基于0-1背包算法的社交网络行为隐写术

高 鹏,柴鹏翔,郎 俊
(东北大学计算机科学与工程学院,辽宁沈阳 110169)

摘 要: 随着社交网络的快速发展,利用人类行为实现信息隐藏成为当前隐写研究热点. 本文提出一种基于0-1背包算法的社交网络下一对多行为隐写术. 该算法将信息的传递方式由一对一变为一对多,通过引入0-1背包算法,提高了传输效率和传输方式的灵活性;加入CMI(Coded Mark Inversion)编码预处理,解决了传输大量连续相同比特秘密信息时有较高误码率的问题;发送者和每个接收者的有效共同好友数量得到降低,从而减少数据冗余. 实验表明,该方案提高了社交网络下行为隐写的实用价值,有较高的安全性.

关键词: 信息隐藏; 隐写术; 行为; 行为信息隐藏; 社交网络; 0-1背包算法
中图分类号: TN918.91 **文献标识码:** A **文章编号:** 0372-2112(2022)03-0753-06
电子学报URL:http://www.ejournal.org.cn **DOI:**10.12263/DZXB.20210742

Behavior Steganography in Social Networks Based on 0-1 Knapsack Algorithm

GAO Peng, CHAI Peng-xiang, LANG Jun
(*College of Computer Science and Engineering, Northeastern University, Shenyang, Liaoning* 110169, *China*)

Abstract: Recently, using human behavior to hide secrecy has become the focus of steganography research. In this paper, we propose an one-to-many behavior steganography in social networks based on the 0-1 knapsack algorithm, which changes the information transmission mode from one-to-one to one-to-many, and introduces the 0-1 knapsack algorithm to improve the transmission efficiency and the flexibility of the transmission mode; the preprocessing of CMI (Coded Mark Inversion) coding is added to solve the high bit error rate problem when transmit a large number of continuous and the same secret information. The number of common friends of the sender and each receiver is reduced, therefore reducing data redundancy. The experimental analysis shows that this scheme improves the practical value of behavior steganography in social networks, and has high security.

Key words: information hiding;steganography;behavior;behavior steganography;social network;0-1 knapsack algorithm

1 引言

隐写术[1~4]也称数据隐藏,是指利用信息嵌入算法,将秘密信息隐藏到非机密载体中的技术. 随着隐写分析技术能力的不断提高,传统隐写术的安全性不容乐观,利用社交网络行为进行信息隐藏能更好地对抗隐写分析. 社交网络的最大的传播特征是及时性与交互性,在社交网络下行为隐写的实例中,曾以Twitter信息的长短来携带秘密信息[5];也可以构建信息隐藏通用框架,将信息嵌入到由选定的社交网络和多个在线账户进行的一系列活动中[6].

文献[7]提出一对一点赞行为隐写,如图1所示. 该方法将点赞矩阵$\boldsymbol{H}$与秘密信息$\boldsymbol{M}$进行二进制内积,并对$b\cdot\boldsymbol{D}$通过点赞概率p进行反算数编码得到发送矩

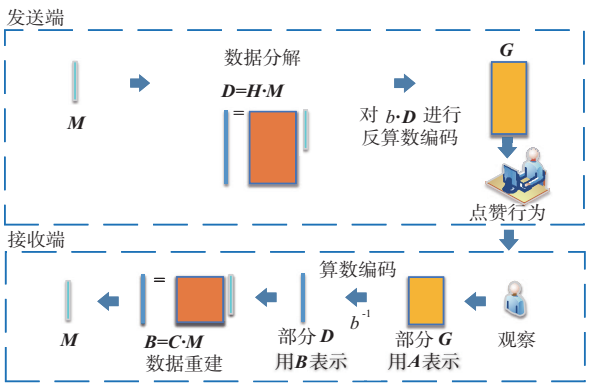


图1 点赞行为隐写

收稿日期:2021-06-10;修回日期:2021-08-11;责任编辑:覃怀银
基金项目:国家自然科学基金(No.61202446);教育部中央高校基本科研业务经费(No.N150404004)

阵 $\boldsymbol{G}$,随后发送者根据 $\boldsymbol{G}$ 进行点赞行为来传送信息. 接收者通过 p 对矩阵 $\boldsymbol{A}$ 进行算数编码,并对结果乘系数 b^{-1} 得到 $\boldsymbol{B}$,最后根据数据重建获得 $\boldsymbol{M}$. 但在实际应用中,该方法无法满足一对多传输模式. 对于传输秘密信息中含有大量连续相同比特的情况,会产生较高的误码率,并且要求发送者和接收者有较多的共同好友,在实际应用中并不容易实现.

