

风险控制方法、风险控制装置、电子设备和存储介质

技术领域

[01]本申请涉及风险控制技术领域，特别涉及一种风险控制方法、风险控制装置、电子设备和存储介质。

5 背景技术

[02]为了保障用户操作的安全性，在已有的风险控制系统中，会捕捉具有很高风险的用户操作，并对这样的用户操作进行规定的风险控制处理，例如对用户进行身份核实，仅允许通过身份核实的用户继续交易，而对具有低风险的用户操作，做放行处理，由此避免了不安全交易的进行。

- 10 [03]应该注意，上面对技术背景的介绍只是为了方便对本发明的技术方案进行清楚、完整的说明，并方便本领域技术人员的理解而阐述的。不能仅仅因为这些方案在本发明的背景技术部分进行了阐述而认为上述技术方案为本领域技术人员所公知。

发明内容

- 15 [04]发明人发现，在已有的上述技术中，未考虑不同用户之间的差异性，也未考虑不同用户操作的风险的差异性，对用户操作的风险分级较为粗略，并且针对风险的防御方案较为单一而不灵活。因此，如果将进行身份核实的标准设定得较为严格，即，使得更多的用户操作被判定为高风险操作，则用户会被频繁地要求进行身份核实；反之，如果将进行身份核实的标准设得较为宽松，则会降低用户操作的安全性。

- 20 [05]为了解决上述问题，本说明书实施例提供一种风险控制方法、风险控制装置、风险控制装置、电子设备和存储介质，能够精确地计算期望资产损失，针对不同的用户和风险灵活地实施风险控制处理，在保障用户操作的安全性的同时，减少由风险控制处理导致的对用户的打扰，提升用户体验。

- 25 [06]根据本说明书实施例的第一方面，提供一种风险控制方法，所述风险控制方法包括：获取当前的用户操作的风险信息，该风险信息包括风险类型和/或表征与该风险类型相对应的风险大小的参数；针对历史身份核实对应的身份核实方式，根据该风险信息和与该身份核实方式对应的安全信息，计算安全系数，其中，该历史身份核实包含在该用户操

作之前对当前的用户进行的身份核实,该安全信息是与该身份核实方式的安全性相关的信息;根据该安全系数和与该用户操作对应的金额,计算期望资产损失;以及在该期望资产损失满足预设条件的情况下,对该用户操作进行规定的风险控制处理,在该期望资产损失未满足该预设条件的情况下,不对该用户操作进行规定的风险控制处理。

- 5 [07]根据本说明书实施例的第二方面,提供一种风险控制装置,该风险控制装置包括:风险获取单元,其获取当前的用户操作的风险信息,该风险信息包括风险类型和/或表征与该风险类型相对应的风险大小的参数;安全系数计算单元,其针对历史身份核实对应的身份核实方式,根据该风险信息和与该身份核实方式对应的安全信息,计算安全系数,其中,该历史身份核实包含在该用户操作之前对当前的用户进行的身份核实,该安全信息是与该身份核实方式的安全性相关的信息;资产损失计算单元,其根据该安全系数和与该用户操作对应的金额,计算期望资产损失;以及风险控制处理单元,其在该期望资产损失满足预设条件的情况下,对该用户操作进行规定的风险控制处理,在该期望资产损失未满足该预设条件的情况下,不对该用户操作进行规定的风险控制处理。

- 10 [08]根据本说明书实施例的第三方面,提供一种电子设备,该电子设备包括处理器以及用于存储计算机可读程序的存储器,该计算机可读程序使得该处理器执行根据上述第一方面所述的风险控制方法。

[09]根据本说明书实施例的第四方面,提供一种存储有计算机可读程序的存储介质,该计算机可读程序使得处理装置执行根据上述第一方面所述的风险控制方法。

- 20 [10]本说明书实施例的有益效果在于,能够精确地计算期望资产损失,针对不同的用户和风险灵活地实施风险控制处理,在保障用户操作的安全性的同时,在保障用户操作的安全性的同时,减少由风险控制处理导致的对用户的打扰,提升用户体验。

