(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 115412903 B
(45)授权公告日 2024.10.15

(21)申请号 202211047117.6

(22)申请日 2022.08.30

(65)同一申请的已公布的文献号
申请公布号 CN 115412903 A

(43)申请公布日 2022.11.29

(73)专利权人 广东工业大学
地址 510060 广东省广州市越秀区东风东路729号大院
专利权人 人工智能与数字经济广东省实验室(广州)

(72)发明人 张军 周家鑫 张枝

(74)专利代理机构 北京集佳知识产权代理有限公司 11227
专利代理师 刘晓娟

(51)Int.Cl.
H04W 12/00(2021.01)
H04W 12/033(2021.01)
H04W 12/04(2021.01)
H04W 12/122(2021.01)
H04L 9/06(2006.01)
H04L 9/08(2006.01)
H04L 9/40(2022.01)

(56)对比文件
CN 105811993 A,2016.07.27
CN 111404639 A,2020.07.10

审查员 刘莹莹

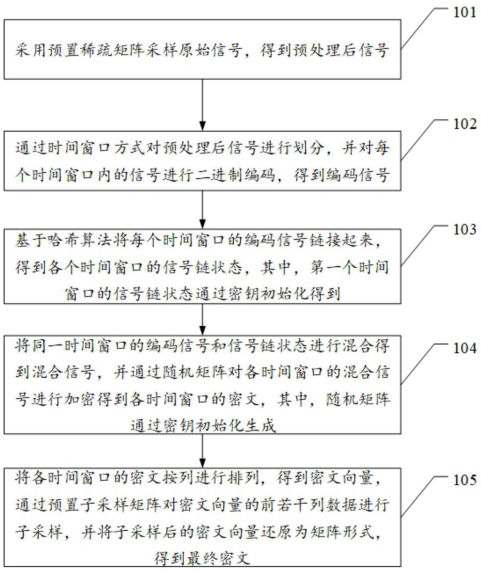
权利要求书3页 说明书10页 附图6页

(54)发明名称

一种链式压缩感知数据流编码方法、解码方法及装置

(57)摘要

本申请公开了一种链式压缩感知数据流编码方法、解码方法及装置,采用预置稀疏矩阵采样原始信号得到预处理后信号;对预处理后信号进行划分,并对划分后的信号进行二进制编码得到编码信号;基于哈希算法将各时间窗口的编码信号链接起来,得到各时间窗口的信号链状态;将同一时间窗口的编码信号和信号链状态进行混合,并通过随机矩阵加密混合信号得到各时间窗口的密文,第一个时间窗口的信号链状态和随机矩阵通过密钥初始化得到;将各时间窗口的密文按列进行排列得到密文向量,通过预置子采样矩阵对密文向量进行子采样并还原为矩阵,得到最终密文,提高了数据传输的安全性,减少了数据传输量,从而降低了系统的能耗,并增强了系统的重构性能。



CN 115412903 B

1.一种链式压缩感知数据流编码方法,其特征在于,包括:

采用预置稀疏矩阵采样原始信号,得到预处理后信号;

通过时间窗口方式对所述预处理后信号进行划分,并对每个时间窗口内的信号进行二进制编码,得到编码信号;

基于哈希算法将每个时间窗口的编码信号链接起来,得到各个时间窗口的信号链状态,其中,第一个时间窗口的信号链状态通过密钥初始化得到;

将同一时间窗口的编码信号和信号链状态进行混合得到混合信号,并通过随机矩阵对各时间窗口的所述混合信号进行加密得到各时间窗口的密文,其中,所述随机矩阵通过所述密钥初始化生成;

将各时间窗口的所述密文按列进行排列,得到密文向量,通过预置子采样矩阵对所述密文向量的前若干列数据进行子采样,并将子采样后的密文向量还原为矩阵形式,得到最终密文。

2.根据权利要求1所述的链式压缩感知数据流编码方法,其特征在于,所述预处理后信号为:

x=A×l;

式中,x为预处理后信号,$A \in \{-1,0,1\}^{N\times N}$为预置稀疏矩阵,l为原始信号。

3.根据权利要求1所述的链式压缩感知数据流编码方法,其特征在于,所述通过时间窗口方式对所述预处理后信号进行划分,并对每个时间窗口内的信号进行二进制编码,得到编码信号,包括:

采用t个时间窗口对所述预处理后信号进行划分,得到t个时间窗口的信号,每个时间窗口的信号为n维;

设置信号的比特数B_x,通过B_x位对每个时间窗口的信号进行二进制编码,得到编码信号X_i,其中,$X_i \in Z(B_x)^n$,$Z(B_x)=\{-2^{Bx}-1,\ldots,0,\ldots,2^{Bx}-1\}$。

4.根据权利要求3所述的链式压缩感知数据流编码方法,其特征在于,所述基于哈希算法将每个时间窗口的编码信号链接起来,得到各个时间窗口的信号链状态,包括:

设置i=1,通过密钥初始化得到第i个时间窗口的信号链状态;

对第i个时间窗口的信号链状态和第i个时间窗口的编码信号进行哈希运算,得到第i+1个时间窗口的信号链状态;

设置i=i+1,返回所述对第i个时间窗口的信号链状态和第i个时间窗口的编码信号进行哈希运算,得到第i+1个时间窗口的信号链状态的步骤,直至i=t,得到各个时间窗口的信号链状态。

5.根据权利要求4所述的链式压缩感知数据流编码方法,其特征在于,哈希运算过程为:

$$C_{i+1}=H(C_i+X_i)=(\xi\times(C_i+X_i)+\eta)\bmod 2^{B_C};$$

式中,C_{i+1}为第i+1个时间窗口的信号链状态,H( )为哈希函数,C_i为第i个时间窗口的信号链状态,X_i为第i个时间窗口的编码信号,$\xi=2^{B_C}-1$、$\eta=1$均为中间参数,B_C为信号链状态的比特数,mod为取模运算。

6.根据权利要求1所述的链式压缩感知数据流编码方法,其特征在于,所述密文的加密过程为:

$$Z_i = \Phi^{(i)} Q_i ;$$

式中,Z_i为第i个时间窗口的密文,$\Phi^{(i)} \in \{-1,1\}^{m \times n}$为第i个时间窗口的随机矩阵,n为每个时间窗口的信号的长度,Q_i为第i个时间窗口的混合矩阵,$Q_i=X_i+C_i$,C_i为第i个时间窗口的信号链状态,X_i为第i个时间窗口的编码信号。

7.一种链式压缩感知数据流解码方法,其特征在于,包括:

S1、通过第一个时刻的信号链状态对接收到第一个时刻的密文进行解码,得到第一时刻的子采样后的预处理后信号,其中,第一个时刻的信号链状态通过密钥初始化得到;

S2、根据第一个时刻的信号链状态和子采样后的预处理后信号获取下一时刻的信号链状态,并通过下一时刻的信号链状态对接收到下一时刻的密文进行解码,得到下一时刻的子采样后的预处理后信号;

S3、将下一时刻的预处理后信号和信号链状态作为第一个时刻的预处理后信号和信号链状态,并返回步骤S2,逐步得到各个时刻的子采样后的预处理后信号;

S4、通过预置子采样矩阵和预置稀疏矩阵生成结构随机矩阵,将所述结构随机矩阵作为测量矩阵,并通过压缩感知重构方法根据所述测量矩阵和各个时刻的子采样后的预处理后信号进行信号重构,得到原始信号。

8.根据权利要求7所述的链式压缩感知数据流解码方法,其特征在于,所述通过预置子采样矩阵和预置稀疏矩阵生成结构随机矩阵,包括:

将预置子采样矩阵和预置稀疏矩阵进行相乘,得到结构随机矩阵。

9.一种链式压缩感知数据流编码装置,其特征在于,包括:

预处理单元,用于采用预置稀疏矩阵采样原始信号,得到预处理后信号;

