(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国 际 局

(43) 国际公布日
2023 年 7 月 27 日 (27.07.2023)

WIPO | PCT

(10) 国际公布号
WO 2023/138265 A1

(51) 国际专利分类号:
G06F 21/60 (2013.01)

(21) 国际申请号: PCT/CN2022/138774

(22) 国际申请日: 2022 年 12 月 13 日 (13.12.2022)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
202210069219.1 2022年1月21日 (21.01.2022) CN

(71) 申请人: 苏州浪潮智能科技有限公司 (INSPUR SUZHOU INTELLIGENT TECHNOLOGY CO., LTD.) [CN/CN]; 中国江苏省苏州市吴中区吴中经济开发区郭巷街道官浦路1号9幢, Jiangsu 215000 (CN)。

(72) 发明人: 张旭 (ZHANG, Xu); 中国江苏省苏州市吴中区吴中经济开发区郭巷街道官浦路1号9幢, Jiangsu 215000 (CN)。 吴睿振 (WU, Ruizhen); 中国江苏省苏州市吴中区吴中经济开发区郭巷街道官浦路1号9幢, Jiangsu 215000 (CN)。 张永兴 (ZHANG, Yongxing); 中国江苏省苏州市吴中区吴中经济开发区郭巷街道官浦路1号9幢, Jiangsu 215000 (CN)。 陈静静 (CHEN, Jingjing); 中国江苏省苏州市吴中区吴中经济开发区郭巷街道官浦路1号9幢, Jiangsu 215000 (CN)。 孙华锦 (SUN, Huajin); 中国江苏省苏州市吴中区吴中经济开发区郭巷街道官浦路1号9幢, Jiangsu 215000 (CN)。 王凛 (WANG, Lin); 中国江苏省苏州市吴中区吴中经济开发区郭巷街道官浦路1号9幢, Jiangsu 215000 (CN)。

(74) 代理人: 北京润泽恒知识产权代理有限公司 (BEIJING RUN ZEHENG INTELLECTUAL

(54) **Title:** DATA ENCRYPTION AND DECRYPTION METHOD AND SYSTEM, DEVICE, AND COMPUTER-READABLE STORAGE MEDIUM

(54) **发明名称:** 一种数据加解密方法、系统、设备及计算机可读存储介质

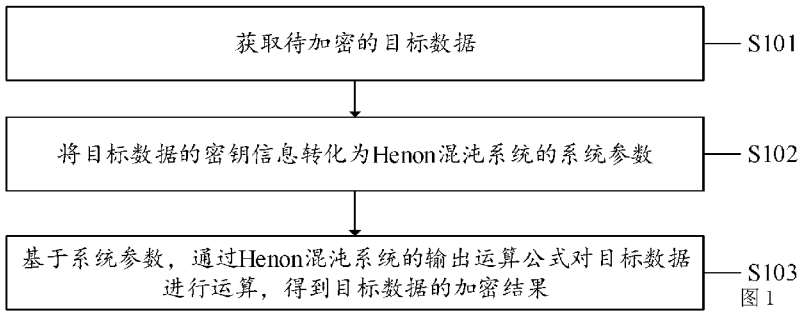

图 1

S101 Obtain target data to be encrypted
S102 Convert cryptographic key information of target data into system parameter of Henon chaotic system
S103 Perform operation on target data by means of output operation formula of Henon chaotic system and on basis of system parameter to obtain encryption result of target data

(57) **Abstract:** The invention discloses a data encryption and decryption method and system, a device, and a computer-readable storage medium. An embodiment comprises obtaining target data to be encrypted; converting cryptographic key information of the target data into a system parameter of a Henon chaotic system; and performing an operation on the target data by means of an output operation formula of the Henon chaotic system and on the basis of the system parameter to obtain an encryption result of the target data. In the present application, a cryptographic key information feature is realized with the aid of a system parameter of a Henon chaotic system, and cryptographic key space can be expanded due to the fact that there are a greater number of system parameters of the Henon chaotic system; and an encryption result can be obtained just by performing an operation on target data by means of an output operation formula of the Henon chaotic system. Due to the fact that the output operation formula only involves a differential equation and a matrix operation, the present invention has a fast encryption speed and good applicability. The data encryption and decryption system, the

WO 2023/138265 A1

[见续页]

PROPERTY LAW FIRM)；中国中关村南大街甲18号北京国际C座6层606, Beijing 100081 (CN)。

(81) 指定国(除另有指明，要求每一种可提供的国家保护)：AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CV, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IQ, IR, IS, IT, JM, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW。

(84) 指定国(除另有指明，要求每一种可提供的地区保护)：ARIPO (BW, CV, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚(AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, ME, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

本国际公布:

— 包括国际检索报告(条约第21条(3))。

device, and the computer-readable storage medium provided by the present application likewise solve corresponding technical problems.

(57) 摘要：本申请公开了一种数据加解密方法、系统、设备及计算机可读存储介质，获取待加密的目标数据；将目标数据的密钥信息转化为Henon混沌系统的系统参数；基于系统参数，通过Henon混沌系统的输出运算公式对目标数据进行运算，得到目标数据的加密结果。本申请中，借助Henon混沌系统的系统参数实现密钥信息的功能，由于Henon混沌系统的系统参数较多，所以本申请可以扩充密钥空间；并且只需通过Henon混沌系统的输出运算公式对目标数据进行运算，便可以得到加密结果。由于该输出运算公式只涉及微分方程及矩阵运算，所以加密速度较快，适用性好。本申请提供的一种数据加解密系统、设备及计算机可读存储介质也解决了相应技术问题。

一种数据加解密方法、系统、设备及计算机可读存储介质

相关申请的交叉引用

本申请要求于 2022 年 01 月 21 日提交中国专利局、申请号 202210069219.1、申请名称为“一种数据加解密方法、系统、设备及计算机可读存储介质”的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

技术领域

本申请涉及数据安全技术领域，更具体地说，涉及一种数据加解密方法、系统、设备及非易失性可读存储介质。

背景技术

近些年，越来越多的图像传输并存储在网络中。在各行各业中，例如计算机视觉，机器人路径规划，医学影像处理，信息的私密性已经成为了一个至关重要的问题。其中，加密算法可以仅让被授权的使用者来获取并处理图像，因此，在信息技术领域，加密算法被专家和学者广泛认可并成为一种有效的数据安全手段。然而，现有的 DES（Data Encryption Standard，数据加密标准）、AES（Advanced Encryption Standard，高级加密标准）、RSA 等加解密方法的局限性较多，比如密钥空间小，加密速度慢等，适用性差。

发明内容

本申请的目的是提供一种数据加解密方法，其能在一定程度上解决如何提高数据加解密方法的适用性的技术问题。本申请还提供了一种数据加解密系统、设备及非易失性可读存储介质。

为了实现上述目的，本申请提供如下技术方案：

一种数据加解密方法，包括：

获取待加密的目标数据；

将目标数据的密钥信息转化为 Henon 混沌系统的系统参数；

基于系统参数，通过 Henon 混沌系统的输出运算公式对目标数据进行运算，得到目标数据的加密结果。

在一些实施例中，基于系统参数，通过 Henon 混沌系统的输出运算公式对目标数据进行运算，得到目标数据的加密结果，包括：

基于系统参数，通过 Henon 混沌系统的输出运算公式对目标数据进行运算，得到目标数

据的加密结果；

Henon 混沌系统的输出运算公式包括：

$y(k)=Cx(k)+Dm(k)$ ； $z(k)=Ex(k)$ ；

$x(k+1)=\sum_{i=1}^{2}\mu_i(\xi(k))(A_i x(k))+b$ ；

$\mu_1(\xi(k))=\frac{1}{2}\left(1+\frac{\xi(k)}{d}\right)$ ； $\mu_2(\xi(k))=\frac{1}{2}\left(1-\frac{\xi(k)}{d}\right)$ ； $\xi(k)=x_1(k)$ ；

$x(k)=\left[x_1(k)\quad x_2(k)\right]^T$ ；

其中，$m(k)$ 表示 k 时刻时的目标数据；$y(k)$、$z(k)$ 表示加密结果；C 表示 Henon 混沌系统的输出矩阵，$C=\begin{bmatrix}c_{11} & c_{12}\\ c_{21} & c_{22}\end{bmatrix}$；$D$ 表示非奇异的直通矩阵；$A_i=\begin{bmatrix}\pm a_{11} & a_{12}\\ a_{21} & a_{22}\end{bmatrix}$；$b$、$d$ 表示预设的参数值，且 $x_1(k)\in[-d,d]$；$x_1(k)$、$x_2(k)$ 表示 Henon 混沌系统的两个状态值；T 表示矩阵的转置；E 表示可逆矩阵。

