基于安全压缩感知的大数据隐私保护

王平[1]，张玉书[2]，何兴[1]，仲盛[3]
1. 西南大学电子信息工程学院，重庆 400715；
2. 南京航空航天大学计算机科学与技术学院，江苏 南京 211106；
3. 南京大学计算机科学与技术系，江苏 南京 210023

摘要
当前的数据“大爆炸”主要受万物互联的驱动，服务于人类衣食住行的各类物联网感知设备时刻在捕获个人隐私数据，然而，这些隐私数据已成为网络攻击的重点目标。分析了资源受限的物联网应用中的数据安全问题，介绍了基于压缩感知理论的隐私保护技术——安全压缩感知，提出了相应的大数据采集方案，并且通过安全性理论和实验分析给出了结论性的呼吁：将安全压缩感知作为一种感知层内置的轻量级加密机制，以近乎零的成本为数据提供第一层安全防护。

关键词
安全压缩感知；大数据；物联网；隐私保护

中图分类号：TP309 文献标识码：A doi: 10.11959/j.issn.2096-0271.2020002

Big data privacy protection based on secure compressive sensing

WANG Ping[1], ZHANG Yushu[2], HE Xing[1], ZHONG Sheng[3]
1. School of Electronics and Information Engineering, Southwest University, Chongqing 400715, China
2. College of Computer Science and Technology, Nanjing University of Aeronautics and Astronautics, Nanjing 211106, China
3. Department of Computer Science and Technology, Nanjing University, Nanjing 210023, China

Abstract
The current “big bang” of data is mainly driven by interconnection of all things. Various types of IoT sensing devices serving in daily life are constantly capturing personal privacy data. However, these privacy data have become the key targets of network attacks. Data security issues in the resource-constrained IoT applications were analyzed, a novel privacy protection technique based on compressive sensing theory was introduced, which is called secure compressed sensing, and a corresponding big data collection scheme was proposed. As demonstrated by the theoretical and experimental security analysis, there is a conclusive appeal for that secure compressive sensing can be used as a lightweight encryption mechanism which is built into the perception layer to provide first-level security protection for data at almost zero cost.

Key words
secure compressive sensing, big data, Internet of things, privacy protection

1 引言

随着数字化和信息化程度的不断提升，全球已进入大数据时代。根据国际数据公司（International Data Corporation，IDC）在2018年11月发布的调研报告显示，全球大数据存储量呈现爆炸式增长。如**图1**所示，全球数据量预计将从2018年的33 ZB增至2025年的175 ZB。值得兴奋的是，中国数据圈占比将从2018年的23.4%（即7.6 ZB）增至2025年的27.8%（即48.6 ZB），成为全球范围内最大数据圈。大数据是人、机和物在网络空间中交互、融合所产生并在互联网上可获得的数据集合，其具有容量大、类型多、集中化存储的特点，通过现代化大数据分析和预测手段，可以充分挖掘其背后隐藏的新知识、新价值和新动力，进而在电信、互联网、金融、交通、医疗等行业创造新的商业模式和应用价值。目前，大数据逐步成为国家基础战略资源和社会基础的生产要素。

目前，数据的增长主要受到来自物联网数据、元数据和与娱乐相关的数据增长的影响，其中物联网数据增速迅猛。在万物互联的时代，成千上万的传感器、服务器和智能终端构成一个比传统互联网更加广泛的物联网，人们可以从外界感知信息，信息交互不再仅限于人与人之间。物联网的发展必然伴随着局域连接与广域连接业务的急剧增长，随着5G商业化落地，联网终端会进一步增多，这将会产生海量的物联网数据。预计到2025年，全球各地联网的数十亿台物联网设备将产生超过90 ZB的数据，这主要受到车联网、无人机网络、可穿戴设备网络和各种监测网络等的驱动。在大数据和物联网时代，人始终是物联网的中心，各种物联网应用服务于人类的衣食住行。无所不在的数据收集技术和专业化、多样化的数据处理技术，使得个人难以控制隐私数据的收集情境和应用途径。因其蕴藏的巨大潜在价值和逐渐集中化的存储管理模式，隐私数据成为网络攻击的重点目标。根据数字安全领域的金雅拓公司（Gemalto）统计，仅2018年上半年，全球范围内公共数据泄露事件达945起，导致45亿条信息泄露。如何保障大数据隐私安全成为一项迫在眉睫的全球性问题。此外，为了追求极致的用户体验，物联网终端设备普遍呈现出轻量化、可植入化的特点，在资源受限的应用环境下数据安全更加难以保障。

