(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 115913552 B
(45)授权公告日 2023.05.16

(21)申请号 202310014772.X
(22)申请日 2023.01.06
(65)同一申请的已公布的文献号
申请公布号 CN 115913552 A
(43)申请公布日 2023.04.04
(73)专利权人 山东卓朗检测股份有限公司
地址 272000 山东省济宁市任城区金宇路18号谢营科技大厦15楼1506-1509
(72)发明人 李芬 公延廷 王磊 刘浩 吴沧海 于夏夏
(74)专利代理机构 济宁仁礼信知识产权代理事务所(普通合伙) 37383
专利代理师 王更星
(51)Int.Cl.
H04L 9/08(2006.01)
(56)对比文件
AU 2016200782 B1,2016.05.05
AU 2016210741 A1,2016.09.01
AU 2016222453 A1,2016.09.22
AU 2019100608 A4,2019.07.11
CN 101755274 A,2010.06.23
CN 103098101 A,2013.05.08
CN 103473733 A,2013.12.25
CN 108111710 A,2018.06.01
US 2022091275 A1,2022.03.24
SUN Lili;CAO Yunhe;WU Wenhua;LIU Yutao.A multi-target tracking algorithm based on Gaussian mixture model.Journal of Systems Engineering and Electronics.2020,(第03期),全文.
同鸣;吴扬成;张建龙;栾英姿.一种面向AVS的视频内容多重水印框架.西安电子科技大学学报.2013,(第04期),全文.
审查员 郭珩

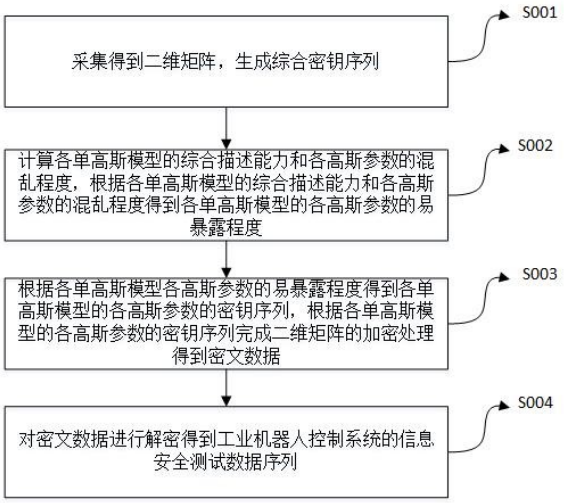
权利要求书2页 说明书10页 附图1页

(54)发明名称

一种工业机器人控制系统的信息安全测试数据处理方法

(57)摘要

本发明涉及安全存储领域,具体涉及一种工业机器人控制系统的信息安全测试数据处理方法,该方法获得二维矩阵以及二维矩阵的混合高斯模型,生成综合密钥序列;根据二维矩阵得到多个区域;根据各单高斯模型及多个区域得到各单高斯模型的综合描述能力;根据各单高斯模型的综合描述能力和各高斯参数的混乱程度得到各单高斯模型的各高斯参数的易暴露程度;根据易暴露程度和综合密钥序列的各密钥值的破解难度得到各单高斯模型的各高斯参数的密钥序列;根据各单高斯模型的各高斯参数的密钥序列的密钥序列得到密文数据;将密文数据存储在服务器中,从而实现工业机器人控制系统的信息安全测试数据的安全存储。



CN 115913552 B

1.一种工业机器人控制系统的信息安全测试数据处理方法,其特征在于,所述方法包括:

采集数据得到二维矩阵,生成综合密钥序列;

获取二维矩阵的混合高斯模型,所述混合高斯模型包含多个单高斯模型;

根据混合高斯模型得到二维矩阵的第一主区域分布面积,根据第一主区域分布面积将二维矩阵划分得到多个区域;根据各单高斯模型对多个区域的描述情况得到各单高斯模型的综合描述能力;根据混合高斯模型的高斯参数得到各高斯参数的混乱程度;根据各单高斯模型的综合描述能力和各高斯参数的混乱程度得到各单高斯模型的各高斯参数的易暴露程度;根据易暴露程度得到各单高斯模型的各高斯参数的加密复杂性,根据综合密钥序列得到各密钥值的破解难度,根据各单高斯模型的各高斯参数的加密复杂性和各密钥值的破解难度得到各单高斯模型的各高斯参数的密钥序列;根据各单高斯模型的各高斯参数的密钥序列对二维矩阵进行加密处理得到密文数据;

将密文数据存储在服务器中。

2.如权利要求1所述的一种工业机器人控制系统的信息安全测试数据处理方法,其特征在于,所述根据混合高斯模型得到二维矩阵的第一主区域分布面积,包括的具体步骤为:

获取混合高斯模型中各单高斯模型的协方差矩阵,根据各单高斯模型的协方差矩阵得到各单高斯模型的主分布面积:

$$S_i = \pi * \frac{9}{4} * ||U_i||$$

其中,U_i表示混合高斯模型的第i个单高斯模型的协方差矩阵,$||\cdot||$表示矩阵的L_2范数,S_i表示混合高斯模型的第i个单高斯模型的主分布区域面积;

根据混合高斯模型的所有单高斯模型的主分布区域面积得到二维矩阵的第一主分布区域面积。

3.如权利要求1所述的一种工业机器人控制系统的信息安全测试数据处理方法,其特征在于,所述根据各单高斯模型对多个区域的描述情况得到各单高斯模型的综合描述能力,包括的具体步骤为:

获取各单高斯模型在各区域的积分,根据各单高斯模型在各区域的积分得到各单高斯模型在对区域的描述能力:

$$M1_{ik} = \frac{F_{ik}}{\sum_{i=1}^{I} F_{ik}}$$

其中,F_{ik}表示第i个单高斯模型在第k个区域的积分,I表示混合高斯模型中单高斯模型的总个数,$M1_{ik}$表示第i个单高斯模型对第k个区域的描述能力;

根据各单高斯模型对各区域的描述能力得到各单高斯模型的综合描述能力为:

$$M_i = \max_{1 \le k \le K} (M1_{ik})$$

其中,$M1_{ik}$表示第i个单高斯模型对第k个区域的描述能力,K表示二维矩阵中划分得到的区域个数,M_i表示第i个单高斯模型的综合描述能力,$\max()$表示获取最大值的函数。

4.如权利要求1所述的一种工业机器人控制系统的信息安全测试数据处理方法,其特征在于,所述根据混合高斯模型的高斯参数得到各高斯参数的混乱程度,包括的具体步骤为:

获取混合高斯模型中所有单高斯模型的各高斯参数组成的集合，记为二维矩阵的各高斯参数集合，根据二维矩阵的各高斯参数集合得到各高斯参数的混乱程度。

5.如权利要求1所述的一种工业机器人控制系统的信息安全测试数据处理方法，其特征在于，所述根据综合密钥序列得到各密钥值的破解难度，包括的具体步骤为：

获取综合密钥序列的混合高斯模型，所述综合密钥序列的混合高斯模型包含多个单高斯模型，将综合密钥序列的混合高斯模型中每个单高斯模型称为综合密钥序列的单高斯模型；将综合密钥序列中各元素称为综合密钥序列的各密钥值；根据综合密钥序列的各单高斯模型得到综合密钥序列的各密钥值的拟合值，根据综合密钥序列的所有单高斯模型得到综合密钥序列的各密钥值的拟合值集合，根据各密钥值的拟合值集合得到各密钥值的破解难度。

6.如权利要求1所述的一种工业机器人控制系统的信息安全测试数据处理方法，其特征在于，所述根据各单高斯模型的各高斯参数的加密复杂性和各密钥值的破解难度得到各单高斯模型的各高斯参数的密钥序列，包括的具体步骤为：

获取各单高斯模型的各高斯参数的加密复杂性作为各单高斯模型的各高斯参数的第一位置，在综合密钥序列中获取第一位置处的密钥值记为第一密钥值，将第一密钥值作为各单高斯模型的各高斯参数的中间密钥序列，根据中间密钥序列中所有密钥值的破解难度得到第一累加和，根据各单高斯模型的各高斯参数的加密复杂性与第一累加和对中间密钥序列进行判定，当第一累加和大于各单高斯模型的各高斯参数的加密复杂性时，将中间密钥序列作为各单高斯模型的各高斯参数的密钥序列，当第一累加和小于各单高斯模型的各高斯参数的加密复杂性时，将第一密钥值作为第二位置，将综合密钥序列中第二位置处的密钥值记为第二密钥值，将第一密钥值与第二密钥值构成中间密钥序列，根据中间密钥序列中所有密钥值的破解难度累加和得到第二累加和，根据各单高斯模型的各高斯参数的加密复杂性与第二累加和对中间密钥序列进行判定，当第二累加和大于各单高斯模型的各高斯参数的加密复杂性时，将中间密钥序列作为各单高斯模型的各高斯参数的密钥序列，当第二累加和小于各单高斯模型的各高斯参数的加密复杂性时，将第二密钥值作为第三位置，将综合密钥序列中第三位置处的密钥值记为第三密钥值，将第一密钥值、第二密钥值和第三密钥值构成中间密钥序列，以此类推，直至得到各单高斯模型的各高斯参数的密钥序列。

7.如权利要求1所述的一种工业机器人控制系统的信息安全测试数据处理方法，其特征在于，所述根据各单高斯模型的各高斯参数的密钥序列对二维矩阵进行加密处理得到密文数据，包括的具体步骤为：

根据各单高斯模型的各高斯参数的密钥序列中各密钥值得到各密钥值的第一位数和，根据各单高斯模型的各高斯参数的密钥序列中所有密钥值的第一位数和得到各单高斯模型的各高斯参数的第二位数和；根据各单高斯模型的各高斯参数和第二位数和得到各单高斯模型的各高斯参数的调整后参数；根据各单高斯模型的所有高斯参数的调整后参数得到各单高斯模型的调整后单高斯模型，根据所有单高斯模型的调整后单高斯模型得到二维矩阵的调整后混合高斯模型；根据二维矩阵的调整后混合高斯模型得到加密矩阵；根据加密矩阵得到密文数据。

一种工业机器人控制系统的信息安全测试数据处理方法

技术领域

[0001] 本申请涉及安全存储领域，具体涉及一种工业机器人控制系统的信息安全测试数据处理方法。

背景技术

[0002] 随着智能化技术的发展，工业机器人在工业现场的应用越发广泛，工业机器人的控制系统的信息作为工业机器人的技术核心，一旦工业机器人的控制系统信息被竞争者窃取利用，很容易导致技术丢失或导致工业机器人的失去控制，进而造成企业的经济损失。为了防止该问题的发生，需对企业的工业机器人控制系统的信息进行加密保护，对工业机器人控制系统的信息的加密数据进行存储。

