POLITECNICO DI TORINO

Collegio di Ingegneria Gestionale
Corso di Laurea Magistrale in Ingegneria Gestionale
A.a. 2020/2021
Sessione di Laurea Dicembre 2021

Studio delle dinamiche dell'innovazione nel campo della biometria

Relatore:
Prof. Marco Cantamessa

Candidato:
Davide Bergamasco
279801

RINGRAZIAMENTI

Prima di procedere con l'elaborato vorrei ringraziare alcune persone che mi hanno accompagnato in questo percorso di laurea.

Innanzitutto vorrei esprimere gratitudine verso il prof. Marco Cantamessa che mi ha permesso di portare avanti il progetto di laurea specialmente in questo nuovo campo. Interesse verso lo studio dell'innovazione nato proprio grazie alle sue lezioni.

In seguito non potrei non ringraziare i miei genitori che mi hanno infuso, con i loro progetti imprenditoriali, la voglia di dare il massimo spingendosi sempre oltre il limite personale.
Purtroppo non sono né un informatico (mi spiace mamma) né un ingegnere civile (mi spiace papà), ma comunque vi siete beccati un bel gestionale. Vi voglio bene!

Altra persona verso cui rendere gratitudine è Giulia, che grazie alla sua pazienza ha saputo sopportarmi anche durante i periodi di esami e relativi progetti (saremo in due a sognarli), confortandomi anche nei momenti più difficili ("*la vita è una scalata, ma la vista è stupenda*"). Sappiamo bene che gli ingegneri non sono brave persone (in realtà siamo perfetti nella nostra imperfezione) ma neanche troppo lo si può dire dei giuristi. Chissà dove ci porterà il tempo, passo dopo passo si può far tutto perché i brutti momenti prima o poi passeranno, ma i belli rimarranno. Tanto sappiamo bene che saremo sempre due bambini folli.

Come potrei non ringraziare anche Oscar che, sin dai primi giorni del mio percorso scolastico, ha saputo sempre farmi divertire oltre che tenermi concentrato sul lavoro che stavo portando avanti. Chissà se risuonano ancora le parole "no Oscar, non si fa", chissà se in tutti questi anni sono state metaforicamente rigirate per non farmi distrare e rimanere sempre focalizzato sull'obiettivo.

Grazie anche per tutto il supporto morale ricevuto da tutto il gruppo di Bordighera e dai nuovi "+1" che oramai fanno parte del team (Fabio, Luca, Aurora, Daniele, Alessia, Letizia, Giorgio, Debora, Barbara, Martina e Gioele). Siamo il gruppo delle passeggiate notturne lunghe chilometri fino alla disperazione, dei tour nelle vigne, delle sagre in giro nel Piemonte, delle conoscenze sui vini, delle esperienze di arrampicata notturna sugli alberi, delle foto turistiche nel luogo da noi tanto amato, ... In sostanza siamo tante cose, ma sicuramente si può definire come la mia seconda famiglia.

Voglio anche citare il gruppo "Poli-building" (Andrea, Simone e William) che mi ha sopportato lungo tutti questi anni di progetti. Vi ricorderete sempre della mia ossessione negli Excel.

Per ultimo ringrazio me stesso per non aver mai mollato, anche quando la montagna degli esami sembrava insormontabile. Sembra impossibile, ma ce l'ho fatta.

Questo lavoro lo dedico a tutti voi che mi avete accompagnato nel mio percorso di crescita. Chissà la vita cosa ha in serbo per me, ma sicuramente manterrò la promessa fatta con te.

INTRODUZIONE

Il presente elaborato è stato scritto con l'intenzione di far luce sulla tematica riguardante l'innovazione tecnologica. Nell'analisi più dettagliata si è cercato di procedere all'illustrazione di come questa si evolva nel tempo, studiandone, quindi, le dinamiche.
Il caso di studio preso in considerazione fa riferimento alla biometria nel campo della sicurezza dell'identità dell'utente finale. In particolare vengono identificate diverse tecnologie e, grazie a specifici database, si suddividono i vari finanziamenti ricevuti dalle aziende in diversi campi applicativi. Tutto questo con la finalità di andare a capire in quale direzione stia andando il mercato, per studiare in quali campi potrebbe emergere la figura del dominant design.

Nel primo capitolo viene presentata la teoria posta alla base dell'elaborato, in cui si parte dall'esposizione dell'evoluzione che ha subito il concetto di dominant design, partendo dai primi elaborati di Abernathy e Utterback del 1975 per approdare, infine, agli anni più recenti.
In secondo luogo sono esposte le varie caratteristiche che vanno a comporre l'architettura dominante, tra cui i motivi di selezione e di stabilità.
Nella parte conclusiva di questa prima parte della trattazione, si vanno ad introdurre le varie critiche che sono state fatte ai modelli precedentemente presentati, specialmente a quello di Abernathy e Utterback. Tra queste valutazioni si evidenzia la presenza di un evento trigger, con successivo periodo di incubazione, l'integrazione dell'organizzazione, la modularità e la questione relativa ai campi applicativi per l'emersione del dominant design.

Nel secondo capitolo si prosegue con la presentazione delle varie tecnologie biometriche, che nella fattispecie sono: riconoscimento dell'impronta digitale, riconoscimento dell'iride, riconoscimento della retina, riconoscimento del battito, riconoscimento della geometria della mano, riconoscimento delle vene della mano, riconoscimento facciale, riconoscimento della camminata, riconoscimento della firma-scrittura e riconoscimento del comportamento digitale. Questo con l'ottica di andare a visionare le modalità di funzionamento e le relative caratteristiche proprie di ciascun metodo di riconoscimento, con relativi vantaggi e svantaggi, sia attuali sia futuri.
Proprio collegandosi a questo aspetto legato alla possibile mutazione ed evoluzione temporale della tecnologia in questione, si mette anche in atto un ragionamento che nasce con un'ottica legata al come si stia procedendo nella ricerca, studiando quali fattori avranno ancora speranza di esistere nei prossimi anni e quali invece saranno destinati a scomparire, essendo soppiantati da una loro versione più evoluta, legata alla loro stessa natura.

Nel terzo capitolo, il cosiddetto cuore dell'elaborato, si procede con l'analisi dell'andamento annuale dei finanziamenti operati sulle varie tecnologie precedentemente esposte, finanziamenti che sono stati percepiti dalle varie aziende che operano nel settore e che sono state qui prese in considerazione. La metodologia presente ad inizio capitolo va ad analizzare più nel dettaglio quali siano le modalità di ricerca che sono state seguite per poter comporre il seguente elaborato.
Successivamente vengono approfondite le applicazioni con esempi concreti di aziende che a questo si dedicano ed eventuali novità che potrebbero insorgere nel mercato di riferimento. In parallelo,

viene presentata anche un'analisi dei relativi brevetti, ma con focus unicamente per tecnologia biometrica, non considerando perciò anche le applicazioni, in quanto i risultati di una ricerca possono essere facilmente ampliati su altri campi applicativi.
In conclusione, sia per i finanziamenti sia per i brevetti, viene analizzato l'indice di Gini, che si prefigge come compito quello di studiare il livello di concentrazione presente nel settore.

INDICE

LISTA DELLE FIGURE

LISTA DELLE TABELLE

1. LA TEORIA DEL DOMINANT DESIGN

1.1 Evoluzione teorica del dominant design

Nell'ambito che ricomprende lo studio delle dinamiche dell'innovazione, viene analizzato l'evolversi della tecnologia, affrontando l'analisi della sua dinamicità nel tempo.
Per effettuare queste considerazioni, esistono due possibili modelli: **Rogers-Moore** e **Abernathy-Utterback**.
Il primo modello si concentra sulle vendite nel tempo, suddividendo il mercato della tecnologia in fasce distinte:

- ***Innovators*** (circa il 2%): in questa fascia sono racchiuse tutte quelle persone che si sono rivelate entusiaste della tecnologia in questione, e che per questo sono state impressionate in particolar modo dalle sue nuove funzionalità. Grazie a quest'ultima caratteristica, i soggetti presi in considerazione non temono che la tecnologia possa diventare obsoleta, ponendo la base del loro interesse anche sui bassi costi di switching (ossia i costi che un utente affronta quando deve cambiare tecnologia).

- ***Early Adopters*** (circa il 14%): sono tutti quei soggetti che sono interessati all'esperienza permessa dalla tecnologia di riferimento, pur non essendo disposti, come invece lo sono i soggetti appartenenti alla fascia degli innovators, a mettersi in gioco verso bassi livelli di maturità. Sono persone, però, ben disposte ad aiutare l'azienda nel suo processo di miglioramento, tramite soprattutto la tecnica del passaparola (che spesso e volentieri si rivela molto funzionale).

- ***Early majority*** (circa il 34%): utenti che basano le loro scelte sulla base di un trade off, fondato sulla correlazione costi-benefici, anche se non si troveranno mai ad adottare una tecnologia che ha performance che gli stessi non ritengono sufficienti. Proprio a causa di ciò, se ritengono che le loro esigenze non siano state soddisfatte, non adotteranno la tecnologia, poiché non corrisponde ad opportune valutazioni legate a usabilità, costi e dismissione del prodotto.
  Passaggio importante tra Early Adopters e Early majority è il cosiddetto "*Chasm"*, il quale rappresenta il successo ricevuto dalla tecnologia in quanto le vendite andranno via via ad aumentare e non a decrescere drasticamente.

- ***Late Majority*** (circa il 34%): racchiude tutte quelle persone che sono avverse al rischio, non possiedono una spinta innovativa e attendono, quindi, che il prodotto raggiunga un livello di mercato molto consistente, diventando così principale.

- ***Laggars*** (circa il 16%): sono quegli utenti che hanno una preferenza per i beni convenzionali, rifiutano propriamente un passaggio ai beni innovativi e che quindi hanno altissimi costi di switching.

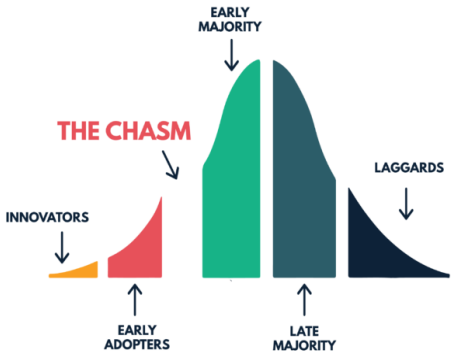


Figura 1: Modello di Rogers-Moore

Il secondo modello, cioè di **Abernathy-Utterback**, è quello che ci interessa maggiormente, in quanto va ad analizzare il concetto di "*Dominant Design*"" che è alla base del presente elaborato.

Il concetto di Dominant Design, che deriva dall'inglese ed è tranquillamente traducibile con "design dominante", fu utilizzato per la prima volta dal professore William J. Abernathy presso l'università di Harvard e dal professore James M. Utterback, docente di innovazione tecnologica e di management strategico presso MIT Sloan School of Management.
I due professori inserirono il termine "dominant design" in uno dei loro primi elaborati, venuto alla luce nel 1975 con il titolo "*A Dynamic Model of Process and Product Innovation*".
I due studiosi collaborarono per comprendere, attraverso dei modelli, gli effetti dell'innovazione in un settore generico. Questi erano legati alla strategia dell'azienda e alle caratteristiche del processo produttivo.
Stimarono inoltre che, in base a diversi fattori (fase di sviluppo del processo produttivo, tecnologia del prodotto e strategia aziendale), l'innovazione assumeva diverse caratteristiche, che mutavano nel tempo.

In tale lavoro diedero una definizione precisa di cosa si debba intendere quando si parla di design dominante, definito come quell'insieme di caratteristiche tecnologiche che diventano, essenzialmente, uno standard per il mercato. È necessario che a questo standard si adeguino i competitors, per poter così rimanere attivi nel settore di riferimento.

A questo punto della trattazione, però, è opportuno che si faccia una distinzione tra il concetto di standard (tecnico) e il concetto di design dominante. É da sottolineare, infatti, come non sempre le due accezioni coincidano, dal momento che per il primo si fa riferimento ad un set di specifiche che fornisce valore al prodotto a causa della conformità allo stesso, mentre con dominant design si intende un'intera architettura (riguardante sia l'aspetto fisico sia tecnico) e non un set di specifiche.

Ciò che emerge da questo quadro da loro tracciato è che le caratteristiche proprie del processo produttivo sono variabili, dipendendo sia dalla fase di sviluppo in cui ci si trova sia dalla tecnologia del prodotto. Entrambe queste componenti, comunque, sono determinate dalla strategia adottata dall'azienda, che mira sempre e comunque ad essere più competitiva nel mercato e a crescere economicamente.
Inizialmente non furono considerati diversi aspetti dell'innovazione nelle sue varie forme, e infatti il modello si riferiva solamente all'industria di produzione di prodotti assemblati, escludendo quindi l'industria di processo o di servizi. L'evolversi della tecnologia e del sistema economico rendono questo modello criticabile e obsoleto sotto molteplici aspetti, considerato che non prende in considerazione diverse caratteristiche che non possono più essere ignorate in un'ottica di sopravvivenza sul lungo periodo.

Meriti di questo metodo però non mancano, poiché è grazie ad esso che vennero cambiate le impostazioni di studio delle dinamiche dell'innovazione. Prima della sua introduzione, infatti, questi studi erano prevalentemente descrittivi, ponendo l'accento sui trend evolutivi, ma solo in misura superficiale, senza approfondire le cause e gli andamenti delle loro variazioni.

L'idea di fondo su cui si basa il concetto appena esposto è quella per cui lo sviluppo del prodotto avviene in diversi periodi temporali, arrivando ad avere performance sempre più elevate, in quanto aumenta il tasso di innovazione (assimilabile al numero di brevetti sviluppati negli anni), il numero di aziende, le vendite, il capitale, la produzione e la qualità.
Il modello non utilizza inevitabilmente l'azienda come metro di giudizio, ma propriamente il processo produttivo alla base, andando a studiare le sue caratteristiche e la sua evoluzione nel tempo.
Si vanno quindi ad identificare precisamente tre fasi di sviluppo, che possono essere riscontrate in diversi settori:

- **Fase fluida**: fase in cui i livelli di performance sono tendenzialmente bassi lungo questo "periodo", anche se ci sono dei fattori (numero di aziende e numero dei brevetti) che tendono a crescere con un andamento maggiore, e di conseguenza più apprezzabile di altri. In particolare, qui vi saranno molte aziende concorrenti che proporranno diversi design, magari dello stesso prodotto, e in cui vi sarà un alto investimento in innovazione riferita più propriamente al prodotto. Proprio per questo non vi è una certa stabilità all'interno del mercato, che vediamo non essere definito, e non ci sono prodotti standardizzati, non essendoci ancora dei processi di produzione ben configurati.
  L'innovazione è principalmente guidata o stimolata da sempre più moderni bisogni del mercato e, per avere successo, bisogna descrivere in primis accuratamente i requisiti del prodotto, piuttosto che passare subito a esporre le sue performance, più legate agli sviluppi scientifici o tecnologici.

- **Fase di transizione**: Fase in cui i livelli di performance si alzano sempre di più, essendosi manifestata l'esistenza di un dominant design, cioè l'apprezzamento all'interno del mercato

solo di alcuni prodotti particolari. Si inizierà anche a manifestare maggiormente una concorrenza legata al prezzo e delle nozioni legate alla routine aziendale.
Le aziende quindi si concentreranno sulle proprie competenze poste alla base di questa nuova tecnologia. Il numero di queste aziende andrà via via a diminuire, vi sarà un fenomeno chiamato "*shake out*", e, chi riuscirà ad allinearsi a questa nuova architettura di prodotto che ha trovato maggior favore da parte del mercato, riuscirà a continuare ad essere presente e competitiva sul mercato di riferimento. In caso contrario, devierà su altri business oppure andrà a competere in una nicchia specifica di mercato.

- **Fase specifica**: fase che sarà dedicata principalmente a migliorare i processi di produzione. Fattore determinante in questo procedimento, quindi, sarà l'aumento del numero dei brevetti legati soprattutto al processo, andando così ad abbattere lo scoglio dei costi di produzione. Questo perché non servirà più brevettare verso il prodotto, essendosi già manifestata un'architettura dominante. Questo porterà sempre di più le aziende a concorrere a livello di prezzo, mantenendo, se possibile, lo stesso margine.
  Si avrà quindi tendenzialmente la creazione di un oligopolio, in cui efficienza ed economie di scala faranno da padrone.

L'idea che sta alla base dello studio dell'innovazione di un prodotto nel tempo è l'invenzione strategica dell'inventore stesso, legata inizialmente alle performance (Performance maximizing) e in un secondo momento guarderà alle altre due componenti, ossia le vendite (Sales maximizing) e i costi (Cost minimizing). Questi tre fattori rappresentano, rispettivamente, le tre fasi sopra elencate.

Quindi, sostanzialmente, prima del manifestarsi del dominant design ci si troverà ad agire in un contesto in cui è presente un maggior numero di aziende, un maggior numero di variazioni legate al design, e una maggiore semplicità nell'ingresso sul mercato di nuove imprese. In questa area saranno maggiori le occasioni di successo di un'azienda in quanto si è davanti ad un ampio spettro di possibilità, a fronte però di un numero non minimo di rischi, dati soprattutto dall'alto grado di competizione che, in caso di "sconfitta", renderebbero gli investimenti spesi dei costi affondati.
In seguito all'affermazione dell'architettura dominante si andrà man mano riducendo il numero di competitors, poiché, avendo un design praticamente definito, ci saranno barriere all'ingresso del mercato del prodotto di riferimento, maggiori possibilità di successo con pochi rischi (ormai è già praticamente tutto definito) e competizione basata su costo/qualità.

A seconda della fase di sviluppo del processo e della strategia, l'innovazione di processo e l'innovazione di prodotto possono essere riassunti nel seguente grafico:

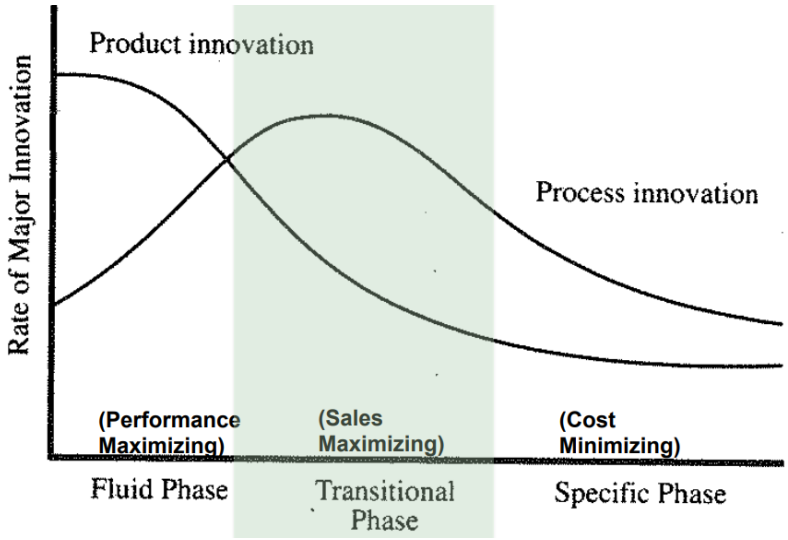


Figura 2: Rappresentazione delle diverse innovazioni

Dopo il successo del primo elaborato, Abernathy e Utterback ne redassero un altro, intitolato "*Patterns of Industrial Innovation*", in cui concentrarono le loro ricerche sullo studio dell'evoluzione di diversi settori produttivi (lampadine a incandescenza, carta, acciaio, motori a combustione interna) che avevano come caratteristica particolare quella di possedere un alto volume di produzione, un mercato target ben definito, una tecnologia efficiente e ben consolidata, bassi margini unitari e una competizione basata soprattutto sul prezzo.

La considerazione finale dello studio, che all'epoca sembrava tanto rivoluzionaria ma che al giorno d'oggi è abbastanza scontata, portava ad affermare che non vi fosse una sola e unica tipologia di innovazione, cioè quella radicale, ma che in realtà ve ne fosse anche un'altra. Grazie alle loro analisi si notò che l'innovazione poteva anche comprendere delle migliorie locali, come quegli sviluppi legati ai prodotti e/o processi già esistenti, senza quindi andare a creare nuovi paradigmi tecnologici, ma migliorando piuttosto le performance dell'azienda. L'innovazione quindi appena introdotta prende il nome di "innovazione incrementale".
Notarono che le innovazioni appartenenti a grandi settori produttivi erano correlate ad un numero elevato di miglioramenti minori e continui all'interno dei processi produttivi delle aziende più piccole. I risultati ottenuti da queste venivano poi sfruttati dalle grandi aziende, andando a creare così una sorta di oligopolio.

Questo fenomeno avviene in settori particolarmente specializzati, dove nozioni di mercato di massa ed economie di scala assumono un particolare significato.
Infatti in tali sistemi integrati, a volte, è molto costoso il cambiamento, a causa di un'alta sensibilità verso valle (cioè verso il cliente) successivi ai cambiamenti svolti a monte. Proprio per questo

l'innovazione che si va a presentare è tipicamente incrementale cioè quella che ha un effetto minimale e graduale a livello della produttività.

Per l'innovazione radicale si hanno nuovi prodotti che necessitano di un cambiamento legato alla strategia dell'azienda o agli impianti di produzione. Abernathy e Utterback notarono, inoltre, che per questo tipo di innovazione vi è un concetto anche collegato alla posizione geografica delle aziende, in quanto sono stati trovati fattori molto positivi in contesti in cui vi sono, ad esempio, università scientifiche e/o enti di ricerca nelle vicinanze.
L'intrinseco vantaggio per questi nuovi prodotti è legato sostanzialmente ad un livello di performance decisamente superiore (invece che risparmiare a livello di costo) rispetto a quelli che sono presenti nel mercato. Proprio per questo i consumatori svolgono un ruolo fondamentale, dato che saranno loro in primis gli utilizzatori finali. Infatti, sarà fondamentale comprendere i bisogni emergenti del consumatore, e di conseguenza dei nuovi modi per poterli soddisfare.
Essendoci appunto un contesto molto instabile, si va a favorire questo tipo di innovazione in aziende meno strutturate, avendo intrinsecamente la possibilità di adattarsi molto velocemente ai cambiamenti, poiché essendo più piccole hanno maggiore flessibilità.
Quando vi è la presenza di un nuovo prodotto con la conseguente creazione di un nuovo ambito di mercato, l'azienda, per poter soddisfare sempre più persone, cerca di aumentare le sue dimensioni, andando prima di tutto a migliorare aspetti legati la produzione, alla pubblicità e ai metodi distributivi. Questo è il segno più evidente del passaggio da un'innovazione radicale a una incrementale, che ricopre un ruolo legato allo sviluppo del dominant design che, come detto in precedenza, rappresenta per i due studiosi la linea temporale della suddetta transizione.
L'architettura di prodotto, ad esempio, andrà a togliere o al più livellare le limitazioni poste dalla vecchia tecnologia.

Nel momento in cui ci si trova invece a confrontarsi con un discorso di produzione su larga scala, si passa da obiettivi mal definiti e incerti a obiettivi articolati e certi. In particolare, nelle fasi iniziali, vi è un'abbondanza di requisiti e di criteri richiesti anche se alcuni di essi non possono essere quantificati. Proprio in questo caso, cioè quando vi sono fattori di ambiguità, gli utenti hanno maggiore probabilità di andare a creare un'innovazione.
In base alla fase in cui vi è lo stimolo a creare qualcosa di nuovo cambia il processo perché ad esempio nella fase fluida le esigenze dei consumatori non sono ben definite in quanto gli stessi hanno grandi livelli di incertezza a causa anche del possibile basso livello tecnologico a cui possono fare affidamento. Vi sono perciò due fonti di ambiguità: una prima legata agli obiettivi e una seconda relativa alla parte tecnica. Avanzando nel tempo, l'incertezza a livello di mercato diminuirà andando così a giustificare livelli maggiori di investimento in ricerca e sviluppo.

Proprio grazie a questo studio si ha, quindi, la prima definizione ufficiale di quello che è il dominant design, cioè "*una singola architettura che stabilisce un dominio nella categoria di prodotto*"[1].