压缩感知（compressive sensing，

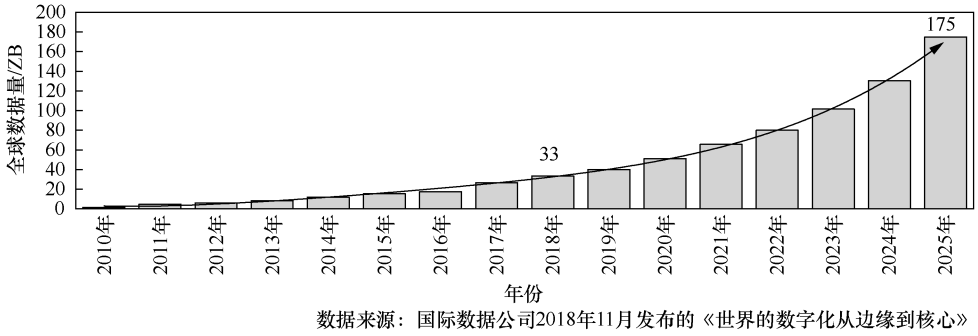

图1 每年全球数据量增长情况预测

CS)[1-3]是一种新兴的信息获取技术，其不仅能摆脱香农/奈奎斯特采样定理的约束，极大地降低数据间的冗余性，而且能在执行采样的同时完成数据压缩，有效地降低信息获取系统的复杂度。近年来，基于CS的信息获取系统获得了学者的广泛关注，其在资源受限的物联网场景中具有重要的应用价值[4-6]。例如，在健康监测体域网[7]中，为了实时监控人体的各项健康数据，同时尽可能完美地与人体契合，智能感知终端往往追求尽可能的便捷化，甚至可植入人体，这便导致终端面临着资源受限的问题，包括计算、存储和能源受限等问题。除了降低采集和通信系统的负担，CS理论也被用于隐私保护领域，本文称之为安全压缩感知(secure compressive sensing，SCS)。本质上，SCS致力于将保密性嵌入压缩采样的过程中，是基于CS的信息获取系统，同时被视为一种特殊的对称密码系统。SCS常用于图像加密领域[8-9]，其不仅考虑到了图像数据间的高冗余性，也考虑到了隐私保护问题。尽管这种方式无法保障采样数据在信息理论上的安全，但其能保障针对密钥或者密文的暴力攻击在计算上不可行[10-11]。鉴于SCS无法单独应用于高安全需求场景的问题，大部分研究工作[12-13]采用混沌密码对采样数据进行二次强加密。也有研究表明[14]，当采用高斯随机数发生器构造测量系统时，通过隐藏样本的能量信息可实现完美加密。此外，一种基于SCS的多级加密框架[15]被提出，针对不同权限级别的用户，从密文中获取的信息量是不同的。

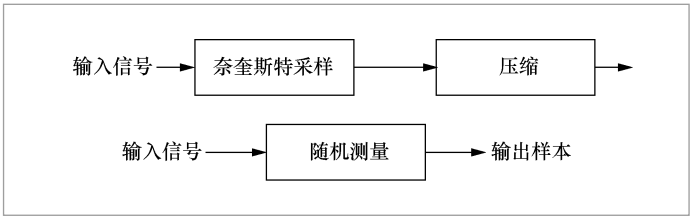

图 2 压缩感知和传统采样对比

本文首先通过介绍CS理论基础引出SCS技术，即嵌入保密性的CS。然后，提出SCS技术普遍适用的物联网场景模型，并且从密码学的角度给出理论分析。最后，通过仿真实验进一步阐述SCS技术的可行性和安全性，并给出结论性的呼吁，即将其作为一种低成本的、内置保密性的信息获取技术，广泛应用在资源受限的物联网场景中。

2 压缩感知理论

CS理论基于信号的稀疏性或可压缩性，不同于传统的先采样后压缩过程(如图2所示)，其能够同步执行采样和压缩操作，并且通过解决欠定方程，系统能够精确地重构出原始信号。假定一个长度为N的一维信号$\boldsymbol{x}$，能够在一个大小为$N\times N$的变换矩阵$\boldsymbol{\Psi}$的作用下稀疏化，那么称之为K-稀疏信号，其中$\boldsymbol{\Psi}=[\psi_1,\psi_2,\cdots,\psi_N]$。稀疏过程表示为：

$$\boldsymbol{x}=\sum_{i=1}^{N}s_i\boldsymbol{\Psi}_i=\boldsymbol{\Psi s} \qquad (1)$$

其中，$\boldsymbol{s}$为一个长度为N的系数向量，包含至多K个非零元。如果$\boldsymbol{s}$是由占绝大多数的小数值元素和少量的大数值元素组成的，那么$\boldsymbol{x}$被称为可压缩信号，可以通过将所有小数值元素视为零元素进行近似稀疏表示。幸运的是，大部分自然信号在预知的一组基上可以进行稀疏化。

在CS理论中，通过构建一个与$\boldsymbol{\Psi}$不相干的大小为$M\times N$($K<M<<N$)的矩阵$\boldsymbol{\Phi}$来线性测量原始信号$\boldsymbol{x}$，该过程可表示为：

$$\boldsymbol{y}=\boldsymbol{\Phi x}=\boldsymbol{\Phi\Psi s}=\boldsymbol{As} \qquad (2)$$

其中，$\boldsymbol{y}$表示长度为M的测量值向量，$\boldsymbol{\Phi}$和$\boldsymbol{A}$($\boldsymbol{A}=\boldsymbol{\Phi\Psi}$)分别叫作测量矩阵和传感矩

