文章编号：2095-2163(2020)01-0144-05 中图分类号：TP393 文献标志码：A

物联网中基于混沌模型的隐私安全算法研究

宫海梅，王 伟，许桂月
（海南工商职业学院 信息工程系，海口 570203）

摘 要：在物联网应用中，各种物体可与物联网互联，人们可以得到便捷的服务。但在信息传输过程中用户隐私信息可能被泄露，如何解决此问题受到人们的广泛关注。针对 2 个问题：一是隐私数据生命周期中前期工作需要加强，二是用户参与到数据隐藏工作中，根据实际需求选择需要隐藏的数据。研究提出在数据采集前，根据用户需求进行数据隐密传输。为了保障隐私信息在传输中不被泄露，本文设计一种轻量级加密方法、即数字水印安全套装结构，进行数据隐藏，保障隐私信息安全。该方法基于离散余弦变换和混沌算法，在图像载体频域内隐藏隐私信息，隐私信息具体嵌入位置通过利用混沌算法，和人眼视觉特性的关系动态进行调整，考虑到混沌算法中的初值和参数万一被破解导致隐私信息被破解问题，对混沌算法产生的随机数位置进行进一步的自创公式选择隐藏位置，这样非法截获者肉眼无法察觉隐密信息的存在，也无法对用户内容解密。仿真结果从隐蔽性、隐藏容量和鲁棒性三方面分析，表明该算法可以实现隐私信息的加解密，对其进行攻击实验，仍可获得信息，相比于直接传输敏感信息更安全可靠。

关键词：隐私保护；离散余弦变换；混沌算法 ；物联网

Research on privacy preservation algorithm based on chaos in IoT

GONG Haimei, WANG Wei, XU Guiyue
(Department of Information Engineering, Hainan Technology and Business College, Haikou 570203, China)

【Abstract】 In the application of the Internet of Things, various objects can be connected with the Internet of Things, and people can get convenient services. however, User privacy information may be leaked in the process of information transmission, how to solve this problem is widely concerned by people. This paper deals with two problems: one is that the preliminary work in the privacy data life cycle needs to be strengthened; the other is that user participates in hiding the data and dynamically selects the data that needs to be hidden. The research presents data need to be encrypted according to user requirements before data acquisition. In this paper, a lightweight encryption method " digital watermark security package structure" is designed for privacy information hiding. This method is based on discrete cosine transformation (DCT) and chaos algorithm, and hides privacy information in frequency domain of image carrier, The specific embedding position of privacy information is adjusted dynamically by using chaos algorithm to generate random numbers and the relationship between human visual characteristics . Moreover, if the initial value and parameters of chaos algorithm are cracked, it can lead to privacy information being cracked, so the random number position generated by the chaos algorithm can be further self-created to select the hidden position. Thus, the illegal interceptors cannot visually detect the existence of the hidden information, nor can they decrypt the user′s content. Simulation results are analyzed from three aspects such as concealment, hiding capacity and robustness, showing that the algorithm can achieve encryption and decryption of privacy information, and the processing time is short. The privacy information can still be obtained by attacking it, and it is more secure and reliable compared with direct transmission of privacy information.

【Key words】 privacy preservation; discrete cosine transformation; chaos algorithm; IoT

0 引 言

2005 年，国际电信联盟（ITU）发布了《ITU Internet Reports 2005：the Internet of Things》[1]。随着时代的进步、物联网的快速发展，智慧城市、智能家居、智慧医疗、基于位置服务等应用技术给人们带来极大的便利。凭借超强的感知和通信能力，物联网将是大数据产生的主要来源。在这些数据中有很多涉及个人隐私，以致企业机密，如果不对这些数据加以妥善处理，将会给身处其中的成员个体带来不可估量的影响。如何保护隐私信息安全的问题引起了人们的广泛关注，2016 年 4 月欧盟颁布《通用数据保护条例》，为人们的隐私保护提供了可参考的应用标准[2-4]。