在一些实施例中，将目标数据的密钥信息转化为 Henon 混沌系统的系统参数，包括：

将目标数据的密钥信息转化为 Henon 混沌系统的状态值。

在一些实施例中，将目标数据的密钥信息转化为 Henon 混沌系统的系统参数，包括：

将目标数据的密钥信息转化为 Henon 混沌系统中 A_i 和/或输出矩阵的对应值。

在一些实施例中，将目标数据的密钥信息转化为 Henon 混沌系统的系统参数，包括：

将目标数据的密钥信息转化为 Henon 混沌系统中的 b 值。

一种数据加解密方法，包括：

获取加密结果，其中，加密结果基于系统参数，通过 Henon 混沌系统的输出运算公式对目标数据进行运算得到，系统参数为将目标数据的密钥信息转化后得到的 Henon 混沌系统的参数；

获取系统参数；

基于系统参数对加密结果进行解密，得到目标数据。

在一些实施例中，基于系统参数对加密结果进行解密，得到目标数据，包括：

通过解密公式，基于系统参数对加密结果进行解密，得到目标数据；

解密公式包括：

$$m(k)=\begin{bmatrix}D\\0\end{bmatrix}^{\dagger}\left(\begin{bmatrix}y(k)\\z(k)\end{bmatrix}-\begin{bmatrix}C\\E\end{bmatrix}\left(\sum_{i=1}^{2}\mu_i(\xi(k-1))\left(A_i(0\ E^{-1})\begin{pmatrix}y(k-1)\\z(k-1)\end{pmatrix}\right)+b\right)\right);$$

$$\mu_1(\xi(k))=\frac{1}{2}\left(1+\frac{\xi(k)}{d}\right);\ \mu_2(\xi(k))=\frac{1}{2}\left(1-\frac{\xi(k)}{d}\right);\ \xi(k)=x_1(k);$$

其中，$m(k)$表示k时刻时的目标数据；D表示非奇异的直通矩阵；$y(k)$、$z(k)$表示加密结果；C表示 Henon 混沌系统的输出矩阵，$C=\begin{bmatrix}c_{11} & c_{12}\\ c_{21} & c_{22}\end{bmatrix}$；$E$表示可逆矩阵；$A_i=\begin{bmatrix}\pm a_{11} & a_{12}\\ a_{21} & a_{22}\end{bmatrix}$；$b$、$d$表示预设的参数值，且$x_1(k)\in[-d,d]$；$x_1(k)$表示 Henon 混沌系统的一个状态值；†表示矩阵的伪逆。

本申请还公开了一种数据加解密系统，包括：

第一获取模块，用于获取待加密的目标数据；

第一转化模块，用于将目标数据的密钥信息转化为Henon混沌系统的系统参数；

第一加密模块，用于基于系统参数，通过 Henon 混沌系统的输出运算公式对目标数据进行运算，得到目标数据的加密结果。

本申请还公开了一种数据加解密设备，包括：

存储器，用于存储计算机程序；

处理器，用于执行计算机程序时实现如上任一数据加解密方法的步骤。

一种非易失性可读存储介质，非易失性可读存储介质中存储有计算机程序，计算机程序被处理器执行时实现如上任一数据加解密方法的步骤。

本申请提供的一种数据加解密方法，获取待加密的目标数据；将目标数据的密钥信息转化为Henon混沌系统的系统参数；基于系统参数，通过Henon混沌系统的输出运算公式对目标数据进行运算，得到目标数据的加密结果。本申请中，借助Henon混沌系统的系统参数实现密钥信息的功能，由于Henon混沌系统的系统参数较多，所以本申请可以扩充密钥空间；并且只需通过Henon混沌系统的输出运算公式对目标数据进行运算，便可以得到加密结果，由于该输出运算公式只涉及微分方程及矩阵运算，所以加密速度较快；适用性好。本申请提供的一种数据加解密系统、设备及非易失性可读存储介质也解决了相应技术问题。

附图说明

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的前提下，还可以根据提供的附图获得其他的附图。

图 1 为本申请实施例提供的一种数据加解密方法的第一流程图；

图 2 为本申请中 Henon 混沌系统的结构图；

图 3 为本申请实施例提供的一种数据加解密方法的第二流程图；

图 4 为本申请实施例提供的一种数据加解密系统的第一结构示意图；

图 5 为本申请实施例提供的一种数据加解密系统的第二结构示意图；

图 6 为本申请实施例提供的一种数据加解密设备的结构示意图；

图 7 为本申请实施例提供的一种数据加解密设备的另一结构示意图；

图 8 为本申请实施例提供的一种非易失性可读存储介质的结构示意图。

具体实施方式

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。

请参阅图 1，图 1 为本申请实施例提供的一种数据加解密方法的第一流程图。

本申请实施例提供的一种数据加解密方法，可以包括以下步骤：

步骤 S101：获取待加密的目标数据。

实际应用中，可以先获取待加密的目标数据，目标数据的类型可以根据实际需要确定，比如可以为文本数据、图像数据等，本申请在此不做具体限定。

步骤 S102：将目标数据的密钥信息转化为 Henon 混沌系统的系统参数。

实际应用中，在获取待加密的目标数据之后，需将目标数据的密钥信息转换为 Henon（混沌映射）混沌系统中的系统参数，比如将密钥信息映射为 Henon 混沌系统的系统参数等，以借助 Henon 混沌系统的系统参数实现目标数据的密钥信息的加解密功能。

需要说明的是，本申请中由密钥信息转化成的 Henon 混沌系统的系统参数的类型、数量等可以根据实际需要确定，本申请在此不做具体限定。

步骤 S103：基于系统参数，通过 Henon 混沌系统的输出运算公式对目标数据进行运算，得到目标数据的加密结果。

实际应用中，在将目标数据的密钥信息转化为 Henon 混沌系统的系统参数之后，便可以

基于系统参数，通过 Henon 混沌系统的输出运算公式对目标数据进行运算，得到目标数据的加密结果。

具体应用场景中，在基于系统参数，通过 Henon 混沌系统的输出运算公式对目标数据进行运算，得到目标数据的加密结果的过程中，所依据的 Henon 混沌系统的输出运算公式可以包括：

$$y(k)=Cx(k)+Dm(k)\text{；}\quad z(k)=Ex(k)\text{；}$$

$$x(k+1)=\sum_{i=1}^{2}\mu_i\left(\xi(k)\right)\left(A_i x(k)\right)+b\text{；}$$

$$\mu_1\left(\xi(k)\right)=\frac{1}{2}\left(1+\frac{\xi(k)}{d}\right)\text{；}\quad \mu_2\left(\xi(k)\right)=\frac{1}{2}\left(1-\frac{\xi(k)}{d}\right)\text{；}\quad \xi(k)=x_1(k)\text{；}$$

$$x(k)=\left[x_1(k)\quad x_2(k)\right]^T\text{；}$$

其中，$m(k)$表示k时刻时的目标数据；$y(k)$、$z(k)$表示加密结果；C表示 Henon 混沌系统的输出矩阵，$C=\begin{bmatrix}c_{11} & c_{12}\\ c_{21} & c_{22}\end{bmatrix}$；$D$表示非奇异的直通矩阵；$A_i=\begin{bmatrix}\pm a_{11} & a_{12}\\ a_{21} & a_{22}\end{bmatrix}$；$b$、$d$表示预设的参数值，且$x_1(k)\in[-d,d]$；$x_1(k)$、$x_2(k)$表示 Henon 混沌系统的两个状态值；$T$表示矩阵的转置；$E$表示可逆矩阵。

相应的，Henon 混沌系统的系统参数可以为$x_1(k)$、$x_2(k)$、A_i、C、b等，进一步的，在将目标数据的密钥信息转化为 Henon 混沌系统的系统参数的过程中，可以将目标数据的密钥信息转化为 Henon 混沌系统的状态值中的$x_1(k)$、$x_2(k)$，A_i中的a_{11}、a_{12}、a_{21}、a_{22}，C中的c_{11}、c_{12}、c_{21}、c_{22}，b中的一个或多个等，本申请在此不做具体限定。

本申请提供的一种数据加解密方法，获取待加密的目标数据；将目标数据的密钥信息转化为 Henon 混沌系统的系统参数；基于系统参数，通过 Henon 混沌系统的输出运算公式对目标数据进行运算，得到目标数据的加密结果。本申请中，借助 Henon 混沌系统的系统参数实现密钥信息的功能，由于 Henon 混沌系统的系统参数较多，所以本申请可以扩充密钥空间；并且只需通过 Henon 混沌系统的输出运算公式对目标数据进行运算，便可以得到加密结果，由于该输出运算公式只涉及微分方程及矩阵运算，所以加密速度较快；适用性好。

为了便于理解本申请的数据加解密方法，现对本申请中 Henon 混沌系统的输出运算公式

的生成过程进行描述：

Henon 映射是一种可以产生混沌现象的离散动态系统，其动态方程可以表示为：

$$\begin{aligned} x_1(k+1) &= -x_1^2(k)+0.3x_2(k)+1.4 \\ x_2(k+1) &= x_1(k) \\ y(k) &= x_1(k) \end{aligned} ;$$

