احراز هویت غیرحضوری

متقاضیان خدمات الکترونیک انتظامی

بر مبنای سنجه‌های بیومتریکی

هدف طرح

هدف اصلی

مطالعه و بررسی روش‌های احراز هویت غیرحضوری مبتنی بر تشخیص چهره و پیاده‌سازی نسخه پایلوت

اهداف کاربردی

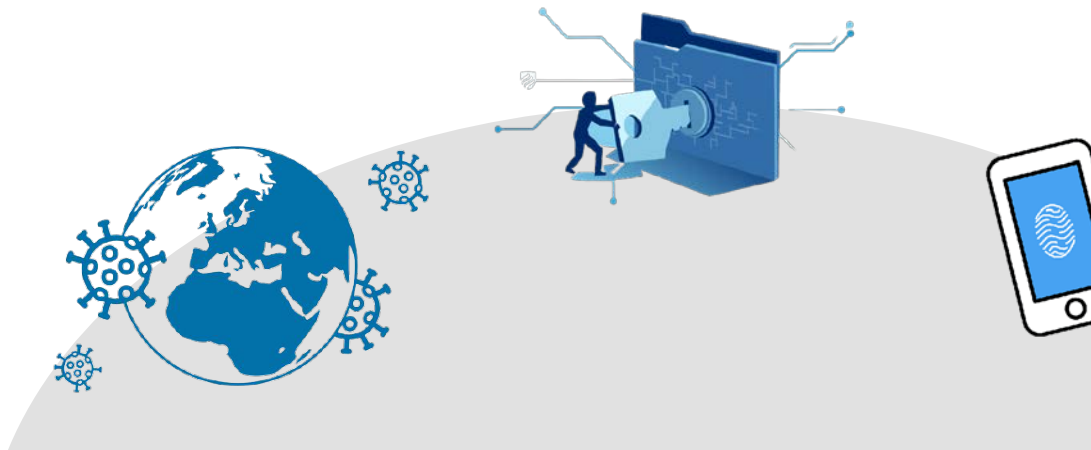
- توسعه پلیس هوشمند و فناور
- فراهم کردن بستری برای توجه به سلامت شهری
- ارتقاء امنیت ملی و افزایش اشرافیت اطلاعاتی
- توسعه خدمات الکترونیک انتظامی
- کاهش اصطکاک و روبرویی پلیس با مردم
- ارتقاء اعتبار و جایگاه پلیس

اهداف فنی

- اشراف بر روش‌ها و مبانی احراز هویت
- دستیابی به ماژول تایید هویت مبتنی بر چهره
- دستیابی به ماژول تشخیص زنده بودن
- امن‌سازی و تبادل اطلاعات در فرایند احراز هویت غیرحضوری
- راه‌اندازی سرویس احراز هویت غیرحضوری

ضرورت طرح

- تقاضای روزافزون ارائه خدمات الکترونیکی و غیرحضوری از سمت مردم
- تاکید نهادهای قانون‌گذار بر ارائه خدمات الکترونیکی و غیرحضوری به مردم به ویژه با تشدید موضوع در کرونا
- ضرورت افزایش امنیت و اشراف اطلاعاتی پلیس با تکمیل پایگاه‌های داده افراد به ویژه در تکمیل اطلاعات زیست‌سنجی
- لزوم کاهش خطاهای انسانی و سواستفاده افراد از اطلاعات و اسناد



منافع طرح برای پلیس . . .

- کمک به تحقق پلیس هوشمند و ارائه خدمات غیرحضوری توسط نیروی انتظامی
- همراستایی با اهداف بالادستی کشور و در راستای تحقق دولت الکترونیک
- تصویرسازی نوآورانه و به‌روز بودن مبتنی بر فناوری از پلیس
- کمک به تحقق مسئولیت‌های پلیس در ارائه ساده و آسان خدمات با رعایت سلامتی شهروندان به ویژه در بحران‌هایی مانند کرونا
- کمک به اشراف اطلاعاتی پلیس و فراهم شدن امکان اعمال کنترل‌های امنیتی قوی‌تر و دقیق‌تر بر اساس روش‌های فناورانه مبتنی بر بیومتریک
- کاهش مراجعات حضوری به دفاتر و کم کردن مشکلات ناشی از آن
- کاهش احتمال خطای انسانی و یا کم‌توجهی نیروهای انسانی
- فراهم کردن دسترسی ۲۴*۷ و حتی در روزهای تعطیل به خدمات
- فراهم کردن امکان نگاشت اطلاعات مختلف افراد به همدیگر در پایگاه داده‌های مختلف (کد ملی، اطلاعات گذرنامه، اطلاعات گواهینامه و ...)

منافع طرح برای پلیس . . .

- **تسریع در تطبیق‌پذیری**
  - با تغییر مقررات، سیستم‌های کنترل دسترسی باید به طور متناوب تغییر کنند. فرایندهای احراز هویت در مواردی که نیاز به تغییر سریع دارد، می‌تواند به سادگی در سامانه به‌روز می‌شود و خیلی سریع با شرایط جدید سازگار شود.

- **یکپارچه‌سازی**
  - eKYCدر بیشتر موارد، با استفاده از APIها، قابلیت احراز هویت را به آسانی به سایر سامانه‌ها اضافه می‌کند. همچنین، داده‌های مشتری، اسناد و اطلاعات به طور ایمن در سوابق الکترونیکی او ذخیره می‌شوند و در صورت لزوم در سایر سامانه‌ها قابل استفاده هستند.

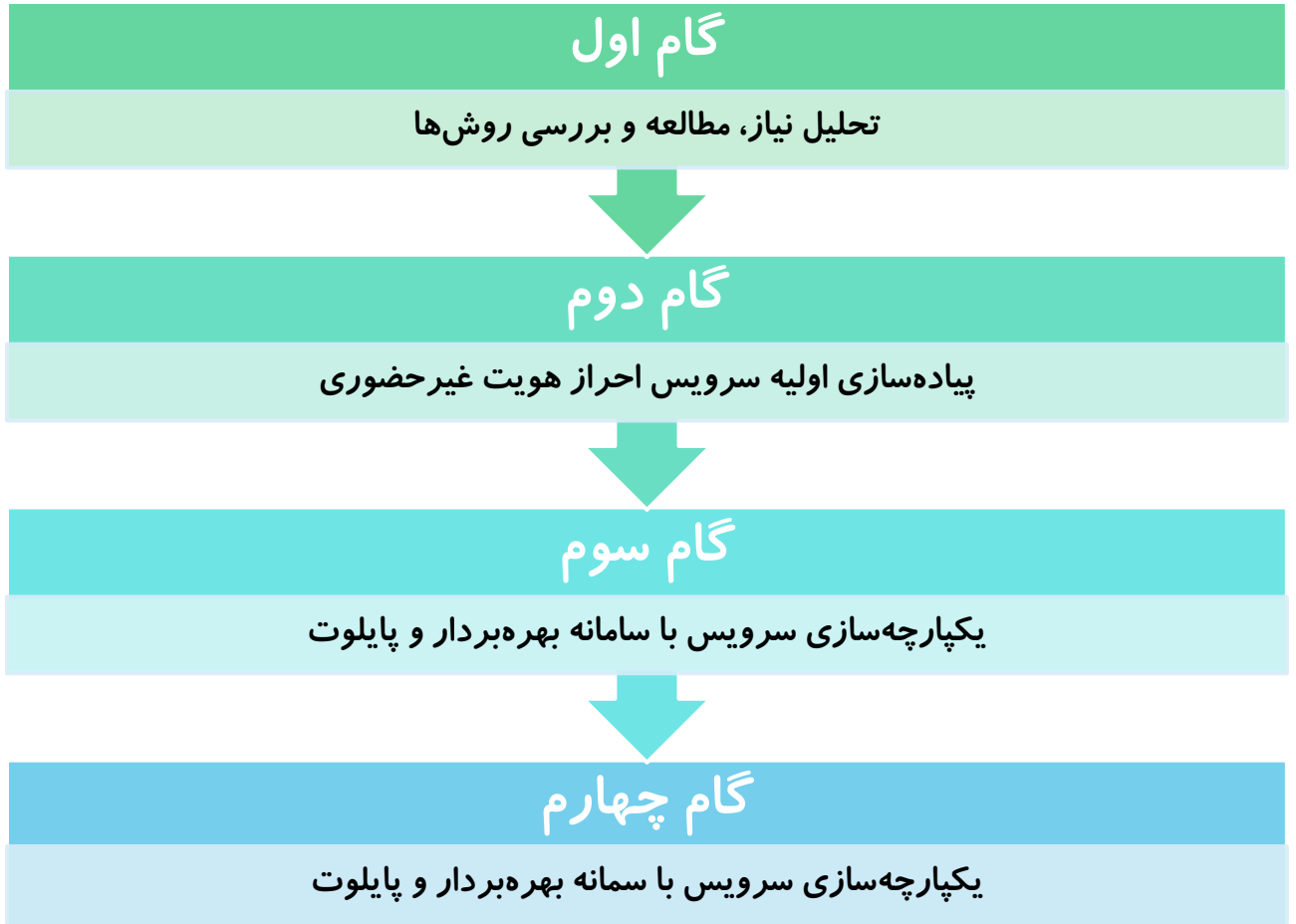
- **پیگیری/گزارش**
  - داده‌های دیجیتالی جمع‌آوری شده در فرایند احراز هویت قابل انتقال به سیستم‌های تحلیل، ممیزی، پیگیری و گزارش‌دهی هستند و فرصت‌هایی را برای بهینه‌سازی و تحلیل استراتژیک ایجاد می‌کنند.

