

文章编号:1001-9081(2010)02-0525-04

基于伪随机点的混合图像融合加密方法

顾萃琛, 胡金初

(上海师范大学 信息与机电工程学院, 上海 200234)

(gucui chen@126.com)

摘要: 图像数据在网上传输需要经过加密处理,而现在很多加密算法都遵循动力学的衰退原理,会退化成具有周期性的算法,而会导致图像信息的泄漏等问题。提出一种基于伪随机点的混合图像融合算法,它先把图像分成 8×8 的小块,然后对每块图像进行变换,产生一个伪随机序列,将图像块内的像素值和按伪随机序列所对应的像素值相融合进行一次置乱,然后对EZW编码后的图像用混沌序列再一次置乱。试验结果表明,该算法具有很好的安全性,也比较容易实现。

关键词: 图像融合; 置乱; 伪随机序列; 混沌序列; 单向函数

中图分类号: TP751; TP309; TP391.41 **文献标志码:** A

Mixed image fusion encryption based on pseudo-random points

GU Cui-chen, HU Jin-chu

(College of Information and Mechanical Engineering, Shanghai Normal University, Shanghai 200234, China)

Abstract: Encryption is very important in image data transmission on Internet, but most of all encryption algorithms following the principle of dynamics of recession will be degraded into a cyclical algorithm, which leads to the leakage of image information and so on. Based on pseudo-random points, a mixed image fusion algorithm was presented. Firstly the image was divided into 8×8 small blocks, and then each block was transformed to create a pseudo-random sequence. The image block pixel values and their related pseudo-random sequence were fused and scrambled, and the image after EZW coding was scrambled again by chaotic sequence. Test results show that the algorithm has good security, and the algorithm is also relatively easy to achieve.

Key words: image fusion; permutation; pseudo-random sequence; chaos sequence; one-way function

0 引言

图像信息已经成为通信和计算机系统中一种重要的处理对象,与文字信息不同的是图像信息占据大量的存储空间。如何很好地保留图像信息并不让信息泄漏就是我们要考虑的首要问题。

图像加密算法是保证图像在网络中传输安全性的主要途径,加密算法主要包括分块加密算法、流加密算法以及置乱加密算法。现在运用的较多的是图像置乱算法,由于置乱加密算法具有加密效率高、加密效果好、鲁棒性强等优势而受到人们的广泛关注。常见的置乱加密算法有:基于Arnold变换的置乱技术^[1]、基于混沌序列的置乱技术^[2]、伪随机序列算法^[3]、DCT系数全置乱算法、幻方算法等。Tang提出的DCT系数全置乱算法^[4]是一种典型的基于一次置乱的DCT系数加密算法,并且由于DC系数明显区别于各AC系数这一特性,该算法很难抵御唯密文攻击。置乱算法在计算机上的实现存在退化,会造成算法的周期性变换而容易被破解,造成信息的泄漏,而现在两种不同置乱算法的混合使用虽然可以使图像的安全性提高,但却增加了算法的时间复杂度。

目前存在的置乱加密算法主要问题有:1)图像的DC系数没有得到保护;2)加密算法运算复杂度高。本文提出了一种运用置乱与像素值替代相结合的加密算法,解决了加密算法存在的一些问题,较好地克服了目前加密算法中存在的主

要问题。

1 基于伪随机点的混合图像融合加密方法

通过对数字图像像素值点分布的分析我们可以发现,图像的重要信息都集中在低频区域中,而高频的部分都是反映图像细节的。小波变换是无损的,能很好地将图像的重要细节保留下来,同时运用小波的多重分解可以把图像按频率进行分离,把图像用高频滤波器和低频滤波器分离开来,根据自己的要求有针对性地对需要的图像进行处理,达到所期望的结果,是现在使用广泛的一种数字图像处理方式。

