

基于社交网络的群体信任算法

鲍捷¹ 程久军²

(同济大学计算机科学与工程系 上海 201804)¹

(同济大学嵌入式系统与服务计算教育部重点实验室 上海 201804)²

摘要 社交网络(Social Network Service, SNS)中群体之间的信任关系是广泛存在的,目前大部分信任模型的研究基本只涉及一对一之间的个体信任关系,并没有充分考虑一对多、多对一以及多对多之间的群体信任关系。在现有信任模型研究的基础上,给出一种群体信任算法。该算法根据社交网络中群体的特点,将交互的两个群体抽象为两个群体节点,将复杂的多种信任关系转化为一对一之间的信任关系,从而对群体间的信任关系进行描述和度量。仿真结果表明,该算法能合理地度量与计算每个节点在群体中的可信度以及群体间的直接信任度。

关键词 社交网络,信任算法,群体,可信度

中图分类号 TP393 **文献标识码** A

Group Trust Algorithm Based on Social Network

BAO Jie¹ CHENG Jiu-jun²

(Department of Computer Science & Engineering, Tongji University, Shanghai 201804, China)¹

(Key Laboratory of Embedded System and Service Computing of Ministry of Education, Tongji University, Shanghai 201804, China)²

Abstract In social network service(SNS), the relationships between groups are pervasive. While much work has been done on the one-to-one trust relationship, the research on one-to-many, many-to-one and many-to-many trust relationships is insufficient. Based on the current trust relationship models, a group trust algorithm was proposed. According to the characteristics of the groups in social network service, this algorithm abstractly considers two interacting groups as two group nodes and therefore converts one-to-many, many-to-one and many-to-many trust relationships into one-to-one trust relationship. After this, the trust relationships among groups are described and measured in the algorithm. The simulations results show that this algorithm can reasonably measure and calculate the credit of each node within a group and the direct trust degree between groups.

Keywords Social network service, Trust algorithm, Group, Trust degree

1 引言

20世纪90年代初, Beth^[1]等人首次尝试将信任关系的研究引入到计算机网络环境中工作,之后国内外许多学者对各种环境下的信任问题也展开了研究工作,建立了不同的信任模型^[2-6]。这些模型都只针对一对一之间的信任关系进行建模,没有提供群体之间信任关系的描述和度量。文献^[7]提出了基于主观逻辑的群体信任模型,它通过顺序、选择、循环以及并行这4种基本的约束模式及其彼此之间的嵌套来表达群体中个体之间的约束,但该模型只适用于群体中个体之间的约束关系可以确定的情况,而网络中的群体中个体之间的约束关系往往很难确定。

信任是人类大部分社会活动的基石,也是人际关系的基础,而社交网络是指个人之间的关系网络^[8],它是建立在人际关系基础上的。与其它一般网络不同,群体是社交网络中一

个重要的组成元素^[9],它的作用在于能够找到更多有共同兴趣爱好的朋友。另外,由于形成群体原因的多样性,社交网络中的每个人还可以属于多个群体。根据文献^[10]的统计结果表明,每个大学生手机社交网络用户平均拥有3~4个群体。群体之间的信任关系在社交网络中也是广泛存在的,如两个单位搞联谊活动,涉及到的是两个单位中的员工,体现为一个单位中群体与另外一个单位中群体之间的信任关系,因此,在社交网络中对群体信任的研究具有一定的意义。目前社交网络中关于信任的研究尚处于起步阶段,也已取得了一些研究成果。Bhuiyan^[11]等人在基于地理位置信息的社交网络的基础上,结合信任及社会声誉来决定哪个节点更值得信任;文献^[12]分析了社交网络中多跳用户之间的跳数与信任度变化的关系,提出了TidalTrust算法;文献^[13]则结合声誉与主观逻辑,在社交网络中提出了一种信任分析方法,该方法通过声誉与朋友间的信任关系来获得信任值。上述研究成果都没有对

到稿日期:2011-04-10 返修日期:2011-07-12 本文受863项目(2009AA011906),国家自然科学基金项目(90818023),上海市项目(08GG08),教育部新教师基金(20090072120048)资助。