[0003] 当入侵者对密文进行破解时，很容易将数据的统计规律作为突破点来对密文进行暴力破解。由于复杂的密钥在后续维护过程中所需成本较大，因而在进行数据加密时需分析数据的统计特征来对不同的数据分配不同复杂度的密钥，对于统计特征明显的数据需要利用复杂的密钥来对该数据进行加密，从而防止入侵者利用该统计特征破解出密钥得到解密数据，对于统计特征不明显的数据需要利用简单的密钥来对该数据加密，从而降低加密的复杂性，因而针对此来设计一种工业机器人控制系统的信息安全测试数据处理方法。

发明内容

[0004] 为了解决上述技术问题，本发明提供一种工业机器人控制系统的信息安全测试数据处理方法，所述方法包括：

[0005] 采集数据得到二维矩阵，生成综合密钥序列；

[0006] 获取二维矩阵的混合高斯模型，所述混合高斯模型包含多个单高斯模型；

[0007] 根据混合高斯模型得到二维矩阵的第一主区域分布面积，根据第一主区域分布面积将二维矩阵划分得到多个区域；根据各单高斯模型对多个区域的描述情况得到各单高斯模型的综合描述能力；根据混合高斯模型的高斯参数得到各高斯参数的混乱程度；根据各单高斯模型的综合描述能力和各高斯参数的混乱程度得到各单高斯模型的各高斯参数的易暴露程度；根据易暴露程度得到各单高斯模型的各高斯参数的加密复杂性，根据综合密钥序列得到各密钥值的破解难度，根据各单高斯模型的各高斯参数的加密复杂性和各密钥值的破解难度得到各单高斯模型的各高斯参数的密钥序列；根据各单高斯模型的各高斯参数的密钥序列对二维矩阵进行加密处理得到密文数据；

[0008] 将密文数据存储在服务器中。

[0009] 优选的，所述根据混合高斯模型得到二维矩阵的第一主区域分布面积，包括的具体步骤为：

[0010] 获取混合高斯模型中各单高斯模型的协方差矩阵，根据各单高斯模型的协方差矩阵得到各单高斯模型的主分布面积：

[0011] $$S_i = \pi * \frac{9}{4} * ||U_i||$$

[0012] 其中，U_i表示混合高斯模型的第i个单高斯模型的协方差矩阵，$||\cdot||$表示矩阵的L_2范数，S_i表示混合高斯模型的第i个单高斯模型的主分布区域面积；

[0013] 根据混合高斯模型的所有单高斯模型的主分布区域面积得到二维矩阵的第一主分布区域面积。

[0014] 优选的，所述根据各单高斯模型对多个区域的描述情况得到各单高斯模型的综合描述能力，包括的具体步骤为：

[0015] 获取各单高斯模型在各区域的积分，根据各单高斯模型在各区域的积分得到各单高斯模型在对区域的描述能力：

[0016] $$M1_{ik} = \frac{F_{ik}}{\sum_{i=1}^{I} F_{ik}}$$

[0017] 其中，F_{ik}表示第i个单高斯模型在第k个区域的积分，I表示混合高斯模型中单高斯模型的总个数，$M1_{ik}$表示第i个单高斯模型对第k个区域的描述能力；

[0018] 根据各单高斯模型对各区域的描述能力得到各单高斯模型的综合描述能力为：

[0019] $$M_i = \max_{1 \le k \le K} (M1_{ik})$$

[0020] 其中，$M1_{ik}$表示第i个单高斯模型对第k个区域的描述能力，K表示二维矩阵中划分得到的区域个数，M_i表示第i个单高斯模型的综合描述能力。

[0021] 优选的，所述根据混合高斯模型的高斯参数得到各高斯参数的混乱程度，包括的具体步骤为：

[0022] 获取混合高斯模型中所有单高斯模型的各高斯参数组成的集合，记为二维矩阵的各高斯参数集合，根据二维矩阵的各高斯参数集合得到各高斯参数的混乱程度。

[0023] 优选的，所述根据综合密钥序列得到各密钥值的破解难度，包括的具体步骤为：

[0024] 获取综合密钥序列的混合高斯模型，所述综合密钥序列的混合高斯模型包含多个单高斯模型，将综合密钥序列的混合高斯模型中每个单高斯模型称为综合密钥序列的单高斯模型；将综合密钥序列中各元素称为综合密钥序列的各密钥值；根据综合密钥序列的各单高斯模型得到综合密钥序列的各密钥值的拟合值，根据综合密钥序列的所有单高斯模型得到综合密钥序列的各密钥值的拟合值集合，根据各密钥值的拟合值集合得到各密钥值的破解难度。

[0025] 优选的，所述根据各单高斯模型的各高斯参数的加密复杂性和各密钥值的破解难度得到各单高斯模型的各高斯参数的密钥序列，包括的具体步骤为：

[0026] 获取各单高斯模型的各高斯参数的加密复杂性作为各单高斯模型的各高斯参数的第一位置，在综合密钥序列中获取第一位置处的密钥值记为第一密钥值，将第一密钥值作为各单高斯模型的各高斯参数的中间密钥序列，根据中间密钥序列中所有密钥值的破解难度得到第一累加和，根据各单高斯模型的各高斯参数的加密复杂性与第一累加和对中间

