(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
2022 年 5 月 12 日 (12.05.2022)

WIPO | PCT

(10) 国际公布号
WO 2022/095355 A1

(51) 国际专利分类号:
G06K 9/00 (2006.01)

(21) 国际申请号: PCT/CN2021/090564

(22) 国际申请日: 2021 年 4 月 28 日 (28.04.2021)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
202011231052.1 2020年11月6日 (06.11.2020) CN

(71) 申请人: 平安科技（深圳）有限公司 (PING AN TECHNOLOGY (SHENZHEN) CO., LTD.) [CN/CN]; 中国广东省深圳市福田区福田街道福安社区益田路5033号平安金融中心23楼, Guangdong 518000 (CN)。

(72) 发明人: 姚宏志 (YAO, Hongzhi); 中国广东省深圳市福田区福田街道福安社区益田路5033号平安金融中心23楼, Guangdong 518000 (CN)。

(74) 代理人: 深圳市精英专利事务所 (SHENZHEN TALENT PATENT SERVICE); 中国广东省深圳市福田区深南中路6009号绿景广场B栋20层B, Guangdong 518000 (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, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, IT, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, 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,

(54) **Title:** DOUBLE ENCRYPTION METHOD FOR FACE RECOGNITION INFORMATION, DEVICE, APPARATUS, AND STORAGE MEDIUM

(54) **发明名称:** 人脸识别信息的二次加密方法、装置、设备及存储介质

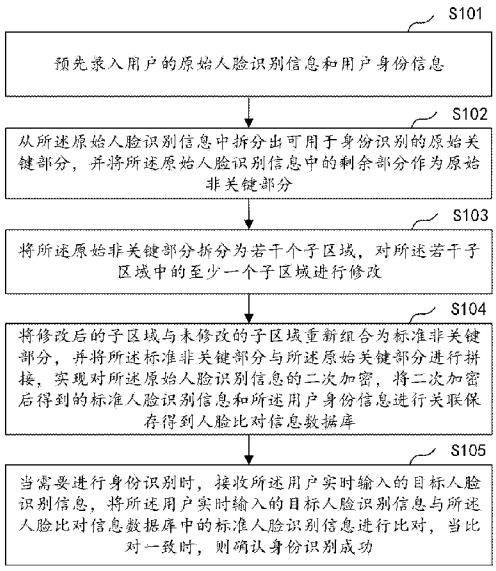

图 1

S101 Acquérir respectivement des premières informations temporelles et des informations événementielles dans une pluralité de documents événementiels, afin d'obtenir une pluralité de premières paires d'événements temporels correspondant à la pluralité de documents événementiels

S102 Normaliser les moyens d'expression temporels d'une pluralité d'éléments de premières informations temporelles dans la pluralité de premières paires d'événements temporels, afin d'obtenir une pluralité d'éléments de secondes informations temporelles normalisées et remplacer de manière correspondante les premières informations temporelles de la pluralité de premières paires d'événements temporels par la pluralité d'éléments de secondes informations temporelles normalisées, afin d'obtenir une pluralité de secondes paires d'événements temporels

S103 Déterminer, d'après la pluralité de secondes paires d'événements temporels, des informations événementielles cibles correspondant à la pluralité d'éléments de secondes informations temporelles

S104 Selon les secondes informations temporelles correspondant aux informations événementielles cibles, trier les informations événementielles cibles, afin de générer un contexte événementiel

(57) **Abstract:** A double encryption method for face recognition information, a device, an apparatus, and a storage medium, pertaining to the technical field of identity recognition. The method comprises: dividing face recognition information into a critical portion and a non-critical portion; dividing the non-critical portion into several sub-regions, extracting at least one sub-region, and modifying the extracted sub-region; re-assembling the modified sub-region with the other sub-regions to obtain a non-critical portion, stitching the re-assembled non-critical portion with the critical portion to realize double-encryption of the face recognition information, and associating the double-encrypted face recognition information with identity information of a user and storing same; and when identity recognition is required to be performed, receiving face recognition information input by a user in real-time, comparing the face recog-

[见续页]

WO 2022/095355 A1

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, 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, 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))。

nition information input by the user in real-time against the double-encrypted face recognition information, and controlling the identity recognition to be successful if the comparison passes recognition. The method improves security of face recognition information.

(57) 摘要：一种人脸识别信息的二次加密方法、装置、设备及存储介质，涉及身份认证技术领域，方法包括：从人脸识别信息中拆分出关键部分和非关键部分；将所述非关键部分拆分为若干个子区域，抽取至少一个子区域，并对所抽取的子区域进行修改；将修改后的子区域与其他子区域重新组合为非关键部分，并将重新组合的非关键部分与关键部分进行拼接，实现对人脸识别信息的二次加密，将二次加密后的人脸识别信息和用户身份信息进行关联保存；当需要进行身份识别时，接收用户实时输入的人脸识别信息，将用户实时输入的人脸识别信息与二次加密后的人脸识别信息进行比对，当比对通过时，则控制身份识别成功。通过所述方法，提高了人脸识别信息的安全性。

人脸识别信息的二次加密方法、装置、设备及存储介质

本申请要求于2020年11月06日提交中国专利局、申请号为202011231052.1，发明名称为“人脸识别信息的二次加密方法、装置、设备及存储介质”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

本申请涉及身份认证技术领域，尤其涉及人脸识别信息的二次加密方法、装置、设备及存储介质。

背景技术

人脸识别已经广泛应用于手机识别、客户支付等商业场景，这种识别方式使用起来非常便捷。但是方便之余，不免让人对信息安全产生担心。常见的用户密码可以经常变更，以确保密码的安全性，但是，发明人意识到人脸等隐私信息具有唯一性、长期不可更改性等特性，这导致人脸识别信息一旦被盗用，用户在人脸认证识别的各种场景都会产生隐患和风险。

申请内容

本申请实施例提供了人脸识别信息的二次加密方法、装置、设备及存储介质，旨在解决现有人脸识别技术存在安全隐患的问题。

第一方面，本申请实施例提供一种人脸识别信息的二次加密方法，其中，包括：

预先录入用户的原始人脸识别信息和用户身份信息；

从所述原始人脸识别信息中拆分出可用于身份识别的原始关键部分，并将所述原始人脸识别信息中的剩余部分作为原始非关键部分；

将所述原始非关键部分拆分为若干个子区域，对所述若干子区域中的至少一个子区域进行修改；

将修改后的子区域与未修改的子区域重新组合为标准非关键部分，并将所述标准非关键部分与所述原始关键部分进行拼接，实现对所述原始人脸识别信息的二次加密，将二次加密后得到的标准人脸识别信息和所述用户身份信息进行关联保存得到人脸比对信息数据库；

当需要进行身份识别时，接收所述用户实时输入的目标人脸识别信息，将所述用户实时输入的目标人脸识别信息与所述人脸比对信息数据库中的标准人脸识别信息进行比对，当比对一致时，则确认身份识别成功。

第二方面，本申请实施例提供一种人脸识别信息的二次加密装置，其中，包括：

录入单元，用于预先录入用户的原始人脸识别信息和用户身份信息；

拆分单元，用于从所述原始人脸识别信息中拆分出可用于身份识别的原始关键部分，并将所述原始人脸识别信息中的剩余部分作为原始非关键部分；

修改单元，用于将所述原始非关键部分拆分为若干个子区域，对所述若干子区域中的至少一个子区域进行修改；

组合单元，用于将修改后的子区域与未修改的子区域重新组合为标准非关键部分，并将

所述标准非关键部分与所述原始关键部分进行拼接，实现对所述原始人脸识别信息的二次加密，将二次加密后得到的标准人脸识别信息和所述用户身份信息进行关联保存得到人脸比对信息数据库；

识别单元，用于当需要进行身份识别时，接收所述用户实时输入的目标人脸识别信息，将所述用户实时输入的目标人脸识别信息与所述人脸比对信息数据库中的标准人脸识别信息进行比对，当比对一致时，则确认身份识别成功。

第三方面，本申请实施例提供一种计算机设备，包括存储器、处理器及存储在所述存储器上并可在所述处理器上运行的计算机程序，其中，所述处理器执行所述计算机程序时实现如第一方面所述的人脸识别信息的二次加密方法。

第四方面，本申请实施例提供一种计算机可读存储介质，其中，所述计算机可读存储介质存储有计算机程序，所述计算机程序当被处理器执行时使所述处理器执行如第一方面所述的人脸识别信息的二次加密方法。

本申请实施例提供了人脸识别信息的二次加密方法、装置、设备及存储介质，本申请实施例中，用户可以定期或随时更改人脸识别信息，从而提高人脸识别信息的安全性，也不影响识别的便捷性。

