Sistemi Multi-Biometrici per l'Autenticazione Continua e Trasparente per l'Accesso a Servizi di Erogazione Contenuti

Silvio Barra, Gianni Fenu e Mirko Marras
Dipartimento di Matematica e Informatica, Università di Cagliari, V. Ospedale 72, 09124 Cagliari, Italia
{silvio.barra, fenu, mirko.marras}@unica.it

Abstract

I sistemi di autenticazione continua stanno abilitando la verifica regolare e trasparente dell'identità di un utente lungo una sessione, senza interferire sulle sue normali attività. Con la crescita del mercato globale dell'apprendimento online, tali sistemi possono supportare gli enti e le istituzioni di formazione nel garantire l'integrità delle attività online dei discenti. In questo contesto, stiamo studiando diversi sistemi di autenticazione multi-biometrica, continua e trasparente, su misura del dispositivo e della modalità d'interazione degli studenti.

1 Contesto di riferimento e motivazione

L'ultimo decennio ha mostrato un sempre più crescente interesse nell'autenticazione biometrica continua [Patel *et al.*, 2016]. Essa consiste nel verificare ripetutamente l'identità di un utente mediante tratti biometrici per prevenire frodi legate all'impersonazione. Tali frodi possono riguardare il furto, la negazione o la condivisione dell'identità. Nel primo caso, un utente viene impersonato da uno sconosciuto che è interessato a condurre attività malevole. Nel secondo caso, un individuo autorizzato conduce azioni illegali e ne ripudia l'esecuzione. Nel terzo caso, un individuo autorizzato condivide le proprie credenziali volontariamente con altri, violando regolamenti.

La formazione online rappresenta un'area di rilievo in cui si possono osservare tali frodi e l'autenticazione continua può aiutare a ridurne il numero [Draaijer *et al.*, 2017]. È emersa, infatti, la necessità di verificare l'identità degli studenti e garantire l'integrità delle loro attività online. Gli esami elettronici possono favorire molteplici comportamenti scorretti rispetto agli esami cartacei, e gli esami a distanza ne introducono ancor di più rispetto agli esami in loco. Le stesse osservazioni sono valide per la fase di erogazione contenuti. Comprendere questi rischi e studiare possibili attenuazioni è importante. Le soluzioni esistenti spaziano dalla supervisione remota umana, al monitoraggio automatizzato, fino a modalità ibride dove uomo e sistema cooperano attivamente.

L'intelligenza artificiale sta promuovendo la nascita di sistemi capaci di apprendere meglio le caratteristiche biometriche degli individui. Per essere applicabili, essi dovrebbero lavorare in maniera continua, affinché l'utente non possa essere impersonato, e trasparente, così da non interferire sulle normali attività. Sono svariati i sistemi biometrici nel settore e-learning [Kumar, 2019]. Quelli che utilizzano biometrie fisiche catturano solitamente i tratti facciali. In altri casi, vengono combinate più biometrie, ma sono spesso richieste azioni intrusive o dispositivi aggiuntivi. Quelli che utilizzano biometrie comportamentali agiscono trasparentemente, ma non sono sufficientemente affidabili da soli. Tendono poi a supportare una data modalità di interazione, come la battitura, ma ne esistono altre, tra cui quella di selezione e quella vocale. In aggiunta, il dispositivo impiegato delinea le soluzioni adottabili in una formazione sempre più orientata ai dispositivi mobili e, sebbene sia un'area poco esplorata, la rilevazione di altre attività scorrette sarebbe auspicabile. Essere in grado di modellare questa complessità può garantire maggiore tracciabilità e integrità del percorso formativo online.

2 Attività di ricerca

Lo scenario presentato vede coinvolto il nostro gruppo di ricerca nell'analisi di immagini e segnali continui, tracciati dai sensori installati nei dispositivi, per fini di autenticazione e identificazione biometrica. Le attività svolte rientrano nella:

- formulazione di teorie di apprendimento automatico per la fusione congiunta di tratti biometrici multipli, fondate su osservazioni e vincoli dei contesti reali;
- addestramento di algoritmi su dati multi-biometrici al fine di estrarre modelli generalizzabili su contesti non controllati con quantità ridotte di dati sul singolo utente;
- studio di metodologie di autenticazione e identificazione che integrano biometrie fisiche e comportamentali e garantiscono continuità e trasparenza del processo;
- sviluppo di prototipi attraverso i quali le componenti studiate possono essere validate in contesti reali.

Tra i contributi proposti, rientrano approcci basati sul volto, sulla zona perioculare, sulla voce, sul tocco sullo schermo, sulla battitura e sul movimento delle mani [Fenu *et al.*, 2018; Fenu e Marras, 2017; Fenu e Marras, 2018].

3 Caso di studio esemplificativo

L'approccio qui descritto integra biometrie del volto, del tocco e del movimento delle mani (Figura 1). La sua descrizione completa è disponibile in [Fenu e Marras, 2018].