密钥序列进行判定，当第一累加和大于各单高斯模型的各高斯参数的加密复杂性时，将中间密钥序列作为各单高斯模型的各高斯参数的密钥序列，当第一累加和小于各单高斯模型的各高斯参数的加密复杂性时，将第一密钥值作为第二位置，将综合密钥序列中第二位置处的密钥值记为第二密钥值，将第一密钥值与第二密钥值构成中间密钥序列，根据中间密钥序列中所有密钥值的破解难度累加和得到第二累加和，根据各单高斯模型的各高斯参数的加密复杂性与第二累加和对中间密钥序列进行判定，当第二累加和大于各单高斯模型的各高斯参数的加密复杂性时，将中间密钥序列作为各单高斯模型的各高斯参数的密钥序列，当第二累加和小于各单高斯模型的各高斯参数的加密复杂性时，将第二密钥值作为第三位置，将综合密钥序列中第三位置处的密钥值记为第三密钥值，将第一密钥值、第二密钥值和第三密钥值构成中间密钥序列，以此类推，直至得到各单高斯模型的各高斯参数的密钥序列。

[0027] 优选的，所述根据各单高斯模型的各高斯参数的密钥序列对二维矩阵进行加密处理得到密文数据，包括的具体步骤为：

[0028] 根据各单高斯模型的各高斯参数的密钥序列中各密钥值得到各密钥值的第一位数和，根据各单高斯模型的各高斯参数的密钥序列中所有密钥值的第一位数和得到各单高斯模型的各高斯参数的第二位数和；根据各单高斯模型的各高斯参数和第二位数和得到各单高斯模型的各高斯参数的调整后参数；根据各单高斯模型的所有高斯参数的调整后参数得到各单高斯模型的调整后单高斯模型，根据所有单高斯模型的调整后单高斯模型得到二维矩阵的调整后混合高斯模型；根据二维矩阵的调整后混合高斯模型得到加密矩阵；根据加密矩阵得到密文数据。

[0029] 本发明实施例至少具有如下有益效果：获得二维矩阵以及二维矩阵的混合高斯模型，通过分析混合高斯模型中各单高斯的主分布区域得到各单高斯模型的第一主分布区域面积，根据各单高斯模型的第一主分布区域面积得到二维矩阵的多个区域，根据各单高斯模型对各区域的描述情况得到各单高斯模型的综合描述能力；计算混合高斯模型中各高斯参数的混乱程度，结合各单高斯模型的综合描述能力和各高斯参数的混乱程度得到各单高斯模型各高斯参数的易暴露程度。通过各单高斯模型的综合描述能力来反应二维矩阵具有各单高斯模型的统计特征的明显情况，当各单高斯模型的综合描述能力越大时，说明该二维矩阵具有该单高斯模型的统计特征越明显，为了防止加密后的密文数据后泄露这种统计特征，因而需给予该单高斯模型一个较复杂的密钥，通过各单高斯模型的各高斯参数的易暴露程度来说明各单高斯模型的各高斯参数的易暴露情况，该值越大说明该单高斯模型的高斯参数越容易泄露，因而需给该单高斯模型的各参数分配一个复杂的密钥，从而使得加密得到的密文数据安全性更强。

[0030] 根据各单高斯模型的各高斯参数的易暴露程度得到加密复杂性，获得综合密钥序列的混合高斯模型，根据综合密钥序列的混合高斯模型得到综合密钥序列中各密钥值的破解难度，根据各单高斯模型的各高斯参数的加密复杂性和各密钥值的破解难度得到各单高斯模型的各高斯参数的密钥序列，根据各单高斯模型的各高斯参数的密钥序列对二维矩阵进行加密得到密文数据，实现给不同易暴露程度的单高斯模型的各高斯参数分配不同复杂的密钥序列，从而达到对二维矩阵的不同数据进行不同复杂程度的加密，再保障去除二维矩阵中统计特征的同时还能提高加密效率。

附图说明

[0031] 为了更清楚地说明本发明实施例或现有技术中的技术方案和优点，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的介绍，显而易见地，下面描述中的附图仅仅是本发明的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其它附图。

[0032] 图1为本发明提供的一种工业机器人控制系统的信息安全测试数据处理方法的流程图。

具体实施方式

[0033] 为了更进一步阐述本发明为达成预定发明目的所采取的技术手段及功效，以下结合附图及较佳实施例，对依据本发明提出的一种工业机器人控制系统的信息安全测试数据处理方法，其具体实施方式、结构、特征及其功效，详细说明如下。在下述说明中，不同的“一个实施例”或“另一个实施例”指的不一定是同一实施例。此外，一或多个实施例中的特定特征、结构或特点可由任何合适形式组合。

[0034] 除非另有定义，本文所使用的所有的技术和科学术语与属于本发明的技术领域的技术人员通常理解的含义相同。

[0035] 下面结合附图具体的说明本发明所提供的一种工业机器人控制系统的信息安全测试数据处理方法的具体方案。

[0036] 请参阅图1，其示出了本发明一个实施例提供的一种工业机器人控制系统的信息安全测试数据处理方法的步骤流程图，该方法包括以下步骤：

[0037] 步骤S001，采集得到二维矩阵，生成综合密钥序列。

[0038] 1、获取工业机器人控制系统的信息安全测试数据序列：

[0039] 为了防止工业机器人控制系统的信息安全测试数据被泄露，造成工业机器人技术泄露等，需对工业机器人控制系统的信息安全测试数据进行加密处理，因而需先采集工业机器人控制系统的信息安全测试数据。

[0040] 将采集的所有信息安全测试数据组成工业机器人控制系统的信息安全测试数据序列。

[0041] 2、构建二维矩阵：

[0042] 由于二维矩阵具有空间关联性特征，因而二维矩阵数能够较好的反映数据之间的关联，因而需将工业机器人控制系统的信息安全测试数据序列转化成二维矩阵。

[0043] 获取工业机器人控制系统的信息安全测试数据序列的长度L，将信息安全测试数据序列均匀分割成长度为N的子序列，得到$\mathrm{M}=\frac{\mathrm{L}}{\mathrm{N}}$个子序列，需要说明的是当L不能被N整除时，需在安全测试数据序列的末尾补0，使得L能被N刚好整除。