منافع طرح برای مردم

- افزایش سرعت دریافت خدمات
- کاهش مراجعات حضوری به دفاتر و دستیابی به مزایای ناشی از آن (ترافیک، زمان، سلامتی و ...)
- فراهم کردن دسترسی شبانه‌روزی و حتی در روزهای تعطیل به خدمات انتظامی
- امکان دریافت خدمات به صورت ساده و آسان
- صرفه جویی در زمان افراد با حذف مراجعه حضوری و منتظر ماندن در دفاتر
- صرفه جویی در هزینه با توجه به کاهش تردد
- کمک به سلامتی و جلوگیری از شیوع در مواردی مانند بحران کرونا
- ایجاد اختیارات سلف‌سرویس و تسهیل فرایندها
- بهبود تجربه مشتری در دریافت خدمات

تصویری از ازدحام مردم در دفاتر

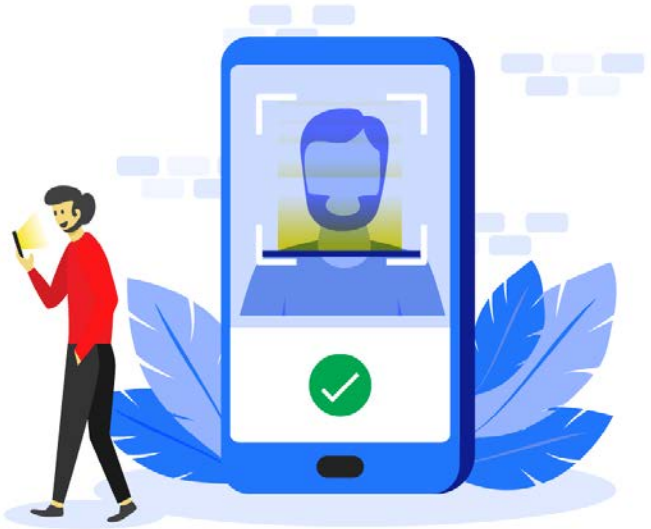
مراحل اجرا


گام اول
تحلیل نیاز، مطالعه و بررسی روش‌ها
گام دوم
پیاده‌سازی اولیه سرویس احراز هویت غیرحضوری
گام سوم
یکپارچه‌سازی سرویس با سامانه بهره‌بردار و پایلوت
گام چهارم
یکپارچه‌سازی سرویس با سمانه بهره‌بردار و پایلوت

خروجی گام های پروژه

گام اول: تحلیل نیاز، مطالعه و بررسی روش‌ها	گام دوم: پیاده‌سازی اولیه سرویس احراز هویت غیرحضوری	گام سوم: یکپارچه‌سازی سرویس با سمانه بهره‌بردار و پایلوت	گام چهارم: یکپارچه‌سازی سرویس با سمانه بهره‌بردار و پایلوت
مطالعه و بررسی روش‌ها تحلیل نیازهای پروژه طراحی پروژه	مجموعه داده‌ها و روال‌های تست ماژول‌های تشخیص چهره و تشخیص زنده بودن ماژول‌های مدیریت کاربران، مدیریت دسترسی و استعلام نسخه اولیه سرویس اختصاصی شده روی سرور کارفرما	سرویس یکپارچه شده با سامانه بهره‌بردار نصب شده روی سرور کارفرما گزارش ارزیابی سرویس و سامانه گزارش تحلیل بازخورها و تعیین اصطلاحات لازم برای پیاده‌سازی	سرویس یکپارچه شده با سامانه بهره‌بردار حاوی اصلاحات بعد از ارزیابی سند راهنمای غنی و بهره‌برداری سامانه، جلسات آموزشی سند راهنمای فعال‌سازی خدمات بر روی سامانه‌های مختلف اسناد فنی نصب، پیکربندی، اجرا، کاربری، راهبری و پشتیبانی سند تحلیل مخاطرات

احراز هویت غیرحضوری



- دیجیتالی و از راه دور شدن فرآیند KYC سنتی
  - شناسایی و تأیید هویت مشتری در زمان واقعی

- ویژگی راه‌حل‌های eKYC
  - سطح بالایی از ایمنی و قابلیت اطمینان و مطابق با قوانین تعیین شده
  - مبتنی بر هوش مصنوعی و یادگیری ماشین
  - استفاده از ویژگی‌های زیست‌سنجی چهره به عنوان معیار شناسایی
  - زمان واقعی
  - به حداقل رساندن هزینه‌ها و بوروکراسی سنتی مورد نیاز در فرآیندهای KYC

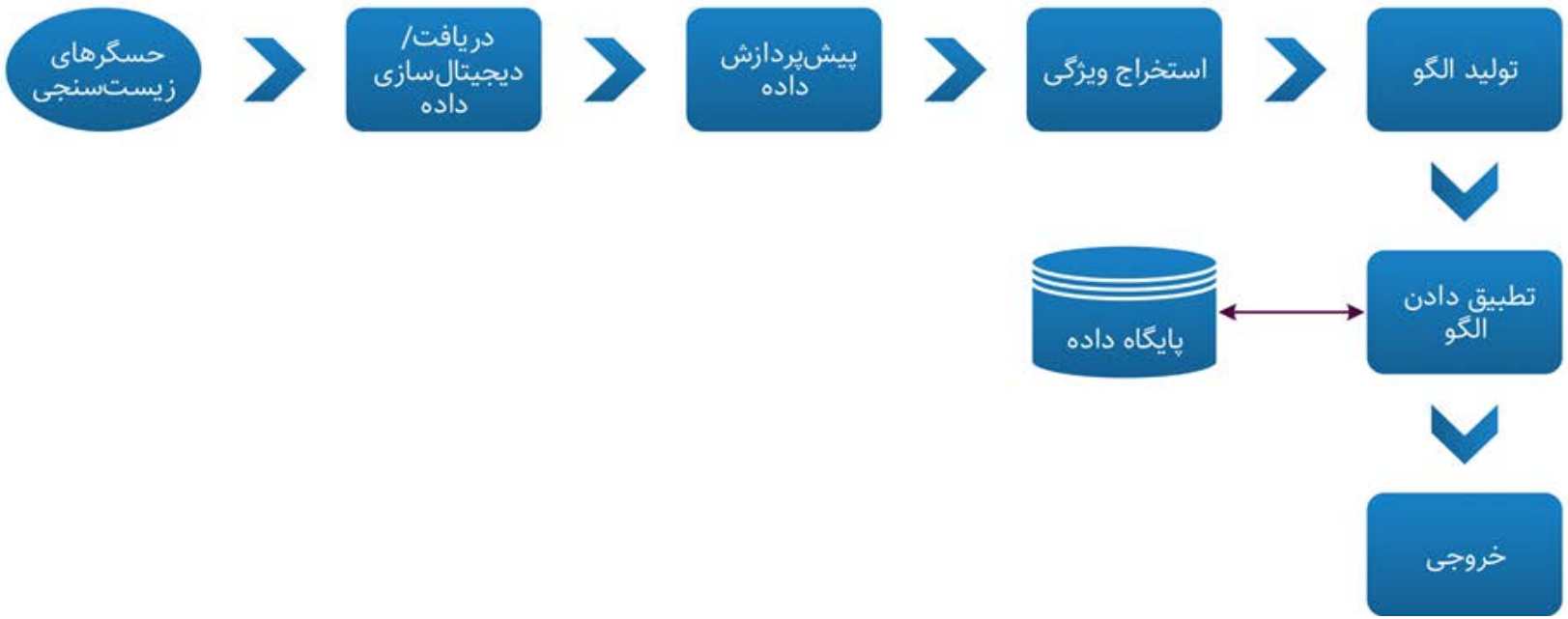
فرایند احراز هویت غیرحضوری

عملیات اصلی در یک سامانه زیست‌سنجی (ثبت‌نام)