编码单元,用于通过时间窗口方式对所述预处理后信号进行划分,并对每个时间窗口内的信号进行二进制编码,得到编码信号;

加链单元,用于基于哈希算法将每个时间窗口的编码信号链接起来,得到各个时间窗口的信号链状态,其中,第一个时间窗口的信号链状态通过密钥初始化得到;

加密单元,用于将同一时间窗口的编码信号和信号链状态进行混合得到混合信号,并通过随机矩阵对各时间窗口的所述混合信号进行加密得到各时间窗口的密文,其中,所述随机矩阵通过所述密钥初始化生成;

子采样单元,用于将各时间窗口的所述密文按列进行排列,得到密文向量,通过预置子采样矩阵对所述密文向量的前若干列数据进行子采样,并将子采样后的密文向量还原为矩阵形式,得到最终密文。

10.一种链式压缩感知数据流解码装置,其特征在于,包括:

解码单元,用于通过第一个时刻的信号链状态对接收到第一个时刻的密文进行解码,得到第一时刻的子采样后的预处理后信号,其中,第一个时刻的信号链状态通过密钥初始化得到;

获取单元,用于根据第一个时刻的信号链状态和子采样后的预处理后信号获取下一时刻的信号链状态,并通过下一时刻的信号链状态对接收到下一时刻的密文进行解码,得到

下一时刻的子采样后的预处理后信号；

触发单元，用于将下一时刻的预处理后信号和信号链状态作为第一个时刻的预处理后信号和信号链状态，并触发所述获取单元，逐步得到各个时刻的子采样后的预处理后信号；

重构单元，用于通过预置子采样矩阵和预置稀疏矩阵生成结构随机矩阵，将所述结构随机矩阵作为测量矩阵，并通过压缩感知重构方法根据所述测量矩阵和各个时刻的子采样后的预处理后信号进行信号重构，得到原始信号。

一种链式压缩感知数据流编码方法、解码方法及装置

技术领域

[0001] 本申请涉及数据安全技术领域,尤其涉及一种链式压缩感知数据流编码方法、解码方法及装置。

背景技术

[0002] 随着人口老龄化的增加,人们易患各种慢性病,包括心血管疾病,这通常需要持续的心脏监测。由于医疗负担不断增加,以医院为中心的医疗保健系统已无法满足这种情况。近年来,基于无线体域网(WBANs)的以家庭为中心的监护模式在学术界和工业界都得到了广泛关注。该技术通过传感器节点对各种生理信号采样并传输到远程医疗系统,使医生能够实时监测患者的身体状况,及时提供专业的医疗指导。

[0003] 而这项技术的主要挑战之一是能量消耗。因为需要持续监测患者的生命体征,这个过程将产生大量数据,并在传输过程中消耗大量能量。同时,为了满足WBANs舒适性和易实现的要求,传感器设备需要由电池供电并且尽可能小。然而,电池中约60%的能量被负责数据传输的无线传感器节点消耗,需要不断对电池进行充电。显然,网络的生命周期由WBANs中传感器节点的能量消耗决定。另一方面,传感器数据包含了敏感的生物医学信息,例如心率,这些信息可能会在传输过程中泄露甚至修改。因此,确保医疗数据的安全性是另一个挑战。

发明内容

[0004] 本申请提供了一种链式压缩感知数据流编码方法、解码方法及装置,用于提高数据传输的安全性,以及减少数据传输量,降低系统的能耗,并增强系统的重构性能。

[0005] 有鉴于此,本申请第一方面提供了一种链式压缩感知数据流编码方法,包括:

[0006] 采用预置稀疏矩阵采样原始信号,得到预处理后信号;

[0007] 通过时间窗口方式对所述预处理后信号进行划分,并对每个时间窗口内的信号进行二进制编码,得到编码信号;

[0008] 基于哈希算法将每个时间窗口的编码信号链接起来,得到各个时间窗口的信号链状态,其中,第一个时间窗口的信号链状态通过密钥初始化得到;

[0009] 将同一时间窗口的编码信号和信号链状态进行混合得到混合信号,并通过随机矩阵对各时间窗口的所述混合信号进行加密得到各时间窗口的密文,其中,所述随机矩阵通过所述密钥初始化生成;

[0010] 将各时间窗口的所述密文按列进行排列,得到密文向量,通过预置子采样矩阵对所述密文向量的前若干列数据进行子采样,并将子采样后的密文向量还原为矩阵形式,得到最终密文。

[0011] 可选的,所述预处理后信号为:

[0012] $x=A\times l$;

[0013] 式中,x为预处理后信号,$A\in\{-1,0,1\}^{N\times N}$为预置稀疏矩阵,l为原始信号。

[0014] 可选的,所述通过滑动时间窗口方式对所述预处理后信号进行处理,并对每个时间窗口内的信号进行二进制编码,得到编码信号,包括:

[0015] 采用t个时间窗口对所述预处理后信号进行划分,得到t个时间窗口的信号,每个时间窗口的信号为n维;

[0016] 设置信号的比特数B_x,通过B_x位对每个时间窗口的信号进行二进制编码,得到编码信号X_i,其中,$X_i \in Z(B_x)^n$,$Z(B_x)=\{-2^{Bx}-1,\ldots,0,\ldots,2^{Bx}-1\}$。

[0017] 可选的,所述基于哈希算法将每个时间窗口的编码信号链接起来,得到各个时间窗口的信号链状态,包括:

[0018] 设置i=1,通过密钥初始化得到第i个时间窗口的信号链状态;

[0019] 对第i个时间窗口的信号链状态和第i个时间窗口的编码信号进行哈希运算,得到第i+1个时间窗口的信号链状态;

[0020] 设置i=i+1,返回所述对第i个时间窗口的信号链状态和第i个时间窗口的编码信号进行哈希运算,得到第i+1个时间窗口的信号链状态的步骤,直至i=t,得到各个时间窗口的信号链状态。

[0021] 可选的,哈希运算过程为:

[0022] $$C_{i+1}=H(C_i+X_i)=(\xi\times(C_i+X_i)+\eta)\bmod 2^{B_C};$$

[0023] 式中,C_{i+1}为第i+1个时间窗口的信号链状态,H()为哈希函数,C_i为第i个时间窗口的信号链状态,X_i为第i个时间窗口的编码信号,$\xi=2^{B_C}-1$、η=1均为中间参数,B_C为链状态的比特数,mod为取模运算。

[0024] 可选的,所述密文的加密过程为:

[0025] $Z_i=\Phi^{(i)}Q_i$;

[0026] 式中,Z_i为第i个时间窗口的密文,$\Phi^{(i)}\in\{-1,1\}^{n\times n}$为第i个时间窗口的随机矩阵,n为每个时间窗口的信号的长度,Q_i为第i个时间窗口的混合矩阵,$Q_i=X_i+C_i$,C_i为第i个时间窗口的信号链状态,X_i为第i个时间窗口的编码信号。

[0027] 本申请第二方面提供了一种链式压缩感知数据流解码方法,包括:

[0028] S1、通过第一个时刻的信号链状态对接收到第一个时刻的密文进行解码,得到第一时刻的子采样后的预处理后信号,其中,第一个时刻的信号链状态通过密钥初始化得到;

[0029] S2、根据第一个时刻的信号链状态和子采样后的预处理后信号获取下一时刻的信号链状态,并通过下一时刻的信号链状态对接收到下一时刻的密文进行解码,得到下一时刻的子采样后的预处理后信号;

[0030] S3、将下一时刻的预处理后信号和信号链状态作为第一个时刻的预处理后信号和信号链状态,并返回步骤S2,逐步得到各个时刻的子采样后的预处理后信号;

[0031] S4、通过预置子采样矩阵和预置稀疏矩阵生成结构随机矩阵,将所述结构随机矩阵作为测量矩阵,并通过压缩感知重构方法根据所述测量矩阵和各个时刻的子采样后的预处理后信号进行信号重构,得到原始信号。