针对文献[7]存在的上述问题,本文提出基于0-1背包算法[8]的社交网络下一对多行为隐写. 首先通过加入CMI编码预处理,降低了误码率. 其次提出一对多行为隐写算法,通过引入0-1背包人员分配协议,降低发送者和接收者有较多的共同好友这一限制条件,并实现了发送者对接收者操作可控.

2 基于0-1背包算法的社交网络下一对多行为隐写

本文提出的基于0-1背包算法的一对多行为隐写整体框架图如图2所示.

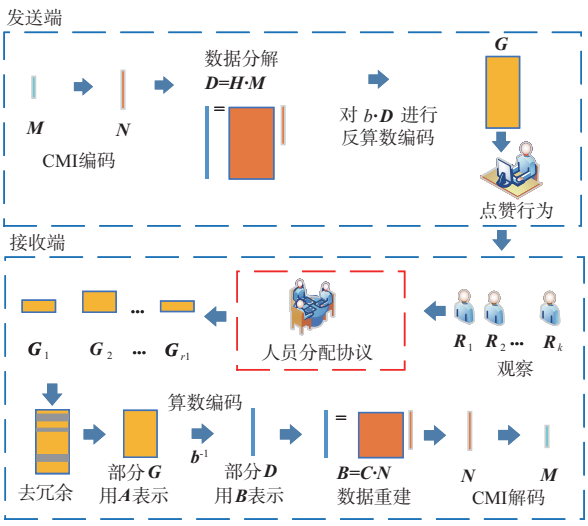


图2 基于0-1背包算法的一对多行为隐写

2.1 发送端

发送端具体流程如下:

(1) $\boldsymbol{M}=[m_1,m_2,\cdots,m_l]^{\mathrm{T}}$ 表示二进制秘密信息,n 表示发送者 S 拥有的全部好友数. $\boldsymbol{H}$ 表示点赞矩阵,用来记录 S 给好友发表过的动态的点赞情况.

$$\boldsymbol{H}=\begin{bmatrix} v(1,1) & v(1,2) & \cdots & v(1,l) \\ v(2,1) & v(2,2) & \cdots & v(2,l) \\ \vdots & \vdots & & \vdots \\ v(n,1) & v(n,2) & \cdots & v(n,l) \end{bmatrix} \tag{1}$$

$\boldsymbol{H}$ 的第 i 行对应 S 的第 i 个好友,$\boldsymbol{H}$ 的第 j 列表示 S 对不同好友的第 j 个动态的点赞状态,若点了赞,则 $\boldsymbol{H}$ 中相应元素记录为1;若未点赞,则 $\boldsymbol{H}$ 中相应元素记录为0.

(2) 发送者 S 给 r_1 个接收者 $R_i(i=1,2,\cdots,r_1)$ 传送秘密信息 $\boldsymbol{M}$. 为了避免 $\boldsymbol{M}$ 中含有大量连续相同比特,将 $\boldsymbol{M}$ 进行CMI编码[9]得到序列 $\boldsymbol{N}$.

(3) $\boldsymbol{H}$ 和 $\boldsymbol{N}$ 进行二进制内积得到发送序列 $\boldsymbol{D}$,并根据以往发送者对每个好友的点赞概率 p,对 $b\cdot\boldsymbol{D}$ 经过反算术编码得到发送矩阵 $\boldsymbol{G}$. 反算数编码是一种数据解压缩的过程[10],目的是通过概率 p 将0和1之间的小数表示成信息串. 概率 p 是通过对 $\boldsymbol{H}$ 的观察所得,其中1的概率为 $\boldsymbol{H}$ 对应行中1所占的比例;0的概率为 $\boldsymbol{H}$ 对应行中0所占的比例. 对 $\boldsymbol{D}$ 乘系数 b 以满足 $\boldsymbol{D}$ 中都为小数的条件,b 的值通常取 10^{-1} 或 10^{-2}.

