DOI
https://doi.org/10.18690/um.feri.4.2026.5

ISBN
978-961-299-111-1

PROJEKT HORIZON EUROPE ONMOVEID: TEHNIČNO OZADJE AVTOMATIZACIJE PREHODA SCHENGENSKE MEJE

KLEMEN VOVK, ROMANELA LAJIĆ, ŽAN KOGOVŠEK, JERNEJ SABADIN, BLAŽ MEDEN, ŽIGA EMERŠIČ, PETER PEER

Univerza v Ljubljani, Fakulteta za računalništvo in informatiko, Ljubljana, Slovenija
klemen.vovk@fri.uni-lj.si, romanela.lajic@fri.uni-lj.si, zan.kogovsek@fri.uni-lj.si, jernej.sabadin@fri.uni-lj.si, blaz.meden@fri.uni-lj.si, ziga.emersic@fri.uni-lj.si, peter.peer@fri.uni-lj.si

Projekt OnMoveID si prizadeva nadomestiti stacionarne kontrole schengenskega mejnega nadzora s preverjanjem "med gibanjem" (move-through) za kopenske, morske in zračne meje. Z uporabo razširjenih denarnic za evropsko digitalno identiteto (EUDI) in standardnih pametnih telefonov želi projekt povečati pretočnost potnikov ter hkrati izboljšati varnost. Članek obravnava dve ključni komponenti 7. delovnega sklopa projekta: razvoj robustnih algoritmov za biometrično prepoznavanje in implementacijo naprednih mehanizmov za odkrivanje napadov. Te naloge naslavljajo tehnične izzive preverjanja istovetnosti z visoko stopnjo zanesljivosti na mobilnih napravah, ki so izpostavljene tveganjem in omejitvam delovanja v nenadzorovanih okoljih.

Ključne besede:
OnMoveID, schengenski mejni nadzor, biometrično prepoznavanje, odkrivanje napadov, mobilno preverjanje istovetnosti, preverjanje med gibanjem

Univerzitetna založba Univerze v Mariboru

DOI
https://doi.org/10.18690/um.feri.4.2026.5

ISBN
978-961-299-111-1

HORIZON PROJECT ONMOVEID: TECHNICAL BACKGROUND OF SCHENGEN BORDER CROSSING AUTOMATION

KLEMEN VOVK, ROMANELA LAJIĆ, ŽAN KOGOVŠEK, JERNEJ SABADIN, BLAŽ MEDEN, ŽIGA EMERŠIČ, PETER PEER

University of Ljubljana, Faculty of Computer Science and Informatics, Ljubljana, Slovenia
klemen.vovk@fri.uni-lj.si, romanela.lajic@fri.uni-lj.si, zan.kogovsek@fri.uni-lj.si, jernej.sabadin@fri.uni-lj.si, blaz.meden@fri.uni-lj.si, ziga.emersic@fri.uni-lj.si, peter.peer@fri.uni-lj.si

Keywords:
OnMoveID, schengen border control, biometric recognition, attack detection, mobile identity verification, move-through verification

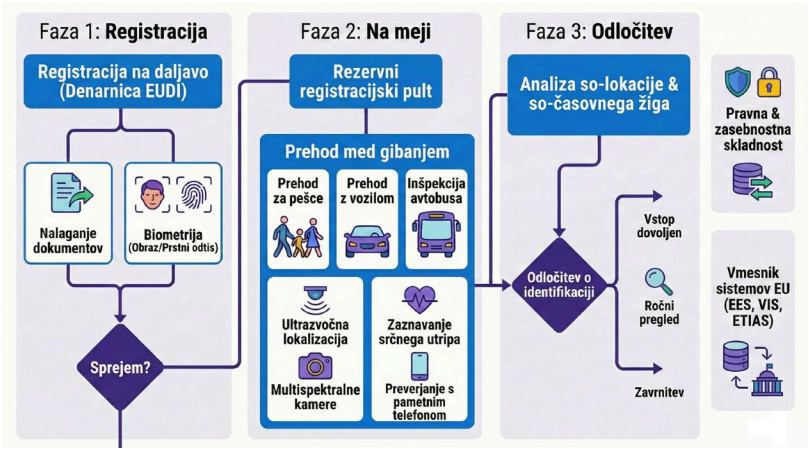
The OnMoveID project aims to replace Schengen border control stationary checks with "move-through" verification for land, sea, and air borders. By using extended European Digital Identity (EUDI) wallets and standard smartphones, the project seeks to increase traveler throughput while enhancing security. This paper examines two critical components of the project's Work Package 7: the development of robust biometric recognition algorithms and the implementation of advanced attack detection mechanisms. These tasks address the technical challenges of performing high-assurance identity verification on non-trusted mobile devices in uncontrolled environments.