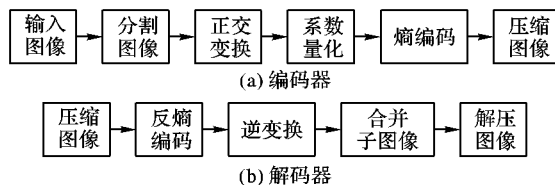


图1 编码器与解码器框图

现在使用的JPEG标准是对图像的DCT系数做熵编码,而基于伪随机点的混合图像融合加密方法采用的是小波编码。

1.1 背景介绍

混沌现象是在确定性的非线性动力系统中出现的类似随机的现象。这种过程既非周期又不收敛,并且对初始值有敏感

收稿日期:2009-08-07;修回日期:2009-09-28。 基金项目:上海市教委基金资助项目(06DZ003)。

作者简介:顾萃琛(1984-),男,浙江宁波人,硕士研究生,主要研究方向:网络与多媒体; 胡金初(1949-),男,上海人,教授,主要研究方向:网络、多媒体。

的依赖性。一维多参数非线性动力系统定义如下: $X_{n+1} = G(X_n, \mu_i)$, 其中 μ_i 为参数, X_n 为状态, 而 G 是一个映射, 把当前状态从 X_n 映射到下一个状态 X_{n+1} 。如果从初始值 X_0 开始反复应用这种映射关系, 就可以得到一个序列 $\{X_m | m = 0, 1, 2, \dots\}$, 这一序列就称为离散时间动力系统的一条轨迹。如果为 μ_i 选择恰当的数值, 使 G 满足三个条件 (即 G 具有对初始条件的敏感性和依赖性, G 是拓扑传递的, G 的点分布稠密), 则对应的动力系统是混沌的。其中 Logistic 映射是比较具有代表性的映射。它的定义为 $X_{n+1} = \mu X_n (1 - X_n)$, 其中 $0 \leq \mu \leq 4$ 称为分支参数, $X_n \in (0, 1)$ 。当 $3.569945972 < \mu \leq 4$ 时, 该动力系统进入混沌状态。进入混沌区域后, 系统的混沌就变得非常复杂。

图2中, X 轴表示 μ 的取值范围, Y 轴表示状态 X_n 的范围。

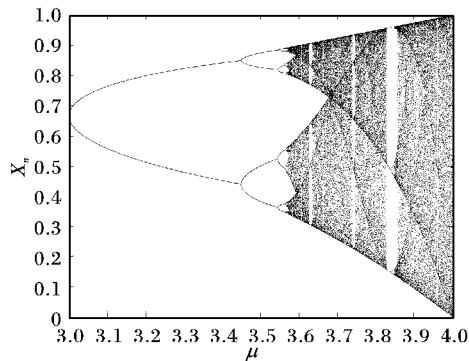


图2 Logistics 分岔图

图3中, a 的初值是5, b 的初值是5.1, c 的初值是5.2。 Y 轴表示取值, X 轴表示迭代的次数。

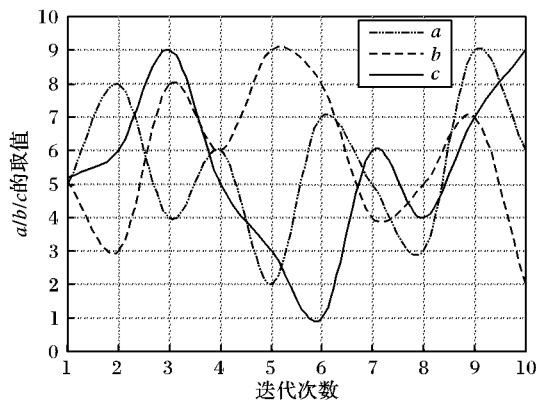


图3 Logistic 映射对初值的敏感性

由以上的实验数据可以清楚看到, Logistic 映射对初始值是相当敏感的, 同时也可以证明初始条件微小的改变都会得到完全不同的结果, 它与混沌序列对初始值敏感是一致的。

$\sin x, \cos x$ 都可以用泰勒级数或麦克劳林级数展开为无穷级数, 具体展开式如下:

$$\sin x = x - \frac{x^3}{3!} + \frac{x^5}{5!} - \frac{x^7}{7!} + \dots = \sum_{n=0}^{\infty} \frac{(-1)^n x^{2n+1}}{(2n+1)!}$$

$$\cos x = 1 - \frac{x^2}{2!} + \frac{x^4}{4!} - \frac{x^6}{6!} + \dots = \sum_{n=0}^{\infty} \frac{(-1)^n x^{2n}}{(2n)!}$$

而且在实数域上分布均匀, 函数的可微性和连续性较好, 又符合图像分布的特性, 所以这里用函数 $G(i, j) = |s \times \sin(u \times i) + t \times \cos(v \times j)|$ 在 $[0, 1]$ 上的映射来确定 X_0 , 并把 X_0 的输出作为 Logistic 映射的控制参数, 由于 s, u, t, v 都是随机数, 这样生成的初始条件具有很强的隐蔽性, 也增强了混沌序列的随机性。