[0032] 可选的,所述通过预置子采样矩阵和预置稀疏矩阵生成结构随机矩阵,包括:

[0033] 将预置子采样矩阵和预置稀疏矩阵进行相乘,得到结构随机矩阵。

[0034] 本申请第三方面提供了一种链式压缩感知数据流编码装置,包括:

[0035] 预处理单元,用于采用预置稀疏矩阵采样原始信号,得到预处理后信号;

[0036] 编码单元,用于通过时间窗口方式对所述预处理后信号进行划分,并对每个时间窗口内的信号进行二进制编码,得到编码信号;

[0037] 加链单元,用于基于哈希算法将每个时间窗口的编码信号链接起来,得到各个时间窗口的信号链状态,其中,第一个时间窗口的信号链状态通过密钥初始化得到;

[0038] 加密单元,用于将同一时间窗口的编码信号和信号链状态进行混合得到混合信号,并通过随机矩阵对各时间窗口的所述混合信号进行加密得到各时间窗口的密文,其中,所述随机矩阵通过所述密钥初始化生成;

[0039] 子采样单元,用于将各时间窗口的所述密文按列进行排列,得到密文向量,通过预置子采样矩阵对所述密文向量的前若干列数据进行子采样,并将子采样后的密文向量还原为矩阵形式,得到最终密文。

[0040] 本申请第四方面提供了一种链式压缩感知数据流解码装置,包括:

[0041] 解码单元,用于通过第一个时刻的信号链状态对接收到第一个时刻的密文进行解码,得到第一时刻的子采样后的预处理后信号,其中,第一个时刻的信号链状态通过密钥初始化得到;

[0042] 获取单元,用于根据第一个时刻的信号链状态和子采样后的预处理后信号获取下一时刻的信号链状态,并通过下一时刻的信号链状态对接收到下一时刻的密文进行解码,得到下一时刻的子采样后的预处理后信号;

[0043] 触发单元,用于将下一时刻的预处理后信号和信号链状态作为第一个时刻的预处理后信号和信号链状态,并触发所述获取单元,逐步得到各个时刻的子采样后的预处理后信号;

[0044] 重构单元,用于通过预置子采样矩阵和预置稀疏矩阵生成结构随机矩阵,将所述结构随机矩阵作为测量矩阵,并通过压缩感知重构方法根据所述测量矩阵和各个时刻的子采样后的预处理后信号进行信号重构,得到原始信号。

[0045] 从以上技术方案可以看出,本申请具有以下优点:

[0046] 本申请提供了一种链式压缩感知数据流编码方法,包括:采用预置稀疏矩阵采样原始信号,得到预处理后信号;通过时间窗口方式对预处理后信号进行划分,并对每个时间窗口内的信号进行二进制编码,得到编码信号;基于哈希算法将每个时间窗口的编码信号链接起来,得到各个时间窗口的信号链状态,其中,第一个时间窗口的信号链状态通过密钥初始化得到;将同一时间窗口的编码信号和信号链状态进行混合得到混合信号,并通过随机矩阵对各时间窗口的混合信号进行加密得到各时间窗口的密文,其中,随机矩阵通过密钥初始化生成;将各时间窗口的密文按列进行排列,得到密文向量,通过预置子采样矩阵对密文向量的前若干列数据进行子采样,并将子采样后的密文向量还原为矩阵形式,得到最终密文。

[0047] 本申请中,在信号预处理过程中,采用超低复杂度的预置稀疏矩阵采样原始信号,通过少量的加法操作增加测量信息冗余,从而提高了信号重构能力,通过时间窗口方式对预处理后信号进行划分,从而对预处理后信号进行分组编码,并引入链式技术将各个时间窗口的信号链接起来,并将同一时间窗口的编码信号与信号链状态进行混合,利用链式的特性屏蔽信号的能量特征,以提高对唯密文攻击、已知明文攻击的抵抗能力,并赋予对中间

人攻击的鲁棒性;进一步采用随机矩阵对混合信号进行加密得到密文,对密文的前部分进行子采样。本申请通过加链隐藏明文的能量信息,提高数据传输的安全性;通过子采样过程减少数据传输量,不仅降低系统的能耗,而且该方法等价于结合预置子采样矩阵和预置稀疏矩阵设计一个结构随机矩阵作为测量矩阵,其感知性能远好于在经典的压缩感知模型中将非结构随机矩阵作为测量矩阵的感知性能,相比于CCS,本申请可以大幅度提高系统的重构性能。

附图说明

[0048] 为了更清楚地说明本申请实施例或现有技术中的技术方案,下面将对实施例或现有技术描述中所需要使用的附图作简单地介绍,显而易见地,下面描述中的附图仅仅是本申请的一些实施例,对于本领域普通技术人员来讲,在不付出创造性劳动性的前提下,还可以根据这些附图获得其它的附图。

[0049] 图1为本申请实施例提供的一种链式压缩感知数据流编码方法的一个流程示意图;

[0050] 图2为本申请实施例提供的一种基于压缩感知的信号处理过程示意图;

[0051] 图3为本申请实施例提供的一种链式压缩感知数据流解码方法的一个流程示意图;

[0052] 图4为本申请实施例提供的一种测量矩阵等效构造示意图;

[0053] 图5为本申请实施例提供的一种链式压缩感知数据流编解码过程的示意图;

[0054] 图6为本申请实施例提供的随机高斯矩阵的互相关性示意图;

[0055] 图7为本申请实施例提供的随机伯努利矩阵的互相关性示意图;

[0056] 图8为本申请实施例提供的结构随机矩阵的互相关性示意图;

[0057] 图9为本申请实施例提供的一种链式压缩感知数据流编码装置的一个结构示意图;

[0058] 图10为本申请实施例提供的一种链式压缩感知数据流解码装置的一个结构示意图。

具体实施方式

[0059] 为了使本技术领域的人员更好地理解本申请方案,下面将结合本申请实施例中的附图,对本申请实施例中的技术方案进行清楚、完整地描述,显然,所描述的实施例仅是本申请一部分实施例,而不是全部的实施例。基于本申请中的实施例,本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例,都属于本申请保护的范围。

[0060] 为了便于理解,请参阅图1,本申请实施例提供了一种链式压缩感知数据流编码方法,包括:

[0061] 步骤101、采用预置稀疏矩阵采样原始信号,得到预处理后信号。

[0062] 在获取到原始信号后,采用超低复杂度的预置稀疏矩阵$A\in\{-1,0,1\}^{N\times N}$采样原始信号1,得到预处理后信号$x=A\times 1$,$x\in R^{N}$,N为原始信号的长度;该预置稀疏矩阵中每行每列只有少数D个元素的绝对值为1,其余元素都为0。通过稀疏矩阵对原始信号进行采样,可以通过少量的加法操作增加测量信息冗余,从而提高重构能力。

[0063] 步骤102、通过时间窗口方式对预处理后信号进行划分，并对每个时间窗口内的信号进行二进制编码，得到编码信号。

[0064] 采用t个时间窗口对预处理后信号进行划分，得到t个时间窗口的信号；每个时间窗口的信号为n维；设置信号的比特数B_x，通过B_x位对每个时间窗口的信号进行二进制编码，得到编码信号X_i，其中，$X_i \in Z(B_x)^n$，$Z(B_x)=\{-2^{Bx}-1,\ldots,0,\ldots,2^{Bx}-1\}$。