附图说明

为了更清楚地说明本申请实施例技术方案，下面将对实施例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的前提下，还可以根据这些附图获得其他的附图。

图 1 为本申请实施例提供的人脸识别信息的二次加密方法的流程示意图；

图 2 为本申请实施例提供的人脸识别信息的二次加密方法的子流程示意图；

图 3 为本申请实施例提供的人脸识别信息的二次加密方法的另一子流程示意图；

图 4 为本申请实施例提供的一种人脸识别信息的二次加密方法的另一子流程示意图；

图 5 为本申请实施例提供的一种人脸识别信息的二次加密装置的示意性框图；

图 6 为本申请实施例提供的一种人脸识别信息的二次加密装置的子单元示意性框图；

图 7 为本申请实施例提供的一种人脸识别信息的二次加密装置的另一子单元示意性框图；

图 8 为本申请实施例提供的一种人脸识别信息的二次加密装置的另一子单元示意性框图；

图 9 为本申请实施例提供的计算机设备的示意性框图。

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人脸识别信息的二次加密方法的流程示意图，如图所示，其包括步骤 S101~S105：

S101、预先录入用户的原始人脸识别信息和用户身份信息；

S102、从所述原始人脸识别信息中拆分出可用于身份识别的原始关键部分，并将所述原始人脸识别信息中的剩余部分作为原始非关键部分；

S103、将所述原始非关键部分拆分为若干个子区域，对所述若干子区域中的至少一个子区域进行修改；

S104、将修改后的子区域与未修改的子区域重新组合为标准非关键部分，并将所述标准非关键部分与所述原始关键部分进行拼接，实现对所述原始人脸识别信息的二次加密，将二次加密后得到的标准人脸识别信息和所述用户身份信息进行关联保存得到人脸比对信息数据库；

S105、当需要进行身份识别时，接收所述用户实时输入的目标人脸识别信息，将所述用户实时输入的目标人脸识别信息与所述人脸比对信息数据库中的标准人脸识别信息进行比对，当比对一致时，则确认身份识别成功。

具体的，在所述步骤 S101 中，所述原始人脸识别信息即指用户的脸部特征信息。

所述用户身份信息即代表用户的身份，可以包含用户的姓名、身份证、用户识别码、联系方式、平台登录信息等。

当需要进行身份识别时，用户只需输入人脸识别信息，然后对实时输入的目标人脸识别信息与保存的标准人脸识别信息进行比对，比对一致则根据标准人脸识别信息与用户身份信息的关联关系，可以获取用户身份信息，从而实现身份识别。

在所述步骤 S102 中，在所述原始人脸识别信息中包含有关键部分（为方便区分，此处称为原始关键部分）和非关键部分（为方便区分，此处称为原始非关键部分），其中关键部分是指能够表征用户特征的最少部分，即只有人脸识别信息包含了关键部分，才能对用户进行唯一识别。非关键部分则是除关键部分之外的可选部分，这部分内容可以帮助识别，但并不是必须的。例如对于人脸识别信息，关键部分可以是面部信息，非关键部分可以是头发、

头发延伸、发型等等。拆分的方式可以是从原始人脸识别信息中的中心开始逐渐进行放大，并将放大后识别成功率达到预设阈值的最小区域作为关键部分，将剩余区域作为非关键部分。放大的方式可以是以标准人脸的形状进行放大，也可以是以矩形或者圆形的形状进行放大。

在所述步骤 S103 中，将原始非关键部分拆分成了多个子区域，以便对这些子区域进行修改。修改的范围可以是一个子区域，也可以是多个子区域，但不是全部的子区域，以便后续进行识别时，可以对非关键部分进行比对。

本申请实施例对子区域的修改方式可以是增加、删除或者替换等。增加是指在子区域中增加一部分内容，使原有的子区域与修改后的子区域不同，删除是指在子区域中删除一部分内容或者全部内容，使原有的子区域与修改后的子区域不同，替换是指将子区域替换成一个新的子区域，从而使原有的子区域与修改后的子区域不同。通过上述修改，都可以使原子区域与新子区域不同。

在一实施例中，如图 2 所示，所述步骤 S103 包括步骤 S201~S203：

S201、将所述原始非关键部分拆分成数量不少于第三阈值的若干个子区域；

为了保证修改后的非关键部分与原有的非关键部分之间产生较大的区别，此处需要将非关键部分拆分成多个子区域，且拆分得到的子区域的数量应不少于第三阈值。在进行拆分时，可先记录原始非关键部分的初始机构，然后按照不规则形状进行划分，从而拆分出若干子区域，并对每一个拆分出的子区域进行标号，以便进行还原。

S202、从所述若干个子区域中随机抽取数量不少于第四阈值的若干个子区域；

本步骤中，会从上一步骤中拆分出的子区域中抽取出若干个子区域，抽取的方式为随机抽取，这样可以提高加密的安全性，避免被反向破解，另外抽取出的子区域的数量也应具有限制，此处设置为不少于第四阈值，以便提高加密的安全性。

此处的第四阈值应小于第三阈值，抽取的方式为随机抽取，例如从十个子区域中抽取 5 个子区域。

S203、按照预设的修改方式对抽取到的若干子区域进行修改。

本步骤中，可以选择增加、删除或替换等修改方式中的一种或几种，对抽取到的若干子区域进行修改。在进行修改时，需对修改的子区域进行标记，这样方便将修改的子区域与未修改的子区域进行组合。

本申请实施例中，为了提高加密的安全性，可以同时使用多种修改方式对多个子区域进行修改，例如使用修改方式一对某个子区域进行修改，使用修改方式二对另外的子区域进行修改，使用修改方式三对其他子区域进行修改。另外，本申请实施例中，还可以同时使用多种修改方式对同一个子区域进行修改，例如对某个子区域进行三种修改。

在一实施例中，所述步骤 S203 包括：

从每一个抽取到的子区域中选择若干特征图，对所选择的特征图进行模糊、删除或者覆盖的操作，并保存修改后的子区域；

或者，从每一个抽取到的子区域中选择若干特征图，并从预设的特征库中随机选择同样数量的特征图，对选择的若干特征图进行替换，并保存修改后的子区域。

本实施例中，在对子区域进行修改时，可以从该子区域中选择若干特征图，然后对特征图进行模糊、删除或者覆盖的操作，这样可以达到对子区域进行修改的目的，模糊的方式可以采用降低像素、打码等方式实现，删除的方式则是直接将选择的特征图删除，使相应的子区域成为不完整的子区域，覆盖的操作则是使用预定的图像对特征图进行覆盖，同样能达到对子区域进行修改的目的。

另外，本实施例中，还可以直接使用特征库中的特征图对所选择的特征图进行替换，从而使相应的子区域与原始的子区域区别开来，与前面的修改方式相比，此处是对所选择的整个特征图进行替换，其改动相对于前面的修改方式更大。

本申请实施例中，可以提前设置好加密方案，即设置好第三阈值、第四阈值和修改方式，以便后续在进行二次加密的过程中按照加密方案进行修改。

所述步骤 S104 中，将修改后的子区域与其他未修改的子区域重新组合，从而还原得到标准非关键部分，该标准非关键部分可以作为一个整体与原始关键部分重新组合，从而还原得到人脸识别信息，此处还原得到的人脸识别信息与原始人脸识别信息并不相同，为方便区分将还原得到的人脸识别信息称为标准人脸识别信息，不同的地方在于非关键部分，这样实现了对原始人脸识别信息的二次加密。

然后将二次加密后得到的标准人脸识别信息和用户身份信息进行关联保存，这样可以实现对用户身份的确认。

在一实施例中，如图 3 所示，所述步骤 S104 包括步骤 S301~S303：

S301、对修改后的子区域进行标记，并按顺序将所述修改后的子区域与所述未修改的子区域进行拼接组合，形成还原后的所述标准非关键部分；

本申请实施例中，先对修改后的子区域进行标记，即标记出哪些子区域进行过修改，这样在进行拼接组合时，就能按照非关键部分的初始结构将修改后的子区域与未修改的子区域进行拼接组合，从而得到还原后的标准非关键部分，并且还原后的标准非关键部分与原始非关键部分结构相同。

S302、获取所述原始人脸识别信息的初始结构，按照所述初始结构设置所述原始人脸识别信息的结构模板，将所述原始关键部分与还原后的所述标准非关键部分填充至所述结构模板中，形成二次加密后的标准人脸识别信息；

此步骤同样是按照顺序将非关键部分与还原后的非关键部分进行重新组合，从而得到二次加密后的人脸识别信息，并且二次加密后的人脸识别信息与原始的人脸识别信息结构相同。具体的，先获取原始人脸识别信息的初始结构，并且根据该初始结构生成原始人脸识别信息的结构模板，在所述结构模板中设置有用于放置关键部分的区域和非关键部分的区域，所以只需将原始关键部分与还原后的标准非关键部分填充到结构模板中的相应位置，即可完成还原的步骤，最终形成二次加密后的标准人脸识别信息。