其中，$x_1(k)$和$x_2(k)$是系统的状态，$y(k)$是系统的输出，$x_1(0)$和$x_2(0)$是系统的初始状态，即$k=0$时刻的状态初始值。系统的前件变量为$x_1(k)$，且它的范围是$x_1(k)\in[-d,d]$，$d=2$。

首先，将 Henon 映射转化为 TS（Takagi-Sugeno）模糊模型，其规则如下：如果$x_1(k)$属于模糊集F_i，那么$x(k+1)=A_i x(k)+b_i$，$y(k)=C_i x(k)$；

其中，$x(k)=\begin{bmatrix} x_1(k) & x_2(k) \end{bmatrix}^T$为系统的状态向量；模糊集为$F_1(x_1(k))=\frac{1}{2}\left(1+\frac{x_1(k)}{d}\right)$，$F_2(x_1(k))=\frac{1}{2}\left(1-\frac{x_1(k)}{d}\right)$；系数矩阵为$A_1=\begin{bmatrix} -d & 0.3 \\ 1 & 0 \end{bmatrix}$，$A_2=\begin{bmatrix} d & 0.3 \\ 1 & 0 \end{bmatrix}$，$b_1=b_2=\begin{bmatrix} 1.4 \\ 0 \end{bmatrix}$，和$C_1=C_2$待设计。由上述公式可以看到常值项 1.4 存在于系统的状态方程中，如果直接注入明文在此状态方程中，将会改变混沌系统的结构，致使混沌序列的产生出现问题，则基于 Henon 映射的混沌动态系统的 TS Fuzzy model（TS 模糊模型）可以写为：

$$x(k+1)=\sum_{i=1}^{2}\mu_i(\xi(k))(A_i x(k)+b_i) ; \quad y(k)=\sum_{i=1}^{2}\mu_i(\xi(k))(C_i x(k)) ;$$

其中$\xi(k)=x_1(k)$，$\mu_1(\xi(k))=\frac{1}{2}\left(1+\frac{\xi(k)}{d}\right)$，$\mu_2(\xi(k))=\frac{1}{2}\left(1-\frac{\xi(k)}{d}\right)$并且其满足$\mu_1(\xi(k))+\mu_2(\xi(k))=1$。

假设加密的数据（明文）为$m(k)$，且在k时刻，$m(k)\in\mathbb{R}^l$可以为向量。将明文注入 Henon 混沌系统的状态方程，系统转换为：

$$x(k+1)=\sum_{i=1}^{2}\mu_i(\xi(k))(A_i x(k)+b_i) ;$$

$$y(k)=\sum_{i=1}^{2}\mu_i(\xi(k))(C_i x(k)+D_i m(k)) ;$$

$$z(k)=Ex(k) ;$$

可以看出，没有明文直接进入系统状态通道，而是直接进入系统输出方程，直通矩阵为

D_i；

简化系统并定义输出矩阵C_i，E和直通矩阵D_i的属性，并令$b=b_1=b_2$，可得：

$$x(k+1)=\sum_{i=1}^{2}\mu_i(\xi(k))(A_i x(k))+b$$；

$$y(k)=Cx(k)+Dm(k)$$；

$$z(k)=Ex(k)$$；

其中，数据注入式 Henon 混沌系统固定了输出矩阵C。这里，选择E为任意可逆矩阵，且直通矩阵D为非奇异。构造的数据注入式 Henon 混沌系统可以如图 2 所示等，包括加和器、移位器、寄存器等，各器件的输入、输出及存储数据等可以如图所示。

下面基于平坦性的安全等级验证来对本申请中Henon混沌系统的加解密功能进行验证：

传统的经典自同步流加密(Self-synchronizing stream cipher)算法是指其中的keystream（密钥流）是由固定前密文位得到的函数所生成。加密过程如下：

$$X_s(k)=\sigma_\Theta^{ss}(c_s(k-l),\ldots,c_s(k-l-\tau_d))$$；

$$c_s(k)=\mathcal{E}(X_s(k),m(k))$$；

其中，X_s是密钥流，Θ是密钥，$m(k)$是k时刻的明文，$c_s(k)$是k时刻的密文，σ_Θ^{ss}是密钥流产生函数，$\mathcal{E}$是加密函数，l为常数，τ_d是记忆延时。从表达式中，很清楚可以看出，自同步流加密方法的密钥流依赖于密文以及固定步数的过去时段的密文，这个固定步数取决于τ_d。下面给出基于系统平坦性的 Henon 混沌加密系统与自同步流加密算法的等价实现。

第一步，验证 Henon 混沌加密系统的平坦性：根据平坦性定义，一个系统的状态和输入可以用输出以及输出的超前位或者迟后位来表示，这样的系统就是平坦系统，它也是线性系统可控性在非线性系统中的拓展。因此，根据 Henon 混沌系统的动态方程，输出矩阵 的可逆性给出了状态关于输出的表达形式，即

$$x(k)=E^{-1}z(k)=\begin{pmatrix}0 & E^{-1}\end{pmatrix}\begin{pmatrix}y(k)\\ z(k)\end{pmatrix}$$；

另外，将 Henon 状态方程代入$x(k-1)$得到

$$x(k)=\sum_{i=1}^{2}\mu_i(\xi(k-1))\left(A_i\begin{pmatrix}0 & E^{-1}\end{pmatrix}\begin{pmatrix}y(k-1)\\ z(k-1)\end{pmatrix}\right)+b$$；

因为D是满秩的，所以明文$m(k)$表示为

$$m(k)=\begin{bmatrix}D\\0\end{bmatrix}^{\dagger}\left(\begin{bmatrix}y(k)\\z(k)\end{bmatrix}-\begin{bmatrix}C\\E\end{bmatrix}x(k)\right)$$
$$=\begin{bmatrix}D\\0\end{bmatrix}^{\dagger}\left(\begin{bmatrix}y(k)\\z(k)\end{bmatrix}-\begin{bmatrix}C\\E\end{bmatrix}\left(\sum_{i=1}^{2}\mu_i(\xi(k-1))\left(A_i(0\ \ E^{-1})\begin{pmatrix}y(k-1)\\z(k-1)\end{pmatrix}\right)+b\right)\right);$$

这里$\begin{bmatrix}D\\0\end{bmatrix}^{\dagger}$是矩阵$\begin{bmatrix}D\\0\end{bmatrix}$的伪逆，即$\begin{bmatrix}D\\0\end{bmatrix}^{\dagger}=\left(\begin{bmatrix}D\\0\end{bmatrix}^{T}\begin{bmatrix}D\\0\end{bmatrix}\right)^{-1}\begin{bmatrix}D\\0\end{bmatrix}^{T}$，因此，数据注入式Henon混沌加密系统满足平坦性要求；

第二步，等价关系：数据注入式 Henon 混沌加密系统的状态方程和输出方程可以改写为：

$$x(k)=\sum_{i=1}^{2}\mu_i(\xi(k-1))\left(A_i(0\quad E^{-1})\begin{pmatrix}y(k-1)\\z(k-1)\end{pmatrix}\right)+b;$$

$$\begin{bmatrix}y(k)\\z(k)\end{bmatrix}=\begin{bmatrix}C\\E\end{bmatrix}x(k)+\begin{bmatrix}D\\0\end{bmatrix}m(k).$$

因此，取系统初始值为密钥，即$\Theta=x(0)$，数据注入式Henon混沌加密系统与传统自同步流加密的一一对应关系如下：

密钥产生器：

$$\sigma_{\Theta}^{n}(c_e(k-l),\ldots,c_e(k-l-\tau_d))\equiv\sum_{i=1}^{2}\mu_i(\xi(k-1))\left(A_i(0\quad E^{-1})\begin{pmatrix}y(k-1)\\z(k-1)\end{pmatrix}\right)+b;$$

密钥流：$X_e\equiv x$；

密文：$c_e\equiv\begin{bmatrix}y\\z\end{bmatrix}$；

加密函数：$\mathcal{E}\equiv\begin{bmatrix}C\\E\end{bmatrix}x(k)+\begin{bmatrix}D\\0\end{bmatrix}m(k)$；

记忆延迟：$\tau_d\equiv|1-0|=1$。

因此，可以看出数据注入式 Henon 混沌加密系统完全等价为一种传统自同步流加密技术，这种数学上的等价性可以保证数据注入式 Henon 混沌加密系统的安全等级，也就是说，这种数据注入式Henon混沌加密系统的安全等级不差于传统自同步流加密技术。

请参阅图 3，图 3 为本申请实施例提供的一种数据加解密方法的第二流程图。

本申请实施例提供的一种数据加解密方法，可以包括以下步骤：

步骤 S201：获取加密结果，其中，加密结果基于系统参数，通过 Henon 混沌系统的输出运算公式对目标数据进行运算得到，系统参数为将目标数据的密钥信息转化后得到的 Henon 混沌系统的参数。