阵。采样时用的是测量矩阵$\boldsymbol{\Phi}$，而重构时用的是传感矩阵$\boldsymbol{A}$。

由条件$K<M<<N$可以看出，CS理论主要解决的是欠采样情况下的信号重构问题。本质上，这是一个病态的求逆问题，即通过式（2）求解$\boldsymbol{x}$是一个欠定问题，不具备唯一解。但是，基于原始信号是K-稀疏的先验信息，即信号$\boldsymbol{x}$只有K+1个自由度，理论上仅需超过该自由度的测量数便可以通过最优化方法重构原始信号。具体的做法是求解以下的l_0最优化问题：

$$\min\|\boldsymbol{s}\|_0 \ \text{s.t.}\ \|\boldsymbol{y}-\boldsymbol{A}\boldsymbol{s}\|_2 \leqslant \varepsilon \qquad (3)$$

其中，ε表示噪声。求解式（3）是通过遍历所有可能情况的集合来找到最稀疏的形式，显然这是一个NP难问题。常用的重构算法包括匹配追踪（matching pursuit，MP）[16]和正交匹配追踪（orthogonal matching pursuit，OMP）[17]。经研究表明[8]，求解式（3）可等价于求解以下的l_1最优化问题：

$$\min\|\boldsymbol{s}\|_1 \ \text{s.t.}\ \|\boldsymbol{y}-\boldsymbol{A}\boldsymbol{s}\|_2 \leqslant \varepsilon \qquad (4)$$

求解式（4）是一个线性规划问题，利用常用的基追踪（basis pursuit，BP）算法[18]便可准确地重构信号。

为了保证能够精确地从测量值$\boldsymbol{y}$中重构出原始信号$\boldsymbol{x}$，除了信号的稀疏性这一先验信息，测量矩阵$\boldsymbol{\Phi}$与变换矩阵$\boldsymbol{\Psi}$应该尽可能不相干。对此，传感矩阵$\boldsymbol{A}$需要具备以下受限等距特性（restricted isometry property，RIP）[19-21]：

$$(1-\delta_K)\|\boldsymbol{s}\|_2^2 \leqslant \|\boldsymbol{A}\boldsymbol{s}\|_2^2 \leqslant (1+\delta_K)\|\boldsymbol{s}\|_2^2 \qquad (5)$$

存在$\delta_K \in (0,1)$，对于所有的K-稀疏信号$\boldsymbol{s}$，使得上述不等式成立。事实上，检验一个矩阵是否满足RIP条件也是一个NP难问题。Candès和Tao指出[22]，由独立同分布的高斯或伯努利随机变量构成的随机测量矩阵与任何一个固定变换矩阵大概率不相干。总体来说，待采样信号的稀疏化程度越高，测量矩阵与变换矩阵之间的不相干程度越高，信号重构效果便会越好。

3 基于压缩感知的大数据隐私保护

该节首先在CS理论的基础上介绍融合混沌理论的SCS技术；然后，针对大数据时代的个人隐私泄露问题，构建了SCS技术普遍适用的物联网场景模型；最后，从信息理论上给出SCS技术的安全性分析。

3.1 安全压缩感知

在CS理论中，原始信号$\boldsymbol{x}$的成功重构依赖于测量矩阵$\boldsymbol{\Phi}$的真实性。因此，当将$\boldsymbol{\Phi}$视为一种特殊的密钥时，基于CS的信息获取系统可同时被视为一种特殊的对称密码系统，这便是所谓的SCS。众所周知，一个密码系统由5个基本元素组成，包括明文、密文、密钥、加密和解密。**图3**直观地展示了CS和对称密码之间的对应关系，也就是原始信号对应明文，采样得到的测量值对应密文，测量矩阵对应密钥，采样过程对应加密过程，重构过程对应解密过程。值得注意的是，由于CS是一种有损压缩技术，解密所得的明文与原始明文注定是非一致的。此外，信息与通信系统中的白噪声和重构算法只进行有限次迭代，而引入的重构噪声也将使解密算法不能完美地得到原始明文。

本质上，CS是一个线性映射过程。当掌握充分多的明密文对时，攻击者可以轻松计算出采用的某个固定测量矩阵。为了达到较高的安全级别，基于CS的对称密码系统需要频繁地更新密钥$\boldsymbol{\Phi}$，甚至采用一次一密的设置。由前文可知，密钥尺寸$\boldsymbol{\Phi}$是远大于明文$\boldsymbol{x}$尺寸的。倘若采用一次性的