[0065] 分组密码是一种基于固定长度比特的确定性方法，在分组密码中，一个单元称为块，它将特定长度的明文块映射为相同长度的密文块。信号波形以时间窗序列的形式获取，其中，i表示时间窗，i＝1,2,...,t，共t个时间窗口，每个时间窗口中的信号为n维；使用B_x位对每个时间窗口的信号进行编码，得到对应时间窗口的编码信号；可以定义整数集$Z(B)=\{-2^B-1,\ldots,0,\ldots,2^B-1\}$，非负整数集$N(B)=\{0,\ldots,2^B-1\}$，设置一个信号的比特数$B_x$，使用$B_x$位对信号进行二进制编码，即将信号的值对应转化为$Z(B_x)$的范围内。将各编码信号存储在矩阵$X \in R^{n\times t}$中，n×t＝N，其中，编码信号$X_i \in Z(B_x)^n$。

[0066] 步骤103、基于哈希算法将每个时间窗口的编码信号链接起来，得到各个时间窗口的信号链状态，其中，第一个时间窗口的信号链状态通过密钥初始化得到。

[0067] 预置信号链状态的比特数B_c，B_c位表示不同时间窗口的链状态的范围，通过哈希算法将每个时间窗口的信号链接起来。具体的，设置i＝1，通过密钥k_{ab}初始化得到第i个时间窗口的信号链状态，即即初始化$C_1=k_{ab}$；对第i个时间窗口的信号链状态和第i个时间窗口的编码信号进行哈希运算，得到第i+1个时间窗口的信号链状态；设置i＝i+1，返回对第i个时间窗口的信号链状态和第i个时间窗口的编码信号进行哈希运算，得到第i+1个时间窗口的信号链状态的步骤，直至i＝t，得到各个时间窗口的信号链状态。其中，哈希运算过程为：

[0068] $$C_{i+1}=H(C_i+X_i)=(\xi\times(C_i+X_i)+\eta)\bmod 2^{B_C}$$；

[0069] 式中，C_{i+1}为第i+1个时间窗口的信号链状态，H()为哈希函数，C_i为第i个时间窗口的信号链状态，X_i为第i个时间窗口的编码信号，$\xi=2^{B_C}-1$、η＝1均为中间参数，mod为取模运算。

[0070] 步骤104、将同一时间窗口的编码信号和信号链状态进行混合得到混合信号，并通过随机矩阵对各时间窗口的混合信号进行加密得到各时间窗口的密文，其中，随机矩阵通过密钥初始化生成。

[0071] 请参考图2，在压缩感知(CS)框架中，对于一个N维的K稀疏信号x，将高维信号通过测量矩阵投影到M维空间上，M<<N，即y＝Φx，$\Phi \in R^{M\times N}$为测量矩阵。整个过程将高维信号(N维)压缩成低维信号(M维)，y作为观测信号进行传输，当其到达观测端时，可以从观测信号y中恢复稀疏信号x。

[0072] 本申请实施例中，将同一时间窗口的编码信号和信号链状态进行混合配对，得到混合信号$Q_i=X_i+C_i$，通过随机矩阵Φ对混合信号进行加密得到密文Z，即$Z_i=\Phi^{(i)}Q_i$，$\Phi^{(i)} \in \{-1,1\}^{n\times n}$为第i个时间窗口的随机矩阵，随机矩阵为方阵，n为每个时间窗口的信号的长度。为了便于硬件的实现，随机矩阵由已知种子的伪随机数生成器生成的随机数，使用密钥k_{ab}作为伪随机数生成器的种子。

[0073] 在CCS(一种链式CS方案)中，采用非方阵的测量矩阵$\Phi \in \{-1,1\}^{m\times n}$对混合信号进行部分采样，从而实现对信号进行压缩，减少数据传输量，降低系统能耗，但这样会存在累

计误差,每通过压缩感知重构一次信号就会产生一次误差,并且会带入到下一次重构过程从而累计误差。为了改善该问题,本申请实施例中采用方阵的随机矩阵对混合信号进行全采样(即加密),这样可以避免在重构的过程中产生误差,从而实现消除累计误差。

[0074] 步骤105、将各时间窗口的密文按列进行排列,得到密文向量,通过预置子采样矩阵对密文向量的前若干列数据进行子采样,并将子采样后的密文向量还原为矩阵形式,得到最终密文。

[0075] 为了减少数据传输量,降低传输成本,本申请实施例将各时间窗口的密文Z按列进行排列,得到密文向量z,通过预置子采样矩阵$D_{M\times N}$对密文向量z的前若干列数据进行子采样,将子采样后的密文向量还原为矩阵形式,得到最终密文$\tilde{z}$,即子采样后的密文向量为z′=D×z,将子采样后的密文向量还原为矩阵形式,得到最终密文$\tilde{z}$,$\tilde{z}\in R^{n\times s}$,s表示子采样之后的列数,n×s=M。该方法等价于结合一个预置子采样矩阵和预置稀疏矩阵设计一个结构随机矩阵作为测量矩阵,其感知性能远好于在经典的压缩感知模型中,非结构随机矩阵作为测量矩阵的感知性能,相比于CCS,本申请可以大幅度提高系统的重构性能。

[0076] 本申请实施例中,在信号预处理过程中,采用超低复杂度的预置稀疏矩阵采样原始信号,通过少量的加法操作增加测量信息冗余,从而提高了信号重构能力,通过时间窗口方式对预处理后信号进行划分,从而对预处理后信号进行分组编码,并引入链式技术将各个时间窗口的信号链接起来,并将同一时间窗口的编码信号与信号链状态进行混合,利用链式的特性屏蔽信号的能量特征,以提高对唯密文攻击、已知明文攻击的抵抗能力,并赋予对中间人攻击的鲁棒性;进一步采用随机矩阵对混合信号进行加密得到密文,对密文的前部分进行子采样。本申请通过加链隐藏明文的能量信息,提高数据传输的安全性;通过子采样过程减少数据传输量,不仅降低系统的能耗,而且该方法等价于结合预置子采样矩阵和预置稀疏矩阵设计一个结构随机矩阵作为测量矩阵,其感知性能远好于在经典的压缩感知模型中将非结构随机矩阵作为测量矩阵的感知性能,相比于CCS,本申请可以大幅度提高系统的重构性能。

[0077] 请参考图3,本申请实施例提供的一种链式压缩感知数据流解码方法,包括:

[0078] 步骤301、通过第一个时刻的信号链状态对接收到第一个时刻的密文进行解码,得到第一时刻的子采样后的预处理后信号,其中,第一个时刻的信号链状态通过密钥初始化得到。

[0079] 可以通过$Y_i=Z_i-\Phi^{(i)}C_i=\Phi^{(i)}X_i$进行解密。在接收到密文$\tilde{z}$时,已知密钥$k_{ab}$,可以确定第一个时刻的信号链状态$C_1$,因此,通过求逆运算可以求解得到第一个时刻的子采样后的预处理后信号。

[0080] 步骤302、根据第一个时刻的信号链状态和子采样后的预处理后信号获取下一时刻的信号链状态,并通过下一时刻的信号链状态对接收到下一时刻的密文进行解码,得到下一时刻的子采样后的预处理后信号。

[0081] 对重构的第一个时刻的子采样后的预处理后信号通过哈希算法加链,得到下一时刻的信号链状态$C_2=H(C_1+X_1)=(\xi\times(C_1+X_1)+\eta)\bmod 2^{B_C}$,其中,$\xi=2^{B_C}-1$、η=1。

[0082] 步骤303、将下一时刻的预处理后信号和信号链状态作为第一个时刻的预处理后信号和信号链状态,并返回步骤302,逐步得到各个时刻的子采样后的预处理后信号。

[0083] 将下一时刻的预处理后信号和信号链状态作为第一个时刻的预处理后信号和信号链状态,重复上述步骤301和302,逐步求解各个时刻(i＝1,2,...,s)的子采样后的预处理信号$\tilde{x}$,其中,$\tilde{x}=D_{M\times N}x$。

[0084] 步骤304、通过预置子采样矩阵和预置稀疏矩阵生成结构随机矩阵,将结构随机矩阵作为测量矩阵,并通过压缩感知重构方法根据测量矩阵和各个时刻的子采样后的预处理后信号进行信号重构,得到原始信号。