- ثبت‌نام
  - اطلاعات فرد در سامانه
- مقایسه و شناسایی
  - تایید هویت
  - تعیین هویت

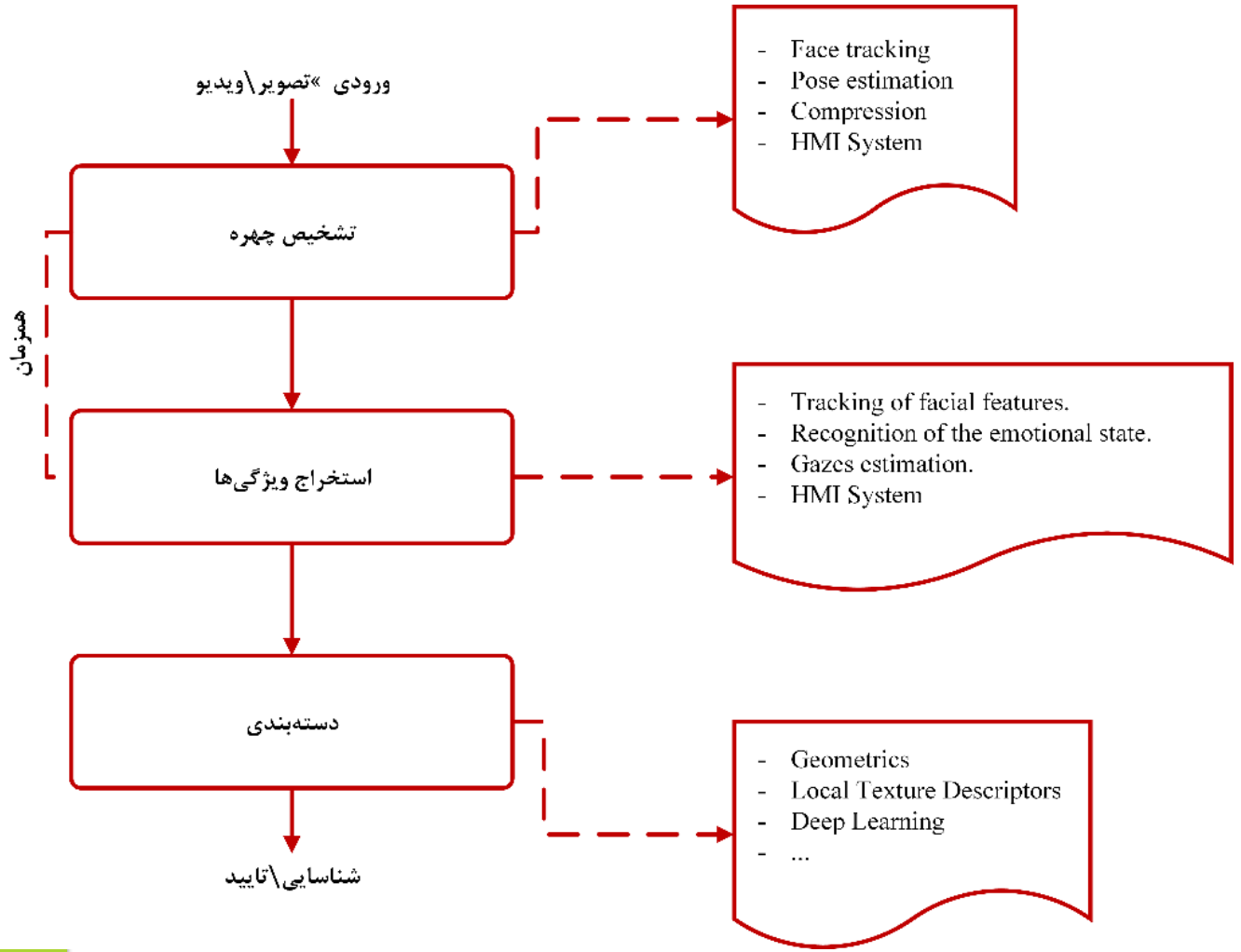
عملیات ثبت‌نام

عملیات اصلی در یک سامانه زیست‌سنجی (تطبیق)



