



Festival Smart
Innovation
Silea 15-17
Settembre 2017

Alberto Cammozzo

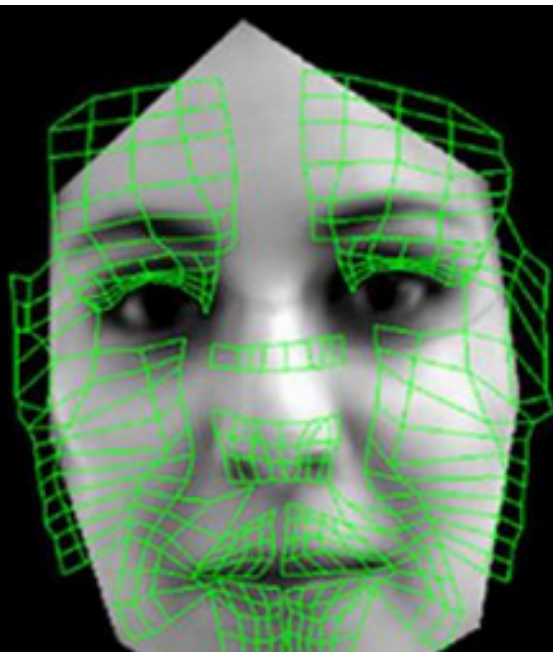
cammozzo.com

tagMeNot.info

unipd.it

Dato *Bio*-metrico

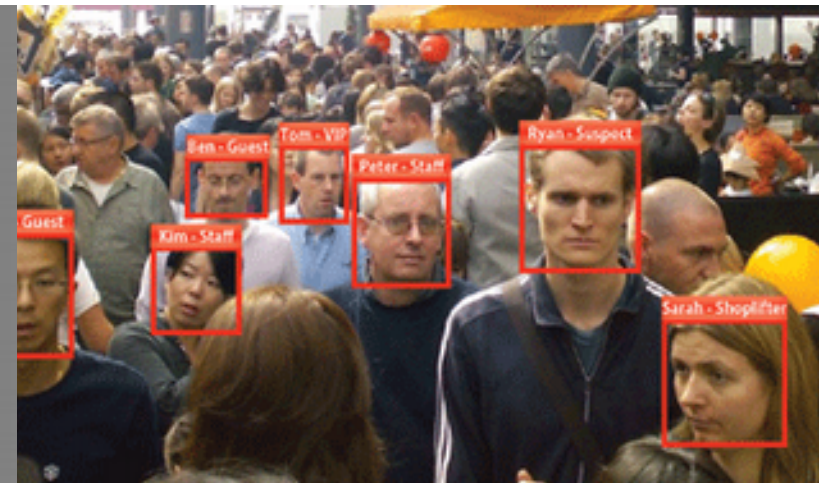
- misure relative a caratteristiche fisiche umane specifiche (uniche) per ogni individuo
- esempi: impronte digitali, DNA, volto, voce, andatura, distribuzione delle vene, iride, padiglione auricolare, ...



```
Happy : 49.24 %
Surprise : 0.11 %
Angry : 0.01 %
Disgust : 0.00 %
Fear : 0.50 %
Sad : 1.62 %

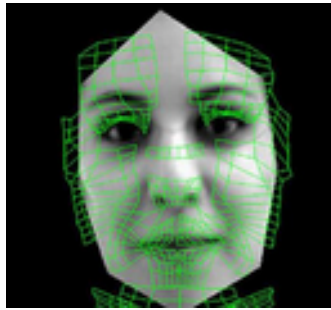
Status:
• Source: Picture
• Player: Playing
• Face: Tracking
• Markers: Loaded Existing

Hint:
Keep your face frontal
```



Come funziona l'identificazione biometrica?

- (1) ISCRIZIONE Dal volto (o dall'impronta, ecc) vengono estratti automaticamente tratti specifici (es. distanza tra punti particolari) che costituiscono una "firma" o "modello" univoci per una data persona
- (2) ARCHIVIAZIONE Questo "modello" univoco viene associato all'identità della persona da identificare
- (3) IDENTIFICAZIONE Ogni volta che il dispositivo incontra un volto con le stesse caratteristiche produce lo stesso "modello". Questo processo viene usato per identificare la persona o verificarne l'identità



Iscrizione
Enrolment

I

estrazione tratti
(*features*)
memorizzazione (*storage*)
del modello (*template*)