S303、将二次加密后的标准人脸识别信息和用户身份信息进行关联，并保存所述二次加密后的标准人脸识别信息和用户身份信息的对应关系。

此步骤即将二次加密后的标准人脸识别信息和用户身份信息关联，即将标准人脸识别信

息与用户身份信息一一对应，然后将对应关系保存，最终需要利用二次加密后的标准人脸识别信息来确认用户身份。

所述步骤 S105 中，当用户在某一场景中进行身份识别时，例如需要通过门禁或者解锁电子设备，那么可以输入自身的人脸识别信息，然后将用户实时输入的人脸识别信息与所保存的二次加密的标准人脸识别信息进行比对，当比对一致时，代表用户身份识别通过，从而打开门禁或者解锁电子设备。

由于人脸识别信息也可能会被盗用，所以通过上述的二次加密可以使得即使人脸识别信息被盗，被盗的也仅仅是经过二次加密后的标准人脸识别信息，此标准人脸识别信息与真实的人脸识别信息有所区别，盗取人除了在当前应用场景下，无法在其他应用场景中使用该标准人脸识别信息，所以大大降低了安全风险。

在一实施例中，如图 4 所示，所述步骤 S105 包括步骤 S401~S403：

S401、对所述用户实时输入的目标人脸识别信息进行拆分，得到其中的目标关键部分和目标非关键部分；

此步骤是将实时输入的目标人脸识别信息进行拆分，从而得到关键部分和非关键部分，为了与二次加密后的标准人脸识别信息进行区分，所以此处将拆分得到的关键部分称为目标关键部分，将拆分得到的非关键部分称为目标非关键部分。

S402、对所述标准人脸识别信息进行拆分，得到其中的原始关键部分和标准非关键部分；

此步骤中，将二次加密后的标准人脸识别信息进行拆分，同样可以得到关键部分和非关键部分，为了与实时输入的目标人脸识别信息进行区分，所以此处将拆分得到的关键部分称为原始关键部分，将拆分得到的非关键部分称为标准非关键部分。

S403、分别从所述目标关键部分和原始关键部分中提取第一特征值和第二特征值，并将所述第一特征值和所述第二特征值进行匹配得到第一匹配度，当第一匹配度超过第一阈值时，则判定所述目标人脸识别信息的目标关键部分识别通过；所述目标人脸识别信息的关键部分识别通过后，分别从所述目标非关键部分和标准非关键部分中提取第三特征值和第四特征值，并将所述第三特征值和第四特征值进行匹配得到第二匹配度，当第二匹配度超过第二阈值时，则判定所述目标人脸识别信息的目标非关键部分识别通过，并确认身份识别成功；

此步骤是先对实时输入的目标人脸识别信息和二次加密后的标准人脸识别信息中的关键部分进行匹配，具体是分别提取目标关键部分和原始关键部分的特征值，然后将提取到的第一特征值和第二特征值进行匹配，从而计算出匹配度，此处计算出的匹配度称为第一匹配度。本申请实施例中对于关键部分和非关键部分的特征值提取方法，可以采用传统的提取方法，例如可以采用直方图特征提取方式或者边缘特征提取方式，本申请对此并不限定，即本申请可以采用现有的特征值提取方法来提取特征，只是本申请需要针对关键部分和非关键部分分别进行提取和处理，从而实现身份识别。匹配度的计算方式可以采用余弦相似度计算方式或者欧式距离计算方式。

由于对于二次加密后的标准人脸识别信息而言，其中的关键部分并未进行过修改，所以实时输入的目标人脸识别信息与二次加密后的标准人脸识别信息中的关键部分应该具有较高

的匹配度，故本申请实施例可以设置一个较高的第一阈值，这样如果计算出的第一匹配度大于第一阈值时，代表基本识别通过，但还不能确认非关键部分是否能够识别通过，所以后续步骤需要继续对非关键部分进行识别。

当所述目标人脸识别信息的目标关键部分识别通过后，提取所述目标非关键部分和标准非关键部分的特征值，并将提取到的第三特征值和第四特征值进行匹配得到第二匹配度，当第二匹配度超过第二阈值时，则判定所述目标人脸识别信息的目标非关键部分识别通过，并确认身份识别成功。

显然第二匹配度的大小与二次加密过程中修改的子区域的数量有较大关系，若修改的子区域越多，那么此处的第二匹配度就越小，若修改的子区域越少，那么此处的第二匹配度就越大，所以本申请实施例可以预先设置一个第二阈值，然后将第二匹配度与第二阈值进行比较，如果第二匹配度大于第二阈值，则认为所述目标人脸识别信息的目标非关键部分识别通过，实际上就代表了未修改的子区域基本匹配，所以可以判定所述目标人脸识别信息的目标非关键部分识别通过。

所述的第二阈值与修改的子区域的数量成反比，即修改的子区域的数量越多，那么可以将第二阈值设置成较小，修改的子区域的数量越少，则可以将第二阈值设置成较大。

在一实施例中，所述步骤 S105 之前，还包括：

接收用户输入的人脸比对请求，从所述人脸比对数据库中提取与所述人脸比对请求中用户识别码具有映射关系的标准人脸识别信息。

本实施例中，用户可先输入人脸比对请求，例如点击认证指令等，然后获取人脸比对请求中的用户识别码，再根据该用户识别码从人脸比对数据库中获取对应的标准人脸识别信息，从而对实时输入的目标人脸识别信息与标准人脸识别信息进行比对。

在一实施例中，所述的人脸识别信息的二次加密方法还包括：

当需要更换标准人脸识别信息时，将所述人脸比对信息数据库中的标准人脸识别信息删除，重新录入用户的原始人脸识别信息，然后对重新录入的原始人脸识别信息进行二次加密，并将二次加密后得到的标准人脸识别信息和用户身份信息进行关联保存。

本步骤中，当需要更换标准人脸识别信息时，只需重新录入用户的原始人脸识别信息，然后按照前述的方法对重新录入的原始人脸识别信息进行二次加密，使得二次加密后的标准人脸识别信息与原有的二次加密后的标准人脸识别信息不同，这样就可以实现随时更换人脸识别信息的目的，实现降低安全风险的目的。

用户可以定期更换标准人脸识别信息，实现与传统定期更换密码同样的效果，这样可以提高人脸识别信息的安全性。用户也可以随时更换标准人脸识别信息，实现与传统随时更换密码同样的效果，也能提高人脸识别信息的安全性。同时相比较于密码被盗用的情况，即使标准人脸识别信息被盗，由于其经过二次加密，所以也只能在当前应用场景下可能产生安全风险，而无法在其他应用场景下使用，所以二次加密的标准人脸识别信息被盗用产生的风险大大降低。

也就是说，本申请实施例中，在不同的应用场景下，可以采用不同的加密方案，这样即

使某个标准人脸识别信息被盗，也不会影响该用户在其他应用场景下的信息安全，从而降低了安全隐患。

本申请实施例还提供一种人脸识别信息的二次加密装置，该一种人脸识别信息的二次加密装置用于执行前述一种人脸识别信息的二次加密方法的任一实施例。具体地，请参阅图 5，图 5 是本申请实施例提供的人脸识别信息的二次加密装置的示意性框图。该人脸识别信息的二次加密装置 500 可以配置于服务器中。

该人脸识别信息的二次加密装置 500 可以包括：

录入单元 501，用于预先录入用户的原始人脸识别信息和用户身份信息；

拆分单元 502，用于从所述原始人脸识别信息中拆分出可用于身份识别的原始关键部分，并将所述原始人脸识别信息中的剩余部分作为原始非关键部分；

修改单元 503，用于将所述原始非关键部分拆分为若干个子区域，对所述若干子区域中的至少一个子区域进行修改；

组合单元 504，用于将修改后的子区域与未修改的子区域重新组合为标准非关键部分，并将所述标准非关键部分与所述原始关键部分进行拼接，实现对所述原始人脸识别信息的二次加密，将二次加密后得到的标准人脸识别信息和所述用户身份信息进行关联保存得到人脸比对信息数据库；

识别单元 505，用于当需要进行身份识别时，接收所述用户实时输入的目标人脸识别信息，将所述用户实时输入的目标人脸识别信息与所述人脸比对信息数据库中的标准人脸识别信息进行比对，当比对一致时，则确认身份识别成功。