[0044] 将$\frac{\mathrm{L}}{\mathrm{N}}$个子序列构建成一个$\mathrm{N}*\mathrm{M}$的二维矩阵。

[0045] 3、生成综合密钥序列：

[0046] 利用混沌映射函数生成一个H维的混沌序列，将混沌序列称为综合密钥序列，该混沌映射函数的超参数是加密方和解密方事先约定好的，无需进行传输。

[0047] 将综合密钥序列中的各数据称为密钥值。

[0048] 步骤S002,计算各单高斯模型的综合描述能力和各高斯参数的混乱程度,根据各单高斯模型的综合描述能力和各高斯参数的混乱程度得到各单高斯模型的各高斯参数的易暴露程度。

[0049] 由于二维矩阵中有些数据具有明显的统计特征,即这些数据通过一个单一的统计模型就能够较准确的描述,因而二维矩阵具有这个统计模型的特征较明显,因而为了防止得到的密文数据具有这种统计特征,需对二维矩阵中统计模型表征的统计特征进行较强破坏,而有些数据需要多个统计模型才能准确的描述,因而二维矩阵具有各统计模型的特征不明显,因而无需对二维矩阵中的统计模型表征的统计特征进行较强破坏就能够打破这种统计特征,因而需先分析每种统计模型对二维矩阵的综合描述能力,进而来对二维矩阵数据进行加密处理。

[0050] 拟合出二维矩阵的混合高斯模型:

[0051] 利用EM算法拟合出二维矩阵的混合高斯模型,该混合高斯模型中包含I个单高斯模型,本实施例 I取20,获取混合高斯模型中各单高斯模型的权值,将各单高斯模型按权值大小排序得到单高斯模型序列,将单高斯模型序列中第i位置的单高斯模型即为二维矩阵的第i个单高斯模型。

[0052] 2、划分区域:

[0053] 由于统计模型对二维矩阵中的各区域的综合描述能力不同,即二维矩阵各区域具有统计模型的特征明显程度不同,而在进行密文破解时,一般是将最明显的统计特征作为破解突破口,因而需将统计模型对所有区域的描述能力的最大值作为该统计模型对该二维矩阵的综合描述能力。

[0054] 在进行划分区域时,应考虑二维矩阵的各单高斯模型的主分布区域面积,各单高斯模型的主分布区域占整个分布区域比重较大,主分布区域基本代表了各单高斯模型的分布情况,因而再对二维矩阵进行区域划分时需考虑二维矩阵混合高斯模型中各单高斯的主分布区域。

[0055] 计算各单高斯模型的主分布区域面积:

[0056] 一般各单高斯模型的主分布区域为各单高斯模型的$[\mu-3\sigma,\ \mu+3\sigma]$区域内,$\mu$表示各单高斯模型的均值,$\sigma$表示单高斯模型的方差,基于此来计算各单高斯模型的主分布区域面积。

[0057] $$S_i=\pi*\frac{9}{4}*||U_i||$$

[0058] 其中,U_i表示二维矩阵的第i个单高斯模型的协方差矩阵,$||\cdot||$表示矩阵的L_2范数,由于二维矩阵的协方差矩阵为$2*2$维的矩阵,即二维矩阵的协方差矩阵中包含4个斜方差值,因而需将协方差矩阵的L_2范数除以4得到所有协方差平方的均值;二维矩阵各单高斯模型的主分布区域一般为椭圆或者圆形,且主分布区域的半径为3σ,因而第i个单高斯模型的主分布区域半径为$\frac{3}{2}*\sqrt{||U_i||}$,因而第$i$个单高斯模型的主分布区域面积为$\pi*\frac{9}{4}*||U_i||$,$S_i$表示二维矩阵的第$i$个单高斯模型的主分布区域面积。

[0059] 将二维矩阵的所有单高斯模型的主分布区域面积求均值得到二维矩阵的第一主

分布区域面积。

[0060] 根据二维矩阵的第一主分布区域面积将二维矩阵均匀划分成多个区域：

[0061] 获取二维矩阵的第一主分布区域面积的开方，并将二维矩阵的第一主分布区域面积的开方向上取整得到区域边长l，将二维矩阵均匀划分成多个$l*l$的区域，需要说明的是，当二维矩阵的面积不是整数倍的区域面积时，就会存在一些小于面积$l*l$的区域，本方案不予考虑，只考虑$l*l$的区域。

[0062] 3、计算各单高斯模型的综合描述能力：

[0063] (1)计算第i个单高斯模型对二维矩阵中第k个区域的描述能力：

[0064] 获取第i个单高斯模型在第k个区域的积分F_{ik}，因而第i个单高斯模型在第k个区域的描述能力为：

[0065] $$M1_{ik}=\frac{F_{ik}}{\sum_{i=1}^{I}F_{ik}}$$

[0066] 其中，F_{ik}表示第i个单高斯模型在第k个区域的积分，该值越接近第k个区域的积分总值时，说明第k个区域是由第i个单高斯模型来描述。I表示二维矩阵的单高斯模型的总个数，$M1_{ik}$表示第i个单高斯模型对第k个区域的描述能力。