[1] Abernathy e Utterback, "*Patterns of Industrial Innovation*"

Qui di seguito due esempi che sono stati presentati nell'elaborato:
La lampadina elettrica ha una storia di miglioramenti evolutivi che sono iniziati con alcune importanti innovazioni, e si sono conclusi con un prodotto altamente standardizzato simile a una merce. Nel 1909 le prime innovazioni del filamento di tungsteno e delle lampadine a vuoto erano in atto; da allora fino al 1955 ci furono una serie di cambiamenti incrementali: migliori leghe metalliche per il filamento, l'uso di "getter" per aiutare a esaurire la lampadina, avvolgere i filamenti, "glassare" il vetro e molti altri. Nello stesso periodo il prezzo di una lampadina da 60 watt è diminuito (anche senza aggiustamento dell'inflazione) da $ 1,60 a 20 centesimi ciascuno, la produzione di lumen è aumentata del 175%, il contenuto di manodopera diretta è stato ridotto di oltre un ordine di grandezza, da 3 a 0,18 minuti per lampadina, e il processo di produzione si è evoluto da una configurazione flessibile del job-shop, coinvolgendo più di 11 operazioni separate e una forte dipendenza dalle abilità del lavoro manuale, ad una singola macchina frequentata da pochi lavoratori.
Il prodotto e il processo si sono evoluti in modo simile nell'industria automobilistica. Durante un periodo di quattro anni prima che Henry Ford producesse la famosa Model T, la sua azienda sviluppò, produsse e vendette cinque diversi motori, che andavano da due a sei cilindri. Questi sono stati realizzati in una fabbrica che era organizzata in modo flessibile come un negozio di lavoro, basandosi su artigiani che lavoravano con macchine utensili per uso generale non così avanzate come le migliori allora disponibili. Ogni motore ha testato un nuovo concetto. Fuori da questo l'esperienza è arrivata a un design dominante: il Modello T; e nel giro di 15 anni 2 milioni di motori di questo unico progetto di base venivano prodotti ogni anno (circa 15 milioni in tutto) in una struttura allora riconosciuta come la più efficiente e altamente integrata al mondo. Durante questo periodo di 15 anni ci sono state innovazione incrementale, ma non fondamentale, nel prodotto Ford.

Il passaggio da innovazione radicale ad incrementale, trattato in questi due esempi, è legato allo sviluppo di un'architettura dominante, che viene accostata ad un aumento di concorrenza sui prezzi e ad una maggiore enfasi sull'innovazione procedimentale.
Si passa, quindi, dal lavoro focalizzato sulle arti manuali e sulle abilità artigianali a processi sempre più automatizzati, caratterizzati da un largo impiego di attrezzature al fine di ottenere un alto volume di produzione.

In un successivo studio svolto da Abernathy, a cui è stato dato il nome di "*The productivity dilemma: roadblock to innovation in the automobile industry*", vengono analizzate evidenze molto importanti legate alla produttività e al suo miglioramento che, come detto in precedenza, non è soltanto una questione di costi ma anche di benefici. Da notare inoltre che vi era riportata la presenza di un trade off a livello aziendale, in quanto i livelli di innovazione rapida e di alta efficienza produttiva andavano in contrasto, da qui il dilemma.

In seguito elaborò anche una sua visione aggiornata del concetto di dominant design. In particolare, notò che, prima del palesarsi dell'architettura dominante, vi è un insieme di sforzi (miglioramento delle funzionalità del prodotto, coordinamento delle parti interessate, …) svolti dalle aziende in

modo tale da rendere massima la probabilità che il proprio design proposto venga selezionato come predominante.
Una volta arrivati ad un'architettura dominante si porranno tutte le forze verso un suo miglioramento legato all'efficienza del processo di produzione; quindi avverrà un'innovazione più legata al prodotto e nel momento in cui si paleserà il dominant design allora l'innovazione verterà più sul processo.
Una volta che si raggiunge l'ottimo con le economie di scala i due tassi di innovazione tenderanno ad uniformarsi.

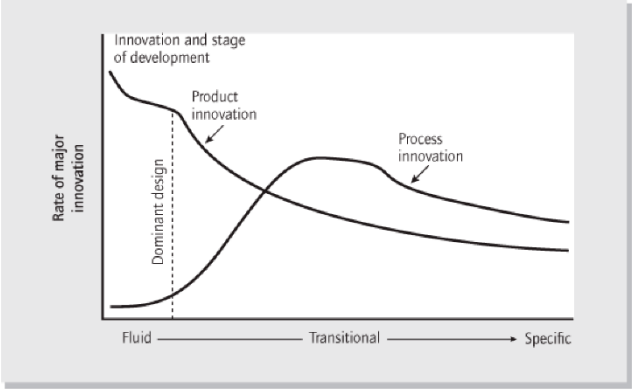


Figura 3: Passaggio da innovazione legata al prodotto a quella legata al processo

Pochi anni dopo, il concetto di dominant design riprese piede soprattutto grazie all'apporto di Philip Anderson e Michael L. Tushman, che pubblicarono un estract dal titolo "*Technological Discontinuities and Dominant Designs: A Cyclical Model of Technological Change*", in cui analizzarono il fatto che, in seguito ad un'innovazione tecnologica (discontinuità), vi è un periodo di selezione dei vari prodotti proposti, che porterà come risultato quello della designazione del dominant design.

Ogni discontinuità tecnologia fa progredire il confine delle prestazioni. Sebbene vi sia un avanzamento nello stato dell'arte, si palesa un modo nuovo per svolgere una determinata mansione, oppure lo sviluppo di un altro design. Le discontinuità possono creare due diversi scenari, dipendenti dalle competenze: "*competence destroying*" e "*competence enhancing*".
La prima, che è tipica dell'innovazione radicale, rende l'organizzazione aziendale obsoleta, in quanto va a minare le competenze di un esperto, rendendolo alla pari di qualsiasi giovane alle prime armi.
La seconda, che è invece tipica dell'innovazione incrementale, va a rafforzare l'organizzazione, andando ad agire sulle competenze già esistenti. In sostanza, va a lavorare, sullo stesso paradigma tecnologico.

Gli studiosi propongono un modello ciclico per il cambiamento tecnologico, in cui vi è una evoluzione socioculturale di variazione, selezione e mantenimento. Le dinamiche sociali, politiche e organizzative vanno a formare le architetture dominanti.

Una volta che si apporta un cambiamento radicale, si ha come conseguenza inevitabile quella di dare inizio a un periodo turbolento, caratterizzato da aziende che mettono in campo qualsiasi forma di sperimentazione, al fine di assorbire questa nuova tecnologia. Momento che sperimenta anche un altro tipo di incertezza, dovuto alle competizioni relative sia allo stesso paradigma sia a quello emergente, trovandosi così a districarsi fra regimi tecnologici alternativi. Questo processo culmina con l'emergere del dominant design e, una volta palesatosi, si andrà a migliorare marginalmente la tecnologia.
Il progresso può quindi essere indirizzato attraverso la combinazione di: variazione (cioè eventi casuali), selezione (cioè azione sociale e politica per la selezione del design dominante) e mantenimento (azioni incrementali delle aziende).

Infatti le discontinuità tecnologiche "*innescano un periodo di fermento che viene chiuso dall'emergere di un design dominante. Segue un periodo di innovazioni incrementali, che viene poi interrotto dalla successiva discontinuità tecnologica*".
Particolarità di questo elaborato è la ricerca di un metodo quantitativo che porti a definire un'architettura come dominante, cioè quando questa guadagna più del 50% del mercato mantenendolo per almeno quattro anni in maniera consecutiva.

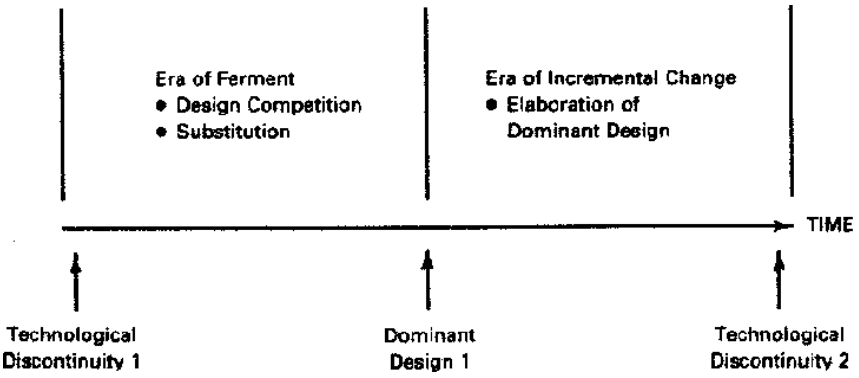


Figura 4: Rappresentazione del modello ciclico per il cambiamento tecnologico

Negli anni successivi, Utterback pubblicò i risultati derivanti da un nuovo studio, "*Mastering the Dynamics of Innovation"*, in cui asserì che il dominant design sarà quello che riuscirà ad ottenere la fedeltà dei consumatori. Quindi le aziende dovranno aderirvi per cercare di diventare leader di quel mercato, o quantomeno di riuscire a ritagliarsi per sé una quota di mercato corposa.

Abernathy e Fernando Suarez pubblicarono uno studio, "*Patterns of Industrial Innovation, Dominant Designs and Firms' Survival*", nel quale definirono il dominant design come quella strategia che riesce a dominare gli altri concorrenti lungo tutto il processo di progettazione.

In particolare, specificarono, come nell'elaborato precedente, che questo concetto raffigura le esigenze di molti utenti.

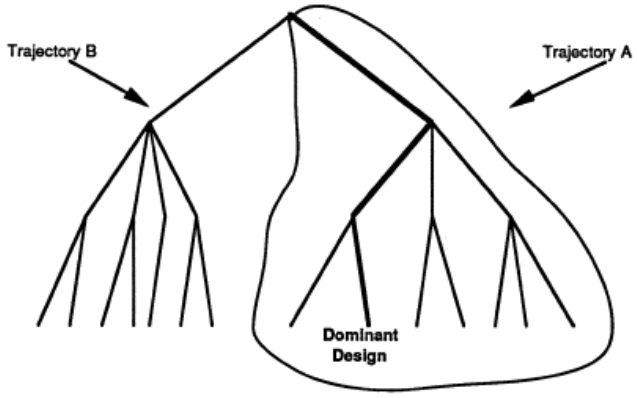


Figura 5: Gerarchie di design e design dominante

Il design dominante comporta il porre in essere un percorso specifico, che vedrà necessariamente coinvolti una serie di fattori produttivi, in modo tale che si arrivi alla costruzione di una gerarchia del settore. Certamente a fondamento del design dominante troviamo la tecnologia, che funziona anche come collante tra le diverse componenti del percorso, ma sono sfruttati anche altri fattori, tra cui:

- **Interventi governativi**: la regolamentazione del settore da parte di uno stato, imponendo uno standard, definisce un'architettura dominante.

- **Strategie** a livello aziendale: il tipo di strategia perseguita da un'impresa, in funzione del suo prodotto o del comportamento dei concorrenti, può individuare quale architettura della stessa diventerà dominante

- **Esternalità di rete**: i vantaggi che possono derivare a un individuo dall'uso di un determinato bene sono sempre maggiori man mano che cresce il numero di soggetti che utilizzano quel bene.

- Possesso di **assets collaterali**: troviamo un'impresa che si trova ad avere attività collaterali, comprendenti attività collaterali quali canali di mercato, immagine di marca e costi di cambio. Il cliente avrà qualche vantaggio rispetto ai suoi concorrenti, determinati dal rafforzamento del suo prodotto come design dominante.

- **Comunicazione** verso i consumatori: essere vicini agli utenti finali aiuta l'azienda a comprendere più nel dettaglio i requisiti del prodotto così da costruire un'architettura ad hoc apprezzata dagli stessi.

Quindi quali effetti comporta il design dominante? Il primo e più importante consiste nel fatto di far rispettare le standardizzazioni, mettendo in piedi una ricerca che tenderà a trovare economie di scala che siano in grado di spostare la concorrenza sul piano dei costi e delle prestazioni del

prodotto. Un secondo effetto determinato dall'emergere di un design dominante è quello di determinare nuovi metodi di concorrenza fra le imprese che operano nel medesimo settore di riferimento facendo quindi scaturire il tema delle economie di scala (fattore importante specialmente se si fa riferimento al periodo successo all'emergere dell'architettura dominante, piuttosto che al momento precedente di turbolenza e di sperimentazione).

1.2 Le dinamiche di sviluppo del dominant design

Alcuni degli studi sul dominant design che sono stati presentati poc'anzi danno un'ampia spiegazione di tale concetto, e fanno risaltare la sua importanza nella selezione naturale, da parte del mercato, della tecnologia vincente.
Grazie agli elaborati si poté, negli anni successivi, sviluppare maggiormente la letteratura in merito, andando ad analizzare più nel dettaglio quali fossero analiticamente e specificatamente le varie cause di selezione dell'architettura dominante, e i fattori che sono in grado di determinare la sua esistenza e sopravvivenza nel mercato di riferimento. Inoltre si concentrarono gli studi anche su quegli aspetti che non erano stati considerati precedentemente nei vari modelli, come ad esempio il discorso della modularità, dell'integrazione verticale e dell'evento trigger con periodo di incubazione.

1.2.1 Le fasi di sviluppo del prodotto

Prima di svolgere queste analisi, viene proposto di seguito un riassunto delle fasi di sviluppo del prodotto e selezione del dominant design, date dall'insieme degli elaborati sopra presentati, cioè la rappresentazione del processo tecnologico anche grazie al lavoro svolto da Funk, *"Standards, dominant designs and preferential acq*uisition of *complementary assets through slight information advantages"*.

1. **Turbamento tecnologico**: consiste nel rinnovamento degli asset tangibili e intangibili dell'azienda, in cui si va a presentare l'emergere di un nuovo prodotto o, ancora, di un nuovo modo per svolgere le stesse funzioni.

2. **Era di fermento** (caratteristica dal lavoro di Anderson e Tushman): si sostanzia nella concorrenza fra inter-prodotto e intra-prodotto, cioè si ha un confronto sia tra nuovo-vecchio sia tra diversi nuovi.
   Le aziende, indipendentemente dal fatto che siano già presenti nel settore o siano nuove, cercano di sfruttare il più possibile le opportunità della nuova conoscenza. Le società tendono ad entrare in questo contesto per proporre diverse architetture, anche non migliorative, in modo tale da cercare di accaparrarsi la maggior quota di mercato possibile. Si avrà così la proposta di diverse alternative tecnologiche relative a uno stesso prodotto.

3. **Selezione** (già enunciata nel primo lavoro di Abernathy e Utterback): scelta da parte dei consumatori del dominant design, cioè quell'architettura di prodotto che riceve il maggior appoggio da parte degli utilizzatori finali. Diverse aziende possono ragionare in un diverso modo rispetto a quella che "punta tutto" per far vincere la sua idea di design. In particolare alcune preferiscono accontentarsi di spartire una grossa fetta di mercato al posto di non avere nulla in mano. Quindi, per fare ciò, si alleano con altre aziende in modo tale da poter investire una quantità di denaro maggiore e di aver contemporaneamente una maggior probabilità affinché venga scelto il loro design come dominante.

Una volta selezionato, il numero di entità fisiche diminuisce drasticamente, facendo uscire quelle a cui i consumatori non hanno dimostrato fedeltà rispetto all'architettura di prodotto proposta dagli stessi. Questo fenomeno, già citato in precedenza, prende il nome di "shake-out".
L'andamento ad imbuto verso un unico design porta con sé il concetto di economia di scala.

4. **Innovazione incrementale**: miglioramenti marginali all'architettura di prodotto scelta.

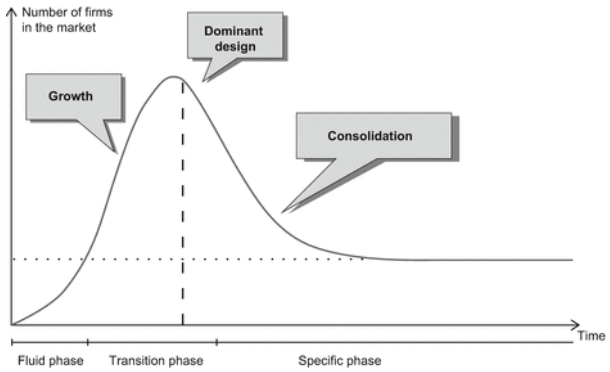


Figura 6: Fenomeno dello "shake-out" post dominant design

1.2.2 I criteri di selezione del dominant design

Quali sono le motivazioni alla base della qualificazione di un'architettura come dominante? Le cause sono molteplici, e possono riguardare indifferentemente l'ambiente esterno e interno all'azienda. I fattori presentati grazie al lavoro di Suarez, nominato "*Battles for technological dominance: an integrative framework*", non sono mutuamente esclusivi, ma, anzi, praticamente sempre vi è una loro combinazione tale da creare, alcune volte, una distorsione dalla posizione di equilibrio che si era creato.

Per quanto riguarda i fattori interni all'azienda, cioè quelli direttamente collegabili all'operato della stessa, si trova:

- **Reputazione dell'azienda**: il fattore della credibilità, validità e solidità dell'azienda gioca un ruolo fondamentale per la determinazione del successo dell'azienda stessa, portandola così ad affermarsi sulle concorrenti. Questo perché, come osserviamo con qualsiasi prodotto offerto da un'impresa già solidamente affermata nel suo campo di riferimento, i consumatori saranno più fiduciosi delle qualità dell'architettura proposta dalla nostra azienda in questione, piuttosto che da qualsiasi altra con minor affermazione a livello sociale. Vige soprattutto qui un discorso di reputazione dell'azienda, in quanto interviene il pensiero che "se ha già fatto bene in passato perché ora non può farlo?".
  La buona reputazione dell'azienda gioca un ruolo molto importante, inoltre, anche in contesti dove è largamente presente una certa incertezza del consumatore, dato che sarà lui che di norma si affiderà ad un'azienda che già conosce o che, quantomeno, sia nota.

Si può osservare questo criterio anche con gli occhi di un'impresa concorrente e non solo dei consumatori. Questo perché se un'azienda ha già creato nella mente degli "avversari" l'idea di azienda leader, allora questa, con la proposta di aiutare le altre ad avanzare tecnologicamente o ad entrare nel mercato di riferimento, licenzia i propri brevetti, facendo così tendere i concorrenti ad adottare il proprio design, così da renderlo dominante.

- **Superiorità tecnologica**: il design proposto dall'azienda incorpora e coordina le migliori caratteristiche della tecnologia al proprio interno, ed è proprio questa combinazione che fornisce al design maggiori possibilità di affermarsi come dominante nel suo settore di riferimento. Naturalmente, affinché ciò accada, gli utenti o consumatori devono essere messi in condizione della superiorità qualitativa del prodotto, affinché lo preferiscano a quelli concorrenti.
  Questa combinazione intrinseca di fattori, per l'appunto, si trova ad essere determinante nel momento di scelta tra prodotti concorrenti effettuata dai consumatori finali. Si tratta quindi di cercare di catturare la fedeltà di quel gruppo di persone non intimorite da un nuovo prodotto. Queste figure sono gli innovators e la prima "fetta" degli early adopters (modello di Rogers-Moore esposto all'inizio dell'elaborato). Questo concetto di cercare una loro approvazione porta con sé il fatto di poter entrare nel mercato e cercare di raccogliere i primi feedback da quelle persone che risultano essere più predisposte a mettersi in gioco a favore della tecnologia.

- **Asset complementari**: l'investimento in immobilizzazioni che aiutano il design a rafforzarsi gioverà sicuramente all'azienda, in quanto si andranno a combinare i valori creati dall'unione delle "forze". Si va quindi a fare affidamento all'effetto denominato di "*lock-in*", cioè a rendere il cliente quasi vincolato al proprio prodotto, fattore che gli permette di creare alti costi di switching.
  Pistorius e Utterback elaborarono questo concetto andando a specificare che tecnologie complementari rappresentavano caratteristiche di simbiosi in quanto una aveva un effetto positivo sulla diffusione dell'altra.

- **Dimensione della base installata di utenti**[2]: criterio che acquisisce un certo effetto in occasione soprattutto di effetti di rete, in quanto all'aumentare della base installata aumenteranno i tassi di adozione per una tecnologia. Quindi, questo fattore andrà a potenziare gli altri criteri presentati poc'anzi, fornendo ulteriori possibilità all'azienda di affermare il proprio design come quello dominante. La dimensione della base di utenti può essere anche rappresentata da una già esistente per altri tipi di prodotti, anche se dipende tutto dalle differenze di performance tra la vecchia e la nuova tecnologia, perché se questa discrepanza risulta grande allora i benefici saranno minori.

[2] Katz-Shapiro del 1985

- **Strategia dell'azienda**: scorporando più nel dettaglio questo criterio, si possono identificare quattro elementi che acquisiscono una determinata importanza a riguardo:

    - **Time-to-market**[3]. Legato sia al momento di ingresso nel mercato sia al momento di inizio del processo di investimenti in ricerca e sviluppo.
      Un'entrata precoce nel mercato aiuta l'azienda ad erigere, prima di altri, una base portante, così da averla più grande di altri, beneficiando al tempo stesso delle ricadute positive che ciò avrà sulla reputazione. Un'entrata precoce nelle attività di ricerca e sviluppo crea importanti effetti di apprendimento, dando quindi alle aziende anche maggior tempo affinché vengano svolte molte sperimentazioni delle alternative tecnologiche.
      Nonostante questi vantaggi, vi sono delle conseguenze possibilmente negative legate al blocco delle aziende in particolari traiettorie tecnologiche anche non coerenti con il design dominante. Inoltre, l'ingresso precoce può non massimizzare le probabilità di sopravvivenza delle imprese dato che si dovrebbe entrare pochi anni prima dell'emergere del dominante design.

    - **Strategia di prezzo**[4]. Un livello di pricing aggressivo nei primi anni, cioè con logica di prezzo basso all'inizio e rialzato successivamente (contrario del "*price skimming*" in cui si parte da un alto prezzo per poi abbassarlo), unito alla possibilità di fattori di rete, può portare ad ottenere la fiducia di una porzione della clientela presente sul mercato molto grande, così da massimizzare le probabilità che la propria architettura diventi quella dominante.

    - **Politica delle licenze dei brevetti**: un'azienda può affrontare l'opzione, come citata precedentemente, di rendere totalmente fruibile la propria tecnologia in modo gratuito. Questo permette alle altre aziende di non dover affrontare ingenti investimenti in R&D, il che potrebbe portare anche a raffrontarsi con soluzioni non percorribili, facendo perdere il denaro utilizzato. Si ha però di contro che in questo modo aumenterà notevolmente la concorrenza, anche in un'ottica riscontrabile nella quarta fase del processo di sviluppo, cioè quella riferibile all'innovazione incrementale dell'architettura, conducendo così ad una possibile perdita di controllo sul percorso di sviluppo.

    - **Intensità della comunicazione verso i clienti**[5]: se sfruttati a dovere, fattori come un ottimo preannuncio del prodotto possono creare un'aspettativa positiva sui prossimi modelli della stessa azienda rendendo, in un certo modo, i consumatori finali legati a lei.

[3]Lieberman-Montgomery del 1998; Klepper del 1996; Rosenbloom-Cusumano del 1987; Carpenter-Nakamoto del 1990; Dosi del 1982; Christensen del 1998.

[4] Katz-Shapiro del 1985

[5] Katz-Shapiro del 1985

Per quanto riguarda i fattori esterni all'azienda, cioè quelli non direttamente collegabili all'operato della stessa, si trova:

- **Effetti di rete**[6]: rappresentano l'utilità che l'utente percepisce in base alla grandezza del bacino di consumatori finali, che già sfruttano il prodotto e/o servizio dell'azienda. Quindi all'aumentare della base di clienti pre-installata aumenterà, grazie all'esternalità di rete, il numero di utenti finali, avendo così sempre più probabilità che il proprio design presentato sia considerato come dominate. Perciò da bassi effetti di rete non deriva un imponente beneficio a mettere in campo una precoce entrata nel mercato.
  La letteratura ricollega a ciò due possibili effetti:
  - Diretti: quando l'ennesimo cliente si unisce alla rete, si crea una connessione nuova per tutti gli altri utenti già presenti nella rete
  - Indiretti: dal risultato dell'aumento della domanda dei beni complementari

- **Costi di switching**: costi che ha un cliente quando vuole "transitare" su un nuovo prodotto. All'aumentare di questi costi, sarà sempre più difficile, per un'azienda, andare a sottrarre i clienti ai concorrenti in quanto gli utenti saranno fedeli all'azienda.