[11]参照后文的说明和附图,详细公开了本发明的具体实施方式,指明了本发明的原理可以被采用的方式。应该理解,本发明的实施方式在范围上并不因而受到限制。在所附权利要求的精神和条款的范围内,本发明的实施方式包括许多改变、修改和等同。

- 25 [12]针对一种实施方式描述和/或示出的特征可以以相同或类似的方式在一个或多个其它实施方式中使用,与其它实施方式中的特征相组合,或替代其它实施方式中的特征。

[13]应该强调,术语“包括/包含/具有”在本文使用时指特征、整件、步骤或组件的存在,但并不排除一个或多个其它特征、整件、步骤或组件的存在或附加。

附图说明

[14]所包括的附图用来提供对本说明书实施例的进一步的理解，其构成了说明书的一部分，用于例示本发明的实施方式，并与文字描述一起来阐释本发明的原理。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性的前提下，还可以根据这些附图获得其他的附图。在附图中：

[15]图 1 是本说明书实施例 1 的风险控制方法的一个示意图。

[16]图 2 是本说明书实施例 1 的步骤 104 的实现方法的一个示意图。

[17]图 3 是本说明书实施例 1 的风险控制方法的另一个示意图。

[18]图 4 是本说明书实施例 1 的风险控制方法的又一个示意图。

10 [19]图 5 是本说明书实施例 1 的风险控制方法的再一个示意图。

[20]图 6 是本说明书实施例 2 的风险控制装置的一个示意图。

[21]图 7 是本说明书实施例 2 的风险控制装置的另一个示意图。

具体实施方式

[22]参照附图，通过下面的说明书，本发明的前述以及其它特征将变得明显。在说明书和附图中，具体公开了本发明的特定实施方式，其表明了其中可以采用本发明的原则的部分实施方式，应了解的是，本发明不限于所描述的实施方式，相反，本发明包括落入所附权利要求的范围内的全部修改、变型以及等同物。

[23]在本说明书实施例中，术语“和/或”包括相关联列出的术语的一种或多个中的任何一个和所有组合。

20 [24]在本说明书实施例中，单数形式“一”、“该”等包括复数形式，应广义地理解为“一种”或“一类”而并不是限定为“一个”的含义；此外术语“所述”应理解为既包括单数形式也包括复数形式，除非上下文另外明确指出。此外术语“根据”应理解为“至少部分根据……”，术语“基于”应理解为“至少部分基于……”，除非上下文另外明确指出。

25 [25]下面结合附图对本说明书实施例的各种实施方式进行说明。这些实施方式只是示例性的，不是对本说明书实施例的限制。

[26]实施例 1

[27]本实施例1提供一种风险控制方法。图1是本实施例的风险控制方法的一个示意图。

[28]如图1所示，该风险控制方法包括：

[29]步骤102，获取当前的用户操作的风险信息，该风险信息包括风险类型和/或表征与该风险类型相对应的风险大小的参数；

- 5 [30]步骤104，针对历史身份核实对应的身份核实方式，根据上述风险信息和与该身份核实方式对应的安全信息，计算安全系数，其中，该历史身份核实包含在所述用户操作之前对当前的用户进行的身份核实，所述安全信息是与所述身份核实方式的安全性相关的信息；

[31]步骤106，根据该安全系数和与该用户操作对应的金额，计算期望资产损失；

- 10 [32]步骤108，在该期望资产损失满足预设条件的情况下，对该用户操作进行规定的风险控制处理，在该期望资产损失未满足该预设条件的情况下，不对该用户操作进行规定的风险控制处理。

[33]由上述实施例可知，通过根据当前的用户操作的风险信息和安全信息计算安全系数，并将该安全系数用于计算期望资产损失，能够精准地计算期望资产损失，由此，能够精准地确定是否进行规定的风险控制处理，从而能够针对不同的用户和风险灵活地实施风险控制处理，在保障用户操作的安全性的同时，减少由风险控制处理导致的对用户的打扰，提升用户体验。