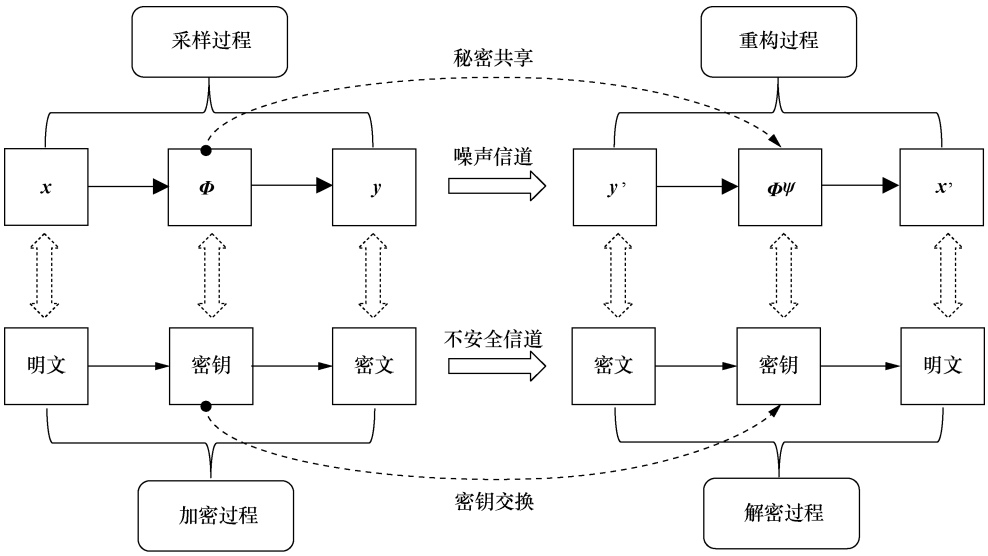

图 3 压缩感知与对称密码之间的对应关系

$\boldsymbol{\Phi}$，每次测量都需要传输远多于采样数据的密钥数据，这反过来将导致严重的数据灾难，明显与CS的设计理念相违背。为了避免直接传输大尺寸的$\boldsymbol{\Phi}$，并且保持CS低复杂度采样的优势，可以尝试通过混沌系统生成混沌序列，进而用来构造测量矩阵。

混沌是非线性动力学系统中特有的一种运动形式。混沌系统本质上是一种确定性系统，但其呈现出非周期性和伪随机特性。一维混沌系统可表示为：

$$c_{i+1}=f(c_i),\quad 0<c_i<1 \tag{6}$$

其中，$f(\cdot)$表示某种确切的映射关系，c_0为该混沌系统的初始输入值，即种子值。由以上混沌系统产生的混沌序列$C(c_0)=\{c_i \mid i=0,1,\cdots,c_i\in(0,1)\}$经等尺度变换和等间距抽样操作后，可得到一个长度为$M\times N$的伪随机序列$Z(c_0)=\{z_j \mid j=1,2,\cdots,M\times N,z_j\in(-1,1)\}$。按照逐列填充的方式，便可构成以下的混沌测量矩阵：

$$\boldsymbol{\Phi}=\frac{1}{\sqrt{M\sigma^2}}\begin{pmatrix} z_1 & z_{M+1} & \cdots & z_{M(N-1)+1} \\ z_2 & z_{M+2} & \cdots & z_{M(N-1)+2} \\ \vdots & \vdots & \ddots & \vdots \\ z_M & z_{2M} & \cdots & z_{MN} \end{pmatrix} \tag{7}$$

其中，σ^2表示混沌序列$Z(c_0)$的方差。由混沌理论可知，混沌系统对种子值c_0十分敏感，一旦c_0发生轻微变化，生成的$\boldsymbol{\Phi}$将大相径庭。因此，将输入混沌系统的种子值c_0作为SCS的密钥，便可避免频繁更新测量矩阵带来的沉重通信负担。值得注意的是，因为传感矩阵$\boldsymbol{A}$必须满足RIP条件，所以并非所有的混沌系统均适合用来构造测量矩阵。

在这里，介绍两种常用的混沌系统，即Logistic映射[23]和Tent映射[24]，它们均已被证明大概率地使传感矩阵满足RIP条件。Logistic映射可表示为：

$$c_{i+1}=\mu c_i(c_i-1),\quad 0<c_i<1,\quad i=0,1,2,\cdots \tag{8}$$

其中，(μ,c_0)是初始输入值。当$\mu\in(3.569\ 945\ 6,4]$时，Logistic映射进入混沌状态。但当

$\mu=4$时，Logistic映射被称为满映射，生成的混沌序列具有最好的伪随机特性。然而，由Logistic映射产生的混沌序列并不满足均匀分布。为了得到更好的随机特性来抵抗统计分析，需要对产生的混沌序列进行额外的非线性变换。对此，采用Tent映射可以产生近似均匀分布的混沌序列。Tent映射可表示为：

$$c(i+1)=\begin{cases}\dfrac{c(i)}{\mu}, & 0<c(i)<\mu\\ \dfrac{1-c(i)}{1-\mu}, & \mu<c(i)<1\end{cases} \quad (9)$$

其中，初始输入值 $\mu,c_0\in(0,1)$ 。

SCS技术的核心是在无法获知$\boldsymbol{\Phi}$的情况下，恢复$\boldsymbol{x}$是不可实现的。因此，如何保障$\boldsymbol{\Phi}$的安全是最关键的任务。在安全威胁小的情况下，可以采取定期改变混沌系统的初始输入值的方案，以节约采样时间。在安全威胁大的情况下，便需要采取一次一密的加密模式。

3.2 隐私保护的大数据采集方案

大数据的发展主要受到物联网和云计算技术的驱动。物联网致力于将自然万物相互关联，构建一个广泛、有序和智能的网络环境，其依靠各种感知设备获取联网物体的信息，以数据的形式完成信息交互。面对物联网的不断扩张，时刻喷涌而出的海量数据逐步向云端迁移。据IDC预测，到2025年，49%的全球已存储数据将驻留在公共云中。在云中心，数据可以被实时地处理和分析，并且将得到的结果及时反馈给终端用户。同时，通过集中化的数据管理机制，海量数据背后隐藏的巨大价值将被进一步挖掘，并服务于人类社会的生活、生产。