在一实施例中，如图 6 所示，所述组合单元 504 包括：

拼接单元 601，用于对修改后的子区域进行标记，并按顺序将所述修改后的子区域与所述未修改的子区域进行拼接组合，形成还原后的所述标准非关键部分；

重新组合单元 602，用于获取所述原始人脸识别信息的初始结构，按照所述初始结构设置所述原始人脸识别信息的结构模板，将所述原始关键部分与还原后的所述标准非关键部分填充至所述结构模板中，形成二次加密后的标准人脸识别信息；

关联保存单元 603，用于将二次加密后的标准人脸识别信息和用户身份信息进行关联，并保存所述二次加密后的标准人脸识别信息和用户身份信息的对应关系。

在一实施例中，如图 7 所示，所述识别单元 505 包括：

第一拆分单元 701，用于对所述用户实时输入的目标人脸识别信息进行拆分，得到其中的目标关键部分和目标非关键部分；

第二拆分单元 702，用于对所述标准人脸识别信息进行拆分，得到其中的原始关键部分和标准非关键部分；

比对单元 703，用于分别从所述目标关键部分和原始关键部分中提取第一特征值和第二特征值，并将所述第一特征值和所述第二特征值进行匹配得到第一匹配度，当第一匹配度超过第一阈值时，则判定所述目标人脸识别信息的目标关键部分识别通过；所述目标人脸识别信息的关键部分识别通过后，分别从所述目标非关键部分和标准非关键部分中提取第三特征

值和第四特征值，并将所述第三特征值和第四特征值进行匹配得到第二匹配度，当第二匹配度超过第二阈值时，则判定所述目标人脸识别信息的目标非关键部分识别通过，并确认身份识别成功。

在一实施例中，如图 8 所示，所述修改单元 503 包括：

拆分子单元 801，用于将所述原始非关键部分拆分成数量不少于第三阈值的若干个子区域；

抽取单元 802，用于从所述若干个子区域中随机抽取数量不少于第四阈值的若干个子区域；

修改子单元 804，用于按照预设的修改方式对抽取到的若干子区域进行修改。

在一实施例中，所述修改子单元 804 包括：

特征图修改单元，用于从每一个抽取到的子区域中选择若干特征图，对所选择的特征图进行模糊、删除或者覆盖的操作，并保存修改后的子区域；

或者，特征图替换单元，用于从每一个抽取到的子区域中选择若干特征图，并从预设的特征库中随机选择同样数量的特征图，对选择的若干特征图进行替换，并保存修改后的子区域

在一实施例中，所述的人脸识别信息的二次加密装置 500 还包括：

提取单元，用于接收用户输入的人脸比对请求，从所述人脸比对数据库中提取与所述人脸比对请求中用户识别码具有映射关系的标准人脸识别信息。

在一实施例中，所述的人脸识别信息的二次加密装置 500 还包括：

更换单元，用于当需要更换标准人脸识别信息时，将所述人脸比对信息数据库中的标准人脸识别信息删除，重新录入用户的原始人脸识别信息，然后对重新录入的原始人脸识别信息进行二次加密，并将二次加密后得到的标准人脸识别信息和用户身份信息进行关联保存。

基于本申请实施例提供的人脸识别信息的二次加密装置 500，可以根据需要随时或定期更换人脸识别信息，从而提高人脸识别信息的安全性。

上述人脸识别信息的二次加密装置 500 可以实现为计算机程序的形式，该计算机程序可以在如图 9 所示的计算机设备上运行。

请参阅图 9，图 9 是本申请实施例提供的计算机设备的示意性框图。该计算机设备 9 是服务器，服务器可以是独立的服务器，也可以是多个服务器组成的服务器集群。

参阅图 9，该计算机设备 900 包括通过系统总线 901 连接的处理器 902、存储器和网络接口 905，其中，存储器可以包括非易失性存储介质 903 和内存储器 904。

该非易失性存储介质 903 可存储操作系统 9031 和计算机程序 9032。该计算机程序 9032 被执行时，可使得处理器 902 执行人脸识别信息的二次加密方法。

该处理器 902 用于提供计算和控制能力，支撑整个计算机设备 900 的运行。

该内存储器 904 为非易失性存储介质 903 中的计算机程序 9032 的运行提供环境，该计算机程序 9032 被处理器 902 执行时，可使得处理器 902 执行人脸识别信息的二次加密方法。

该网络接口 905 用于进行网络通信，如提供数据信息的传输等。本领域技术人员可以理

解，图 9 中示出的结构，仅仅是与本申请方案相关的部分结构的框图，并不构成对本申请方案所应用于其上的计算机设备 900 的限定，具体的计算机设备 900 可以包括比图中所示更多或更少的部件，或者组合某些部件，或者具有不同的部件布置。

其中，所述处理器 902 用于运行存储在存储器中的计算机程序 9032，以实现如下功能：预先录入用户的原始人脸识别信息和用户身份信息；从所述原始人脸识别信息中拆分出可用于身份识别的原始关键部分，并将所述原始人脸识别信息中的剩余部分作为原始非关键部分；将所述原始非关键部分拆分为若干个子区域，对所述若干子区域中的至少一个子区域进行修改；将修改后的子区域与未修改的子区域重新组合为标准非关键部分，并将所述标准非关键部分与所述原始关键部分进行拼接，实现对所述原始人脸识别信息的二次加密，将二次加密后得到的标准人脸识别信息和所述用户身份信息进行关联保存得到人脸比对信息数据库；当需要进行身份识别时，接收所述用户实时输入的目标人脸识别信息，将所述用户实时输入的目标人脸识别信息与所述人脸比对信息数据库中的标准人脸识别信息进行比对，当比对一致时，则确认身份识别成功。

本领域技术人员可以理解，图 9 中示出的计算机设备的实施例并不构成对计算机设备具体构成的限定，在其他实施例中，计算机设备可以包括比图示更多或更少的部件，或者组合某些部件，或者不同的部件布置。例如，在一些实施例中，计算机设备可以仅包括存储器及处理器，在这样的实施例中，存储器及处理器的结构及功能与图 9 所示实施例一致，在此不再赘述。

应当理解，在本申请实施例中，处理器 902 可以是中央处理单元 (Central Processing Unit，CPU)，该处理器 902 还可以是其他通用处理器、数字信号处理器 (Digital Signal Processor，DSP)、专用集成电路 (Application Specific Integrated Circuit，ASIC)、现成可编程门阵列 (Field-Programmable Gate Array，FPGA) 或者其他可编程逻辑器件、分立门或者晶体管逻辑器件、分立硬件组件等。其中，通用处理器可以是微处理器或者该处理器也可以是任何常规的处理器等。

在本申请的另一实施例中提供计算机可读存储介质。该计算机可读存储介质可以为非易失性的计算机可读存储介质，也可以是易失性的计算机可读存储介质。该计算机可读存储介质存储有计算机程序，其中计算机程序被处理器执行时实现以下步骤：预先录入用户的原始人脸识别信息和用户身份信息；从所述原始人脸识别信息中拆分出可用于身份识别的原始关键部分，并将所述原始人脸识别信息中的剩余部分作为原始非关键部分；将所述原始非关键部分拆分为若干个子区域，对所述若干子区域中的至少一个子区域进行修改；将修改后的子区域与未修改的子区域重新组合为标准非关键部分，并将所述标准非关键部分与所述原始关键部分进行拼接，实现对所述原始人脸识别信息的二次加密，将二次加密后得到的标准人脸识别信息和所述用户身份信息进行关联保存得到人脸比对信息数据库；当需要进行身份识别时，接收所述用户实时输入的目标人脸识别信息，将所述用户实时输入的目标人脸识别信息与所述人脸比对信息数据库中的标准人脸识别信息进行比对，当比对一致时，则确认身份识别成功。

所属领域的技术人员可以清楚地了解到，为了描述的方便和简洁，上述描述的设备、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。本领域普通技术人员可以意识到，结合本文中所公开的实施例描述的各示例的单元及算法步骤，能够以电子硬件、计算机软件或者二者的结合来实现，为了清楚地说明硬件和软件的可互换性，在上述说明中已经按照功能一般性地描述了各示例的组成及步骤。这些功能究竟以硬件还是软件方式来执行取决于技术方案的特定应用和设计约束条件。专业技术人员可以对每个特定的应用来使用不同方法来实现所描述的功能，但是这种实现不应认为超出本申请的范围。

在本申请所提供的几个实施例中，应该理解到，所揭露的设备、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，仅仅为逻辑功能划分，实际实现时可以有另外的划分方式，也可以将具有相同功能的单元集合成一个单元，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。另外，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，也可以是电的，机械的或其它的形式连接。

以上所述，仅为本申请的具体实施方式，但本申请的保护范围并不局限于此，任何熟悉本技术领域的技术人员在本申请揭露的技术范围内，可轻易想到各种等效的修改或替换，这些修改或替换都应涵盖在本申请的保护范围之内。因此，本申请的保护范围应以权利要求的保护范围为准。