(4) 发送者按照 $\boldsymbol{G}$ 对其 n 个好友后续的动态进行点赞,若 $\boldsymbol{G}$ 中某元素为1,则进行点赞;若 $\boldsymbol{G}$ 中某元素为0,则不进行点赞.

2.2 接收端

接收端采用发送者对多个接收者进行人员分配的方案. 接收者用 R_i 表示($i=1,2,\cdots,r_1$,r_1 为接收者的个数),非接收者用 N_j 表示($j=1,2,\cdots,r_2$,r_2 为非接收者的个数). R_i 和 N_j 统称为可能接收者 $P_\lambda(\lambda=1,2,\cdots,k)$. k 满足:

$$k=r_1+r_2 \tag{2}$$

接收端具体流程如下:

(1) 根据人员分配协议,从 $P_\lambda(\lambda=1,2,\cdots,r_1+r_2)$ 中选出 $R_i(i=1,2,\cdots,r_1)$. R_i 根据点赞情况重构 $\boldsymbol{G}_i$,$\boldsymbol{G}_i$ 代表 S 与 R_i 的共同好友所对应的发送矩阵. 接收端将 $\boldsymbol{G}_i$ 依次按行连接,去除相同的行(冗余)并用矩阵 $\boldsymbol{A}$ 表示.

(2) 根据 p 对 $\boldsymbol{A}$ 进行算数编码,并将编码后结果乘 b^{-1} 得到 $\boldsymbol{B}$. 算术编码是一种数据压缩过程[10],目的是通过概率 p 将信息串表示成0和1之间的小数,其中 p 的获得与2.1节相同. $\boldsymbol{A}$ 是 $\boldsymbol{G}$ 的子矩阵,$\boldsymbol{C}$ 是 $\boldsymbol{H}$ 的子矩阵. 由于 $\boldsymbol{G}$ 的每一行与 $\boldsymbol{H}$ 是相对应的,接收端通过观察 $\boldsymbol{H}$ 来获得与 $\boldsymbol{A}$ 所对应的 $\boldsymbol{C}$. 利用数据重建求解 $\boldsymbol{N}$,对 $\boldsymbol{N}$ 进行CMI解码得到 $\boldsymbol{M}$.

为了实现发送者对接收者状态的操作可控,人员分配协议需满足以下两个条件:接收端的状态可用数值 y 表示;发送者通过控制 y 的值,对接收端的状态进行控制.

将 w_λ 表示 P_λ 的权重. 当 P_λ 为接收者,$w_\lambda>0$;当 P_λ 为非接收者,$w_\lambda=0$. 令

$$\sum_{\lambda=1}^{r_1+r_2} w_\lambda = y \tag{3}$$

故 y 的值反映了可能接收者 P_λ 的状态. 发送者设定一个阈值 $a(a>y)$,通过改变 a 的值来控制 P_λ 的状态. a 和 y 的关系满足:

$$\arg\min\left(a-y\right)=y \tag{4}$$

现将w_λ用$w_\lambda\cdot x_\lambda$表示,其中$x_\lambda\in\{0,1\}$,$x_\lambda=1$时,P_λ为接收者;$x_\lambda=0$时,P_λ为非接收者. 则以上关系的数学模型为

$$\sum_{\lambda=1}^{r_1+r_2} w_\lambda\cdot x_\lambda\le a \tag{5}$$

此数学模型的文字叙述为:发送者设定阈值a来控制P_λ的状态,P_λ状态的最优解满足a与y的差值最小. 故针对一对多行为隐写的人员分配协议,可用0-1背包算法来解决.

0-1背包人员分配协议如图3所示,P_λ各自拥有重量w_λ和价值v_λ,并且根据发送者S公布的0-1背包信息,利用动态规划法计算得知最优解时背包问题的最大价值$v_{[k][c]}$[11]. 接收端在k个P_λ中随机选出r_1个P_λ,他们的价值用$v_{k\varphi}(\varphi=1,2,\cdots,r_1)$表示,并判断式(6)是否成立.