物联网中的设备可以产生大量的数据，如何更好地保护这些用户数据，需要对其做出详尽的分析。根据数据生命周期可以分为 4 个阶段，即：获得、处

基金项目：海南省高等学校科学研究项目（Hnky2018-95）。

作者简介：宫海梅（1983-），女，副教授，主要研究方向：移动通信、通信与信息系统、图像处理；王 伟（1952-），男，高级工程师，主要研究方向：计算机、图像处理；许桂月（1988-），女，讲师，主要研究方向：电子与通信工程、图像处理。

收稿日期：2019-10-16

理、存储和传播。物联网数据获取来自于感知物体，数据采集过程中可能被不同的机构所存储，在处理存储前如果不引入任何加密保护，可能会造成信息泄露，所以在获取数据阶段就需要对数据进行保护[4-6]。人们在处理和存储阶段前后开展了多项工作进行数据的隐私保护[7-10]。经过前面三个阶段的处理，用户数据才可以安全传播。

为了保障物联网中用户数据安全，研究者采用匿名路由、数据模糊或数据加密等方法，针对具体隐私对象如实体位置[11-15]、实体身份[16-17]和其它内容信息等进行大量的研究[18]。文献[4]并未着重针对某一隐私对象进行隐藏，而是提出了根据用户实际语境需求动态的模糊用户的相关数据。

本文设计了一种轻量级加密方法、即数字水印安全套装结构，进行数据隐藏，保障隐私信息安全。该算法可以安装到物联网设备上，根据用户实际需求，将需要隐藏的信息隐藏起来，发送给数据采集者，综上得出的设计结构如图 1 所示。

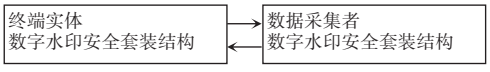


图 1　物联网终端信息隐藏结构

Fig. 1　Internet of Things terminal information hiding structure

1　离散余弦变换

离散余弦变换(DCT)是数字水印技术中最常用的频谱分析方法[19]，其优点是算法快速，低误码率，对各种干扰信号有着良好的抗攻击能力。

二维离散余弦变换(2D-DCT)定义为：

$$X_{uv} = \alpha_u \alpha_v \sum_{i=0}^{N-1} \sum_{k=0}^{N-1} x_{ik} \cos\left[\frac{(2i+1)u\pi}{2N}\right] \cos\left[\frac{(2k+1)v\pi}{2N}\right], \quad (1)$$

二维离散余弦逆变换(2D-IDCT)的定义为：

$$X_{ik} = \sum_{u=0}^{N-1} \sum_{v=0}^{N-1} \alpha_u \alpha_v X_{uv} \cos\left[\frac{(2i+1)u\pi}{2N}\right] \cos\left[\frac{(2k+1)v\pi}{2N}\right]. \quad (2)$$

其中，系数 α_u，α_v 的数学运算公式可写为：

$$\alpha_u = \begin{cases} \sqrt{1/N} & u = 0 \\ \sqrt{2/N} & u = 1,2,\ldots,N-1 \end{cases}$$

$$\alpha_v = \begin{cases} \sqrt{1/N} & v = 0 \\ \sqrt{2/N} & v = 1,2,\ldots N-1 \end{cases}$$

2　混沌密码学

混沌密码学是混沌理论的一个重要的应用领域。目前较为常用的是一维的 Logistic 映射[20]，该映射方程又称为虫口模型，最初是描述生态学的生物种群繁衍的数学模型，后演变为一种研究随机现象的数学模型。运算时需用到如下数学公式：