步骤 S202：获取系统参数。

步骤 S203：基于系统参数对加密结果进行解密，得到目标数据。

具体应用场景中，明文 $m(k)$ 由密文 $y(k)$，$z(k)$ 和 $y(k-1)$，$z(k-1)$ 来表示，所以在基于系统参数对加密结果进行解密，得到目标数据的过程中，可以通过解密公式，基于系统参数对加密结果进行解密，得到目标数据；

解密公式包括：

$$m(k)=\begin{bmatrix}D\\0\end{bmatrix}^{\dagger}\left(\begin{bmatrix}y(k)\\z(k)\end{bmatrix}-\begin{bmatrix}C\\E\end{bmatrix}\left(\sum_{i=1}^{2}\mu_i(\xi(k-1))\left(A_i(0\ E^{-1})\begin{pmatrix}y(k-1)\\z(k-1)\end{pmatrix}\right)+b\right)\right);$$

$$\mu_1(\xi(k))=\frac{1}{2}\left(1+\frac{\xi(k)}{d}\right),\ \mu_2(\xi(k))=\frac{1}{2}\left(1-\frac{\xi(k)}{d}\right),\ \xi(k)=x_1(k);$$

其中，$m(k)$ 表示 k 时刻时的目标数据；D 表示非奇异的直通矩阵；$y(k)$、$z(k)$ 表示加密结果；C 表示 Henon 混沌系统的输出矩阵，$C=\begin{bmatrix}c_{11} & c_{12}\\ c_{21} & c_{22}\end{bmatrix}$；$E$ 表示可逆矩阵；$A_i=\begin{bmatrix}\pm a_{11} & a_{12}\\ a_{21} & a_{22}\end{bmatrix}$；$b$、$d$ 表示预设的参数值，且 $x_1(k)\in[-d,d]$；$x_1(k)$ 表示 Henon 混沌系统的一个状态值；† 表示矩阵的伪逆。

本申请中相应步骤的描述可以参阅上述记载，在此不再赘述。

请参阅图 4，图 4 为本申请实施例提供的一种数据加解密系统的第一结构示意图。

本申请实施例提供的一种数据加解密系统，可以包括：

第一获取模块 101，用于获取待加密的目标数据；

第一转化模块 102，用于将目标数据的密钥信息转化为 Henon 混沌系统的系统参数；

第一加密模块 103，用于基于系统参数，通过 Henon 混沌系统的输出运算公式对目标数据进行运算，得到目标数据的加密结果。

本申请实施例提供的一种数据加解密系统，第一加密模块可以包括：

第一加密单元，用于基于系统参数，通过 Henon 混沌系统的输出运算公式对目标数据进

行运算，得到目标数据的加密结果；

Henon 混沌系统的输出运算公式包括：

$$y(k)=Cx(k)+Dm(k)\text{；}\quad z(k)=Ex(k)\text{；}$$

$$x(k+1)=\sum_{i=1}^{2}\mu_i\left(\xi(k)\right)\left(A_i x(k)\right)+b\text{；}$$

$$\mu_1\left(\xi(k)\right)=\frac{1}{2}\left(1+\frac{\xi(k)}{d}\right)\text{；}\quad \mu_2\left(\xi(k)\right)=\frac{1}{2}\left(1-\frac{\xi(k)}{d}\right)\text{；}\quad \xi(k)=x_1(k)\text{；}$$

$$x(k)=\left[x_1(k)\quad x_2(k)\right]^T\text{；}$$

其中，$m(k)$表示k时刻时的目标数据；$y(k)$、$z(k)$表示加密结果；C表示 Henon 混沌系统的输出矩阵，$C=\begin{bmatrix}c_{11} & c_{12}\\ c_{21} & c_{22}\end{bmatrix}$；$D$表示非奇异的直通矩阵；$A_i=\begin{bmatrix}\pm a_{11} & a_{12}\\ a_{21} & a_{22}\end{bmatrix}$；$b$、$d$表示预设的参数值，且$x_1(k)\in[-d,d]$；$x_1(k)$、$x_2(k)$表示 Henon 混沌系统的两个状态值；$T$表示矩阵的转置；$E$表示可逆矩阵。

本申请实施例提供的一种数据加解密系统，第一转化模块可以包括：

第一转化单元，用于将目标数据的密钥信息转化为 Henon 混沌系统的状态值。

本申请实施例提供的一种数据加解密系统，第一转化模块可以包括：

第二转化单元，用于将目标数据的密钥信息转化为 Henon 混沌系统中A_i和/或输出矩阵的对应值。

本申请实施例提供的一种数据加解密系统，第一转化模块可以包括：

第三转化单元，用于将目标数据的密钥信息转化为 Henon 混沌系统中的b值。

请参阅图 5，图 5 为本申请实施例提供的一种数据加解密系统的第二结构示意图。

本申请实施例提供的一种数据加解密系统，可以包括：

第二获取模块 201，用于获取加密结果，其中，加密结果基于系统参数，通过 Henon 混沌系统的输出运算公式对目标数据进行运算得到，系统参数为将目标数据的密钥信息转化后得到的 Henon 混沌系统的参数；

第三获取模块 202，用于获取系统参数；

第一解密模块 203，用于基于系统参数对加密结果进行解密，得到目标数据。

本申请实施例提供的一种数据加解密系统，第一解密模块可以包括：

第一解密单元，用于通过解密公式，基于系统参数对加密结果进行解密，得到目标数据；

解密公式包括：

$$m(k)=\begin{bmatrix}D\\0\end{bmatrix}^{\dagger}\left(\begin{bmatrix}y(k)\\z(k)\end{bmatrix}-\begin{bmatrix}C\\E\end{bmatrix}\left(\sum_{i=1}^{2}\mu_i(\xi(k-1))\left(A_i(0\ E^{-1})\begin{pmatrix}y(k-1)\\z(k-1)\end{pmatrix}\right)+b\right)\right)$$；

$$\mu_1(\xi(k))=\frac{1}{2}\left(1+\frac{\xi(k)}{d}\right)$$，$$\mu_2(\xi(k))=\frac{1}{2}\left(1-\frac{\xi(k)}{d}\right)$$；$$\xi(k)=x_1(k)$$；

其中，$m(k)$表示k时刻时的目标数据；D表示非奇异的直通矩阵；$y(k)$、$z(k)$表示加密结果；C表示 Henon 混沌系统的输出矩阵，$C=\begin{bmatrix}c_{11}&c_{12}\\c_{21}&c_{22}\end{bmatrix}$；$E$表示可逆矩阵；$A_i=\begin{bmatrix}\pm a_{11}&a_{12}\\a_{21}&a_{22}\end{bmatrix}$；$b$、$d$表示预设的参数值，且$x_1(k)\in[-d,d]$；$x_1(k)$表示 Henon 混沌系统的一个状态值；†表示矩阵的伪逆。

本申请还提供了一种数据加解密设备及非易失性可读存储介质，其均具有本申请实施例提供的一种数据加解密方法具有的对应效果。请参阅图 6，图 6 为本申请实施例提供的一种数据加解密设备的结构示意图。

本申请实施例提供的一种数据加解密设备，包括存储器 201 和处理器 202，存储器 201 中存储有计算机程序，处理器 202 执行计算机程序时实现如下步骤：

获取待加密的目标数据；

将目标数据的密钥信息转化为 Henon 混沌系统的系统参数；

基于系统参数，通过 Henon 混沌系统的输出运算公式对目标数据进行运算，得到目标数据的加密结果。

本申请实施例提供的一种数据加解密设备，包括存储器 201 和处理器 202，存储器 201 中存储有计算机程序，处理器 202 执行计算机程序时实现如下步骤：基于系统参数，通过 Henon 混沌系统的输出运算公式对目标数据进行运算，得到目标数据的加密结果；

Henon 混沌系统的输出运算公式包括：

$$y(k)=Cx(k)+Dm(k)$$；$$z(k)=Ex(k)$$；

$$x(k+1)=\sum_{i=1}^{2}\mu_i(\xi(k))(A_ix(k))+b$$；

$\mu_1(\xi(k))=\frac{1}{2}\left(1+\frac{\xi(k)}{d}\right)$；$\mu_2(\xi(k))=\frac{1}{2}\left(1-\frac{\xi(k)}{d}\right)$；$\xi(k)=x_1(k)$；

$x(k)=\begin{bmatrix}x_1(k) & x_2(k)\end{bmatrix}^T$；

其中，$m(k)$表示k时刻时的目标数据；$y(k)$、$z(k)$表示加密结果；C表示 Henon 混沌系统的输出矩阵，$C=\begin{bmatrix}c_{11} & c_{12}\\ c_{21} & c_{22}\end{bmatrix}$；$D$表示非奇异的直通矩阵；$A_i=\begin{bmatrix}\pm a_{11} & a_{12}\\ a_{21} & a_{22}\end{bmatrix}$；$b$、$d$表示预设的参数值，且$x_1(k)\in[-d,d]$；$x_1(k)$、$x_2(k)$表示 Henon 混沌系统的两个状态值；$T$表示矩阵的转置；$E$表示可逆矩阵。