بررسی سامانه‌های بازشناسی چهره

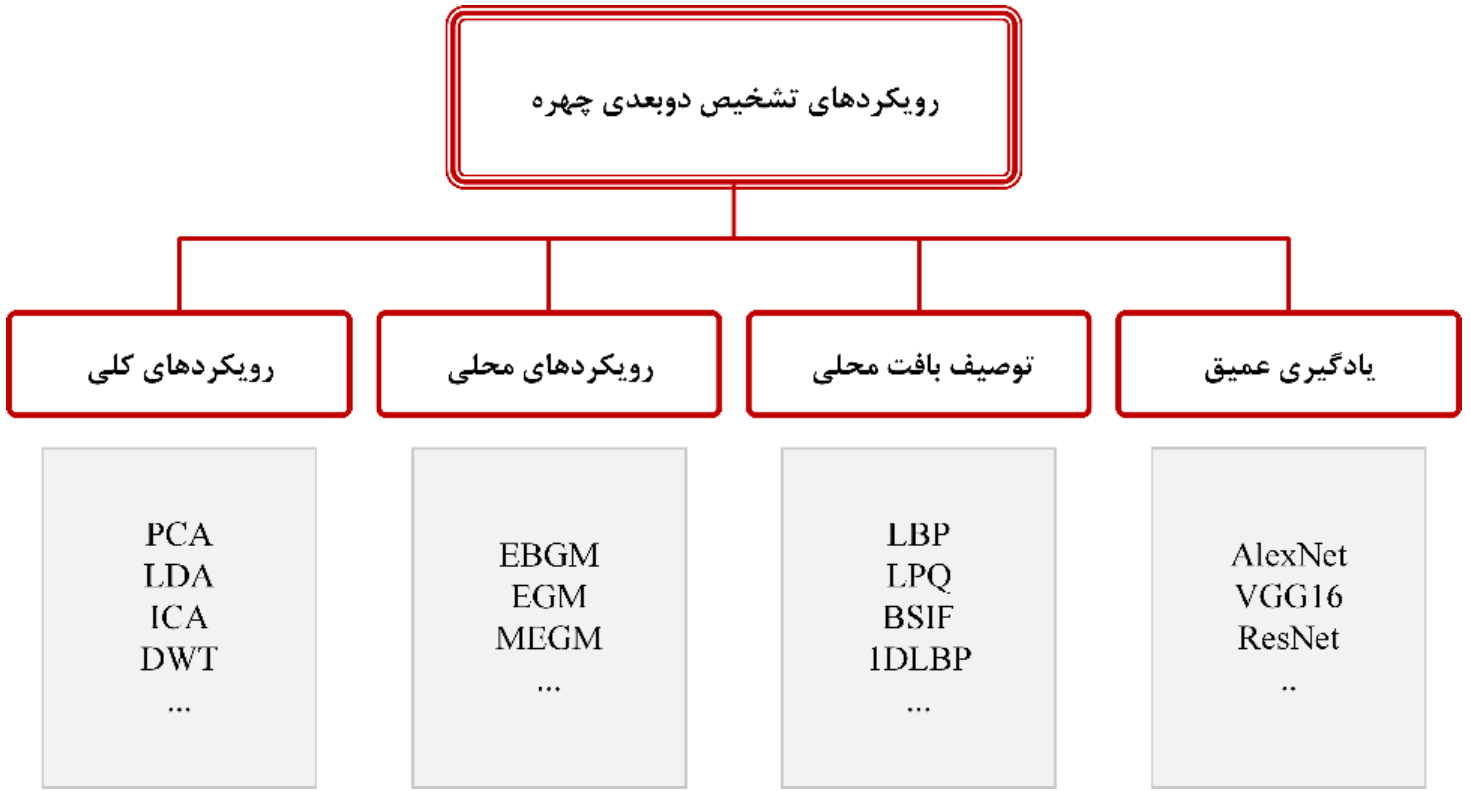
- مراحل اصلی در یک سامانه بازشناسی چهره



پایگاه داده چهره

مجموعه داده	سال پیدایش	تعداد تصاویر	تعداد افراد	تعداد تصاویر / هر فرد
ORL	۱۹۹۴	۴۰۰	۴۰	۱۰
FERET	۱۹۹۶	۱۴۱۲۶	۱۱۹۹	–
AR	۱۹۹۸	۳۰۱۶	۱۱۶	۲۶
XM2VTS	۱۹۹۹	–	۲۹۵	–
BANCA	۲۰۰۳	–	۲۰۸	–
FRGC	۲۰۰۶	۵۰۰۰۰	–	۷
LFW	۲۰۰۷	۱۳۲۳۳	۵۷۴۹	≈ ۲,۳
CMU Multi PIE	۲۰۰۹	>۷۵۰۰۰۰	۳۳۷	–
CASIA WebFace	۲۰۱۴	۴۹۴۴۱۴	۱۰۵۷۵	≈ ۴۶,۸
IJB-A	۲۰۱۵	۵۷۱۲	۵۰۰	≈ ۱۱,۴
MegaFace	۲۰۱۶	۱۰۲۷۰۶۰	۶۹۰۵۷۲	≈ ۱,۴
CFP	۲۰۱۶	۷۰۰۰	۵۰۰	>۱۴
MS-Celeb-1M	۲۰۱۶	۱۰ میلیون	۱۰۰۰۰۰	۱۰۰
DMFD	۲۰۱۷	۲۴۶۰	۴۱۰	۶
VGGFACE	۲۰۱۶	۲,۶ میلیون	۲۶۲۲	۱۰۰۰
VGGFACE	۲۰۱۷	۳,۳۱ میلیون	۹۱۳۱	≈ ۳۶۲,۶
IJB-B	۲۰۱۷	۲۱۷۹۸	۱۸۴۵	≈ ۳۶,۲
MF2	۲۰۱۸	۴,۷ میلیون	۶۷۲۰۵۷	≈ ۷
DFW	۲۰۲۰	۱۱۱۵۷	۱۰۰۰	≈ ۵,۲۶
IJB-C	۲۰۲۰	۳۱۳۳۴	۳۵۳۱	≈ ۶
LFR	۲۰۲۰	۳۰۰۰۰	۵۴۲	۱۰ – ۲۶۰
RMFRD	۲۰۲۰	۹۵۰۰۰	۵۲۵	–
SMFRD	۲۰۲۰	۵۰۰۰۰۰	۱۰۰۰۰	–

رویکردهای بازشناسی چهره

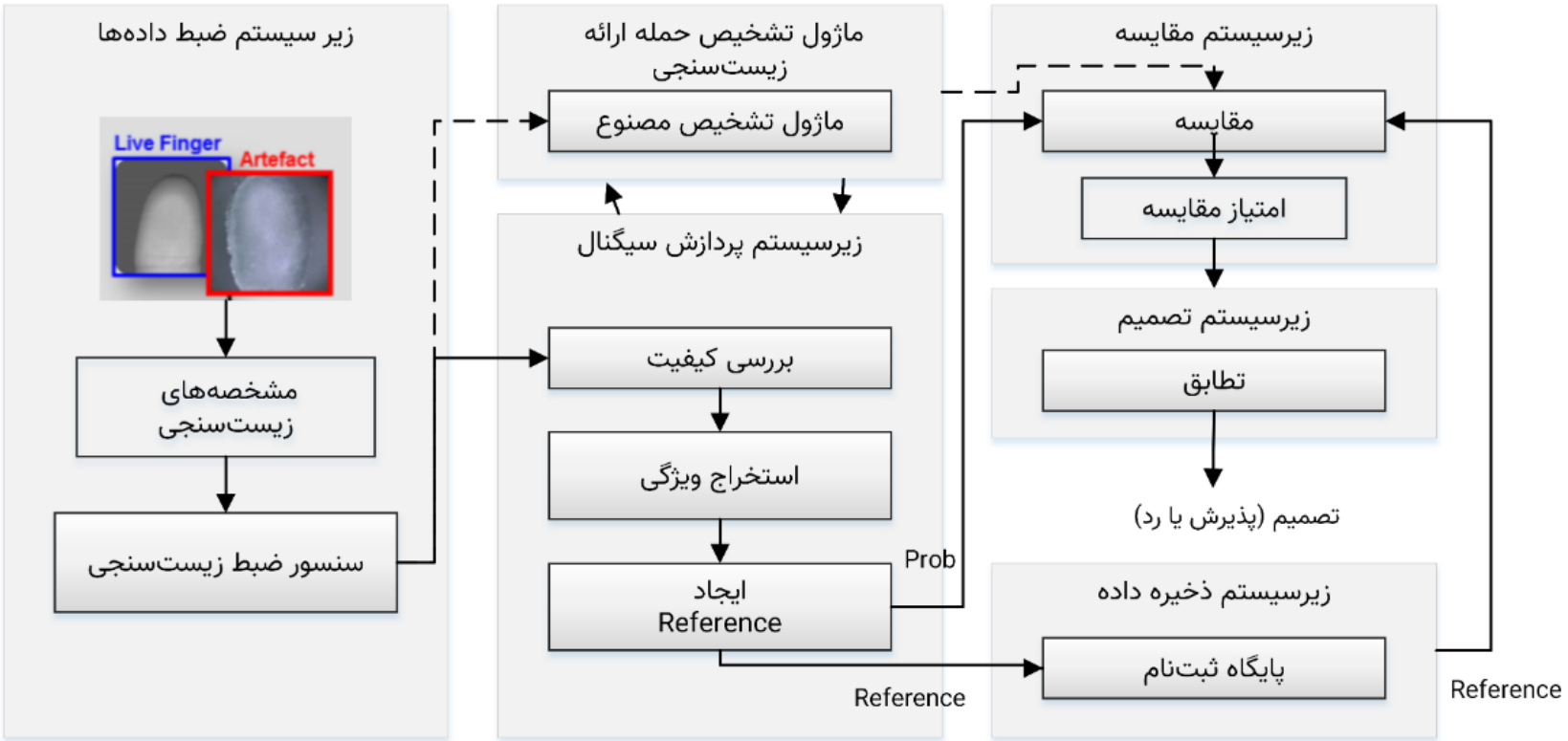


تشخیص زنده بودن

- زنده‌بودن(Liveness)
  - کیفیت یا حالت زنده بودن (خصوصیات آناتومیکی، واکنش‌های غیرارادی و واکنش‌های ارادی)
- تشخیص زنده بودن(Liveness Detection)
  - تشخیص خصوصیات آناتومیکی یا واکنش‌های غیرارادی یا داوطلبانه
- جعل(spoof)
  - ایجاد تداخل در یک سامانه زیست‌سنجی با ارائه یک مصنوع

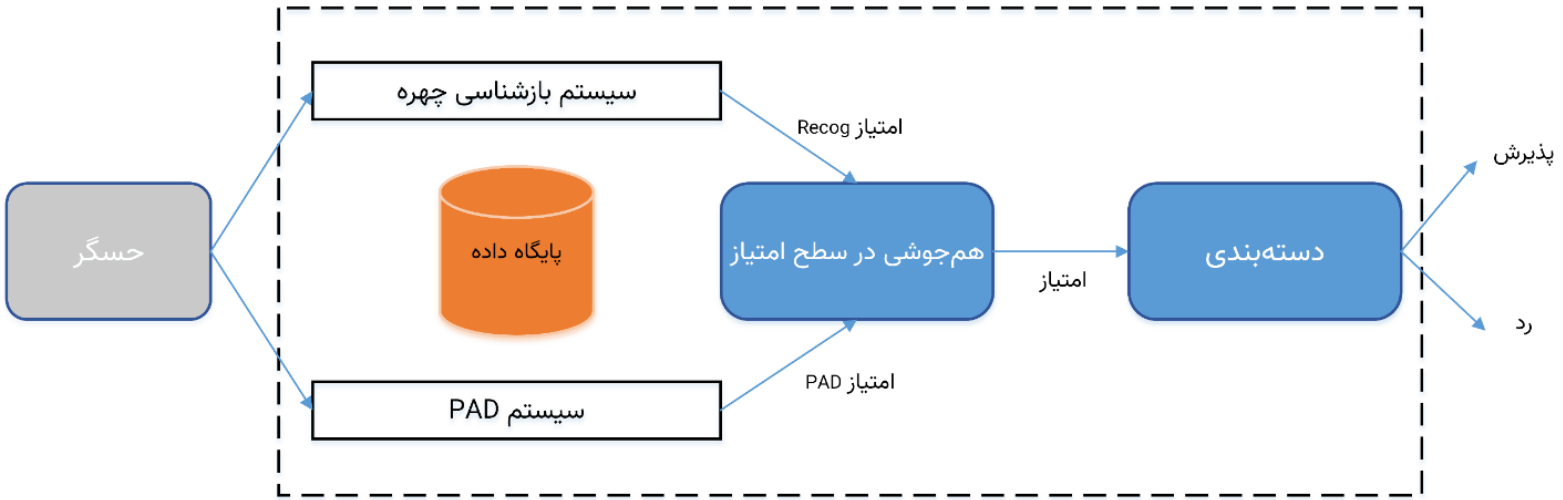
- حمله نمایش(Presentation Attack)
  - نمایش (ارائه‌ی) یک مصنوع یا مشخصه‌ی انسانی به زیرسامانه ضبط زیست‌سنجی با هدف ایجاد تداخل در کار سامانه
- ابزار حمله نمایش (Presentation Attack Instrument)
  - به مشخصه‌های زیست‌سنجی یا شی مورد استفاده در حمله نمایش
- تشخیص حمله نمایش(Presentation Attack Detection)
  - تشخیص خودکار حمله‌ی نمایش به یک سامانه ضبط مشخصه‌های زیست‌سنجی

ساختار کلی سامانه تشخیص زنده بودن



تشخیص زنده بودن در سامانه بازشناسی چهره . . .