1.2 方法的具体实现

先将 $m \times n$ 的图像分成 8×8 的块, 对每块图像进行处理。然后利用图像融合的方法将图像进行操作生成一个新的图像, 确定一个输入序列, 作为单向函数的输入, 生成一个伪随机序列, 将两个像素值进行融合。然后将得到的图像做 EZW 编码, 再把编码后的图像用混沌序列进行再次置乱, 使图像的安全性大大提高。

a, b, s, t, u, v 是随机正整数, μ 是一个确定的常数。记原图像为 F , 由 $a + b \times c$ 的值作为输入端生成的伪随机序列对应的目标图像为 O , 融合结果图像为 E , 两幅图像上对应像素 (i, j) 的灰度值分别记为 $F(i, j)$ 和 $O(i, j)$, 其中 $F(i, j)$ 为原图像在 (i, j) 处的像素灰度值, $O(i, j)$ 为目标图像在 (i, j) 处的像素灰度值。 c 是图像块内图像按 zigzag 方式得到的离散余弦变换 (Discrete Cosine Transform, DCT) 系数序列的编号。采用 SHA 中的散列函数来作为单向函数。

1.2.1 加密算法

将参数 a, b 代入, 计算 $a + b \times c$ 的值, 把它作为单向函数的输入, 可以得到新的序列。此序列就是图像融合的对象序列, 用融合公式生成新的图像灰度值, 计算 $s \times (b + a \times c) + t \times (a + b \times c)$ 的值并以此作为单向函数的输入, 由序列生成置乱矩阵, 把融合后的图像置乱, 至此离散余弦变换 DCT 系数置乱结束。用 Logistic 映射对 EZW 编码后的系数再次进行置乱。

1) 利用图像融合加密公式: $E(i, j) = (O(i, j) + F(i, j)) / 2$, 生成新的灰度图像值。

2) 将图中所有块全部采用上面的方法进行融合。

3) 计算 $s \times (b + a \times c) + t \times (a + b \times c)$ 的值并以此作为单向函数的输入生成一个伪随机序列, 由该序列组成一个置乱矩阵。

4) 重复3) 直到把全部图像块的系数全部置乱。

5) 计算 $G(i, j) = |s \times \sin(u \times i) + t \times \cos(v \times j)|$ 的值, 作为 Logistic 映射的状态值 X_n 。

6) 重复5) 直到把编码后的每块图像用混沌序列进行加密置乱。

1.2.2 解密算法

加密用的参数 μ, a, b, s, t, u, v 和单向函数要告诉解密方, 用 μ, s, t, u, v 的值可以算出 $G(i, j)$ 的值, 对编码后的图像进行解密, 得到编码前的系数矩阵。再计算 $s \times (b + a \times c) + t \times (a + b \times c)$ 的值作为单向函数的输入, 得到原置乱矩阵, 算出还原矩阵。计算 $a + b \times c$ 的结果作为单向函数的输入重新得到序列, 通过逆运算可以得到原图像。

1) 根据 μ, s, t, u, v 的值重新计算出 $G(i, j)$ 的值。

2) 根据算出的值就可以复原图像块的点的信息和相应点的位置。

3) 重复2), 将每块图像都恢复。

4) 计算 $s \times (b + a \times c) + t \times (a + b \times c)$ 并把它作为单向函数的输入重新生成一个解密序列, 由该序列生成一个置乱矩阵。

5) 通过置乱矩阵可以算出还原矩阵。

6) 根据还原矩阵得到融合后的图像。

7) 重新计算 $a + b \times c$ 的结果作为单向函数的输入重新得到序列。

8) 对加密公式求逆得: $F(i, j) = (|O(i, j) - 2E(i, j)|)$,

得到融合前的图像灰度值,这样就恢复了原始图像。

9) 对后续图像块执行 7)、8) 的操作直到恢复出所有图像块的灰度值,解密完成。

2 实验结果和分析

本方案是在 CPU-T2130 1.86 GHz, 2 GB 内存的电脑上实现的,用 Matlab 作为图像的处理工具,选取具有典型特性的四幅图像作为实验数据。具体的实验结果如图 4 所示。