- **Regime di appropriabilità**[7]: l'appropriabilità altro non è che la "*capacità di un'impresa di acquisire e trattenere i profitti generati dalla sua attività di ricerca, bloccando l'imitazione da parte dei concorrenti*" (definizione della Treccani). La presenza di un forte regime di appropriabilità aiuterà le aziende che presentano soluzioni tecnologiche più avanzate, in quanto andrà a limitare e a cercare di impedire ai concorrenti di appropriarsi dei loro clienti. Sarà quindi difficoltoso per le aziende che presentano un'architettura non tecnologicamente superiore imporre il loro design come dominante.

- **Regolamentazione ed intervento istituzionale**: è possibile che un governo agisca affinché venga imposto l'uso di una particolare tecnologia per evitare situazioni di elevata, e alcune volte eccessiva, competizione tra le aziende, andando anche ad accelerare l'inizio delle economie di scala.
  Altro scenario ipotizzabile è quello che vede la possibile situazione di fatto in cui uno stato acquista un prodotto piuttosto che un altro, facendo così pendere l'ago della bilancia più verso un design piuttosto che verso un altro.
  Ulteriore caso riguarda le associazioni private le quali possono influenzare l'ascesa di una tecnologia in un mercato prima di altre.

[6] Katz-Shapiro del 1985

[7] Teece del 1986

- **Caratteristiche del campo tecnologico** (struttura e dinamiche)[8]: all'interno di un campo tecnologico, diverse alternative tecnologiche concorrono per dominare. Le caratteristiche del campo tecnologico (numero di attori, potere relativo di ogni attore e livello di cooperazione-concorrenza), quindi, determinano una maggiore o minore capacità di un'impresa di trovare accordi con altre che operano all'interno dello stesso campo (abitato da ricercatori e da aziende che operano lungo la catena del valore). Ne discende come conseguenza la bravura dell'azienda stessa di andare a trovare il giusto equilibro tra le diverse caratteristiche.

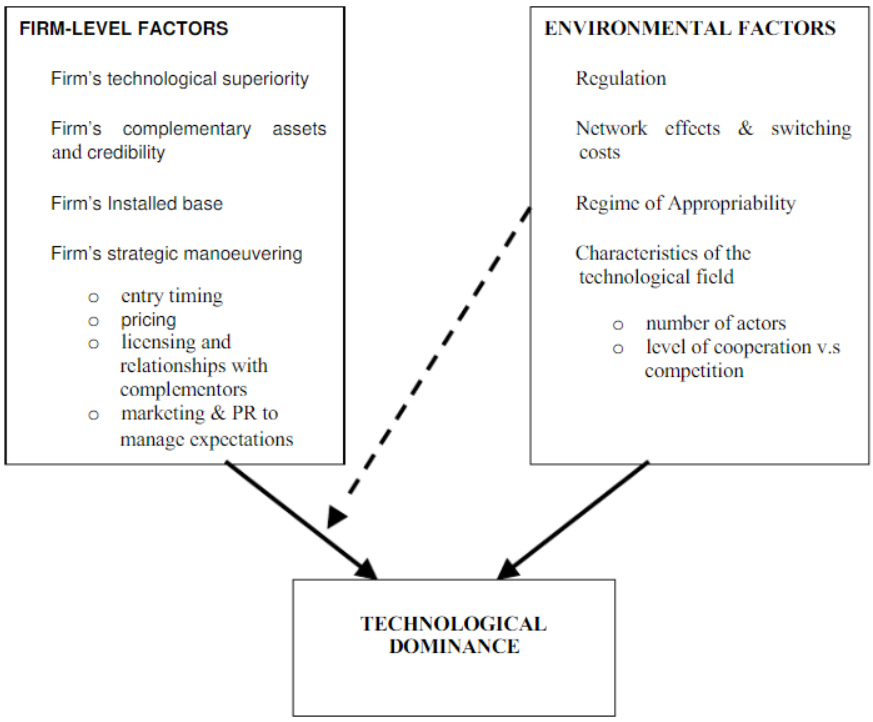


Figura 7: Riassunto delle cause di selezione del Dominant Design

1.2.3 I criteri di stabilità del dominant design

In seguito al palesarsi del dominant design, e quindi terza fase del processo di sviluppo dell'architettura, vi è la parte di innovazione incrementale, in cui si cercano di apportare delle migliorie, anche marginali, al design.

Possiamo per questo dire di essere presenti nella fase in cui vi è l'uscita delle imprese alternative e concorrenti che non hanno trovato la fiducia da parte del mercato. Le aziende che hanno elaborato quelle proposte hanno davanti a loro due possibili decisioni: uscire direttamente dal mercato, dedicandosi ad altro, oppure cercare di soddisfare solo una nicchia di consumatori. Questa seconda alternativa comporta la possibilità per l'impresa di mantenere in vita la sua alternativa, ma non in

[8] Garud del 2002

ottica di accontentare un mercato intero, quanto invece per soddisfare una minima parte con determinate necessità, che richiedono che il prodotto abbia delle specifiche caratteristiche che, per disparati motivi, il design che ha dominato gli altri non può garantire, per la sua intrinseca natura oppure per gli obiettivi che l'azienda "madre" si è data con la sua architettura vincente.

Essendo il design dominante quello che ha raccolto la maggior fiducia da parte degli utilizzatori finali, le altre aziende, per evitare di lasciare il mercato nelle mani di un'unica o al più ad un manipolo di poche imprese, entrano nel suddetto business utilizzando l'architettura vincente e adattandosi ad essa.

Questa stabilità può essere paragonata all'effetto "lock-in" degli utenti, dato che un'architettura dominante è difficile da eliminare dal mercato, in quanto vi sono diversi fattori che incorrono:

- **Economie di scala**: il palesarsi di un dominant design porta con sé a un aumento della produzione, e quindi alla diminuzione dei costi e, di conseguenza, dei relativi prezzi. Si spinge così sulla diffusione del prodotto in seguito alla standardizzazione del processo di produzione dopo i vari efficientamenti dello stesso.
  Caratteristica importante è la creazione di alte barriere all'ingresso per il mercato di riferimento che, insieme alla creazione di processi produttivi ad hoc, rende le aziende sempre più ancorate al design dominante.

- **Esternalità di rete**: contribuiscono, come visto in precedenza, ad aumentare la base di clienti favorendo l'espandersi del dominant design.

- **Sunk costs**: sono i costi affondati dell'azienda, cioè quelli che sono stati investiti per la produzione specifica di quel particolare prodotto che sfrutta il design che è emerso. Ovviamente, all'aumento dei sunk costs aumenterà la permanenza dell'architettura dominante, poiché quel denaro non può essere reinvestito in altre attività.

- **Asset complementari**: investendo in beni complementari si va ad aumentare l'utilità dei clienti, andando così a generare alti costi di transazione verso altri prodotti così da creare un'inerzia al cambiamento.

- **Economie di apprendimento**: consente all'organizzazione di apprendere, sul lungo periodo produttivo, e di specializzarsi sull'architettura emersa, andando a ridurre i costi e garantendo anche maggiore qualità.
  Come per le economie di scala, genera delle alte barriere all'ingresso.
  Inoltre se si presenteranno delle nuove alternative, i produttori non le troveranno attrattive, in quanto avranno maggiori benefici a non effettuare il passaggio.

- **Scelte di integrazione**: il palesarsi del dominant design va a bloccare la struttura organizzativa della catena del valore andando così a rimanere "incastrati" nell'architettura emersa.

1.2.4 Le critiche ai modelli

È stato appena descritto il percorso naturale studiato nei vari elaborati. Prendendo come punto di riferimento il primo studio effettuato da Abernathy e Utterback, possiamo riscontrare che non si trovano degli elementi che risultino essere importanti per porre in essere uno studio accurato delle dinamiche dell'innovazione, e di conseguenza dell'emergere del dominant design. In particolare, mancano temi riguardanti la modularità, l'integrazione verticale, la causa scatenante della fase fluida e la questione relativa ai campi applicativi per l'emersione del dominant design. Sono presenti, comunque, altre critiche al modello appena descritto ma le quattro appena presentate sono quelle con un maggior rilievo e seguito.

Grazie agli studi di Cebon e Hauptman, raccolti sotto il nome di "*Industries in the making: Product modularity, technological innovation and the product lifecycle*", viene analizzato il tema della **modularità**.
La modularità dei prodotti cambia radicalmente le basi della strategia tecnologica? Ebbene sì. La modularità non va a considerare il dominant design come il palesarsi di un prodotto finito "tutto di un sol pezzo", ma va piuttosto ad analizzare il manifestarsi dell'architettura dominante all'interno di tutti i componenti, che, una volta assemblati, andranno a costruire il prodotto finito.
Abernathy e Utterback non ragionarono in questo senso, perché considerarono come se si stesse trattando di architetture integrate costituite da una sola azienda, ma sappiamo che nella pratica così non è, dal momento che il dominant design può emergere da ognuno dei moduli del prodotto. Un esempio di prodotto modulare è la macchina (composta da motore, display, …) i cui componenti hanno una funzione indipendente e che poi assemblati danno origine al prodotto finito.

Analizzando più nel dettaglio gli effetti della modularità sul dominant design, si presentano le seguenti osservazioni:

- Tendenzialmente la modularità costringe a rendere **esplicita** quella parte di **conoscenza** tacita relativa alle interazioni tra i diversi moduli. Tuttavia, lascia alle organizzazioni le conoscenze confinate entro i singoli moduli.

- Andando a studiare i singoli componenti, si andrà a formare una elevata **competenza specializzata**[9] (progettazione e produzione) per ogni singolo modulo, conoscenza che potrà essere riversata sull'esperienza legata all'architettura di prodotto. Questo, quindi, permetterà di portare la struttura organizzativa ad essere il più vicina possibile a quella del processo produttivo, rendendola di conseguenza poco soggetta ai cambiamenti che possono

[9] Sanchez del 2001

intervenire anche nel caso più estremo di out-sourcing senza quindi andare ad intaccare il resto.

- Riduce l'effetto lock-in causato dalle **esternalità di rete**, in quanto la modularità andrà ad intaccare, diminuendo, il legame che si crea tra prodotto finito e beni complementari[10]. Qualora questi asset siano sostituibili (aiutato dalla modularità), l'effetto di "blocco" è ridotto.

- Impatto molto importante anche sul fronte delle **economie di scala**, dato che non si andrà più a vedere il prodotto assemblato, quanto si andrà piuttosto a studiare per singolo componente. In questo modo, quindi, si ottimizzerà il processo dello specifico modulo, andando a rendere più efficiente, nel tempo, il relativo costo. Al posto di cercare di avere il livello minore di costo per il prodotto finito, si andrà ad avere tanti ottimi locali che insieme comporranno il prodotto assemblato.
  In parallelo si possono sfruttare le scale minime efficienti dei moduli affinché vengano utilizzati per altri prodotti (ad esempio un display può essere collegato alla tv come ad un computer).

In concreto, se si guardano i principali driver di lock-in per il dominant design, si nota che la modularità serve a ridurre, se non eliminare del tutto, la loro importanza. Quindi ci si potrà ragionevolmente aspettare che il ciclo di vita del prodotto sia drammaticamente attenuato, se non cancellato, nei sistemi modulari.

Prima di andare ad analizzare la scelta strategica di effettuare o meno l'**integrazione** verticale, discorso tra l'altro non affrontato da Abernathy e Utterback, è opportuno specificare di quale tipo si stia parlando. Vi possono essere due possibilità. La prima, c.d. "verso valle", vede il fornitore che andrà ad integrarsi con l'azienda distributrice, che si assumerà il compito di vendere effettivamente il prodotto ai consumatori finali. La seconda, c.d. "verso monte", in cui invece vediamo il distributore finale effettuare delle scelte di integrazione verso il fornitore, ossia si andrà a guardare lo sviluppo e/o la produzione di componenti.
Per effettuare tali scelte è necessario prendere in considerazione dei fattori che espongono le condizioni del mercato e la complessità dell'architettura del prodotto.

Nel caso di **integrazione a valle**, il problema si trova nel valore che gli asset complementari forniscono ai clienti. Se vi si presenta un valore molto elevato, è possibile seguire due diverse strade. La prima comprende delle partnership con le aziende che producono questi beni complementari. La seconda contempla la scelta di seguire la strada dell'integrazione. Quest'ultima strada richiede sicuramente un corposo finanziamento, che quindi l'azienda dovrebbe essere in grado di sostenere. Parallelamente a ciò, però, un basso grado di integrazione sarà possibile solo nella situazione in cui

[10] David del 1985

la relazione tra il prodotto e i beni complementari non è specifica, e in cui non vi è un definito modello di business che permetta di avere un ritorno dagli investimenti praticati su questi beni.

Nel caso dell'**integrazione a monte**, si possono avere due casi:

- Con prodotti aventi **bassa modularità** (quindi il design di ciascun componente è dipendente dal design degli altri). In questa ipotesi si contempla il caso in cui si può osservare un alto grado di integrazione verticale fino a quando vi è innovazione di prodotto, cioè fino a quando non è emerso il dominant design. Questo perché, a meno che non si abbia la certezza che un design diventi dominante, è improbabile che altre aziende vogliano diventare un fornitore specifico per un componente caratteristico dell'architettura. Quindi, le responsabilità sullo sviluppo dei componenti saranno accollati alle aziende che si occupano del prodotto finale.

- Con prodotti aventi **alta modularità** (quindi il design di ciascun componente non dipende dal design degli altri). Nel secondo caso che analizziamo ci troviamo ad osservare un basso grado di integrazione, dove il mero assemblaggio del prodotto verrà effettuato dalle aziende che lavorano sul prodotto finale. Se ci dovesse essere un alto grado di integrazione ci sarebbe un alto livello di controllo sui componenti. Questo però richiederebbe un corposo investimento che, a meno che non si stia parlando di aziende ben finanziate, renderebbe la scelta impossibile.

Indipendentemente dalla scelta, l'integrazione porterà sicuramente ad avere un livello di controllo sulla tecnologia e sul paradigma che sta emergendo, ben maggiore di quello che si otterrebbe dall'avere aziende separate. Persistono però due ordini di problemi: il primo riguardante il corposo ammontare dei finanziamenti, il secondo concernente l'aumento della complessità organizzativa.
Oltre all'incertezza tecnologica, le aziende devono anche cercare di comprendere l'insicurezza relativa al comportamento del mercato, cioè dei consumatori, dato che all'inizio del ciclo di vita del prodotto non si hanno dei veri e delineati bisogni dei clienti, essendo questi ancora latenti.

Un criterio generale, cosicché un'azienda possa seguirlo, è praticamente impossibile da dettare. Le imprese dovranno tener d'occhio il mercato affinché possano comprendere il prima possibile dove si presenterà il primo collo di bottiglia che rallenterà la diffusione, andando a cercare delle soluzioni a riguardo.
Anche agendo da first mover, cioè da primi entranti nel mercato, si possono avere dei problemi correlati principalmente ai bisogni dei clienti, non garantendo quindi a queste aziende un vantaggio relativo le economie di apprendimento, pur avendo un ampio arco temporale da sfruttare davanti a sé.

Sicuramente però interviene il discorso relativo al dominant design, in quanto tendenzialmente le aziende andranno ad integrarsi prima del palesarsi di tale architettura, essendo anche difficile reperire componenti del prodotto che dovrebbe portare l'impresa ad essere dominante nel campo

di riferimento. Successivamente, andranno a disintegrarsi verticalmente al fine di poter sfruttare al massimo le economie di scala dovute principalmente alle standardizzazioni dei singoli componenti.

Altro fattore importante per l'emergere del dominant design riguarda la questione dei diversi **ambiti applicativi**.
Quando Abernathy, Utterback e Suarez hanno presentato i loro elaborati riguardanti le metodologie con cui era possibile, secondo loro, che emergesse l'architettura dominante, hanno analizzato il fenomeno sempre da un punto di vista tecnico. Invece, gli studiosi moderni, hanno rilevato che non ci si debba basare unicamente sul fatto che le varie alternative funzionino o meno. Caratteristica aggiuntiva, difatti, è quella riguardante le possibili applicazioni che possono avere le diverse tecnologie. Questo discende dal fatto che ci possono essere tecnologie e prodotti che funzionano anche molto bene ma che a livello pratico e contrariamente ad altre, hanno un numero ridotto di possibilità di applicazione o, più semplicemente, ambiti applicativi diversi.
L'esempio più lampante è quello del motore a scoppio che, rispetto ad altri modelli, ha avuto grandissimo successo negli anni. Questo è dato sia dal successo tecnico (funziona) sia dal successo applicativo. In particolare, oltre a lavorare bene nella macchina, funziona benissimo in molti altri prodotti, che spaziano dalla piccola motosega alle grosse navi.
Quindi, lasciando da parte per un momento le considerazioni corrette fatte negli anni dagli studiosi, bisognerà analizzare anche gli ambiti applicativi, perché tendenzialmente all'aumentare degli stessi aumenterà il livello di gradimento da parte degli utenti finali, rendendo quindi localmente quell'architettura come dominante. Discorso aggiuntivo si potrebbe fare prendendo come indicatore di evoluzione il livello di investimenti. In questo caso si andrà a studiare ogni incrocio tecnologia-applicazione, e così si può andare a trovare quale soluzione specifica sarà in grado di conferire il dominio di mercato alle aziende che si focalizzeranno su ciò.

In parallelo a quest'ultimo fattore appena citato, si correla la questione relativa la fase fluida, e più specificatamente l'evento trigger e il periodo di incubazione non presenti all'interno degli studi sopra esposti.
In particolare, si va ad analizzare più nel dettaglio la prima delle tre fasi trattata nello studio di Abernathy e Utterback del 1975. In questo primo periodo dello sviluppo industriale si valutano le varie traiettorie tecnologiche, con annessa strategia, che saranno potenzialmente in grado di portare le aziende al successo con la propria proposta di design. In questa fase si andranno quindi a proporre diverse alternative atte a modificare l'equilibro del mercato preesistente o creandone uno nuovo.
Caratteristica principale di questo periodo nella sua alta ambiguità sia a livello di mercato sia a livello di tecnologia, rendendo molto complicate eventuali previsioni sull'architettura dominante. In particolare, qui si andranno ad effettuare sperimentazioni per cercare di cogliere i massimi benefici della tecnologia in questione, derivanti da ogni sua possibile applicazione, attraverso l'uso di diversi prototipi. Inoltre, l'incertezza andrà a far sì che vi siano numerose aziende, anche di piccole dimensioni, che, grazie a finanziamenti e posizionamenti geografici strategici, svilupperanno sempre nuovi archetipi.

Particolare interesse si ha verso la causa scatenante della fase fluida, il cosiddetto **evento "Trigger"**, e relativo periodo successivo di incubazione.
L'evento aizzante il nuovo ciclo di vita tecnologico può essere causato da una scoperta scientifica (avviene tendenzialmente presso gli enti di ricerca come le università e tale conoscenza viene poi riversata in aziende private nuove, cioè startup, oppure in altre già esistenti), dal soddisfacimento di un bisogno non ancora accontentato (prototipo creato da utenti che risolvono un problema che hanno loro stessi in prima persona, per poi riversare l'invenzione nel mercato) o da una "grand challenge" (sfida creata da grossi enti statali, con l'obiettivo di creare un impatto positivo sulla collettività). Possono anche esistere dei casi in cui si presenti la possibilità di avere diversi eventi che causano l'inizio della fase fluida.

La **fase** successiva è quella riguardante l'**incubazione** (dalla durata non precisata), la quale permette alle imprese di perfezionare la tecnologia, andando anche ad analizzare gli ambiti applicativi. Si cercherà, dunque, di customizzare il prodotto per la relativa applicazione così da cercare di catturare la massima fiducia dei clienti. Questo avrà l'obiettivo di abbassare i livelli di incertezza tecnologica e di mercato, in quanto si punterà a commercializzare il prototipo abbozzato dall'evento trigger.

In seguito ai modelli proposti dalla letteratura, ci sono società di consulenza che ne hanno presentati di propri. Uno tra i più famosi, l'*Hype Cycle*, è quello esposto da Gartner, il quale, grazie ad una curva aggiornata costantemente, può mostrare le aspettative, nel tempo, dei consumatori di una tecnologia emergente.

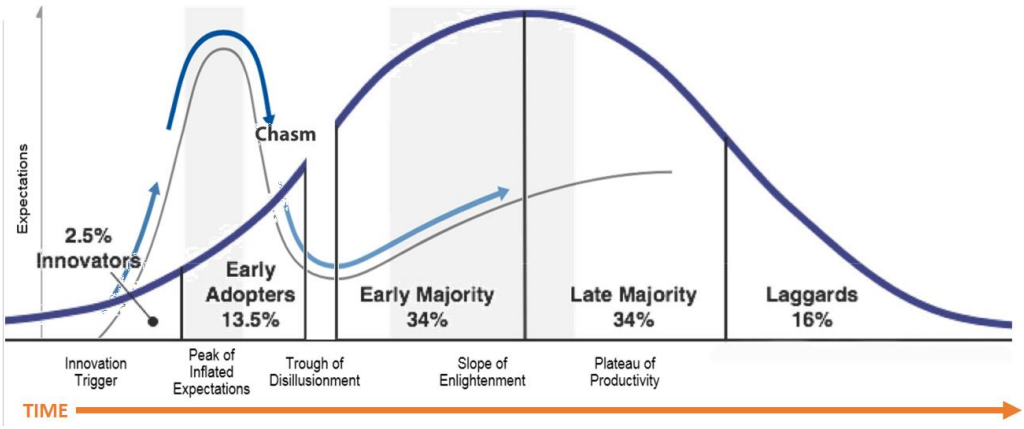


Figura 8: Rappresentazione delle fasi dell'Hype Cycle di Gartner in parallelo al modello di Rogers-Moore

Il modello serve alle aziende per comprendere quando è meglio investire in una determinata tecnologia. In particolare vengono evidenziate cinque fasi temporali caratterizzate da informazioni divulgate differenti.

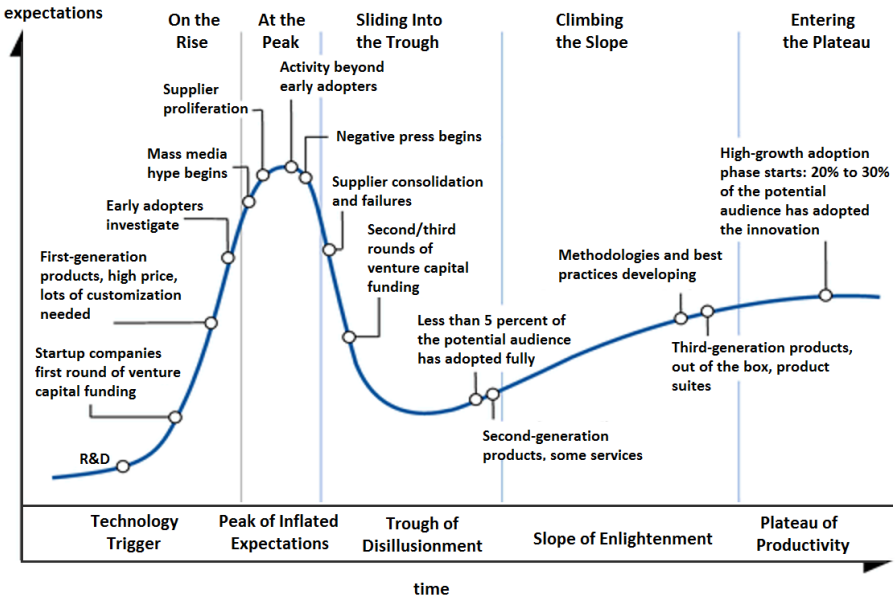


Figura 9: Cinque fasi e relative informazioni divulgate

Le fasi del modello sono le seguenti:

- **Trigger innovativo**: fase che ha come origine una qualsiasi messa in atto a livello pratico del modello. Da questo scaturisce una attenzione quasi esplosiva per la nuova tecnologia legata soprattutto a fattori mediatici. Gli investitori di capitale corrono per accaparrarsi la posizione di first mover, per ottenere i vantaggi connessi a questa qualificazione sebbene non ci siano ancora dei prodotti utilizzabili e una legittimità commerciale.