数据是一种特殊的资产，个人隐私数据尤其容易招致恶意攻击。目前，物联网感知设备日益轻量化，资源受限问题也越来越突出。在大量的物联网应用中，无线传感器网络（wireless sensor network，WSN）是最底层的信息感知方式。对于单个传感器节点来说，可利用的资源十分有限，高复杂度的非对称密码系统常常不适合嵌入其中。SCS技术能在近乎不增加硬件成本的情况下，将保密性嵌入压缩采样的过程中。同时，CS充分考虑了数据的冗余性，仅需远低于传统采样理论要求的样本数量便可准确地重构原始信号，这将显著降低网络中的数据量，进而有效地减轻信息与通信系统的负担。但是本质上，CS是一个复杂度转移过程，即发送端的低功耗采样是以接收端的高复杂度重构算法为代价的。幸运的是，随着智能终端算力的不断提升和云计算技术的迅速发展，重构算法的高复杂度问题能够在云端或者终端得到有效解决。

在这里，SCS技术的普遍适用场景模型被提出，如**图4**所示。首先，置于感知设备物理层的伪随机数发生器根据输入的种子值（即SCS密钥）生成混沌序列，进而构造出混沌测量矩阵；然后，随机采样得到的测量值经过量化、编码后，数据流向相应的客户机，在这里可通过非对称加密算法进行二次强加密处理；接着，加密数据经过通信基站进入公共互联网；最后，通过公共信道传输至云数据中心进行存储和处理。当授权用户需要访问原始信息时，SCS密钥被授权给可信任的云服务提供商进行重构（解密），然后将重构结果进行反馈。当然，云数据中心也可以仅发挥大数据存储的作用，发回的测量值在算力充足的智能终端上进行重构。

值得注意的是，SCS密钥在发送端和接收端之间的安全传输需要凭借安全信道或者公钥密码技术完成，它的权限掌握在合法用户或者可信任的第三方手中，并且需要被频繁地更新。在如此的应用场景

