احراز هویت الکترونیک بر مبنای سنجه‌های بیومتریکی

گردآورنده: هدیه پورقاسم
استاد راهنما: دکتر رضا صفابخش

چشم‌انداز ارائه

مقدمه

- اهمیت احراز هویت بیومتریک
- مزایای احراز هویت بیومتریک
- ویژگی‌های بیومتریکی

سیستم‌های احراز هویت بیومتریکی

- ساختار سیستم‌های احراز هویت بر مبنای ویژگی‌های بیومتریکی
- خطرهای بالقوه در این سیستم‌ها
- انواع حملات به این سیستم‌ها
- مبنای ارزیابی عملکرد

روش‌های بهود برای ویژگی‌های ایستا

- بهبود تشخیص چهره و زنده بودن
- بهبود تشخیص اثر انگشت

روش‌های بهود برای ویژگی‌های پویا

- بهبود تشخیص صدا
- بهبود تشخیص ضربه به صفحه کلید و پویایی لمسی

جمع‌بندی

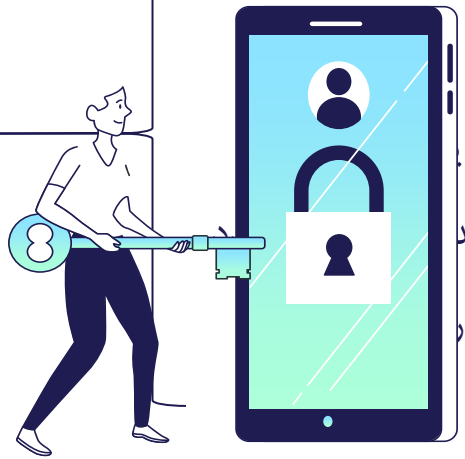
- نتیجه‌گیری
- پیشنهادات

اهمیت احراز هویت بیومتریک

احراز هویت فرآیند شناسایی کاربرانی است که درخواست دسترسی به یک سیستم، شبکه یا دستگاه را دارند.

- رشد سریع اینترنت و دستگاه‌های تلفن همراه
- استفاده‌ی روزافزون مردم از سرویس‌های اینترنتی
- افزایش حساب‌های کاربری افراد
- افزایش حملات و کلاه‌برداری‌های ا
- آسان بودن حمله به رمزهایی با تعد
- اهمیت امنیت و حریم خصوصی کار