本申请实施例提供的一种数据加解密设备，包括存储器 201 和处理器 202，存储器 201 中存储有计算机程序，处理器 202 执行计算机程序时实现如下步骤：将目标数据的密钥信息转化为 Henon 混沌系统的状态值。

本申请实施例提供的一种数据加解密设备，包括存储器 201 和处理器 202，存储器 201 中存储有计算机程序，处理器 202 执行计算机程序时实现如下步骤：将目标数据的密钥信息转化为 Henon 混沌系统中A_i和/或输出矩阵的对应值。

本申请实施例提供的一种数据加解密设备，包括存储器 201 和处理器 202，存储器 201 中存储有计算机程序，处理器 202 执行计算机程序时实现如下步骤：将目标数据的密钥信息转化为 Henon 混沌系统中的b值。

本申请实施例提供的一种数据加解密设备，包括存储器 201 和处理器 202，存储器 201 中存储有计算机程序，处理器 202 执行计算机程序时实现如下步骤：

获取加密结果，其中，加密结果基于系统参数，通过 Henon 混沌系统的输出运算公式对目标数据进行运算得到，系统参数为将目标数据的密钥信息转化后得到的 Henon 混沌系统的参数；

获取系统参数；

基于系统参数对加密结果进行解密，得到目标数据。

本申请实施例提供的一种数据加解密设备，包括存储器 201 和处理器 202，存储器 201 中存储有计算机程序，处理器 202 执行计算机程序时实现如下步骤：通过解密公式，基于系统参数对加密结果进行解密，得到目标数据；

解密公式包括：

$$m(k)=\begin{bmatrix}D\\0\end{bmatrix}^{\dagger}\left(\begin{bmatrix}y(k)\\z(k)\end{bmatrix}-\begin{bmatrix}C\\E\end{bmatrix}\left(\sum_{i=1}^{2}\mu_i\left(\xi(k-1)\right)\left(A_i(0\ E^{-1})\begin{pmatrix}y(k-1)\\z(k-1)\end{pmatrix}\right)+b\right)\right);$$

$$\mu_1\left(\xi(k)\right)=\frac{1}{2}\left(1+\frac{\xi(k)}{d}\right);\quad \mu_2\left(\xi(k)\right)=\frac{1}{2}\left(1-\frac{\xi(k)}{d}\right);\quad \xi(k)=x_1(k);$$

其中，$m(k)$表示k时刻时的目标数据；D表示非奇异的直通矩阵；$y(k)$、$z(k)$表示加密结果；C表示 Henon 混沌系统的输出矩阵，$C=\begin{bmatrix}c_{11} & c_{12}\\ c_{21} & c_{22}\end{bmatrix}$；$E$表示可逆矩阵；$A_i=\begin{bmatrix}\pm a_{11} & a_{12}\\ a_{21} & a_{22}\end{bmatrix}$；$b$、$d$表示预设的参数值，且$x_1(k)\in[-d,d]$；$x_1(k)$表示 Henon 混沌系统的一个状态值；†表示矩阵的伪逆。

请参阅图 7，本申请实施例提供的另一种数据加解密设备中还可以包括：与处理器 202 连接的输入端口 203，用于传输外界输入的命令至处理器 202；与处理器 202 连接的显示单元 204，用于显示处理器 202 的处理结果至外界；与处理器 202 连接的通信模块 205，用于实现数据加解密设备与外界的通信。显示单元 204 可以为显示面板、激光扫描使显示器等；通信模块 205 所采用的通信方式包括但不局限于移动高清链接技术（Mobile High-Definition Link，MHL）、通用串行总线（Universal Serial Bus，USB）、高清多媒体接口（High Definition Multimedia Interface，HDMI）、无线连接：无线保真技术（Wireless Fidelity，WiFi）、蓝牙通信技术、低功耗蓝牙通信技术、基于 IEEE802.11s（Institute of Electrical an Electronics Engineers，电气与电子工程师协会）的通信技术。

参照图 8 所示，本申请实施例还提供了一种非易失性可读存储介质，非易失性可读存储介质 30 上存储有计算机程序 31，计算机程序 31 被处理器执行执行时实现如下步骤：

获取待加密的目标数据；

将目标数据的密钥信息转化为 Henon 混沌系统的系统参数；

基于系统参数，通过 Henon 混沌系统的输出运算公式对目标数据进行运算，得到目标数据的加密结果。

本申请实施例提供的一种非易失性可读存储介质，非易失性可读存储介质中存储有计算机程序，计算机程序被处理器执行时实现如下步骤：基于系统参数，通过 Henon 混沌系统的输出运算公式对目标数据进行运算，得到目标数据的加密结果；

Henon 混沌系统的输出运算公式包括：

$$y(k)=Cx(k)+Dm(k)\text{；}\quad z(k)=Ex(k)\text{；}$$

$$x(k+1)=\sum_{i=1}^{2}\mu_i\left(\xi(k)\right)\left(A_i x(k)\right)+b\text{；}$$

$$\mu_1\left(\xi(k)\right)=\frac{1}{2}\left(1+\frac{\xi(k)}{d}\right)\text{；}\quad \mu_2\left(\xi(k)\right)=\frac{1}{2}\left(1-\frac{\xi(k)}{d}\right)\text{；}\quad \xi(k)=x_1(k)\text{；}$$

$$x(k)=\begin{bmatrix}x_1(k) & x_2(k)\end{bmatrix}^T\text{；}$$

其中，$m(k)$表示k时刻时的目标数据；$y(k)$、$z(k)$表示加密结果；C表示 Henon 混沌系统的输出矩阵，$C=\begin{bmatrix}c_{11} & c_{12}\\ c_{21} & c_{22}\end{bmatrix}$；$D$表示非奇异的直通矩阵；$A_i=\begin{bmatrix}\pm a_{11} & a_{12}\\ a_{21} & a_{22}\end{bmatrix}$；$b$、$d$表示预设的参数值，且$x_1(k)\in[-d,d]$；$x_1(k)$、$x_2(k)$表示 Henon 混沌系统的两个状态值；$T$表示矩阵的转置；$E$表示可逆矩阵。

本申请实施例提供的一种非易失性可读存储介质，非易失性可读存储介质中存储有计算机程序，计算机程序被处理器执行时实现如下步骤：将目标数据的密钥信息转化为 Henon 混沌系统的状态值。

本申请实施例提供的一种非易失性可读存储介质，非易失性可读存储介质中存储有计算机程序，计算机程序被处理器执行时实现如下步骤：将目标数据的密钥信息转化为 Henon 混沌系统中A_i和/或输出矩阵的对应值。

本申请实施例提供的一种非易失性可读存储介质，非易失性可读存储介质中存储有计算机程序，计算机程序被处理器执行时实现如下步骤：将目标数据的密钥信息转化为 Henon 混沌系统中的b值。

本申请实施例提供的一种非易失性可读存储介质，非易失性可读存储介质中存储有计算机程序，计算机程序被处理器执行时实现如下步骤：

获取加密结果，其中，加密结果基于系统参数，通过 Henon 混沌系统的输出运算公式对目标数据进行运算得到，系统参数为将目标数据的密钥信息转化后得到的 Henon 混沌系统的参数；

获取系统参数；

基于系统参数对加密结果进行解密，得到目标数据。

本申请实施例提供的一种非易失性可读存储介质，非易失性可读存储介质中存储有计算机程序，计算机程序被处理器执行时实现如下步骤：通过解密公式，基于系统参数对加密结

果进行解密，得到目标数据；

解密公式包括：

$$m(k)=\begin{bmatrix}D\\0\end{bmatrix}^{\dagger}\left(\begin{bmatrix}y(k)\\z(k)\end{bmatrix}-\begin{bmatrix}C\\E\end{bmatrix}\left(\sum_{i=1}^{2}\mu_i(\xi(k-1))\left(A_i(0\ E^{-1})\begin{pmatrix}y(k-1)\\z(k-1)\end{pmatrix}\right)+b\right)\right)$$；

$$\mu_1(\xi(k))=\frac{1}{2}\left(1+\frac{\xi(k)}{d}\right)$$；$$\mu_2(\xi(k))=\frac{1}{2}\left(1-\frac{\xi(k)}{d}\right)$$；$$\xi(k)=x_1(k)$$；

其中，$m(k)$表示k时刻时的目标数据；D表示非奇异的直通矩阵；$y(k)$、$z(k)$表示加密结果；C表示 Henon 混沌系统的输出矩阵，$C=\begin{bmatrix}c_{11}&c_{12}\\c_{21}&c_{22}\end{bmatrix}$；$E$表示可逆矩阵；$A_i=\begin{bmatrix}\pm a_{11}&a_{12}\\a_{21}&a_{22}\end{bmatrix}$；$b$、$d$表示预设的参数值，且$x_1(k)\in[-d,d]$；$x_1(k)$表示 Henon 混沌系统的一个状态值；†表示矩阵的伪逆。

