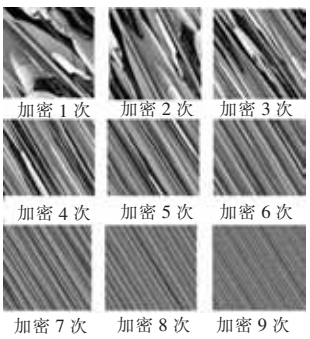

图 3　Lena 在 Fibonacci 变换下的加密结果图像

2　一种新的评价方法

2.1　Bhattacharyya 系数

在信息论中,对于两个概率分布 $X=\{x_1,x_2,\cdots,x_i,\cdots,x_n\}$ 与 $Y=\{y_1,y_2,\cdots,y_i,\cdots,y_n\}$ 之间的相似度可以用 Bhattacharyya 系数进行度量[5],其定义式为

$$B(X,Y)=\sum_{i=1}^{n}\sqrt{x_i y_i} \tag{2}$$

利用 Bhattacharyya 系数度量相似度的最大优点是不用考虑分布中概率值是否为零的情形,在一定程度上避免了使用交叉熵[3]时必须考虑在分布的概率值相除时分母必须不为零的情形,这也是本文选用 Bhattacharyya 系数的主要原因。将 Bhattacharyya 系数引入图像置乱程度的评价中,可以理解为观察者根据原图像和加密图像具有的概率分布而获得的对于图像变换前后信息量的差异。借助于 Bhattacharyya 系数,对图像变化前后概率分布具有的差异进行度量,可以反映出图像在置乱变换下具有的置乱度。

2.2　实验原理及步骤

原图像记为 A,大小为 $M\times N$,经过置乱变换后得到的加密结果图像记为 B。为了评价选用的置乱变换具有的置乱度,分别对原图像和加密图像进行分块处理,分块方式分为有重叠和无重叠两种。为了防止由于对图像不能进行完全分块而忽略图像信息的情形,或者由于对图像进行补零处理时引入不必要的误差信息,算法中要求图像的分块大小宜为图像大小的整数分之一。

在每一个小分块中,记像素总数为 N,以行序为主序,记原图像(i,j)处像素值在分块中所有像素值中所占概率为 p_i,加密图像(i,j)处像素值在分块中所有像素值中所占概率为 q_i,任一分块在变换前后概率值变化的 Bhattacharyya 系数定义为

$$D(i,j)=\sum_{i=1}^{N}\sqrt{p_i\times q_i} \tag{3}$$

该值越小,加密图像的效果越好;反之,加密图像的效果越差。对各个分块得到的 Bhattacharyya 系数值进行统计平均,以平均值作为算法具有的置乱程度。

算法的具体过程如下:

a)对原图像和加密图像按照相同的分块大小进行分块处理。为了便于计算,分块大小一般选为图像大小的整数分之一。

b)经分块处理后,原图像的任一个小分块在加密图像的相应位置处均有一个对应的小分块,分别统计原图像和加密图像所有分块中像素值的概率分布。对于每一个小分块中所有像素值的概率分布,利用式(3)计算出每一个分块的 Bhattacharyya 系数。

c)对所有小分块的 Bhattacharyya 系数进行求和,除以分块个数和分块大小的乘积,得到所用置乱变换具有的置乱度。

3　实验结果及分析

图 4 给出了 Lena 图像在 Arnold 变换下选用不同大小的分块(2×2,4×4,8×8)时得到的置乱程度与加密次数的关系曲线,分块方式为无重叠。

从图 4 中可以看出,对于任意一种分块方式,所得到的置乱度曲线具有大致相同的趋势,并且在一个周期内,置乱度曲线关于半周期具有明显的对称性,符合 Arnold 变换具有的半周期性。由于分块大小的不同,导致对原图和加密图像进行分块后分块数目以及各个分块中的元素个数有所差异,因此,所得到的置乱度曲线在数值上有所差异,但并不影响对加密效果的评价。

图 5 给出了 Lena 图像采用 Arnold 变换和 Fibonacci 变换得到的置乱度与加密次数的关系曲线。其中分块大小为 8×8,分块方式为无重叠。

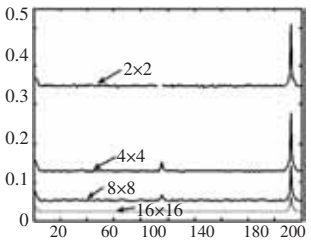

图 4　Lena 在不同分块大小下的置乱度曲线

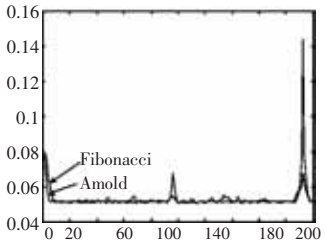

图 5　分块大小为 8×8 时得到的置乱度曲线

表 1 给出了 Lena 图像在两种变换下前 10 次加密中具有的置乱效果。可以看出在相同的加密次数下,Arnold 变换比 Fibonacci 变换的加密效果在整体上都要好一些,这一点与本文给出的图 2 和 3 的实验结果是一致的。

表 1　分块大小为 8 ×8 时得到的置乱程度

加密次数	1	2	3	4	5	6	7	8	9
Arnold	0.0775	0.0691	0.0601	0.0545	0.0516	0.0513	0.0514	0.0515	0.0515
Fibonacci	0.0796	0.0782	0.0745	0.0642	0.0624	0.0575	0.0541	0.0525	0.0519