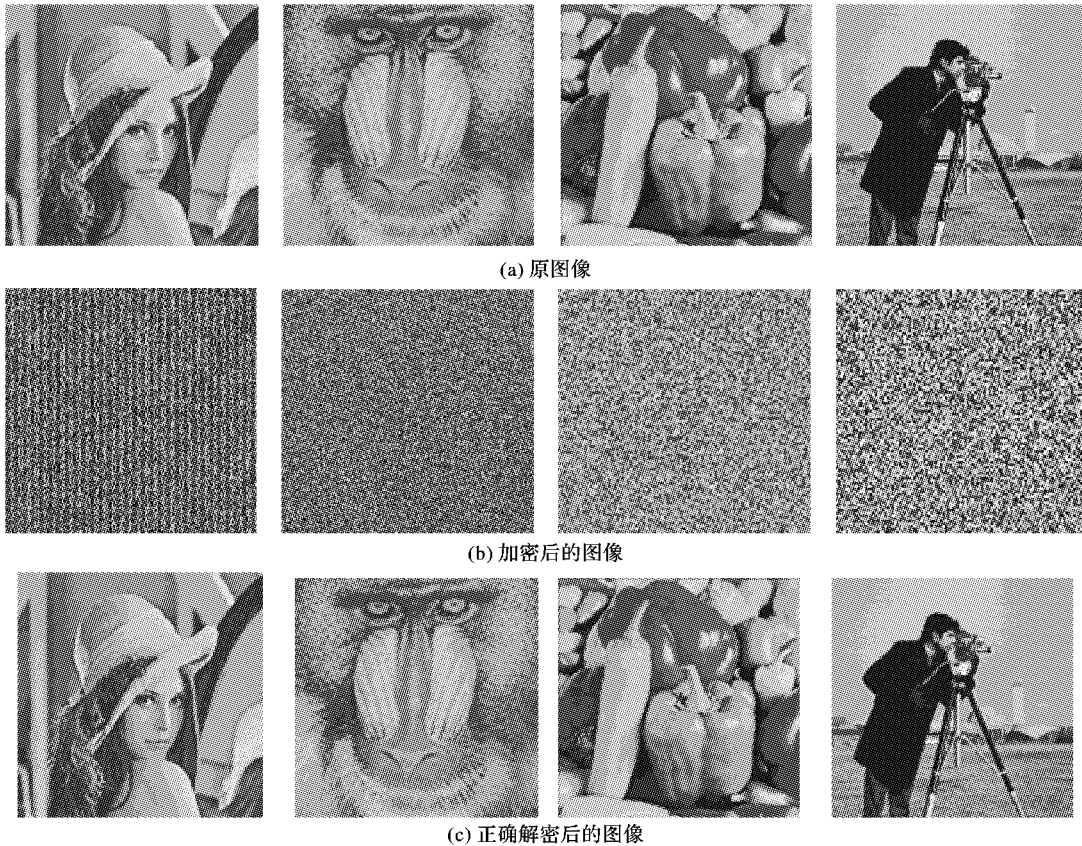


图 4 实验结果

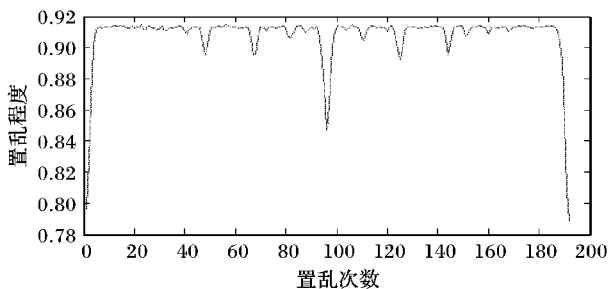


图 5 Arnold 变换曲线图

本文对目标图像进行了两次加密处理,第一次是在图像生成 DCT 系数的时候,第二次是在编码结束后。第一次加密很好地保护了 DC 系数,第二次加密保护了编码后的系数。先将图像的 DCT 系数进行融合,然后用置乱矩阵来进行第一次置乱,之后经过 EZW 编码后进行第二次置乱。经过这两次的置乱可以较好地保证图像安全,而且函数 $G(i, j)$ 是由基本初等函数经过初等变换得到的,也可以根据需要来选择函数,并对选取的函数作不同的变化。这里之所以要选取初等函数是因为它运算简单而且效率高,可以增加混沌序列的随机性,同时也使想要破解图像的信息变得困难。Logistic 映射对初值是极其敏感的,因此只有正确的密钥才能恢复原图像,得到