鲍捷(1987-),男,硕士生,主要研究方向为移动社交网络、信任机制等, E-mail: jiebao19870113@126.com; 程久军 男,副教授,主要研究方向为移动计算、物联网等。

社交网络中群体之间的信任关系进行描述和度量,但为社交网络中群体信任关系的研究提供了必要的理论基础。

本文根据社交网络中群体的特点,在现有一对一之间信任关系研究的基础上,针对一对多、多对一以及多对多之间的信任关系,给出了一种群体信任算法。该算法将交互的两个群体抽象为两个群体节点,通过计算群体节点与群体外节点的直接信任关系将复杂的一对多、多对一以及多对多之间的信任关系转化为一对一之间的信任关系,从而合理地描述与度量群体之间的信任关系。

2 相关概念

目前关于信任没有统一的定义,本文参考文献[14,15],并结合文中社交网络这一特定环境,给出信任的描述性定义以及与信任相关的一些概念。

定义 1(信任, trust) 在社交网络中,信任是一个节点在已有知识的基础上对另外一个节点行为的可靠性观点。

定义 2(信任度, trust degree) 信任度是信任的量化表示,在文中用连续区间 $[0,1]$ 表示。信任度可分为直接信任度、间接信任度以及总体信任度。直接信任度是指一个节点根据以往和另一节点发生的直接交互历史得出的对此节点的可信程度;间接信任度是指一个节点通过到达另一节点的多条信任路径综合计算得到的对此节点的信任程度;总体信任度是指一个节点根据对另一节点的直接信任度及间接信任度而得出的对其的总体可信性度量。

如图 1 中,节点 A 对节点 B 的直接信任度为 e_{AB} ,节点 B 对节点 D 的直接信任度为 e_{BD} ,节点 A 与节点 D 之间存在两条信任路径,分别为 P_{ABD} 和 P_{ACD} ,由这两条信任路径综合计算可得到节点 A 对节点 D 的间接信任度为 t_{AD} 。

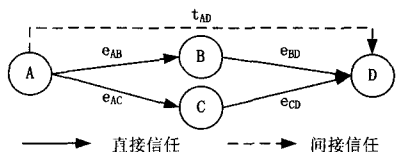


图 1 直接信任度与间接信任度

定义 3(群体, group) 在社交网络中,群体是指一些节点因为某些共同的目的组成的一个团体,该团体可以由多个节点组成,特殊地,也可以仅由一个节点组成。

根据以上定义,社交网络中的每个节点都可以看作是一个特殊的群体,文中多种信任关系(一对一、一对多、多对一、多对多)都可以看作是两个群体之间的信任关系。另外,在社交网络中,一个节点可以同时属于多个群体,并且一个节点可以随时加入或离开一个群体。

3 社交网络中群体信任算法

传统的信任算法用总体信任度来表示网络中一个节点对另外一个节点的可信程度。文献[2-6]中,总体信任度的计算方法可以抽象为 $WD + (1-W)I$,其中 D 是直接信任度, I 是间接信任度, W 与 $1-W$ 分别为直接信任度与间接信任度的权重。在社交网络中要计算的是两个群体之间的总体信任度,计算时可以把每个群体都抽象为一个群体节点,确定群体节点与群体外节点(包括另一个群体节点)间的直接信任关系后就可根据传统的方法计算出两个群体节点之间的总体信任

度。问题的关键在于如何得到群体节点与群体外节点间的直接信任关系。

3.1 节点在群体中的可信度

不同节点在群体中的可信度是不同的,有些节点可能被群体中大部分节点所信任,而有些节点在群体中可能几乎没有节点信任它。一个节点越被群体中其它节点所信任,且信任该节点的节点本身在群体中的可信度越高,那么该节点在群体中的可信度应当越高。因此,一个节点在群体中的可信度为群体中其它节点对该节点直接信任度值的加权平均,权重为对应节点在群体中的可信度,即节点在群体中的可信度计算公式为

$$s(i, R) = \frac{1}{\sum_{j \in V(R)} s(j, R)} \sum_{j \in V(R)} (s(j, R) \times e_{ji}) \quad (1)$$