پیشنهاد روش‌هایی برای احراز هویت بر مبنای سنجه‌های بیومتریکی



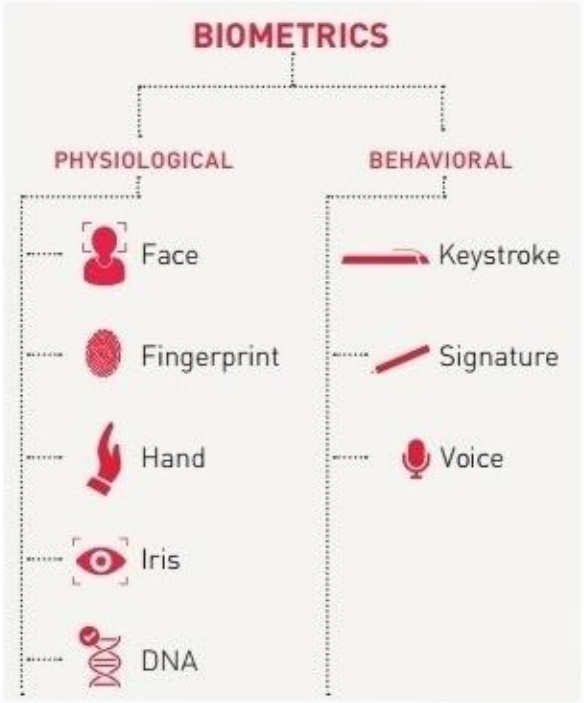
مزایای احراز هویت بیومتریک

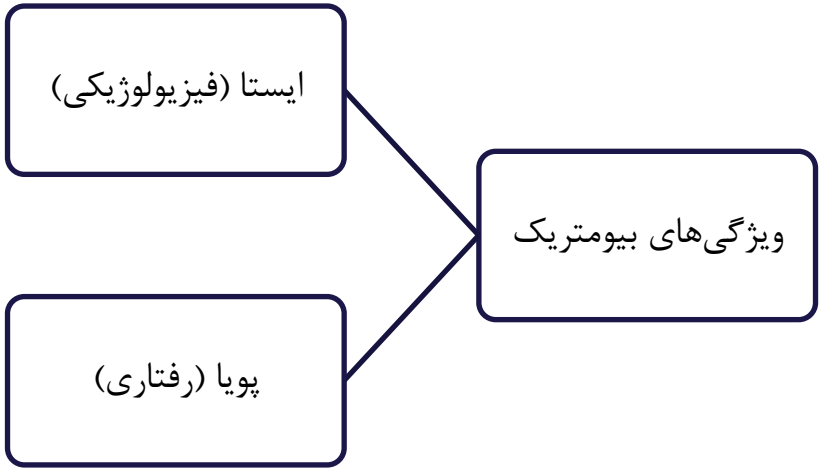
- غیرممکن بودن گم شدن یا فراموش شدن رمزهای بیومتریکی
- دشواری کپی کردن و یا اشتراک گذاری این رمزها
- دشواری جعل و توزیع رمزهای بیومتریکی
- دشواری حدس زدن این رمزها