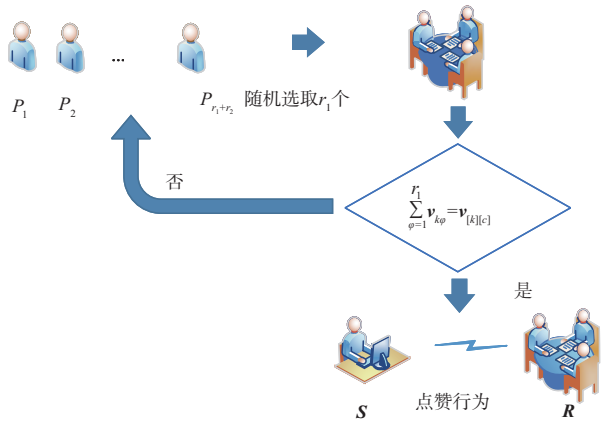


图3　0-1背包人员分配协议

$$\sum_{\varphi=1}^{r_1} v_{k\varphi}=v_{[k][c]} \tag{6}$$

如果式(6)成立,则这r_1个P_λ均为接收者;否则再次进行0-1背包人员分配协议过程.

2.3　算法流程

将上述发送端和接收端整合,则本文所提出的基于0-1背包算法的一对多行为隐写技术详细流程如算法1所示.

算法1　基于0-1背包算法的一对多行为隐写

输入:秘密信息$\boldsymbol{M}$,点赞矩阵$\boldsymbol{H}$,点赞概率p,背包容量c,可能接收者的价值信息$\boldsymbol{v}=[v_1,v_2,\cdots,v_k]$,重量信息$\boldsymbol{w}=[w_1,w_2,\cdots,w_k]$,$v[0][]=0$,$v[][0]=0$

输出:秘密信息$\boldsymbol{M}$

1. 将$\boldsymbol{M}$进行CMI编码得到$\boldsymbol{N}$;
2. $\boldsymbol{D}\leftarrow\boldsymbol{H}*\boldsymbol{N}$
3. 根据p计算$b\cdot\boldsymbol{D}$的反算数编码得到$\boldsymbol{G}$;
4. 随机选取k个$\boldsymbol{G}$的子矩阵作为发送者与k个接收者的共同好友;
5. For $i\leftarrow1$ To k
6. Do For $j\leftarrow1$ To c
7. $v[i][j]\leftarrow v[i-1][j]$;
8. If $\left(j\ge w_i\right)$
9. $v[i][j]\leftarrow$ Max $\left(v[i][j],\ v[i-1][j-w_i]+v_i\right)$;
10. Return $v[k][c]$;
11. 在$v=[v_1,v_2,\cdots,v_k]$中随机选取r_1个元素直到满足式(6)
12. 依次连接矩阵$\boldsymbol{G}_i$,并去除$\boldsymbol{G}_i$相同行得到矩阵$\boldsymbol{A}$;
13. 在$\boldsymbol{H}$中找到与$\boldsymbol{A}$对应的$\boldsymbol{C}$;
14. 根据p计算$\boldsymbol{A}$的算数编码,并将结果与b^{-1}相乘得到$\boldsymbol{B}$;
15. 根据数据重建解出$\boldsymbol{N}$;
16. 将$\boldsymbol{N}$进行CMI解码得到$\boldsymbol{M}$

算法1中,发送端对应伪代码中1~4行,接收端对应伪代码中5~16行,0-1背包问题的求解过程对应伪代码中5~10行,0-1背包分配协议对应伪代码中第11行. 算法的时间及空间复杂度均为O(ck).