式中, $s(i, R)$ 表示节点 i 在群体 R 中的可信度; $V(R)$ 表示群体 R 中节点的集合; e_{ji} 表示节点 j 对节点 i 的直接信任度,若节点 j 与节点 i 没有过直接交互,则 $e_{ji} = 0$ 。

若群体 R 中有 n 个节点,则可列出 n 个类似于式(1)的方程,其中 $s(i, R)$ 、 $s(j, R)$ 均为未知数。求解这个问题即是要求一个 n 元二次方程组,可采用迭代算法来进行求解。

算法 1 迭代求解各节点在该群体中的可信度。

Step1 在群体 R 中,对于每个节点 i ,初始化 $s(i, R)$ 为一个 $(0,1]$ 之间的值。

Step2 对于群体 R 中的每个节点 i ,根据以下公式计算 $\overline{s(i, R)}$ 。

$$\overline{s(i, R)} = \frac{1}{\sum_{j \in V(R)} s(j, R)} \sum_{j \in V(R)} (s(j, R) \times e_{ji}) \quad (2)$$

Step3 判断 $\sum_{i \in V(R)} |\overline{s(i, R)} - s(i, R)|$ 的值是否小于 Δ , Δ 为求解的精度误差,即判断连续两次求出的结果是否相近,若相近(小于 Δ),则转 Step4;否则对群体 R 中的每个节点 i ,令 $s(i, R) = \overline{s(i, R)}$,转 Step2。

Step4 算法执行结束,所求的结果为

$$S = \{s(i, R) | i \in V(R)\}$$

算法 1 首先对群体 R 内的所有节点在群体中的可信度赋一个 $(0,1]$ 之间的初值,然后根据式(2)不断进行迭代,最后的收敛结果即为群体内每个节点在群体中的可信度。在图 2 的群体 R_1 中,若令 $s(A, R_1)$ 、 $s(B, R_1)$ 以及 $s(C, R_1)$ 的初始值都为 1.0,则进行一次迭代后 $s(A, R_1) = (0.9 + 0.3)/2 = 0.6$,同样可算出 $s(B, R_1) = 0.6$, $s(C, R_1) = 0.2$ 。按照相同的方法不断进行迭代,若设定 $\Delta = 0.001$,则最后迭代算法的收敛结果为 $s(A, R_1) = 0.737$, $s(B, R_1) = 0.478$, $s(C, R_1) = 0.179$ 。

在社交网络中,一个节点可以加入或离开一个群体,这时群体内所剩节点在群体中的可信度也会随之而发生变化,算法 2 和算法 3 可以方便地更新这些变化。

算法 2 节点加入一个已存在的群体时各节点在群体中可信度的更新算法。

Step1 将新加入的节点在该群体中的可信度赋一个 $(0,1]$ 之间的初值,其余节点在群体中的可信度仍为那些节点加入前的值。

Step2 从算法 1 的 Step2 起开始执行算法 1。

Step3 算法执行结束,所求的结果为

$$S = \{s(i, R) | i \in V(R)\}$$

算法 3 节点离开群体时剩余节点在群体中可信度的更新算法。

Step1 令群体中剩余节点在群体中的可信度为节点离开前的值。

Step2 从算法 1 的 Step2 起开始执行算法 1。

Step3 算法执行结束,所求的结果为

$$S = \{s(i, R) | i \in V(R)\}$$

3.2 群体与群体外节点间直接信任度

在计算群体 R 对群体外节点 k 的直接信任度时,群体 R 中各节点对节点 k 的直接信任度将起到关键的作用,因此首先须计算出群体 R 对节点 k 有过直接交互的节点对节点 k 直接信任度值的加权平均,其权重为这些节点在群体 R 中的可信度。另外在群体 R 中与节点 k 有过直接交互的节点的数量以及这些节点在群体 R 中的可信度高也会对该直接信任度值产生影响。综上,群体节点对群体外节点的直接信任度计算公式为

$$e_{Rk} = I(R, k) \times \frac{1}{\sum_{i \in D(R, k)} s(i, R)} \sum_{i \in D(R, k)} (s(i, R) \times e_{ik}) \quad (3)$$

