

(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
2024 年 7 月 25 日 (25.07.2024)



(10) 国际公布号
WO 2024/152768 A1

(51) 国际专利分类号:
G06F 21/62 (2013.01)

(21) 国际申请号: PCT/CN2023/136119

(22) 国际申请日: 2023 年 12 月 4 日 (04.12.2023)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
202310095121.8 2023 年 1 月 20 日 (20.01.2023) CN

(71) 申请人: 中国银联股份有限公司 (CHINA UNIONPAY CO., LTD.) [CN/CN]; 中国上海市浦东新区含笑路 36 号, Shanghai 200135 (CN)。

(72) 发明人: 刘红宝 (LIU, Hongbao); 中国上海市浦东新区含笑路 36 号, Shanghai 200135 (CN)。邱震尧 (QIU, Zhenyao); 中国上海市浦东新区含笑路 36 号, Shanghai 200135 (CN)。秦璐 (QIN, Lu); 中国上海市浦东新区含笑路 36 号, Shanghai 200135 (CN)。汤韬 (TANG, Tao); 中国上海市浦东新区含笑路 36 号, Shanghai 200135 (CN)。高鹏飞 (GAO, Pengfei); 中国上海市浦东新区含笑路 36 号, Shanghai 200135 (CN)。何朔 (HE, Shuo);

中国上海市浦东新区含笑路 36 号, Shanghai 200135 (CN)。郑建宾 (ZHENG, Jianbin); 中国上海市浦东新区含笑路 36 号, Shanghai 200135 (CN)。杨阳 (YANG, Yang); 中国上海市浦东新区含笑路 36 号, Shanghai 200135 (CN)。

(74) 代理人: 北京东方亿思知识产权代理有限公司 (BEIJING EAST IP LTD.); 中国北京市东城区东长安街 1 号东方广场东方经贸城东 2 座 1601 室, Beijing 100738 (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, MU, 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,

(54) Title: BIOLOGICAL FEATURE MATCHING METHOD, TERMINAL DEVICE, SERVER, SYSTEM, AND MEDIUM

(54) 发明名称: 生物特征匹配方法、终端设备、服务器、系统及介质

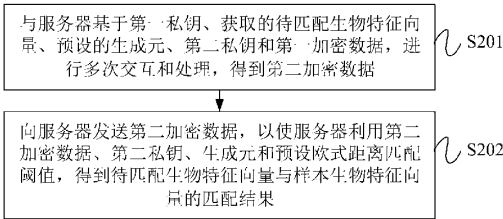


图 2

- S201 Perform multiple instances of interaction and processing with a server on the basis of a first private key, an acquired biological feature vector to be matched, a preset generator, a second private key, and first encrypted data, so as to obtain second encrypted data
- S202 Send the second encrypted data to the server, such that the server uses the second encrypted data, the second private key, the generator and a preset Euclidean distance matching threshold to obtain a matching result between the biological feature vector to be matched and a sample biological feature vector

(57) Abstract: The present application belongs to the field of data processing. Disclosed are a biological feature matching method, a terminal device, a server, a system, and a medium. The method comprises: performing multiple instances of interaction and processing with a server on the basis of a first private key, an acquired biological feature vector to be matched, a preset generator, a second private key, and first encrypted data, so as to obtain second encrypted data (S201), wherein the first encrypted data is obtained by means of a terminal device pre-encrypting a sample biological feature vector using the generator and the first private key, and is sent to the server, and a computing operator which includes the second private key and a target Euclidean distance is formed in the second encrypted data; and sending the second encrypted data to the server, such that the server uses the second encrypted data, the generator, the second private key and a preset Euclidean distance matching threshold to obtain a matching result between the biological feature vector to be matched and the sample biological feature vector (S202).

[见续页]

WO 2024/152768 A1

NA, RW, SC, 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))。

(57) 摘要: 本申请公开了一种生物特征匹配方法、终端设备、服务器、系统及介质, 属于数据处理领域。
方法包括: 与服务器基于第一私钥、获取的待匹配生物特征向量、预设的生成元、第二私钥和第一加密数据, 进行多次交互和处理, 得到第二加密数据 (S201), 第一加密数据由终端设备预先利用生成元和第一私钥对样本生物特征向量加密得到并发送至服务器, 第二加密数据中形成包括第二私钥和目标欧氏距离的计算算子; 向服务器发送第二加密数据, 以使服务器利用第二加密数据、生成元、第二私钥和预设欧式距离匹配阈值, 得到待匹配生物特征向量与样本生物特征向量的匹配结果 (S202)。