University of Maribor Press

1 Uvod

Z eksponentno rastjo števila potnikov na zunanjih mejah EU postajajo konvencionalne metode mejnega nadzora nevzdržne. Projekt OnMoveID naslavlja ta izziv s prehodom na avtomatizirano preverjanje med gibanjem (glej sliko 1), ki drastično povečuje pretočnost brez kompromisov pri varnosti. V predlagani arhitekturi mobilne naprave in pametni telefoni ne delujejo kot samostojne enote za odločanje, temveč služijo primarno kot senzorski vmesniki za detekcijo obrazov in morebitni izračun osnovnih biometričnih značilk. Sama prepoznava identitete in ujemanje pa se zaradi varnosti in računske zahtevnosti izvajata centralizirano na zavarovanih strežnikih.

Glavni inženirski in raziskovalni izziv projekta predstavlja zagotavljanje zanesljive prepoznave oseb v izjemno raznolikih in nenadzorovanih okoljih, ki se bistveno razlikujejo od kontroliranih e-vrat (angl. e-gates). Sistem mora namreč delovati robustno ne le na letališčih, temveč tudi v kompleksnejših scenarijih na kopenskih mejah. To vključuje prepoznavo potnikov v notranjosti osebnih vozil preko zunanjih kamer ter situacije, kjer mejni policist z mobilno napravo v roki hodi skozi avtobus in sproti zajema biometrične podatke potnikov.



Slika 1: Diagram postopka prehajanja potnikov prikazuje tristopenjski sistem mejnega nadzora, ki z uporabo oddaljene registracije in biometričnih senzorjev omogoča tekoč prehod med gibanjem brez ustavljanja. Cilj je, da proces zagotavlja visoko stopnjo varnosti s preverjanjem v realnem času in neposredno povezavo z relevantnimi informacijskimi sistemi EU.

Vir: lasten.

Ta prispevek se osredotoča na specifične tehnične rešitve znotraj delovnega paketa, ki omogočajo takšno fleksibilnost. Podrobneje predstavljamo razvoj algoritmov, ki so sposobni kompenzirati spremenljive pogoje (osvetlitev, kot snemanja, premikanje policista ali vozila) ter nove pristope za zaznavo napadov, ki bi poskušali zmanipulirati zajem podatkov na terenu.

2 Razpoznava obrazov in prstnih odtisov

Za delovanje sistema je ključen razvoj robustnega multimodalnega biometričnega cevovoda, zasnovanega za obdelavo podatkov iz heterogenih virov zajema. Čeprav sodobni biometrični sistemi dosegajo visoko zanesljivost v standardiziranih okoljih (kot so e-vrata), se pri prehodu na dinamične mejne kontrole soočamo s ključnim izzivom: variabilnostjo vhodnih podatkov, ki prihajajo iz različnih naprav.

Cilj projekta OnMoveID je tako zagotoviti zanesljivo strežniško primerjavo biometričnih značilk, ne glede na to, ali so bile te zajete s stacionarno kamero, policijsko tablico ali drugim senzorjem. Sistem pragmatično izkorišča standardne modalnosti – kamero za prepoznavo obraza in senzorje za prstne odtise – ter zagotavlja, da se ti raznoliki vnosi kljub različnim pogojem zajema uspešno preslikajo v enoten in varen proces verifikacije identitete na centralnem strežniku.