$$x_{n+1} = ux_n(1 - x_n). \quad (3)$$

其中，n 是自然数(1,2,3…)，当 X_1 固定，即虫口的最初数量，u 用来控制整个函数的增长。

进行大量实验，此处仅列举当设初值 $X_1 = 0.5$ 时，$u = 3.5$、3.8、3.9、4.0 时的图形，迭代 100 次，如图 2~图 5 所示。由图 2~图 5 得出，当初值已定，随着 u 值变大，随机数呈现混沌状态，当 $u = 3.9$ 时，混沌状态最佳，当 $u > 4$ 后不呈现混沌状态。分析得出当 $u = 3.5 \sim 4$ 之间，随着迭代次数增多，该映射方程的随机数具有伪随机性、轨道不可预测性以及对初值极度敏感性的特点。利用混沌系统的这种特性，可以用于信息置乱。考虑到混沌算法中的初值和参数一旦遭遇非法窃取，可以利用本文研究得到的自创公式进一步地选择隐私信息隐藏位置。该自创公式在运算中可以产生加密和解密密钥 Key。

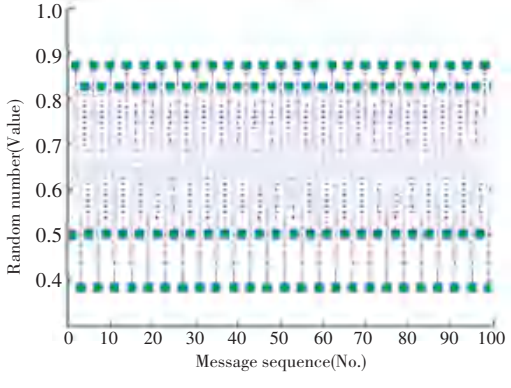


图 2　$u = 3.5$

Fig. 2　$u = 3.5$

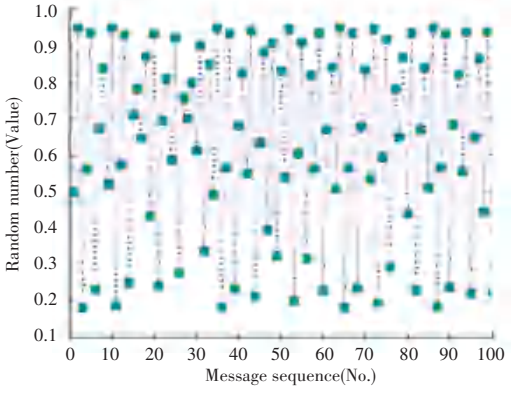


图 3　$u = 3.8$

Fig. 3　$u = 3.8$

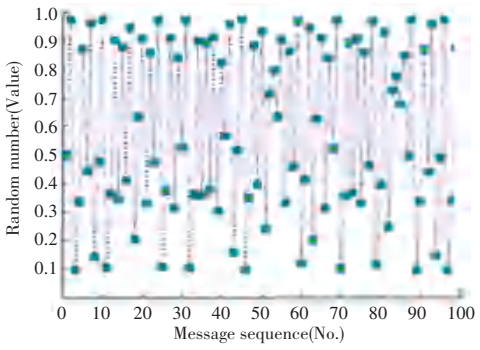


图 4 $u=3.9$

Fig. 4 $u=3.9$

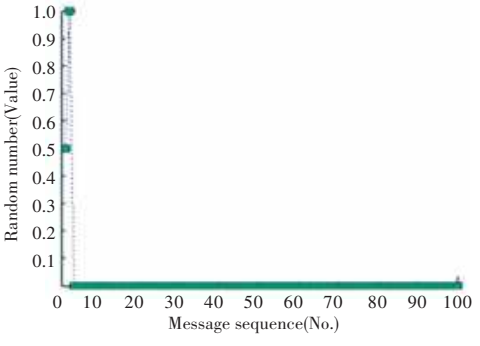


图 5 $u=4.0$

Fig. 5 $u=4.0$

3 数字水印安全套装结构

数字水印安全套装结构的算法流程图如图 6 所示,该过程包括 3 部分,分别是:信息准备、信息隐藏和信息接收。对此可做阐释分述如下。

(1)信息准备。选择载体图像,待传信息的选择由用户决定。

(2)信息隐藏。对载体图像进行分块,再对分块后图像进行 DCT 变换,获得欲嵌入隐私信息的系数序列,根据实际待传信息大小确定 Logistic 模型迭代次数,求取隐密信息嵌入位置,同时结合人眼视觉特性的关系动态调整最终嵌入位置,经过以上隐藏位置的选择,获得置乱的信息序列,嵌入载体图像,形成频域系数序列矩阵。在此基础上将进行 DCT 反变换,实现了信息的加密过程。在上述过程中密钥 Key 是自创公式的结果,即双方约定好的算法。