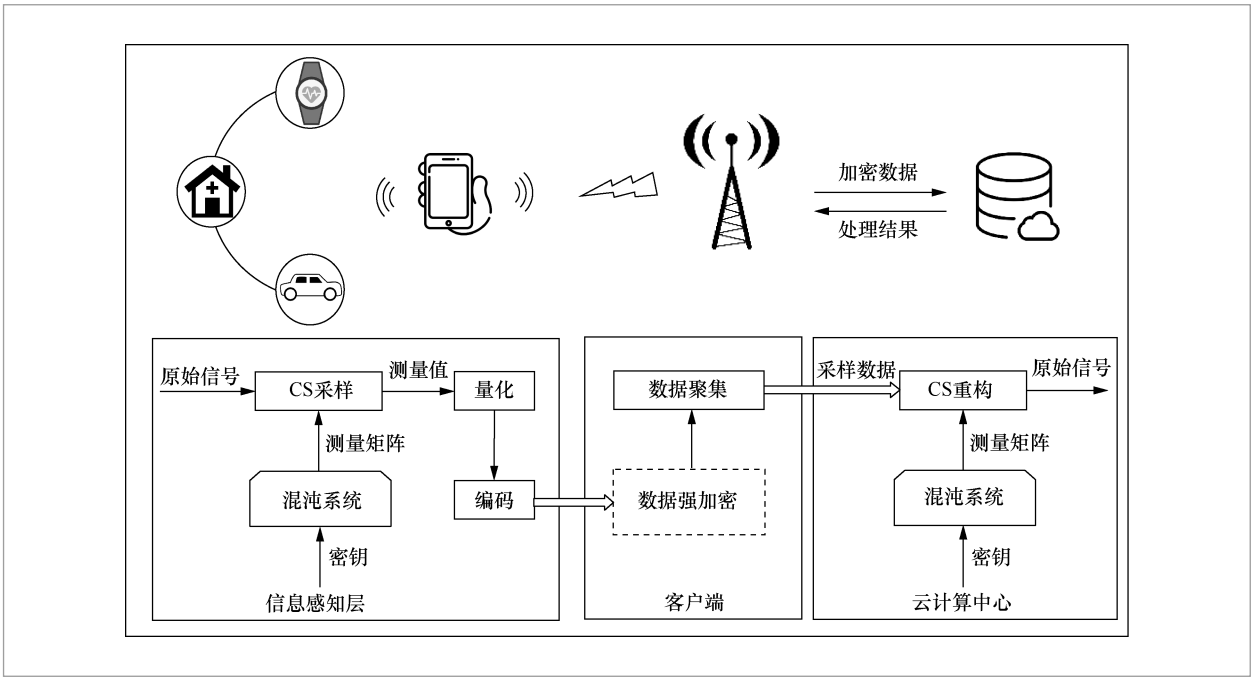

图 4 安全压缩感知技术的应用场景模型

下，通过基于混沌和CS的信息获取技术可以安全高效地采集数据，这极大地降低了物联网中感知设备和通信设备的负担。

3.3 安全性分析

从密码学的角度来看，基于SCS的信息获取系统也是一种轻量级对称密码系统。根据香农对信息理论安全的定义，绝对安全的密码系统能够保障攻击者无法从非法窃取的密文$\boldsymbol{y}$中获取任何有关于明文$\boldsymbol{x}$的信息，即满足$P(\boldsymbol{x}|\boldsymbol{y})=P(\boldsymbol{x})$。换句话说，明文$\boldsymbol{x}$和密文$\boldsymbol{y}$之间的互信息为零，即满足$I(\boldsymbol{x};\boldsymbol{y})=0$。本质上，SCS是一个线性映射过程，缺乏非线性混淆机制，明文$\boldsymbol{x}$和密文$\boldsymbol{y}$之间存在着线性相关，无法实现信息理论安全[8]。但是，当采用高斯随机测量矩阵时，密文$\boldsymbol{y}$仅暴露明文的能量信息$\|\boldsymbol{x}\|_2^2$，且仅密文的能量信息$\|\boldsymbol{y}\|_2^2$能泄露与明文$\boldsymbol{x}$有关的信息[14]，这种情况被称为渐进球面安全[19]。这也意味着，可以通过隐藏密文的能量来实现信息理论安全。

面对融合混沌理论的SCS应用，攻击者若想得到真实的测量矩阵$\boldsymbol{\Phi}$，进而从窃听的密文$\boldsymbol{y}$中非法重构出明文，将必须面临着破解混沌密码系统或者随机猜测的困难。SCS应用在计算上的安全强度主要取决于密钥空间大小，即攻击者能否在有效时间内调用所有可支配的计算资源成功遍历完整个密钥空间，这种暴力攻击的方式对混沌密码系统来说一般是徒劳无功的。尽管SCS缺乏非线性混淆机制，但若采用一次一密的加密模式，攻击者依然无法通过已知信息或选择明文的攻击手段从可利用的明密文对中获取任何有价值的消息[25]。

4 实验结果和分析

本节通过仿真实验简要地验证了融

合混沌理论的SCS技术的可行性和安全性。本文选择512×512像素的标准Lena图作为测试对象，选择Tent映射和Logistic映射构建混沌测量矩阵，并且利用二维离散小波变换（2DWT）进行信号稀疏表示。此外，所有的实验均采用OMP算法重构信号，通过峰值信噪比（peak signal-to-noise ratio，PSNR）衡量重构信号质量。需要说明的是，所有的仿真实验都在MATLAB R2015b软件中执行，并且以上实验条件的设定与SCS技术的可行性无关。

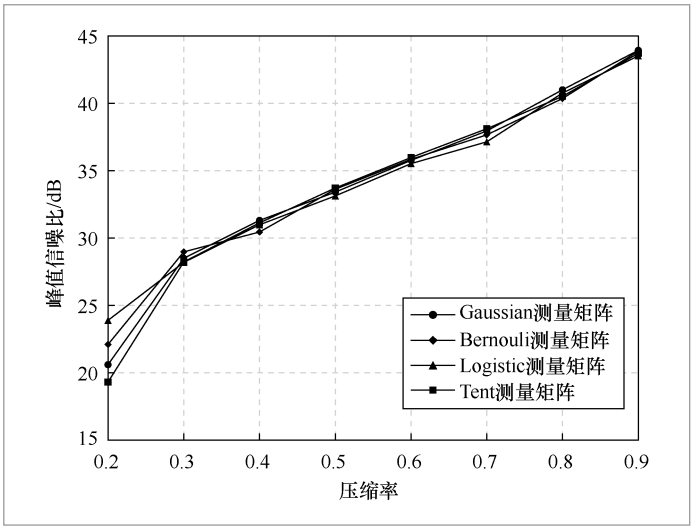

图 5 不同测量矩阵的重构效果对比

4.1 可行性

为了验证混沌测量矩阵能够发挥与传统随机测量矩阵相似的效果，本文利用Logistic映射和Tent映射构建混沌测量矩阵，并且将它们与Gaussian测量矩阵、Bernoulli测量矩阵进行实验对比。在本实验中，Logistic映射和Tent映射的初始输入值(μ,c_0)分别为(0.35, 0.65)和(4, 0.65)，为了保证较好的伪随机特性，输出序列的前1 200位被摒弃，并且按照15位的等间距抽样获得最终的混沌序列。

由**图5**可知，在不同的压缩率下，由Logistic映射、Tent映射生成的混沌测量矩阵与Gaussian测量矩阵、Bernoulli测量矩阵达到几乎相同的重构效果。这意味着，混沌测量矩阵也适用于CS技术，这样不仅可以避免传输大尺寸的测量矩阵，而且可以通过混沌系统将一定水平的保密性嵌入压缩采样的过程中。

4.2 安全性

由前文的安全性理论分析可知，SCS技术无法提供绝对的安全保障，但是其能以一种近乎零成本的方式将额外的保护层嵌入感知设备中。在这里，本文将进一步通过仿真实验展现面对暴力攻击时融合混沌系统的SCS技术的安全性能。在本实验中，压缩率被固定为0.5，采用Tent映射构建混沌测量矩阵。同样先摒弃输出序列的前1 200位，然后按照15位的等间距抽样获得最终的混沌序列。假定采用的密钥是(μ,c_0) =(0.45, 0.55)，攻击者猜想的虚假密钥包括$(\mu+\Delta,c_0)$、$(\mu,c_0+\Delta)$和$(\mu+\Delta/2,c_0+\Delta/2)$，其中$\Delta=10^{-16}$是真实密钥和猜测密钥之间的偏差。