式中, $D(R, k)$ 为群体 R 中与节点 k 有过直接交互的节点的集合, $\frac{1}{\sum_{i \in D(R, k)} s(i, R)} \sum_{i \in D(R, k)} (s(i, R) \times e_{ik})$ 为 $D(R, k)$ 中节点对节点 k 直接信任度的加权平均值, $I(R, k)$ 为群体 R 对节点 k 的信任因子,其计算公式为 $I(R, k) = 1 - \prod_{i \in D(R, k)} (1 - s(i, R))$ 。当群体 R 与节点 k 有过直接交互的节点数量越多以及这些节点在群体 R 中的可信度越高时,群体 R 对节点 k 的信任因子就越大。图 2 中

$$I(R_1, E) = 1 - (1 - 0.737)(1 - 0.179) = 0.784$$

$$e_{R_1 E} = 0.784 \times \frac{0.737 \times 0.3 + 0.179 \times 0.9}{0.737 + 0.179} = 0.327$$

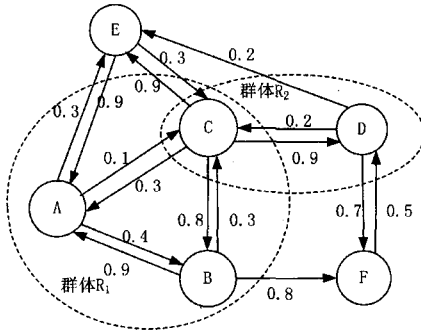


图2 信任关系网络示例图

由于信任关系的不对称性,还须计算群体外节点对群体节点的直接信任度,于是可得到其计算公式为

$$e_{kR} = I(k, R) \times \frac{1}{\sum_{i \in D(k, R)} s(i, R)} \sum_{i \in D(k, R)} (s(i, R) \times e_{ki}) \quad (4)$$

式中, $I(k, R) = 1 - \prod_{i \in D(k, R)} (1 - s(i, R))$ 为节点 k 对群体 R 的信任因子, $D(k, R)$ 为在群体 R 中节点 k 与其有过直接交互的节点的集合。

3.3 两群体间直接信任度

在计算群体 R_1 对群体 R_2 的直接信任度时,若 R_1 中的一个节点与 R_2 中的一个节点有过直接交互,则称这对节点为群体 R_1 对群体 R_2 中有过直接交互的一对节点。若群体 R_1 对群体 R_2 中有过直接交互的节点对数量越多,且这些节点在各自群体中可信度越高,则群体 R_1 对群体 R_2 的直接信任度也越高。另外,由于社交网络中每个节点可以属于多个群体,因此在群体 R_1 、 R_2 中可能会出现一些相同的节点,这种情况称之为两个群体相交,如图 2 中群体 R_1 与群体 R_2 相交于节点 C 。两个群体相交的节点数量越多,这两个群体的关系就越紧密,信任关系也越好。

为了讨论方便,首先考虑两个群体不相交的情况。对式

(3)进行扩展,可得到两个不相交群体之间的直接信任度计算公式为

$$e_{R_1 R_2} = I(R_1, R_2) \times \frac{\sum_{(i, j) \in D(R_1, R_2)} (s(i, R_1) \times s(j, R_2) \times e_{ij})}{\sum_{(i, j) \in D(R_1, R_2)} (s(i, R_1) \times s(j, R_2))} \quad (5)$$

式中, $D(R_1, R_2)$ 为群体 R_1 与群体 R_2 有过直接交互的节点对的集合, $\frac{\sum_{(i, j) \in D(R_1, R_2)} (s(i, R_1) \times s(j, R_2) \times e_{ij})}{\sum_{(i, j) \in D(R_1, R_2)} (s(i, R_1) \times s(j, R_2))}$ 为 $D(R_1, R_2)$ 中直接信任度的加权平均值, $I(R_1, R_2)$ 为群体 R_1 对群体 R_2 的信任因子,公式为 $I(R_1, R_2) = 1 - \prod_{(i, j) \in D(R_1, R_2)} (1 - s(i, R_1) \times s(j, R_2))$ 。群体 R_1 与群体 R_2 有过直接交互的节点对数量越多,且这些节点对在各自群体中的可信度越高时,群体 R_1 对群体 R_2 的信任因子就越大。

