



PROGETTO BIOFACE - STUDIO DI FATTIBILITÀ PER UN SISTEMA DI RICONOSCIMENTO BIOMETRICO FACCIALE

ABSTRACT

OBIETTIVI

Il problema di identificare la presenza di una persona e verificarne l'identità dichiarata in situazioni non controllate è ancora aperto, nonostante i decenni di ricerca dedicati a queste tematiche dai ricercatori delle comunità della visione artificiale e dell'apprendimento automatico. Gli algoritmi di riconoscimento di volti presenti in letteratura, richiedono quasi sempre un'implicita cooperazione dell'utente che deve posizionarsi in modo opportuno rispetto alla telecamera. I pochi tentativi che sono stati fatti nella direzione di sistemi di validazione per applicazioni reali di videosorveglianza si scontrano con il fatto che il problema è troppo difficile per portare alle alte percentuali di riconoscimento che solitamente interessano il mercato dei prodotti.

Rispetto al classico caso di identificazione di volti in situazioni controllate, la *face validation* in ambienti non controllati deve affrontare i seguenti problemi:

- la qualità delle immagini tende ad essere peggiore
- i volti non sono necessariamente frontali
- non vi sono garanzie sulla distanza relativa tra sistema di visione e persona osservata, di conseguenza non si possono fare assunzioni sulle dimensioni del volto all'interno dell'immagine
- i requisiti temporali richiedono soluzioni semplici ed ottimizzate

Gli obiettivi di questo progetto sono volti a valutare la possibilità e la convenienza di sviluppare e sperimentare soluzioni tecnologicamente avanzate per un supporto al mercato delle tecniche di

riconoscimento avanzate, caratterizzato da una crescente attenzione per vari motivi (sicurezza, controllo degli accessi, etc..).

In particolare il progetto è stato mirato alla realizzazione di un sistema di individuazione e validazione dei volti di persone di passaggio in situazioni ambientali non controllate, ovvero senza necessità che si fermino e/o che si mettano “in posa” davanti alla telecamera per il riconoscimento, integrando le seguenti tecnologie :

- smart-card RFID a contatto o di prossimità;
- identificazione di persone mediante tecniche di biometria avanzate (acquisizione dinamica della biometria del volto attraverso stream video).

In Italia non vi è notizia di sistemi “ufficialmente” installati per il controllo degli accessi a istituzioni pubbliche o private di natura civile. A questo proposito, è necessario menzionare il documento “Provvedimento del Garante riguardo la Protezione dei Dati Personali” del 28 Settembre 2001, che ha decretato la disattivazione di un sistema di identificazione positiva basato su impronte digitali, sito all’ingresso della Banca CRT – Cassa di Risparmio di Torino e della Veneto Banca S.c.a.r.l., con queste motivazioni:

«L’Autorità ha constatato che l’utilizzo generalizzato e indiscriminato di tali sistemi non è consentito in quanto viola il principio di proporzionalità tra gli strumenti impiegati e le finalità prospettate (art. 9 legge n.695/1996), perseguibili attraverso altri mezzi che comportano minori problemi per la tutela dei diritti e della dignità delle persone interessate. Un’attività indifferenziata di raccolta di dati significativi, quali quelli relativi alle impronte digitali, imposta a tutti coloro - clienti o meno - che entrano in un istituto bancario non può ritenersi legittimata da una generica esigenza di sicurezza. In mancanza di specifici elementi che evidenzino una concreta situazione di rischio tale attività si tradurrebbe in un sacrificio sproporzionato della sfera di libertà e della dignità delle persone interessate. Ciò anche in considerazione della particolare natura delle informazioni raccolte. (...).»

Va quindi considerato, nell’applicabilità al mercato prospettico, anche l’aspetto di gestione dei dati personali sensibili e del rispetto della privacy.

SPERIMENTAZIONE

Per la sperimentazione si è pensato di attrezzare un corridoio, strutturato come un varco a percorso obbligato, denominato convenzionalmente Gate, con lunghezza 4 m e larghezza di circa 1.5 m (vedi Figura 1).

All’inizio del corridoio è posizionato un lettore di smartcard, all’altra estremità la telecamera (in posizione semifrontale), il monitor informativo e gli attuatori per il controllo di apertura/chiusura del varco.

Un ulteriore varco, subito dopo il lettore di smartcard, assolve alla funzione di blocco dell’accesso ai soggetti non in possesso di una smartcard valida.

La prima verifica dell’identità del soggetto, mediante smartcard, viene effettuata al varco A. L’identificativo letto dalla smartcard viene sottoposto a validazione.

Se il soggetto presenta un identificativo smartcard non valido il varco viene mantenuto chiuso e il soggetto non accede alla sezione B per il riconoscimento biometrico. Al soggetto viene mostrato un messaggio informativo del tipo “Utente non valido”.