3　实验结果

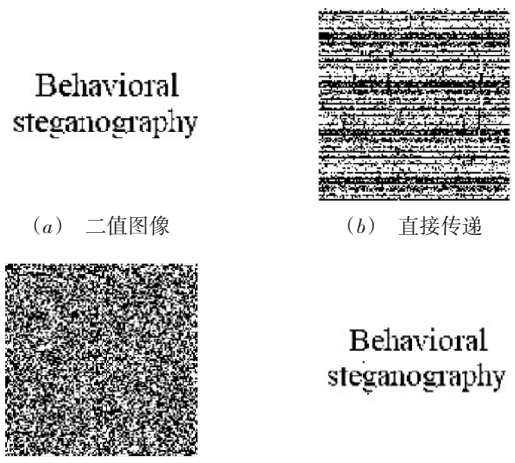
本文以微信中某一个用户作为发送者,使用We Chat Moment Stat检索其朋友在Android设备上发布的动态,选择满足条件的朋友作为接收者,以此为基础进行测试实验并分析. 实验采用酷睿4核i5-6300HQ,8 GB内存,NVIDIA GeForce GTX 950M GPU,操作系统为Windows 10的设备上进行,使用MATLAB编程语言实现.

3.1　可行性分析

我们以S的某8位朋友作为可能接收者,将$\boldsymbol{M}$的位数l设为16,反算数编码的位数设为8. 在传递大小为128×128的二值图实际实验中,依次按列选取16个像素点作为秘密信息,并选出至少与S有8位共同好友的6位作为可能接收者,每传递16位秘密信息,发送者根据0-1背包分配协议随机选取4位接收者,2位非接收者;在传递大小为256×256的灰度图模拟实验中,发送端将灰度图分解为八个二值图进行遍历操作,接收端将恢复后的八个二值图合成为灰度图进行误码率分析.

3.1.1　传递二值图可行性分析

图4(a)为待传递的二值图像,图4(b)为直接传递后的结果,误码率高达49.29%,可见对于二值图中大量连续相同比特的情况,算数编码具有较大的误差. 图4(c)为加入混沌变换[12]图像处理后的结果,误码率高达52.44%,分析得知,混沌变换不能彻底解决大量连续相同比特的情况. 图4(d)为加入CMI编码图像处理后的结果,误码率为0.02%. 由此可见,本文中提出的加入CMI编码图像预处理方法误码率较低,有较好的可行性.



（a） 二值图像 （b） 直接传递

（c） 混沌变换 （d） CMI编码

图4 传递二值图的可行性分析

3.1.2 传递灰度图可行性分析

图5(*a*)为Lena灰度图，图5(*b*)至图5(*i*)依次为灰度图分解的八个位图，图5(*j*)为接收端恢复后的灰度图．8个位图总误码率为0.461%，灰度图误码率为3.06%．实验结果表明，本方案有较低的误码率，并且有较好的可行性．

3.2 接收者掉线情况下可行性分析

要保证接收端正确提取秘密信息$\boldsymbol{M}_{l\times 1}$，就要确保其他接收者收到的发送矩阵的并集不小于$2l$行．$R_i(i=1,2,\cdots,r_1)$与$S$的共同好友数用$n_i(i=1,2,\cdots,r_1)$来表示．$h$表示$R_i(i=1,2,\cdots,r_1)$与$S$共同好友数的算术平均值：

$$h=\sum_{i=1}^{r_1}n_i\Big/r_1 \tag{7}$$

掉线情况分析如下：

（1）当至少有1位接收者（用R_f表示，$f\in\{1,2,\cdots,r_1\}$）与S的共同好友数大于或等于$2l$时，R_f与其他在线接收者不会受掉线接收者的影响；

（2）当$R_i(i=1,2,\cdots,r_1)$与S的共同好友数都小于$2l$时，r_1个接收者中仅有$s(s\leqslant r_1)$个人在线的情况下，在线接收者能收到发送矩阵的并集不小于$2l$行的概率p_1为：