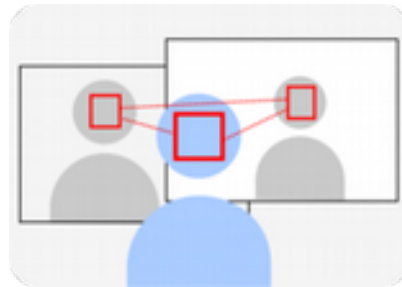


II

**associazione
di identità**



face matching
(abbinamento
di volti) anche
anonimi



verifica di identità
/autenticazione



identificazione



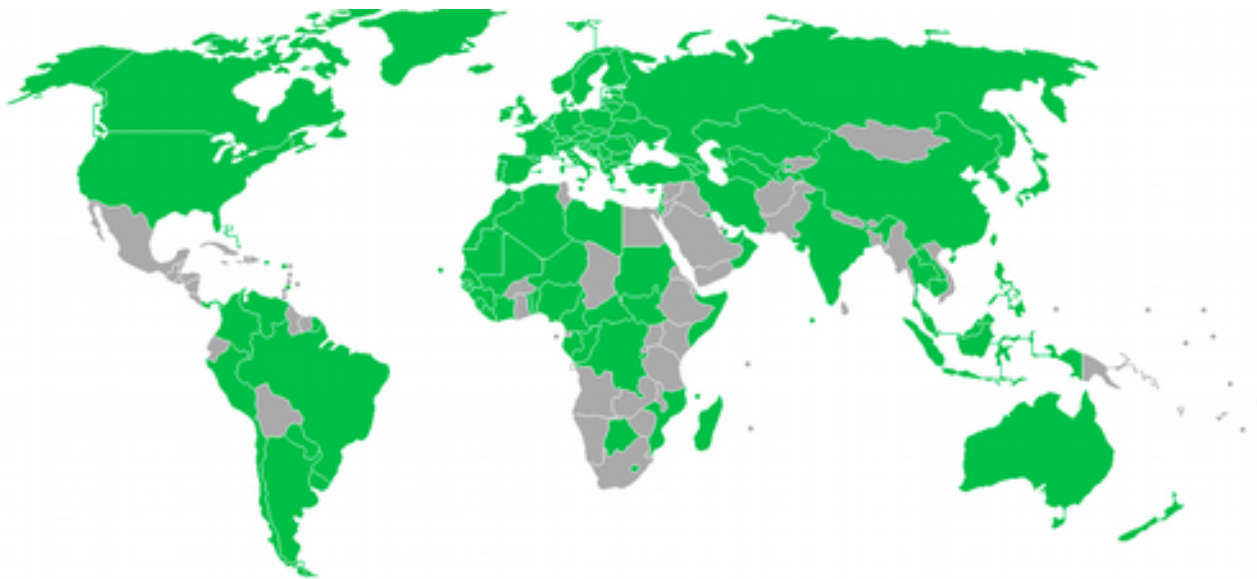
categorizzazione in base
a caratteristiche fisiche:
età, sesso, umore,
ma anche salute,
propensione al crimine
[**categorization/**
segregation]

Esempi

- Passaporto biometrico



- la foto della persona viene scansionata e il “modello” biometrico introdotta nel passaporto
- Il “modello” viene letto dal passaporto e confrontato con l’immagine di chi lo porta, che viene ammesso solo se combacia





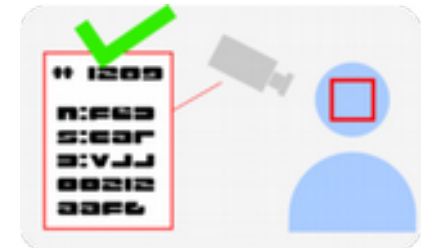
estrazione tratti
(*features*)
e memorizzazione del
modello (*template*)



associazione
di identità



verifica di identità



Sistema ADHAAR indiano:

- foto del volto, impronte delle 10 dita e scansione di due iridi + Dati anagrafici → Numero identificativo a 12 cifre (unique identification number – UID)
- Da uno o più dei dati biometrici si può risalire all'identità (dati biometrici multimodali)

What is AADHAAR?

Unique Identification Authority of India
Planning Commission, Government of India

"I've got my Aadhaar Number. I can tell you something about it."

What is Aadhaar?
A 12 digit Unique Identification Number, issued by Government of India.

Who can get Aadhaar?
All residents of India, including children, trans-genders and the differently-abled.

What are the benefits of Aadhaar?

- Aadhaar is valid all over India as a Proof of Identity and Proof of Address.
- Aadhaar can help you open a bank account, get a mobile connection and avail LPG.
- In future, you would be able to access other Government and non-Government services.