- 15 [34]并且，由于针对身份核实方式计算安全系数，因此能够针对各种身份核实方式实现保障安全性并减少打扰，即，能够在各种用户身份核实方式的场景下实现保障安全性并减少打扰。

[35]在图1中，上述步骤100在步骤102之前执行，但本实施例不限于此，步骤100也可以在步骤102之后且步骤104之前执行，或者与步骤102并行执行。

[36]在本实施例中，用户操作针对一定金额的操作。例如可以是用户与商户间的交易操作，也可以是用户的资产转移操作，该资产转移操作例如可以是转账操作等。

- 25 [37]在本实施例中，风险类型例如可以包括设备丢失风险、个人电脑远程风险、二次放号风险、常规盗用风险等，其中常规盗用风险表征设备丢失以外的操作账号被盗用的风险，但本实施例不限于此，也可以包含能够识别的其他风险类型。另外，表征与该风险类型相对应的风险大小的参数例如可以是与该风险类型相对应的风险分值，该分值例

如可以是 0-1 之间的数值，用于表征相应的风险大小。但本实施例不限于此，该分值也可以采用其他数值范围，并且，也可以不采用风险分值作为该参数，而是采用风险等级作为该参数。

5 [38]在本实施例中，风险信息除了可以包括风险类型和/或上述参数以外，还可以包括与风险相关的其他信息，例如表示与风险类型相对应的风险权重等。本实施例的风险信息可利用现有的风险识别策略进行识别。

[39]在本实施例中，身份核实方式例如包括人工核实方式、人脸核实方式、隐私核实方式等，隐私核实例如可以是安保问题核实、身份证号码核实、银行卡核实等。但本实施例不限于此，还可以包括其他能够实现身份核实的方式。

10 [40]在本实施例中，上述安全信息是与一定的身份核实方式相对应的、与安全性相关的信息。例如，该安全信息可以包括以下信息中的至少一种：该身份核实方式所对应的身份核实所使用的设备的标识、该身份核实方式所对应的身份核实的执行环境、该身份核实方式所对应的身份核实的执行时间、该身份核实方式所对应的身份核实的结果、以及
15 该身份核实方式所对应的身份核实的频率或次数。但本实施例不限于此，安全信息也可以包括其他信息。

[41]在本实施例中，设备的标识例如可以是设备的识别码和/或地址等。设备的识别码例如可以是设备的唯一素材识别码（Unique Material Identifier, UMID）等；设备的地址例如可以是硬件地址或者互联网地址等；身份核实的执行环境例如可以是互联网、无线局域网、基于位置的服务（Location Based Service, LBS）等；身份核实的结果例如可以
20 是通过或者不通过。但本实施例不以此作为限制，也可以采用其他的设备标识以及操作环境。

[42]在本实施例中，规定的风险控制处理是使风险降低的处理，例如，包括不允许进行该用户操作、对该用户操作限制权限、要求用户进行身份核实等，但本实施例不限于此，还可包括其他的风险控制处理方式。该风险控制处理可根据实际情况而进行规定。不
25 进行该风险控制处理即对用户操作直接放行。

[43]在本实施例中，上述步骤 104 可将上述风险信息和安全信息中的各具体信息量化为数值，并针对这些不同的具体信息赋予相应的权重，以一定的规则将其组合起来，由此计算出安全系数。具体的量化方式以及规则可根据实际需求而确定。例如，可采用德尔菲法计算安全系数。

[44]例如,在下述情况下:“风险类型为常规盗用风险,风险大小为 0.4,安全信息包括:身份核实在 24 小时内执行,相同设备下进行了 1 次人脸身份核实,核实结果为通过”,可根据上述信息以及德尔菲法进行安全系数的计算,例如将其计算为 0.95(安全系数的最高值为 1 的情况下)。