$$p_1=1-\frac{C_n^{2l-1}}{(C_n^h)^s} \tag{8}$$

本小节在数据集样本的基础上，传递4位秘密信息，选取与S共同好友数为3的5位朋友作为可能接收者．每一种情况都进行1000次测试，结果如图6所示．

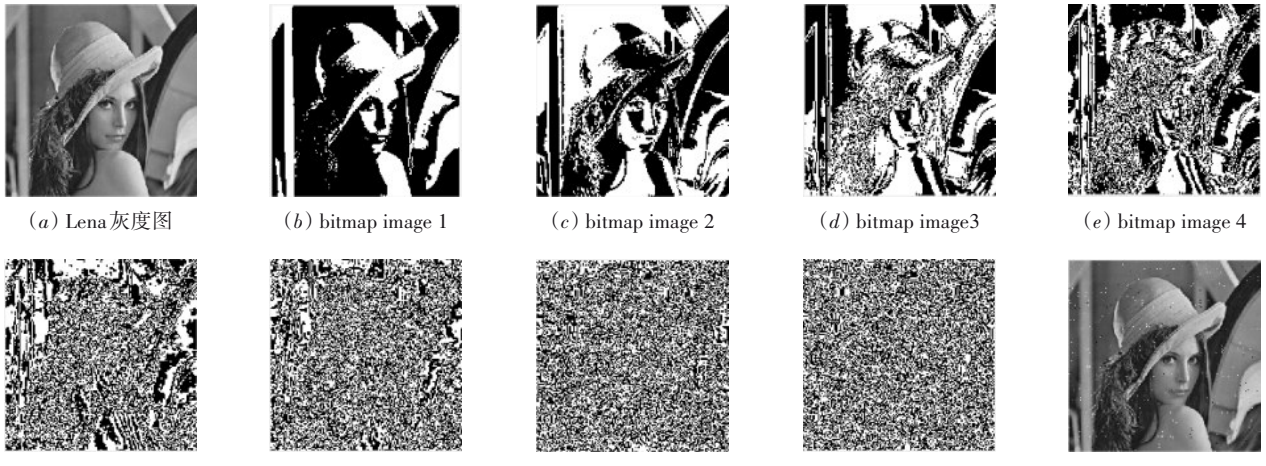
实验分析如下：

对比绿色和橙色条形图可知，在线接收者的个数s并不是决定是否接收成功的关键，关键在于h与s的乘积是否大于$2l$．对比黄色和橙色条形图可知，其他条件不变的情况下，h对成功率影响较大，故在实际应用可以提高h来提高传递秘密信息的成功率．

3.3 暴力攻击下的安全性分析

暴力破解攻击[13]往往针对具有有限容量的密码字典并且有破解成功提醒的加密方案，社交网络下行为隐写虽然具有有限容量的密码字典，但并没有破解成功提醒．所以针对暴力破解攻击，本文的方案理论上是绝对安全的．

文献[14]提出了利用行为相关性检测异常点赞行为的隐写分析算法，该算法将动态按点赞的数量升序排序．点赞数量占三分之一以下的动态数目用d_1表示；点赞数量占三分之二以上的动态数目用d_2表示．将这两种类型可疑者做出的点赞数目分别用d_1'和d_2'表示，计算差值$d=d_1'/d_1-d_2'/d_2$，如果$d<0.25$，则点赞行为异常，否则点赞行为正常．



（a）Lena灰度图 （b）bitmap image 1 （c）bitmap image 2 （d）bitmap image3 （e）bitmap image 4

（f）bitmap image 5 （g）bitmap image 6 （h）bitmap image 7 （i）bitmap image 8 （j）恢复后的Lena灰度图

图5 传递灰度图的可行性分析

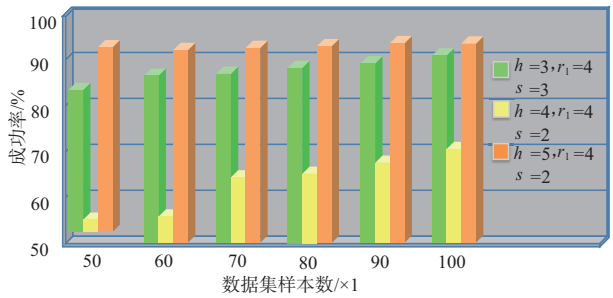


图6　接收端不同种掉线情况下的可行性分析

本实验利用暴力破解攻击和文献[14]的隐写分析方法对文献[7]与本文方案在不同测试集下进行攻击破解,数据集统计如表1所示.

表1　数据集样本统计

数据集样本数	共同好友数
50	10
60	12
70	13
80	15
90	17

在此数据集的条件下,暴力破解攻击结果如图7所示.