2.1 Večdelna razpoznava obraza

Za obvladovanje variabilnosti v nenadzorovanih okoljih projekt uvaja napreden pristop, ki temelji na obdelavi video posnetkov namesto zgolj posameznih statičnih slik. Ključna prednost tega pristopa je gradnja robustnega modela identitete skozi časovno okno. Sistem iz zaporedja slik videa (ang. frames) sproti izlušči in akumulira najkvalitetnejše biometrične informacije, s čimer kompenzira trenutne motnje, kot so premikanje glave, spremenljiva razdalja ali neenakomerna osvetlitev.

Znotraj tega procesa se vsaka posamezna slika v zaporedju še dodatno analizira po segmentih (npr. oči, nos, usta), namesto da bi se obraz obravnaval le kot celota. To omogoča, da algoritem v končni model identitete selektivno vključi tiste dele obraza, ki so v določenem trenutku najbolje vidni in nezakriti. Takšna kombinacija časovne integracije in prostorske segmentacije je ključna za zanesljivost, saj empirične študije potrjujejo, da k uspešnosti razpoznave ne prispevajo vsi deli obraza enako in je

njihova kakovost v mobilnih scenarijih spremenljiva (Lestriandoko, Veldhuis & Spreeuwers, 2022)

2.2 Razpoznavanje prstnih odtisov

Čeprav je biometrija na pametnih telefonih danes vseprisotna, je njena uporaba skoraj izključno omejena na lokalno verifikacijo 1:1 (odklepanje naprave) znotraj zaprtega varnostnega ekosistema operacijskega sistema. Tu projekt naslavlja bistveno zahtevnejši inženirski izziv: omogočiti identifikacijo 1:N in preverjanje identitete v sistemih mejne kontrole, ne da bi pri tem potrebovali namensko zunanjo strojno opremo.

Glavna ovira pri tem je t.i. strojna fragmentacija. Ker razvijalci nimajo neposrednega dostopa do surovih podatkov vgrajenih kapacitivnih senzorjev (zlasti v okolju iOS), projekt uvaja rešitev, ki temelji na brezstičnem optičnem zajemu. S tem pristopom pametni telefon spremenimo v visokoločljivostni čitalec, ki ne zahteva fizičnega stika s površino.

Ključna inovacija ni le v samem zajemu, temveč v procesiranju signala. Da bi zagotovili združljivost z obstoječimi policijskimi in mejnimi bazami, ki temeljijo na kontaktnih odtisih, algoritem v realnem času ocenjuje kakovost slike po standardu NFIQ 2.0 (NIST Fingerprint Image Quality). Sistem samodejno kompenzira spremenljivo osvetlitev in perspektivna popačenja, s čimer zagotavlja skladnost s standardom ISO/IEC 29794-5. To pomeni, da lahko brezstično zajeti odtis na telefonu doseže enako raven zaupanja kot tradicionalni stacionarni čitalci, kar je predpogoj za uporabo v varnostno kritičnih procesih, kot je prestop meje. Čeprav je kakovosten zajem ključen za natančno razpoznavo, v nenadzorovanem mobilnem okolju sama natančnost ne zadostuje. Zato v naslednjem poglavju obravnavamo napade in mehanizme ugotavljanja živosti.

3 Analiza napadov in ugotavljanje živosti

Prehod na mobilno verifikacijo prinaša korenito spremembo v varnostni arhitekturi: ločitev naprave za zajem (nezaupanja vreden pametni telefon) od strežnika za odločanje. Predlog rešitve, ki ga vodi Cabinet Louis Reynaud (CLR) v sodelovanju s partnerji (vključno z UL in THALES), naslavlja tveganja te vrzeli zaupanja.

