بررسی ویژگی‌های پایدار سیگنال‌های عصبی جهت استفاده در سیستم تولید کلید بیولوژیکی

دانشجو: پوریا نورزاده

استاد راهنما: دکتر بیژن علیزاده

دانشکده مهندسی برق و کامپیوتر، دانشگاه تهران

مقدمه

با استفاده از سیگنال‌های عصبی اخذ شده از انسان می‌توان یک سیستم شناسایی و احرازهویت ارائه داد که برخلاف دیگر بیومتریک‌ها، محدودیت در تعداد و تنوع را نداشته باشند، برای مثال ما فقط ده اثرانگشت در دستانمان داریم و ممکن است آن‌ها را از دست بدهیم و جایگزینی برایشان نداشته باشیم. این سیستم می‌تواند یک سری از مشکلات سیستم‌های رمزنگاری فعلی را نداشته باشد.

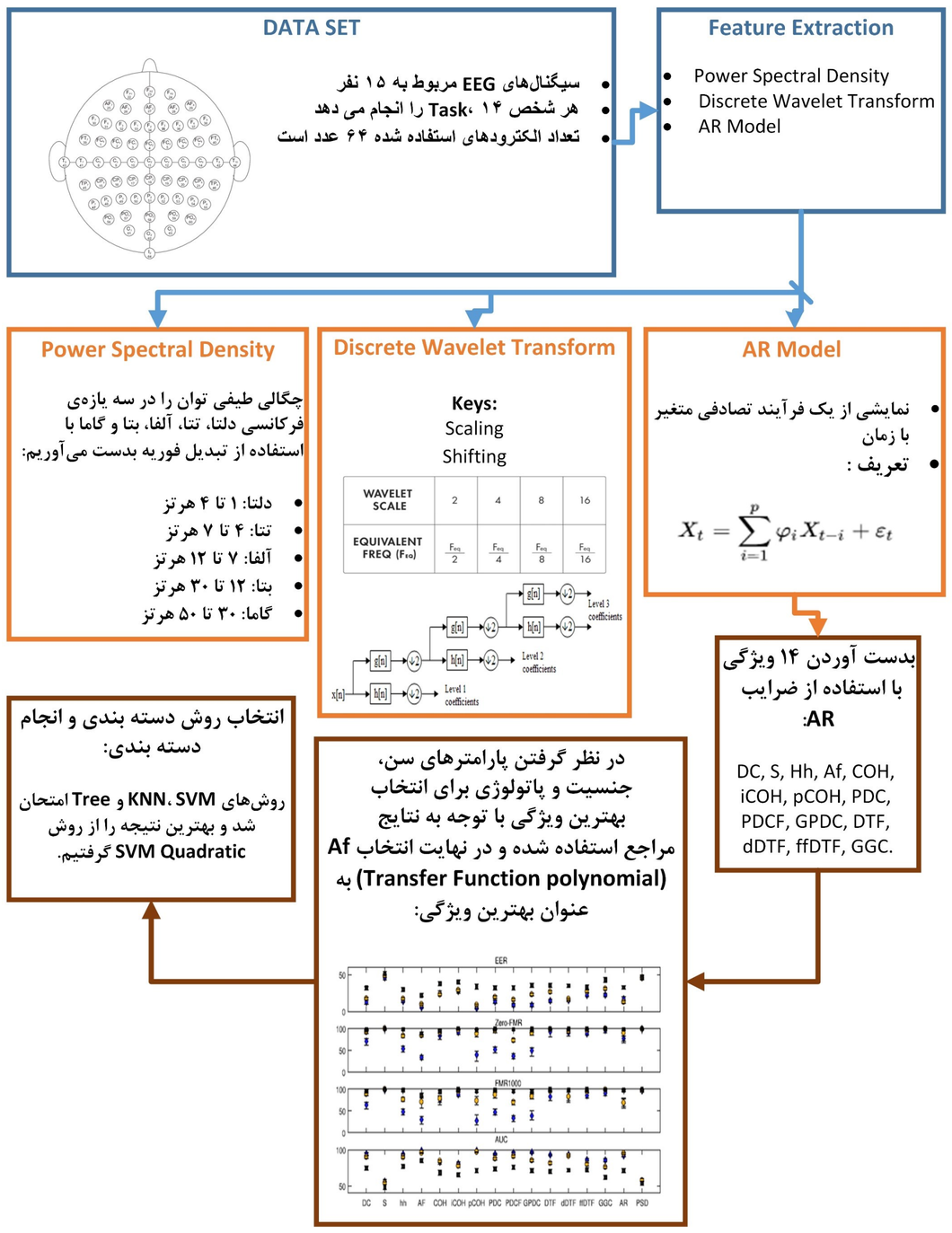
مشکلات سیستم‌های رمزنگاری:

- ذخیره سازی کلید
- تولید اعداد تصادفی
- الگوریتم‌های پیچیده
- وابستگی امنیت کل سیستم به ضعیف‌ترین لینک
- احتمال کارآمد نبودن الگوریتم‌های فعلی در صورت پیشرفت کامپیوترها و ساخت کامپیوترهای کوانتومی

هدف این بود که روش‌های شناسایی و احرازهویت افراد با استفاده از سیگنال‌های EEG را بررسی کرده، بهترین روش را انتخاب کنیم و با شبیه سازی در نرم افزار متلب نتایج کار خود را ارائه دهیم.

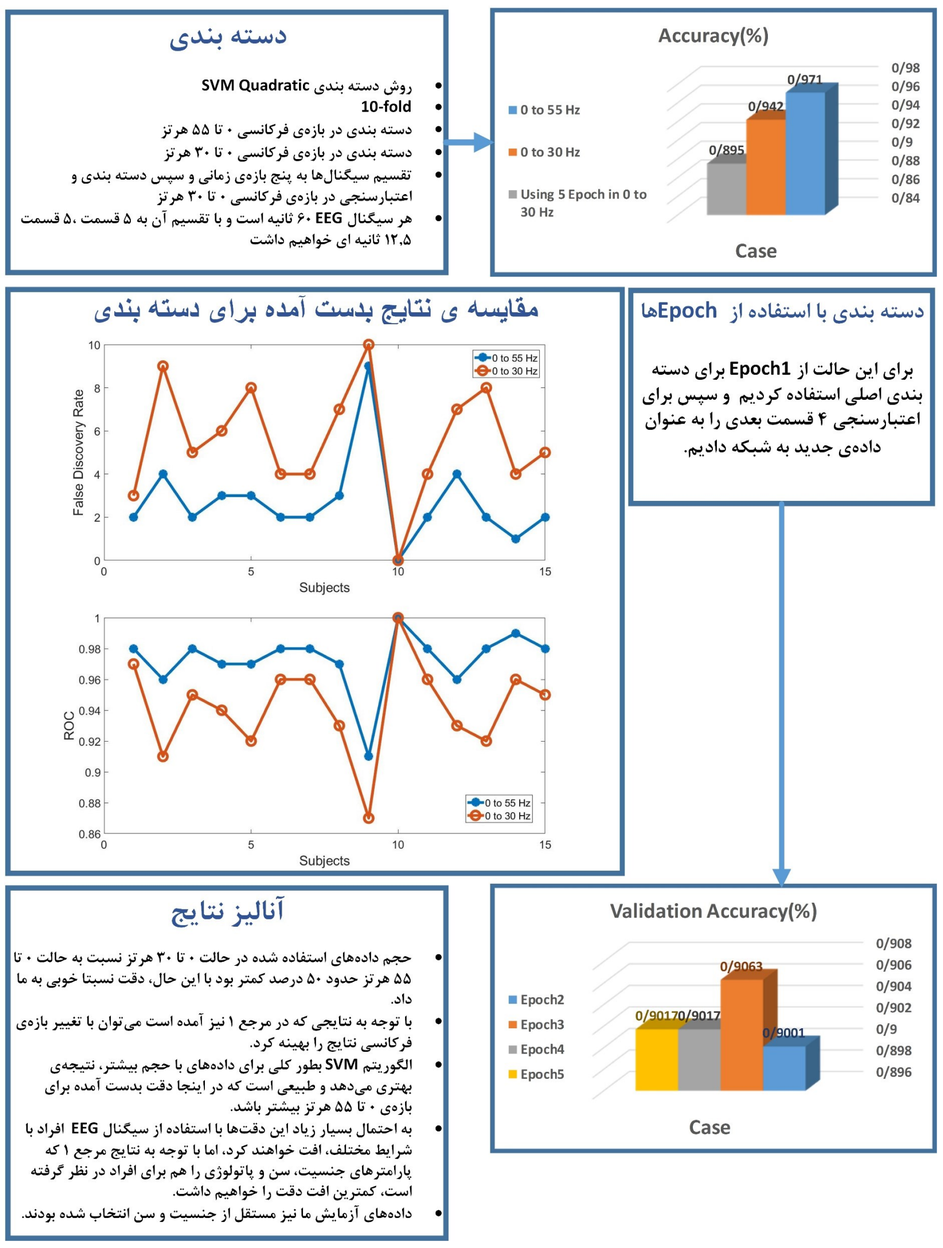
روش پیشنهادی

ابتدا صرف نظر از اینکه کدام روش بهتر است، ما راه هر دو مرجع ۱ و ۲ را طی کردیم، سپس با استفاده از نتایج مرجع ۱ که ادامه‌ی کار مرجع ۲ است، روش خود را انتخاب کردیم. در مراجع ما از PSD، DWT و AR Model استفاده شده بود که در نهایت ما AR Model را انتخاب کردیم و با استفاده از ضرایب AR و ویژگی‌هایی که از آن بدست می‌آید شبیه سازی و دسته‌بندی خود را در نرم افزار متلب انجام دادیم. باید قابلیت تکرار پذیری، با اعمال پارامترهای سن، جنسیت و پاتولوژی نیز در نظر گرفته می‌شد، برای این منظور از نتایج مرجع ۱ استفاده کردیم، که تاثیر این پارامترها را بررسی کرده است.



نتایج

دسته بندی را با استفاده از الگوریتم SVM Quadratic، برای ویژگی Af بدست آمده، در چند حالت با تغییر بازه‌ی فرکانسی سیگنال EEG انجام دادیم، بازه‌های فرکانسی را یکبار ۰تا ۵۵ هرتز و بار