图 6 给出了测试图像 Lena 与 people 在 Arnold 变换下,分块大小为 8 ×8 时分别得到的置乱度曲线,分块方式为无重叠。由图 6 可知,对于不同的测试图像均可以选用本方法进行测试在不同加密次数下加密图像具有的置乱程度。曲线关于各个图像均具有半对称性,不同图像置乱程度的差异可能是图像自身存在的差异所引起的,并不影响该方法对单个图像在不同加密次数下置乱程度的衡量。

图 7 给出了采用有重叠的分块方式时,对 Lena 图像在 Arnold变换下得到的一个周期内的置乱度曲线与加密次数的关系曲线。图像原分块大小为 16 ×16,有重叠的方式为下一个分块与上一个分块的距离选为原分块大小的一半,即等价于每次只移动 8 ×8 的距离。

由实验结果可知,采用有重叠的分块方式得到的置乱度曲线与采用无重叠分块方式得到的置乱度曲线具有相同的形状,而两者在数值上的差异可能是由于计算平均置乱度时,分块中像素个数不同而导致概率分布的不同以及分块个数的不同引起的,但并不影响对图像置乱效果的评价。

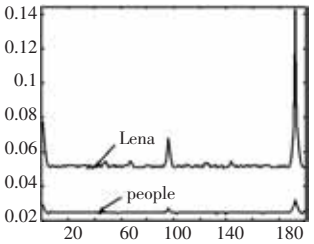

图 6　Lena 与 people 的置乱度曲线

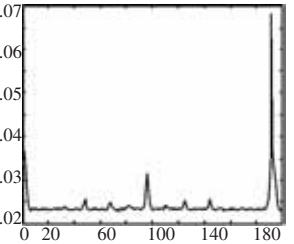
图 7　有重叠下的置乱度与加密次数的关系曲线

4　结束语

本文利用 Bhattacharyya 系数给出了一种新的评价图像置乱效果的方法。通过实验可知,该方法可以很好地刻画图像在同一变换下在不同加密次数下具有的置乱程度,符合人类的视觉特性,因此可以作为一种衡量图像置乱效果的方法。

参考文献:

[1] 秦红磊,郝燕玲,孙枫. 一种基于混沌的图像置乱网络设计[J]. 计算机工程与应用,2002,38(7):104-106.

[2] 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,2006:94-108.

[3] 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.

[4] 张华熊,吕辉,翁向军. 基于信息熵的图像置乱程度评价方法[J]. 电路与系统学报,2007, 12(6):95-98.

[5] BHATTACHARYYA A. On a measure of divergence between two statistical populations[J]. SIAM Journal Algebraic Discrete Methods,1964(5):1-8.

(上接第 1073 页)

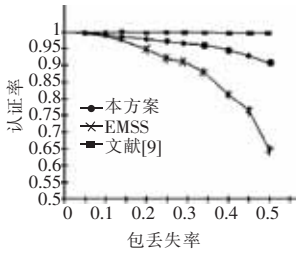

图 3　通信代价为 60 时的仿真结果

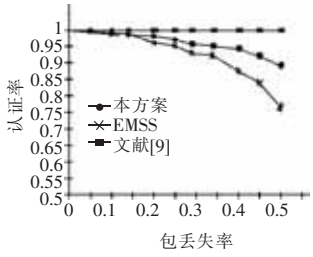

图 4　通信代价为 80 时的仿真结果

表 2　本方案和 T-CSA 方案的比较

比较项	本方案	T-CSA
收到一个密钥可验证的数据包个数	2^k	1
包平均延迟时间	小	大

3　结束语

组播源认证作为组播的核心问题备受关注,设计一个安全、高效的不可否认组播源认证协议迫在眉睫[10]。本文在分析以往提出的一些组播源认证方案的基础上,提出了一种新的组播源认证方案。分析表明,基于数链认证技术的新方案最大的特色在于:随着数据流的不断增多,每个包平均的认证代价会不断下降,而且对接收方缓存要求不高,延迟较小,但其认证率低于文献[9]方案。该方案特别适用于数据量比较大、接收方资源有限,而且对延迟敏感的一些组播应用。

参考文献:

[1] WONG C K,LAM S S. Digital signatures for flows and multicasts[J]. IEEE ACM Trans on Networking, 1999,7(4):502-513.

[2] GENNARO R,ROHATGI P. How to sign digital streams[J]. Information and Computation,2001,165(1):100-116.

[3] GOLLE P,MODADUGO N. Streamed authentication in the presence of random packet loss[C]//Proc of ISOC Network and Distributed System Security Symposium. 2001:13-22.

[4] PERRIG A,CANETTI R,TYGAR J D,*et al*. Efficient authentication and signing of multicast streams over lossy channels[C]//Proc of IEEE Symposium on Security and Privacy. 2000:56-73.

[5] BERGADANO F,CAVAGNINO D. Dealing with packet loss in the interactive chained stream authentication protocol[J]. Computers & Security,2005,24(2):139-146.

[6] WANG Wei-dong,LI Zhi-tang,LU Chui-wei,*et al*. An efficient multicast source authentication protocol[J]. Wuhan University Journal of Natural Sciences,2006,11(6):1831-1834.

[7] LI Bao-hong, HOU Yi-bin. Performance optimization for multicast packet authentication[J]. Journal of Chongqing University: English Edition,2005,4(3):154-157.

[8] BERGADANO F,CAVAGNINO D,CRISPO B. Individual authentication in multiparty communications[J]. Computers & Security, 2002,21(8):719-735.

[9] PARK Y S,CHUNG T S,CHO Y. An efficient stream authentication scheme using tree chaining[J]. Information Processing Letters, 2003,86(1):1-8.

[10] BARNETT C A. Efficient reliable and secure source authentication schemes for real-time multicast[D]. Maryland: University of Maryland, 2003.