You can Enrol Anywhere in India | Aadhaar Enrolment is Free of Cost | You need to Enrol Only Once
www.uidai.gov.in

AADHAAR
Aam Aadmi Ka Adhikaar



Lotta alla doppia patente in USA

- Al momento della richiesta della patente posso fornire un nome che può essere falso, e una foto, che vengono archiviati.
- I titolari di patenti con lo stesso volto intestate a nomi diversi vengono identificati
 - Database biometrico FBI Next generation Identification: 1/2 popolazione USA schedata

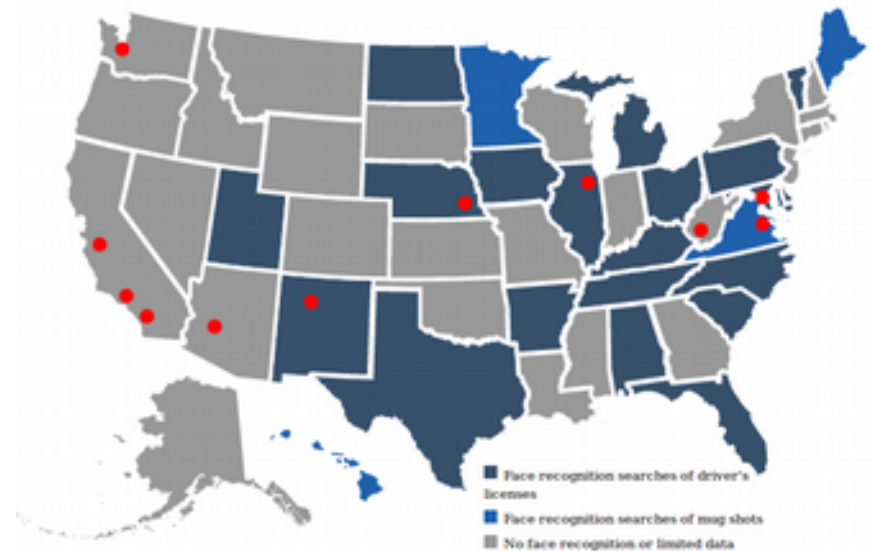


Figure 1: Law Enforcement Face Recognition Use By Jurisdiction

<https://www.perpetuallineup.org/>

Cina, gogna per i pedoni indisciplinati: se passi col rosso finisci sullo schermo

La tecnica del riconoscimento facciale consentirà alle autorità cinesi di sbattere il volto del trasgressore su uno schermo gigante. A essere puniti saranno i pedoni, soggetti a multa o a mini-corso sul codice della strada

di RAFFAELLA SCUDERI

21 giugno 2017

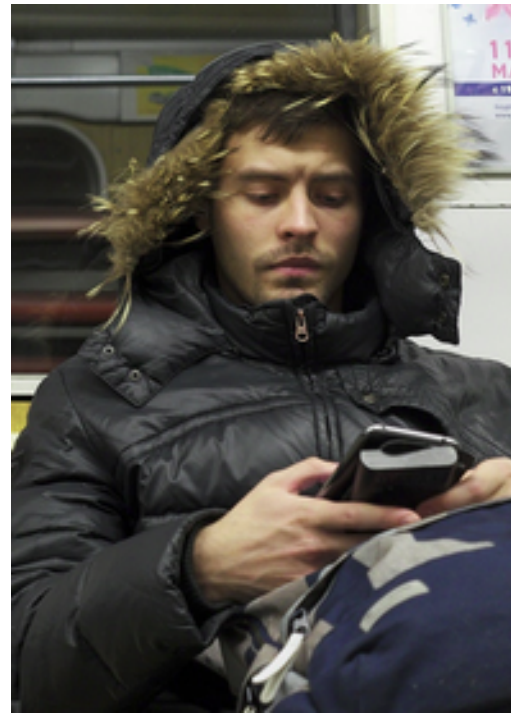
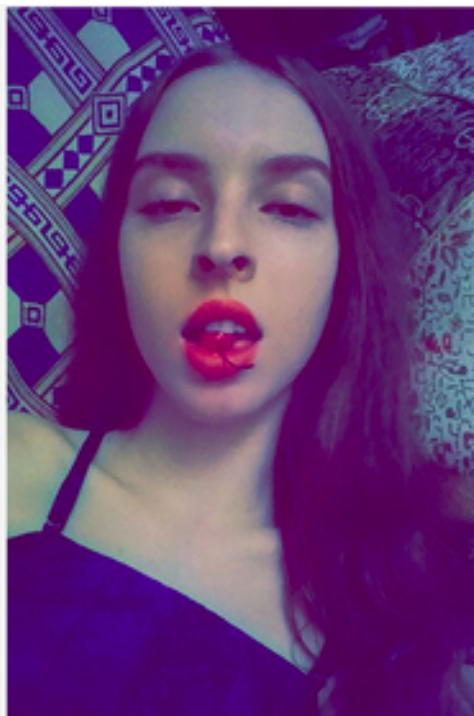
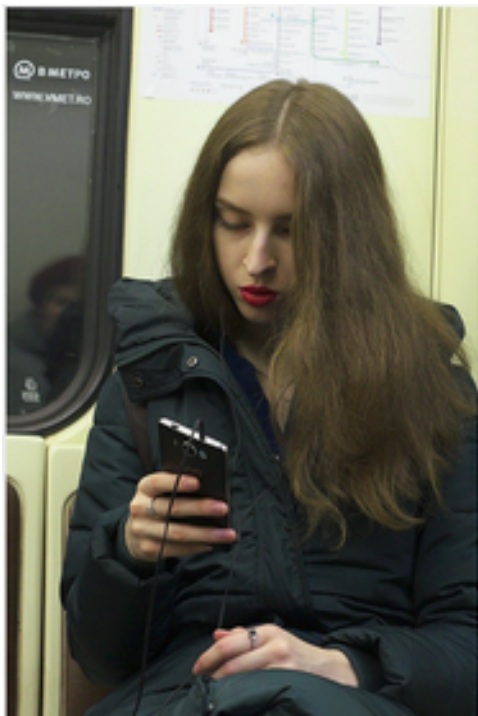