[0085] SRM(结构随机矩阵)通过集成三步操作以获取CS测量值。首先,通过置换矩阵R对原始信号进行随机化处理,得到随机信号;然后,将快速计算变换F应用于随机信号得到变换系数;最终,通过子采样矩阵D采样变换系数,从而得到测量矩阵。本申请实施例中,在解码端,构造了新的测量矩阵,在结构上等效于SRM,本申请实施例将预置子采样矩阵$D_{M\times N}$和预置稀疏矩阵A进行相乘,得到新的测量矩阵$W_{M\times N}=D_{M\times N}A_{N\times N}$,可以参考图4。本申请实施例构造了新的测量矩阵,在结构上等效于SRM,相较于非结构的随机矩阵,SRM具有快速高效的特性,并且通过改变结构,可以消除CCS(一种链式CS方案)中重构所带来的累计误差,在保证信息完整的情况下,尽可能的降低传输成本,增强系统的重构能力。

[0086] 在获取到测量矩阵后,重构原始信号的过程可以转换成压缩感知模型,即$\tilde{x}$相当于测量值y,测量矩阵W相当于测量矩阵Φ,通过测量矩阵和测量值可以重构得到原始信号1,即有$l=\mathrm{Rec}(\tilde{x},W)$,其中,Rec()为压缩感知重构算法,压缩感知重构算法属于现有技术,在此不再对其具体过程进行赘述。本申请实施例中的编码解码过程具体可以参考图5。

[0087] 在远程医疗监护系统中,不仅要解决能耗和安全性这两大关键问题,而且从心电等敏感数据中提取信息的准确性和对其关键信息的提取能力至关重要。因此,需要关注在各种压缩比下,信号的重构质量,其决定了该方法是否可以长期用于心电监护等应用。

[0088] 尽管CCS是一种很有前途的方法,CCS使用链块将其与CS配对,实现数据的轻量加密,但使用非结构化传感矩阵会导致重建性能不佳。同时,由于CCS的每一步都与之前的重建结果相关,并且CS是一种有损压缩,因此不可避免地会在恢复过程中引入累积误差。以上两个原因在很大程度上会降低系统的重构质量,使医生对病人病情的诊断不准确,容易造成医疗事故。

[0089] 本申请在不影响安全性的情况下,提高CCS的重建性能,基于SRM的性质,提出了链式压缩感知数据流编解码方法。有效的测量矩阵在数据恢复中起着至关重要的作用,本申请构造一种快速高效的测量矩阵,以提高信号的重构质量,并且增强了系统的隐私级别,使远程医疗技术的可用性大幅度提升。

[0090] 有效的测量矩阵在数据恢复中起着至关重要的作用,本申请采用互相关性来衡量测量矩阵性能的质量,通过比较随机高斯矩阵、随机伯努利矩阵和本申请中的结构随机矩阵的互相关性,图6为随机高斯矩阵的互相关性,图7为随机伯努利矩阵的互相关性,图8为结构随机矩阵的互相关性,通过对比可知,本申请实施例提出的结构随机矩阵的性能要优于非结构化的感知矩阵。

[0091] 在物联网传输过程中,传感器和网关之间的通信可以表述为,发送器(Alice)将明文编码为密文,并将其发送给接收器(Bob)。各种潜在攻击者(Eve、Mallory)试图利用加密泄漏的信息获取明文信息。在通信过程中,存在包括COA(唯密文攻击)、KPA(已知明文攻击)

和MITM(中间人攻击)等几种潜在的攻击。因此,面对多个潜在的攻击,加强系统的鲁棒性至关重要。链式技术具有如下特性:在X_i的统计分布平缓条件下,当$i\to\infty$时,C_i的项均匀分布在$N(B_c)$中,这使得其可以保证IoT节点和网关之间数据传输的安全。

[0092] 在COA中,Eve试图通过查看密文的统计来猜测明文。在一般的压缩感知中,攻击者可以通过密文获取到明文的能量信息,导致明文信息泄露。在本申请实施例中,$Z_i=\Phi^{(i)}Q_i$是一个线性映射,由Z_i的分布可以推出的Q_i能量信息,但由于C_i均匀分布在$N(B_c)$中,Q_i的统计与X_i无关,攻击者很难从密文中获取到明文的信息。并且,本申请实施例对密文子采样,在解码端得到的预处理信号是$\tilde{x}$,攻击者很难从$\tilde{x}$中准确猜测到明文l。因此,这大大提高了系统对COA的抵抗能力。

[0093] 在KPA中,Eve通过捕捉一定数量的明文密文对来计算测量矩阵,从而解码明文。在一般的压缩感知中,Eve需要通过求解欠定方程组来计算测量矩阵,这需要区分大量的候选解,难度较大。在本申请实施例中,由于此时的明文密文对是l_i和Z_i,而且解码端接收到的是不完整的z,这将很难解码明文,大大提高了系统抵抗KPA的能力。

[0094] 在MITM中,Mallory知道密钥k_{ab},它可以假装Alice向Bob发送消息,Bob可能收到伪造的信息。在本申请实施例中,解码器接收的是子采样的密文$\tilde{z}$,根据$\tilde{x}$无法得到x。因此,Mallory无法重建明文,从而赋予对MITM的鲁棒性。

[0095] 请参考图9,本申请实施例提供的一种链式压缩感知数据流编码装置,其特征在于,包括:

[0096] 预处理单元,用于采用预置稀疏矩阵采样原始信号,得到预处理后信号;

[0097] 编码单元,用于通过时间窗口方式对预处理后信号进行划分,并对每个时间窗口内的信号进行二进制编码,得到编码信号;

[0098] 加链单元,用于基于哈希算法将每个时间窗口的编码信号链接起来,得到各个时间窗口的信号链状态,其中,第一个时间窗口的信号链状态通过密钥初始化得到;

[0099] 加密单元,用于将同一时间窗口的编码信号和信号链状态进行混合得到混合信号,并通过随机矩阵对各时间窗口的混合信号进行加密得到各时间窗口的密文,其中,随机矩阵通过密钥初始化生成;

[0100] 子采样单元,用于将各时间窗口的密文按列进行排列,得到密文向量,通过预置子采样矩阵对密文向量的前若干列数据进行子采样,并将子采样后的密文向量还原为矩阵形式,得到最终密文。

[0101] 本申请中,在信号预处理过程中,采用超低复杂度的预置稀疏矩阵采样原始信号,通过少量的加法操作增加测量信息冗余,从而提高了信号重构能力,通过时间窗口方式对预处理后信号进行划分,从而对预处理后信号进行分组编码,并引入链式技术将各个时间窗口的信号链接起来,并将同一时间窗口的编码信号与信号链状态进行混合,利用链式的特性屏蔽信号的能量特征,以提高对唯密文攻击、已知明文攻击的抵抗能力,并赋予对中间人攻击的鲁棒性;进一步采用结构随机矩阵对混合信号进行加密得到密文,对密文的前部分进行子采样。本申请通过加链隐藏明文的能量信息,提高数据传输的安全性;通过子采样过程减少数据传输量,不仅降低系统的能耗,而且该方法等价于结合预置子采样矩阵和预置稀疏矩阵设计一个结构随机矩阵作为测量矩阵,其感知性能远好于在经典的压缩感知模型中将非结构随机矩阵作为测量矩阵的感知性能,相比于CCS,本申请可以大幅度提高系统

的重构性能。

[0102] 请参考图10,本申请实施例提供的一种链式压缩感知数据流解码装置,包括:

[0103] 解码单元,用于通过第一个时刻的信号链状态对接收到第一个时刻的密文进行解码,得到第一时刻的子采样后的预处理后信号,其中,第一个时刻的信号链状态通过密钥初始化得到;