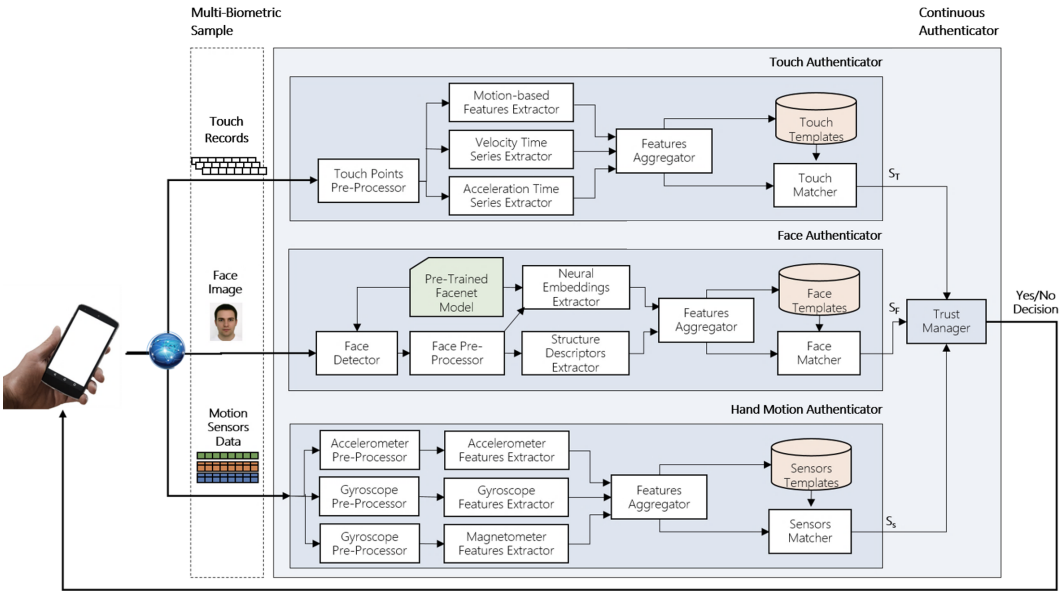

Figura 1: L'approccio proposto per l'autenticazione continua basata su volto, tocco e movimento delle mani su dispositivi mobili.

L'approccio funziona come segue. Dalla fase di login, un modulo di tracciamento continuo, operante nel dispositivo, colleziona i dati relativi al tratto del tocco, le immagini acquisite dalla fotocamera e i dati dell'accelerometro, del giroscopio e del magnetometro rilevati in prossimità del tocco. Il campione multi-biometrico viene inviato all'autenticatore continuo. In esso, ogni autenticatore biometrico singolo esegue autonomamente una comparazione tra le caratteristiche estratte dall'immagine del volto, dai dati del tocco o dai sensori di movimento e i corrispondenti modelli biometrici generati in precedenza per quel dato utente, restituendo ciascuno un punteggio di similarità. I punteggi sono fusi e sulla base del punteggio complessivo risultante viene deciso se l'utente potrà continuare ad interagire nell'attuale sessione.

Per valutarne l'applicabilità, l'approccio è stato testato su un dataset multi-biometrico di 100 utenti, ottenuto dalla fusione di due dataset pubblicamente disponibili. Le prestazioni sono state misurate calcolando l'Equal Error Rate (EER), indice di una uguale proporzione tra false accettazioni e falsi rifiuti. Più è basso il valore, più è alta la precisione. Nella prima configurazione, sono state misurate le prestazioni quando la registrazione del modello biometrico e l'autenticazione avvengono nella stessa sessione. Si presuppone che l'utente autorizzato effettui il login e la registrazione del modello parta all'inizio della sessione. Dopo aver tracciato alcuni campioni, l'approccio passa alla modalità di autenticazione, potendo rilevare se un'altra persona sostituisce l'utente autorizzato. In questa configurazione, è stato calcolato un EER del 0.84%. Nella seconda configurazione, sono state misurate le prestazioni quando l'autenticazione è eseguita alcune settimane dopo la registrazione del modello biometrico. Per autenticare l'utente, si sono confrontate le caratteristiche dei dati raccolti con il modello creato nelle sessioni precedenti. In questo scenario più realistico, si è misurato un EER del 3,56%.

Le attività future sono articolate sui seguenti fronti. Si prevede l'impiego di infrastrutture capaci di garantire operatività su larga scala e di migliorare ed integrare gli approcci sviluppati, includendo anche altre biometrie. Inoltre, si prevede la validazione delle soluzioni in scenari reali e la creazione di un dataset multi-biometrico specifico del contesto, con particolare attenzione alla privacy degli utenti.

Ringraziamenti

Le attività sono parzialmente supportate dal Ministero dell'Istruzione, dell'Università e della Ricerca (MIUR) nell'ambito del progetto "iLearnTV Anywhere Anytime" (DD n.1937 05.06.2014, CUP F74G14000200008 F19G14000910008).

Riferimenti bibliografici

[Draaijer *et al.*, 2017] S. Draaijer, A. Jefferies, e G. Somers. Online proctoring for remote examination: A state of play in higher education in the eu. In *International Conference on Technology Enhanced Assessment*, pages 96–108. Springer, 2017.

[Fenu *et al.*, 2018] G. Fenu, M. Marras, e L. Boratto. A multi-biometric system for continuous student authentication in e-learning platforms. *Pattern Recognition Letters*, 113, 2018.

[Fenu e Marras, 2017] G. Fenu e M. Marras. Leveraging continuous multi-modal authentication for access control in mobile cloud environments. In *International Conference on Image Analysis and Processing*, pages 331–342. Springer, 2017.

[Fenu e Marras, 2018] G. Fenu e M. Marras. Controlling user access to cloud-connected mobile applications by means of biometrics. *IEEE Cloud Computing*, 5(4):47–57, 2018.

[Kumar, 2019] A. Kumar. Biometric authentication in online learning environments. pages 1–314. IGI Global, 2019.

[Patel *et al.*, 2016] V. M Patel, R. Chellappa, D. Chandra, e B. Barbello. Continuous user authentication on mobile devices: Recent progress and remaining challenges. *IEEE Signal Processing Magazine*, 33(4):49–61, 2016.