

POSTER 49

Metodologias de deteção de impressões digitais forjadas

Sandra Cerdeira Campos Costa^{1*}, Rui MS Azevedo¹, Áurea Madureira-Carvalho^{1,2}

¹TOXRUN – Unidade de Investigação em Toxicologia, Instituto Universitário de Ciências da Saúde, CESPU, CRL, 4585-116 Gandra, Portugal.

²REQUIMTE/LAQV, Laboratório de Farmacognosia, Departamento de Ciências Químicas, Faculdade de Farmácia, Universidade do Porto, Rua Jorge Viterbo Ferreira, 228, 4050-313 Porto, Portugal.

*✉ smccc@hotmial.com

Doi: <https://doi.org/10.51126/revsalus.v4iSup.316>

Resumo

Introdução: A impressão digital (ID) pode, entre outros, funcionar como meio de autenticação pessoal, sendo perene, imutável e diversiforme, agindo tal como uma senha ou cartão de acesso. Embora de fácil utilização, tem a desvantagem de que uma vez comprometida, não pode ser alterada. A existência de IDs forjadas que permitem autenticações não genuínas e escapam a sistemas “Presentation Attack Detection” (PAD) é uma preocupação crescente para os especialistas forenses. A resistência a ataques depende da tecnologia utilizada e dos mecanismos de processamento implementados [1].

Objetivos: Identificar os diversos materiais existentes para a produção de IDs falsas e de métodos para a sua deteção. **Material e Métodos:** Os termos “falsificação de impressões digitais”, “ciência forense proactiva” e “novos materiais”, foram pesquisados na PubMed (U.S. National Library of Medicine), na EBSCOhost e no Google Académico, sem limitação temporal e geográfica. **Resultados:** Existem diversos sistemas de reconhecimento de IDs, entre os quais sensores óticos, capacitivos, ultrasónicos e térmicos. Nos sensores óticos é formada apenas uma imagem bidimensional da ID sendo que nos capacitivos são utilizadas diferenças de carga

elétrica produzidas entre cristas e sulcos. Os sensores ultrasónicos usam ondas acústicas que possibilitam uma representação 3D, e os sensores térmicos registam gradientes de temperatura entre diferentes zonas da ID. São utilizados diversos materiais para a falsificação de IDs, nomeadamente, silicone, gelatina, Play-Doh, látex, plasticina, Ecoflex, argila, hidrogéis, entre outros. Novos materiais poliméricos, numa lógica de aplicação da estratégia “ciência forense proactiva”, demonstram potencial utilização ilícita, contornando os mecanismos de deteção de vivacidade [1,2,3]. São deste modo relevantes todas as técnicas que vão surgindo para garantir uma maior segurança nos sistemas, baseadas em software ou hardware [1,3]. Alguns estudos referem a utilização de inteligência artificial para contornar uma limitação dos sistemas PAD atuais, como a capacidade de generalização a novos materiais e sensores [4]. Existem ainda outras metodologias baseadas em tomografia de coerência ótica, capazes de extrair características até 1/2mm de profundidade na pele [5]. **Conclusões:** As metodologias referidas auxiliam na deteção de IDs forjadas com diferentes níveis de eficácia, sendo que o risco de sucesso na utilização das mesmas ainda não é negligenciável.

Palavras-chave: Ciência Forense Proactiva; Identificação humana; Lofoscopia; Presentation Attack Detection; Sensores.

Referências:

- [1] Marasco, E. and Rossa, A, A Survey on Antispoofing Schemes for Fingerprint Recognition Systems. *ACM Computing Surveys*, 2014. 47(2): p. 1-36.
- [2] Saguy, M., et al., Proactive forensic science in biometrics: Novel materials for fingerprint spoofing. *J Forensic Sci*, 2022. 67(2): p. 534-542
- [3] Sequeira, A.F. and J.S. Cardoso, Fingerprint Liveness Detection in the Presence of Capable Intruders. *Sensors (Basel)*, 2015. 15(6): p. 14615-38.
- [4] Groz, S., et al., Fingerprint Presentation Attack Detection: A Sensor and Material Agnostic Approach. *IEEE International Joint Conference on Biometrics (IJCB)*, 2020. p. 1-10.
- [5] Auksorius, E., et al., Compact and Mobile Full-Field Optical Coherence Tomography Sensor for Subsurface Fingerprint Imaging. *IEEE Access*, 2020. 8: p. 15194-15204.