5 [45]在本实施例中,上述历史身份核实可以对应于一种或至少两种身份核实方式。

[46]在上述历史身份核实对应于一种身份核实方式的情况下,针对该种身份核实方式,根据风险信息 and 与该种身份认证方式对应的安全信息,计算该种身份核实方式对应的安全系数。

[47]图 2 是上述步骤 104 的实现方法的一个示意图。如图 2 所示,在上述历史身份核实
10 对应于至少两种身份核实方式的情况下,上述步骤 104 可以包括:

[48]步骤 202,针对至少两种身份核实方式中的每一种身份核实方式,根据风险信息和与该种身份核实方式对应的安全信息,计算该种身份核实方式对应的子安全系数;

[49]步骤 204,对该至少两种身份核实方式各自对应的子安全系数进行加权计算,将加权后的值作为该安全系数。

15 [50]上述步骤 202-204 为可选步骤。

[51]在本实施例中,在上述步骤 106 中,可按照预设的规则,根据安全系数和用户操作对应的金额,计算期望资产损失。该期望资产损失能够表征潜在的资产损失。

[52]在本实施例中,上述步骤 106 例如可根据下述公式(1)计算期望资产损失:

[53]期望资产损失 = 用户操作对应的金额 $\times$ (1-安全系数) (1)

20 [54]其中,安全系数的值被限定为在 0-1 变化。但本实施例不限于此,也可以将安全系数的取值范围限定为其他范围。安全系数的取值范围的限定可通过调整计算安全系数时使用的具体规则而实现。

[55]但本实施例不限于以上述公式(1)计算期望资产损失,也可采用其他适当的公式进行计算。

25 [56]图 3 是本实施例的风险控制方法的另一个示意图。如图 3 所示,该风险控制方法还可以包括:

[57]步骤 110,根据表征针对该用户操作的聚集性风险的特征变量,获得调整系数;

[58]并且,在上述步骤 104 之后,该风险控制方法还可以包括:

[59]步骤 112,根据该调整系数调整该安全系数。

[60]此时,上述步骤 106 可根据调整后的安全系数和与用户操作对应的金额,计算期望资产损失。由此,能够在计算出的期望资产损失中反映聚集性风险的影响,从而更精确地计算期望资产损失,使得风险控制能够对聚集性风险作出快速应对。这里,聚集性风险例如可以是批量攻击风险,但本实施例不限于此,也可以是其他类型的聚集性风险。

[61]上述步骤 110-112 为可选步骤。

[62]在图 3 中,上述步骤 110 在步骤 104 之后执行,但本实施例不限于此,步骤 110 也可以在步骤 104 之前执行,或者与步骤 104 并行执行。

10 [63]在本实施例中,上述步骤 112 可包括:将该调整系数乘以该安全系数的值作为调整后的安全系数。

[64]在执行了上述步骤 110、112 的情况下,上述步骤 106 可根据下述公式(2)计算期望资产损失:

[65]期望资产损失 = 用户操作对应的金额 $\times$ (1-调整后的安全系数) (2)

15 [66]图 4 是本实施例的风险控制方法的又一个示意图。如图 4 所示,在上述步骤 110 之前,该风险控制方法还可包括:

[67]步骤 114,基于根据预设的两个维度而划分的网格和各网格内的历史数据,计算各网格内的预设指标,并根据各网格内的该预设指标确定该特征变量,其中,该历史数据是网格内与当前的用户操作之前的用户操作相关的数据。

20 [68]例如,上述预设的两个维度是与当前的用户操作对应的第一维度和第二维度,第一维度例如可以是当前用户操作对应的商户或互联网地址等,第二维度例如可以是当前用户操作的时间、环境或地区等。上述预设指标例如可以是表示风险识别策略的命中率的事件稽核率、表示身份核实的未通过率的校验失败率、表示可信任环境下和/或可信任设备下进行的用户操作数量占总用户操作数量的比例的可信操作占比、或规定天数内(例如 30 天)的案件发生率等,但本实施例不以此作为限制,还可以为其他指标。上述历史数据可以是网格内与当前的用户操作之前的用户操作相关的、用于计算上述预设指标的任意的数据。