权利要求书

1.一种人脸识别信息的二次加密方法，其中，包括：

预先录入用户的原始人脸识别信息和用户身份信息；

从所述原始人脸识别信息中拆分出可用于身份识别的原始关键部分，并将所述原始人脸识别信息中的剩余部分作为原始非关键部分；

将所述原始非关键部分拆分为若干个子区域，对所述若干子区域中的至少一个子区域进行修改；

将修改后的子区域与未修改的子区域重新组合为标准非关键部分，并将所述标准非关键部分与所述原始关键部分进行拼接，实现对所述原始人脸识别信息的二次加密，将二次加密后得到的标准人脸识别信息和所述用户身份信息进行关联保存得到人脸比对信息数据库；

当需要进行身份识别时，接收所述用户实时输入的目标人脸识别信息，将所述用户实时输入的目标人脸识别信息与所述人脸比对信息数据库中的标准人脸识别信息进行比对，当比对一致时，则确认身份识别成功。

2.根据权利要求 1 所述的人脸识别信息的二次加密方法，其中，所述将修改后的子区域与未修改的子区域重新组合为标准非关键部分，并将所述标准非关键部分与所述原始关键部分进行拼接，实现对所述原始人脸识别信息的二次加密，将二次加密后得到的标准人脸识别信息和所述用户身份信息进行关联保存得到人脸比对信息数据库，包括：

对修改后的子区域进行标记，并按顺序将所述修改后的子区域与所述未修改的子区域进行拼接组合，形成还原后的所述标准非关键部分；

获取所述原始人脸识别信息的初始结构，按照所述初始结构设置所述原始人脸识别信息的结构模板，将所述原始关键部分与还原后的所述标准非关键部分填充至所述结构模板中，形成二次加密后的标准人脸识别信息；

将二次加密后的标准人脸识别信息和用户身份信息进行关联，并保存所述二次加密后的标准人脸识别信息和用户身份信息的对应关系。

3.根据权利要求 1 所述的人脸识别信息的二次加密方法，其中，所述将所述用户实时输入的目标人脸识别信息与所述人脸比对信息数据库中的标准人脸识别信息进行比对，当比对一致时，则确认身份识别成功，包括：

对所述用户实时输入的目标人脸识别信息进行拆分，得到其中的目标关键部分和目标非关键部分；

对所述标准人脸识别信息进行拆分，得到其中的原始关键部分和标准非关键部分；

分别从所述目标关键部分和原始关键部分中提取第一特征值和第二特征值，并将所述第一特征值和所述第二特征值进行匹配得到第一匹配度，当第一匹配度超过第一阈值时，则判定所述目标人脸识别信息的目标关键部分识别通过；所述目标人脸识别信息的关键部分识别通过后，分别从所述目标非关键部分和标准非关键部分中提取第三特征值和第四特征值，并将所述第三特征值和第四特征值进行匹配得到第二匹配度，当第二匹配度超过第二阈值时，

则判定所述目标人脸识别信息的目标非关键部分识别通过，并确认身份识别成功。

4.根据权利要求 1 所述的人脸识别信息的二次加密方法，其中，所述将所述原始非关键部分拆分为若干个子区域，对所述若干子区域中的至少一个子区域进行修改，包括：

将所述原始非关键部分拆分成数量不少于第三阈值的若干个子区域；

从所述若干个子区域中随机抽取数量不少于第四阈值的若干个子区域；

按照预设的修改方式对抽取到的若干子区域进行修改。

5.根据权利要求 4 所述的人脸识别信息的二次加密方法，其中，所述按照预设的修改方式对抽取到的若干子区域进行修改，包括：

从每一个抽取到的子区域中选择若干特征图，对所选择的特征图进行模糊、删除或者覆盖的操作，并保存修改后的子区域；

或者，从每一个抽取到的子区域中选择若干特征图，并从预设的特征库中随机选择同样数量的特征图，对选择的若干特征图进行替换，并保存修改后的子区域。

6.根据权利要求 1 所述的人脸识别信息的二次加密方法，其中，所述当需要进行身份识别时，接收所述用户实时输入的目标人脸识别信息，将所述用户实时输入的目标人脸识别信息与所述人脸比对信息数据库中的标准人脸识别信息进行比对，当比对一致时，则确认身份识别成功之前，还包括：

接收用户输入的人脸比对请求，从所述人脸比对数据库中提取与所述人脸比对请求中用户识别码具有映射关系的标准人脸识别信息。

7.根据权利要求 1 所述的人脸识别信息的二次加密方法，其中，还包括：

当需要更换标准人脸识别信息时，将所述人脸比对信息数据库中的标准人脸识别信息删除，重新录入用户的原始人脸识别信息，然后对重新录入的原始人脸识别信息进行二次加密，并将二次加密后得到的标准人脸识别信息和用户身份信息进行关联保存。

8.一种人脸识别信息的二次加密装置，其中，包括：

录入单元，用于预先录入用户的原始人脸识别信息和用户身份信息；

拆分单元，用于从所述原始人脸识别信息中拆分出可用于身份识别的原始关键部分，并将所述原始人脸识别信息中的剩余部分作为原始非关键部分；

修改单元，用于将所述原始非关键部分拆分为若干个子区域，对所述若干子区域中的至少一个子区域进行修改；

组合单元，用于将修改后的子区域与未修改的子区域重新组合为标准非关键部分，并将所述标准非关键部分与所述原始关键部分进行拼接，实现对所述原始人脸识别信息的二次加密，将二次加密后得到的标准人脸识别信息和所述用户身份信息进行关联保存得到人脸比对信息数据库；

识别单元，用于当需要进行身份识别时，接收所述用户实时输入的目标人脸识别信息，将所述用户实时输入的目标人脸识别信息与所述人脸比对信息数据库中的标准人脸识别信息进行比对，当比对一致时，则确认身份识别成功。

9.一种计算机设备，包括存储器、处理器及存储在所述存储器上并可在所述处理器上运

行的计算机程序，其中，所述处理器执行所述计算机程序时实现如权利要求 1 所述的人脸识别信息的二次加密方法。

10.根据权利要求 9 所述的计算机设备，其中，所述将修改后的子区域与未修改的子区域重新组合为标准非关键部分，并将所述标准非关键部分与所述原始关键部分进行拼接，实现对所述原始人脸识别信息的二次加密，将二次加密后得到的标准人脸识别信息和所述用户身份信息进行关联保存得到人脸比对信息数据库，包括：

对修改后的子区域进行标记，并按顺序将所述修改后的子区域与所述未修改的子区域进行拼接组合，形成还原后的所述标准非关键部分；

获取所述原始人脸识别信息的初始结构，按照所述初始结构设置所述原始人脸识别信息的结构模板，将所述原始关键部分与还原后的所述标准非关键部分填充至所述结构模板中，形成二次加密后的标准人脸识别信息；

将二次加密后的标准人脸识别信息和用户身份信息进行关联，并保存所述二次加密后的标准人脸识别信息和用户身份信息的对应关系。

11.根据权利要求 9 所述的计算机设备，其中，所述将所述用户实时输入的目标人脸识别信息与所述人脸比对信息数据库中的标准人脸识别信息进行比对，当比对一致时，则确认身份识别成功，包括：

对所述用户实时输入的目标人脸识别信息进行拆分，得到其中的目标关键部分和目标非关键部分；

对所述标准人脸识别信息进行拆分，得到其中的原始关键部分和标准非关键部分；

分别从所述目标关键部分和原始关键部分中提取第一特征值和第二特征值，并将所述第一特征值和所述第二特征值进行匹配得到第一匹配度，当第一匹配度超过第一阈值时，则判定所述目标人脸识别信息的目标关键部分识别通过；所述目标人脸识别信息的关键部分识别通过后，分别从所述目标非关键部分和标准非关键部分中提取第三特征值和第四特征值，并将所述第三特征值和第四特征值进行匹配得到第二匹配度，当第二匹配度超过第二阈值时，则判定所述目标人脸识别信息的目标非关键部分识别通过，并确认身份识别成功。

