PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 20 - numero 4235 di Lunedì 14 maggio 2018

Il confronto delle impronte digitali: sembra facile!

I lettori che osservano con frequenza le trasmissioni televisive, che fanno riferimento a contesti criminosi, hanno certamente rilevato come il confronto delle impronte digitali avvenga in pochi secondi e con estrema accuratezza. La realtà è molto diversa

Molti lettori sono professionisti della security, che debbono avere una conoscenza almeno elementare del comportamento sulla scena del crimine e di altri aspetti afferenti alle attività di indagine, a fronte del verificarsi di un atto delittuoso.

Orbene, appare chiaro che l'analisi delle impronte digitali rappresenti un aspetto fondamentale in queste tecniche di indagine ed ecco la ragione per la quale ho deciso di mettere a disposizione dei lettori un documento, sviluppato nell'ambito di un progetto di ricerca dell'Università della California, che mette in evidenza come vi siano molti miti da sfatare, su questo argomento.

L'opportunità di questo intervento nasce anche dal fatto che ho avuto modo di intervistare alcuni colleghi e ho visto che le idee sul tema hanno certamente bisogno di un approfondimento.

I professionisti del settore criminologico sanno bene che il confronto di impronte latenti può essere un processo piuttosto complesso con variazioni notevoli, in relazione al grado di difficoltà presente nell'effettuare specifici confronti.

Ecco perché l'Università della California ha ritenuto opportuno sviluppare un documento, che ha stabilito una metodologia scientifica per dare un valore quantitativo all'accuratezza ed al rateo di errori di questi fondamentali elementi probatori, soprattutto nell'ambito della identificazione di impronte latenti.

Pubblicità
<#? QUI-PUBBLICITA-MIM-[SWGDPR] ?#>

I ricercatori hanno lavorato sodo per diverso tempo, cercando di mettere a punto una strategia obbiettiva, che potesse essere strumentale nel determinare il livello di accuratezza.

Gli esaminatori hanno messo a confronto delle impronte e si sono posti delle domande in relazione alla origine delle impronte, alla difficoltà del confronto, al livello di fiducia negli esiti del confronto.

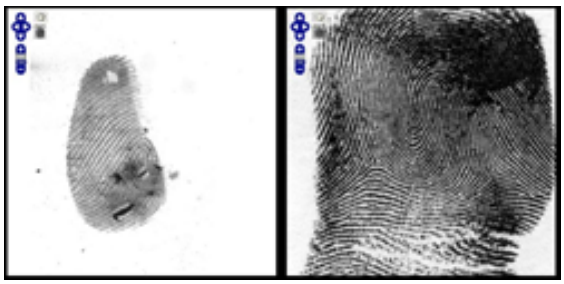

Foto fornita da NIJ

In particolare, i ricercatori hanno cercato di definire i fattori coinvolti su vari aspetti del confronto delle analisi, associando ogni fattore ad un grado di difficoltà e collegando quindi il rateo di difficoltà di vari fattori, in maniera da poter avere un valore numerico della probabilità di errore.

I ricercatori si sono accorti che vi possono essere differenze straordinarie nella affidabilità dei confronti tra impronte latenti e che il rateo di errore è una diretta funzione della difficoltà di confronto.

Dal momento che il rateo di errore può essere collegato alla difficoltà del confronto, può essere fuorviante cercare di individuare un fattore generalizzate per individuare il livello di errore nel confronto.

Attualmente, il confronto tra impronte digitali latenti è fatto da esperti, e ci si è quindi chiesto fino a che punto questi esperti sono in grado di valutare la difficoltà del confronto.

Ad esempio, ci si è posta la domanda: questi esperti possono valutare la difficoltà di un confronto?

Una domanda connessa discende dal fatto che gli esaminatori possono giudicare la difficoltà di un confronto in una maniera obiettiva, vale a dire mediante parametri che possono essere condivisi da tutta la famiglia degli esaminatori.

Ecco perché i ricercatori hanno affrontato in maniera leggermente diversa il problema, attraverso un approccio psicologico chiamato meta cognizione, vale a dire la capacità di un individuo di valutare il proprio livello di abilità.

Per sviluppare questa gerarchia di difficoltà di confronto delle impronte latenti, i ricercatori hanno creato un database con 104 impronte digitali. Ogni impronta è stata catturata dapprima utilizzando inchiostro, come normalmente avviene nei commissariati di polizia, per avere una stampa la più nitida possibile.

Indi la persona, di cui era stata catturata l'impronta digitale, è stata invitata a toccare varie superfici, in maniera da creare una serie di impronte latenti, tipiche dello scenario che si incontra sulla scena del crimine.

Le impronte latenti sono state catturate con tecniche convenzionali, utilizzando le specifiche polveri, e quindi scannerizzate con un sistema informatico.

A questo punto i ricercatori hanno creato un database di impronte latenti e di impronte rilevate con inchiostro, chiedendo ad un gruppo di esperti di effettuare dei confronti.

Complessivamente, gli esperti sono stati in grado di accoppiare correttamente le impronte nel 91% dei casi.

In particolare, gli esperti, che però erano stati debitamente sensibilizzati, prestavano particolare attenzione a possibili fattori che potessero alterare le loro valutazioni.

Questa indagine ha quindi messo in evidenza, con metodi oggettivi, che vi sono fattori che possono influenzare in maniera significativa la difficoltà del confronto e quindi la possibilità che si verifichino degli errori.

Ecco perché, ad avviso dei ricercatori, bisognerebbe che gli esperti, che vengono chiamati in causa, quando si devono effettuare confronti tra impronte latenti ed impronte catturate ad esempio direttamente dalle dita di soggetti sospettati, introducessero un fattore di probabilità di accuratezza, oppure di probabilità di errore, in modo che le giurie, coinvolte nella valutazione complessiva della situazione, abbiano a disposizione un ulteriore elemento di valutazione.

Ciò significa che anche sistemi automatici attuali di confronto, i cosiddetti AFIS-automatic fingerprint identification system, dovrebbero attribuire un coefficiente di probabilità ad eventuali accoppiamenti, che vengono presentati all'esperto.

Per i lettori che desiderano approfondire questo importantissimo tema, metto a disposizione l'intero documento, sviluppato dagli esperti universitari (PDF)

Adalberto Biasiotti

Questo articolo è pubblicato sotto una Licenza Creative Commons.

I contenuti presenti sul sito PuntoSicuro non possono essere utilizzati al fine di addestrare sistemi di intelligenza artificiale.