Rubano la carta igienica nelle toilette pubbliche, truffano ai bancomat, si intrufolano nei dormitori femminili dei college. E passano sulle strisce col rosso.

Verrà usata, entro fine giugno, una tecnica di riconoscimento facciale che in pochi secondi diffonderà la foto del malcapitato, con comparsa istantanea, su schermi a bordo strada. E non finisce qui. Verrà anche registrato un video di 15 secondi che mostrerà le immagini dell'infrazione commessa. Le foto scattate saranno comparate a quelle archiviate nel database della polizia assieme alle informazioni relative a documenti di identità e indirizzo. Ci vorranno solo venti minuti per identificare il contravventore. Le punizioni saranno tre: una multa di circa tre dollari, la frequenza obbligatoria di un mini corso di mezz'ora sul codice della strada o la collaborazione per venti minuti con la polizia municipale alla regolazione del traffico.

Reidentificazione da profilo “social” Vkontakte

motore di ricerca interno al SN associa la foto in upload al profilo social dell'interessato



(c) Yegor Tsvetkov

<https://birdinflight.com/ru/vdohnovenie/fotoproect/06042016-face-big-data.html>

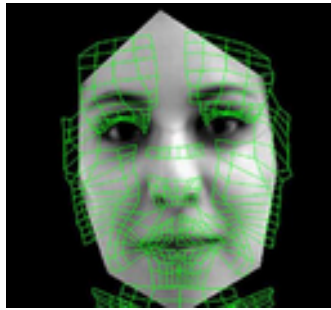
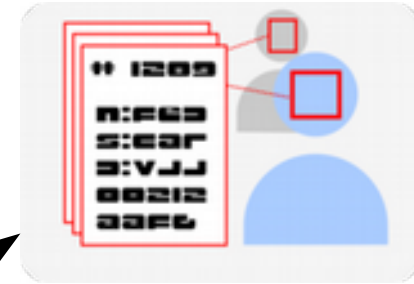
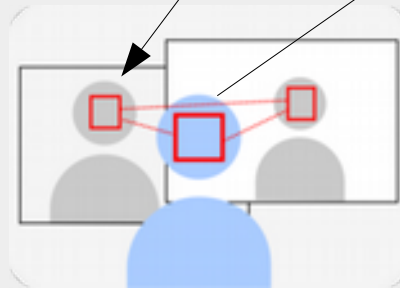


Foto del
profilo FB



nome dal
profilo FB,
tagging

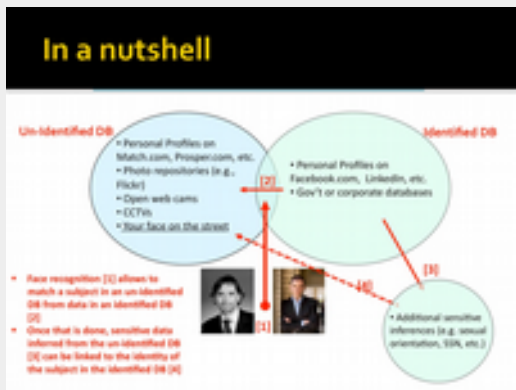
face matching
(tutte le foto in
Internet con la
stessa faccia)



verifica di identità



identificazione



re-identificazione: immagini anonime
possono essere collegate a profili
identificabili

Acquisti A, Gross R and Stutzman F (2011) Faces Of Facebook-Or, How The Largest Real ID Database In The World Came To Be. In: Blackhat 2011. Available from: <http://www.blackhat.com/html/bh-us-11/bh-us-11-archives.html#Acquisti>.

Acquisti A, Gross R and Stutzman F (2014) Face Recognition and Privacy in the Age of Augmented Reality. Journal of Privacy and Confidentiality 6(2). Available from: <http://repository.cmu.edu/jpc/vol6/iss2/1>.