两个群体相交,可对网络图稍做修改:将两个群体中相交的节点复制一份,分别放入两个群体中,将两个群体中原本相同的节点之间的直接信任度赋为最高值 1.0 (即自己完全信任自己),这样两个群体不再相交,然后再根据式(5)计算两个群体间的直接信任度值。为了避免复制节点所造成的节点泛滥,在计算完两个群体节点间的直接信任度后,将网络图复原即可。

图 2 中,在计算群体 R_1 对群体 R_2 的直接信任度时,首先将两个群体相交的节点 C 复制一份,称为节点 C' ,可将相关网络图修改成如图 3 所示的网络关系,图中 $e_{C'C} = e_{CC} = 1.0$ 。根据式(5)来计算群体 R_1 对群体 R_2 的直接信任度后,将网络图恢复至图 2。

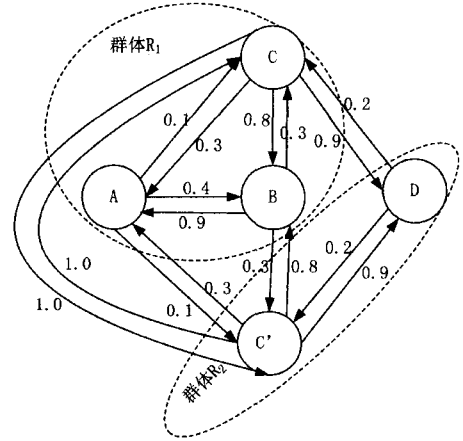


图3 两群体相交时对网络图的修改

3.4 两群体间总体信任度

社交网络中一个群体对另外一个群体的可信程度用总体信任度来表示。在计算两群体间的总体信任度时,首先将这两个群体抽象为两个群体节点,然后计算这两个群体节点间的总体信任度。由定义 2 可知,总体信任度的值是由直接信任度与间接信任度综合计算得到的,而直接信任度则表现为两群体节点间的直接信任度,间接信任度则是由一个群体节点通过其它节点到达另一个群体节点的多条信任路径综合计算得到的。因此在将一个群体抽象为一个群体节点后,需要计算出该群体节点与群体外节点(包括另一个群体节点)的直接信任关系,可根据式(3)一式(5)进行计算。

在图 2 中,在计算群体 R_1 对群体 R_2 的总体信任度时,将节点 A 、 B 、 C 看成一个群体节点 R_1 ,将节点 C 、 D 看成一个群

体节点 R_2 , 然后计算 R_1 、 R_2 与 E 、 F 之间以及 R_1 与 R_2 之间的直接信任度, 其简化后的信任关系如图 4 所示。

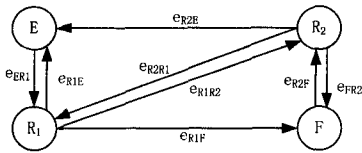


图 4 简化后的信任关系网络图

群体 R_1 对群体 R_2 的直接信任度为 $e_{R_1R_2}$, 从 R_1 到 R_2 共有两条信任路径, 分别为 R_1ER_2 、 R_1FR_2 , 由这两条信任路径综合计算可得到群体 R_1 对群体 R_2 的间接信任度, 最后计算得到群体 R_1 对群体 R_2 的总体信任度。

4 仿真结果与分析

本节对给出的群体信任算法进行仿真。仿真的硬件环境为 Intel(R) Core(TM)2 Duo CPU E8400, 内存 2GB, 系统类型为 32 位操作系统。仿真规模包括 10000 个节点, 节点的分布符合 Power-Law 分布^[16], 有过直接交互的节点之间的直接信任度值均在 $[0, 1]$ 之间。

