Multi-factor authentication model based on multipurpose speech watermarking and online speaker recognition

ABSTRACT

In this paper, a Multi-Factor Authentication (MFA) method is developed by a combination of Personal Identification Number (PIN), One Time Password (OTP), and speaker biometric through the speech watermarks. For this reason, a multipurpose digital speech watermarking applied to embed semi-fragile and robust watermarks simultaneously in the speech signal, respectively to provide tamper detection and proof of ownership. Similarly, the blind semi-fragile speech watermarking technique, Discrete Wavelet Packet Transform (DWPT) and Quantization Index Modulation (QIM) are used to embed the watermark in an angle of the waveletôs sub-bands where more speaker specific information is available. For copyright protection of the speech, a blind and robust speech watermarking are used by applying DWPT and multiplication. Where less speaker specific information is available the robust watermark is embedded through manipulating the amplitude of the waveletôs sub-bands. Experimental results on TIMIT, MIT, and MOBIO demonstrate that there is a trade-off among recognition performance of speaker recognition systems, robustness, and capacity which are presented by various triangles. Furthermore, threat model and attack analysis are used to evaluate the feasibility of the developed MFA model. Accordingly, the developed MFA model is able to enhance the security of the systems against spoofing and communication attacks while improving the recognition performance via solving problems and overcoming limitations.

Keyword: Attack analysis; Discrete wavelet packet transform; Multi-factor authentication; Online speaker recognition; Speech watermarking; Threat model