Altri usi

- Indagini giudiziarie (telecamere)
- Visori AR real time (polizia)
- Riconoscimento di vittime (in caso di disastri)
- Sistemi di “timbratura” dipendenti (rilevazione presenze)
- Distributori automatici, sistemi di pagamento
- Insegne pubblicitarie

Rischi

- Privacy e democrazia: *rischio controllo sociale generalizzato* (Garante)
 - uso previsto (autorizzato) → uso esteso → abuso
 - *unauthorized secondary use* [Smith, Milberg, Burke 1996]
- Sicurezza e *furto di identità biometrica*: (data breach).
Se mi rubano la password posso cambiarla.
Se mi rubano la faccia non posso
- Il dato biometrico tende a rivelare altre informazioni, anche sensibili
- Falsificabile
- Difficile rispettare anonimato e pseudonimato: rischio reidentificazione a partire dal dato biometrico
(è come se avessi la stessa password ovunque)

Affidabilità

- Attualmente ~ 98% accuratezza (test *Labeled Faces in the Wild*)
- Problemi con gli algoritmi di riconoscimento biometrico:
 - falsi *negativi*: non riconosce la persona giusta
 - la serratura biometrica mi lascia fuori di casa
 - falsi *positivi*: riconosce la persona sbagliata
 - arresto per rapina erroneo, su suggerimento della AI (*)
 - *bias* (faziosità): algoritmi “razzisti” (**)
 - Il corpo cambia (invecchiamento, traumi...)
 - *spoofing*: sono ingannabili

(*) <https://theintercept.com/2016/10/13/how-a-facial-recognition-mismatch-can-ruin-your-life/>

(**) <https://www.technologyreview.com/s/601786/are-face-recognition-systems-accurate-depends-on-your-race/>

come ingannare il dispositivo biometrico?

- Fingerprint
 - 2014: impronte del ministro della difesa tedesco prese da una fotografia del polpastrello presa a distanza. Possono poi essere stampate.
- Voice recognition
 - Voice Impersonation via sintesi vocale (bastano pochi minuti di registrazione)
- Face recognition
 - foto al posto del volto
 - video impersonation
 - tecniche più raffinate che si basano su come funzionano le AI



UAB research finds automated voice imitation can fool humans and machines

by Katherine Stephen

September 25, 2015 | Print | Email

University of Alabama at Birmingham researchers have found that automated and human verification for voice-based user authentication systems are vulnerable to voice impersonation attacks. This new research is being presented at the European Symposium on Research in Computer Security, or ESORICS, today in Vienna, Austria.

Using an off-the-shelf voice-morphing tool, the researchers developed a voice impersonation attack to attempt to penetrate automated and human verification systems.

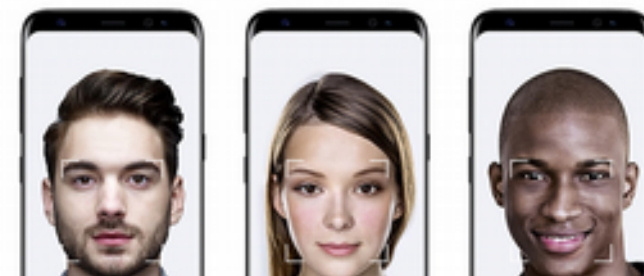
A person's voice is an integral



Galaxy S8 face recognition can be spoofed with an image

March 31, 2017 by Siddhanth — Leave a Comment

5 10 15 20 25 30 35 40 45 50 55 60 65 70 75 80 85 90 95 100



Police asked this 3D printing lab to recreate a dead man's fingers to unlock his phone



Rose Eveleth

7/21/16 7:45am • Filed to: REAL FUTURE



Accessorize to a Crime: Real and Stealthy Attacks on State-of-the-Art Face Recognition

Mahmood Sharif
Carnegie Mellon University
Pittsburgh, PA, USA
mahmoods@cmu.edu

Sruti Bhagavatula
Carnegie Mellon University
Pittsburgh, PA, USA
srutib@cmu.edu

Lujo Bauer
Carnegie Mellon University
Pittsburgh, PA, USA
lbauer@cmu.edu

Michael K. Reiter
University of North Carolina
Chapel Hill, NC, USA
reiter@cs.unc.edu

Sharif, M., Bhagavatula, S., Bauer, L., & Reiter, M.
Accessorize to a
Crime: Real and Stealthy Attacks on State-Of-The-Art
Face Recognition.
In Proc. CCS, 2016.
<<https://users.ece.cmu.edu/~mahmoods/publications/ccs16-adv-ml.pdf>>