图6是原始图像和重构图像质量的对比。从**图6**可知，利用SCS技术加密得到的密文（即测量值，如**图6（b）**所示）在视觉上无法泄露任何有意义的信息。此外，尽管攻击者猜测的密钥与真实的密钥如此接近，但是依然无法通过它从窃听到的密文中解密出明文。

5 结束语

在万物互联的时代，物联网中时刻生成着大量与个人隐私有关的数据，这些数据在互联网上流动以及汇向云端的过程

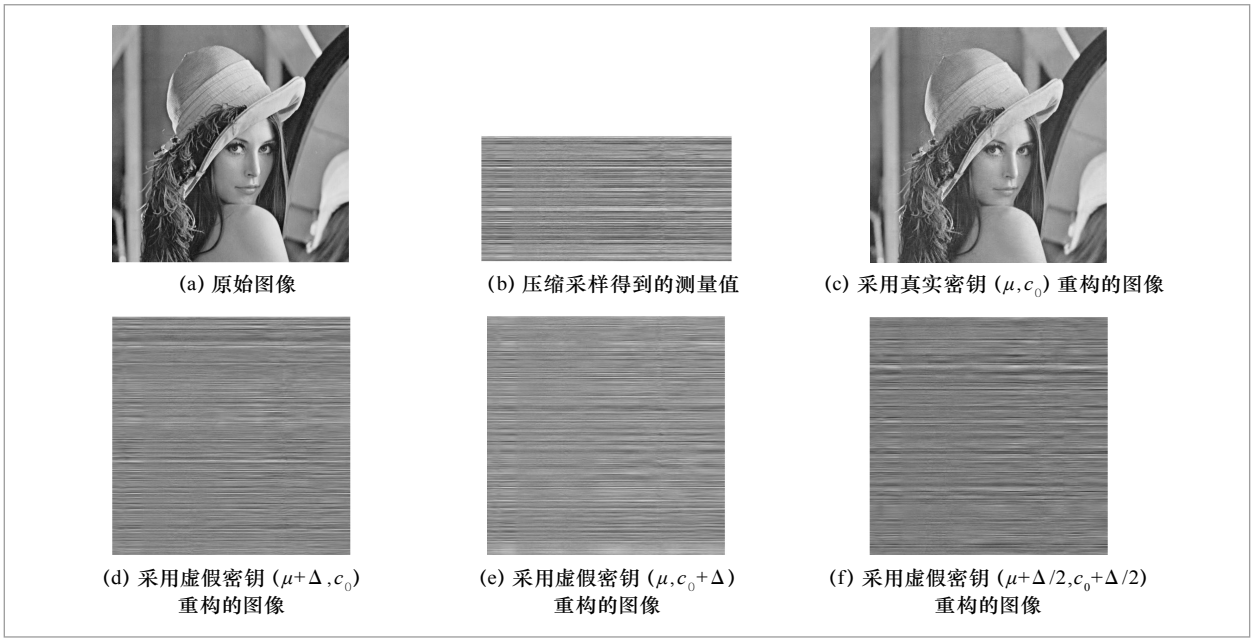

图 6 原始图像和重构图像质量对比

中容易受到恶意攻击。特别在一些资源受限的物联网场景下，底层信息感知设备不支持嵌入高能耗的传统密码系统，数据安全问题尤为突出。针对这种问题，本文融合混沌理论和CS理论提出了新兴的SCS技术。尽管SCS技术无法实现信息理论安全，但其能在近乎不增加任何硬件成本的情况下同步完成采样、压缩和加密3种操作。紧接着，本文给出了SCS技术普遍使用的物联网场景模型，并通过仿真实验阐述了该技术的可行性和安全性。由于SCS技术具备低能耗采样和轻量加密特性，笔者呼吁将其作为一种低成本的、内置保密性的信息获取技术，在资源受限的物联网场景下为采样数据提供第一层安全防护。

参考文献:

[1] CANDÈS E J, ROMBERG J, TAO T. Robust uncertainty principles: exact signal reconstruction from highly incomplete frequency information[J]. IEEE Transactions on Information Theory, 2006, 52(2): 489-509.

[2] DONOHO D L. Compressed sensing[J]. IEEE Transactions on Information Theory, 2006, 52(4): 1289-1306.

[3] 戴琼海, 付长军, 季向阳. 压缩感知研究[J]. 计算机学报, 2011, 34(3): 425-434.
DAI Q H, FU C J, JI X Y. Research on compressed sensing[J]. Chinese Journal of Computers, 2011, 34(3): 425-434.

[4] LI S, XU L D, WANG X. Compressed sensing signal and data acquisition in wireless sensor networks and internet of things[J]. IEEE Transactions on Industrial Informatics, 2013, 9(4): 2177-2186.

[5] FRAGKIADAKIS A, CHARALAMPIDIS P, TRAGOS E. Adaptive compressive sensing for energy efficient smart objects in IoT applications[C]// The 4th International Conference on Wireless Communications, Vehicular Technology, Information Theory and Aerospace & Electronic Systems (VITAE), May 11-14, 2014, Aalborg, Denmark. Piscataway: IEEE Press, 2014: 1-5.