[0067] (2)计算第i个单高斯模型的综合描述能力：

[0068] 由于单高斯模型对二维矩阵中的各区域的描述能力不同，即二维矩阵各区域具有单高斯模型的特征明显程度不同，而在进行密文破解时，一般是将最明显的统计特征作为破解突破口，因而需将单高斯模型对所有区域的描述能力的最大值作为该单高斯模型对该二维矩阵的综合描述能力。

[0069] 因而第i个单高斯模型的综合描述能力为$M_i=\max_{1\le k\le K}(M1_{ik})$，其中$M1_{ik}$表示第$i$个单高斯模型对第$k$个区域的描述能力，$K$表示二维矩阵中划分得到的区域个数，$M_i$表示第$i$个单高斯模型的综合描述能力，$\max()$表示获取最大值的函数。

[0070] 4、计算高斯参数的混乱程度：

[0071] 获取I个单高斯模型的第z个高斯参数得到二维矩阵的第z个高斯参数集合，例如第i个单高斯模型的第z个高斯参数为第i个单高斯模型的其中一个协方差值，计算二维矩阵的第z个高斯参数集合的信息熵Y_z，记为第z个高斯参数的混乱程度，该值越大说明二维矩阵的第z个参数的取值越混乱，越没有规律，因而该高斯参数越不容易被泄露。

[0072] 5、计算各单高斯模型的各高斯参数的易暴露程度：

[0073] 将第i个单高斯模型的综合描述能力M_i与第z个高斯参数的混乱程度Y_z的乘积值作为第i个单高斯模型的第z个高斯参数的易暴露程度B_{iz}，该值越大说明第i个单高斯模型的第z个高斯参数越明显，越容易暴露，因而第i个单高斯模型的第z个高斯参数的密钥序列越复杂，这样才能防止被破解。

[0074] 至此，得到各单高斯模型的各高斯参数的易暴露程度，在获取各单高斯模型的各高斯参数的易暴露程度时，分析了二维矩阵中具有各单高斯模型的统计特征的明显情况，从而得到各单高斯模型的综合描述能力，同时根据二维矩阵的混合高斯模型中各高斯参数

的取值混乱程度得到各高斯参数的混乱程度，根据各单高斯模型的综合描述能力和各高斯参数的混乱程度得到各单高斯模型的各高斯参数的易暴露程度，通过各单高斯模型的各高斯参数的易暴露程度来反应各单高斯模型各高斯参数的易暴露程度，从而为后根据各单高斯模型各高斯参数的易暴露程度给各单高斯模型各高斯参数的密钥序列，从而对各单高斯模型各高斯参数进行不同的加密。

[0075] 步骤S003，根据各单高斯模型各高斯参数的易暴露程度得到各单高斯模型的各高斯参数的密钥序列，根据各单高斯模型的各高斯参数的密钥序列完成二维矩阵的加密处理得到密文数据。

[0076] 计算综合密钥序列中各密钥值的破解难度：

[0077] 利用EM算法拟合出综合密钥序列的混合高斯模型，所述综合密钥序列的混合高斯模型包含Z个单高斯模型，本实施例中Z取20，在其他实施例中，实施者可根据应用场景进行设置，将综合密钥序列的混合高斯模型中每个单高斯模型称为综合密钥序列的单高斯模型。

[0078] 利用综合密钥序列的第j个单高斯模型拟合出综合密钥序列的第t个密钥值的拟合值W_{tj}，同理利用综合密钥序列的各单高斯模型拟合出综合密钥序列的第t个密钥值的拟合值，得到第t个密钥值的拟合值集合，根据各单高斯模型对第t个密钥值的拟合值得到第t个密钥值的破解难度为：

[0079] 计算出第t个密钥值的拟合值集合的信息熵作为第t个密钥值的破解难度P_t，该值越大说明第t个密钥值的所有拟合值越混乱，即该密钥值具有各单高斯模型的统计特征均较少，因而不会凸显出单高斯模型统计特征，因而第t个密钥值的破解难度较大。

[0080] 根据各单高斯模型的各高斯参数的易暴露程度得到各单高斯模型的各高斯参数的加密复杂性：

[0081] $$P1_{iz} = \lceil B_{iz} * \alpha \rceil$$

[0082] 其中，B_{iz}表示第i个单高斯模型的第z个高斯参数的易暴露程度，该值越大说明二维矩阵的第i个单高斯模型的第z个高斯参数越容易暴露，因而，越应该给该参数进行复杂加密，才能不暴露出二维矩阵的统计特征，α表示超参数，本方案取5，$P1_{iz}$表示第i个单高斯模型的第z个高斯参数的加密复杂性，$\lceil\rceil$表示向上取整符号。

[0083] 根据各单高斯模型的各高斯参数的加密复杂性和各密钥值的破解难度得到各单高斯模型的各高斯参数的密钥序列：

[0084] 获取第i个单高斯模型的第z个高斯参数的加密复杂性作为第i个单高斯模型的第z个高斯参数的第一位置，在综合密钥序列中获取第一位置处的密钥值记为第一密钥值，将第一密钥自作为第i个单高斯模型的第z个高斯参数的中间密钥序列，计算中间密钥序列中所有密钥值的破解难度累加和记为第一累加和，将第一累加和与第i个单高斯模型的第z个高斯参数的加密复杂性比较，当第一累加和大于第i个单高斯模型的第z个高斯参数的加密复杂性时，将中间密钥序列作为第i个单高斯模型的第z个高斯参数的密钥序列，当第一累加和小于第i个单高斯模型的第z个高斯参数的加密复杂性时，将第一密钥值作为第二位置，将综合密钥序列中第二位置处的密钥值记为第二密钥值，将第一密钥值与第二密钥值构成中