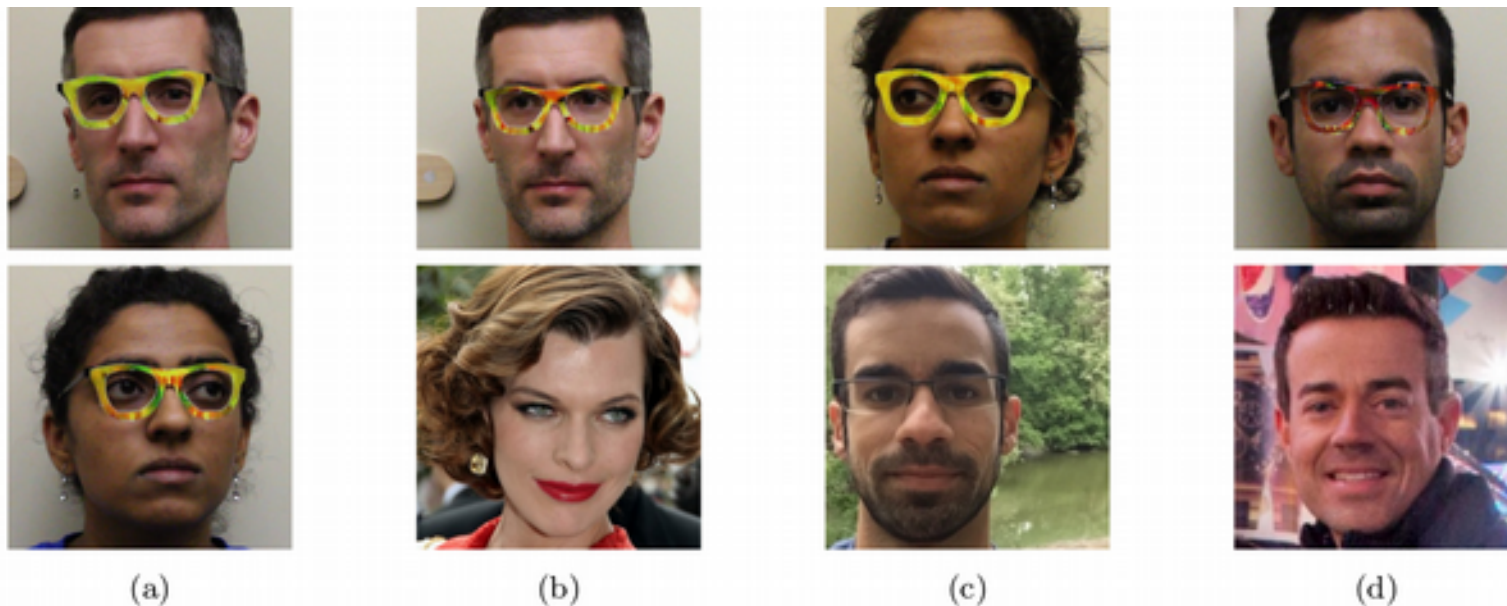
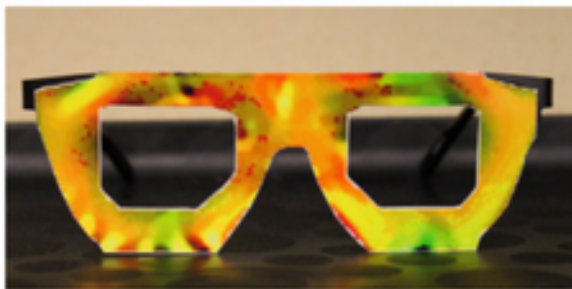


Figure 4: Examples of successful impersonation and dodging attacks. Fig. (a) shows S_A (top) and S_B (bottom) dodging against DNN_B . Fig. (b)–(d) show impersonations. Impersonators carrying out the attack are shown in the top row and corresponding impersonation targets in the bottom row. Fig. (b) shows S_A impersonating Milla Jovovich (by Georges Biard / CC BY-SA / cropped from <https://goo.gl/GlsWIC>); (c) S_B impersonating S_C ; and (d) S_C impersonating Carson Daly (by Anthony Quintano / CC BY / cropped from <https://goo.gl/VfnDct>).



6. EXTENSION TO BLACK-BOX MODELS

So far we have examined attacks where the adversary has access to the model she is trying to deceive. In general, previous work on fooling ML systems has assumed knowledge of the architecture of the system (see Sec. 2). In this section we demonstrate how similar attacks can be applied in a black-box scenario. In such a scenario, the adversary



GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

LINEE-GUIDA IN MATERIA DI RICONOSCIMENTO BIOMETRICO E FIRMA GRAFOMETRICA

Allegato A al Provvedimento del Garante del 12 novembre 2014

“I dati biometrici sono, per loro natura, direttamente e univocamente collegati all’individuo e denotano in generale un’intrinseca, universale e irreversibile relazione tra corpo e identità, per cui è necessario garantire **particolari cautele** in caso di trattamento.”

Obblighi e bilanciamento di interessi

trattati per le sole finalità legittime (nessun altro fine)

proporzionale (non dati esuberanti rispetto alle finalità)

Richiesti:

- cifratura, non centralizzazione (se possibile), registrazione degli accessi, memorizzazione per il tempo strettamente necessario
- consenso informato, revocabile
- verifica preliminare
- notificazione, comunicazione di violazione

Non richiesti nei casi in cui il Garante, con proprio specifico provvedimento, [...] abbia ritenuto prevalente il perseguimento di un legittimo interesse del titolare.

es. verifica preliminare non richiesta per

- controllo di accesso fisico ad aree “sensibili”
- controllo dell’identità per l’utilizzo di apparati e macchinari pericolosi.