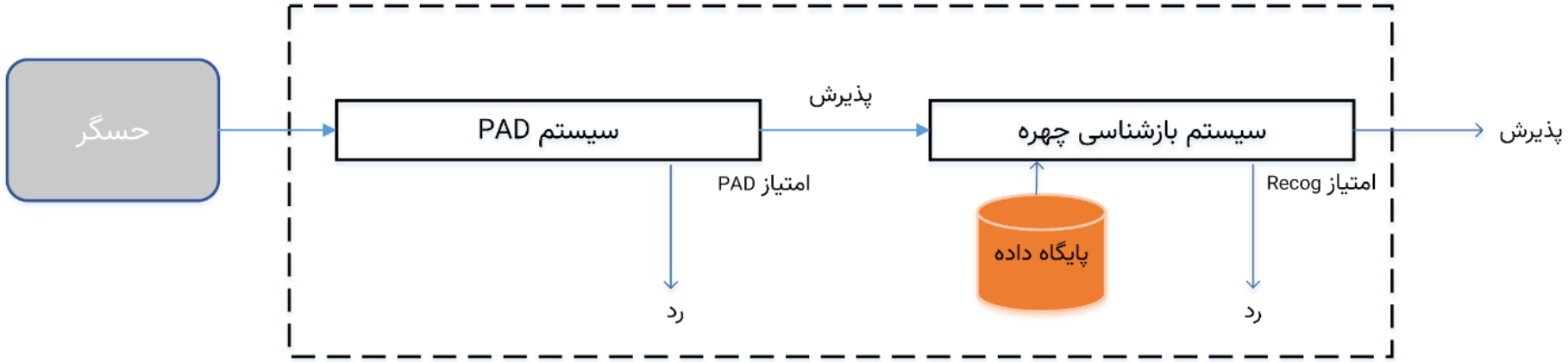
- متداول‌ترین سنجه زیست‌سنجی در برنامه‌های شخصی و تجاری عمومی
- دارای قابلیت دسترسی بیشتر نسبت به سایر سنجه‌ها و راحتی در تقلید و تقلب
- ادغام راهکارهای تشخیص زنده بودن با بازشناسی چهره به منظور افزایش ایمنی
  - ادغام به صورت موازی
  - ادغام به صورت سری



ادغام به صورت موازی و ترکیب در مرحله امتیاز

تشخیص زنده بودن در سامانه بازشناسی چهره

- سرعت بیشتر روش موازی نسبت به سری
- جلوگیری روش سری از کار اضافی سامانه شناسایی چهره در صورت پذیرفته نشدن زنده بودن در مراحل اولیه