间密钥序列，将中间密钥序列中所有密钥值的破解难度累加和记为第二累加和，将第二累加和与第i个单高斯模型的第z个高斯参数的加密复杂性比较，当第二累加和大于第i个单高斯模型的第z个高斯参数的加密复杂性时，将中间密钥序列作为第i个单高斯模型的第z个高斯参数的密钥序列，当第二累加和小于第i个单高斯模型的第z个高斯参数的加密复杂性时，将第二密钥值作为第三位置，将综合密钥序列中第三位置处的密钥值记为第三密钥值，将第一密钥值、第二密钥值和第三密钥值构成中间密钥序列，以此类推，直至得到第i个单高斯模型的第z个高斯参数的密钥序列。

[0085] 根据各单高斯模型的各高斯参数的密钥序列对二维矩阵进行加密处理得到密文数据：

[0086] 将第i个单高斯模型的第z个高斯参数的密钥序列的各密钥值的各位上的数据计算累计和记为各密钥值的第一位数和，例如密钥值为123，将密钥值各位上数据“1”、“2”、“3”计算累加和得到6，因而密钥值的第一位数和为6。将第i个单高斯模型的第z个高斯参数的密钥序列所有密钥值的第一位数和的累加和作为第i个单高斯模型的第z个高斯参数的第二位数和。

[0087] 将第i个单高斯模型的第z个高斯参数加上第二位数和得到第i个单高斯模型的第z个高斯参数的调整后参数。

[0088] 需要说明的是，二维矩阵的各单高斯模型的第一个高斯参数为均值向量，该均值向量为二维向量，因而二维矩阵的各单高斯模型的第一个高斯参数加密方式为：

[0089] 获取第i个单高斯模型的第1个高斯参数的密钥序列，获取第i个单高斯模型的第1个高斯参数的密钥序列包含的元素个数C_i，获取第i个单高斯模型的第1个高斯参数的密钥序列中前$\frac{C_i}{2}$维的序列记为第一序列，获取第i个单高斯模型的第1个高斯参数的密钥序列中后$\frac{C_i}{2}$维的序列记为第二序列，将第一序列中各密钥值的累加和记为第一序列的累加和，将第二序列中各密钥值的累加和记为第二序列的累加和，将第一序列的累加和与第i个单高斯模型的均值向量的第一个位置的数据的累加和作为第i个单高斯模型的均值向量的第一个位置的调整后参数，将第二序列的累加和与第i个单高斯模型的均值向量的第二个位置的数据的累加和作为第i个单高斯模型的均值向量的第二个位置的调整后参数，第i个单高斯模型的均值向量的第一个位置的调整后参数与第二个位置的调整后参数构成的向量作为第i个单高斯模型的调整后均值向量，即第i个单高斯模型的第1个高斯参数的调整后参数。

[0090] 将第i个单高斯模型的所有高斯参数的调整后参数构成的单高斯模型作为第i个单高斯模型的调整后单高斯模型，将二维矩阵的所有单高斯模型的调整后单高斯模型构成的混合高斯模型作为二维矩阵的调整后混合高斯模型。

[0091] 将二维矩阵的调整后混合高斯模型生成新的二维矩阵记为加密矩阵。

[0092] 将加密矩阵恢复成的数据序列作为密文数据。

[0093] 至此，完成了二维矩阵的加密得到密文数据，在对二维矩阵加密的过程中需先根据二维矩阵各单高斯模型各高斯参数的易暴露程度来得到各单高斯模型各高斯参数的密钥序列，然后根据密钥序列对二维矩阵进行加密处理得到密文数据，通过该加密方式能够

将二维矩阵的统计特征较好的隐藏，使得加密后的密文数据很难通过统计特征进行破解。

[0094] 步骤S004，对密文数据进行解密得到工业机器人控制系统的信息安全测试数据序列。

[0095] 加密方将密文数据和各单高斯模型的各高斯参数的易暴露程度传递给解密方。由于得到综合密钥序列的混沌映射函数的超参数是事先约定好的，因而解密方可根据超参数确定混沌映射函数，进而得到综合密钥序列。

[0096] 解密方根据密文数据得到加密矩阵，根据加密矩阵得到加密矩阵的混合高斯模型，将加密矩阵的混合高斯模型中的各单高斯模型根据权重大小排列得到单高斯模型序列。

[0097] 根据各单高斯模型的各高斯参数的易暴露程度得到加密复杂性，根据各单高斯模型的各高斯参数的加密复杂性得到各单高斯模型的各高斯参数的密钥序列。

[0098] 根据各单高斯模型的各高斯参数的密钥序列，利用加密方法的逆向过程对加密矩阵进行解密处理得到二维矩阵。

[0099] 将二维矩阵恢复成数据序列得到工业机器人控制系统的信息安全测试数据序列。

[0100] 综上所述，本发明实施例提供了一种工业机器人控制系统的信息安全测试数据处理方法，获得二维矩阵以及二维矩阵的混合高斯模型，通过分析混合高斯模型中各单高斯的主分布区域得到各单高斯模型的第一主分布区域面积，根据各单高斯模型的第一主分布区域面积得到二维矩阵的多个区域，根据各单高斯模型对各区域的描述情况得到各单高斯模型的综合描述能力；计算混合高斯模型中各高斯参数的混乱程度，结合各单高斯模型的综合描述能力和各高斯参数的混乱程度得到各单高斯模型各高斯参数的易暴露程度。通过各单高斯模型的综合描述能力来反应二维矩阵具有各单高斯模型的统计特征的明显情况，当各单高斯模型的综合描述能力越大时，说明该二维矩阵具有该单高斯模型的统计特征越明显，为了防止加密后的密文数据后泄露这种统计特征，因而需将该单高斯模型给予较复杂的密钥，通过各单高斯模型的各高斯参数的易暴露程度来说明各单高斯模型的各高斯参数的易暴露情况，该值越大说明该单高斯模型的高斯参数越容易泄露，因而需对该单高斯模型的各参数分配一个复杂的密钥，从而使得加密得到的密文数据安全性更强。