Definizione del Garante

caratteristica biologica o comportamentale di un individuo da cui possono essere estratti in modo ripetibile dei *tratti biometrici* (biometric features) distintivi e idonei al riconoscimento biometrico

[ovvero] **riconoscimento** di individui basato su loro caratteristiche biologiche o comportamentali, *includendo in tale accezione le nozioni di verifica biometrica e di identificazione biometrica;*

GDPR

dati personali ottenuti da un **trattamento tecnico specifico** relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica *che ne consentono o confermano l'identificazione univoca*, quali l'immagine facciale o i dati dattiloscopici

Dispositivo tecnico specifico

- Di **identificazione**
 - *in questa foto si riconosce Tizio*
 - il dato biometrico viene usato per risalire all'identità
- Di **autenticazione**, o conferma di identità
 - *sei veramente tu, Tizio?*
 - il dato biometrico viene usato come credenziale di accesso

per GDPR una foto è un dato sensibile?

- Dipende:

Recital 51: “Il trattamento di fotografie non dovrebbe costituire sistematicamente un trattamento di categorie particolari di dati personali, poiché esse rientrano nella definizione di **dati biometrici** *soltanto quando [...] trattate attraverso un **dispositivo tecnico specifico** che consente **l'identificazione univoca o l'autenticazione di una persona fisica.**”*

Recital 26 :

- Il regolamento non si applica al trattamento di **informazioni anonime** [...].
- I dati personali sottoposti a **pseudonimizzazione**, i quali potrebbero essere attribuiti a una persona fisica mediante l'utilizzo di ulteriori informazioni, dovrebbero essere considerati informazioni su una persona fisica identificabile.

Trattamento di categorie particolari di dati personali

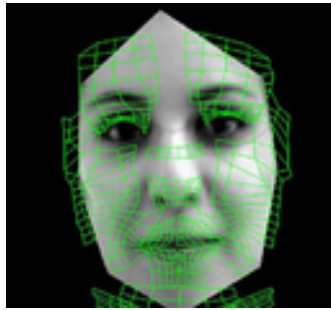
- Art 9.1

È **vietato** trattare dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, **dati biometrici** *intesi a (*) identificare in modo univoco una persona fisica*, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.

(*) “*for the purpose of*” : allo scopo di

Trattamento consentito se (9.2)

- a) l'interessato ha prestato il proprio **consenso esplicito** (purchè possa farlo)
- b) è **necessario** per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale
- c) è necessario per **tutelare un interesse vitale dell'interessato**
- d) per organizzazioni e associazioni politiche nei confronti dei **soci**
- e) il trattamento riguarda **dati personali resi manifestamente pubblici** dall'interessato
- f) accertare, esercitare o difendere un diritto in **sede giudiziaria**
- g) per motivi di **interesse pubblico rilevante** sulla base del diritto UE o statale
- h) per finalità di **medicina preventiva** o di medicina del **lavoro**, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale (sotto la responsabilità di un professionista soggetto al segreto professionale – Art 9.3)
- i) per motivi di interesse pubblico nel settore della **sanità pubblica**,
- j) a fini di archiviazione nel pubblico interesse, di **ricerca** scientifica o storica o a fini statistici

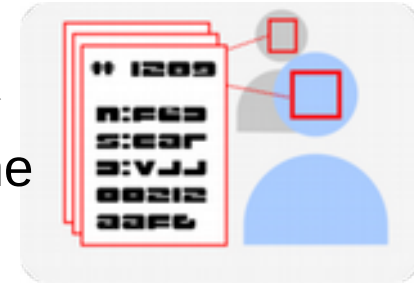


Iscrizione

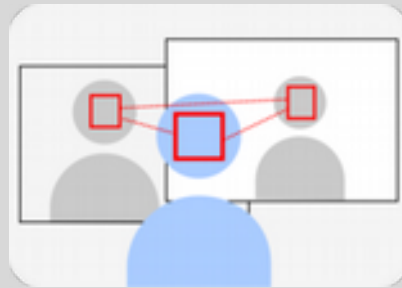
estrazione tratti e
memorizzazione del
modello



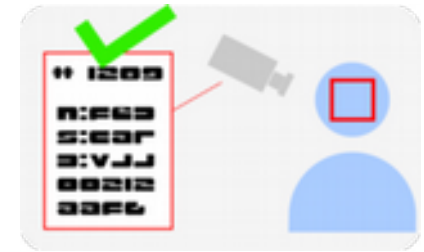
associazione
di identità



abbinamento
e
categorizzazione



verifica di identità



identificazione



Zona grigia

Scenari /1

Foto conferite volontariamente a un SN possono essere usate attraverso un dispositivo tecnico con lo scopo di identificare o autenticare?