12.根据权利要求 9 所述的计算机设备，其中，所述将所述原始非关键部分拆分为若干个子区域，对所述若干子区域中的至少一个子区域进行修改，包括：

将所述原始非关键部分拆分成数量不少于第三阈值的若干个子区域；

从所述若干个子区域中随机抽取数量不少于第四阈值的若干个子区域；

按照预设的修改方式对抽取到的若干子区域进行修改。

13.根据权利要求 12 所述的计算机设备，其中，所述按照预设的修改方式对抽取到的若干子区域进行修改，包括：

从每一个抽取到的子区域中选择若干特征图，对所选择的特征图进行模糊、删除或者覆盖的操作，并保存修改后的子区域；

或者，从每一个抽取到的子区域中选择若干特征图，并从预设的特征库中随机选择同样数量的特征图，对选择的若干特征图进行替换，并保存修改后的子区域。

14.根据权利要求 9 所述的计算机设备，其中，所述当需要进行身份识别时，接收所述用户实时输入的目标人脸识别信息，将所述用户实时输入的目标人脸识别信息与所述人脸比对信息数据库中的标准人脸识别信息进行比对，当比对一致时，则确认身份识别成功之前，还包括：

接收用户输入的人脸比对请求，从所述人脸比对数据库中提取与所述人脸比对请求中用户识别码具有映射关系的标准人脸识别信息。

15.一种计算机可读存储介质，其中，所述计算机可读存储介质存储有计算机程序，所述计算机程序当被处理器执行时使所述处理器执行如权利要求 1 所述的人脸识别信息的二次加密方法。

16.根据权利要求 15 所述的计算机可读存储介质，其中，所述将修改后的子区域与未修改的子区域重新组合为标准非关键部分，并将所述标准非关键部分与所述原始关键部分进行拼接，实现对所述原始人脸识别信息的二次加密，将二次加密后得到的标准人脸识别信息和所述用户身份信息进行关联保存得到人脸比对信息数据库，包括：

对修改后的子区域进行标记，并按顺序将所述修改后的子区域与所述未修改的子区域进行拼接组合，形成还原后的所述标准非关键部分；

获取所述原始人脸识别信息的初始结构，按照所述初始结构设置所述原始人脸识别信息的结构模板，将所述原始关键部分与还原后的所述标准非关键部分填充至所述结构模板中，形成二次加密后的标准人脸识别信息；

将二次加密后的标准人脸识别信息和用户身份信息进行关联，并保存所述二次加密后的标准人脸识别信息和用户身份信息的对应关系。

17.根据权利要求 15 所述的计算机可读存储介质，其中，所述将所述用户实时输入的目标人脸识别信息与所述人脸比对信息数据库中的标准人脸识别信息进行比对，当比对一致时，则确认身份识别成功，包括：

对所述用户实时输入的目标人脸识别信息进行拆分，得到其中的目标关键部分和目标非关键部分；

对所述标准人脸识别信息进行拆分，得到其中的原始关键部分和标准非关键部分；

分别从所述目标关键部分和原始关键部分中提取第一特征值和第二特征值，并将所述第一特征值和所述第二特征值进行匹配得到第一匹配度，当第一匹配度超过第一阈值时，则判定所述目标人脸识别信息的目标关键部分识别通过；所述目标人脸识别信息的关键部分识别通过后，分别从所述目标非关键部分和标准非关键部分中提取第三特征值和第四特征值，并将所述第三特征值和第四特征值进行匹配得到第二匹配度，当第二匹配度超过第二阈值时，则判定所述目标人脸识别信息的目标非关键部分识别通过，并确认身份识别成功。

18.根据权利要求 15 所述的计算机可读存储介质，其中，所述将所述原始非关键部分拆分为若干个子区域，对所述若干子区域中的至少一个子区域进行修改，包括：

将所述原始非关键部分拆分成数量不少于第三阈值的若干个子区域；

从所述若干个子区域中随机抽取数量不少于第四阈值的若干个子区域；

按照预设的修改方式对抽取到的若干子区域进行修改。

19.根据权利要求 18 所述的计算机可读存储介质，其中，所述按照预设的修改方式对抽取到的若干子区域进行修改，包括：

从每一个抽取到的子区域中选择若干特征图，对所选择的特征图进行模糊、删除或者覆盖的操作，并保存修改后的子区域；

或者，从每一个抽取到的子区域中选择若干特征图，并从预设的特征库中随机选择同样数量的特征图，对选择的若干特征图进行替换，并保存修改后的子区域。

20.根据权利要求 15 所述的计算机可读存储介质，其中，所述当需要进行身份识别时，接收所述用户实时输入的目标人脸识别信息，将所述用户实时输入的目标人脸识别信息与所述人脸比对信息数据库中的标准人脸识别信息进行比对，当比对一致时，则确认身份识别成功之前，还包括：

接收用户输入的人脸比对请求，从所述人脸比对数据库中提取与所述人脸比对请求中用户识别码具有映射关系的标准人脸识别信息。

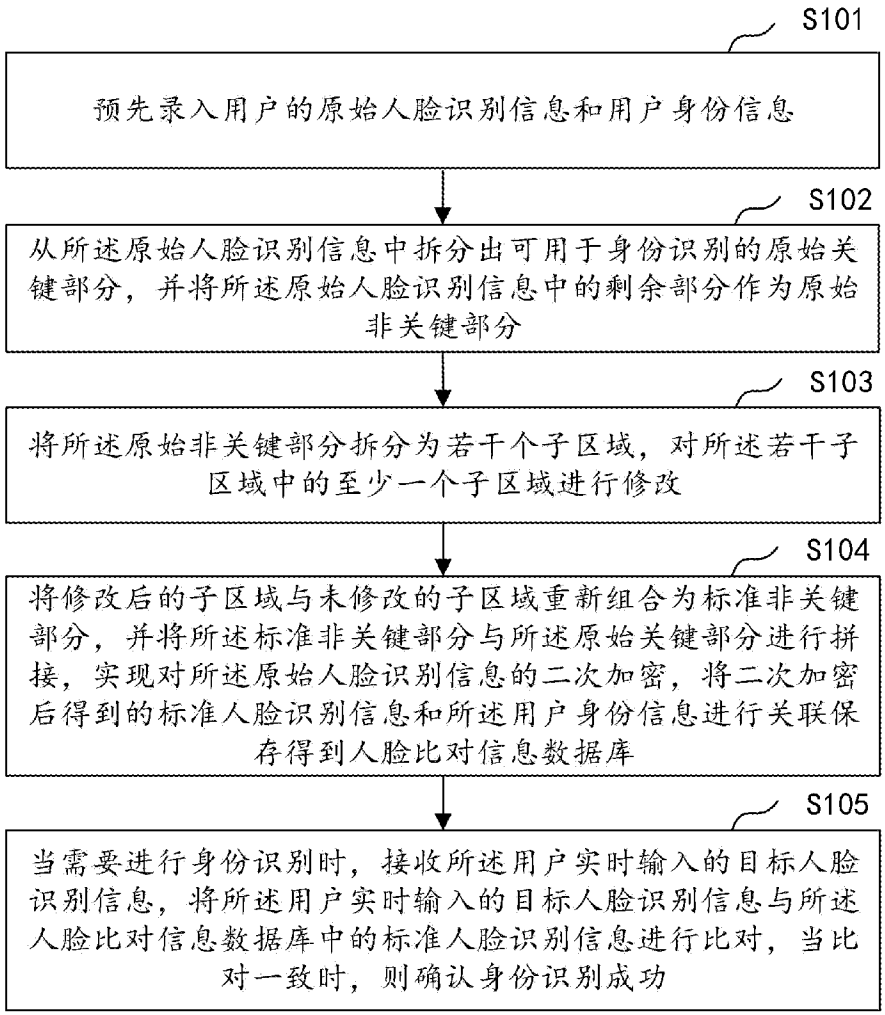
S101
预先录入用户的原始人脸识别信息和用户身份信息
S102
从所述原始人脸识别信息中拆分出可用于身份识别的原始关键部分，并将所述原始人脸识别信息中的剩余部分作为原始非关键部分
S103
将所述原始非关键部分拆分为若干个子区域，对所述若干子区域中的至少一个子区域进行修改
S104
将修改后的子区域与未修改的子区域重新组合为标准非关键部分，并将所述标准非关键部分与所述原始关键部分进行拼接，实现对所述原始人脸识别信息的二次加密，将二次加密后得到的标准人脸识别信息和所述用户身份信息进行关联保存得到人脸比对信息数据库
S105
当需要进行身份识别时，接收所述用户实时输入的目标人脸识别信息，将所述用户实时输入的目标人脸识别信息与所述人脸比对信息数据库中的标准人脸识别信息进行比对，当比对一致时，则确认身份识别成功