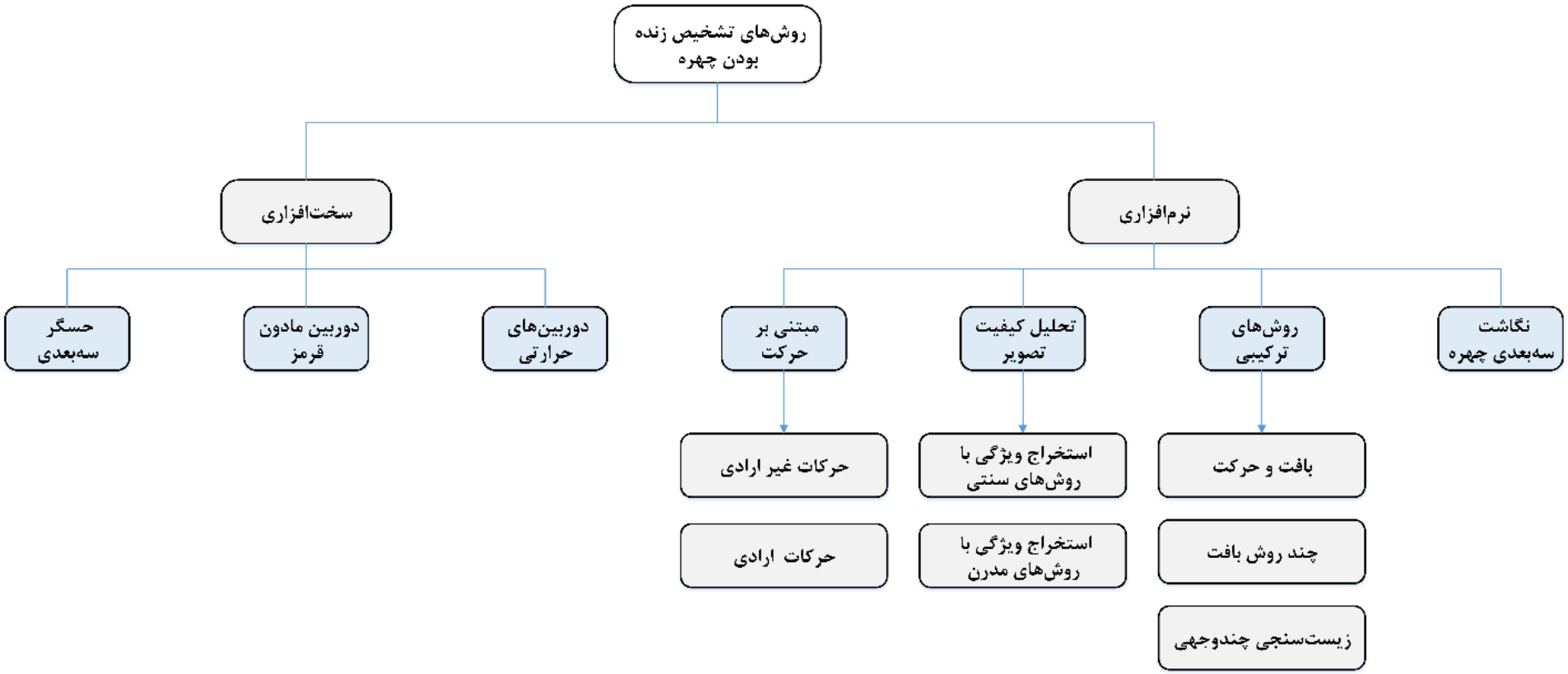


ادغام به صورت سری

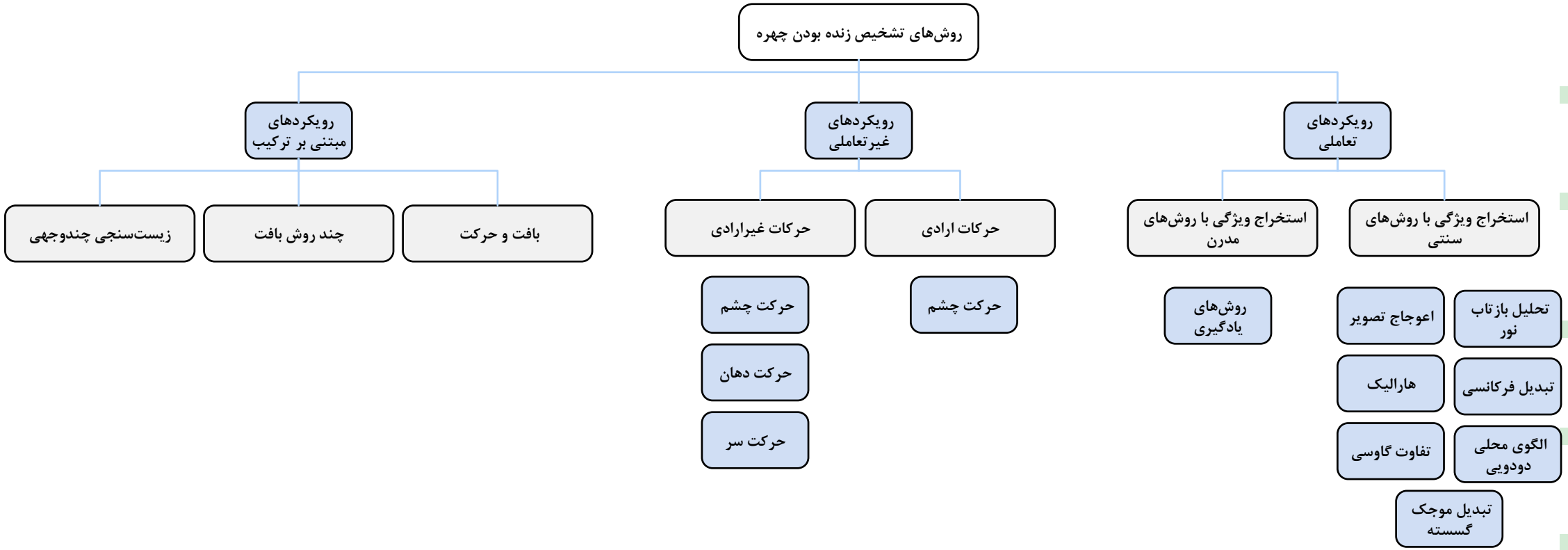
پایگاه داده تشخیص زنده بودن برای چهره

پایگاه داده	نوع داده	نوع جعل	تعداد نمونه‌ها (واقعی/ جعلی)	افراد
Celeba Spoof	تصویر	تصویر چاپ شده و ویدیو بازپخش شده، ماسک سه بعدی	۶۲۵/۵۳۷	۱۰۱۷۷
NUAA PI DB	تصویر	تصویر چاپ شده	۵۱۰۵/۷۵۰۹	۱۵
PRINT-ATTACK DB	ویدیو	تصویر چاپ شده و ماسک	۲۰۰/۲۰۰	۵۰
REPLAY-ATTACK DB	ویدیو	ویدیو بازپخش شده	۲۰۰/۱۰۰۰	۵۰
CASIA FAS DB	ویدیو	تصویر چاپ شده و ویدیو بازپخش شده	۱۵۰/۴۵۰	۵۰
MASK-ATTACK DB	ویدیو	تصویر چاپ شده و ویدیو بازپخش شده، ماسک سه بعدی	۱۷۰/۸۵	۱۷
YALE-RECAPT DB	تصویر	تصویر چاپ شده	۶۴۰/۱۹۲۰	۱۰

طبقه‌بندی روش‌های تشخیص زنده بودن . . .



طبقه‌بندی روش‌های تشخیص زنده بودن



مقایسه رویکرهای تعاملی و غیرتعاملی

- تشخیص زنده بودن تعاملی
  - الزام کاربر به انجام یک کار ساده مانند پلک زدن، چرخاندن سر یا حرکت تلفن خود به جلو و عقب
  - کلاهبرداری با نمایش عکسی با برش‌های محدوده‌ای، استفاده از ماسک یا ویدیو
  - ایجاد اصطکاک با کاربر و زمان‌بر بودن

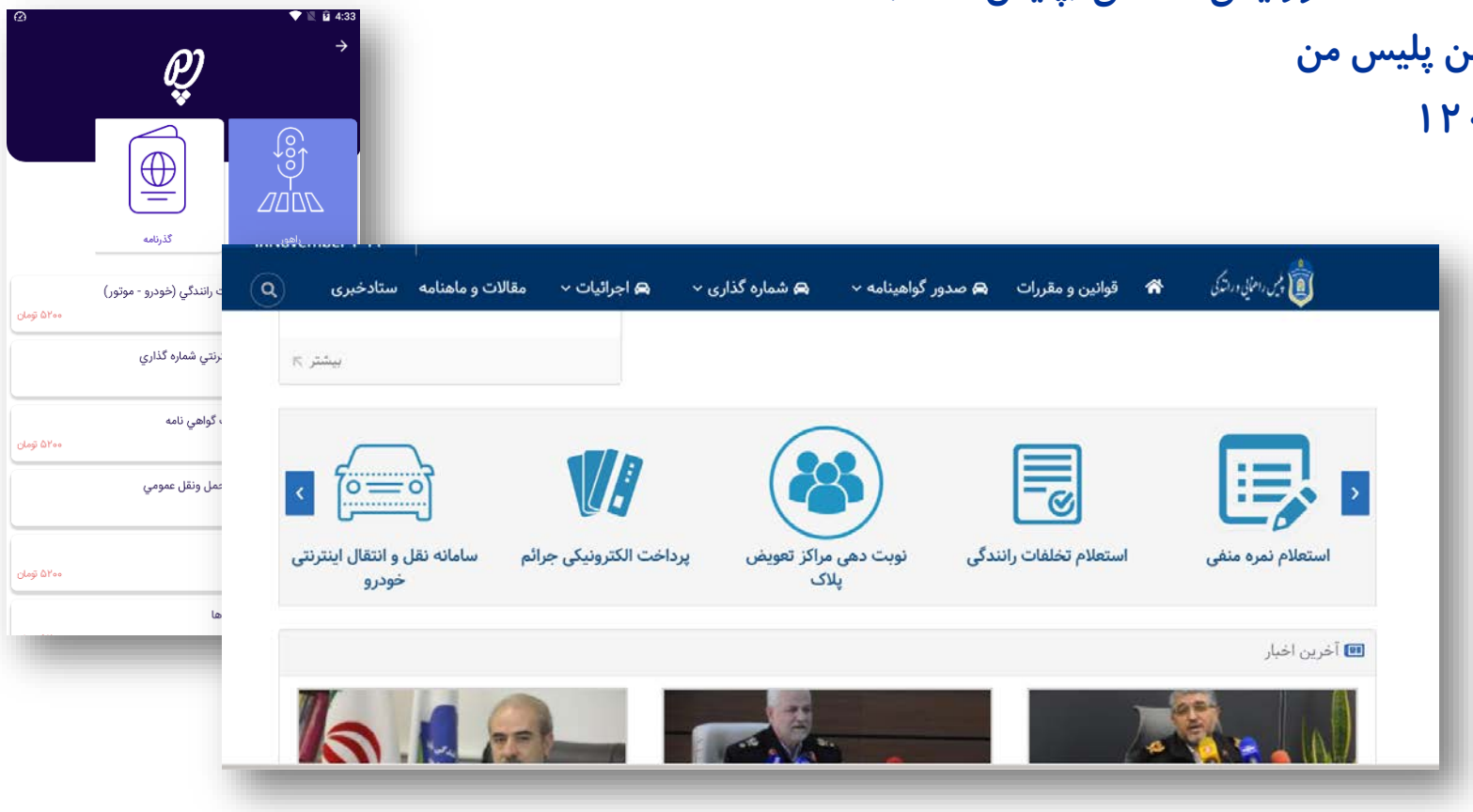
- تشخیص زنده بودن غیرتعاملی
  - مبتنی بر هوش مصنوعی
  - هیچ نشانه‌ای به کاربران در حال آزمایش نمی‌دهد و کاربران نیازی به انجام هیچ گونه حرکت اضافی ندارند
  - کشف چگونگی دور زدن این فناوری برای متقلبان سخت‌تر است

تحلیل و مقایسه رویکردهای تشخیص زنده بودن

- توانایی تعمیم محدود در استخراج ویژگی‌ها به صورت دستی
- بیش‌برازش و در نتیجه تعمیم‌پذیری ضعیف در روش‌های یادگیری عمیق
- روش‌های مبتنی بر بافت پویا، قادر به تشخیص تقریباً همه انواع حملات هستند.
- عملکرد چشمگیر روش‌های مبتنی بر یادگیری عمیق در مقایسه با روش‌های مبتنی بر ویژگی‌های دستی
- پیچیدگی محاسباتی روش‌های مبتنی بر هندسه سه‌بعدی
- روند مناسب = ترکیب چندین روش
- محدودیت روش‌های تشخیص زنده بودن از نظر تعمیم
  - پیچیدگی مسئله تشخیص زنده بودن چهره
  - تنوع زیاد در حملات احتمالی
  - عدم وجود مجموعه داده که شامل نمونه‌های کافی با تنوع کافی باشد

خدمات الکترونیک و هوشمند نیروی انتظامی

- دفاتر خدمات الکترونیکی انتظامی (پلیس + ۱۰)
- اپلیکیشن پلیس من
- راهور ۱۲۰



دفاتر خدمات الکترونیک انتظامی (پلیس+۱۰)