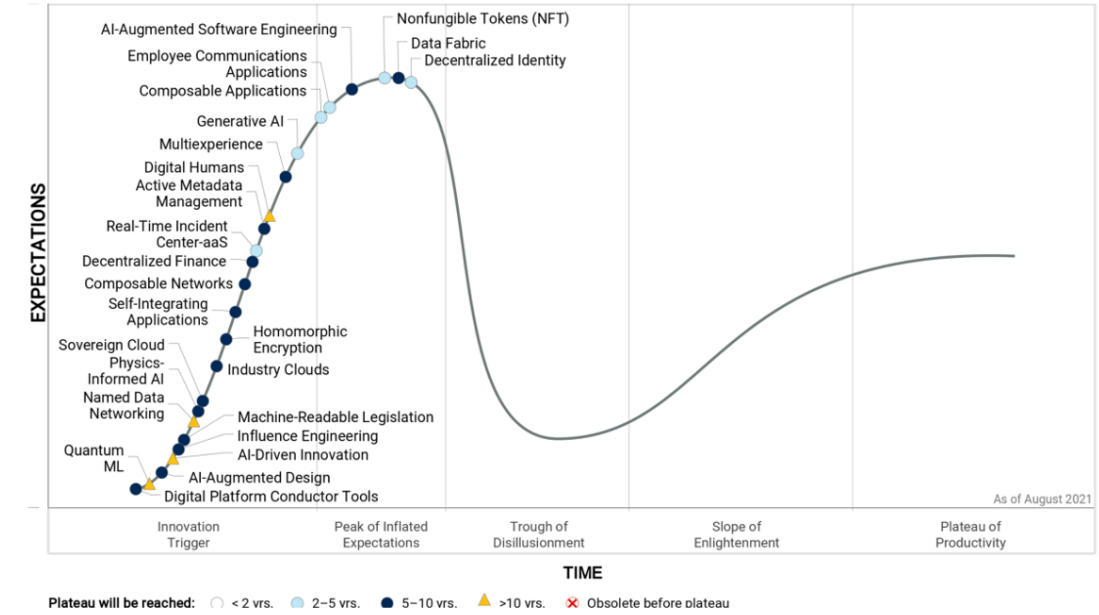
- **Picco delle aspettative sovradimensionate**: la copertura pubblicitaria iniziale si concentra essenzialmente sul successo generato dall'interesse dei media, che sono in grado influenzare positivamente i consumatori. Iniziano ad agire alcune imprese, che a volte, proprio basandosi solo su questo iniziale interesse diffuso, brancolano più o meno al buio, muovendosi senza una chiara strategia di business, mentre altre iniziano a disinteressarsene.

- **Bacino della disillusione**: svanisce l'interesse nei confronti della tecnologia in questione, e questo quando non vengono prodotti risultati consistenti e prospettati rispetto alle informazioni prodotte dalle aspettative gonfiate. Sopravvivono solo quelle aziende che si sono rivelate in grado di soddisfare i bisogni degli utenti iniziali (innovators e parte di early adopters), mentre le altre possono pervenire allo stato di fallimento. Si ha perciò una disillusione data dalla pubblicità negativa dai media in seguito alle vicissitudini e alla maturità che si è acquisita.

- **Inclinazione dell'illuminazione**: si iniziano a gettare le fondamenta della nuova tecnologia, analizzando più nel dettaglio come le aziende possano trarne beneficio. Queste creano via via degli upgrades della tecnologia, migliorando le performance grazie anche all'apporto sempre più consistente dei finanziamenti.

- **Altopiano della produttività**: si ha l'apprezzamento continuo da parte dei consumatori e la convalida delle applicazioni di successo per il mercato. L'adozione della tecnologia aumenta. Gartner prevede nella curva fra quanti anni si tenderà a raggiungere il plateau per ogni tecnologia presa in esame.

Questo modello, specialmente l'ultima fase, "ricalca" il discorso fatto in precedenza sulle applicazioni delle diverse tecnologie, cioè che non basta focalizzarsi sul suo successo tecnico ma anche sul suo ambito applicativo.



Source: Gartner (August 2021)
747576

Figura 10: Hype Cycle aggiornato ad Agosto 2021

2. LA BIOMETRIA

Il termine “biometria” deriva dalle parole greche *bios* (vita) e *metros* (conteggio), e rappresenta la scienza che studia le misurazioni di variabili fisiologiche o comportamentali tipiche degli organismi umani.
La biometria dunque è il settore della biologia che cerca di misurare e studiare statisticamente i dati rilevati, per estrapolarne comparativamente classificazioni e leggi.
Permette l’identificazione dell’individuo andando ad analizzare “una cosa che sei”, cioè parti del corpo o comportamenti dell’utente; utilizzata soprattutto in ambiti di sicurezza informatica in quanto è uno strumento capace di verificare l’identità.

2.1 **La storia della biometria**

Nel 1882, Alphonse Bertillon (1853-1914), capo del servizio di identificazione della polizia di Parigi, introdusse un nuovo sistema di misurazione corporea basato sull’altezza, sulla lunghezza delle braccia, dei piedi, delle dita di tutti gli arti. Questo metodo venne approntato appositamente per riuscire a dare un identikit dei criminali.

Figura 11: Misurazione di Bertillon

Il tutto partì dalla curiosa coincidenza data dal fatto che due uomini, detenuti a pochi anni di distanza nel penitenziario di LeavenWorth (Kansas-USA), possedessero misure molto simili, se ci si basava su quanto ideato da Bertillon. Su tale sistema si pronunciò Francis Galton. Quest’ultimo era un antropologo ed esploratore britannico, che aveva concentrato parte della sua carriera sullo studio delle impronte digitali e sulla loro classificazione. Il metodo di identificazione tramite impronte digitali era stato già introdotto da William James Herschel nel 1860, e il suo uso in ambito criminale e giudiziario già proposto da Henry Faulds nel 1880. Ma fu grazie alle ricerche di Galton che si riuscì ad impostare su base scientifica lo sviluppo e le applicazioni di tale metodo, favorendone di conseguenza l'effettiva e concreta adozione nelle aule giudiziarie.

Francis Galton criticò il sistema di Bertillon essenzialmente da un punto di vista statistico. Nel 1892 introdusse la nozione di minuzia, e suggerì un primo sistema di classificazione di impronte molto semplice.
Nel 1893, l'Home Ministry Office in Inghilterra, statuì che non potessero esistere due individui possedenti la stessa impronta digitale. In seguito a questa affermazione, nacque il sistema conosciuto come "Sistema Galton-Henry", risalente al 1900.
L'apporto dato dagli studi di Galton permise di stabilire che le serie di composti segmenti curvilinei, di cui sono formate le impronte digitali, conferiscono carattere sia di permanenza nel tempo, dal momento che sono tendenzialmente immutabili, sia di unicità dell'impronta, poichè appartengono solo al soggetto di riferimento.
Gli studi di Henry, invece, portarono alla prima schematizzazione della struttura globale di un'impronta digitale.
Dato però il processo lungo e costoso per l'identificazione manuale, già nel 1960, le polizie di Parigi e di Londra misero in atto le prime prove che permisero di realizzare un sistema, di per sè automatico, che consentisse il riconoscimento delle impronte digitali.
Questi studi ricevettero un notevole apporto, nel 1969, dall'FBI americana, che investì in essi.

Grazie agli studi sulle impronte digitali poi nacquero gli altri metodi di riconoscimento biometrico che conosciamo oggi, e che qui di seguito verranno analizzati.
Infatti, attualmente, le tecniche biometriche di identificazione sono adoperate in diversi ambiti, tra cui troviamo:

- Controllo degli accessi e conseguente controllo delle presenze;
- Identificazione di sicurezza, come avviene ad esempio giornalmente negli aeroporti;
- Avviamento dei veicoli (ancora in fase di studio);
- Accesso e sblocco pc/telefono;
- Autenticazione remota attraverso internet;
- Transazioni bancarie;
- Protezione e scambio sicuro di documenti (firma elettronica);
- Verifica documenti;
- Controlli per gli esami;
- Assistenza alla clientela.

2.2 **I metodi di identificazione**

Per essere riconosciuti, si utilizza il metodo con:

- Un fattore;
- Multi-fattore (MFA): a sua volta scorporabile in:
    a) Due fattori appartenenti a due bolle differenti (2FA);
    b) Tre fattori appartenenti a tre bolle differenti (3FA).

Al giorno d'oggi si sta espandendo l'utilizzo della biometria come metodo di riconoscimento dell'identità al fine di aumentare i livelli di sicurezza. Per proteggersi, infatti, esistono diversi modi per fare ciò tra cui la biometria che, specialmente in questi anni, si sta sempre più espandendo.

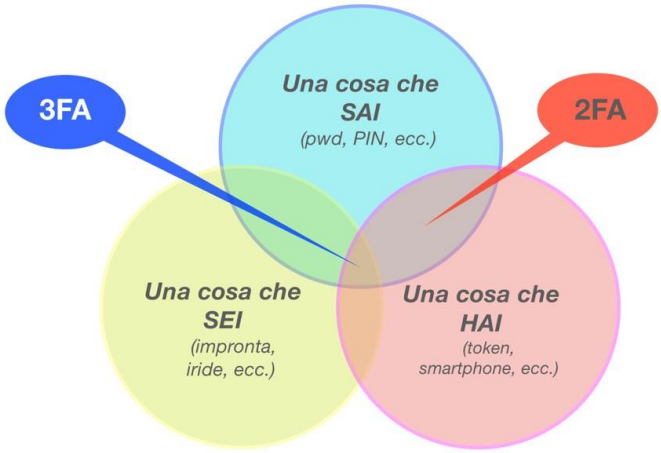


Figura 12: Tipologie di fattori di riconoscimento

2.2.1 **Le password**

Le password vennero utilizzate per la prima volta negli anni 60 del secolo scorso, dai primi utenti di computer, formati in larga parte da accademici e specialisti. All'epoca non vi erano tutte le credenziali dei vari account che è richiesto di ricordare a noi oggi, e non c'erano d'altronde così tanti criminali informatici, il cui scopo è ottenere l'accesso, illecitamente, ad esse.
I sistemi, a quei tempi, non erano così interconnessi con le reti globali, come invece siamo abituati a pensarli oggi.

Questi fattori, associati anche ad una remota e superficiale conoscenza richiesta per il loro utilizzo, comportavano delle lacune non indifferenti, la cui conseguenza era un facile accesso alle informazioni che avrebbero dovuto essere coperte dalla sicurezza informatica e da una tipica irrilevanza per le preoccupazioni inerenti l'utente.

Oggi viviamo in una società caratterizzata da una sfiducia sempre crescente nei confronti degli altri. Questo clima è dato anche dal fatto che ci sia un numero via via maggiore di malintenzionati che rendono gli attuali metodi di identificazione basati su documenti cartacei (come la carta di identità o la patente di guida) facilmente contraffabili.
Questo rappresenta uno dei primi limiti del sistema informatico, poiché non è in grado di riconoscere, con assoluta affidabilità, se l'utente a cui viene concesso un certo diritto è effettivamente lo stesso soggetto che ne sta usufruendo.

Al mondo vivono circa 7 miliardi di persone, e molte di esse sono occupate nel comparto del lavoro digitale. Gli utenti devono accedere a decine o addirittura centinaia di account personali e aziendali. Siamo ormai abituati, nelle azioni di tutti i giorni, a dover memorizzare numerose password (relative

a carte di credito, accesso a porte, controllo del computer di bordo delle auto...), al punto che si stima che gli utenti abbiano una media di 21 password a testa. Secondo uno studio condotto sugli utenti del web, inoltre, è emerso che l'81% impostano una password di facile individuazione, che la maggior parte delle volte è data dalla combinazione del proprio nome e della data di nascita e solo il 30% annota le proprie password.

Figura 13: Combinazioni di password più utilizzate a livello globale

Dall'immagine sopra riportata si nota soprattutto che le password non sono caratterizzate da un'elevata difficoltà di rilevazione, e questo è anche dovuto al fatto che sono necessari sempre più codici per accedere, ad esempio, ad un portale.

Un'autenticazione basata solo su password è dunque decisamente debole, anche se la stessa password impostata possiede un alto livello di sicurezza, essendo formata da caratteri di diversa natura, ossia non solo da lettere, ma anche da numeri e simboli.
Con l'obiettivo di accrescere tale sicurezza aziendale, e di conseguenza anche quella personale, è sempre più diffusa la consapevolezza di dover rendere più difficile e impegnativo l'accesso agli account e ai dati aziendali, tramite l'utilizzo di metodi di riconoscimento biometrico.

Oggi giorno, visto l'evolversi ininterrottamente del mondo tech, si cerca in maniera esponenziale di trovare la combinazione giusta di protezione, sviluppando diverse soluzioni, alle volte date dall'unione tra le stesse:

1. Qualcosa che l'utente conosce («*una cosa che sai*»);
2. Qualcosa che l'utente ha («*una cosa che hai*»);

3. Qualcosa che l'utente conosce + qualcosa che l'utente ha (ad esempio, token + password);
4. Qualcosa che l'utente è o fa («*una cosa che sei*»);
5. Qualcosa che l'utente ha + qualcosa che l'utente è (ad esempio passaporto biometrico);
6. Qualcosa che l'utente conosce + qualcosa che l'utente è o fa;
7. Qualcosa che l'utente conosce + qualcosa che l'utente ha + qualcosa che l'utente è o fa.

Nonostante l'interesse sempre più diffuso e pregnante nei confronti di questi metodi di riconoscimento e di identificazione, la tecnologia si sta espandendo ad una velocità tale che anche solo usare i dati biometrici si sta rilevando non tanto sicuro. Ecco perché ci si sta anche approcciando alla combinazione di diversi sistemi biometrici sebbene si diminuisce l'esperienza utente dato che ogni volta dovrà compiere almeno il doppio delle azioni che svolgeva in precedenza.

2.2.1.1 **L'aiuto alla quotidianità** (e memoria!)

Vista la molteplicità di password utilizzate, cosa potrebbe semplificare la nostra vita, e aiutarci a non scordare le nostre chiavi di accesso?
Per fortuna è stata approntata per rispondere a questa esigenza la figura del «**password-manager**», ossia un software progettato per rendere più facile la fruizione e il ricordo delle varie password agli utenti finali.

Generalmente l'applicazione è protetta da una password principale, che permette in seguito di recuperare i singoli username-password, indipendentemente dal sito o applicazione. Questa però può anche rappresentare un'arma a doppio taglio, poiché al malintenzionato di turno sarà sufficiente **scoprire** quell'**unico codice** «primario» per poter così accedere in maniera molto semplice a qualunque altro nostro account.

Tra le tante aziende che si occupano di ciò, se ne evidenziano due:

- *PasswordBox*, finanziata per 8.5 milioni di dollari e in seguito acquisita nel 2014 da *Intel*. Utilizza una o più password generali che permettono di accedere al programma in cui sono registrate tutte le altre. È possibile usufruire della biometria per proteggersi ulteriormente dai truffatori, ma solo su quei dispositivi cellulari che possiedono già la combinazione di hardware e software fornita dal produttore del telefono per identificarsi. Quindi, per l'accesso attraverso i personal computer rimane l'utilizzo di combinazioni di lettere e numeri.

- *LastPass*, acquisita nel 2015 per 110 milioni di dollari da *LogMeIn*. Offre, oltre al fatto di memorizzare le password come sopra, anche la possibilità di usufruire della sua "cassaforte online" per registrare documenti sensibili come carte di credito, passaporto. Tutto questo in un'ottica di aumentare l'esperienza online dell'utente, così da non creargli degli ostacoli e rendere fluido il suo trascorso su internet.

Bisogna quindi che il singolo utente decida quale sia per lui, tra le alternative che gli si pongono, il male minore, valutando se propendere maggiormente per una semplificazione degli accessi o se intraprendere la strada più lunga, trascrivendosi personalmente le password e non rischiando così che queste possano essere scoperte.

2.2.2 **Le caratteristiche della biometria**

Partendo da un discorso generale sulla biometria, possiamo distinguere alcuni vantaggi e svantaggi. Iniziando dall'analisi dei primi, si nota che i metodi di riconoscimento sono facili e veloci da usare, poiché vanno ad identificare una caratteristica che ognuno di noi possiede, impiegandoci solo pochi istanti (ad esempio agli smartphone sono sufficienti pochissimi secondi per riconoscere un'impronta digitale).

La base di partenza di ogni sistema di riconoscimento biometrico è una caratteristica pressoché univoca in ogni essere umano, e ulteriore difficoltà per il malintenzionato è data dal fatto che esso debba essere vicino alla vittima, per poter essere in grado di raccogliere le informazioni necessarie a bypassare il login. Caso recente e concreto mostra come sia anche solo sufficiente possedere degli ottimi modelli sostitutivi, e mi sto riferendo a quanto accaduto con l'impronta digitale di Ursula Von Der Leyen: "*Jan Krissler, noto anche con il suo alias «Starbug», ha dichiarato a una conferenza di hacker di aver copiato l'impronta del ministro della Difesa tedesco Ursula von der Leyen. Krissler, usufruendo diverse foto a distanza ravvicinata per catturare ogni angolazione, ha utilizzato un software disponibile in commercio per creare un'immagine dell'impronta digitale del ministro*"[11].

Facendo un focus sulla biometria basata sul comportamento, piuttosto che sulla fisionomia, potrebbe risultare un notevole passo avanti per via della sua maggiore resistenza alla rappresentazione e della sua vulnerabilità sensibilmente ridotta in relazione alle problematiche relative alla privacy.

Per quanto riguarda gli svantaggi, invece, causati dall'uso dei metodi di riconoscimento biometrico si nota come sia possibile trarre in inganno gli scanner, dato che non si avrà mai una corrispondenza al 100% in fase di riconoscimento con l'impronta biometrica registrata sul database sotto forma di codice binario (esistono degli errori di prima e di seconda specie, chiamati FRR e FAR).
Lo svantaggio più rilevante è quello che si riscontra in caso di "furto" della caratteristica in esame, poiché non è possibile modificarla a piacimento, come invece può avvenire per le password.
Altra difficoltà è rappresentata dalla circostanza che alcune persone possiedono delle menomazioni fisiche o delle disabilità, e quindi per loro il riconoscimento risulterà essere più complesso ed articolato.

[11] Citazione presa dal giornale online DW-Made for Minds. https://www.dw.com/en/german-defense-minister-von-der-leyens-fingerprint-copied-by-chaos-computer-club/a-18154832

Andando più nel dettaglio di quelli che sono i rischi legati alla biometria, si può trovare:

- **Privacy**: essendo considerati dati personali sensibili, i dati biometrici e i diritti di privacy delle persone devono essere protetti secondo la normativa sulla privacy.

- **Prestazioni**: le prestazioni nel mondo reale di ogni modalità biometrica possono dipendere da una varietà di fattori. Per esempio, con il riconoscimento del volto, una scarsa illuminazione ambientale e una scarsa qualità della fotocamera rendono più arduo il processo di cattura delle immagini utilizzabili. Tuttora, infatti, gran parte dei nuovi brevetti sviluppati dalle aziende, hanno come obiettivo quello di migliorare le tecnologie in questa direzione.

- **Attacchi di presentazione**: l'autenticazione biometrica si basa sulla difficoltà di replicare la caratteristica di un umano. Quindi, un metodo biometrico robusto deve incorporare un efficace rilevamento dell'attacco di presentazione (PAD) o "liveness testing" (introducendo funzionalità anti-spoofing) per mitigare questo rischio, cosa che oggi si cerca sempre più di migliorare.

- **Attacchi alla piattaforma**: ci sono rischi significativi correlati alla sicurezza end-to-end di qualsiasi piattaforma di autenticazione biometrica. I leader della sicurezza devono valutare i punti deboli e i rischi dati dalla progettazione, costruzione, funzionamento, uso improprio o configurazione errata della piattaforma stessa.

2.2.3 **I parametri di valutazione**

I parametri di valutazione della biometria sono i seguenti:

1) Accuratezza con cui vengono analizzati i valori di frequenza al verificarsi di determinati eventi, come quelli riportati dei falsi riconoscimenti.
   Ci sono due tipologie di errore, strettamente correlate al fatto che con il diminuire di uno cresce l'altro, portando a una sensibile modifica del sistema:

   - **FRR** (False Rejection Rate): è la percentuale di falsi rifiuti [errore di prima specie], cioè rappresenta gli utenti che sarebbero autorizzati ma che erroneamente vengono respinti, poiché a soggetti che sarebbero davvero titolari di questo diritto, esso gli è negato;
   - **FAR** (False Acceptance Rate) rappresenta la percentuale di false ammissioni [errore di seconda specie], cioè utenti non autorizzati ma che vengono comunque accettati.

   Il **grado di tolleranza del sistema,** che serve a definire l'accuratezza dello stesso in termini di sicurezza, è dato dalla variabile t. Questa variabile può assumere diversi valori:

   - Con t basso vi è un alto FRR (=numero elevato di falsi rifiuti);

- Con t alto vi è un alto FAR (=numero elevato di false accettazioni).

Una volta definito t, è possibile costruire le funzioni FAR(t) e FRR(t) che ci permetteranno di calcolare l'**ERR** (Equal Error Rate) cioè l'errore intrinseco del sistema, per cui FAR(t*) = FRR(t*) = ERR, cioè il punto di equilibrio del sistema. Ad esempio, nel momento in cui si entra in una banca, e si supera il primo tornello, per non far sprecare tempo ai controlli ai clienti, è opportuno impostare su "alto" il rischio di accettazioni false. Al contrario, per l'accesso ai caveau si ritiene più utile tenere in considerazione un aumento del rischio di falsi rifiuti per far sì che ci sia un elevato grado di sicurezza, riducendo al minimo le false accettazioni.
Nella realtà si trovano dei valori di tolleranza al di sotto di t*, al fine di ottenere un basso numero di false accettazioni. All'aumentare dell'accuratezza della selettività del riconoscimento, aumenterà la probabilità che una persona autorizzata venga respinta.

2) Resistenza a false caratteristiche biometriche, quindi lo studio della vivacità delle stesse;

3) Resistenza a manomissioni del dispositivo;

4) Robustezza in fase operativa in modo tale da riuscire a sopravvivere anche nelle condizioni che presenta la realtà, ossia in tutte quelle situazioni non ottimali di utilizzo (ad esempio eventuali rumori improvvisi nel caso di riconoscimento vocale);

5) Robustezza in fase di acquisizione, ossia quando il soggetto da cui viene assunta la caratteristica non si trova nelle migliori condizioni per effettuare il riconoscimento sotto l'aspetto della tipicità delle situazioni in cui di norma si verifica il riconoscimento;

6) Sensibilità all'instabilità della caratteristica biometrica (non tutte le tecniche ne risentono);

7) Eventuali problemi con alcune tipologie di soggetti (ad esempio se si volesse adottare il riconoscimento delle impronte digitali, non va bene per chi esegue molti lavori manuali data la possibile rovina dei polpastrelli);

8) Usabilità, cioè capire il livello di gradimento nell'utilizzare il metodo di riconoscimento preso in considerazione;

9) Accettabilità, cioè il livello di gradimento nel sottoporsi al riconoscimento biometrico;

10) Varie (costo, occupazione di spazio, dimensione del template [=dati caratteristici e codificati ottenuti dalle feature uniche di un esempio biometrico], possibilità di integrazione, adattabilità).