Naš pristop naslavlja kritično pomanjkljivost v obstoječih sistemih: v nenadzorovanih okoljih so prevladujoči vektorji prevare tako predstavitveni napadi (npr. tiskane fotografije, predvajanje videa, maske) kot tudi napadi z vrivanjem biometričnih podatkov, pri katerih se biometrični tok v aplikacijo vstavi programsko (npr. prek navidezne kamere, emulatorja ali namenskih orodij). Zato ugotavljanje živosti in zaznavanje vrivanja podatkov obravnavamo kot dopolnjujoča se varnostna sloja.

3.1 Zaznavanje napadov z vrivanjem podatkov

Primarni cilj tega dela je zaznavanje napadov, pri katerih napadalec uporabi navidezno kamero, emulator ali namensko programsko opremo za neposredno vstavljanje lažnih videoposnetkov v pomnilnik aplikacije, s čimer povsem obide fizično lečo kamere.

Čeprav zakonodaja (eIDAS) in okviri (PVID) že opozarjajo na to tveganje, trg ponuja malo učinkovitih rešitev. V okviru projekta razvijamo mehanizme zaznavanja, ki so skladni z novim evropskim standardom CEN/TS 18099:2024 in ciljajo na visoko raven zagotovila. Sistem analizira metapodatke senzorja in anomalije v video-toku, da zanesljivo loči med organskim posnetkom žive kamere in sintetičnim ali vrinjenim videom.

3.2 Zaznavanje predstavitvenih napadov

Za preprečevanje kraje identitete s fizičnimi pripomočki (maske, fotografije, zasloni) sistem implementira robustno ugotavljanje živosti, skladno s standardom ISO/IEC 30107-3. Namesto zastarelih aktivnih metod (zahteva po mežikanju ali nasmehu), ki jih je lažje zaobiti, se uvajajo pasivne tehnike, kot jih povzema tudi pregled sodobnih pristopov k preprečevanju predstavitvenih napadov na obrazih (Yu et al., 2023).

- **Analiza mikrogibov in teksture**: Rešitev uporablja fotopletizmografijo na daljavo (rPPG) za zaznavanje nevidnih sprememb v barvi kože, ki so posledica srčnega utripa (Liu, Lan in Yuen, 2018). Utrip je lastnost, ki je statične maske ne morejo replicirati. Hkrati modeli globokega učenja analizirajo sipanje svetlobe na površini, s čimer ločijo pravo človeško kožo od silikona, papirja ali svetlobnih pik na zaslonu (Yu et al., 2023).

– **Globina in 3D struktura:** Kjer strojna oprema to dopušča (senzorji globine ali stereo-kamere), sistem preverja 3D obliko obraza. V standardnih RGB scenarijih pa uporabljamo algoritme za strukturo iz gibanja, ki na podlagi pojava paralakse ocenijo prostorskost obraza in tako preprečijo predvajanje ploskih videoposnetkov ali fotografij (Wang et al., 2013).

3.3 Diferencialno zaznavanje napadov z morfiranjem

Napadi z morfiranjem (zlivanje dveh obrazov v eno fotografijo, kar lahko omogoča dvema osebama uporabo istega dokumenta) predstavljajo resno grožnjo mejni kontroli (Ferrara, Franco in Maltoni, 2014). Za boj proti temu je ena izmed bolj popularnih metod metoda diferencialnega zaznavanja (D-MAD): za razliko od analize ene slike, ki išče nepravilnosti na fotografiji, ta pristop izkorišča zaupanja vreden referenčni vir – sliko, varno prebrano s čipa potnega lista, in jo primerja z živo zajeto sliko (Scherhag et al., 2020). Implementacijo planiramo izvesti skladno s smernicami ISO/IEC 20059:2025 (ISO/IEC, 2025): modul primerja globoke značilke referenčne slike s čipa z živo zajeto sliko. Naši modeli bodo dodatno naučeni na naborih podatkov s transformacijami »print-scan«, kar zagotavlja odpornost tudi proti napadalcem, ki morfirano fotografijo fizično natisnejo, da bi prikrili digitalne sledi (Scherhag et al., 2020).