No, a meno che il soggetto non abbia prestato espresso consenso, e se le leggi nazionali lo consentono.

Possono essere aggregate e categorizzate?

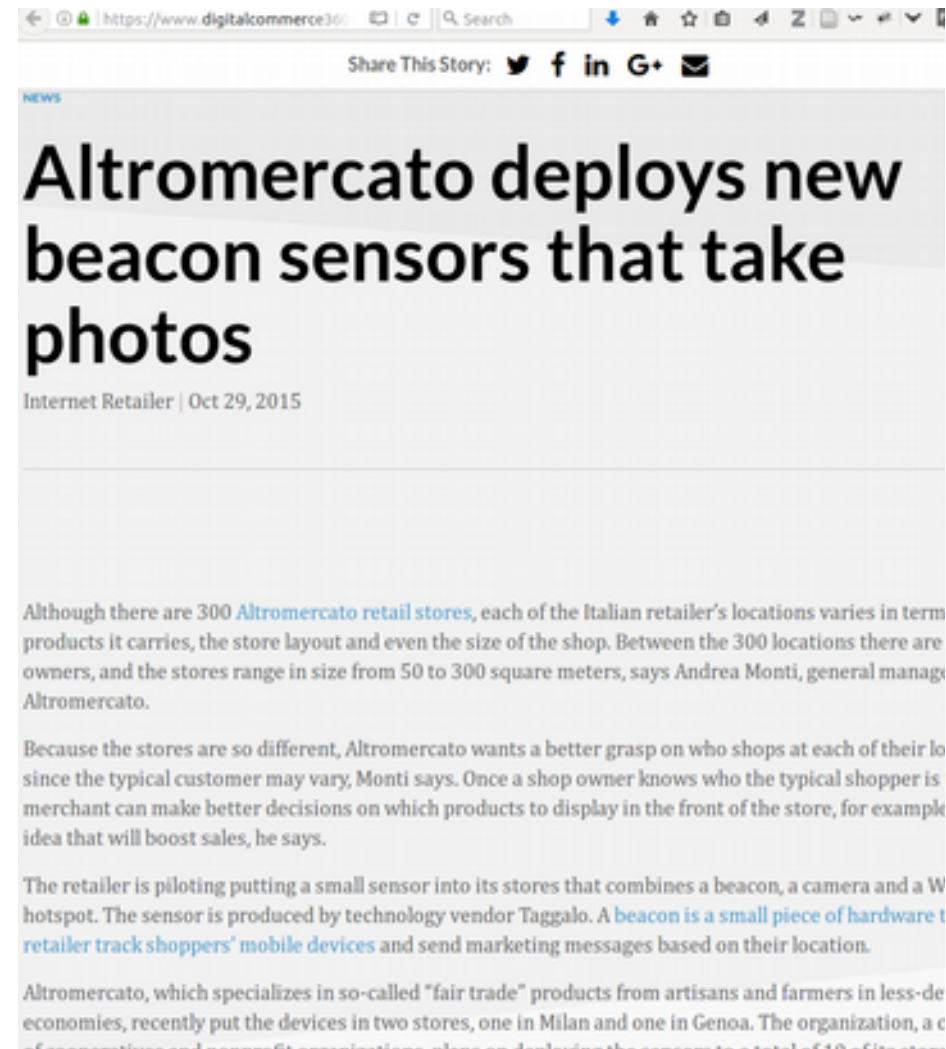
Scenari/2

- Riprese all'interno di un negozio *senza identificazione*, ma con riconoscimento da parte del dispositivo tecnico per tracciare i percorsi dei clienti.
- Ripresa da una vetrina ai passanti nella pubblica via, conservando dati per verificare se ritornano.
- Idem dal cartello pubblicitario

Ammesso di non accedere in nessun modo all'identità del soggetto nemmeno in tempi successivi, trattasi di indentificazione o no?

E se viene registrato anche SSID wi-fi?

Le immagini sono anonime ma vi è distinzione di ogni identità dalle altre, e potenziale reidentificazione...



Scenari/3

- Fotografo manifestanti sulla pubblica via senza identificarli e aggrego le presenze
- Offro un servizio di motore di riconoscimento facciale (senza identificazione dell'interessato) che dato un volto in upload restituisce il link alle sole immagini pubbliche

Opt-out

- manca completamente la possibilità tecnica e giuridica di un **opt-out preventivo** all'arruolamento involontario e successive re-identificazioni
- tagMeNot:
una proposta per sollevare il problema



Consapevolezza

- Manca completamente la consapevolezza che ogni foto pubblicata in Internet, magari corredata di informazioni anagrafiche consente reidentificazione anche sulla pubblica via
- Forte asimmetria informativa ($\rightarrow$ potere) in mano a chi può compiere il match: può sapere cose che l'interessato stesso non sa

Grazie

alberto  cammozzo.com

 @dontTag