2.2.4 **Le tecnologie biometriche**

Per quanto riguarda le tecnologie esistenti nell'ambito del riconoscimento biometrico, si possono identificare due macro-gruppi e suddividerli in diversi metodi:

- **Fisiologiche**, possedute da tutti gli esseri umani. Queste comprendono:
    1. Impronte digitali;
    2. Iride;
    3. Retina;
    4. Geometria della mano;
    5. Geometrie delle vene della mano;
    6. Fisionomia del volto;
    7. ECG.

- **Comportamentali**, cioè quelle derivanti dal nostro modo di approcciarsi alle cose. In questa categoria sono ricomprese:
    1. Impronta vocale parlatore;
    2. Scrittura grafica - Firma grafometrica;
    3. Stile di battitura sulla tastiera e movimento del mouse;
    4. Camminata.

Per l'identificazione personale ci sono certi elementi considerati essenziali, affinché queste caratteristiche, fisiologiche o comportamentali che siano, possano essere utilizzate per il riconoscimento biometrico:

- Universalità (caratteristica presente in ogni individuo);
- Unicità (livello di condivisione del medesimo carattere biometrico);
- Permanenza (la caratteristica biometrica deve rimanere quasi immutata nel tempo);
- "Catturabilità" (nel senso che la caratteristica biometrica deve poter essere misurata quantitativamente);
- Facilità di utilizzo;
- Precisione;
- Percezione pubblica positiva.

Tutti i dispositivi utilizzati per il riconoscimento biometrico sono composti da una fase prima di addestramento, detta anche "*enrollment*". In questa fase il sistema procede con una identificazione delle caratteristiche biometriche del soggetto da riconoscere, salvandole nella memoria del database del sistema in forma di template.
Nella fase preliminare di addestramento, l'utente che sarà inserito nel sistema verrà identificato, e successivamente, tramite il sensore (scanner, telecamere, microfoni, ecc…), si acquisirà una sua immagine o un suono, che sarà ricollegato al tratto biometrico dell'individuo. In questa fase è

essenziale una buona qualità dei dati acquisiti, per permettere il pieno e corretto svolgimento dei successivi step di autenticazione.
Proprio per far sì che questo procedimento dia risultati ottimali, può rendersi utile consultare personale specializzato, affinché questo dia indicazioni agli utenti.
I dati rilevati dal sensore sono in seguito elaborati per il tramite di un algoritmo, che estrae le caratteristiche necessarie. Quest'ultimo varia da sistema a sistema, creando un'impronta biometrica chiamata «*biometric template*». Il template, da ultimo, sarà memorizzato nel sistema, cosicchè possa in seguito essere utilizzato come base di riferimento per tutte le fasi di riconoscimento che seguiranno.
La fase seguente è quella di autenticazione vera e propria, in cui viene posta a confronto la nuova impronta biometrica con quella registrata a sistema.

La fase di autenticazione si compone di due metodi alternativi:

- Il **processo di verifica**, 1:1, si ha quando il soggetto dichiara la sua identità. Si effettua un raffronto tra il template presente nel database e l'immagine acquisita in tempo reale.

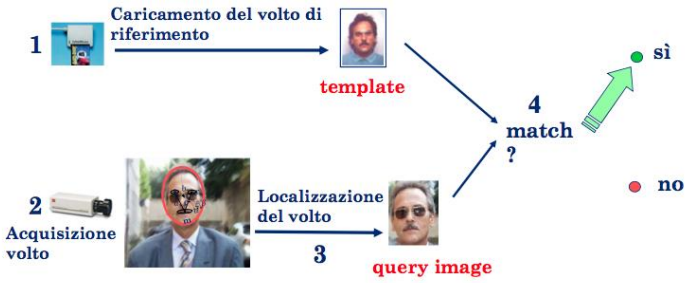


Figura 14: Caso di verifica

- L'**identificazione**, 1:n, si ottiene tutte le volte in cui la figura, che si è ottenuta con l'elaborazione in tempo reale, viene posta a confronto con le immagini già memorizzare nel database di riferimento. Questa figura, successivamente, verrà riportata tramite l'associazione a quelle che sono risultate ad essa più simili.

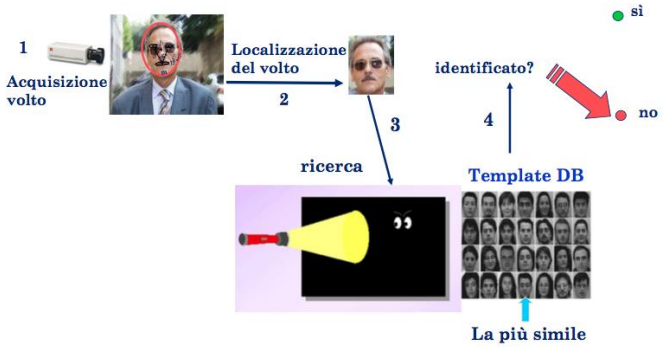


Figura 15: Caso di identificazione

Quali possono essere i moduli di identificazione? Prettamente, sono presi in considerazione cinque moduli:

- Il **sensore**, preposto ad individuare un dispositivo di input, come può essere lo scanner, le fotocamere, il microfono, permette di rilevare l'immagine o il segnale proprio della variabile biometrica.

- Il **modulo di estrazione** delle caratteristiche, che ha il compito di svolgere una elaborazione dell'immagine oppure del segnale che il sensore ha ottenuto, esportando le caratteristiche ritenute necessarie.

- Il **modulo di confronto** delle identità, che esegue la comparazione tra le due immagini (una acquisita e una già memorizzata) restituendone una misura di somiglianza

- Il **decisore,** che basandosi su una soglia precedentemente fissata dal sistema elaborerà una decisione booleana. In questa fattispecie, si otterrà un responso positivo se la misura di somiglianza è minore o uguale alla soglia, e negativa nel caso contrario.
  Se, al contrario, ci troviamo a doverci rapportare con il sistema di identificazione, dobbiamo mettere in conto la possibilità che il decisore ci dia come risultato finale una misura di somiglianza relativamente minore della soglia.

- Il **database,** contiene tutti i modelli dei dati, anche detti templates, su cui ci si baserà per porre in essere il confronto. Sovente, però, quando ci si accinge ad iniziare la progettazione di un sistema, si può incorrere in un problema di base, ossia quello che riguarda propriamente la fase di scelta del tipo di supporto e di struttura utilizzati per la memorizzazione dei dati, dal momento che il riconoscimento si basa sul confronto dei dati biometrici relativi al soggetto di riferimento con quelli memorizzati nel database.

Analizzando più nello specifico quale soluzione biometrica sia meglio adottare, si cerca di rispondere alle seguenti domande relative al bisogno che si vuole soddisfare:

- L'applicazione necessita di un percorso di identificazione o di riconoscimento?
- Qual è il livello di automazione del processo (semiautomatico o completamente automatico)?
- Ci si può basare sulla capacità di adattamento degli utenti, confidando in una loro facile accettazione della tecnologia di riferimento scelta?
- Qual è lo spazio di memoria richiesta? (ogni differente applicazione impone di fissare dei limiti, relativi alla grandezza dei caratteri biometrici in questione all'interno della rappresentazione stessa)

- Quanta rigorosità è richiesta nell'identificazione/autenticazione? (E' chiaro che più l'applicazione richiede un alto grado di precisione e più è necessario individuare caratteristiche biometriche uniche).

2.2.4.1 **Il riconoscimento fisiologico**

L'impronta digitale

Il metodo che viene considerato universalmente come il più antico e noto per riuscire a fissare l'immagine relativa alle impronte digitali è quello che utilizza l'inchiostro, il quale viene applicato sui polpastrelli dei soggetti che sono da analizzare, mettendo così nero su bianco l'impronta, paragonabile a un vero e proprio timbro.
Risultati migliori si possono ottenere utilizzando sistemi digitali come, ad esempio, l'acquisizione dell'immagine attraverso una microcamera, che realizza una scansione (scanning) dell'impronta digitale. Anche in questo caso, però, non è infrequente che si ottengano immagini distorte, date da cause naturali, quali ad esempio la secchezza della pelle, sudore, sporco o umidità.

Ritornando al metodo in questione, ci sono tre tipi di scanner di impronte digitali: ottico, capacitivo e a ultrasuoni.

- Scanner **ottico**: focalizza l'immagine su un sensore di visione, basandosi sulla legge di riflessione per produrre immagini ben contrastate;
- Scanner **capacitivo**: si parte da piastrine di silicio contenenti una matrice di piccoli sensori, che leggono le informazioni sulla corrispondente porzione di impronta;
- Scanner **a ultrasuoni**: sfrutta onde sonore che colpiscono la superficie del dito, e dall'eco si ricavano le informazioni sulle creste e sulle valli che costituiscono in maniera assolutamente naturale il nostro polpastrello.

Una volta acquisita l'immagine dell'impronta digitale, si può procedere a dare luogo ad elaborazioni elettroniche ed informatiche (c.d. "*fingerprint image processing*"):

1. **Riconoscimento degli aspetti**: l'impronta in questione viene raffigurata come una sequenza alternata di segmenti, che sono a loro volta costituiti da *solchi* e da *valli*, separati da intervalli di discontinuità. Questi tratti caratteristici sono detti *minutiae* (terminazioni, biforcazioni delle creste).

2. **Classificazione delle impronte**: per poter effettuarne una classificazione sono prettamente seguiti questi metodi:

    - sintattico (syntactic approach);
    - strutturale (structural approach);

- rete neurale (neural network approach);
- statistico (statistical approach);

3. **Confronto tra impronte digitali**: si tratta di un procedimento che porta a comparare e misurare la similitudine tra il template attuale con quello registrato.

Passiamo ora ad analizzare più nel dettaglio quali sono le caratteristiche strutturali più evidenti dell'impronta digitale. Tra queste troviamo le *creste*, ossia linee in rilievo, e le *valli*, cioè gli spazi tra quelle stesse linee, che scorrono in flussi paralleli e che sporadicamente si intersecano o si interrompono, dando così origine ai noti disegni dell'impronta digitale che chiunque comunemente può osservare.

- A **livello globale**, lo schema di creste-valli mostra una o più regioni, caratterizzate ciascuna da una forma particolare, che costituiscono delle zone uniche e singolari per ognuno di noi. Inoltre, la loro presenza permette la classificazione dell'intera impronta in una delle cinque classi, qui di seguito elencate:

  - *Right Loop*: si tratta di impronte che hanno una o più creste che entrano dal lato destro, si ripiegano e in seguito fuoriescono dallo stesso lato.
  - *Left Loop*: rappresentazione come le precedenti, ma piegate verso il lato opposto;
  - *Arch*: sono impronte che hanno le creste entranti da un lato, crescenti in direzione del centro, e che infine usciranno dal lato opposto.
  - *Tented Arch*: riguarda impronte che possiedono lo stesso andamento di quelle appena descritte sopra, ma la particolarità qui è data dal fatto che le creste formano un angolo o una piega nella parte centrale;
  - *Whorl*: siamo in presenza di un'impronta caratterizzata dalla figura chiusa, che può assumere forma circolare, ellittica o a spirale.

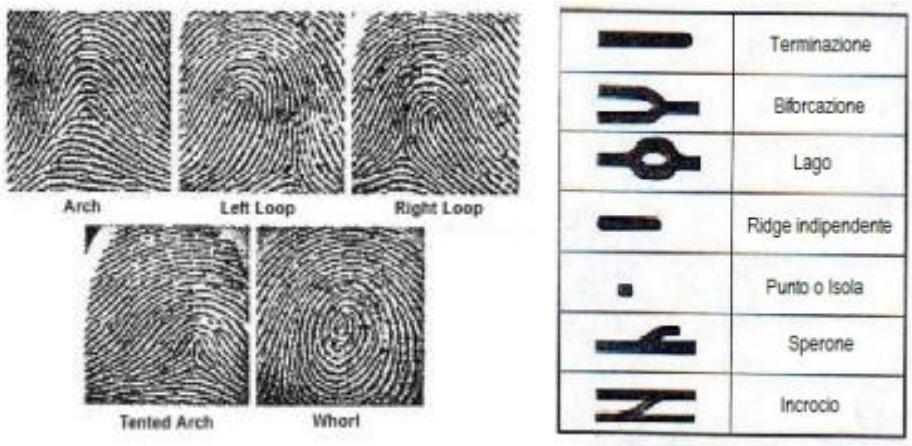


Figura 16: Rappresentazione delle diverse impronte con annesse tipologie di biforcazioni e incroci

- A **livello locale,** le discontinuità delle creste vengono denominate *minuzie*. Con questo termine ci si riferisce alle terminazioni o biforcazioni delle creste. Andando ad osservarle nel dettaglio ci permette di poter descrivere la loro forma il più dettagliatamente possibile, poiché a distinguere le une dalle altre sono minimi dettagli, come *minuzie a forma di punto o isola, lago, biforcazione e speroni, incroci*. È proprio grazie a queste caratteristiche che è facilitata la comparazione tra diverse impronte digitali. Inoltre, questo raffronto rappresenta una via certa per poter identificare un determinato individuo, dato il carattere di invariabilità delle impronte digitali nel corso della vita di un soggetto, a meno di sopravvenienze esterne e cause di forza maggiore.

L'impronta digitale come metodo di riconoscimento gode di alti livelli di unicità e di gradimento da parte del pubblico, oltre che di permanenza nel tempo. Purtroppo però, data la letteratura storica a cui è associato tale metodo, vi è anche una concezione negativa ad esso collegata, in quanto rimanda a rapporti effettuati sui criminali. Inoltre, essendo parte delle mani, può subire dei danneggiamenti a causa di lavori manuali o per menomazioni.

Un vantaggio, comunque, della tecnologia presa in esame è dato dal fatto che essa goda di un basso costo e, soprattutto, di un'alta rapidità nell'elaborazione della risposta, grazie in special modo al livello avanzato di sviluppo della tecnologia stessa, anche se è necessario avere le mani pulite affinché non ci siano dei problemi con il riconoscimento. Purtroppo è fondamentale la cooperazione dell'individuo in quanto la posizione delle dita può intaccare il riconoscimento; cosa che può anche accadere con cambiamenti di umidità, temperatura, stagione, luce/sfondo non controllato. Per verificare la presenza di vivacità dell'user vengono usati dei moduli Reliable Presentation Attack Detection (PAD), ovvero anti-spoofing.

Per quanto riguarda lo sfruttamento della caratteristica dell'impronta digitale per il telefono, al fine di identificare/verificare l'identità di un individuo, possono esserci diverse realtà concrete: sensore presente sotto un tasto del cellulare (*Apple* e la sua acquisita *AuthenTec* ci hanno lavorato), sensore presente sotto lo schermo (*Isorg* e *Flexanable* ci stanno lavorando) oppure sensore/i presente/i ai lati del dispositivo (l'azienda *Touch biometrix* sta attualmente lavorando su questo ultimo punto).

Invece, luogo diverso dal telefono, aziende come *Touch Biometric* sta studiando l'apposizione del chip di verifica biometrica all'interno del mouse del computer affinché oltre ad identificare l'individuo appena si accende il pc, anche durante tutta la durata della sessione essendo praticamente obbligati ad usare il mouse per muoversi tra le finestre. Qualora non si utilizzasse il mouse, ad esempio se si tratta di un pc portatile, si inserisce il sensore al di sotto del touchpad come sta facendo *Synaptics*.

Essendo però obbligato il posizionamento del dito sul sensore vi è mancanza di igiene. In questo campo, specialmente dovuto alla pandemia da Covid-19, stanno aumentando le procedure di sicurezza personale, non richiedendosi più il tocco fisico ma bastando una scansione ravvicinata senza il tocco.

I dispositivi di acquisizione touchless possiedono una maggiore fruibilità, rispetto al tocco, combinando la praticità del riconoscimento facciale con la sicurezza dell'iride ottenuta mediante:

1. Distanza sensore-dito scelta liberamente;
2. Angolo di posa del dito scelto liberamente;
3. Processo di acquisizione rapido;
4. Feedback molto positivo dell'utente di facile comprensione.

Però attenzione perché servirebbe una maggiore potenza di calcolo e molto probabilmente un'istruzione dedicata.
In quest'ottica ci stanno lavorando alcune aziende come, ad esempio, *Diamond Fortress Technologies* la quale, attraverso il prodotto Onice, permette di sfruttare il riconoscimento dell'impronta digitale con l'uso della fotocamera del telefono quindi senza la necessità di un sensore presente all'interno del telefono. Questo è portato intrinsecamente dalle migliorie apportate di anno in anno da parte dei produttori dei cellulari in ambito di fotocamere.

Come esempio pratico che investe la nostra vita di tutti i giorni, possiamo prendere il TouchID di *Apple*, in cui viene solo memorizzata una rappresentazione matematica criptata dell'immagine dell'impronta.
Certo, è possibile hackerare un iPhone sfruttando i sensori TouchID, ma sussisterebbe anche la necessità di sfruttare un modello ottimo dell'impronta digitale del soggetto in questione.
Inoltre, nemmeno il sistema operativo del dispositivo ha l'accesso diretto ai dati delle impronte digitali, tanto meno un'app, grazie ad un software di sicurezza chiamato "Secure Enclave", che lavora tra i dati delle impronte digitali e il programma utilizzato per le richieste di scansione.

L’occhio

L’occhio è uno degli organi facenti parte l'apparato visivo, il cui compito è quello di utilizzare la luce e ricavarne delle informazioni. La stessa passa attraverso un sistema di lenti poste in sequenza:

- Cornea (stessa funzione di una lente);
- Cristallino (lente elastica con il compito di mettere a fuoco);
- Corpo vitreo (sostanza posizionata nella parte posteriore dell’occhio);
- Retina (area dove viene proiettata la luce messa a fuoco);
- Nervo ottico (parte del sistema nervoso centrale).

Osservando l’occhio umano si nota una superficie bianca che delimita un’area pigmentata detta iride. All’interno dell’organo si trova una sottile membrana, detta retina, che riveste la superficie interna dell’occhio.

L’iride

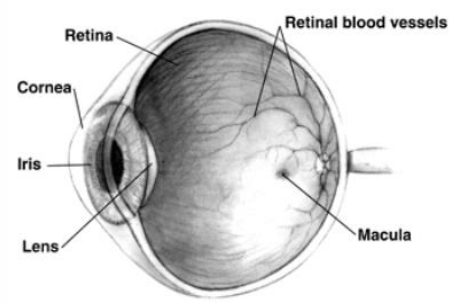


Figura 17: Anatomia dell’occhio umano

Osservando il bulbo oculare si nota una superficie bianca, detta sclera, che delimita un’area pigmentata, detta iride, la quale circonda la pupilla. Essendo una parte interna del corpo si utilizza un software in cui vengono isolate delle porzioni dell’iride e trasformate in elementi caratteristici dell’identità (template).

L’iride garantisce:

- Un altro elemento di unicità del soggetto, poiché si vanno a considerare solchi, creste, anelli, etc.
- Una pressoché stabilità nel tempo, anche considerando i disturbi ambientali e data anche la sua posizione dietro la cornea che la protegge, fatta eccezione per la risposta istintiva alla luce (anche se ci si sta muovendo in questo verso cercando di risolvere questo limite naturale dell’occhio per evitare compromissioni a livello di riconoscimento).
- Una semplice fruizione del riconoscimento, essendo una parte visibile.

- Un’alta universalità, dal momento che molte persone possiedono la caratteristica utilizzata dal sistema.
- Una precisione dodici volte maggiore rispetto le impronte digitali.

Sebbene la scansione dell’iride singolo abbia dei valori bassi di errori di seconda specie, ossia i FAR, ci sono aziende come *Eyelock* che sviluppano anche soluzioni in cui vengono scansionate contemporaneamente due iridi, facendo così tendere il FAR praticamente a zero.

I passaggi per l’identificazione sono:

1. **Acquisizione**: si cerca di catturare l’immagine con la qualità maggiore possibile, ponendo attenzione all’illuminazione circostante il soggetto in questione e alla posizione dell’utente nel momento in cui avviene la scansione.
2. **Localizzazione**: si cerca di delimitare i confini dell’iride.
3. **Confronto**: si confronta l’immagine appena acquisita con il template già inserito nei database.

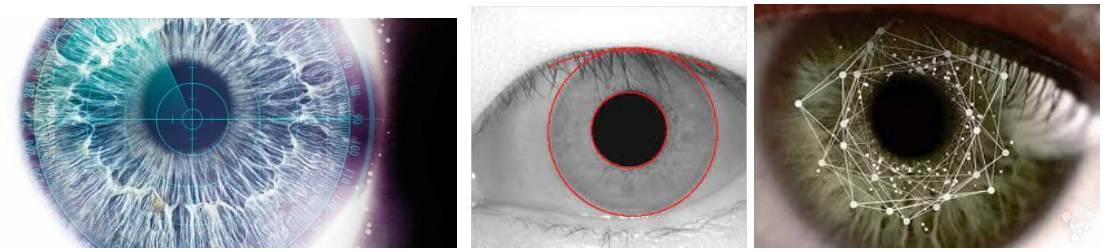


Figura 18: Iride umano e punti per le particolarità

Il metodo di riconoscimento dell’iride va a raccogliere, per poter procedere con l’identificazione, sei volte le caratteristiche considerate per l’impronta digitale, non andando a diffondere in giro informazioni ogni volta che si va a toccare un oggetto, possedendo anche delle performance molto elevate.

Fattore molto importante per la diffusione del metodo di riconoscimento è l'abbassamento dei prezzi dei sensori, dato che si sta sempre più cercando di utilizzare delle semplici telecamere senza un hardware particolare. Questo porta inoltre ad un'eliminazione di un vecchio svantaggio cioè quello legato alla fermezza nel momento di cattura dell'immagine andando ad aiutare soprattutto in contesti dove non vi è molta collaborazione.
Purtroppo però l'utilizzo di telecamere porta con sé una concezione non molto positiva da parte del pubblico, poiché spesso e volentieri viene vista come un tecnologia intrusiva.

Come anche per l'impronta digitale sopra esposta, anche qui vi è una particolare attenzione alla vivacità dell’utente. Infatti, gran parte dei nuovi algoritmi stanno affrontando questo argomento per garantire che l'utente che sta verificando la propria identità sia veramente lui e non un malintenzionato con una copia delle caratteristiche. Sempre nella stessa direzione, cioè di garantire

una migliore facilità e fruizione del riconoscimento, ci si sta muovendo per non provocare un errore nel processo a causa di occhiali, palpebre, ciglia, capelli, etc. Anzi, si sta cercando di utilizzare, anche se ancora poco oggi, le informazioni circostanti il bulbo oculare, con il fine di poter utilizzare, a scopo di sicurezza, caratteristiche aggiuntive.

Nonostante i grandi passi avanti fatti fino ad ora, sussiste un "problema" di base, cioè quello dato dalla possibilità di possedere delle immagini di alta qualità. Per di più, se si utilizzano delle telecamere, ci potrebbero essere dei problemi legati ai diversi formati delle riprese.

La retina

Il riconoscimento della retina offre un metodo preciso di identificazione dell'individuo attraverso l'analisi di un'immagine interna dell'occhio.
Studi eseguiti nel 1935 da due oftalmologi, Simon e Goldstein, portarono in evidenza come lo schema di vasi sanguigni presenti all'interno della retina, rendesse il riconoscimento biometrico della persona quasi impossibile da falsificare, garantendo una elevata unicità e una sostanziale stabilità nel tempo. Inoltre, è stato mostrato che possedeva una universalità unica, essendo presente in ogni individuo, a meno di menomazioni o disabilità dell'utente stesso.

Uno degli approcci che si usa per catturare l'unicità dei vasi retinici è quello di abbinare le biforcazioni agli incroci formati dalla struttura dei vasi sanguigni (come si è potuto notare già per le impronte digitali). Andando ad analizzare i punti di incontro e di biforcazione dello schema, si consente di non andare a visionare l'intera struttura ad albero dei vasi sanguigni.

Per il riconoscimento dello schema retinico viene utilizzato uno scanner, che lo illumina attraverso una luce ad infrarossi memorizzandone così il contrasto. Questo è un processo costoso che, oltre ad essere estremamente invasivo e con bassa utilizzabilità, presenta anche uno scarso consenso al suo utilizzo, a causa della percezione del pubblico che dovrebbe esservi sottoposto di correre il rischio di sviluppare negli anni a seguire dei problemi al bulbo oculare. Questo, purtroppo, rende il metodo di riconoscimento poco "user-friendly", costituendone uno dei principali limiti all'impiego.