دیگر ۰ تا ۳۰ هرتز در نظر گرفتیم. بطور کلی الگوریتم SVM برای داده‌های با حجم زیاد نتیجه‌ی بهتری می‌دهد. همچنین سیگنال‌های EEG را به ۵ بازه‌ی زمانی تقسیم کردیم و با مدل‌سازی با روش AR، ویژگی‌ها را برای این ۵ بازه بدست آورده و از این ویژگی‌ها برای اعتبارسنجی استفاده کردیم.



جمع بندی

از سیگنال‌های EEG می‌توان به عنوان یک بیومتریک برای احرازهویت افراد استفاده کرد و ما برای تعریف taskها محدودیتی نخواهیم داشت.

زمانی که طول می‌کشد تا ضرایب AR Model محاسبه شوند و سپس ویژگی‌ها را بدست آوریم، نسبتا زیاد می‌باشد، به همین دلیل می‌توان به عنوان یک پیشنهاد پیاده سازی سخت افزاری قسمت‌های مختلف را ارائه داد. در صورت پیاده سازی سخت افزاری روی FPGA علاوه براینکه در زمان صرفه جویی خواهیم داشت، توان بسیار کمتری نیز مصرف خواهد شد.

مراجع اصلی

1. *Y. Höller , A. C. Bathke, and A. Uhl, "Age, Sex, and Pathology Effects on Stability of Electroencephalographic Biometric Features Based on Measures of Interaction," IEEE Transactions on Information Forensics and security, vol. 14, no. 2, 2019.*

2. *G. Bajwa, R. Dantu, "Neurokey: Towards a new paradigm of cancelable biometrics-based key generation using electroencephalograms," Computer and Security, vol. 62, 2016.*

شماره پوستر: ۳۹