图 1

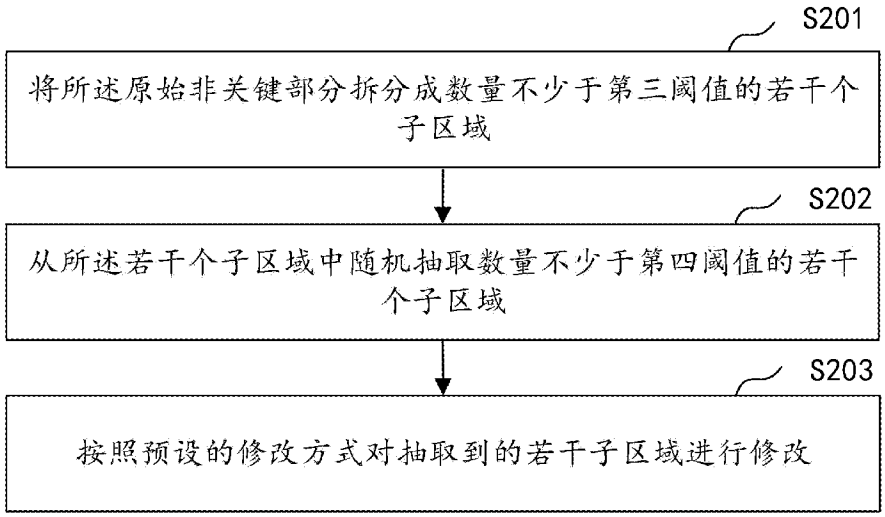
S201
将所述原始非关键部分拆分成数量不少于第三阈值的若干个子区域
S202
从所述若干个子区域中随机抽取数量不少于第四阈值的若干个子区域
S203
按照预设的修改方式对抽取到的若干子区域进行修改

图 2

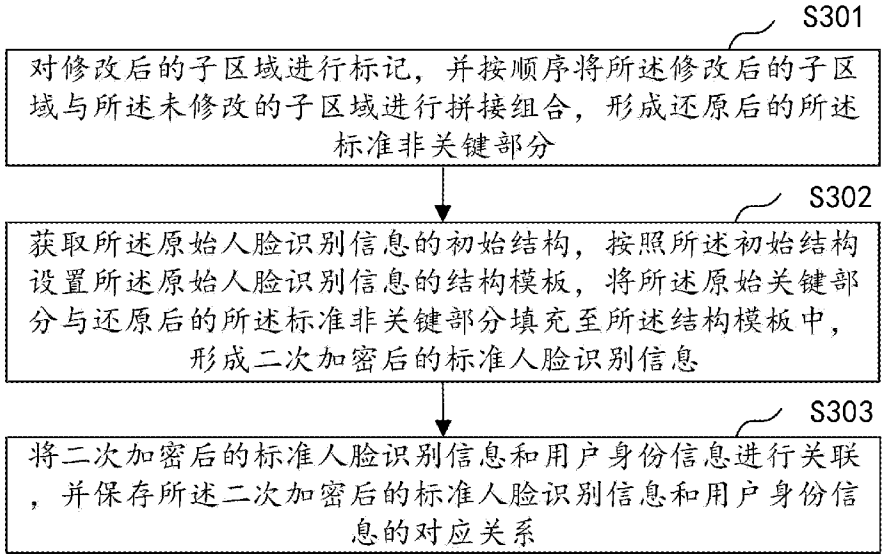
S301
对修改后的子区域进行标记，并按顺序将所述修改后的子区域与所述未修改的子区域进行拼接组合，形成还原后的所述标准非关键部分
S302
获取所述原始人脸识别信息的初始结构，按照所述初始结构设置所述原始人脸识别信息的结构模板，将所述原始关键部分与还原后的所述标准非关键部分填充至所述结构模板中，形成二次加密后的标准人脸识别信息
S303
将二次加密后的标准人脸识别信息和用户身份信息进行关联，并保存所述二次加密后的标准人脸识别信息和用户身份信息的对应关系

图 3

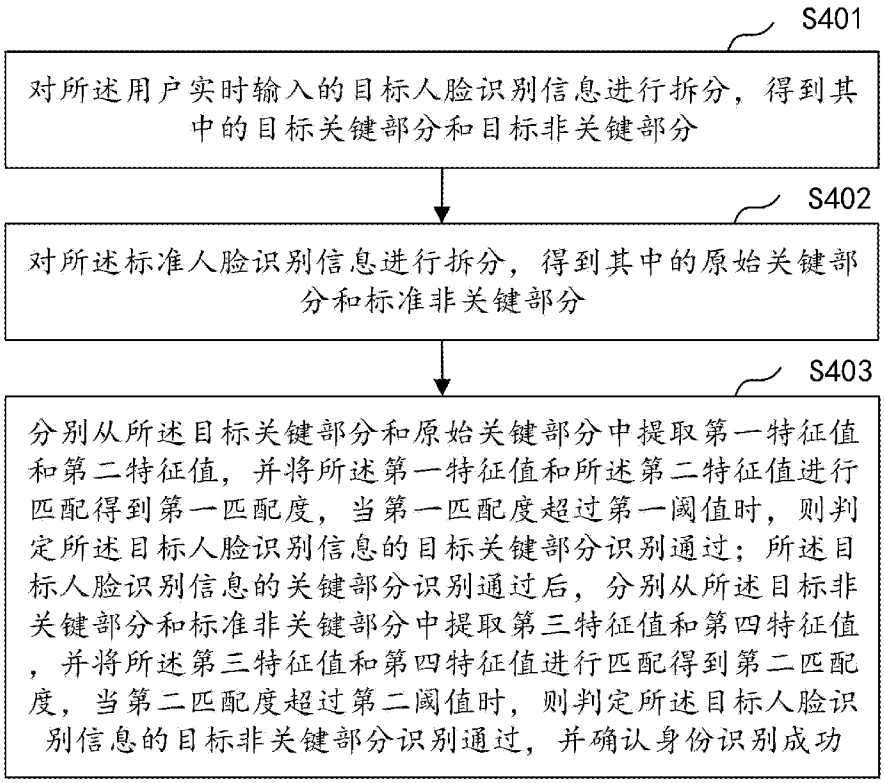
S401
对所述用户实时输入的目标人脸识别信息进行拆分，得到其中的目标关键部分和目标非关键部分
S402
对所述标准人脸识别信息进行拆分，得到其中的原始关键部分和标准非关键部分
S403
分别从所述目标关键部分和原始关键部分中提取第一特征值和第二特征值，并将所述第一特征值和所述第二特征值进行匹配得到第一匹配度，当第一匹配度超过第一阈值时，则判定所述目标人脸识别信息的目标关键部分识别通过；所述目标人脸识别信息的关键部分识别通过后，分别从所述目标非关键部分和标准非关键部分中提取第三特征值和第四特征值，并将所述第三特征值和第四特征值进行匹配得到第二匹配度，当第二匹配度超过第二阈值时，则判定所述目标人脸识别信息的目标非关键部分识别通过，并确认身份识别成功

图 4

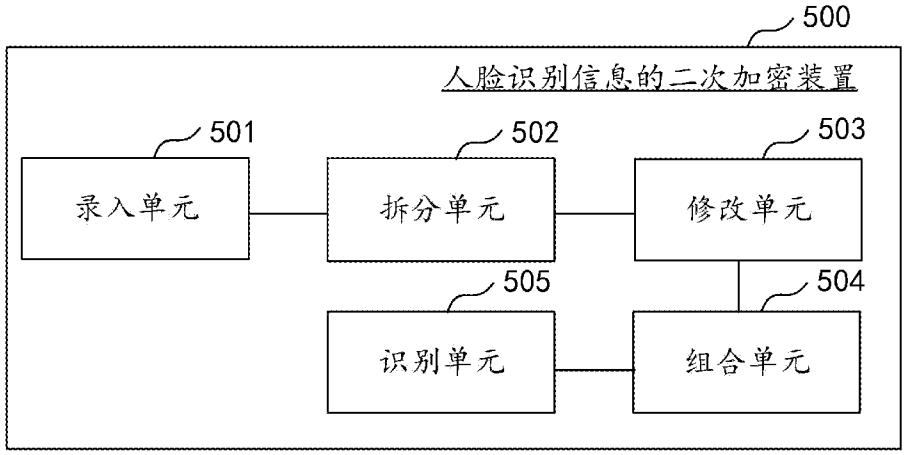
500
人脸识别信息的二次加密装置
501
录入单元
502
拆分单元
503
修改单元
505
识别单元
504
组合单元