[69]上述步骤 114 为可选步骤。并且,在图 4 中,上述步骤 114 在步骤 104 之后执行,

但本实施例不限于此,步骤 114 也可以在步骤 104 之前执行,或者与步骤 104 并行执行。

[70]在本实施例中,上述特征变量可以为一个或者至少两个。

[71]在上述特征变量为一个的情况下,根据该特征变量,获得调整系数。

[72]在本实施例中,在上述特征变量为至少两个的情况下,该风险控制方法还可包括步骤 (未图示): 对该至少两个特征变量进行加权计算,得到特征变量的加权值。该步骤为可选步骤。

[73]此时,上述步骤 110 可包括: 根据上述特征变量的加权值,获得调整系数。

[74]在本实施例中,上述步骤 108 可包括: 在该期望资产损失超过阈值的情况下,对该用户操作进行规定的风险控制处理,在该期望资产损失未超过该阈值的情况下,不对该用户操作进行规定的风险控制处理。即,步骤 108 中的上述预设条件为超过阈值。

[75]此外,也可以根据实际需求设置其他的预设条件。

[76]在本实施例中,在该期望资产损失超过阈值的情况下,对该用户操作进行规定的风险控制处理,还可以包括: 在该期望资产损失超过上述阈值且未超过另一阈值的情况下,对该用户操作进行规定的第二风险控制处理; 在该期望资产损失超过该另一阈值的情况下,对该用户操作进行规定的第三风险控制处理。该步骤为可选步骤。

[77]在上述步骤 108 之前,该风险控制方法还可包括步骤 (未图示): 根据上述风险信息 and 与用户操作对应的金额,设定阈值。由此,可与期望资产损失的计算相对应地,更合理地设置阈值。该步骤为可选步骤。

[78]图 5 是本实施例的风险控制方法的再一个示意图。如图 5 所示,在上述步骤 104 之前,该风险控制方法还可包括:

[79]步骤 100,对用户进行分类而获得分类结果。

[80]此时,上述步骤 104 可包括: 根据该分类结果、上述风险信息和安全信息,计算安全系数。由此,能够在计算出的期望资产损失中进一步反映用户分类的影响,从而更精确地计算期望资产损失。

[81]在图 5 中,上述步骤 100 在步骤 102 之前执行,但本实施例不限于此,步骤 100 也可以在步骤 102 之后且步骤 104 之前执行,或者与步骤 102 并行执行。

[82]在本实施例中,可以依据下述信息中的至少一种,对当前的用户进行分类: 用户消费行为、用户的社会属性、用户使用的设备的信息、历史身份核实对应的身份核实方式

及其结果、用户的投诉、用户的案件（例如用户报案的诈骗案件）、用户的安全意识。但本实施例不限于此，也可以依据与用户相关的其他信息对用户进行分类。

5 [83]在本实施例中，分类的原则例如可以考虑用户的易受骗程度和/或用户的打扰敏感度等因素，由此分类结果可以相应为易受骗用户、打扰敏感用户等。例如，对于易受骗用户，在其他条件相同的情况下，在步骤 104 中，使安全系数更低；对于打扰敏感用户，在其他条件相同的情况下，在步骤 104 中，使安全系数更高。但本实施例不限于此，也可以考虑能够对安全系数产生影响的其他因素对用户进行分类。

10 [84]在图 5 所示的方法中，如果将预设条件设定为超过阈值，则可根据上述分类结果、风险信息或与用户操作对应的金额，设定该阈值。由此，可与期望资产损失的计算方式相对应地，更合理地设置阈值。

[85]通过本实施例的风险控制方法，能够精确地计算期望资产损失，针对不同的用户和风险灵活地实施风险控制处理，在保障用户操作的安全性的同时，减少由风险控制处理导致的对用户的打扰，提升用户体验。