4 Zaključek

Razvojne aktivnosti znotraj projekta OnMoveID ne predstavljajo le programske nadgradnje, temveč temeljni inženirski odziv na omejitve trenutne mejne infrastrukture. S prehodom na večdelno razpoznavo obraza in prstnih odtisov pokažemo, da je mogoče biometrično natančnost, primerljivo s stacionarnimi e-vrati, doseči tudi na komercialnih mobilnih napravah v nenadzorovanih pogojih.

Vendar pa sama biometrična natančnost brez ustrezne varnosti v odprtem ekosistemu ne zadostuje. Z implementacijo naprednih obrambnih mehanizmov, ki so skladni z najnovejšimi standardi (kot sta CEN/TS 18099 in ISO/IEC 30107-3), projekt uspešno naslavlja kritično vrzel zaupanja. Zmožnost sistema, da v realnem času loči med avtentičnim potnikom in sofisticiranim napadom s ponarejenimi podatki, je tisti ključni element, ki pametni telefon pretvori v varen potovalni žeton.

Tehnologije, predstavljene v tem članku, so pomemben korak za implementacijo vizije tekočega, brezkontaktnega prehajanja meja, ki ne sklepa kompromisov med varnostjo držav in pretočnostjo potnikov.

Viri in literatura

Clewlow, R. R. (2016). Carsharing and sustainable travel behavior: Results from the San Francisco Bay Area. *Transport Policy, 51*, 158-164. doi:10.1016/j.tranpol.2016.01.013

Lestriandoko, N. H., Veldhuis, R., & Spreeuwers, L. (2022). *The contribution of different face parts to deep face recognition. Frontiers in Computer Science, 4*, 958629. doi:10.3389/fcomp.2022.958629

CEN. (2024). *CEN/TS 18099:2024: Biometric data injection attack detection*. European Committee for Standardization.

ISO/IEC. (2023). ISO/IEC 30107-3:2023 Information technology — Biometric presentation attack detection — Part 3: Testing and reporting. International Organization for Standardization.

ISO/IEC. (2025). ISO/IEC 20059:2025 Information technology — Methodologies to evaluate the resistance of biometric systems to morphing attacks. International Organization for Standardization.

Yu, Z., Qin, Y., Li, X., Zhao, C., Lei, Z., & Zhao, G. (2023). Deep learning for face anti-spoofing: A survey. IEEE Transactions on Pattern Analysis and Machine Intelligence, 45(5), 5609–5631. https://doi.org/10.1109/TPAMI.2022.3215850

Liu, S.-Q., Lan, X., & Yuen, P. C. (2018). Remote photoplethysmography correspondence feature for 3D mask face presentation attack detection. In Proceedings of the European Conference on Computer Vision (ECCV 2018). https://doi.org/10.1007/978-3-030-01270-0_34

Wang, T., Yang, J., Lei, Z., Liao, S., & Li, S. Z. (2013). Face liveness detection using 3D structure recovered from a single camera. In Proceedings of the International Conference on Biometrics (ICB 2013). https://doi.org/10.1109/ICB.2013.6612957

Ferrara, M., Franco, A., & Maltoni, D. (2014). The magic passport. In Proceedings of the International Joint Conference on Biometrics (IJCB 2014), 1–7.

Scherhag, U., Rathgeb, C., Merkle, J., & Busch, C. (2020). Deep face representations for differential morphing attack detection. IEEE Transactions on Information Forensics and Security, 15, 3625–3639. https://doi.org/10.1109/TIFS.2020.2994750

ISO/IEC. (2017). ISO/IEC 29794-4:2017 Information technology — Biometric sample quality — Part 4: Finger image data. International Organization for Standardization.

Tabassi, E., Olsen, M., Bausinger, O., Busch, C., Figlarz, A., Fiumara, G., Henniger, O., Merkle, J., Ruhland, T., Schiel, C., & Schwaiger, M. (2021). NFIQ 2: NIST Fingerprint Image Quality (NIST Interagency Report 8382). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8382