Se la validazione ha successo, viene attivata l’acquisizione video, il soggetto percorre la sezione B del corridoio di accesso e contestualmente viene effettuata l’analisi biometrica dello stream video.

Se il riscontro biometrico è positivo all'utente viene mostrato un messaggio di benvenuto personalizzato e contestualmente viene aperto il varco B, se negativo viene mostrato un messaggio informativo del tipo "Utente non riconosciuto" e il varco viene mantenuto chiuso.

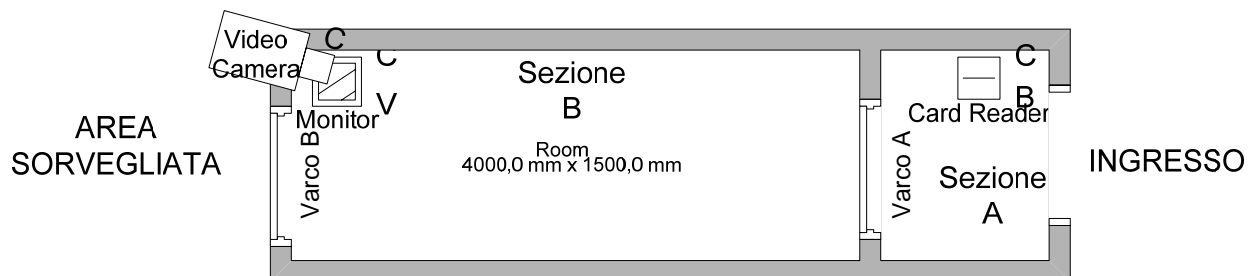


Figura 1: Schema Gate

Gli algoritmi di riconoscimento biometrico sono stati valutati e verificati dal Dipartimento di Informatica e Scienze dell'Informazione dell'Università di Genova, che attraverso di essi, ha realizzato il sistema logico di elaborazione di immagini e detezione dei volti.

Nella loro scelta si tenuto conto dei seguenti requisiti :

- Identificare metodi che non si basino su immagini ad alta risoluzione, ma semmai sfruttino un'informazione ridondante lungo la componente temporale.
- Realizzare un sistema di validazione efficiente e in grado di lavorare, se possibile, in tempo reale.
- Utilizzare in fase di validazione una rappresentazione che rispetti requisiti di compattezza spaziale
- Progettare la fase di training in modo da ottimizzare l'inserimento di un nuovo individuo nel sistema.

Questo sistema di elaborazione di immagini e detezione dei volti è in funzione presso il DISI a partire dal gennaio 2008.

In aggiunta, a partire dal mese di giugno 2008 è iniziata la fase sperimentale vera e propria, basata su una installazione prototipale rispondente all'architettura descritta nella figura 1.

I principali componenti hw e sw che vengono utilizzati sono :

- Una unità di controllo accessi dotata di un lettore di smartcard RFID ISO14443.
- Una telecamera CCTV.
- Un PC dotato di frame-grabber e di librerie di basso livello per l'acquisizione video.
- Un sw di colloquio tra l'unità di controllo accessi e il sistema di elaborazione di immagini e detezione dei volti.

L'installazione è stata effettuata in un corridoio del DISI. Sono state distribuite a circa un centinaio di soggetti volontari, che transitano abitualmente nel corridoio, delle tessere a radio frequenza numerate progressivamente, che permettono al sistema di identificare il portatore attraverso il contatto della tessera con l'apposito lettore. Il lettore, al contatto con la tessera, attiva la ripresa del soggetto da parte di una telecamera anch'essa situata nel corridoio. Tramite l'abbinamento tessera/frame di immagini il

sistema è in grado di stabilire se i dati biometrici del soggetto corrispondono a quelli identificati attraverso il codice della tessera.

Ai soggetti volontari è richiesto esclusivamente di passare la sua tessera sul lettore ogni qualvolta transita nel corridoio, dopodichè transitano normalmente nel corridoio senza “mettersi in posa”. I varchi sono ovviamente “virtuali”, cioè simulati attraverso display di messaggi (riconosciuto/non riconosciuto) . Le condizioni di illuminazione in cui avviene il passaggio sono costanti ma non hanno richiesto particolari accorgimenti legati al processo di riconoscimento (l’illuminazione è la stessa di quella standard realizzata in tutti i piani e corridoi dell’intero edificio).

L’ utilizzo del prototipo realizzato va quindi oltre quello di un semplice dimostratore. Con la semplice collaborazione del volontario a passare la sua tessera sul lettore ogni qualvolta passa nel corridoio, il sistema acquisirà un significativo volume di dati utilizzabile per valutare la percentuale di riconoscimenti positivi, e identificare e capire le motivazioni dei casi di riconoscimento negativo.

Altrettanto sarà possibile analizzare i casi di corretto riconoscimento negativo, semplicemente dotando il volontario di una tessera diversa da quella con cui e’ conosciuto al sistema.