本申请所涉及的非易失性可读存储介质包括随机存储器（RAM）、内存、只读存储器（ROM）、电可编程 ROM、电可擦除可编程 ROM、寄存器、硬盘、可移动磁盘、CD-ROM 或技术领域内所公知的任意其它形式的存储介质。

本申请实施例提供的数据加解密系统、设备及非易失性可读存储介质中相关部分的说明请参见本申请实施例提供的数据加解密方法中对应部分的详细说明，在此不再赘述。另外，本申请实施例提供的上述技术方案中与现有技术中对应技术方案实现原理一致的部分并未详细说明，以免过多赘述。

还需要说明的是，在本文中，诸如第一和第二等之类的关系术语仅仅用来将一个实体或者操作与另一个实体或操作区分开来，而不一定要求或者暗示这些实体或操作之间存在任何这种实际的关系或者顺序。而且，术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含，从而使得包括一系列要素的过程、方法、物品或者设备不仅包括那些要素，而且还包括没有明确列出的其他要素，或者是还包括为这种过程、方法、物品或者设备所固有的要素。在没有更多限制的情况下，由语句“包括一个……”限定的要素，并不排除在包括要素的过程、方法、物品或者设备中还存在另外的相同要素。

对所公开的实施例的上述说明，使本领域技术人员能够实现或使用本申请。对这些实施例的多种修改对本领域技术人员来说将是显而易见的，本文中所定义的一般原理可以在不脱离本申请的精神或范围的情况下，在其它实施例中实现。因此，本申请将不会被限制于本文所示的这些实施例，而是要符合与本文所公开的原理和新颖特点相一致的最宽的范围。

权 利 要 求 书

1、一种数据加解密方法，其特征在于，包括：

获取待加密的目标数据；

将所述目标数据的密钥信息转化为Henon混沌系统的系统参数；

基于所述系统参数，通过所述 Henon 混沌系统的输出运算公式对所述目标数据进行运算，得到所述目标数据的加密结果。

2、根据权利要求 1 所述的方法，其特征在于，所述基于所述系统参数，通过所述 Henon 混沌系统的输出运算公式对所述目标数据进行运算，得到所述目标数据的加密结果，包括：

基于所述系统参数，通过所述 Henon 混沌系统的输出运算公式对所述目标数据进行运算，得到所述目标数据的所述加密结果；

所述Henon混沌系统的输出运算公式包括：

$y(k)=Cx(k)+Dm(k)$；$z(k)=Ex(k)$；

$$x(k+1)=\sum_{i=1}^{2}\mu_i(\xi(k))(A_i x(k))+b$$；

$\mu_1(\xi(k))=\frac{1}{2}\left(1+\frac{\xi(k)}{d}\right)$；$\mu_2(\xi(k))=\frac{1}{2}\left(1-\frac{\xi(k)}{d}\right)$；$\xi(k)=x_1(k)$；

$x(k)=\begin{bmatrix}x_1(k) & x_2(k)\end{bmatrix}^T$；

其中，$m(k)$表示k时刻时的所述目标数据；$y(k)$、$z(k)$表示所述加密结果；C表示所述 Henon 混沌系统的输出矩阵，$C=\begin{bmatrix}c_{11} & c_{12}\\ c_{21} & c_{22}\end{bmatrix}$；$D$表示非奇异的直通矩阵；$A_i=\begin{bmatrix}\pm a_{11} & a_{12}\\ a_{21} & a_{22}\end{bmatrix}$；$b$、$d$表示预设的参数值，且$x_1(k)\in[-d,d]$；$x_1(k)$、$x_2(k)$表示所述Henon混沌系统的两个状态值；$T$表示矩阵的转置；$E$表示可逆矩阵。

3、根据权利要求 2 所述的方法，其特征在于，所述目标数据包括文本数据和图像数据，所述获取待加密的目标数据，包括：

获取待加密的文本数据和/或图像数据。

4、根据权利要求 3 所述的方法，其特征在于，所述将所述目标数据的密钥信息转化为Henon混沌系统的系统参数，包括：

通过将所述文本数据和/或所述图像数据的密钥信息映射为所述 Henon 混沌系统的系统参数，对所述密钥信息进行加密处理。

5、根据权利要求 4 所述的方法，其特征在于，所述通过将所述文本数据和/或所述图像数据的密钥信息映射为所述 Henon 混沌系统的系统参数，对所述密钥信息进行加密处理，包括：

按照预设参数类型和预设参数数量将所述文本数据和/或所述图像数据的密钥信息映射为所述 Henon 混沌系统的系统参数，对所述密钥信息进行加密处理。

6、根据权利要求 2 所述的方法，其特征在于，所述将所述目标数据的密钥信息转化为 Henon 混沌系统的系统参数，包括：

将所述目标数据的密钥信息转化为所述 Henon 混沌系统的状态值。

7、根据权利要求 2 所述的方法，其特征在于，所述将所述目标数据的密钥信息转化为 Henon 混沌系统的系统参数，包括：

将所述目标数据的密钥信息转化为所述 Henon 混沌系统中 A_i 和/或所述输出矩阵的对应值。

8、根据权利要求 7 所述的方法，其特征在于，所述将所述目标数据的密钥信息转化为所述 Henon 混沌系统中 A_i 和/或所述输出矩阵的对应值，包括：

将所述目标数据的密钥信息转化为所述 Henon 混沌系统中 A_i 的 a_{11}、a_{12}、a_{21}、a_{22} 的一个或多个；

和/或，将所述目标数据的密钥信息转化为所述 Henon 混沌系统中所述输出矩阵的对应值。

9、根据权利要求 7 所述的方法，其特征在于，所述将所述目标数据的密钥信息转化为所述 Henon 混沌系统中所述输出矩阵的对应值，包括：

将所述目标数据的密钥信息转化为所述 Henon 混沌系统中所述输出矩阵的 c_{11}、c_{12}、c_{21}、c_{22} 的一个或多个。

10、根据权利要求 2 所述的方法，其特征在于，所述将所述目标数据的密钥信息转化为 Henon 混沌系统的系统参数，包括：

将所述目标数据的密钥信息转化为所述 Henon 混沌系统中的 b 值。

11、一种数据加解密方法，其特征在于，包括：

获取加密结果，其中，所述加密结果基于系统参数，通过 Henon 混沌系统的输出运算公式对目标数据进行运算得到，所述系统参数为将所述目标数据的密钥信息转化后得到的所述 Henon 混沌系统的参数；

获取所述系统参数；

基于所述系统参数对所述加密结果进行解密，得到所述目标数据。

12、根据权利要求 11 所述的方法，其特征在于，所述基于所述系统参数对所述加密结果进行解密，得到所述目标数据，包括：

通过解密公式，基于所述系统参数对所述加密结果进行解密，得到所述目标数据；

所述解密公式包括：

$$m(k)=\begin{bmatrix}D\\0\end{bmatrix}^{\dagger}\left(\begin{bmatrix}y(k)\\z(k)\end{bmatrix}-\begin{bmatrix}C\\E\end{bmatrix}\left(\sum_{i=1}^{2}\mu_i(\xi(k-1))\left(A_i(0\ E^{-1})\begin{pmatrix}y(k-1)\\z(k-1)\end{pmatrix}\right)+b\right)\right)$$；

$$\mu_1(\xi(k))=\frac{1}{2}\left(1+\frac{\xi(k)}{d}\right)$$；$$\mu_2(\xi(k))=\frac{1}{2}\left(1-\frac{\xi(k)}{d}\right)$$；$$\xi(k)=x_1(k)$$；

其中，$m(k)$表示k时刻时的所述目标数据；D表示非奇异的直通矩阵；$y(k)$、$z(k)$表示所述加密结果；C表示所述 Henon 混沌系统的输出矩阵，$C=\begin{bmatrix}c_{11}&c_{12}\\c_{21}&c_{22}\end{bmatrix}$；$E$表示可逆矩阵；$A_i=\begin{bmatrix}\pm a_{11}&a_{12}\\a_{21}&a_{22}\end{bmatrix}$；$b$、$d$表示预设的参数值，且$x_1(k)\in[-d,d]$；$x_1(k)$表示所述 Henon 混沌系统的一个状态值；$\dagger$表示矩阵的伪逆。

13、根据权利要求 12 所述的方法，其特征在于，所述系统参数包括所述 Henon 混沌系统的状态值，所述状态值包括$x_1(k)$，所述获取所述系统参数，包括：