若采用 Arnold 变换^[5],加密的图像存在周期性的变换,在一定周期内总存在一幅复原图像,这样就会失去加密的效果,存在一定的风险性。

图 5 是 Arnold 变换的置乱程度与之乱次数的关系曲线图,当迭代到 192 次时图像正好恢复原状。

采用融合变换^[6]由于 DC 系数普遍大于 AC 系数的关系,通过对直方图的分析容易被识别,进而造成图像信息的泄露。而采用本论文提出的方法能较有效地防止出现这种情况。

正确信息。即使图像的部分信息被拦截,没有密钥或是错误的密钥所得到的图像也是经过变换的图像,无法获知图像原来的信息。综合运用置乱和像素值替代算法,可以大大提高图像的安全性,解决了采用单一置乱算法的周期性问题也克服了像素值替代算法容易被破解的缺点。用上述方法对原图像经过 50 次的反复变换操作,处理所得的图像与原图像相比肉眼几乎看不出失真。若需对原图操作连续处理超过 50 次,新的图像可能存在一定失真。为了得到比较好的效果,超过 50 次以上的处理用原图像再次处理的效果更好。

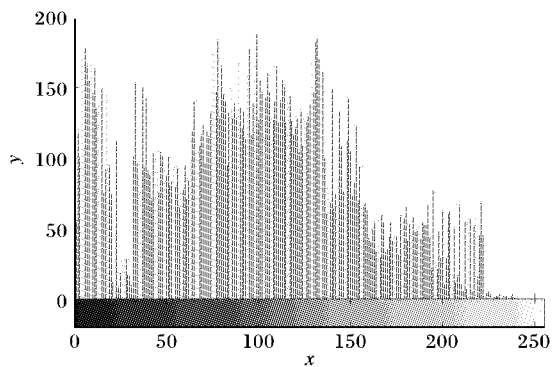


图 6 Lena 的直方图

3 算法分析

以一幅 512×512 的图像为例进行分析,该图像可以分成 4096 块 8×8 的图像。第一次融合加密的时候置乱的样本空间大小是 $4096 \times P64$,第二次加密的时候置乱的样本空间 $\left(\prod_{n=1}^{64} n!\right)^{4096}$,两次加密后的样本空间为 $4096 \times P64 \times \left(\prod_{n=1}^{64} n!\right)^{4096}$ 。

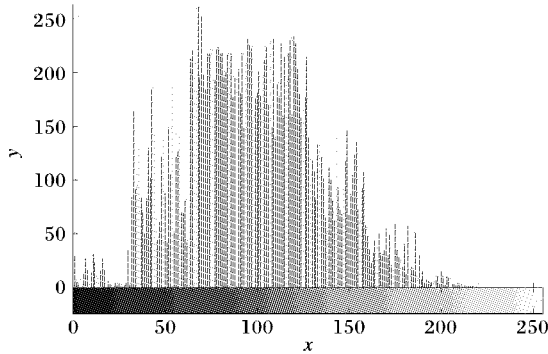


图7 融合后 Lena 图像的直方图

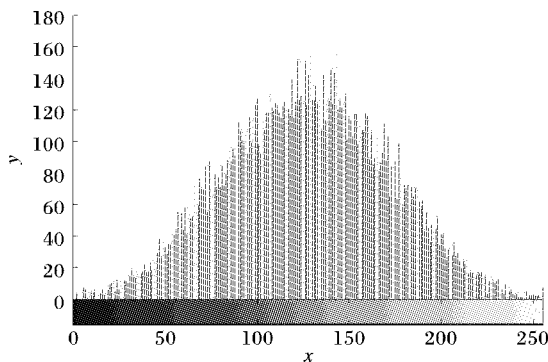


图8 采用本方法后得到的 Lena 图像直方图

4 结语

本文提出的基于伪随机点的混合图像融合加密算法能满足一般对图像加密的需求,同时也能运用到一些对图像安全性要求较高的场合,例如航空航天领域、GPS 的应用、大气、地质勘探等领域。相比于一些一次置乱算法和其他置乱算法,安全性得到了有效的保证,同时在计算机上的实现也相对容易,具有可操作性。但是该算法只考虑了图像的加密,对其他形式的媒体传输没有考虑,例如对于数据流的处理。

参考文献:

- [1] SHANG ZHEN-WEI, REN HONG-E, ZHANG JIAN. A block location scrambling algorithm of digital image based on Arnold transformation [C]// ICYCS 2008: The 9th International Conference for Young Computer Scientists. Washington, DC: IEEE Press, 2008: 2942–2947.
- [2] CHEN WEI-BIN, ZHANG XIN. Image encryption algorithm based on chaotic system [C]// IASP 2009: International Conference on Image Analysis and Signal Processing. Washington, DC: IEEE Press, 2009: 94–97.
- [3] 姚晔,徐正华,杨志云. 基于伪随机序列的宏块置乱视频加密方案[J]. 计算机工程,2005, 31(20): 162–164.
- [4] TANG LEI. Methods for encrypting and decryption MPEG video data efficiently [C]// Proceedings of the 4th ACM International Multimedia. New York: ACM Press, 1996: 219–229.
- [5] DING WEI, YAN WEI-QI, QI DONG-XU. Digital image scrambling technology based on Arnold transformation [J]. Journal of Computer-aided Design & Computer Graphics, 2006, 13(4): 338–341.
- [6] KOCAREV L. Chaos-based cryptography: A brief overview [J]. IEEE Circuits and Systems Magazine, 2001, 1(3): 6–21.
- [7] 齐东旭,邹建成,韩效宥. 一类新的置乱变换及其在图像信息隐蔽中的应用[J]. 中国科学: E 辑,2000, 30(5): 440–447.

(上接第524页)

销。3)在每次洪泛前,随机等待一段时间,将大量广播信息较均匀地分散,减轻网络负担并能够有效利用空闲带宽。4)考虑到战术互联网应用的部队特色,增加备份簇首角色,减少了簇首重新选举引起的网络开销并延长簇的生存时间,使得生成簇更加稳定。

仿真实验表明,TBKCM 方案产生的簇有适度且统一的簇尺寸,与其他方案相比,具有更长的簇首持续时间,簇结构更加稳定。

参考文献:

- [1] KONSTANTOPOULOS C, GAVALAS D, PANTZIOUC G. Clustering in mobile Ad Hoc networks through neighborhood stability-based mobility prediction[J]. ScienceDirect, 2008, 52(9): 1797–1824.
- [2] COKUSHU D, ERICIYES K. A hierarchical connected dominating set based clustering algorithm for mobile Ad Hoc networks [C]// 15th International Symposium on Modeling, Analysis, and Simulation of Computer and Telecommunication Systems. Washington, DC: IEEE Computer Society, 2007: 60–66.
- [3] CHEN Y P, LIESTMAN A L, LIU JIANG-CHUAN. Clustering algorithms for Ad Hoc wireless networks [EB/OL]. [2009–08–01]. <http://www.cs.sfu.ca/~jeliu/Papers/chapter-adhoc.pdf>.
- [4] AMIS A D, PRAKASH R. Load-balancing clusters in wireless Ad Hoc networks [C]// Proceedings of the 3rd IEEE Symposium on Application-Specific Systems and Software Engineering Technology. Washington, DC: IEEE Computer Society, 2000: 25.
- [5] SIVAVAKEESAR S, PAVLOU G. A prediction-based clustering algorithm to achieve quality of service in multi-hop Ad Hoc networks [C]// Proceedings of the London Communications Symposium (LCS). London: [s. n.], 2002: 17–20.
- [6] YU J Y, CHONG P H J. 3hBAC: A novel non-overlapping clustering algorithm for mobile Ad Hoc networks [C]// Proceedings of IEEE Pacrim'03. [S. l.]: IEEE, 2003, 1: 318–321.
- [7] AMIS A D, PRAKASH R, HUYNH D, et al. Max-Min d-cluster formation in wireless Ad Hoc networks [C]// Proceedings of IEEE INFOCOM 2000. Washington, DC: IEEE, 2000, 1: 32–41.
- [8] McDONALD A B, ZNATI T F. A mobility-based framework for adaptive clustering in wireless Ad Hoc networks [J]. IEEE Journal on Selected Areas in Communications, 1999, 17(8): 1466–1487.
- [9] CHEN G, NOCETTI F G, GONZALEZ J, et al. Connectivity based k-hop clustering in wireless networks [C]// Proceedings of 35th Annual Hawaii International Conference on System Sciences. Washington, DC: IEEE Computer Society, 2002, 7: 2450–2459.