[6] 肖玲, 李仁发, 罗娟. 体域网中一种基于压缩感知的人体动作识别方法[J]. 电子与信息学报, 2013, 35(1): 119-225.
XIAO L, LI R F, LUO J. Recognition of human activity based on compressed sensing in body sensor networks[J]. Journal of Electronics & Information Technology, 2013, 35(1): 119-225.

[7] MAMAGHANIAN H, KHALED N, ATIENZA D, et al. Compressed sensing for real-time energy-efficient ECG compression on wireless body sensor nodes[J]. IEEE Transactions on Biomedical Engineering, 2011, 58(9): 2456-2466.

[8] HUANG R, RHEE K H, UCHIDA S. A parallel image encryption method based on compressive sensing[J]. Multimedia Tools and Applications, 2014, 72(1): 71-93.

[9] CHAI X, GAN Z, CHEN Y, et al. A visually secure image encryption scheme based on compressive sensing[J]. Signal Processing, 2016, 134:35-51.

[10] RACHLIN Y, BARONB D. The secrecy of compressed sensing measurements[C]// The 46th Annual Allerton Conference on Communication, Control and Computing, September 23-26, 2008, Urbana-Champaign, USA. Piscataway: IEEE Press, 2008: 813-817.

[11] HOSSEIN S A, TABATABAEI A E, ZIVIC N. Security analysis of the joint encryption and compressed sensing[C]// The 20th Telecommunications Forum, November 20-22, 2012, Belgrade, Serbia. Piscataway: IEEE Press, 2012: 799-802.

[12] LIU X, MEI W, DU H. Simultaneous image compression, fusion and encryption algorithm based on compressive sensing and chaos[J]. Optics Communications, 2016, 366: 22-32.

[13] ZHOU N, PAN S, CHENG S, et al. Image compression-encryption scheme based on hyper-chaotic system and 2D compressive sensing[J]. Optics & Laser Technology, 2016, 82: 121-133.

[14] BIANCHI T, BIOGLIO V, MAGLI E. On the security of random linear measurements[C]// 2014 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), May 4-9, 2014, Florence, Italy. Piscataway: IEEE Press, 2014: 3992-3996.

[15] CAMBARERI V, MANGIAM M, PARESCHI F, et al. Low-complexity multiclass encryption by compressed sensing[J]. IEEE Transactions on Signal Processing, 2015, 63(9): 2183-2195.

[16] MALLAT S G, ZHANG Z. Matching pursuits with time-frequency dictionaries[J]. IEEE Transactions on Signal Processing, 1993, 41(12): 3397-3415.

[17] TTROPP J A, GILBERT A C. Signal recovery from random measurements via orthogonal matching pursuit[J]. IEEE Transactions on Information Theory, 2007, 53(12): 4655-4666.

[18] CHEN S, DONOHO D L, SAUNDERS M A. Atomic decomposition by basis pursuit[J]. SIAM Review, 2001, 43(1): 129-159.

[19] CANDÈS E J, TAO T. Decoding by linear programming[J]. IEEE Transactions on Information Theory, 2005, 51(12): 4203-4215.

[20] CANDÈS E J, EMMANUEL J. The restricted isometry property and its implications for compressed sensing[J]. Comptes Rendus Mathematique, 2008, 346(9): 589-592.

[21] BARANIUK R, DAVENPORT M, DEVORED R, et al. A simple proof of the restricted isometry property for random matrices[J]. Constructive Approximation, 2008, 28 (3): 253-263.

[22] CANDÈS E J, TAO T. Near-optimal signal recovery from random projections: universal encoding strategies?[J]. IEEE Transactions on Information Theory, 2006, 52(12): 5406-5425.

[23] LEI Y, BARBOT J P, GANG Z, et al. Compressive sensing with chaotic sequence[J]. IEEE Signal Processing Letters, 2010, 17(8): 731-734.

[24] FRUNZETE M, LEI Y, BARBOT J P, et al.

Compressive sensing matrix designed by tent map, for secure data transmission[C]// Signal Processing Algorithms, Architectures, Arrangements, and Applications, September 29-30, 2011, Poznan, Poland. Piscataway: IEEE Press, 2011: 1-6.

[25] CAMBARERI V, MANGIA M, PARESCHIP F, et al. On known-plaintext attacks to a compressed sensing-based encryption: a quantitative analysis[J]. IEEE Transactions on Information Forensics and Security, 2015, 10(10): 2182-2195.

作者简介

王平(1993-),男,西南大学电子信息工程学院硕士生,主要研究方向为多媒体安全。

张玉书(1987-),男,博士,南京航空航天大学计算机科学与技术学院教授,主要研究方向为多媒体安全、物联网与云计算安全。

何兴(1986-),男,博士,西南大学电子信息工程学院教授,主要研究方向为计算智能。

仲盛(1974-),男,博士,南京大学计算机科学与技术系教授,主要研究方向为密码学、博弈论及其在计算机网络、分布式系统中的应用。

收稿日期: 2019-08-24

基金项目: 国家重点研发计划基金资助项目(No. 2017YFB0802300);广西可信软件重点实验室研究课题基金资助项目(No. kx201904)

Foundation Items: The National Key Research and Development Program of China(No. 2017YFB0802300), Guangxi Trusted Software Key Laboratory Research Project(No. kx201904)