Figura 19: Rappresentazione della scansione e retina dell'occhio

La geometria della mano

Uno dei più antichi metodi per verificare l'individuo è grazie all'analisi della geometria della mano.

Figura 20: Misurazione delle misure del palmo della mano

La tecnologia, apprezzata dagli utenti grazie alla facilità e praticità di utilizzo, alla bassa invasività e alla alta universalità, impiega una telecamera digitale per catturare la *silhouette* dell'immagine della mano.
Con ciò vengono calcolate alcune misure geometriche della mano dell'individuo (lunghezze, distanze, angoli, spessore del palmo, distanza delle nocche, ecc.) senza andare a considerare le minuzie e caratteristiche che presenta la superficie della pelle (ad esempio, le impronte digitali).

Le fasi di funzionamento del sistema sono:

- Addestramento: allenamento dell'user affinché posizioni correttamente la mano;
- Registrazione: si chiede all'individuo di posizionare un paio di volte la mano così da calcolare delle misurazioni medie che andranno a formare il template;
- Verifica: si verifica l'utente rispetto al modello presente nel database.

Il dispositivo risulta oggigiorno abbastanza ingombrante e privo di igiene (fattore importante soprattutto nel periodo pandemico causato dal covid-19). Proprio per motivazioni legate a queste tematiche si sta lavorando su questi punti, in modo tale da sfruttare delle telecamere che riconoscano le distanze senza che sia necessario il contatto diretto con lo strumento per il riconoscimento, cioè senza la necessità di usufruire né dei pioli né di una piattaforma per l'acquisizione dell'immagine della mano.

Figura 21: Scanner senza contatto

Inoltre, non vi è un costo eccessivo legato all'impiego di questa tecnologia, non vi è un intaccamento del riconoscimento dovuto a cicatrici o eventuale sporcizia sulla mano (non come con le impronte digitali) e non è richiesto uno spazio consistente per allocare il template (utile soprattutto quando siamo in presenza di un numero elevato di persone da riconoscere).

Anche se questa tecnologia è utilizzata da molti anni, è utile comunque far notare che si dibatte molto sull'aspetto dell'unicità, poiché vi è una bassa permanenza del template nel tempo, legata soprattutto all'elevato rischio che intercorrano, nella vita del soggetto da riconoscere, serie probabilità di menomazioni o disabilità all'arto. Di contro, però, è più difficile da falsificare, in quanto servirebbe un modello in tre dimensioni della mano.
Inoltre il metodo di riconoscimento risulta molto utile nei casi si condizioni ambientali più difficili dove altre tecnologie falliscono.

La vascolarizzazione della mano

Andando ad analizzare la mano nelle sue componenti interne, possiamo utilizzare, come sistema di riconoscimento, il suo schema sanguigno.

Figura 22: Scanner per le vene della mano e risultato finale

Mantenendo le fasi di funzionamento di prima si va, però, incontro ad un'alta stabilità nel tempo e un'alta unicità, tale che perfino due gemelli non possiedano lo stesso layout.

Essendo visibili solo in condizioni controllate, sono difficili da copiare e rubare. In particolare, viene utilizzata una luce ad infrarossi affinché le vene siano visibili. Inoltre, sembrerà ovvio, ma serve anche che ci sia il flusso fisico di sangue che rende ancora più complicata la duplicazione e/o falsificazione dello schema sanguigno.

Per di più il software di riconoscimento garantisce un'alta velocità di elaborazione, e non restituisce falsi positivi/negativi causati da eventuale sporcizia, lividi, calli, etc.
Nonostante i grandi vantaggi, si è davanti ad una tecnologia ancora non molto matura che porta anche con sé un alto costo dei dispositivi, spostando l'espansione più in là nel tempo.

La fisionomia del volto

Una caratteristica molto usata fin dal XIX secolo per riconoscere un individuo è il volto.
Con l'evolversi della biometria, grazie soprattutto all'ampio utilizzo delle impronte digitali, si arriva nel 1960 all'introduzione di un primo modello di riconoscimento facciale semi automatico.

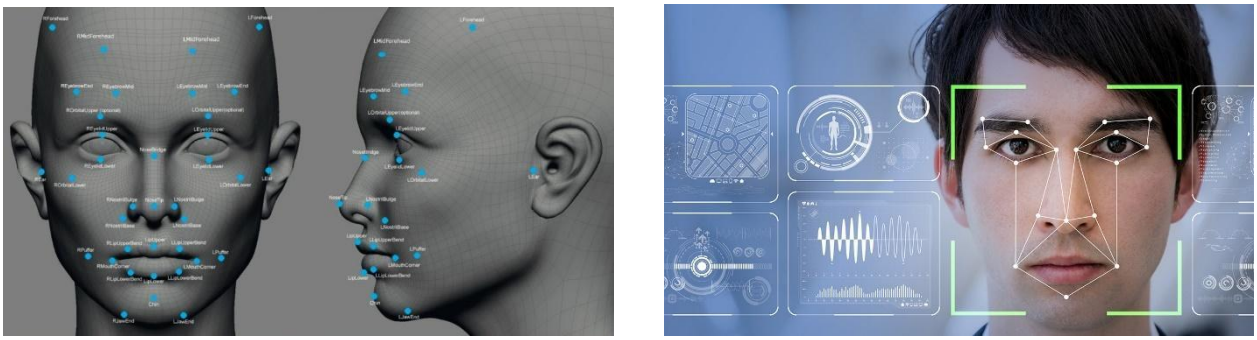


Figura 23: Punti di particolarità del volto

L'uomo, per riconoscere un individuo e capire se gli sia familiare o meno, cerca di estrapolare una faccia "media", piuttosto comune, e poi la utilizza per compararla con le altre facce.
Molti studiosi hanno cercato di portare questo modello naturale in un sistema automatico, creando così negli anni '60 un primo modello di riconoscimento facciale semi automatico, grazie anche all'evolversi della biometria soprattutto nel campo delle impronte digitali. In sostanza si è cercato di elaborare dei programmi che riuscissero ad estrapolare i dati significativi del volto.

I sistemi biometrici si basano, per eseguire il riconoscimento, su caratteristiche universali possedute da ogni individuo oggetto del riconoscimento stesso (come le autofacce, ottenute dalla differenza tra l'immagine del volto in questione che si è ottenuta con la procedura di riconoscimento e il volto medio ottenuto da una base di dati biometrici) o su misurazioni locali (che invece si basano su informazioni geometriche, ricavate dalla misurazione delle distanze relative tra punti distintivi come occhi, bocca e naso).

Il riconoscimento facciale può intervenire in due modi: in maniera statica, in cui il riconoscimento avviene quasi in condizioni ideali, poichè l'individuo si trova fermo frontalmente davanti lo scanner

in condizioni controllate di illuminazione, oppure in maniera dinamica, in cui l'identificazione avviene grazie ad un susseguirsi di fotogrammi, mentre la persona ad esempio passeggia o comunque è in movimento.

Il processo di riconoscimento si articola in:

- Rilevamento del viso e della silhouette nell'immagine: da un fotogramma la rete neurale rileva la sagoma e, se si tratta di riconoscimento dinamico, il percorso della persona che transita davanti la telecamera. In questo secondo caso viene conteggiato, inoltre, istantaneamente il numero di persone che sono presenti all'interno dell'immagine.
  Attenzione alla distanza dalla videocamera/scanner che può influenzare negativamente, quanto più è elevata, le prestazioni. Oggigiorno, proprio per questioni pratiche, ci sono aziende (esempio concreto la *Stereo Vision Imaging* e la sua acquisita *Digital Signal*) che si stanno specializzando sempre più nella tecnica utilizzabile per il lungo raggio, grazie in special modo alla tecnologia Lidar, che permette di raggiungere distanze anche pari a 30 metri.
  Particolarità che si osserva è la presenza di vivacità dell'immagine.

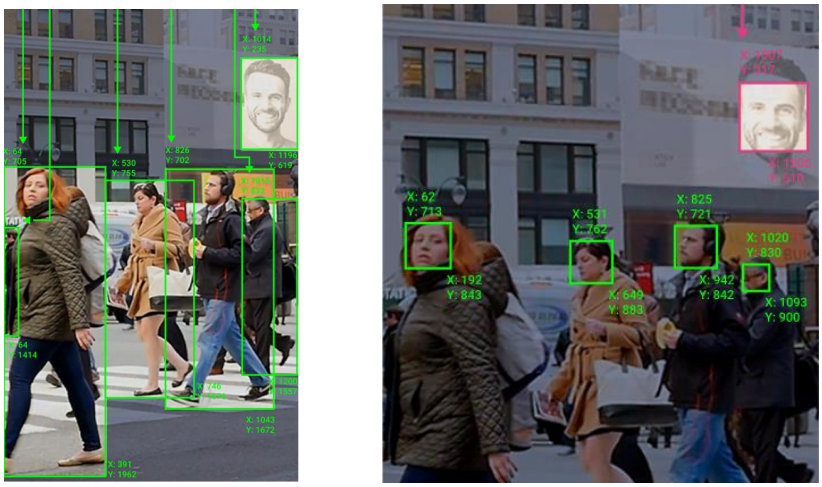


Figura 24: Rappresentazione di calcolo delle coordinate dove si trova il volto nell'immagine e validazione della vivacità (contorno *rosso)*

- Correzione della distorsione visiva: l'algoritmo determina la posizione della testa e corregge la vista, ad esempio, ruotando il volto in caso di dinamicità

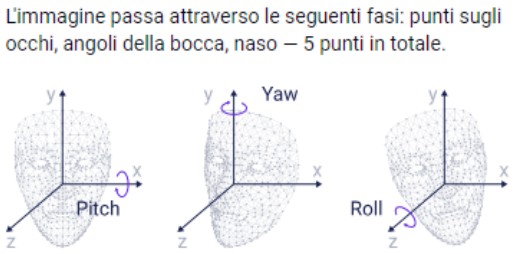


Figura 25: Dimostrazione di rotazione del volto

- Recupero dei tratti del viso: si assegna a ciascun volto un vettore di caratteristiche, cioè un modello biometrico.

- Verifica o identificazione di un volto: si valida l'hash binario appena ricavato con quello/i registrato/i nel database.

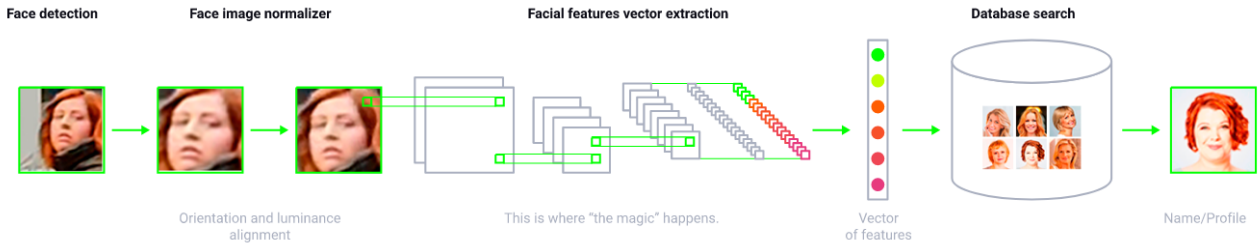


Figura 26: Processo di identificazione del volto

L'utilizzo del volto come fisionomia da controllare si basa su alcuni vantaggi, quali l'alto grado di accettazione da parte dell'utente, il fatto che non sia invasivo (e che quindi richieda una minima o persino nulla cooperazione da parte del soggetto, data anche la possibile mancanza di necessità di avvicinarsi da parte dell'utente) e che possiede un alto grado di universalità.
Di contro, però, si hanno alcuni svantaggi legati all'uso di questa connotazione umana, che possono essere rappresentati dalla bassa stabilità nel tempo, dovuta essenzialmente a fattori naturali quali l'età (per ovviare a questo si prevede un aggiornamento continuo del template, oppure, soprattutto nel caso di bambini scomparsi, si usano dei software che studiano l'invecchiamento del volto, permettendo di adattare così la ricerca all'età che avrebbe il soggetto scomparso), i cambiamenti di look (barba, capelli ,…), le espressioni del volto, la presenza di occhiali…
Nonostante si possa avere un relativamente basso livello di unicità, oggigiorno questo svantaggio sta via via andando a diminuire, in quanto vengono prese in considerazione un numero sempre maggiore di particolarità da osservare.

Inoltre la tecnica di riconoscimento dinamico presenta anche un basso grado di gradimento da parte dell'utente, che non gradisce certamente essere costantemente sorvegliato (si veda la sicurezza aeroportuale), portando quindi ad una possibile violazione della privacy.

Il dispositivo che si utilizza per effettuare il riconoscimento facciale gode di un'elevata economicità in quanto si utilizzano prettamente delle telecamere già installate per la videosorveglianza, alle quali viene applicato un software per la verifica biometrica, permettendo così una facile integrazione e acquisizione dell'immagine, in una maniera essenzialmente molto pratica e rapida di elaborazione.
Purtroppo, e questa è la parte negativa, si viene in contatto con diversi fattori che possono andare ad intaccare il riconoscimento quali le diverse luci, la variazione di posa (dato soprattutto dall'elevato grado di movimento della testa), la vivacità dell'utente e l'utilizzo di trucco e maschere.

Per la vivacità si va a guardare uno o più delle seguenti caratteristiche con la consapevolezza che maggiore sarà il numero di controlli, minore sarà l'esperienza dell'utente: angolo di inclinazione del volto (alto-basso), angolo di imbardata (destra-sinistra), vitalità della bocca (aperta-chiusa), vitalità degli occhi (aperti-chiusi), vitalità delle sopracciglia (inarcate-piatte), vitalità del sorriso, vitalità ad infrarossi. Su questo ultimo controllo ci ha lavorato *Apple* con il Face ID in cui, oltre a questo, utilizza più di 30.000 punti per mappare il viso, quindi crea essenzialmente una mappa in tre dimensioni del volto. Questa, come per il Touch ID, viene inviata alla Secure Enclave nella CPU per essere confrontata con quella già memorizzata sul dispositivo.

Figura 27: Luce ad infrarossi per il Face ID

Invece per quanto concerne il discorso relativo alle maschere, molto sentito specialmente in questo periodo pandemico, troviamo aziende come *Cyber Extruder* che hanno lavorato su un sistema che non potesse essere messo in discussione in caso di apposizione di mascherina sul volto da parte dell'individuo.

Per quanto riguarda i principali fattori che guidano la crescita del mercato del riconoscimento facciale, si nota la presenza di una crescente importanza del settore della sorveglianza, e di un incremento esponenziale degli investimenti da parte del comparto della difesa (settore governativo).
Tuttavia ci sono delle problematiche di non poca importanza e rilevanza. In particolare, l'errore di rilevamento del volto e la mancanza di conoscenza e consapevolezza sono alcune delle principali sfide che ostacolano la crescita del mercato del riconoscimento facciale.

L’ecg

Fino ad ora abbiamo analizzato i sistemi di riconoscimento sicuramente più noti e anche più utilizzati. Detto questo, può essere realizzata una analisi più precisa, attraverso altri sistemi di identificazione biometrica. In questa ipotesi, questi sistemi basano la loro analisi su caratteristiche fisiche propriamente personali di non difficile ricavo (e soprattutto di cui non è possibile una replica esistente, o se lo è, si tratta comunque di un atto di difficilissima realizzazione). Un esempio concreto è il battito cardiaco, che ben si presta a ciò.

L'elettrocardiogramma, qui di seguito abbreviato con ECG, è la registrazione grafica dell'attività bioelettrica del cuore durante un battito cardiaco, ossia durante il suo funzionamento, raccolta per mezzo di elettrodi. La sorgente bioelettrica nasce durante il processo di eccitazione elettrica del cuore, per produrre un flusso di corrente elettrica nei tessuti circostanti.
La forma dell’onda dipende da diversi fattori umani quali la dimensione e la forma del cuore, la posizione all'interno del torace e le proprietà conduttive del busto. Sono proprio queste informazioni che rendono l’insieme, cioè l’ECG, praticamente unico, perchè il modello realizzato dall'analisi del nostro battito cardiaco si basa essenzialmente sulle caratteristiche fisiologiche del cuore, che è, appunto, unico.

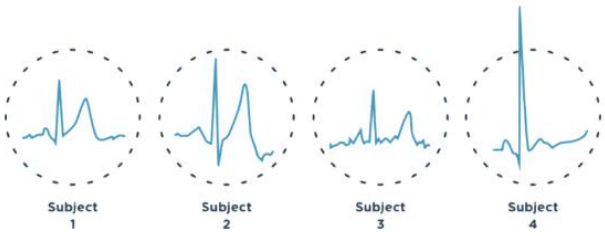


Figura 28: ECG di diversi soggetti

Ritornando all’insieme di informazioni che l’ECG porta con sé, infatti, notiamo molta variabilità tra gli esseri umani e i loro battiti cardiaci individuali che può essere compresa da due stati:

- Intervariabilità: la forma d'onda di ogni individuo sarà diversa da un'altra poiché diverse le geometrie del cuore e gli attributi individuali. Ha il fine di identificare l’individuo.

- Intravariabilità: variazione dell'ECG all'interno di un soggetto causato da fattori come la postura, lo stato emotivo, …. Ha il fine di scoprire, ad esempio, principi d’ansia.

La forma d'onda di ogni individuo sarà diversa da un'altra (intervariabilità), come un'impronta digitale, ma, oltre a ciò, ogni battito cardiaco forma anche un segnale diverso (intravariabilità).

Lo studio dell’ECG, cioè utilizzare il battito cardiaco come metodo di riconoscimento, porta con sé il principale fatto che sia un’azione completamente naturale, quindi con alti livelli di semplicità, oltre

ad essere una caratteristica con il più alto livello di universalità perché altrimenti significherebbe che la persona è deceduta.
Inoltre, la caratteristica garantisce alta unicità, anche se lo stress e le attività fisiche possono intaccare il riconoscimento.
In aggiunta è anche complicato andare a falsificare o copiare il template, in quanto è richiesta la vivacità dell'utente affinché venga completato il riconoscimento.

Nonostante ciò, l'elaborazione necessita di un particolare periodo di tempo, oltre che di un numero consistente di dati storici.
Sebbene ci siano ancora delle barriere legate al costo e al fatto che sia una tecnologia abbastanza giovane si sta cercando di migliorarla passando al controllo continuo dell'individuo con l'implementazione del software nei Wearable come nel caso di *Nymi*.

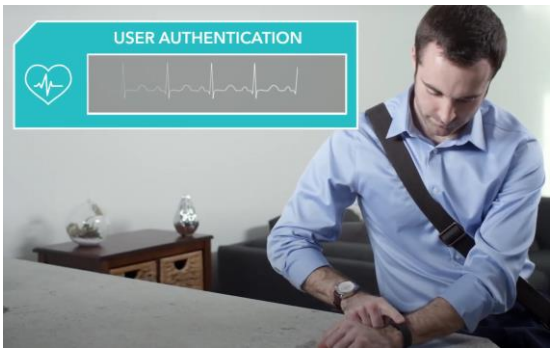


Figura 29: Verifica del battito grazie al wearable di *Nymi*

Non si dovrà compiere alcun gesto "fuori dall'ordinario" per verificare l'identità, in quanto questa verrà analizzata lungo il periodo in cui l'orologio, ad esempio, viene indossato (possibile soluzione al fatto che la caratteristica non abbia un'alta permanenza nel tempo) dato che non verrebbe richiesta alcuna collaborazione dall'utente.

Sebbene ci siano degli studi medici di fondo per la studio della caratteristica biometrica, si va incontro ancora ad un mercato agli albori in quanto solo in questi ultimi anni molte aziende, come *B-Secur*, che si stanno adoperando per trasportare la conoscenza medica per il riconoscimento.
Anche in questo caso, però, la tecnologia deve ancora apportare delle migliorie, affinché possa essere utilizzata come sistema di identificazione biometrico, in modo che questo sia sufficientemente pratico per poter essere diffuso in maniera efficiente e capillare. Ma le potenzialità che rappresenta sono di rilievo, in primo luogo perchè, ad esempio, il battito cardiaco può essere rilevato in maniera costante, il che fa sì che sia un parametro per un controllo continuativo dell'identità del soggetto in questione, piuttosto che essere una caratteristica utile solo nel momento in cui interviene il riconoscimento.

2.2.4.2 **Il riconoscimento comportamentale**

Tutto iniziò quando negli anni ’40 Samuel Morse inventò un sistema telegrafico elettrico che permetteva la codificazione delle lettere alfabetiche attraverso una sequenza di impulsi aventi durata differente l'uno dall'altro andando a creare dei punti e delle linee, il famoso “*codice Morse*”, con l’utilizzo di un’apposita leva.

Figura 30: Il telegrafo

Soprattutto durante la Seconda Guerra Mondiale si fece largo uso di questo strumento per trasmettere messaggi militari. Proprio in questo periodo si riconobbe che il modo di creare i simboli dell’alfabeto morse con lo strumento risultavano “unici” da persona a persona in particolare si andavano ad analizzare i punti e le linee per capire se il messaggio arrivava da una persona specifica.

La biometria comportamentale, a differenza del riconoscimento fisiologico, autentica gli utenti in base a modelli di comportamento identificando delle regolarità uniche e individuali. La caratteristica principale è che l’autenticazione avviene pressoché continuamente studiando in tempo reale la caratteristica considerata e non una tantum come con i precedenti metodi di riconoscimento.

Si hanno diversi vantaggi connessi a questo metodo:

- I dati memorizzati non sono una rappresentazione fisica, rendendo quindi complicato lo sfruttamento di dati rubati;
- L’autenticazione avviene tendenzialmente per tutta la durata della sessione;
- Ci sono meno implicazioni legate alla privacy.

L’impronta vocale

La voce, onda acustica prodotta quando l’aria dai polmoni passa per la trachea attraverso le corde vocali, è considerata come una tra le tecnologie che presenta il maggior grado di accettazione presso il pubblico, in quanto è un’azione effettuata in maniera assolutamente naturale dall’utente. Inoltre, questo metodo di riconoscimento gioca anche un ruolo importante per risolvere problemi pratici che non permetterebbero di usare questa tecnologia molto semplice, quali, ad esempio, quelli rappresentati da quelle persone che hanno dei problemi con le mani.

In particolare, si vanno ad analizzare i seguenti fattori biometrici:

- L'altezza della voce determinata dalla frequenza di vibrazione delle corde vocali;
- Il timbro individuato dalle posizioni e dalle forme delle labbra, della lingua e del naso;
- Il volume della voce determinato dalla compressione dei polmoni.

Quindi, per impostare il template presente nel database, basterà ripetere 3-5 volte l'impostazione.

La caratteristica soffre però del rischio di mancata unicità, in quanto particolarmente legata allo stato psicologico dell'individuo e conseguente instabilità nel tempo, oltre al fatto che il timbro vocale muta nel tempo con l'invecchiamento (si sta cercando di allenare le reti neurali per contrastare questo svantaggio).

Intervengono due tipologie di riconoscimento: una relativa a cosa viene detto e una relativa a riconoscere il soggetto che sta parlando.

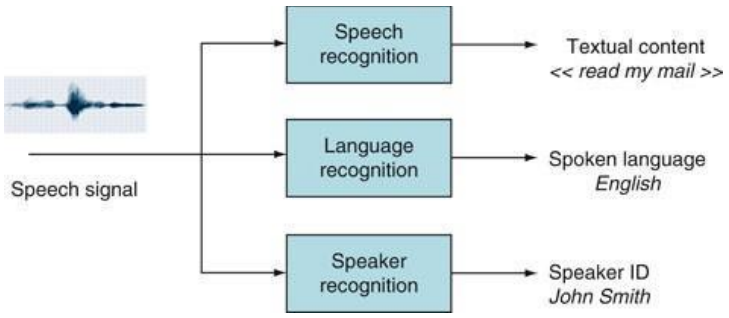


Figura 31: Tipologie di riconoscimento del suono

I sistemi che permettono il riconoscimento del soggetto in questione tramite la sua voce sono suddivisibili in due categorie:

- Dipendenti dal messaggio (cosiddetti *text-dependent*);
- Indipendenti dal messaggio (cosiddetti *text-independent*).