❑ خدمات دفاتر پلیس+۱۰

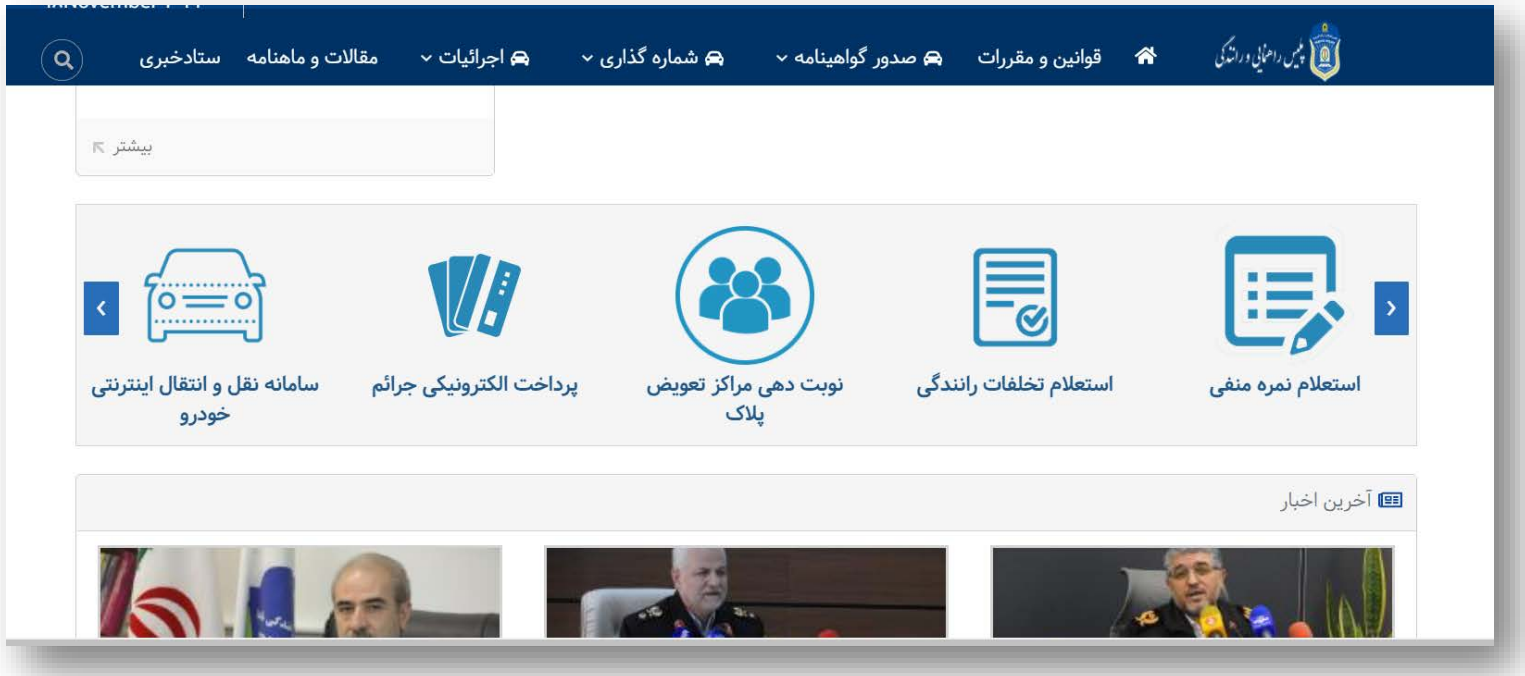
- ◄ خدمات گواهینامه شامل تمدید و تعویض انواع گواهینامه رانندگی و صدور المثنی
- ◄ خدمات صدور گذرنامه شامل اخذ مدارک متقاضی گذرنامه و ثبت اطلاعات در سیستم
- ◄ خدمات اجرائیات شامل صدور صورت وضعیت خلافی خودرو
- ◄ خدمات صدور و تمدید پروانه کسب (اماکن)
- ◄ استعلام تشخیص هویت (سوء پیشینه کیفری)
- ◄ ثبت درخواست‌های مشمولین (نظام وظیفه)
- ◄ رسیدگی غیرحضوری به شکایات صورت وضعیت
- ◄ صدور و المثنی کارت هوشمند سوخت
- ◄ تغییر آدرس مالکان خودرو

اپلیکیشن پلیس من

- اپلیکیشن پلیس من قسمت راهور

- استعلام تخلفات رانندگی خودرو و موتورسیکلت
- نوبت دهی اینترنتی شماره گذاری (تعویض پلاک)
- آخرین وضعیت گواهینامه
- گزارش تخلف حمل و نقل عمومی
- نمره منفی
- وضعیت پلاک ها
- استعلام کارت و سند خودرو
- شماره گذاری اینترنتی

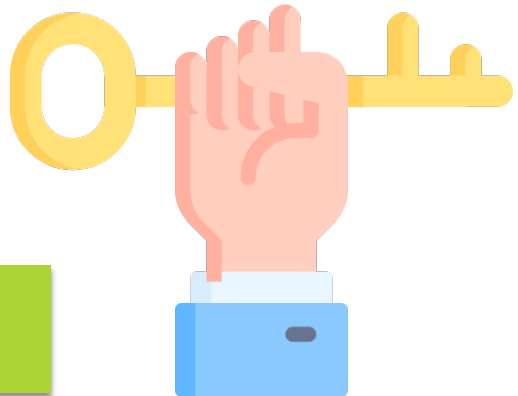
راهور ۱۲۰


پلیس راهنمایی و رانندگی
قوانین و مقررات
صدور گواهینامه
شماره گذاری
اجرائیات
مقالات و ماهنامه
ستادخبری
بیشتر
استعلام نمره منفی
استعلام تخلفات رانندگی
نوبت دهی مراکز تعویض پلاک
پرداخت الکترونیکی جرائم
سامانه نقل و انتقال اینترنتی خودرو
آخرین اخبار

راهکار پیشنهادی پروژه

- **راه‌حل شماره یک: استفاده از رابط‌های برنامه نویسی SDK و API**
  - سرویس‌های پایه سامانه‌های احراز هویت (تطبیق چهره و تشخیص زنده بودن) به صورت SDK و API در اختیار سایر سامانه‌ها قرار می‌گیرد

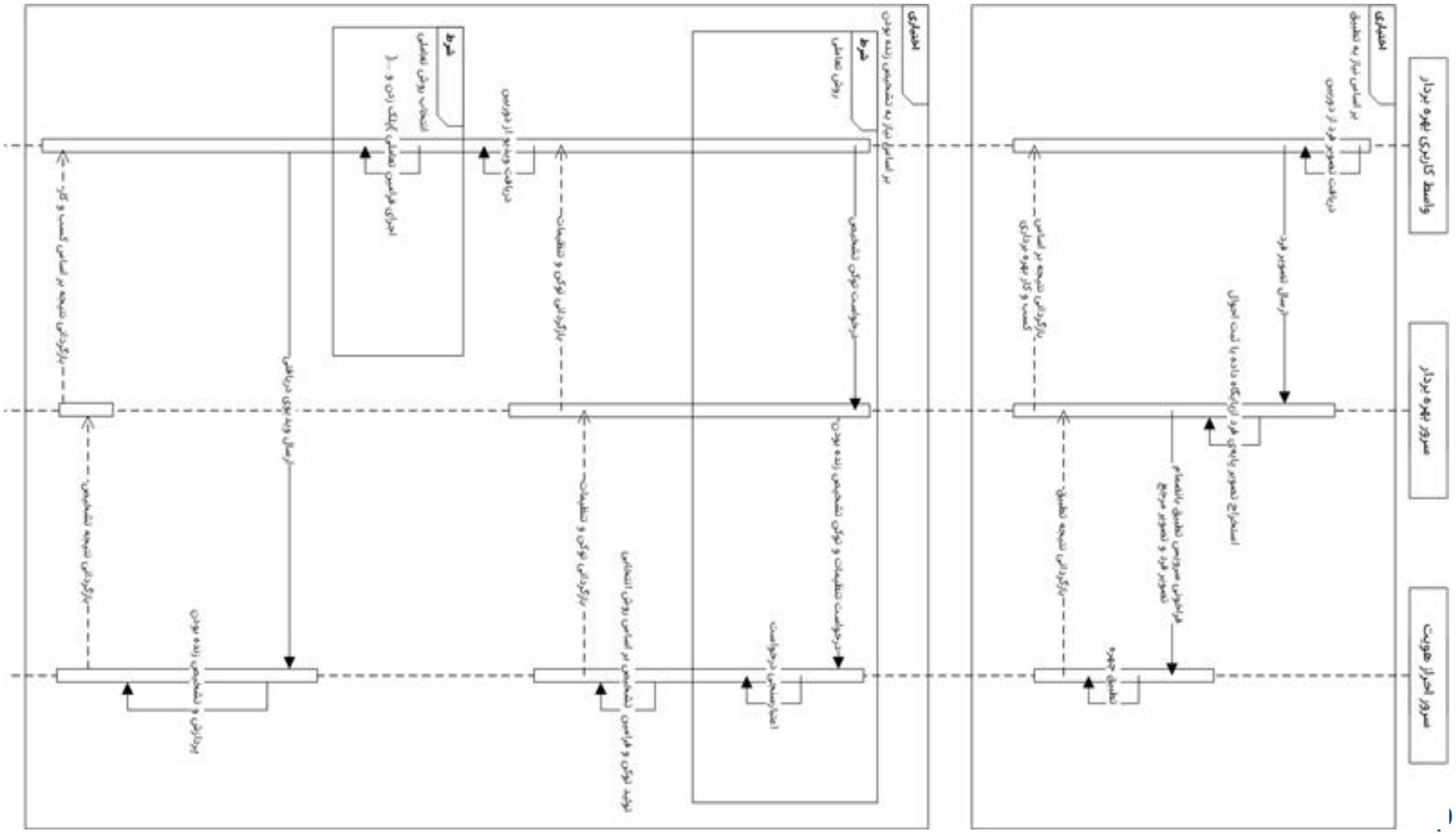
- **راه‌حل شماره دو: استفاده از درگاه احراز هویت**
  - رابط احراز هویت دیگری به نام درگاه دارد (درگاه‌های بانکی)
  - کاربران به سمت یک صفحه ثالث هدایت می‌شوند و روند احراز هویت در آن صفحه (سایت) صورت می‌گیرد
  - نتیجه موفق و یا ناموفق بودن آن برای سرویس گیرنده بازگردانده می‌شود