[86]实施例 2

15 [87]本实施例 2 提供一种风险控制装置。图 6 是本实施例的风险控制装置的一个示意图。本实施例中与实施例 1 相同的部分不再赘述。

[88]如图 6 所示，风险控制装置 600 包括风险获取单元 601、安全系数计算单元 602、资产损失计算单元 603、风险控制处理单元 604。

20 [89]其中，风险获取单元 601 获取当前的用户操作的风险信息，该风险信息包括风险类型和/或表征与该风险类型相对应的风险大小的参数；安全系数计算单元 602 针对历史身份核实对应的身份核实方式，根据该风险信息和与该身份核实方式对应的安全信息，计算安全系数，其中，该历史身份核实包含在该用户操作之前对当前的用户进行的身份核实，该安全信息是与该身份核实方式的安全性相关的信息；资产损失计算单元 603 根据该安全系数和与该用户操作对应的金额，计算期望资产损失；风险控制处理单元 604 在
25 该期望资产损失满足预设条件的情况下，对该用户操作进行规定的风险控制处理，在该期望资产损失未满足该预设条件的情况下，不对该用户操作进行规定的风险控制处理。

[90]在本实施例中，在历史身份核实对应于一种身份核实方式的情况下，安全系数计算单元 602 可针对该种身份核实方式，根据上述风险信息和上述安全信息，计算该种身份核实方式对应的安全系数。

[91]在本实施例中，在历史身份核实对应于至少两种身份核实方式的情况下，安全系数计算单元 602 可针对该至少两种身份核实方式中的每一种身份核实方式，根据上述风险信息以及与该种身份核实方式对应的安全信息，计算该种身份核实方式对应的子安全系数，并对该至少两种身份核实方式各自对应的子安全系数进行加权计算，将加权后的值作为安全系数。

[92]图 7 是本实施例的风险控制装置的另一个示意图。如图 7 所示，风险控制单元 700 包括风险获取单元 601、安全系数计算单元 702、资产损失计算单元 703 和风险控制处理单元 704。

[93]风险获取单元 601 如上所述，此处不再赘述。安全系数计算单元 702、资产损失计算单元 703、风险控制处理单元 704 分别能够实现上述安全系数计算单元 602、资产损失计算单元 603、风险控制处理单元 604 所实现的功能。

[94]在本实施例中，如图 7 所示，风险控制单元 700 还可包括调整系数获得单元 705 和调整单元 706。调整系数获得单元 705 可根据表征针对用户操作的聚集性风险的特征变量，获得调整系数，调整单元 706 可根据该调整系数调整所述安全系数，资产损失计算单元 703 可根据调整后的安全系数和与用户操作对应的金额，计算期望资产损失。

[95]上述调整系数获得单元 705 和调整单元 706 为可选单元。

[96]在本实施例中，如图 7 所示，风险控制装置 700 还可包括特征变量确定单元 707，特征变量确定单元 707 可基于根据预设的两个维度而划分的网格和各网格内的历史数据，计算各网格内的预设指标，并根据各网格内的该预设指标确定该特征变量，其中，该历史数据是网格内与当前的用户操作之前的用户操作相关的数据。

[97]在本实施例中，如图 7 所示，特征变量确定单元 707 还可在上述特征变量为至少两个的情况下，对该至少两个特征变量进行加权计算，得到特征变量的加权值，并且，调整系数获得单元 705 可根据该特征变量的加权值，获得调整系数。

[98]上述特征变量确定单元 707 为可选单元。

[99]在本实施例中，风险控制处理单元 704 可在期望资产损失超过阈值的情况下，对用户操作进行规定的风险控制处理，在期望资产损失未超过阈值的情况下，不对该用户操作进行规定的风险控制处理。