[0104] 获取单元,用于根据第一个时刻的信号链状态和子采样后的预处理后信号获取下一时刻的信号链状态,并通过下一时刻的信号链状态对接收到下一时刻的密文进行解码,得到下一时刻的子采样后的预处理后信号;

[0105] 触发单元,用于将下一时刻的预处理后信号和信号链状态作为第一个时刻的预处理后信号和信号链状态,并触发获取单元,逐步得到各个时刻的子采样后的预处理后信号;

[0106] 重构单元,用于通过预置子采样矩阵和预置稀疏矩阵生成结构随机矩阵,将结构随机矩阵作为测量矩阵,并通过压缩感知重构方法根据测量矩阵和各个时刻的子采样后的预处理后信号进行信号重构,得到原始信号。

[0107] 本申请实施例,已知密钥从而可以解码第一个时刻的密文,进而求得下一个时刻的信号链状态,以此逐步求解得到子采样后的预处理信号。此时,此模型转换成了经典的CS模型,通过预置子采样矩阵和预置稀疏矩阵设计一个结构随机矩阵作为新的测量矩阵,进而可以将子采样后的预处理信号与SRM通过压缩感知重构方法可以准确地重构出原始信号;构造的新的测量矩阵,在结构上等效于SRM,相较于非结构的随机矩阵,SRM具有快速高效的特性,并且通过改变结构,可以消除CCS中重构所带来的累计误差,在保证信息完整的情况下,尽可能的降低传输成本,增强系统的重构能力。

[0108] 所属领域的技术人员可以清楚地了解到,为描述的方便和简洁,上述描述的装置和单元的具体工作过程,可以参考前述方法实施例中的对应过程,在此不再赘述。

[0109] 本申请的说明书及上述附图中的术语“第一”、“第二”、“第三”、“第四”等(如果存在)是用于区别类似的对象,而不必用于描述特定的顺序或先后次序。应该理解这样使用的数据在适当情况下可以互换,以便这里描述的本申请的实施例例如能够以除了在这里图示或描述的那些以外的顺序实施。此外,术语“包括”和“具有”以及他们的任何变形,意图在于覆盖不排他的包含,例如,包含了一系列步骤或单元的过程、方法、系统、产品或设备不必限于清楚地列出的那些步骤或单元,而是可包括没有清楚地列出的或对于这些过程、方法、产品或设备固有的其它步骤或单元。

[0110] 应当理解,在本申请中,“至少一个(项)”是指一个或者多个,“多个”是指两个或两个以上。“和/或”,用于描述关联对象的关联关系,表示可以存在三种关系,例如,“A和/或B”可以表示:只存在A,只存在B以及同时存在A和B三种情况,其中A,B可以是单数或者复数。字符“/”一般表示前后关联对象是一种“或”的关系。“以下至少一项(个)”或其类似表达,是指这些项中的任意组合,包括单项(个)或复数项(个)的任意组合。例如,a,b或c中的至少一项(个),可以表示:a,b,c,“a和b”,“a和c”,“b和c”,或“a和b和c”,其中a,b,c可以是单个,也可以是多个。

[0111] 在本申请所提供的几个实施例中,应该理解到,所揭露的装置和方法,可以通过其它的方式实现。例如,以上所描述的装置实施例仅仅是示意性的,例如,所述单元的划分,仅仅为一种逻辑功能划分,实际实现时可以有另外的划分方式,例如多个单元或组件可以结

合或者可以集成到另一个系统,或一些特征可以忽略,或不执行。另一点,所显示或讨论的相互之间的耦合或直接耦合或通信连接可以是通过一些接口,装置或单元的间接耦合或通信连接,可以是电性,机械或其它的形式。

[0112] 所述作为分离部件说明的单元可以是或者也可以不是物理上分开的,作为单元显示的部件可以是或者也可以不是物理单元,即可以位于一个地方,或者也可以分布到多个网络单元上。可以根据实际的需要选择其中的部分或者全部单元来实现本实施例方案的目的。

[0113] 另外,在本申请各个实施例中的各功能单元可以集成在一个处理单元中,也可以是各个单元单独物理存在,也可以两个或两个以上单元集成在一个单元中。上述集成的单元既可以采用硬件的形式实现,也可以采用软件功能单元的形式实现。

[0114] 所述集成的单元如果以软件功能单元的形式实现并作为独立的产品销售或使用时,可以存储在一个计算机可读取存储介质中。基于这样的理解,本申请的技术方案本质上或者说对现有技术做出贡献的部分或者该技术方案的全部或部分可以以软件产品的形式体现出来,该计算机软件产品存储在一个存储介质中,包括若干指令用以通过一台计算机设备(可以是个人计算机,服务器,或者网络设备等)执行本申请各个实施例所述方法的全部或部分步骤。而前述的存储介质包括:U盘、移动硬盘、只读存储器(英文全称:Read-Only Memory,英文缩写:ROM)、随机存取存储器(英文全称:Random Access Memory,英文缩写:RAM)、磁碟或者光盘等各种可以存储程序代码的介质。

[0115] 以上所述,以上实施例仅用以说明本申请的技术方案,而非对其限制;尽管参照前述实施例对本申请进行了详细的说明,本领域的普通技术人员应当理解:其依然可以对前述各实施例所记载的技术方案进行修改,或者对其中部分技术特征进行等同替换;而这些修改或者替换,并不使相应技术方案的本质脱离本申请各实施例技术方案的精神和范围。

