Science & Technology in Policing

POLICE STAR FUND 24/25

# PULSE (PROFILE UNMASKING & LINKING SOFTWARE ENGINE)


## Summary

PULSE aims to enhance digital law enforcement by identifying concealed online identities. PULSE addresses the gap in current methods of online identity verification and crime detection, which are manual, time consuming, and limited. Leveraging advanced technologies like artificial intelligence, PULSE will automate and improve the process of unmasking individuals behind pseudonymous profiles.



## Organisations

**Hertfordshire Constabulary**
University of Hertfordshire
OSIRT


## Challenge

This project was inspired by the challenges faced by Internet Intelligence and Investigation (III) staff across law enforcement who are trying to uncover the real-life identities of offenders online. Whilst other lines of investigation exist, such as communication data requests to telecoms providers, many offenders have high operational security and as such these enquires do not lead to the real-life identity.

Current manual and time-consuming approaches to online identity verification are inadequate given today's complex online threats. Studies like Nichele et al. (2022)[1] highlight the difficulties in managing pseudo-anonymous digital platforms, while Woods and Ruscher (2021)[2] illustrate the challenges in unmasking individuals behind coordinated hate campaigns.

## Innovation or research

PULSE is designed to assist in the detection and linkage of harmful or pseudonymous online profiles by applying advanced machine learning and computational linguistics. The technology is rooted in established scientific research in Natural Language Processing (NLP), authorship attribution and network analysis, and seeks to automate tasks that are currently time-consuming and inconsistent when performed manually by investigators.

PULSE integrates structured intelligence data with open-source content and, where available, Computer Network Operations (CNO) inputs to create a multi-layered analytical framework. The tool applies content analysis, sentiment assessment, and stylometric techniques to dissect nuanced patterns in user-generated content. This is particularly useful when dealing with cloaked or anonymised profiles that evade conventional investigative approaches. As Rabe (2023)[3] notes, such cloaked digital personas pose methodological challenges due to the intentional obfuscation of identifiers, making automated linguistic inference a vital tool for identification.

A key innovation within PULSE is its visualisation layer, which translates complex algorithmic outputs into interpretable formats for investigators. Building on principles from digital forensics and visual semiotics, the system offers visual clustering that makes it easier for users to identify relationships among accounts and content based on inferred authorship or behavioural similarity (Leone, 2021)[4].

## Findings

Culmination of project was the successful development of a functional prototype designed to enhance the ability of law enforcement to detect and link pseudonymous online profiles. It represents a significant step forward in addressing the challenge of identifying individuals operating anonymously online for harmful or unlawful purposes.

Throughout the project, key findings emerged that will inform further development and potential operational deployment. Among the most encouraging was the level of analytical enhancement observed during early tests. The system was able to process and surface linkages that would typically take human analysts far longer to detect, especially where traditional username or profile clues were obfuscated. At the same time, some imitations were identified, particularly in relation to performance on media-heavy or short-form content platforms, where the absence of rich textual data poses an ongoing challenge for automated processing.

## Next steps

Further funding has been gained, this will allow the PULSE concept to develop further. Further testing and development of the prototype and incorporation of an ethical governance framework to provide transparency and reassurance on use of artificial Intelligence and algorithms.

1 Nichele, E., Lavorgna, A. and Middleton, S.E. (2022) 'Identifying key challenges and needs in digital mental health moderation practies supporting users exhibiting risk behaviours to develop responsible AI tools: The case study of Kooth', SN Social Sciences, 2, 217. doi: 10.1007/s43545-022-00532-3.

2 Woods, F.A. and Ruscher, J.B. (2021) 'Viral sticks, virtual stones: Addressing anonymous hate speech online', Patterns of Prejudice, 55(3), pp. 265–289. doi: 10.1080/0031322X.2021.1968586

3 Rabe, T. (2023) 'Addressing the methodological challenges that cloaked profiles pose to digital observations', Journal of Contemporary Ethnography,

4 Leone, M. (2021) 'From fingers to faces: Visual semiotics and digital forensics', International Journal for the Semiotics of Law, 34(2), pp. 579–599. doi: 10.1007/s11196-020-09766-x.