



مبانی رایانش امن مقدمات

محسن هوشمند
دانشکده تکنولوژی اطلاعات و علم رایانه
دانشگاه تحصیلات تکمیلی علوم پایه زنجان

ارزیابی

Digital filters [7]–[10]: sophisticated filter banks [7] were designed to recognize QRS complexes in which they analyzed the positions and magnitudes of sharp waves and used a special digital band-pass filter to reduce the false detection of ECG signals in the MIT-BIH database [11]. The difference operation method (DOM) [8] scheme including two stages was proposed: the first stage was to find the point R by applying the difference equation operation to an ECG signal, then the second stage looked for the points Q and S based on the point R to find the QRS complex. The work [9] used some special digital filters to detect and classify ECG signal in time or frequency domain. Slope- and peak-sensitive band-pass filters were employed for the detection [10]. The morphological smoothing further improved its performance.

Wavelet transform (WT) [12]–[16]: the transform yields a time-scale representation similar to the time-frequency representation of the short-time Fourier transform (STFT) [12], while the WT uses a set of analyzing functions that allows a variable time and frequency resolution for different frequency bands [13]. By the multiscale feature of WT, the QRS complex can be distinguished from high P or T waves, noise, and baseline drift. The dyadic discrete WT (DWT) was usually implemented using a dyadic filter bank where the filter coefficients were directly derived from the wavelet function [14]. The WT based on the adaptive threshold [15] and WT based on multi-lead ECG [16] were evaluated on the QT database [17].

Adaptive matched filters [18]–[22]: a two-stage successive cancellation algorithm that sequentially separates

تمرین‌ها

▪ کتبی

▪ عملی

امتحان

▪ خلق دانش

▪ کپی پیست (گرفتن گذاشتن) اعلام منابع هر تمرین

مراجع و منابع

[استالینگز] W. Stallings, "Cryptography and Network Security_ Principles and Practice," Global Edition-Pearson, 2017.

[استینسن] D. R. Stinson, M. B. Paterson, "Cryptography_ Theory and Practice," CRC Press, 2018.

[میهایلسکو] M. I. Mihailescu, S. L. Nita, "Cryptography and Cryptanalysis in MATLAB- Creating and Programming Advanced Algorithms," Apress, 2021.

[لوئینرگر] A. J. Menezes, S. A. Vanstone, P. C. Van Oorschot, "Handbook of applied cryptography," CRC Press, 2001.

منابع کمکی

[لاودن] K. C. Laudon, C. G. Traver, "E-Commerce-business. technology. society," Pearson, 14th ed, 2018-2019.

[میتنیک] K. D. Mitnick, "Ghost in the Wires- My Adventures as the World's Most Wanted Hacker," Little, Brown and Company, 2011.

[میتنیک ۱۷] K. D. Mitnick, R. Vamosi, "The Art of Invisibility- The World's Most Famous Hacker Teaches You How to Be Safe in the Age of Big Brother and Big Data," Little, Brown and Company 2017.

اینترنت و مقالات

[فرهنگستان] واژه‌های مصوب فرهنگستان، دسترسی از طریق مانه

[انوری] ح. انوری و دیگران، «فرهنگ بزرگ سخن»، انتشارات سخن، ۱۳۹۲

[رانکوهی] م.ت. روحانی رانکوهی، «فرهنگ داده»، انتشارات جلوه،

اعلانات

حل تمرین درس: کیانا قصابی

نحوه ارسال تمرین‌ها، پروژه‌ها، دیگر موارد

▪ ا-نامه amniat.iasbs@gmail.com

▪ عنوان: «امنیت-تمرین سری اول»

▪ فایل متنی: قالب پی‌دی‌اف

▪ نام فایل: [A-T#-Afshar-Mahmoud_Sotode-Morteza.pdf](#)

▪ نام فایل: [A-P#-Afshar-Mahmoud_Sotode-Morteza.pdf](#)

▪ دیگر فایل‌ها

▪ نام فایل: [A-T#-Afshar-Mahmoud_Sotode-Morteza.zip](#)

ارتباط با حل تمرین - https://t.me/amniat_iasbs

صفحه درس: <https://iasbs.ac.ir/~mohsen.hooshmand//courses/0001/2/MRA00012.html>