(3)信息接收。该过程接收是盲检测,对收到的图像分块进行 DCT 变换,分解成系数序列,根据约定的密钥 Key,检出隐藏的信息位,恢复原信息序列,获得所需的隐密信息。

4 实验分析

该实验仿真环境 Intel(R) corei5, 1.6 GHz, Matlab7OR14。任意选择一个彩色图片 $M*N$ 作为载密体,实验选择的图片尺寸为 720 * 960,位深度为 24。对这段明文信息“Miss wang, female, ID Number 1234567891234567 89”隐藏处理。将该明文转换为二进制代码,可以得到 376 bit。

载体图像见图 7,载体的 DCT 主要能量集聚区见图 8,通过该数据确定 DCT 变换嵌入的阈值及信息嵌入位置。取载体的 R 层见图 9,进行隐私信息嵌入,隐私信息的具体嵌入位置也可以是 G 层和 B 层。嵌入信息后的图像见图 10。

本次研究拟分别从隐蔽性、隐藏容量和鲁棒性三个方面进行分析。研究内容详述如下。

(1)安全性分析。对载体图像(图 7)和嵌入信息后的图像(图 10)进行比较分析,隐私信息嵌入到载体图片后,不会造成画面质量的明显下降,视觉系统无法感觉到信号的存在。同时为了对图像的隐藏效果进行分析,采用了峰值信噪比(*PSNR*)。*PSNR* 用来衡量载体图像 C 和秘密图像 M 之间的保真度,*PSNR* 值越高说明算法性能越好,数学运算公式可表示为:

$$PSNR = 10 \times \lg\left[\frac{M \times N \times 255^2}{\sum_{i=1}^{M}\sum_{j=1}^{N}(C(i,j) - M(i,j))}\right]. \quad (4)$$