[100] 在本实施例中，如图 7 所示，风险控制装置 700 还可包括阈值设定单元 708，其根据风险信息和用户操作对应的金额，设定上述阈值。

[101] 上述阈值设定单元 708 为可选单元。

[102] 在本实施例中，如图 7 所示，风险控制装置 700 还可包括用户分类单元 709，用户分类单元 709 可对用户进行分类而获得分类结果，并且，安全系数计算单元 702 可根据该分类结果、上述风险信息和安全信息，计算安全系数。

5 [103] 上述用户分类单元 709 为可选单元。

[104] 本实施例中上述各单元的功能的具体实现可参见实施例 1，此处不再赘述。

[105] 通过本实施例的风险控制装置，能够精确地计算期望资产损失，针对不同的用户和风险灵活地实施风险控制处理，在保障用户操作的安全性的同时，减少由风险控制处理导致的对用户的打扰，提升用户体验。

10 [106] 本说明书实施例还提供一种计算机可读程序，该计算机可读程序使得处理器执行实施例 1 所述的方法。

[107] 本说明书实施例还提供一种存储有计算机可读程序的存储介质，其中，存储有计算机可读程序的存储介质，该计算机可读程序使得处理器执行实施例 1 所述的方法。

[108] 本说明书实施例还提供一种电子设备，该电子设备包括处理器以及用于存储计算机可读程序的存储器，该计算机可读程序使得该处理器执行实施例 1 所述的方法。本
15 实施例的电子设备可以是任意类型的电子设备，例如可以是用户侧的终端设备，也可以是网络侧的服务器设备，还可以由终端设备与服务器设备协同实现，并且，上述服务器设备可以是一台服务器设备或者由多台服务器设备构成的服务器设备集群。也就是说，本实施例的电子设备的处理器和存储器可以是在一台设备中设置的处理器和存储器，也
20 可以是多台设备中分布式设置的处理器和存储器。

[109] 结合本说明书实施例描述的风险控制装置可直接体现为硬件、由处理器执行的软件模块或二者组合。例如，图 6 中所示的功能框图中的一个或多个和/或功能框图的一个或多个组合，既可以对应于计算机程序流程的各个软件模块，亦可以对应于各个硬件模块。这些软件模块，可以分别对应于图 1 所示的各个步骤。这些硬件模块例如可利用
25 现场可编程门阵列（FPGA）将这些软件模块固化而实现。

[110] 软件模块可以位于 RAM 存储器、闪存、ROM 存储器、EPROM 存储器、EEPROM 存储器、寄存器、硬盘、移动磁盘、CD-ROM 或者本领域已知的任何其它形式的存储介质。可以将一种存储介质耦接至处理器，从而使处理器能够从该存储介质读取信息，且可向该存储介质写入信息；或者该存储介质可以是处理器的组成部分。处理器和存储介

质可以位于 ASIC 中。该软件模块可以存储在电子设备的存储器中，也可以存储在可插入电子设备的存储卡中。例如，若电子设备采用的是较大容量的 MEGA-SIM 卡或者大容量的闪存装置，则该软件模块可存储在该 MEGA-SIM 卡或者大容量的闪存装置中。

- [111] 针对图描述的功能框图中的一个或多个和/或功能框图的一个或多个组合，可以实现为用于执行本申请所描述功能的通用处理器、数字信号处理器（DSP）、专用集成电路（ASIC）、现场可编程门阵列（FPGA）或其它可编程逻辑器件、分立门或晶体管逻辑器件、分立硬件组件、或者其任意适当组合。针对附图描述的功能框图中的一个或多个和/或功能框图的一个或多个组合，还可以实现为计算设备的组合，例如，DSP 和微处理器的组合、多个微处理器、与 DSP 通信结合的一个或多个微处理器或者任何其它这种配置。

[112] 以上结合具体的实施方式对本发明进行了描述，但本领域技术人员应该清楚，这些描述都是示例性的，并不是对本发明保护范围的限制。本领域技术人员可以根据本发明的原理对本发明做出各种变型和修改，这些变型和修改也在本发明的范围内。