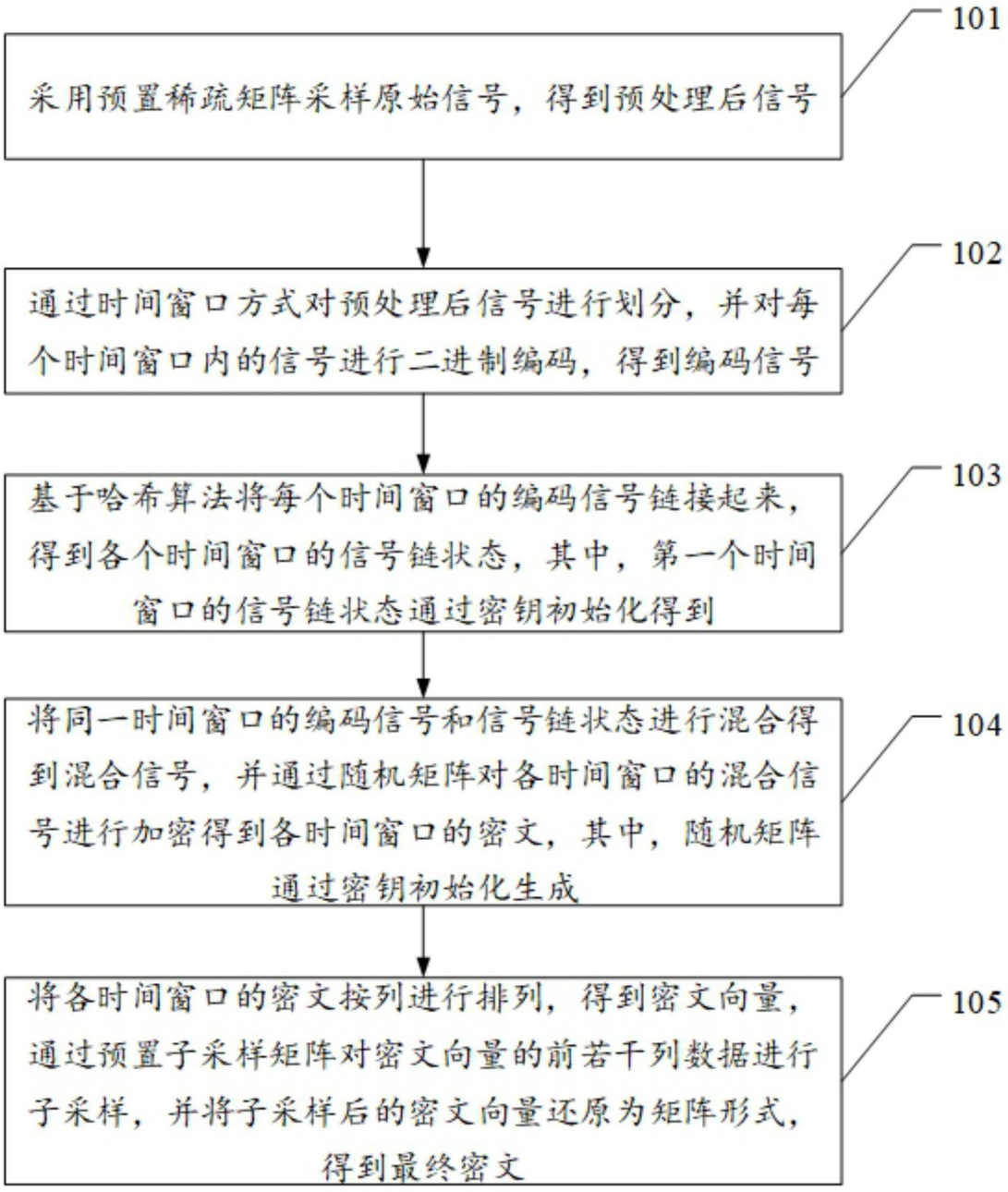

101
采用预置稀疏矩阵采样原始信号，得到预处理后信号
102
通过时间窗口方式对预处理后信号进行划分，并对每个时间窗口内的信号进行二进制编码，得到编码信号
103
基于哈希算法将每个时间窗口的编码信号链接起来，得到各个时间窗口的信号链状态，其中，第一个时间窗口的信号链状态通过密钥初始化得到
104
将同一时间窗口的编码信号和信号链状态进行混合得到混合信号，并通过随机矩阵对各时间窗口的混合信号进行加密得到各时间窗口的密文，其中，随机矩阵通过密钥初始化生成
105
将各时间窗口的密文按列进行排列，得到密文向量，通过预置子采样矩阵对密文向量的前若干列数据进行子采样，并将子采样后的密文向量还原为矩阵形式，得到最终密文

图1

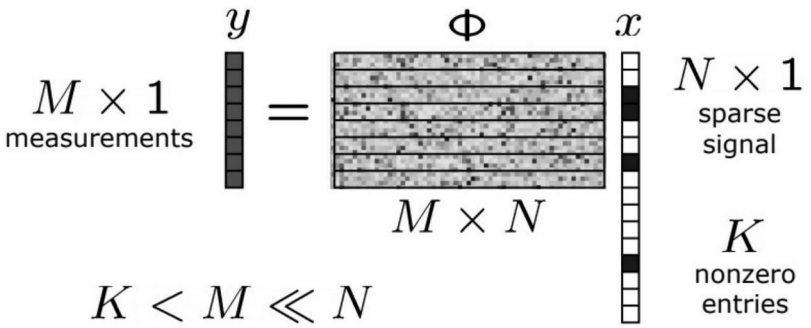

y
Φ
x
M × 1
measurements
=
N × 1
sparse
signal
M × N
K
nonzero
entries
K < M ≪ N

图2

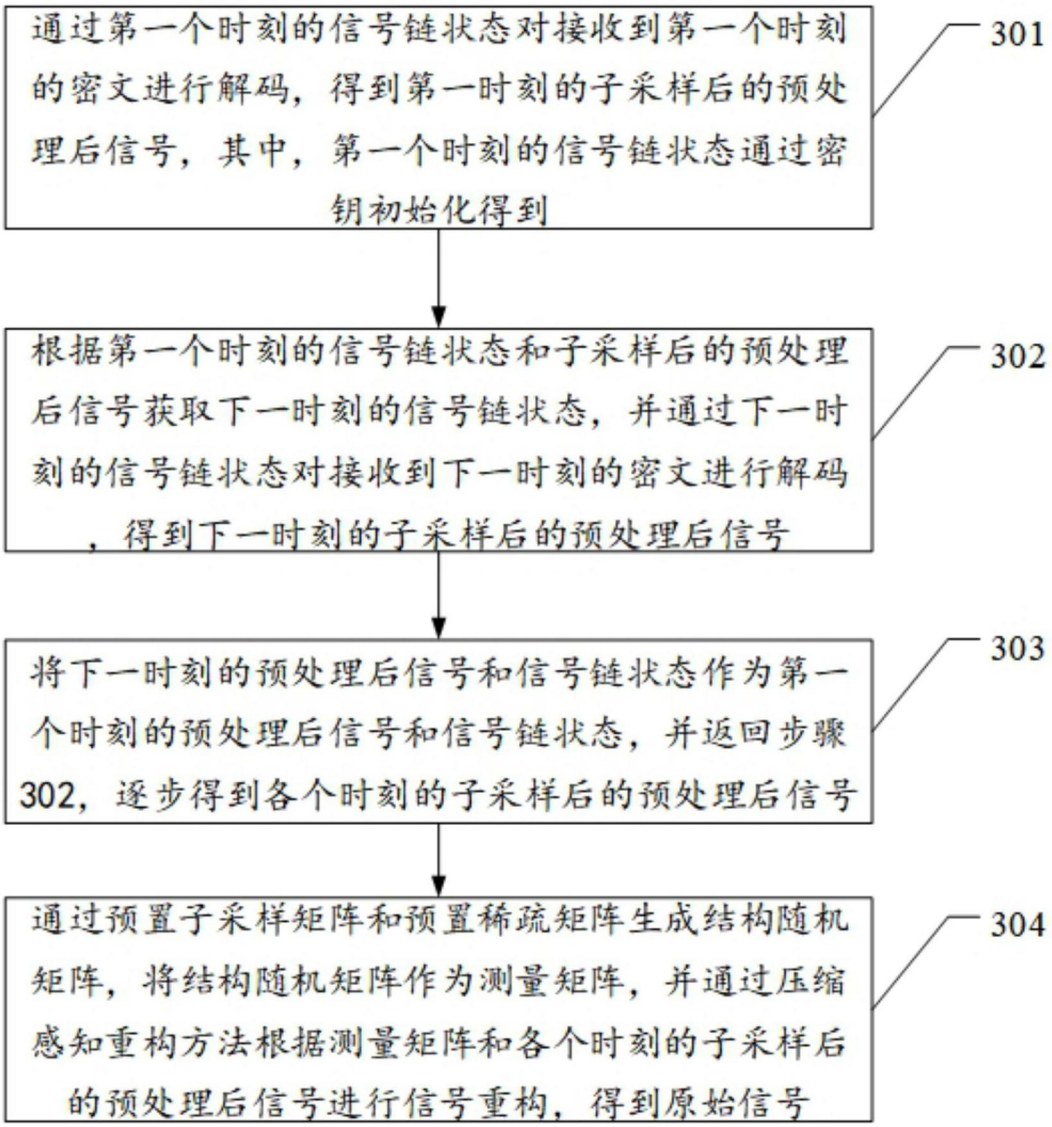

通过第一个时刻的信号链状态对接收到第一个时刻的密文进行解码，得到第一时刻的子采样后的预处理后信号，其中，第一个时刻的信号链状态通过密钥初始化得到
301
根据第一个时刻的信号链状态和子采样后的预处理后信号获取下一时刻的信号链状态，并通过下一时刻的信号链状态对接收到下一时刻的密文进行解码，得到下一时刻的子采样后的预处理后信号
302
将下一时刻的预处理后信号和信号链状态作为第一个时刻的预处理后信号和信号链状态，并返回步骤302，逐步得到各个时刻的子采样后的预处理后信号
303
通过预置子采样矩阵和预置稀疏矩阵生成结构随机矩阵，将结构随机矩阵作为测量矩阵，并通过压缩感知重构方法根据测量矩阵和各个时刻的子采样后的预处理后信号进行信号重构，得到原始信号
304