图 5

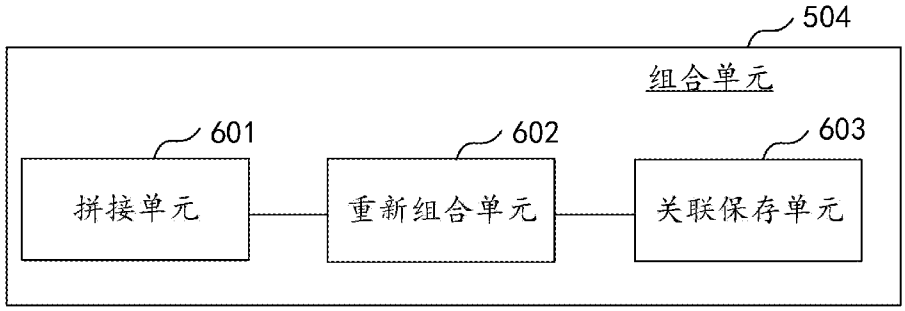
504
组合单元
601
拼接单元
602
重新组合单元
603
关联保存单元

图 6

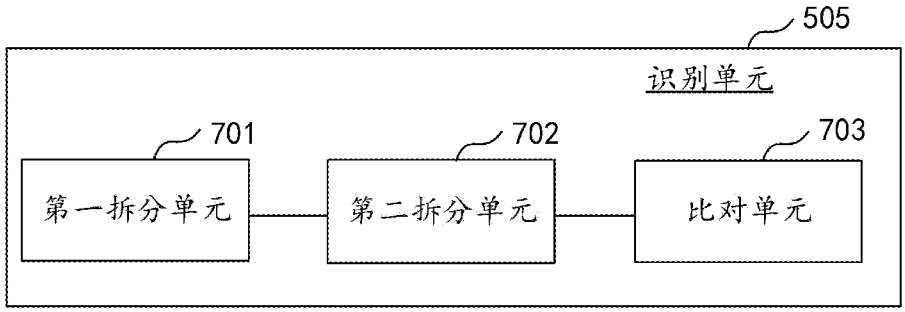
505
识别单元
701
第一拆分单元
702
第二拆分单元
703
比对单元

图 7

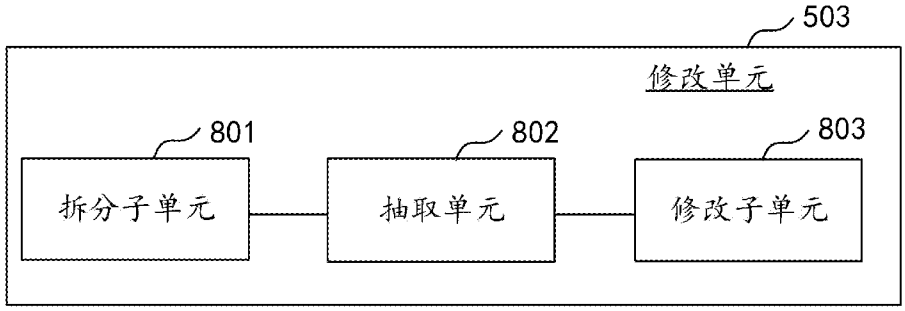
503
修改单元
801
拆分子单元
802
抽取单元
803
修改子单元

图 8

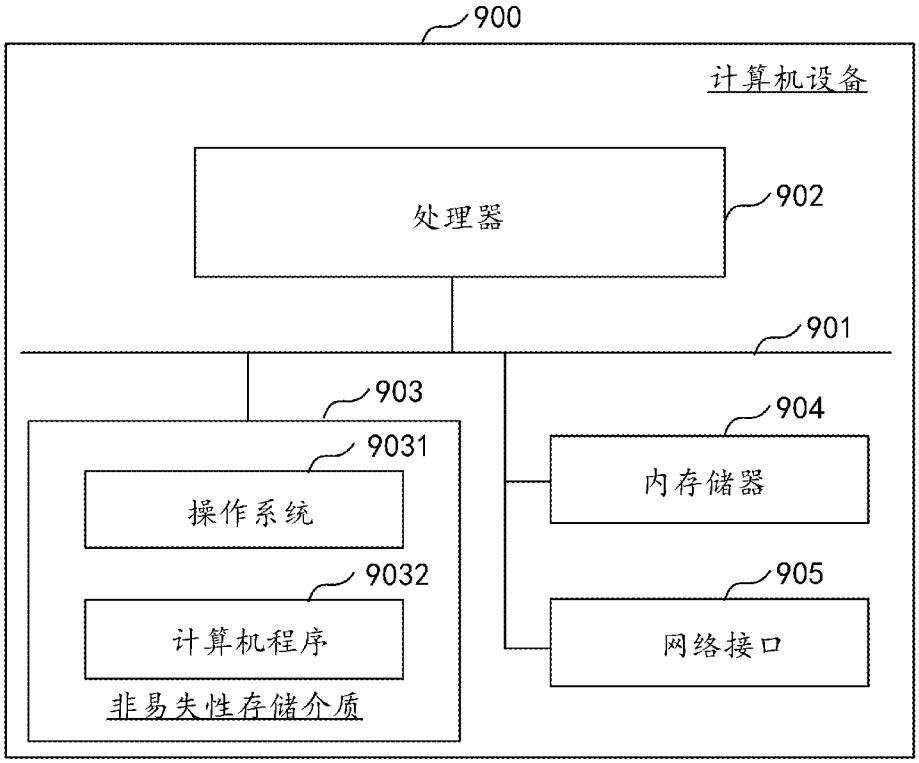
900
计算机设备
处理器
902
901
903
9031
操作系统
9032
计算机程序
非易失性存储介质
904
内存储器
905
网络接口

图 9

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2021/090564

A. CLASSIFICATION OF SUBJECT MATTER

G06K 9/00(2006.01)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)

G06K

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)

CNPAT, CNKI, WPI, EPODOC: 人脸, 指纹, 生物特征, 识别, 关键, 基础, 划分, 拆分, 加密, 修改, 安全, face, identification, encryption, key, splice, safety, biological, modify

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 112183496 A (PING AN TECHNOLOGY (SHENZHEN) CO., LTD.) 05 January 2021 (2021-01-05) description, paragraphs [0033]-[0124]	1-20
A	CN 106897590 A (ALIBABA GROUP HOLDING LIMITED) 27 June 2017 (2017-06-27) description paragraphs [0021]-[0095]	1-20
A	CN 109492407 A (ZTE CORPORATION) 19 March 2019 (2019-03-19) entire document	1-20
A	CN 110119608 A (ALIBABA GROUP HOLDING LIMITED) 13 August 2019 (2019-08-13) entire document	1-20
A	US 2014072185 A1 (DUNLAP, David D. et al.) 13 March 2014 (2014-03-13) 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
"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
20 July 2021	**04 August 2021**
Name and mailing address of the ISA/CN **China National Intellectual Property Administration (ISA/CN)** **No. 6, Xitucheng Road, Jimenqiao, Haidian District, Beijing 100088, China** Facsimile No. **(86-10)62019451**	Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2021/090564

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN 112183496 A	05 January 2021	None	
CN 106897590 A	27 June 2017	HK1237931 A0	20 April 2018
CN 109492407 A	19 March 2019	None	
CN 110119608 A	13 August 2019	CN 104951680 A	30 September 2015
		HK 1211106 A1	13 May 2016
US 2014072185 A1	13 March 2014	US 2017308740 A1	26 October 2017

国际检索报告

国际申请号
PCT/CN2021/090564

A. 主题的分类

G06K 9/00(2006.01)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)

G06K

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））

CNPAT, CNKI, WPI, EPODOC：人脸，指纹，生物特征，识别，关键，基础，划分，拆分，加密，修改，安全，face, identification, encryption, key, splice, safety, biological, modify

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
PX	CN 112183496 A (平安科技深圳有限公司) 2021年 1月 5日 (2021-01-05) 说明书第[0033]-[0124]段	1-20
A	CN 106897590 A (阿里巴巴集团控股有限公司) 2017年 6月 27日 (2017-06-27) 说明书第[0021]-[0095]段	1-20
A	CN 109492407 A (中兴通讯股份有限公司) 2019年 3月 19日 (2019-03-19) 全文	1-20
A	CN 110119608 A (阿里巴巴集团控股有限公司) 2019年 8月 13日 (2019-08-13) 全文	1-20
A	US 2014072185 A1 (DUNLAP, David D. 等) 2014年 3月 13日 (2014-03-13) 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

“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
2021年 7月 20日	2021年 8月 4日

ISA/CN的名称和邮寄地址	受权官员
中国国家知识产权局(ISA/CN) 中国 北京市海淀区蓟门桥西土城路6号 100088	梁艳
传真号 (86-10)62019451	电话号码 86-(10)-53961298

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2021/090564

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	112183496	A	2021年 1月 5日	无			
CN	106897590	A	2017年 6月 27日	HK1237931	A0		2018年 4月 20日
CN	109492407	A	2019年 3月 19日	无			
CN	110119608	A	2019年 8月 13日	CN	104951680	A	2015年 9月 30日
				HK	1211106	A1	2016年 5月 13日
US	2014072185	A1	2014年 3月 13日	US	2017308740	A1	2017年 10月 26日