[0101] 根据各单高斯模型的各高斯参数的易暴露程度得到加密复杂性，获得综合密钥序列的混合高斯模型，根据综合密钥序列的混合高斯模型得到综合密钥序列中各密钥值的破解难度，根据各单高斯模型的各高斯参数的加密复杂性和各密钥值的破解难度得到各单高斯模型的各高斯参数的密钥序列，根据各单高斯模型的各高斯参数的密钥序列对二维矩阵进行加密得到密文数据，通过此来实现给不同易暴露程度的单高斯模型的各高斯参数分配不同复杂的密钥序列，从而达到对二维矩阵的不同数据进行不同复杂的加密，再保障去除二维矩阵中统计特征的同时还能提高加密效率。

[0102] 需要说明的是：上述本发明实施例先后顺序仅仅为了描述，不代表实施例的优劣。且上述对本说明书特定实施例进行了描述。另外，在附图中描绘的过程不一定要求示出的特定顺序或者连续顺序才能实现期望的结果。在某些实施方式中，多任务处理和并行处理也是可以的或者可能是有利的。

[0103] 本说明书中的各个实施例均采用递进的方式描述，各个实施例之间相同相似的部分互相参见即可，每个实施例重点说明的都是与其他实施例的不同之处。

[0104] 以上所述仅为本发明的较佳实施例，并不用以限制本发明，凡在本发明的原则之内，所作的任何修改、等同替换、改进等，均应包含在本发明的保护范围之内。

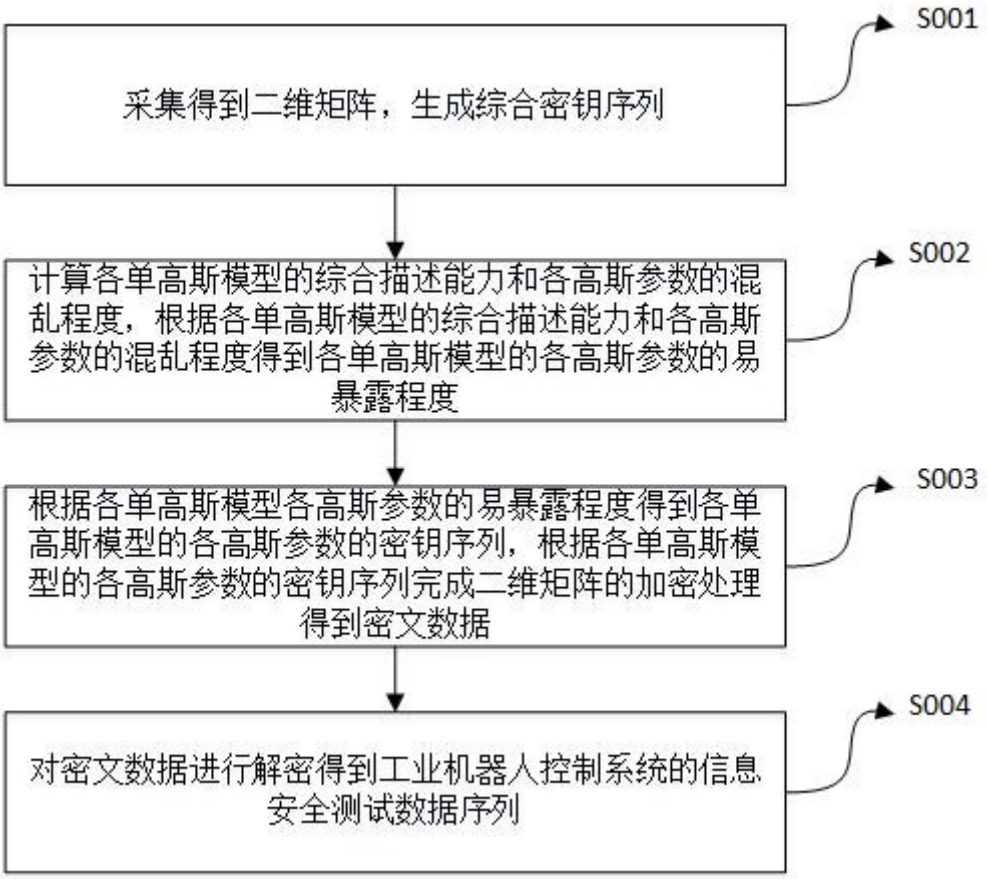

S001
采集得到二维矩阵，生成综合密钥序列
S002
计算各单高斯模型的综合描述能力和各高斯参数的混乱程度，根据各单高斯模型的综合描述能力和各高斯参数的混乱程度得到各单高斯模型的各高斯参数的易暴露程度
S003
根据各单高斯模型各高斯参数的易暴露程度得到各单高斯模型的各高斯参数的密钥序列，根据各单高斯模型的各高斯参数的密钥序列完成二维矩阵的加密处理得到密文数据
S004
对密文数据进行解密得到工业机器人控制系统的信息安全测试数据序列

图1