获取所述 Henon 混沌系统的状态值中的$x_1(k)$。

14、根据权利要求 12 所述的方法，其特征在于，所述系统参数包括所述 Henon 混沌系统中A_i，所述获取所述系统参数，包括：

获取所述 Henon 混沌系统中A_i的a_{11}、a_{12}、a_{21}、a_{22}的一个或多个。

15、根据权利要求 12 所述的方法，其特征在于，所述系统参数包括所述 Henon 混沌系统中所述输出矩阵的对应值，所述获取所述系统参数，包括：

获取所述 Henon 混沌系统中所述输出矩阵的对应值的c_{11}、c_{12}、c_{21}、c_{22}的一个或多个。

16、根据权利要求 12 所述的方法，其特征在于，所述系统参数包括所述预设的参数值，所述预设的参数值包括b，所述获取所述系统参数，包括：

获取所述 Henon 混沌系统中的b值。

17、根据权利要求 11 所述的方法，其特征在于，所述目标数据包括文本数据和图像

数据，所述基于所述系统参数对所述加密结果进行解密，得到所述目标数据，包括：

基于所述系统参数对所述加密结果进行解密，获得解密后的文本数据和/或图像数据。

18、一种数据加解密系统，其特征在于，包括：

第一获取模块，用于获取待加密的目标数据；

第一转化模块，用于将所述目标数据的密钥信息转化为 Henon 混沌系统的系统参数；

第一加密模块，用于基于所述系统参数，通过所述 Henon 混沌系统的输出运算公式对所述目标数据进行运算，得到所述目标数据的加密结果。

19、一种数据加解密设备，其特征在于，包括：

存储器，用于存储计算机程序；

处理器，用于执行所述计算机程序时实现如权利要求 1 至 17 任一项所述数据加解密方法的步骤。

20、一种非易失性可读存储介质，其特征在于，所述非易失性可读存储介质中存储有计算机程序，所述计算机程序被处理器执行时实现如权利要求 1 至 17 任一项所述数据加解密方法的步骤。

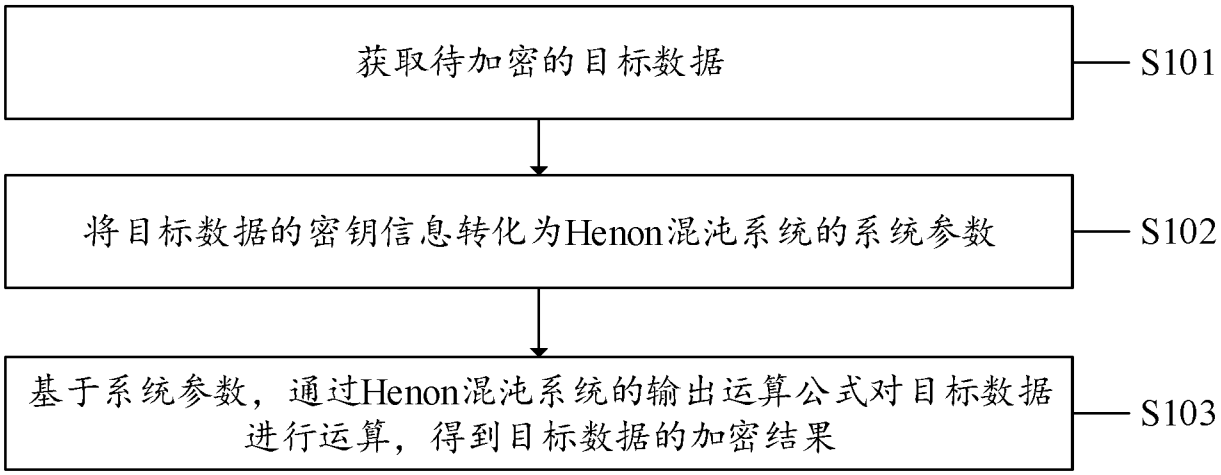
获取待加密的目标数据
S101
将目标数据的密钥信息转化为Henon混沌系统的系统参数
S102
基于系统参数，通过Henon混沌系统的输出运算公式对目标数据进行运算，得到目标数据的加密结果
S103

图 1

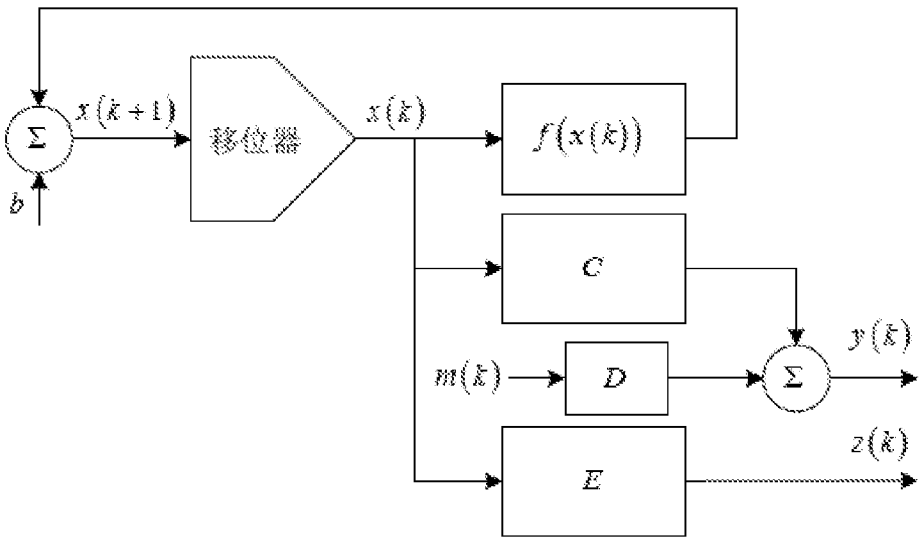
Σ
x(k+1)
移位器
x(k)
f(x(k))
b
C
m(k)
D
Σ
y(k)
E
z(k)

图 2

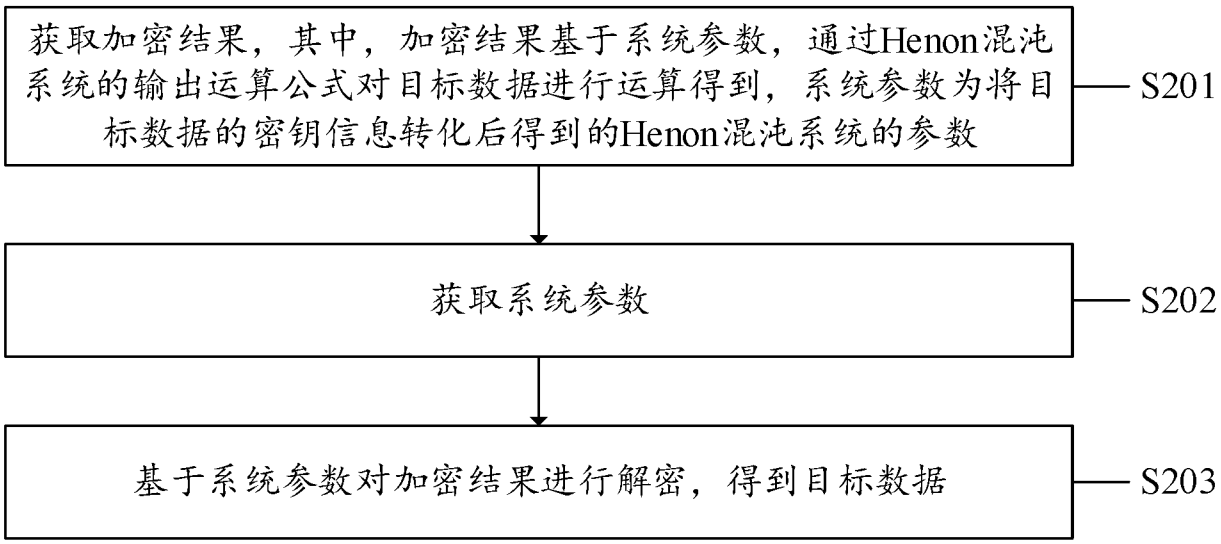
获取加密结果，其中，加密结果基于系统参数，通过Henon混沌系统的输出运算公式对目标数据进行运算得到，系统参数为将目标数据的密钥信息转化后得到的Henon混沌系统的参数
S201
获取系统参数
S202
基于系统参数对加密结果进行解密，得到目标数据
S203