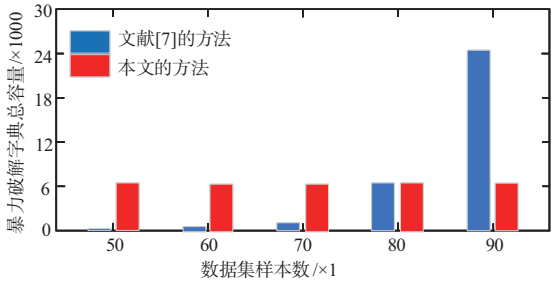


图7　安全性分析

结果显示,随着文献[7]中数据集的增大,发送者和接收者的共同好友增多,会导致暴力破解总次数变多;而0-1背包算法下的点赞隐写由于发送者和接收者们的共同好友数并没改变,所以暴力破解字典总容量并未改变.

我们将暴力破解字典容量用t_1表示,为了测试0-1背包算法对安全性的提升,对不同数据集情况下的安全性进行分析,实验结果如表2所示.

结果表明,随着h的增加,暴力破解字典容量显著增多,安全性显著提高.

3.4　假冒攻击下的安全性分析

本节利用假冒攻击[15],对本文的安全性进行测试. 假冒攻击过程如下:非接收者获得接收者的信息并假冒成接收者,由于协议中每次选取r_1个可能接收者的过程是随机的,假冒者存在一定的假冒成功的几率. 但是假冒者收到的发送矩阵是置乱的,即使假冒者假冒成功,也并不能窃取到秘密信息,所以假冒者对通信过程是破坏,而不是窃取.

表2　不同数据集下的安全性分析

数据集样本数	h	t_1
50	3	6435
60	4	125970
70	5	1081575
80	6	5852925
90	7	23535820
100	8	76904685

由于假冒攻击与数据集样本容量无关,故不考虑数据集样本容量的影响. r_3为非接收者中假冒攻击者的个数,p_2为r_1个接收者被成功确认的概率,p_3为假冒攻击者成功破坏的概率,p_4为检测出假冒者从而中断通信的概率. 对每种情况测试1000次,为了符合社交网络的随机性,每次实验都将接收者和非接收者随机排列.

每次实验只存在3种情况:接收者被成功确认;假冒攻击者成功破坏;协议执行过程中,出现两个及以上可能接收者的背包信息相同,则假冒者一定存在,此时中断通信. 如果不满足3种情况的其中之一,则继续重复协议执行过程. 在假冒攻击者个数为2的情况下,假冒攻击者可能存在两种假冒情况:分别假冒成不同的接收者;假冒成同一个接收者. 这两种情况的统计次数分别置于表3单元格左侧和右侧.

表3　假冒攻击下的安全性测试

r_1	r_2	r_3	p_2(%)	p_3(%)	p_4(%)
3	2	1	20.1	19.7	60.2
3	2	2	7.2 3.0	20.3 7.0	39.2 23.3
4	2	1	14.2	14.6	71.2
4	2	2	5.3 1.5	14.0 3.0	55.7 20.5

实验表明,假冒攻击对本文协议有很强的破坏性,假冒者个数为1时,破坏成功率高达80%到86%;假冒者个数为2时,破坏成功率高达90%到93%.

4　结论

本文提出了基于0-1背包算法的社交网络下行为隐写模型,协议双方由一对一变为一对多,并且接收者的状态可以由发送者控制,更加符合社交网络下随机性的特点. 通过模拟分析得知,该方案有很好的可行性;在安全性上,该方案有很好的抗解密性,但抗检测性不足,假冒攻击下的安全性不高,并且在传递秘密信息的容量上有待提升.

参考文献

[1] LI S, ZHANG X. Towards construction based data hiding:

from secrets to fingerprint images[J]. IEEE Transactions on Image Processing, 2019, 28(3): 1482-1497.

[2] EVSUTIN O O, MELMAN A S, MESHCHERYAKOV R V. Digital steganography and watermarking for digital images: a review of current research directions[J]. IEEE Access, 2020, 8: 166589-166611.

[3] WANG Z, ZHANG X, YIN Z. Joint cover-selection and payload-allocation by steganographic distortion optimization[J]. IEEE Signal Process Lett, 2018, 25(10): 1530-1534.

[4] DUTTA H, DAS R K, NANDI S, et al. An overview of digital audio steganography[J]. IETE Technical Review, 2020, 37(6): 632-650.