Per quanto concerne la prima categoria, a tutti i parlatori è affibbiato un messaggio univoco e comune (come, ad esempio, una unica parola d'ordine per tutti). Inoltre, per poter procede alla creazione di scenari che prevedano una autenticazione effettuata con l'ausilio di diversi fattori, è permesso l'utilizzo di informazioni segrete condivise (come un PIN) oppure basate sulla conoscenza.

La seconda categoria viene soprattutto utilizzata nei casi di identificazione, in quanto non necessitano della collaborazione dello speaker. In questo caso si unisce il riconoscimento del parlatore con il riconoscimento vocale così da rendere confrontabili le fasi di raccolta e di verifica dato che non verranno pronunciate le stesse parole.

Il riconoscimento del parlatore è, comunque, di facile implementazione, in quanto non richiede nessun hardware specifico (un semplice microfono) non avendo così alcuna barriera legata al costo del dispositivo e presentando anche un alto grado di semplicità in termini di acquisizione della voce, dato che non richiede un particolare training dell'utente. Purtroppo, però, il microfono diventa un fattore critico, perché può condizionare drasticamente il riconoscimento della voce, visto che si basa sulla qualità del dispositivo.

L'ambiente, e il cosiddetto "rumore esterno", andranno di conseguenza ad essere una tra le cause principali di mancato riconoscimento. Sono proprio i nuovi algoritmi (come VISPR, Voice Isolation for Sonic Perceptual Recognition, di *Yobe* e *AISpeech*) che si stanno sviluppando in questa direzione ad essere sotto la lente di ingrandimento, andando ad isolare e a comprendere meglio la voce dello speaker sia nel caso in cui sia presente della confusione sia nel caso in cui delle parole abbiano una pronuncia molto simile.
Inoltre, l'utilizzo dell'intelligenza artificiale va a diminuire la grandezza che è richiesta per il template, potendo così diminuire l'allocazione di memoria necessaria per la sua memorizzazione.

Discostandosi dal discorso "solo-software", c'è un'azienda, *Aspinity*, che sviluppa un prodotto hardware e software capace di riconoscere la voce interessata diminuendo il rumore e, indirettamente, aumentando la durata della batteria, in quanto impedisce al chip interessato di continuare ad ascoltare l'ambiente esterno facendolo così "intervenire" qualora gli arrivasse un segnale che rappresenterebbe la voce.

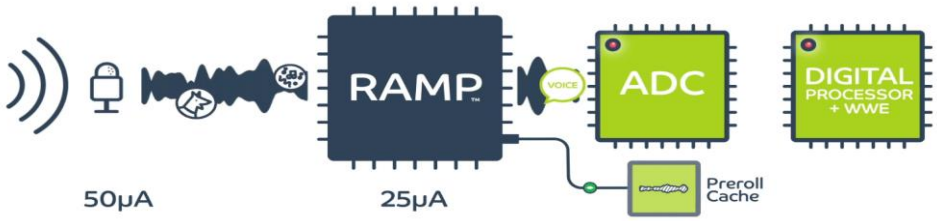


Figura 32: Funzionamento prodotto di Aspinity

La scrittura grafica - firma grafometrica

Al giorno d'oggi, soprattutto con l'avvento del digitale, viene sempre più spesso utilizzata la firma per verificare l'identità del soggetto in questione, soprattutto presso gli istituti bancari e finanziari.

Essendo una pratica utilizzata da sempre (ora si è virato su tavolette elettroniche) vi è un elevato grado di accettazione essendo, oltre che un'abitudine, molto intuitiva e minimamente intrusiva.

Figura 33: La tavoletta per la firma

Nell'approccio originario di riconoscimento era prevista l'effettuazione di una stima degli scostamenti messi in atto dagli aspetti geometrici della firma dal modello registrato. Nell'approccio evolutivo (già nel 1965 si è cercato di eseguire una registrazione automatica) sono presenti, all'interno del template creato la prima volta che si effettua la firma, indicazioni sulla velocità di scrittura, sulle accelerazioni di movimento, sulla pressione esercitata, sull'angolo di inclinazione con il pennino e sul numero di volte in cui si crea il vuoto con la tavoletta. Insieme di fattori che andranno a diminuire il rischio di mancanza unicità. Sebbene vengano utilizzati diversi parametri e non vi siano particolari costi, bisogna fare attenzione ai dispositivi utilizzati in quanto sono critici per il successo del riconoscimento.

Purtroppo essendoci un legame con lo stato psicologico può non esserci un'alta stabilità nel tempo. Inoltre non vi è un alto grado di universalità, e in più si incontrerebbero degli ostacoli in caso di menomazioni o disabilità.

Con il digital c'è stata una "deviazione" da questa tecnologia, come dimostra *Biometric Signature ID*, cioè lo studio della scrittura dell'utente. Nonostante possa sembrare lo studio di una caratteristica nuova, in realtà i fattori analizzati sono i medesimi della firma cartacea.

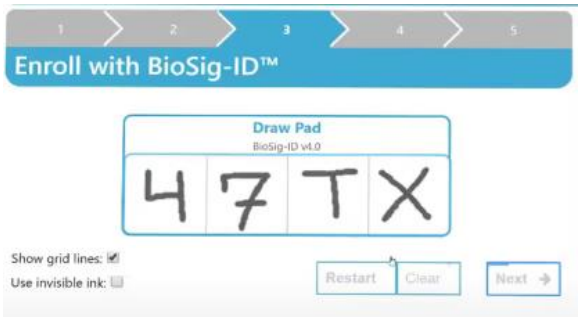


Figura 34: Software di verifica della scrittura di *Biometric Signature ID* attraverso il mouse

Lo stile di battitura sulla tastiera, movimento del mouse e dello schermo

Oggigiorno, ogni utente che utilizza, ad esempio, un personal computer genera automaticamente un profilo comportamentale che riflette come questo interagisce con il sistema, andando quindi a studiare le sequenze di tasti, lo scorrimento dello schermo e i movimenti del mouse.

Una volta che viene creato il template, cioè quando si apprende il profilo, si studiano silenziosamente in tempo reale i gesti dell'individuo, così da autenticare continuamente la sua identità. Se non vi è la corrispondenza con il modello registrato, il sistema si blocca completamente o richiede altre forme di autenticazione per poter continuare.

I tre possibili fattori studiati sono:

- Dinamica dei tasti, cioè lo studio dei modelli di digitazione sulla tastiera in cui viene analizzata la velocità e la durata di battitura, i particolari sequenziamenti di tasti ravvicinati o parole comuni;

- Scorrimenti sul touchscreen (dispositivo mobile), cioè lo studio del modo in cui si usa lo schermo, che prevede quindi scorrimento, tocco, ingrandimento e digitazione (quindi, in sostanza, esercitare una pressione di qualunque tipo sullo schermo);

- Movimenti del mouse, cioè l'analisi della velocità e dei cambi di direzione, con annessi percorsi, del cursore, delle pressioni (i "click") sull'hardware.

Figura 35: Verifica comportamentale attraverso i sistemi informatici

La tecnologia, facendo ormai parte, soprattutto a seguito del periodo pandemico, della nostra vita quotidiana va incontro ad un alto grado di accettazione da parte del pubblico, di tutte le età si può dire, in quanto l'utente non dovrà neanche compiere un'azione di riconoscimento come apporre il pollice sul lettore per l'impronta digitale, poiché sarà sufficiente iniziare a lavorare che il pc verificherà l'identità dell'individuo. Inoltre i dati sarebbero quasi non "rivendibili" dato che comunque il ladro dovrebbe autenticarsi continuamente.

Anche se la tecnologia è discreta, accessibile (si parla praticamente solo di software quindi semplice da distribuire e da integrare dato anche il basso costo) e non invasiva, si va comunque incontro a degli svantaggi, soprattutto legati al template perché, oltre al fatto che i modelli possono essere sensibili allo stato in cui si trova l'utente (fatica, malumore o anche menomazione/disabilità) non garantendo quindi un'alta stabilità nel tempo, c'è la necessità di possedere un gran numero di dati storici rendendo quindi, nel breve periodo, inutilizzabile la tecnologia.

Inoltre, bisogna fare attenzione ai diversi hardware: per la tastiera ci possono essere dei cambiamenti nei modelli di digitazione, mentre per il mouse ci può essere un cambiamento nella qualità di cattura del movimento.
Anche se si è dei provetti ad utilizzare questo tipo di tecnologia, bisogna comunque inizialmente trovare la familiarità con mouse/tastiera/schermo per ottenere un'analisi accurata.

La camminata

Lo studio della camminata, come metodo di riconoscimento, utilizza la forma del corpo umano e il modo in cui si muove per identificarlo, e può essere eseguito in due modi: con telecamere o con wearable.
La tecnologia garantisce, soprattutto nel secondo metodo, una verifica continua nel tempo, utilizzando il giroscopio e l'accelerometro, rendendo più complicata l'azione di malintenzionati.

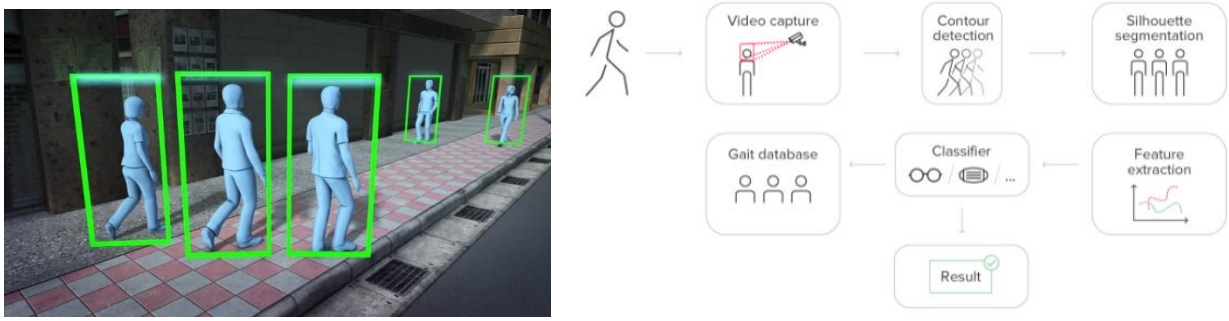


Figura 36: Segmentazione della sagoma e identificazione dell'individuo

Le fasi di funzionamento sono:

- Acquisizione dati sull'andatura attraverso videocamere o sensori indossabili;
- Segmentazione della sagoma (qualora vi fosse l'uso di telecamere): estrazione dalla registrazione di una immagine binaria della silhouette e studio da parte degli algoritmi;
- Rilevamento del contorno del corpo umano (qualora vi fosse l'uso di telecamere);
- Estrazione e classificazione delle caratteristiche: individuazione delle particolarità dell'andatura.

Lo sfruttamento di questa caratteristica per identificare l'individuo, oltre ad essere molto discreta e non invasiva (non richiedendo la collaborazione del soggetto coinvolto) garantisce un ottimo livello

di accettazione presso il pubblico, soprattutto per la naturalezza dell'azione dell'utente unita ad un alto tasso di unicità.

Nonostante tutto però, soprattutto nell'uso di telecamere, è necessaria un'alta durata di elaborazione con uso di registrazioni video e immagini a distanza, anche se non è richiesta una elevata risoluzione.
Inoltre, se non si è in un contesto controllato, sono necessarie diverse angolazioni anche per evitare possibili problemi in caso di occlusioni da parte di altre persone. Necessità che viene meno in caso di tecnologia unita ad esempio ad un orologio da polso.

Attenzione particolare sarebbe poi da compiere sulla superficie su cui si svolge la camminata, l'abbigliamento indossato e le calzature utilizzate. In sostanza, bisognerebbe identificare le caratteristiche che sono meno "attaccabili" dall'aspetto per migliorare la precisione del riconoscimento (ad esempio nel subcontinente indiano le donne indossano il saree, l'abito tradizionale, che influisce sui modelli di andatura rispetto alle donne che indossano gonne corte o jeans).
Infine, la tecnologia risulta inadeguata nell'infanzia e se sono presenti delle menomazioni o disabilità.

Poiché la tecnologia è ancora nella fase di sviluppo, i risultati non possono sempre essere considerati totalmente attendibili, seppur dimostrino bassi valori di errori.
Ci sta lavorando un'azienda cinese, *Watrix*, che ha raccolto fondi per 14.8 milioni di dollari e che riesce ad identificare gli individui anche a distanze di 50 metri anche con volto coperto.

3. L'ANALISI DEI RISULTATI

3.1 La metodologia scelta

L'elaborato verte sull'analisi dei finanziamenti alle aziende (dati in milioni di dollari) che lavorano in ambito biometrico, più specificatamente nel suo uso per riconoscere l'identità dell'individuo.
A seguito di un incontro con un esperto facente parte dell'ambito della cyber sicurezza di Hewlett Packard Enterprise, sono venuto a conoscenza del fatto che sarebbe stato praticamente impossibile conoscere i livelli puntuali di soldi investiti in tecnologie riguardanti la sicurezza. Questo perché i malintenzionati riuscirebbero a comprendere, grazie all'ammontare specifico investito, quale tecnologia e, soprattutto, livello di sicurezza è stato adoperato.
Quindi, contrariamente al fatto di considerare i livelli di investimento interni all'azienda, si è studiato, grazie a CrunchBase e Dealroom, l'ammontare del denaro ricevuto come finanziamento da enti esterni alla società. Pertanto non ci si posizionerà nelle vesta dell'azienda che investe in prima persona del denaro in una tecnologia biometrica, ma si andrà a considerare quanto gli investitori (terze parti) credono in quel metodo di riconoscimento biometrico per quella specifica applicazione.
Si tratta di un buon punto di partenza anche se si potrebbe andare incontro ad un modello approssimativo.

All'inizio sono state considerate le aziende presenti all'interno di "Biometric Update", un portale riguardante la biometria in cui oltre ad informazioni, notizie ed eventi è presente un elenco di aziende (circa 750) che lavorano in questo ambito. Da queste è stata fatta una prima scrematura considerando solo quelle che erano presenti all'interno dei database sopra citati.
In seguito sono state selezionate solo quelle che avevano un sito aziendale funzionante e, successivamente, quelle per le quali erano presenti i livelli di finanziamento. Infine sono state considerate solo coloro che erano legate alla biometria per il riconoscimento dell'identità dell'utente.

In un secondo tempo è stata fatta una ricerca più ampia sfruttando la sezione "settore" delle aziende presenti su Crunchbase. In particolare, grazie a diversi filtri, sono state identificate circa 800 aziende. Da queste sono state selezionate solo quelle per le quali erano presenti dei finanziamenti. Con lo stesso metodo sono state poi scartate le aziende che presentavano dei problemi con il sito e/o che non lavoravano/utilizzavano la biometria per l'identità.

Una volta costruito il database personale di circa 250 aziende, per non compromettere l'integrità dell'analisi e cercare di avere una visione che più si avvicinasse alla realtà, si è fatta un'ulteriore scrematura. Sono state escluse le aziende che presentavano ulteriori forme di business, che si interfacciavano ad altri mercati e che sfruttavano la biometria sviluppata da altri partner (come ad esempio l'utilizzo dei riconoscimento grazie al Face ID o al Touch ID) dato che non ci stanno lavorando in prima persona.

Oltre a ciò, non sono state anche considerate quelle aziende, come *ImageWare System*, che non si specializzano in una tecnologia biometrica precisa, ma che si interfacciano al mondo della cyber sicurezza come delle Saas lasciando così decidere al cliente finale quale metodo di verifica/identificazione utilizzare.
Alla fine, quindi, sono risultate circa 180 aziende in cui la biometria per l'identità unita ad una applicazione particolare risultasse il business preponderante.

Per andare poi ad analizzare gli incroci tra tecnologia biometrica e campo applicativo, sono stati studiati i siti aziendali in modo tale da comprendere in quale business biometrico lavorassero le aziende. In seguito è stato ipotizzato che i finanziamenti ricevuti venissero investiti dalle compagnie in parti uguali per tutte le tecnologie e applicazioni che sviluppavano senza effettuare delle considerazioni secondo le quali l'ammontare potesse essere diviso in diverse porzioni (ad esempio 1/3 e 2/3). Perciò se un'azienda aveva ricevuto un finanziamento di 100 milioni di dollari per l'impronta digitale con l'obiettivo di sfruttarla nel controllo delle presenze e negli accessi del telefono, allora si hanno due somme di denaro da 50 milioni ciascuno. Stesso discorso se ci fosse stato l'utilizzo di due tecnologie biometriche per la stessa applicazione.

3.1.1 Le applicazioni

Prima di procedere con la spiegazione della matrice dei finanziamenti e relative considerazioni su una possibile combinazione vincente per il mercato, si passa a spiegare, con qualche esempio pratico, le applicazioni appena citate all'inizio del capitolo precedente.

Le applicazioni individuate attraverso lo studio dei siti aziendali si possono raggruppare in:

- **Controllo degli accessi degli edifici**: consta nell'identificazione dell'individuo che vuole accedere in un luogo fisico che può essere la zona protetta del laboratorio, l'edificio, la stanza di un hotel, il mezzo pubblico, l'aeroporto, e altri vari. Si tratta quindi di tutti quegli utilizzi che riguardano l'accesso fisico.
  Le possibilità di impiego della biometria sono molteplici, perché può andare dalla verifica dell'identità del proprietario sul telefono personale, dove ha registrato la propria impronta o volto per poter confermare di essere proprio lui che vuole sbloccare il telefono, fino all'apposizione sulla porta di ingresso di un dispositivo fisso affinché identifichi, ad esempio, l'impronta digitale.
  Oppure è anche possibile una via di mezzo, che si riscontra, per dare una prova concreta, nel prodotto portatile sviluppato da *Crayonic* senza la necessità di andare a comprare, lato azienda, un dispositivo ad ogni porta del laboratorio.

  Alcune aziende come *Dessmann* hanno spaziato il mondo dell'accesso fisico, andando a specializzarsi maggiormente nelle maniglie delle porte, così da aggiungere le impronte digitali anche con eventuale combinazione numerica per fornire maggiore sicurezza negli accessi.
  Biometria che va anche a toccare gli angoli più segreti delle banche, cioè i caveau, cosa che sviluppa *Eyecool* con l'utilizzo della tecnologia dell'iride.

  Ci sono poi aziende come *Clear* che aiutano l'espansione del riconoscimento biometrico creando dei "percorsi vip" per le persone che lo sfruttano per identificarsi. La stessa viene utilizzata specificatamente in aeroporto per effettuare le normali azioni di check-in che ciascun passeggero è obbligato a compiere una volta che decide di utilizzare l'aeroplano per muoversi. Al fine di creare un'esperienza positiva, sfrutta la potenza della tecnologia biometrica per formare delle zone dedicate per il controllo documenti. L'individuo potrà così beneficiare della velocità e dell'alta unicità dei metodi di riconoscimento. Una volta che un altro passeggero in coda vede la potenza della biometria all'aeroporto, la utilizzerà anche lui andando così a creare un passaparola implicito della tecnologia.

Figura 37: Esempio di corsia preferenziale di Clear all'aeroporto

- **Controllo delle presenze**: sottocategoria del controllo accessi sopra esposto, ma che unitamente a permettere l'ingresso in ufficio, consente anche di memorizzare i dati del dipendente affinché venga stilata una reportistica per le risorse umane. Questa conterrà informazioni sulla gestione del dipendente andando quindi ad analizzare le pianificazioni di lavoro, il congedo di malattia, i costi del lavoro, le assenze, le presenze, …
  Si andrà ad utilizzare ad esempio il riconoscimento facciale sul dispositivo di timbratura così da possedere anche quella sicurezza aggiuntiva rispetto ad una semplice smart card. Oppure è anche possibile sfruttare un braccialetto biometrico che identifica una caratteristica comportamentale.

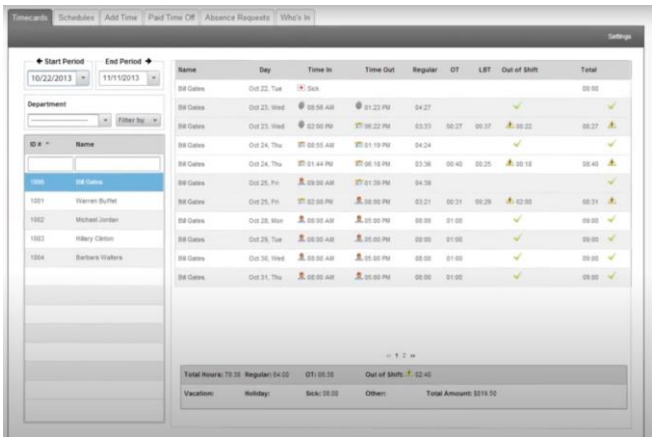


Figura 38: Controllo delle presenze del personale di *Easy Clocking*

In particolare, per questa applicazione, è stata fatta la seguente considerazione. Essendo una sorta di "di più" per le aziende che sviluppano il controllo degli accessi, è stato calcolato il finanziamento per questo verticale suddividendo in parti uguali l'ammontare di denaro che originariamente era destinato unicamente al controllo degli accessi. Quindi si è preso quest'ultimo livello degli investimenti e si è diviso in due, una metà per gli accessi e l'altra metà per le presenze.

- **Identificazione criminali e Controlli di sicurezza**: si sostanzia nel controllo e identificazione degli individui principalmente per ragioni attinenti la sicurezza, sia pubblica sia privata.
  Come si nota dalla figura qui in basso, si andrà ad esempio a sfruttare il riconoscimento facciale per identificare le persone presenti all'interno del fotogramma del video catturato da una videocamera. Il software va quindi a riconoscere eventuali individui già presenti in liste di controllo della polizia oppure alcuni vip. Quest'ultima soluzione risulta particolarmente importante in contesti di gestione della clientela di hotel, conservando così un rapporto raffinato con le giuste persone così che possano poi trasmettere l'efficienza ed accuratezza del servizio anche ad altri.

Figura 39: Identificazione persone con il riconoscimento facciale

- **Avviamento veicoli e macchine industriali**: identificazione dell'individuo all'interno dell'autoveicolo per guidare e/o accedere, ad esempio, al tablet di bordo.
  Soluzione che sicuramente andrà via via migliorandosi, anche e soprattutto, con l'avanzamento degli studi e della pratica relativa all'auto a guida autonoma. Questo perché, grazie a codesti nuovi modelli di auto, non sarà neanche più necessario usufruire della chiave di accensione per permettere al proprietario l'utilizzo dell'autoveicolo: l'avanzamento della tecnologia permetterà alla biometria di identificare il detentore del veicolo.
  Dato sempre più l'evolversi dei livelli di guida autonoma, si potrà presto arrivare agli stadi 4 e 5, che rappresentano quasi la totale assenza dell'esperienza di guida, che renderà anche il guidatore stesso un semplice conducente. In quest'ottica stanno lavorando anche gli stessi produttori di auto, e i loro partner, sfruttando, ad esempio, il tablet di bordo, apportando sempre più migliorie, anche per far vivere un'esperienza a cinque stelle a tutti i passeggeri.
  My Voice sfrutta la tecnologia biometrica della voce per identificare il conducente ed effettuare anche transazioni e pagamenti a mani libere senza far distogliere lo sguardo dalla strada sfruttando il tablet di bordo. Con una visione un po' futuristica, vuole sfruttare la biometria nel contesto del riconoscimento del conducente per avviare anche l'auto. Questo è anche portato dal dirompente avanzamento del fenomeno del car sharing coinvolgendo altre persone a guidare la stessa auto.
  Esistono perfino delle suggestioni da parte di Tesla di poter attivare la condivisione dell'auto quando il proprietario sta lavorando facendo muovere il veicolo in autonomia presso il cliente che richiederà un passaggio, quasi come se fosse un Uber.