在仿真的社交网络系统中有两种类型的节点: 一类是友好节点, 这些节点在系统中具有良好的行为, 因此有过直接交互的这些节点之间的直接信任度值都比较高; 另一类是恶意节点, 这些节点在系统中有不良行为, 进行恶意评分。仿真中将有过直接交互的节点之间的直接信任度赋值为 $[0, 1]$ 之间。一个健康的社交网络中大部分有过直接交互的节点之间应该是互相信任的, 因此将 80% 的友好节点间的直接信任度值设在 $[0.5, 1]$ 之间, 其余 20% 设在 $[0, 0.5]$ 之间。

4.1 节点在群体中可信度算法的合理性

在仿真过程中, 设计一个由 100 个节点组成的群体, 在这 100 个节点中有若干个恶意节点。假设恶意节点对友好节点的直接信任度值在 $[0, 0.2]$ 之间, 恶意节点对恶意节点的直接信任度值在 $[0.8, 1]$ 之间, 友好节点对恶意节点之间的直接信任度值在 $[0, 0.2]$ 之间。计算并统计这 100 个节点在群体中的可信度, 仿真结果如表 1 所列。

表 1 节点在群体中可信度算法的合理性

节点在群体中的可信度	有 10 个恶意节点		有 20 个恶意节点		有 30 个恶意节点		有 40 个恶意节点	
	非恶意	恶意	非恶意	恶意	非恶意	恶意	非恶意	恶意
$[0, 0.2)$	0	10	0	20	0	25	0	0
$[0.2, 0.4)$	0	0	0	0	0	5	5	28
$[0.4, 0.6)$	4	0	13	0	49	0	55	12
$[0.6, 0.8)$	86	0	67	0	21	0	0	0
$[0.8, 1]$	0	0	0	0	0	0	0	0

由表 1 可以看出, 当群体中恶意节点较少时, 绝大部分友好节点在群体中的可信度在 $[0.6, 0.8)$ 区间内, 而恶意节点在群体中的可信度几乎在 $[0, 0.2)$ 区间内。即使群体中存在 40% 的恶意节点, 大部分友好节点在群体中的可信度也比恶意节点在群体中的可信度高。由此可见, 群体中的恶意节点很难在群体中有比较高的信任度。

4.2 群体间直接信任度算法的合理性

仿真分别在两个 30 个节点的群体之间以及在两个 100 个节点的群体之间进行, 初始时设定两个群体间的节点之间没有任何直接交互(即两个群体之间没有连线)。现对每个群

体内部有过直接交互的节点对数量进行固定, 通过不断增加两群体之间有过直接交互的节点对数量来模拟社交网络中两个群体之间节点的不断交互, 以期考察对两群体间直接信任度的影响。每次仿真分别在 4 种情况下进行, 即每个群体内部有 n 对、 $2n$ 对、 $4n$ 对、 $8n$ 对(其中 n 为群体中节点的数量, 为 30 或 100)节点之间有过直接交互, 仿真结果如图 5 所示。

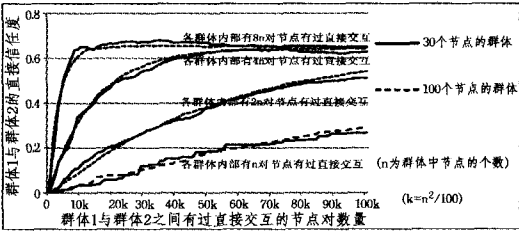


图 5 群体间直接信任度算法的合理性

由图 5 可以看出, 两群体内部有直接交互的节点对数越多, 两群体间的直接信任度就越高, 这说明在社交网络中一个群体内部本身互相信任越高, 这个群体与其它群体的信任关系也会越好。另外, 两群体间的直接信任度随两群体间节点的不断交互而增长。在群体内部直接交互量较少的情况下(如图中最下方的两条曲线), 两群体间的直接信任度值增长速度较缓慢, 即使群体间两两节点间都有过直接交互, 两群体间的直接信任度也只有 0.3 左右。这是因为群体内部的节点之间互相都不信任对方, 那么这个群体对外部的节点的信任度值也不会高。反之, 在群体内部直接交互量较大的情况下(如图中最上方的两条曲线), 两群体间的直接信任度值初期会随着两群体间节点的不断交互而迅速增长, 随后处于平稳趋势。在群体间的直接交互量达到 10% 的时候, 两群体间的直接信任度就已经超过了 0.6。这是因为群体中的每一个节点都被群体内大部分节点所信任, 这些节点对群体外其它节点的信任也会被群体内其它节点所接受, 显然, 这在社交网络中是一种比较合理的情况。