[5] PANTIC N, HUSAIN M I. Covert botnet command and control using twitter[C]//Michael Ley. Proceedings of the 31st Annual Computer Security Applications Conference. Los Angeles: Associine for Computer Mair coolinghinery, 2015: 171-180.

[6] LI S, HO A T S, WANG Z, et al. Lost in the digital wild: hiding information in digital activities[C]//Shujun Li. Proceedings of the 2nd International Workshop on Multimedia Privacy and Security. Toronto, Canada: Associine for Computer Mair Coolinghinery, 2018: 27-37.

[7] ZHANG X. Behavior Ssteganography in Social Network [M]. Taiwan, China: Springer International Publishing, 2017: 21-23.

[8] HU F. A probabilistic solution discovery algorithm for solving 0-1 knapsack problem[J]. International Journal of Parallel, Emergent and Distributed Systems, 2018, 33(6) : 618-626.

[9] 赵晓东, 程煜洋, 左磊, 方圆. 基于 FPGA 的 CMI 编解码设计[J]. 现代信息科技, 2020, 4(19): 35-37.
ZHAO Xiaodong, CHENG Yuyang, ZUO Lei, FANG Yuan. Design of CMI CODEC based on FPGA[J]. Modern Information Technology, 2020, 4(19): 35-37. (in Chinese)

[10] SUBRAMANIAN B, YESUDHAS H R, ENOCH G J. Channel-based encrypted binary arithmetic coding in wireless sensor networks[J]. Ingénierie des Systèmes d´Information, 2020, 25(2): 199-206.

[11] 鄢莉 .0-1 背包问题的算法决策分析[J]. 电脑知识与技术, 2020, 16(04): 259-264.
YAN Li. Algorithmic decision analysis of 0-1 knapsack problem[J]. Computer Knowledge and Technology, 2020, 16(04): 259-264. (in Chinese)

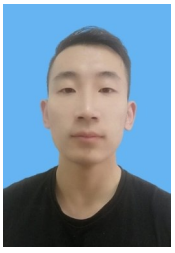
[12] 韩雪娟,李国东 . 动态猫变换和混沌映射的图像加密算法[J]. 计算机工程与设计, 2020, 41(08): 2381-2387.
HAN Xue-juan, LI Guo-dong. Dynamic cat transformation and chaotic mapping image encryption algorithm[J]. Computer Engineering and Design, 2020, 41(08): 2381-2387. (in Chinese)

[13] 张文金,覃仲宇,冯钊,刘嘉奇,刘纬,唐锡南 . 大数据下的 web 暴力破解攻击检测[J]. 深圳大学学报(理工版), 2020, 37(S1): 44-49.
ZHANG Wenjin, QIN Zhongyu, FENG Zhao, LIU Jiaqi, LIU Wei, TANG Xinan. Big data analysis for detection of web brute-force attack[J]. Journal of Shenzhen University Science and Engineering), 2020, 37(S1): 44-49. (in Chinese)

[14] HU Y, WANG Z, ZHANG X. Steganography in social networks based on behavioral correlation[J]. IETE Technical Review, 2020, 38(1): 93-99.

[15] KANTARTOPOULOS P, PITROPAKIS N, MYLONAS A, et al. Exploring adversarial attacks and defences for fake twitter account detection[J]. Technologies, 2020, 8 (4): 64.

作者简介



高 鹏 男,1993 年 7 月生于吉林省双辽市 . 现为东北大学计算机科学与工程学院硕士研究生 . 主要研究方向为信息安全技术 .
E-mail: 2864521280@qq.com

柴鹏翔 男,1999 年 2 月生于辽宁省鞍山市 . 现为东北大学计算机科学与工程学院硕士研究生 . 主要研究方向为信息安全技术 .
E-mail: 2466887390@qq.com

郎 俊(通讯作者) 男,1982 年 2 月生于黑龙江省齐齐哈尔市 . 现为东北大学计算机科学与工程学院副教授,硕士生导师 . 主要研究方向为信息安全与对抗、生物医学成像、压缩感知及应用 .
E-mail: langjun@mail.neu.edu.cn