استفاده از رابط‌های برنامه نویسی SDK و API

- قرار دادن احراز هویت با تطبیق چهره و تشخیص زنده بودن داخل خود SSO ناجا

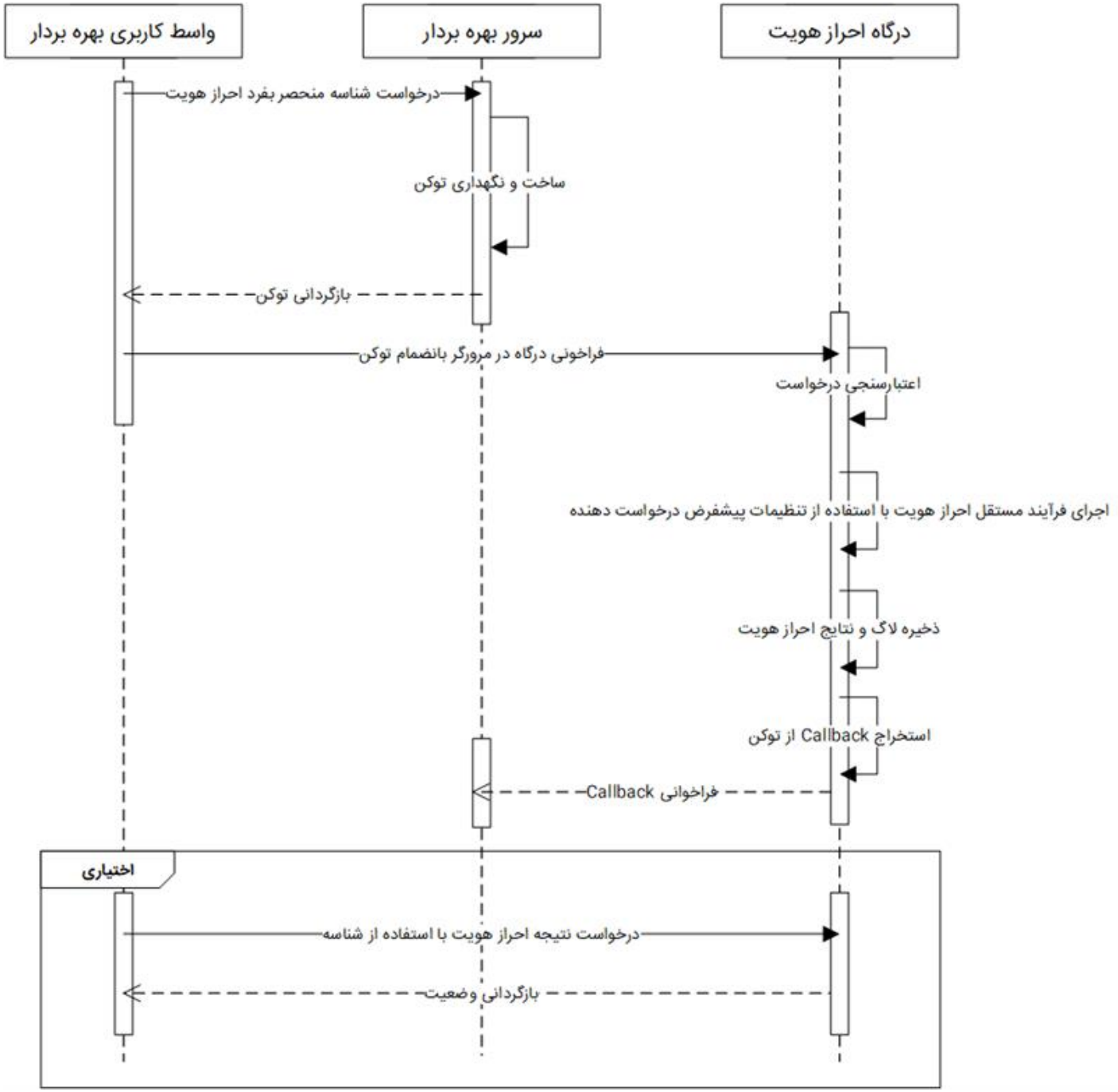
نمودار ترتیب برای راه حل پیشنهادی اول



استفاده از درگاه احراز هویت

- راهکار مستقل از سامانه SSO بوده و تمام پیاده‌سازی‌های آن سمت تیم مجری

نمودار ترتیب برای راه حل پیشنهادی دوم



مزایا و معایب هر کدام از دو روش پیشنهادی

راه‌حل	مزایا	معایب
اتصال از طریق API	یکپارچگی بیشتر در نرم افزارهای ناجا ایجاد کرده و باعث ایجاد انعطاف‌پذیری بیشتر در این نرم‌افزارها شده و می‌توان با توجه به نیاز، تغییرات خاصی را اعمال کرد	نیاز به پیاده‌سازی بیشتر در نرم‌افزارها و سرویس‌های دریافت کننده خدمات برای مدیریت روال‌های احراز هویت (مانند نگهداری اطلاعات وارد شده توسط کاربران، وضعیت احراز هویت آن‌ها، مراحل مورد نیاز برای احراز هویت و ...)
اتصال از طریق درگاه	نرم‌افزارهای استفاده کننده از سرویس احراز هویت غیرحضوری نسبت به روال‌های احراز هویت مستقل و بی‌خبر بوده و استفاده از آن مستقل از پیچیدگی‌های روال احراز هویت است (پیاده‌سازی آسان).	یکپارچگی کمتر با سامانه‌های استفاده‌کننده از سرویس‌های احراز هویت و انعطاف پایین‌تر

خروجی گام های پروژه

گام اول:
تحلیل نیاز، مطالعه و بررسی روش‌ها

مطالعه و بررسی روش‌ها

تحلیل نیازهای پروژه

طراحی پروژه

گام دوم:
پیاده‌سازی اولیه سرویس احراز هویت غیرحضوری

مجموعه داده‌ها و روال‌های تست ماژول‌های تشخیص چهره و تشخیص زنده بودن

ماژول‌های مدیریت کاربران، مدیریت دسترسی و استعلام

نسخه اولیه سرویس اختصاصی شده روی سرور کارفرما

گام سوم:
یکپارچه‌سازی سرویس با سمانه بهره‌بردار و پایلوت

سرویس یکپارچه شده با سامانه بهره‌بردار نصب شده روی سرور کارفرما

گزارش ارزیابی سرویس و سامانه

گزارش تحلیل بازخورها و تعیین اصطلاحات لازم برای پیاده‌سازی

گام چهارم:
یکپارچه‌سازی سرویس با سمانه بهره‌بردار و پایلوت

سرویس یکپارچه شده با سامانه بهره‌بردار حاوی اصلاحات بعد از ارزیابی

سند راهنمای غنی و بهره‌برداری سامانه، جلسات آموزشی

سند راهنمای فعال‌سازی خدمات بر روی سامانه‌های مختلف

اسناد فنی نصب، پیکربندی، اجرا، کاربری، راهبری و پشتیبانی

سند تحلیل مخاطرات