结束语 群体是社交网络中一个重要的组成元素, 在社交网络中对群体信任进行研究具有一定的意义。社交网络中一个节点可以随时加入或离开一个群体, 并且一个节点可以属于多个群体。本文针对社交网络中群体的这些特点, 给出一种群体信任算法, 该算法将网络中的群体抽象为一个群体节点, 将一对多、多对一以及多对多之间的信任关系全部转换为一对一之间的信任关系来求解。在转换过程中, 考虑到各节点在群体中可信度的不同, 首先求出各节点在群体中的可信度, 然后将求出的各节点在群体中的可信度作为权重计算出群体节点与群体外节点(包括另一个群体节点)之间的直接信任度, 最后再用传统的信任算法求出两群体之间的间接信任度与总体信任度。仿真结果表明, 该算法充分考虑到两群体内部有过直接交互的节点对数量与群体间有过直接交互的节点对数量对群体间直接信任度的影响, 并能合理地度量与计算每个节点在群体中的可信度以及群体间的直接信任度。

参考文献

[1] Beth T, Borchering M, Klein B. Valuation of trust in open network[C] // Proceedings of the European Symposium on Research in Security. Brighton: Springer-Verlag, 1994: 3-18

(下转第 51 页)

结束语 充分利用图像邻近像素相关的特性,提出了一种基于图像块参照像素的无损信息隐藏算法,即在像素差直方图移位后能产生大量的冗余空间以嵌入信息。同时利用固定的参数(如轮次、块大小和阈值 δ)以及多层嵌入的策略在保持较低图像失真的同时实现了大容量的信息嵌入。另外,与其它类似算法不同的是,本方法提取机密信息和恢复载体图像不需要除机密信息长度之外的任何信息。实验表明,与传统算法相比,所提算法更具优势。