至此,研究求得的本文算法在攻击下提取的信息及 *PSNR* 见表 1。

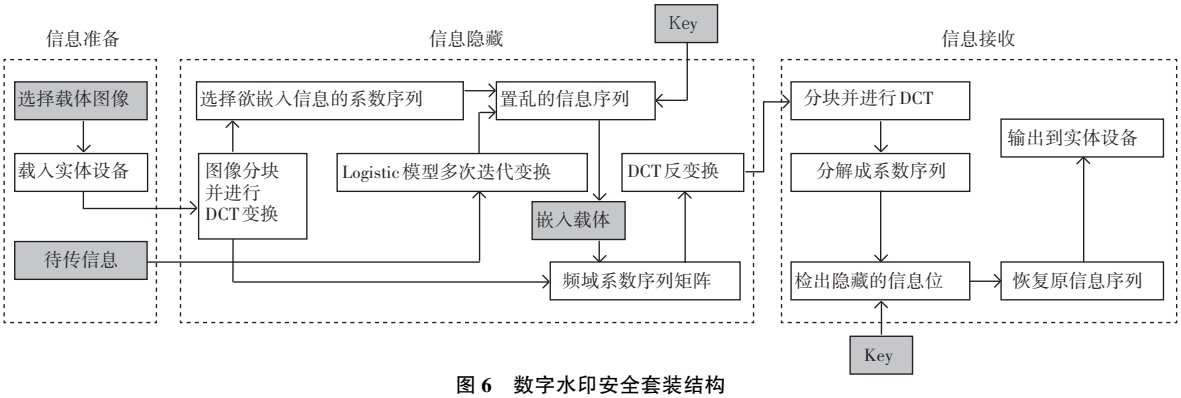


图 6 数字水印安全套装结构

Fig. 6 Digital watermark security package structure

图 7　载体图像

Fig. 7　Carrier image

图 8　载体 DCT 主要能量集聚区

Fig. 8　Main energy area of carrier image DCT

图 9　嵌入载体的 R 层图像

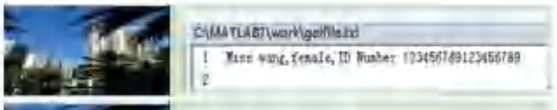
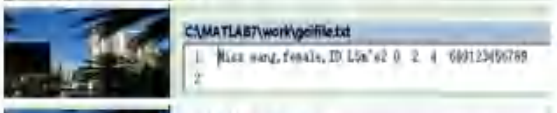
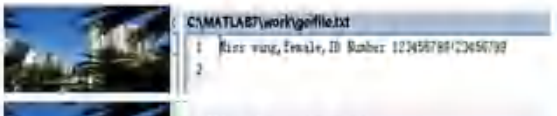
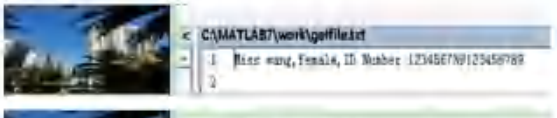
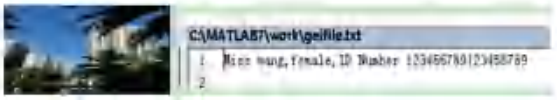
Fig. 9　R layer of watermarked image

图 10　嵌入信息后的图像

Fig. 10　Watermarked image

表 1　算法在攻击下提取的信息及 *PSNR*（嵌入深度为 2.0 时）

Tab. 1　Information extracted under attack and *PSNR* (embedding depth is 2.0)

	嵌入信息后的图像	提取出的隐私信息	*PSNR*/dB
无噪声			34.399 0
剪切攻击			16.732 1
涂鸦攻击			32.058 4
高斯噪声攻击			22.944 4
椒盐噪声攻击			27.071 5
乘性噪声攻击			24.827 5
泊松噪声攻击			33.801 3

(2)容量分析。该数字水印安全套装结构取图像的某一层进行 8 * 8 分块,图 7 载体图像的尺寸 720 * 960,分块后可以隐藏 10 800 bit,要隐藏的隐私信息是 376 bit,冗余度为 28.7。为了保证信息可靠传输,隐私信息可以被冗余嵌入。如果嵌入信息时考虑其他两层也重复嵌入隐密信息,则嵌入信息的可靠性可以提高 3 倍的冗余度,但却要考虑可见的影响。在日常生活中要传输的关键信息、如身份信息、电话号码、地址信息等均可以选用此法进行隐藏。

(3)鲁棒性分析。通过改变载体频域内的一对系数的值来嵌入信息,嵌入深度是对系数改变的大小,嵌入较深时图像改变较大,影响外观,嵌入较浅时,对图像影响少,但在传输时受自然干扰和攻击时的鲁棒性却欠佳。对隐藏有信息的图片进行攻击实验,研究中给出了嵌入深度为 2.0 时所得的测试结果见表 1。由表 1 可以得出,该算法可以对抗无意攻击,能够提取隐私信息。人为攻击时,如剪切攻击不能有效提取隐私信息。该实验结果中,隐私信息嵌入一次,如经多次冗余嵌入,可以预见抗剪切攻击性能可以提高。

5 结束语

为了保障隐私信息在传输中不被泄露,本文设计提出了一种轻量级加密方法、即数字水印安全套装结构,进行数据隐藏,保障隐私信息安全。本次研究从隐蔽性、隐藏容量和鲁棒性三方面进行仿真分析,结果表明该算法可以实现隐私信息的加解密,对其进行攻击实验,在对抗无意攻击时仍可获得信息,相比于直接传输敏感信息更为安全可靠。

参考文献

[1] ITU Strategy and Policy Unit(SPU).ITU Internet Reports 2005: The Internet of Things [R]. Geneva: Geneva International Telecommunication Union(ITU),2005.