- شکستن رمز بیومتریکی یک فرد راحت تر از فرد دیگری نیست
- دقت بالا
- منحصر به فرد بودن این ویژگی‌ها
- دسترسی از راه دور

کاربردها:

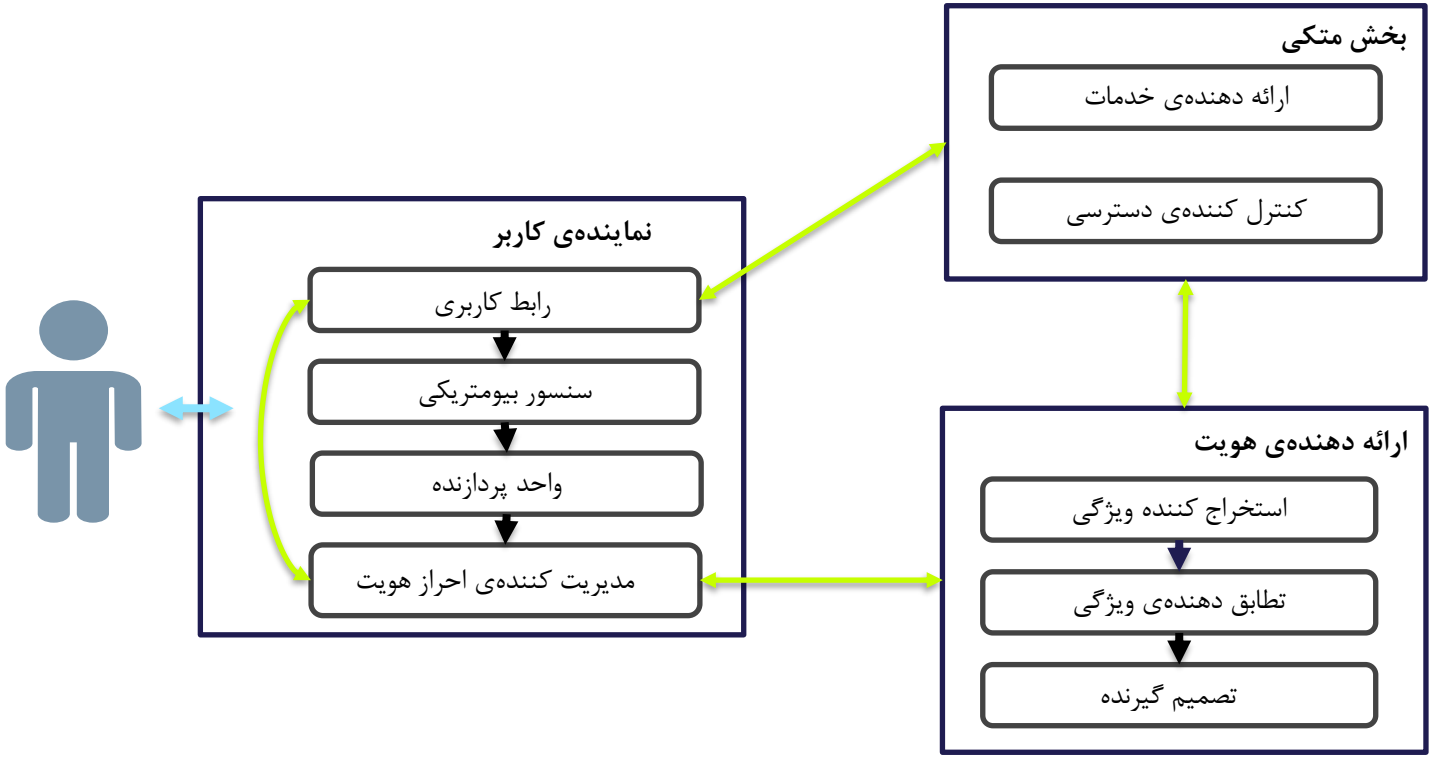
- اجرای قانون و امنیت عمومی
- صنایع نظامی
- کنترل مرز ، مسافرت و مهاجرت
- شناسنامه مدنی
- بهداشت و درمان
- دسترسی فیزیکی و منطقی
- استفاده‌های تجاری