参 考 文 献

- [1] Honsinger C W, Jones P, Rabbani M, et al. Lossless Recovery of an Original Image Containing Embedded Data [P]. U. S. Patent 6278791. Aug. 2001
- [2] Fridrich J, Goljan M, Du R. Lossless data embedding-New paradigm in digital watermarking [J]. EURASIP Journal on Applied Signal Processing, 2002(2):185-196
- [3] Celik M U, Sharma G, Tekalp A M, et al. Lossless Generalized-LSB Data Embedding [J]. IEEE Transactions on Image Processing, 2005, 14(2):253-266
- [4] Vleeschouwer C D, Delaigle J F, Macq B. Circular Interpretation of Bijective Transformations in Lossless Watermarking for Media Asset Management [J]. IEEE Transactions on Multimedia, 2003, 5(3):97-105
- [5] Tian J. Reversible Data Embedding Using a Difference Expansion [J]. IEEE Transactions on Circuits and Systems for Video Technology, 2003, 13(8):890-896
- [6] Alattar A M. Reversible Watermark Using the Difference Expansion of a Generalized Integer Transform [J]. IEEE Transactions on Image Processing, 2004, 13(8):1147-1156
- [7] Thodi Diljith M, Rodriguez Jeffrey J. Prediction—error based reversible watermarking [C]//Proceedings of 2004 IEEE International Conference on Image Processing. ICIP 2004:1549-1552
- [8] Thodi Diljith M, Rodriguez Jeffrey J. Expansion embedding techniques for reversible watermarking [J]. IEEE Transactions on Image Processing, 2007, 16(3):721-730
- [9] Kamstra L, HHeijmans J A M. Reversible data embedding into images using wavelet techniques and sorting [J]. IEEE Transactions on Image Processing, 2005, 14(12):2082-2090
- [10] Xuan G, Zhu J, Chen J, et al. Distortionless data hiding based on integer wavelet transform [J]. IEE Electron Letters, 2002, 38:1646-1648
- [11] Chang Chin-chen, Chou Yung-chen, Lin Chih-yang. Reversible data hiding in the VQ-compressed domain [J]. IEICE Transactions on Information and Systems, 2007, E90-D(9):1422-1429
- [12] Ni Z, Shi Y Q, Ansari N, et al. Reversible Data Hiding [J]. IEEE Transactions on Circuits and Systems for Video Technology, 2006, 16(3):354-362
- [13] Tseng H W, Hsieh C P. Reversible data hiding based on image histogram modification [J]. Imaging Science Journal, 2008, 56(5):271-278
- [14] Lin Chia-chen, Tai Wei-liang, Chang Chim-chen. Multilevel reversible data hiding based on histogram modification of difference images [J]. Pattern Recognition, 2008, 41(12):3582-3591
- [15] Tai Wei-liang, Yeh Chia-ming, Chang Chin-chen. Reversible Data Hiding Based on Histogram Modification of Pixel Differences [J]. IEEE Transactions on Circuits and Systems for Video Technology, 2009, 19(6):904-908
- [16] (上接第41页)
- [2] Almenarez F, Marin A, Diaz D, et al. Developing a model for trust management in pervasive devices[C]//Proceedings of the 4th annual IEEE International Conference on Pervasive Computing and Communication Workshop. Washington: IEEE Computer Society Press, 2006:267-272
- [3] Theodorakopoulos G, Baras J S. Trust evaluation in ad-hoc networks[C]//Proceedings of the 3rd ACM Workshop on Wireless Security. Philadelphia, Pennsylvania, USA, 2004:1-10
- [4] Liang Zheng-qiang, Shi Wei-song. PET: A Personalized trust model with reputation and risk evaluation for P2P resource sharing[C]//Proceedings of the 38th Hawaii International Conference on System Sciences. Washington: IEEE Computer Society, 2005:287-295
- [5] Liu Xiong, Liu Ling. PeerTrust: Supporting reputation-based trust for Peer-to-Peer electronic communities[J]. IEEE Transactions on Knowledge Data Engineering, 2004, 16(7):843-857
- [6] 李小勇, 桂小林. 动态信任预测的认知模型[J]. 软件学报, 2010, 21(1):163-176
- [7] 王勇, 代桂平, 姜正涛, 等. 基于主观逻辑的群体信任模型[J]. 通信学报, 2009, 30(11):8-14
- [8] 包昌火, 谢新洲, 申宁. 人际网络分析[J]. 情报学报, 2003, 22(3):366-374
- [9] 刘耀庭. 社交网络结构研究[D]. 杭州: 浙江大学计算机学院, 2008
- [10] 乔献新, 朱吉虹, 沈勇. 手机移动社交网络的用户研究[J]. 电信科学, 2010, 26(10):109-113
- [11] Bhuiyan T, Xu Y, Jørgensen A. Integrating trust with public reputation in location-based social networks for recommendation making[C]//Proceedings of IEEE/WIC/ACM International Conference on Web Intelligence and Intelligent Agent Technology. Sydney, NSW, 2008:107-110
- [12] Katz Y, Golbeck J. Social network-based trust in prioritized default logic[C]//Proceedings of the 21st National Conference on Artificial Intelligence, 2006:1345-1350
- [13] 雷环, 彭舰. SNS中结合声誉与主观逻辑的信任网络分析[J]. 计算机应用研究, 2010, 27(6):2321-2323
- [14] 李勇军, 代亚非. 对等网络信任机制研究[J]. 计算机学报, 2010, 33(3):390-405
- [15] 李小勇, 桂小林. 大规模分布式环境下动态信任模型研究[J]. 软件学报, 2007, 18(6):1510-1521
- [16] Toivonen R, Onnela J P, Saramaki J, et al. A model for social networks[J]. Statistical & Theoretical Physics, 2006, 371(2):851-860