图 3

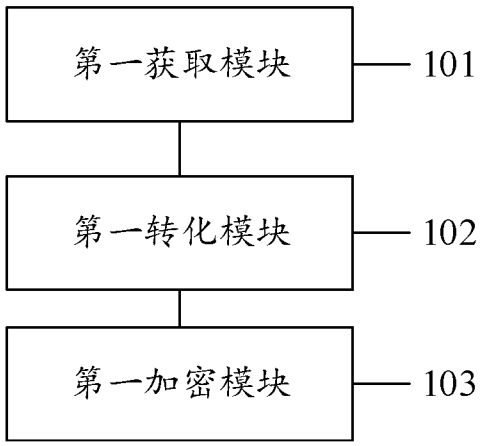
第一获取模块
101
第一转化模块
102
第一加密模块
103

图 4

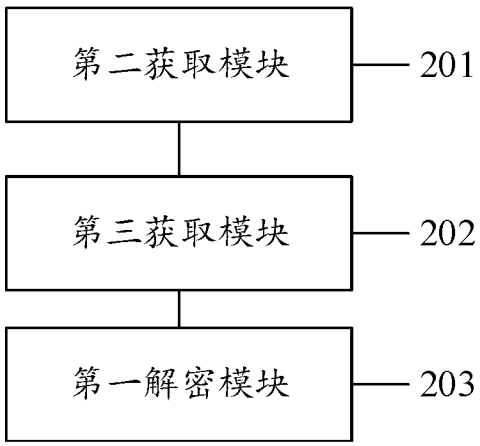
第二获取模块
201
第三获取模块
202
第一解密模块
203

图 5

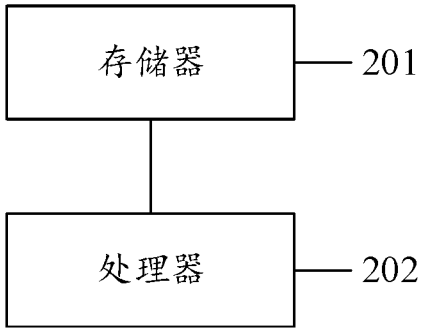
存储器
201
处理器
202

图 6

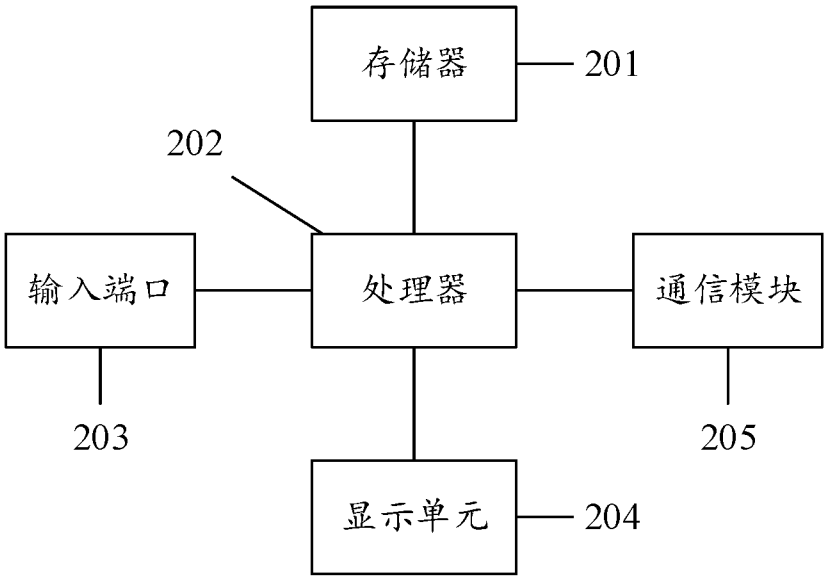
存储器
201
202
输入端口
处理器
通信模块
203
205
显示单元
204

图 7

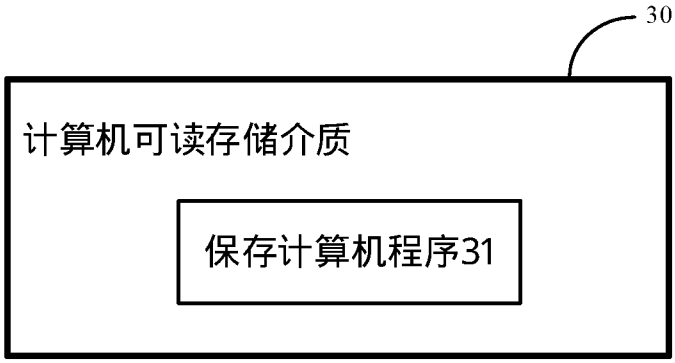

图 8

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2022/138774

A. CLASSIFICATION OF SUBJECT MATTER

G06F21/60(2013.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC:G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNKI, CNTXT, DWPI, ENTXT, ENTXTC, WPABSC: 参数, 公式, 混沌, 加密, 矩阵, 可逆, 目标, 输出, 图像, 直通, 置乱, 转置, 状态, henon, parameter, formula, chaos, encryption, matrix, reversible, target, output, image, pass-through, shuffle, transpose, state.

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	CN 107896144 A (CPC CENTRAL COMMITTEE GENERAL OFFICE ELECTRONICS SCIENCE & TECHNOLOGY INSTITUTE) 10 April 2018 (2018-04-10) claim 1, description, paragraphs 44-62, and figures 1-2	1, 11, 17-20
Y	CN 107094072 A (GUANGDONG UNIVERSITY OF TECHNOLOGY) 25 August 2017 (2017-08-25) claim 1, and description, paragraphs 29-42	1, 11, 17-20
Y	CN 109391463 A (SANECHIPS TECHNOLOGY CO., LTD.) 26 February 2019 (2019-02-26) description, paragraphs 60-181	1, 11, 17-20
PX	CN 114117502 A (SUZHOU INSPUR INTELLIGENT TECHNOLOGY CO., LTD.) 01 March 2022 (2022-03-01) claims 1-10, and description, paragraphs 19-40	1-20
A	US 2017085367 A1 (THE BOARD OF REGENTS OF THE UNIVERSITY OF TEXAS SYSTEM, AUSTIN, TX(US)) 23 March 2017 (2017-03-23) entire document	1-20

☐ Further documents are listed in the continuation of Box C. ☑ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"D" document cited by the applicant in the international application
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
13 February 2023	**20 February 2023**

Name and mailing address of the ISA/CN	Authorized officer
China National Intellectual Property Administration (ISA/CN) **China No. 6, Xitucheng Road, Jimenqiao, Haidian District, Beijing 100088**	
Facsimile No. **(86-10)62019451**	Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2022/138774

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN 107896144 A	10 April 2018	None	
CN 107094072 A	25 August 2017	None	
CN 109391463 A	26 February 2019	None	
CN 114117502 A	01 March 2022	None	
US 2017085367 A1	23 March 2017	WO 2016161134 A1	06 October 2016
		US 9853809 B2	26 December 2017

国际检索报告

国际申请号
PCT/CN2022/138774

A. 主题的分类

G06F21/60(2013.01)i

按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

IPC:G06F

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称，和使用的检索词（如使用））

CNKI,CNTXT,DWPI,ENTXT,ENTXTC,WPABSC:参数,公式,混沌,加密,矩阵,可逆,目标,输出,图像,直通,置乱,转置,状态,henon,parameter, formula, chaos, encryption, matrix, reversible,target,output,image, pass-through, shuffle, transpose, state。

C. 相关文件

类 型*	引用文件，必要时，指明相关段落	相关的权利要求
Y	CN 107896144 A (中共中央办公厅电子科技学院) 2018年4月10日 (2018-04-10) 权利要求1、说明书第44-62段、图1-2	1、11、17-20
Y	CN 107094072 A (广东工业大学) 2017年8月25日 (2017-08-25) 权利要求1、说明书第29-42段	1、11、17-20
Y	CN 109391463 A (深圳市中兴微电子技术有限公司) 2019年2月26日 (2019-02-26) 说明书第60-181段	1、11、17-20
PX	CN 114117502 A (苏州浪潮智能科技有限公司) 2022年3月1日 (2022-03-01) 权利要求1-10，说明书第19-40段	1-20
A	US 2017085367 A1 (The Board of Regents of The University of Texas System,Austin,TX(US)) 2017年3月23日 (2017-03-23) 全文	1-20

☐ 其余文件在C栏的续页中列出。

☑ 见同族专利附件。

* 引用文件的具体类型：

"A" 认为不特别相关的表示了现有技术一般状态的文件

"D" 申请人在国际申请中引证的文件

"E" 在国际申请日的当天或之后公布的在先申请或专利

"L" 可能对优先权要求构成怀疑的文件，或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件（如具体说明的）

"O" 涉及口头公开、使用、展览或其他方式公开的文件

"P" 公布日先于国际申请日但迟于所要求的优先权日的文件

"T" 在申请日或优先权日之后公布，与申请不相抵触，但为了理解发明之理论或原理的在后文件

"X" 特别相关的文件，单独考虑该文件，认定要求保护的发明不是新颖的或不具有创造性

"Y" 特别相关的文件，当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时，要求保护的发明不具有创造性

"&" 同族专利的文件

国际检索实际完成的日期	国际检索报告邮寄日期
2023年2月13日	2023年2月20日

ISA/CN的名称和邮寄地址

中国国家知识产权局
中国北京市海淀区蓟门桥西土城路6号 100088

传真号 (86-10)62019451

受权官员

刘琪

电话号码 (+86) 62411377

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2022/138774

检索报告引用的专利文件			公布日 (年/月/日)	同族专利			公布日 (年/月/日)
CN	107896144	A	2018年4月10日	无			
CN	107094072	A	2017年8月25日	无			
CN	109391463	A	2019年2月26日	无			
CN	114117502	A	2022年3月1日	无			
US	2017085367	A1	2017年3月23日	WO	2016161134	A1	2016年10月6日
				US	9853809	B2	2017年12月26日