ویژگی‌های بیومتریکی

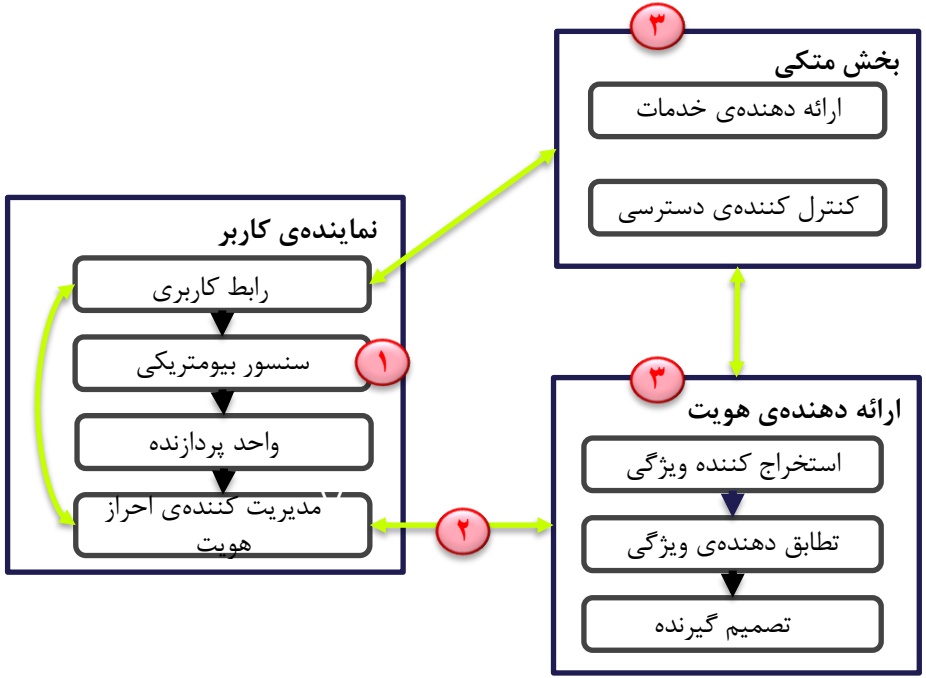




ساختار سیستم‌های احراز هویت بر مبنای ویژگی‌های بیومتریکی



خطرهای بالقوه‌ی این سیستم‌ها

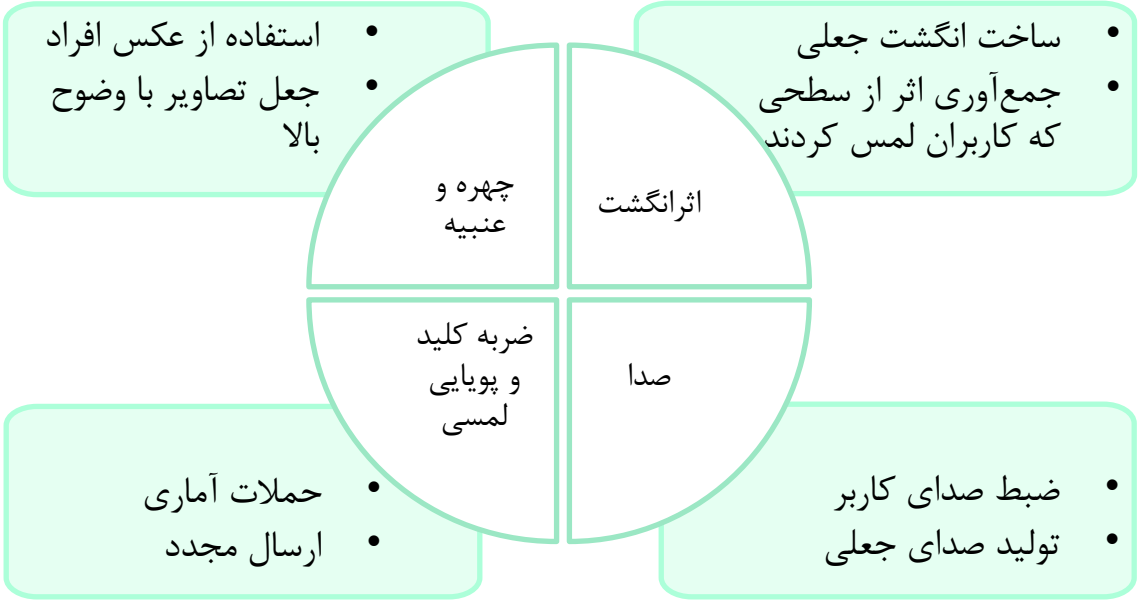


۱. جعل سنسور

۲. ارسال مجدد سیگنال‌های بیومتریکی

۳. حملات متداول شبکه به سرورها

انواع حملات به این سیستم‌ها



استراتژی‌های دفاعی معمول:

- سیستم بیومتریک چند حالته
- استفاده از تکنیکهای رمزنگاری
- استفاده از الگوریتم‌های بهتر
- ذخیره اطلاعات حساس در مکان امن، مانند شخص ثالث

مبنای ارزیابی عملکرد این سیستم‌ها

دقت	کارایی	قابلیت استفاده	امنیت و حریم خصوصی
نرخ پذیرش نادرست	زمان جمع‌آوری داده‌ها	جهانی بودن	توانایی مقاومت در برابر حملات مختلف
نرخ عدم پذیرش نادرست	زمان پردازش داده‌ها	منحصر به فرد بودن	غیرقابل بازگشت بودن
نرخ خطای برابر	زمان استخراج ویژگی‌ها	ماندگاری	قابل تجدید پذیری
دقت احراز هویت	زمان تصمیم گیری	مقبولیت	
		نیاز به تجهیزات اضافی	

روش‌های بهبود تشخیص چهره و زنده بودن

- مدل توزیع نقطه‌ای
  - ✓ دقت و امنیت پایین
  - ✓ قابلیت استفاده متوسط

جهان شمول بودن

ماندگاری و منحصر به فرد بودن نامطلوب

- اندازه‌گیری میزان نفوذ سطح
  - ✓ دقت، کارایی و قابلیت استفاده در حد معمول
  - ✓ امنیت بالا

- مدل مورد استفاده‌ی شرکت اپل
  - ✓ کارایی و امنیت بالا

روش‌های بهبود تشخیص اثر انگشت

جهان شمول بودن، منحصر به فرد بودن، مقبولیت بالا، قابلیت استفاده بالا

- استفاده از ویژگی‌های بیومتریکی رگ انگشت
  - ✓ امنیت بالا
  - ✓ دقت، کارایی و قابلیت استفاده متوسط
- استفاده از طیف مادون قرمز با طول موج کوتاه
  - ✓ دقت بالا