[2] ZHENG Mengyao, XU Dixing, JIANG Linshan, et al. Challenges of privacy-preserving machine learning in IoT [C]// AI Challenge IOT´19. NewYork, USA: Association for Computing Machinery, 2019:1-7.

[3] BERTINO E, CHOO K K R, GEORGAKOPOLOUS D, et al. Internet of things (IOT): Smart and secure service delivery[J]. ACM Transactions on Internet Technology (TOIT), 2016, 16(4):22.

[4] PANAH A S, YAVARI A, van SCHYNDEL R G, et al. Context-driven granular disclosure control for Internet of Things applications[J]. IEEE Transactions on Big Data,2019,5(3):408-422.

[5] ROMAN R, ZHOU J, LOPEZ J. On the features and challenges of security and privacy in distributed Internet of Things[J]. Computer Networks, 2013,57(10):2266-2279.

[6] GRISPOS G, GLISSON W B, CHOO K K R. Medical cyber-physical systems development: A forensics-driven approach [C]//Proc. of IEEE/ACM Conference on Connected Health: Applications, Systems and Engineering Technologies (CHASE). Philadelphia, Pennsylvania, USA:IEEE, 2017:108-114.

[7] BERTINO E. Big data-security and privacy[C]//2015 IEEE International Congress on Big Data. New York:USA, 2015:757-761.

[8] QIN Zhan, WENG Jian, CUI Yong, et al. Privacy-preserving image processing in the cloud[J]. IEEE Cloud Computing, 2018, 5(2):48-57.

[9] JOSHI V B, RAVAL M S, KURIBAYASHI M. Reversible data hiding based compressible privacy preserving system for color image[J]. Multimedia Tools and Applications, 2018, 77(13): 16597-16622.

[10] NIU Xuejing, YIN Zhaoxia, ZHANG Xinpeng, et al. Reversible data hiding in encrypted AMBTC compressed images[M]// SHI Y, KIM H, PEREZ-GONZALEZ F, et al. Digital forensics and watermarking. IWDW 2016. Lecture Notes in Computer Science. Cham:Springer, 2016,10082:436-445.

[11] GRUTESER M, GRUNWALD D. Anonymous usage of location-based services through spatial and temporal cloaking [C]// MobiSys 2003: The First International on Mobile Systems, Applications, and Services. San Francisco, CA, USA: Usenix Association,2003:31-42.

[12] GRISSA M, YAVUZ A A, HAMDAOUI B. Location privacy preservation in database-driven wireless cognitive networks through encrypted probabilistic data structures[J]. arXiv preprint arXiv:1806.03557,2018.

[13] SUN Gang, LIAO Dan, LI Hui, et al. L2P2: A location-label based approach for privacy preserving in LBS [J]. Future Generation Computer Systems,2017,74:375-384.

[14] SUN Gang, CHANG V, RAMACHANDRAN M, et al. Efficient location privacy algorithm for Internet of Things (IoT) services and applications [J]. Journal of Network and Computer Applications,2017,89:3-13.

[15] DIMITRIOU K, ROUSSAKI I. Location privacy protection in distributed IoT environments based on dynamic sensor node clustering[J]. Sensors, 2019,19(13):3022.

[16] HAQUE A K M B, NISA S T N, BARI M A, et al. Anonymity network tor and performance analysis of 'ARANEA' - an IOT based privacy-preserving router[J]. arXiv preprint arXiv: 1906.01276, 2019.

[17] YU Jie. Measuring and visualizing anonymous network[D]. Madison ,USA:Dakota State University, 2008,

[18] PORAMBAGE P, SCHMITT C, KUMAR P, et al. The quest for privacy in the Internet of Things[J]. IEEE Cloud Computing, 2016,3(2):36-45.

[19]王琪. 基于 DCT 的图像数字水印算法研究[D]. 西安:西北大学,2016.

[20]马翠平. 基于混沌 Logistic 方程的哈希算法的设计与实现[D]. 哈尔滨:哈尔滨理工大学,2018.