图3

$$\mathbf{W} = \underset{\mathbf{D}}{\begin{pmatrix}1&0&0&0\\0&1&0&0\end{pmatrix}} \underset{\mathbf{A}}{\begin{pmatrix}-1&0&1&0\\1&0&-1&0\\0&1&0&-1\\0&-1&0&1\end{pmatrix}}$$

$$= \underset{\mathbf{D}}{\begin{pmatrix}1&0&0&0\\0&1&0&0\end{pmatrix}} \underset{\mathbf{F}}{\begin{pmatrix}1&-1&0&0\\-1&1&0&0\\0&0&1&-1\\0&0&-1&1\end{pmatrix}} \underset{\mathbf{R}}{\begin{pmatrix}0&0&1&0\\1&0&0&0\\0&1&0&0\\0&0&0&1\end{pmatrix}}$$

图4

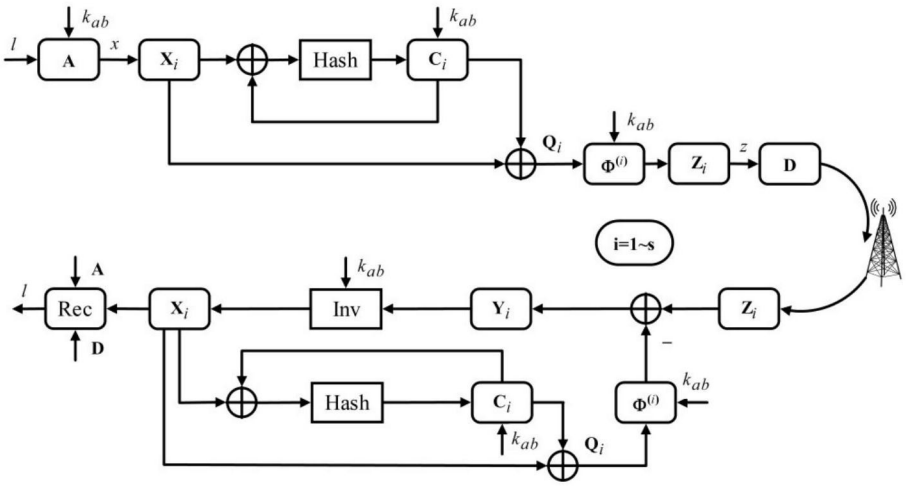


图5

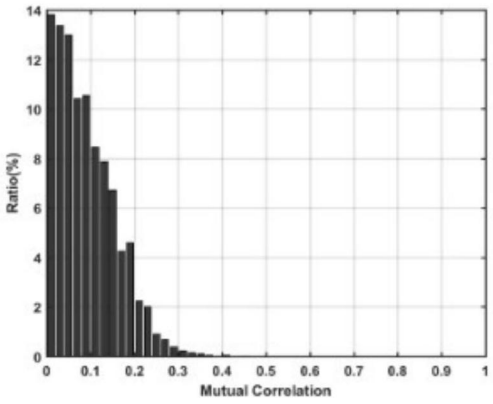


图6

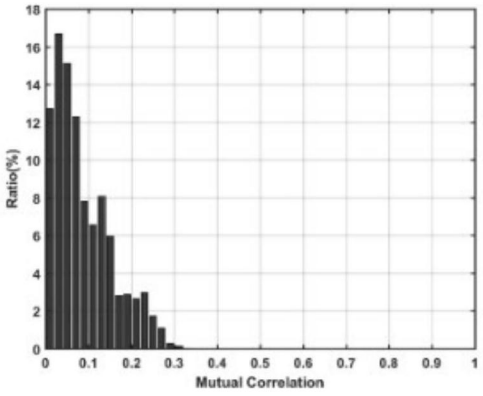

Ratio(%)
Mutual Correlation
0
2
4
6
8
10
12
14
16
18
0.1
0.2
0.3
0.4
0.5
0.6
0.7
0.8
0.9
1

图7

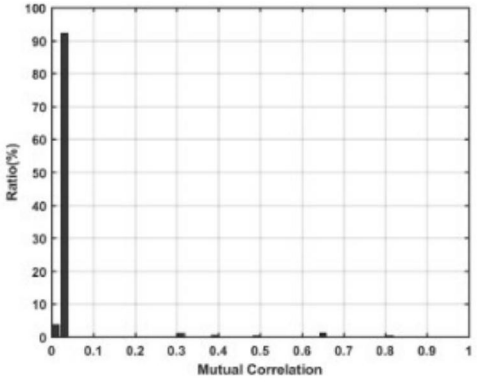

Ratio(%)
Mutual Correlation
0
10
20
30
40
50
60
70
80
90
100
0.1
0.2
0.3
0.4
0.5
0.6
0.7
0.8
0.9
1

图8

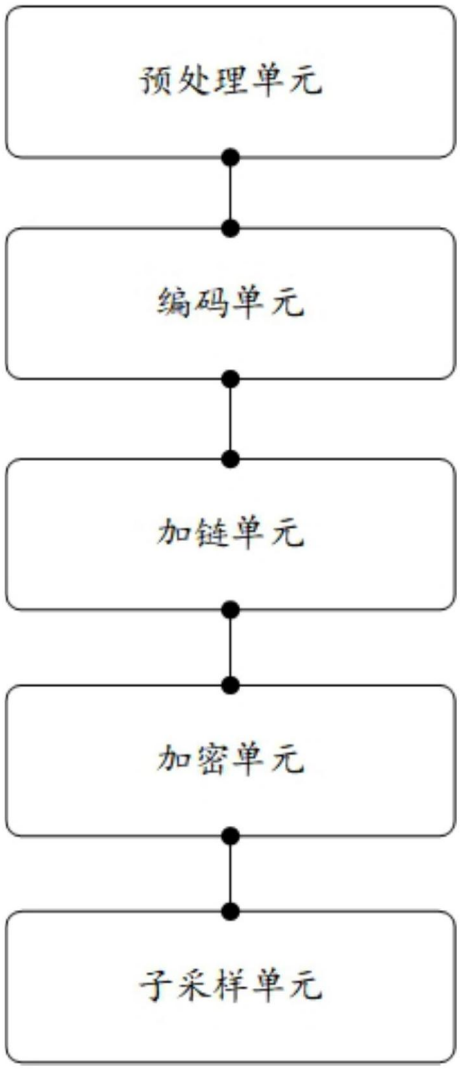


图9

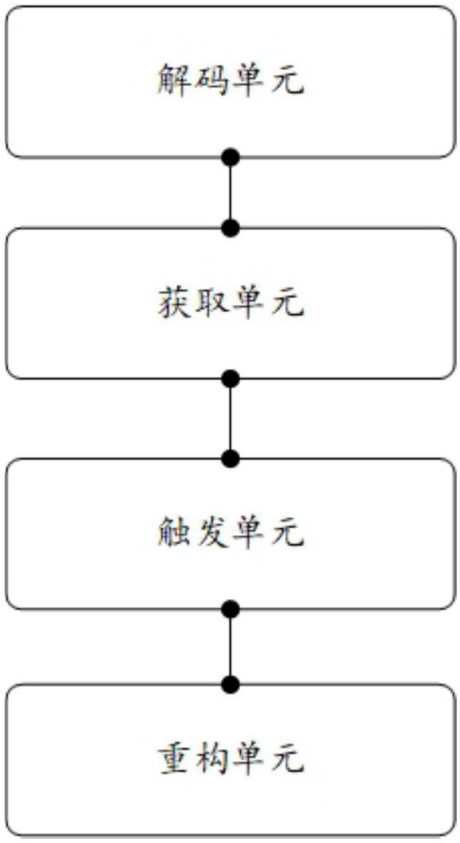


图10