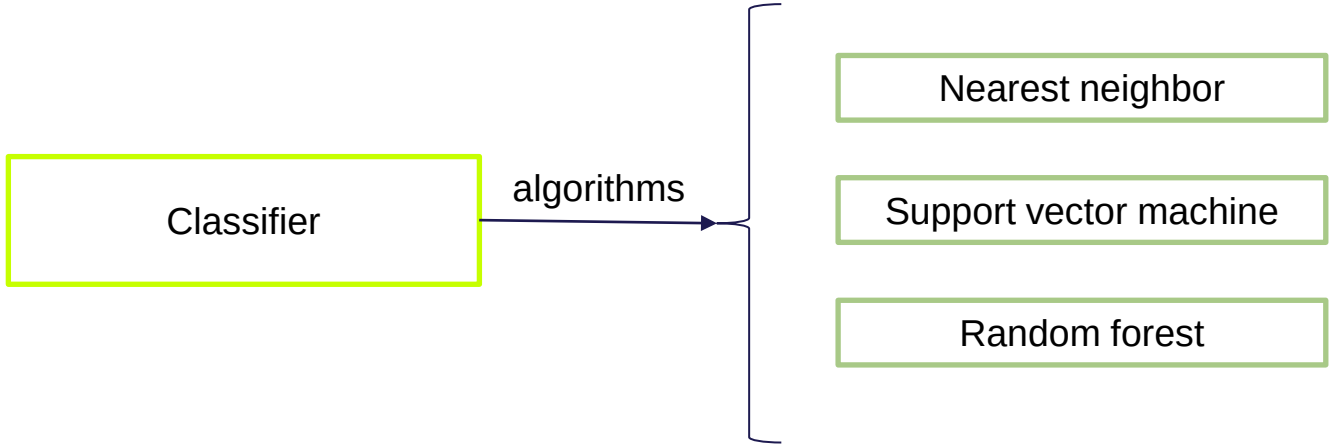
روش‌های بهبود تشخیص صدا

جهان شمول بودن، منحصر به فرد بودن، مقبولیت بالا، قابلیت استفاده بالا

- استفاده از مدل مخفی مارکوف(HMM)
  - ✓ دارای امنیت بالا
- مدل مخفی مارکوف – مدل مخلوط گاوسی(HMM-GMM)
  - ✓ دقت بالا

روش‌های بهبود تشخیص ضربه به صفحه کلید و پویایی لمسی

این نوع روش‌ها به سرعت با روش‌های تشخیص اثر انگشت جایگزین شدند



جمع‌بندی

ویژگی بیومتریک	روش	دقت	کارایی	قابلیت استفاده	امنیت	حریم خصوصی
چهره	مدل توزیع نقطه‌ای	کم	-	متوسط	کم	-
	اندازه‌گیری میزان نفوذ سطح	متوسط	متوسط	متوسط	زیاد	-
	iProov	زیاد	زیاد	متوسط	زیاد	کم
اثر انگشت	استفاده از ویژگی‌های بیومتریک رگ انگشت	متوسط	متوسط	زیاد	زیاد	-
	استفاده از طیف مادون قرمز	متوسط	-	متوسط	زیاد	-
صدا	HMM	کم	-	زیاد	زیاد	-
	HMM-GMM	متوسط	-	زیاد	زیاد	-
تسخیص ضربه و پویایی لمسی	استفاده از الگوریتم‌های یادگیری ماشین	متوسط	کم	متوسط	متوسط	-

پیشنهادات

- بهبود تشخیص زنده بودن در تشخیص چهره و اثر انگشت
- بهبود حریم خصوصی کاربران
- بهبود رابط کاربری و روش‌های جمع‌آوری داده‌ها

منابع

[1] Rui, Z. and Yan, Z., *2018*. A survey on biometric authentication: Toward secure and privacy-preserving identification. *IEEE Access*, *7*, pp.*5994-6009*.

[2] González-Jiménez, D. and Alba-Castro, J.L., *2007*. Toward pose-invariant *2*-d face recognition through point distribution models and facial symmetry. *IEEE Transactions on Information Forensics and Security*, *2*(*3*), pp.*413-429*.

[3] Queirolo, C.C., Silva, L., Bellon, O.R. and Segundo, M.P., *2009*. *3*D face recognition using simulated annealing and the surface interpenetration measure. *IEEE transactions on pattern analysis and machine intelligence*, *32*(*2*), pp.*206-219*.

[4] Jadhav, M. and Nerkar, P.M., *2015*, December. Implementation of an embedded hardware of FVRS on FPGA. In *2015 International Conference on Information Processing (ICIP)* (pp. *48-53*). IEEE.

[5] Ferrer, M.A., Morales, A. and Díaz, A., *2014*. An approach to SWIR hyperspectral hand biometrics. *Information Sciences*, *268*, pp.*3-19*.

[6] Jayamaha, R.M.M., Senadheera, M.R., Gamage, T.N.C., Weerasekara, K.P.B., Dissanayaka, G.A. and Kodagoda, G.N., *2008*, December. Voizlock-human voice authentication system using hidden markov model. In *2008 4th International Conference on Information and Automation for Sustainability* (pp. *330-335*). IEEE.

[7] Gałka, J., Masior, M. and Salasa, M., *2014*. Voice authentication embedded solution for secured access control. *IEEE Transactions on Consumer Electronics*, *60*(*4*), pp.*653-661*.

خواهشمندم سوالات خود را مطرح فرمایید.

باتشکر از توجه شما