Figura 40: Possibile riconoscimento del conducente con l'utilizzo della fisionomia del volto

- **Accesso al PC e al Telefono**: consta nell'accesso ai dispositivi telefonici e ai computer. All'interno di questa applicazione sono state considerate tutte quelle aziende che sfruttano un software, comprensivo o meno, di hardware che permetta di sbloccare il dispositivo in questione.
  Possono esserci diversi metodi per identificare il corrispondente utente come, ad esempio, *Nymi* che sfrutta l'orologio al polso dell'individuo per verificare il corretto template di ecg e impronta digitale per poter accedere al PC. Oppure *AuthenTec*, acquisita poi da *Apple*, ha sviluppato hardware e software per poter accedere al telefono con l'impronta digitale.

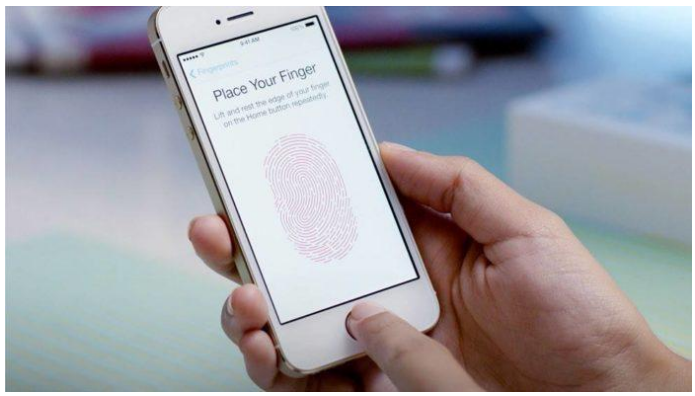


Figura 41: Touch ID dell'IPhone

- **Autenticazione remota su internet**: consta nell'insieme di verifica dell'identità dell'utente una volta che vuole accedere ad app, programmi, siti web, account e chatbot. Si tratta quindi di tutti quegli utilizzi che riguardano l'accesso logico.
  Esistono molteplici modi che rientrano sotto questa macro-voce. Si trova ad esempio l'utilizzo della verifica biometrica del detentore dell'account online, sia che si tratti del sito bancario sia di quello per i videogiochi, attraverso l'applicazione del telefono. L'utente quindi si farà riconoscere andando a "presentare" la caratteristica che sarà richiesta in fase di registrazione. Si ricorda che qui sono state considerate solo quelle aziende che hanno lavorato in prima persona sulla biometria. Quindi, se servirà ad accedere al conto corrente grazie alla verifica portata avanti dalla combinazione di hardware e software del produttore

del telefono, non si considererà il finanziamento ricevuto dall'azienda nella matrice che viene presentata successivamente.
Possibile anche il caso di verificare l'identità per poter parlare, attraverso la chat, con il servizio clienti cosicché le persone interessate dietro lo schermo non rischino di rivelare informazioni personali ad uno sconosciuto o, peggio, ad un malintenzionato.

- **Transazioni**: si tratta dell'effettuazione di pagamenti in ambienti esterni, quindi quelli in cui viene escluso l'accesso al conto corrente.
  In particolare, per poter utilizzare questa tecnologia unita alla biometria, vi è un processo di registrazione dell'utente. Il soggetto, attraverso un'applicazione specifica o direttamente in filiale, ha la possibilità di memorizzare la caratteristica biometria al fine di poter effettuare il movimento di denaro in luoghi, tendenzialmente, attrezzati. Il fatto di non dover andare solo in attività commerciali pronti è perché vi possono essere due alternative.
  La prima implica lo sfruttamento di un dispositivo dedicato per, ad esempio, scansionare il volto, e se non ci fosse non sarebbe possibile far intervenire la biometria costringendo così l'utente a portare con sé la carta bancaria o i contanti.
  La seconda alternativa utilizza una nuova tecnologia su cui le grandi aziende si stanno concentrando duramente, credendoci e mettendoci la faccia in prima persona. Ad esempio *Delta ID*, poi acquisita da *Fingerprint Cards AB*, sta attualmente lavorando su dei chip particolari che verificano l'identità della persona al momento del pagamento con il pos, attraverso la tecnologia delle impronte digitali. Questo metodo, oltre ad essere più sicuro per l'utente finale e per la banca, porta con sé il fatto di non doversi ricordare più alcun pin neanche per cifre superiori ai 25 euro.
  L'applicazione poi spazia fino ad arrivare al dispositivo studiato da *Case*. Questa azienda ha unito la biometria sicura dell'impronta con l'espansione, sempre più imponente, delle valute digitali (o criptovalute). Seppur l'ultimo finanziamento ricevuto di 2.3 milioni di dollari risalga al 2015, sicuramente i recenti avvenimenti di Tesla-Bitcoin e la situazione in America Centrale (in cui alcune economie, seppur piccole, stanno iniziando ad utilizzare la valuta) porteranno ad una rapidissima espansione della tecnologia.

Figura 42: Soluzione della carta di credito portata avanti da *Zwipe*

Figura 43: Pagamento con le criptovalute di *Case*

- **Firma digitale - Protezione e scambio sicuro di documenti**: consta nello sfruttamento della biometria per certificare la condivisione di file, verificando il mittente e il destinatario. Si tende ad avere questo livello di sicurezza, dato che i file in questione contengono dati altamente sensibili, come quelli finanziari, o relativi a contratti legali, informazioni sui dipendenti, idee nuove per l'innovazione, ….

  Questa protezione potrà essere raggiunta con diverse modalità. Per fare un esempio concreto, possiamo guardare all'azienda *Smart Eye*, che aggiunge alla "normale" tecnologia del riconoscimento facciale il fatto di effettuare la verifica lungo tutta la durata della sessione, cioè fino al momento in cui il documento non viene spedito.

  Invece, *Trust Stamp* inserisce all'interno del file l'hash binario corrispondente al mittente. Il destinatario, così, andrà a verificare che l'hash che gli è arrivato via mail sia uguale a quello registrato.

  Parallelamente allo scambio sicuro, vi è la firma elettronica che altro non è che l'apposizione della propria firma sopra un documento. Oltre a questo, aziende come *Cursor Insight*, garantiscono, prima dell'inserimento sul file dell'autografo, una verifica biometrica dell'utente. Inoltre, l'utilizzo di questa tipologia di firma garantisce di conoscere chi sono stati i vari autori e chi ha eseguito le eventuali modifiche al documento, informazioni molto importanti a livello aziendale.

  Facendo un breve excursus sulla firma elettronica, è stata creata come forma di crittografia per validare un documento. Infatti, per la Legislazione Italiana, ai sensi del D.P.R. n.513/1997 e relativi Regolamenti Attuativi, la firma digitale si presenta come un sistema che sigla e consente di attestare l'autenticità di un documento che è stato trasmesso per via informatica (Internet, posta elettronica, reti locali, memorie portatili ecc.)". La firma elettronica altro non è che un software di criptatura che viene rilasciato grazie ad apposite società, dette certificatori. Quest'ultimo andrà a verificare l'identità dell'utente e a creare in primis un certificato di identità, correlato da due chiavi personali, le quali verranno inserite in una smart card che contiene in memoria i dati per l'identificazione. Questa, in secondo luogo, verrà attivata grazie ad un codice segreto che l'utente dovrà digitare.

Oggigiorno si sta appunto pensando di utilizzare delle caratteristiche biometriche del firmatario del documento per aumentare notevolmente l'autenticità dei documenti informatici.

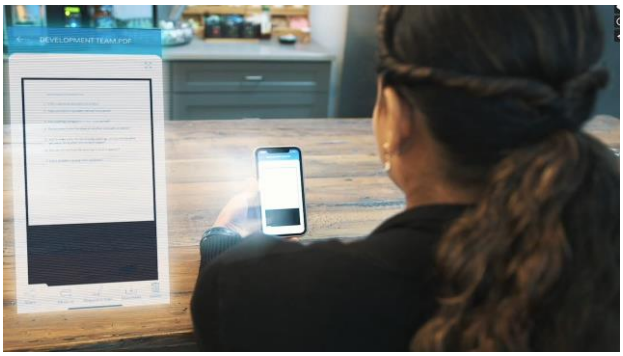


Figura 44: Soluzione di controllo facciale per i file di *Smart Eye*

- **Verifica dei documenti**: considera la biometria applicata alla verifica dei documenti, con il fine di poter convalidare l'identità della persona senza che vi sia la necessità di una sua registrazione svolta in precedenza.
  Si va ad esempio, come previsto da *Veriff*, a verificare la caratteristica facciale, facendo una comparazione tra un selfie e l'immagine presente sopra il documento di identità, come può essere il passaporto o la patente. Si parte con l'intenzione, ad esempio, di aprire un conto corrente online. In seguito, viene indicato sullo schermo di scattarsi un selfie e successivamente l'algoritmo elaborerà la verifica dell'identità. Tendenzialmente, per poter compiere un riconoscimento esatto dell'utente, si va anche incontro ad un processo di acquisizione corretta delle immagini, oltre che ad una verifica della vitalità. Contestualmente a questo, interviene anche un software in grado di elaborare l'immagine del documento, al fine di poter trascrivere autonomamente le informazioni presenti, e così da lasciare all'utente solo il facile compito di convalidare i dati inseriti automaticamente dal software.
  In un secondo momento interviene un altro software, affinché vengano confrontate le informazioni appena raccolte con quelle già presenti all'interno dei database governativi, luoghi dove sono registrati i dati dei cittadini. Questa operazione permette quindi di validare anche il documento di per sé.
  Il metodo appena descritto garantisce l'onboarding dei clienti in maniera snella, facile e veloce, permettendo di concludere il processo in meno di tre minuti, dei quali neanche quindici secondi sono dedicati al riconoscimento facciale.
  Obiettivo principale di questa applicazione è quello di fermare, o, quantomeno rendere più complicate, le frodi.

Altro esempio di caratteristica biometrica utilizzata è quella dell'impronta digitale. Tecnologia che è sviluppata particolarmente nei territori asiatici in cui, specialmente nei luoghi pubblici, viene verificata la corrispondenza dell'impronta presa in quel momento rispetto a quella registrata presso l'ente governativo. Più specificatamente, può intervenire la tecnologia per riconoscere l'individuo arrivato alla frontiera con il visto e il passaporto.

Questi due casi appena mostrati rappresentano sempre la verifica del documento, ma messi in atto in due contesti diversi, perché per il primo si parla del mondo online, mentre per il secondo si parla del mondo offline.
Ci sono poi aziende che, al posto di dare una soluzione chiave in mano, concordano con gli interessati una sequenza personalizzata, magari richiedendo un numero maggiore di informazioni.
All'interno di questa applicazione sono state considerate solo e unicamente le aziende che, grazie al loro sito, si è appreso che non sfruttavano tecnologie appartenenti a partner (fattore principalmente presente nelle aziende più strutturate che garantivano la proprietà del software di riconoscimento facciale).
Ci sono poi aziende come *Voatz* che utilizzano sempre il riconoscimento facciale per la verifica del documento, ma che si sono ancora più specializzate, andando a studiare la tecnologia in questione più nel dettaglio. In particolare, la società in questione, si occupa del riconoscimento dell'identità dell'individuo nel momento in cui è chiamato a compiere il suo dovere di cittadino in occasione di votazioni, siano esse comunali, provinciali o nazionali. Quindi l'azienda Voatz, oltre a sfruttare la tecnologia biometrica, si occupa anche della sicurezza per le votazioni al governo.

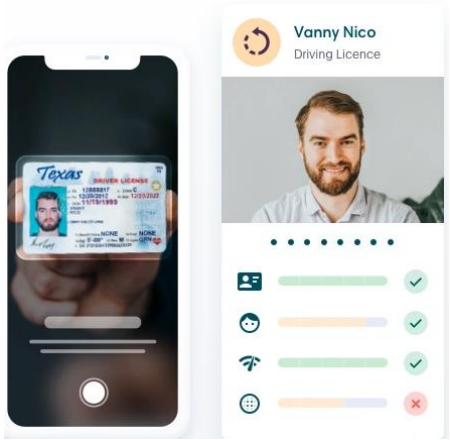


Figura 45: Face Match di *Veriff*

- **Esami**: applicazione che va ad inserire quelle aziende che lavorano, anche e soprattutto, in ambito scolastico, per effettuare una verifica sul soggetto che sta svolgendo l'esame.
  Si pensava di inserirlo all'interno degli accessi, dato che le società interessate lavorano in special modo in campi del controllo degli accessi, ma è stato voluto effettuare una seppur lieve differenziazione, in modo da vedere se e quanto è stato finanziato, pur non conoscendo tuttavia il valore preciso.
  Per quanto riguarda il livello di partecipazione alle lezioni da parte degli studenti, ci si è posti la domanda se potesse essere utile creare un'applicazione separata o meno, ma alla fine si è pensato di inserire questa funzione nell'applicazione già esistente, dal momento che l'obiettivo finale è il medesimo.

- **Assistenza alla clientela**: si sostanzia nella verifica dell'identità dell'individuo che sta contattando il call center o il centro assistenza. Questa applicazione, simile a quanto detto per l'autenticazione online con i chatbot, serve soprattutto per avere una maggior sicurezza nella convalida del fatto che il soggetto con cui si sta parlando sia effettivamente la persona giusta, e non rischiando così di divulgare informazioni personali e riservate a qualcuno che non è l'effettivo titolare del diritto.

Applicazione che in realtà è il cosiddetto "gran paniere" è l'IAM (Identity and Access Management), acronimo con cui si intende l'insieme dei sistemi che permettono alle organizzazioni di controllare e facilitare gli accessi degli utenti, proteggendo i dati personali da ingressi non autorizzati.
In sostanza, ci si assicura che solo gli individui effettivamente a ciò autorizzati abbiano il corretto accesso ai propri dati, applicazioni e risorse. Molte aziende si stanno approcciando ai servizi, essendo il database locale quasi ormai diventato obsoleto. L'IAM permette di garantire agli utenti, indipendentemente dal fatto che si tratti di macchine o umani, di ottenere l'accesso solo alle risorse a cui hanno diritto. Per di più si stima che più del 90% delle aziende ritiene che l'autenticazione senza password rappresenti il futuro.

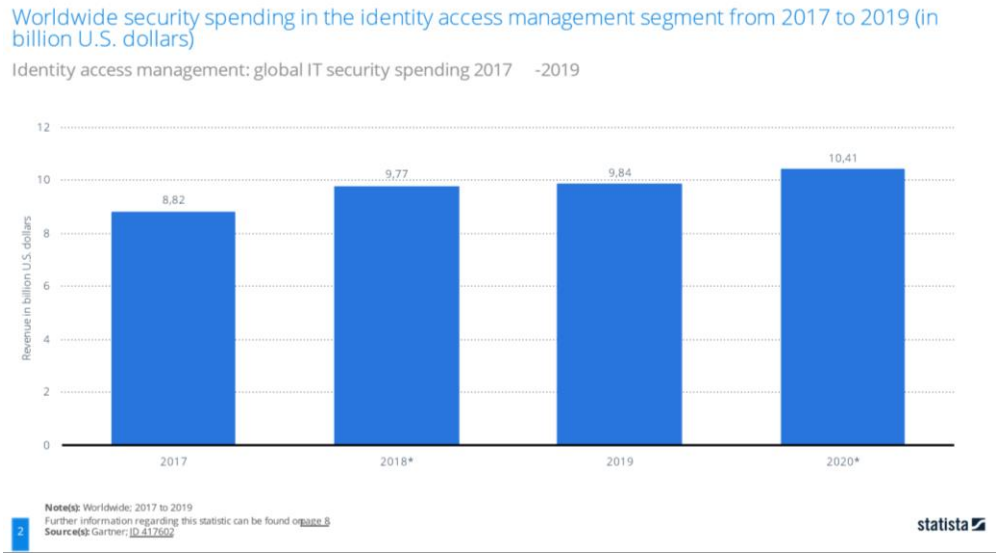


Figura 46: Spesa crescente mondiale per l'IAM

Esempi di aziende incentrate in questa visione ampia dell'accesso sono *HYPR* e *Msite*. Queste due compagnie, che hanno raccolto rispettivamente 67.1 milioni di dollari e due milioni di dollari nel 2008 (poi acquista poi nel 2021 da *Infobric*), presentano fattori biometrici all'interno dei prodotti offerti, ma non essendo questo il business centrale delle aziende oppure perché viene utilizzata la tecnologia mobile, non sono state considerate all'interno della matrice dei finanziamenti.

3.1.1.1 Le novità

Parallelamente all'analisi delle aziende, sono state trovate delle società con pochi capitali ricevuti, che lavorano e concentrano le loro ricerche sulla messa a punto di altre applicazioni, che utilizzano sempre la biometria, ma si specializzano in uno o più campi applicativi "personalizzati".

Un esempio lampante di queste novità lo possiamo trovare nel lavoro effettuato da *Ayonix*, azienda giapponese che già sfrutta la tecnologia del riconoscimento facciale per diverse finalità, come il controllo degli accessi, le funzioni di sicurezza pubblica e verifica dei documenti. Oltre a queste funzionalità, utilizza il metodo appena citato anche per riconoscere i potenziali clienti mentre camminano in luoghi con alto "traffico", ossia molto frequentati, come lo possono essere i centri commerciali.

Figura 47: Sistema di *Ayonix* con i clienti presso il centro commerciale

Altro caso concreto lo possiamo rilevare guardando al lavoro di *Biometrica*, azienda americana che sfrutta già il riconoscimento facciale nell'ambito della sicurezza pubblica. Ha sviluppato una soluzione che utilizza la caratteristica del volto per effettuare dei controlli di sicurezza nei casinò e sale da gioco, al fine di sfruttare i video di sorveglianza per essere in grado di rilevare eventuali imbrogli da parte dei giocatori.

Terzo caso è rappresentato dalla *Dispension*, azienda canadese che sfrutta il riconoscimento venoso (quindi senza contatto) affinché vengano distribuiti i prodotti giusti alle persone che devono riceverli.
In sostanza, si tratta di distribuzione regolamentata. Consente di fornire un accesso sicuro e protetto alle sostanze controllate, come ad esempio alcuni medicinali che richiedono, per la commercializzazione, una ricetta medica apposita.

Figura 48: Prodotto di *Dispension*

Quarta soluzione è quella messa a punto da *Simprints Technology*, azienda no-profit inglese, che lavora con l'intento di sfruttare la conoscenza tecnologia della biometria per rendere più facile la rilevazione dello stato di salute delle persone che vivono nelle aree più povere e svantaggiate del pianeta. Qui, infatti, utilizza l'impronta digitale e il rilevamento facciale per identificare e schedare le persone, atti da cui sarà possibile ricavare il loro stato medico.

Figura 49: Prodotto di *Simprints Technology*

Infine, è stata trovata un'azienda americana, *Global e-dentity*, che sfrutta la tecnologia delle vene della mano unita allo schema osseo per effettuare il riconoscimento.
Come già abbiamo visto funzionare per l'ECG, il flusso sanguigno e il battito cardiaco forniscono un'ulteriore doppia prova di vita.

Figura 50: Funzionamento del prodotto di *Global e-dentity*

3.1.2 L'indice di Gini

Prima di presentare le matrici ricavate e le relative analisi, viene di seguito introdotto l'indice di Gini, che servirà ad elaborare i dati raccolti.
Il suddetto coefficiente di concentrazione è stato introdotto dallo statistico, economista e sociologo italiano da cui prende il nome, Corrado Gini, professore universitario prima e poi, dal 1941, Presidente e fondatore della società italiana di statistica, dove operò fino alla sua morte, avvenuta nel 1965.
L'indice è usato notoriamente per far fronte all'analisi della diseguaglianza che sussiste nella distribuzione del reddito nella popolazione, o nella sua ricchezza (anche se può essere usato in altri ambiti) e restituisce una valutazione compresa tra 0 e 1. Più ci si avvicina a numeri bassi, quindi tendenti lo zero, più si avrà una distribuzione omogenea, fino ad arrivare all'equa distribuzione del reddito (situazione ideale e utopica, dal momento che si creerebbe solo in quei casi in cui tutti gli individui percepiscano lo stesso reddito). All'aumentare dell'indice si avranno situazioni sempre più tendenti alla diseguaglianza, fino ad arrivare a 1 in cui si avrà la massima concentrazione del reddito, dove si avrà la situazione in cui una persona percepisce tutto il reddito del paese, mentre tutti gli altri avranno un reddito nullo.
Prima di spiegare come si calcola il coefficiente di Gini, bisogna introdurre la curva di Lorenz (studiata da M. Lorenz in cui nel 1905 riuscì a mostrare la distribuzione del reddito), sulla cui definizione matematica si basa il coefficiente di Gini stesso.

Per la costruzione del grafico bisogna effettuare i seguenti passaggi:

1. Mettere in ordine crescente i redditi/capitali (o le osservazioni), andrà a rappresentare la colonna Xi.

2. Si inseriscono i numeri naturali a fianco della colonna fino alla cifra pari le osservazioni, andrà a rappresentare la colonna i.

3. Si calcolano le percentuali di osservazioni, a fianco della colonna, calcolato come i/N (con N il totale delle osservazioni), andrà a rappresentare la colonna Pi.
   Bisogna controllare che l'ultima riga del suddetto verticale sia pari a 1.

4. Si calcolano i rapporti rappresentanti la quantità cumulata di osservazioni sul totale di osservazioni calcolata come la somma fino i-esimo Xi diviso la somma di tutti gli Xi, andrà a rappresentare la colonna Qi.
   Bisogna controllare che l'ultima riga del suddetto verticale sia pari a 1.

Socio (i)	Capitale	A_i	Q_i	P_i
1	25	25	25/1475 = 0.0169	1/7 = 0.1429
2	89	25+89 = 114	114/1475 = 0.0773	2/7 = 0.2857
3	106	114+106 = 220	220/1475 = 0.1492	3/7 = 0.4286
4	155	220+ 155 = 375	375/1475 = 0.2542	4/7 = 0.5714
5	223	375+223 = 598	598/1475 = 0.4054	5/7 = 0.7143
6	368	598+368 = 966	966/1475 = 0.6549	6/7 = 0.8571
7	509	966+509 = 1475	1475/1475= 1	7/7 = 1
Totale	1475		1.5580	3

Tabella 1: Esempio calcolo curva di Lorenz

Per disegnare la curva di Lorenz si andranno ad inserire i valori Pi nell'asse delle ascisse e i Qi nell'asse delle ordinate. Si creerà quindi la "spezzata di concentrazione" o curva di Lorenz.
In seguito, bisognerà tracciare la linea di "equiripartizione" inserendo sia per l'asse delle x sia per l'asse delle y i valori degli Pi.

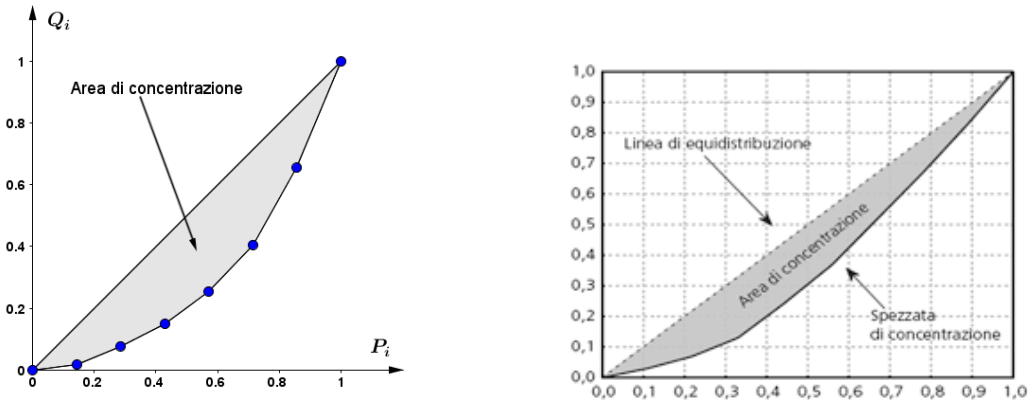


Figura 51: Rappresentazione curva di Lorenz

Quindi, più la curva di Lorenz andrà ad avvicinarsi fino a ricalcare la linea di equidistribuzione, più si avrà una distribuzione equa, ad esempio, del reddito (nel caso di massima concentrazione la spezzata di concentrazione o curva di Lorenz sarebbe caratterizzata da una forma a L).

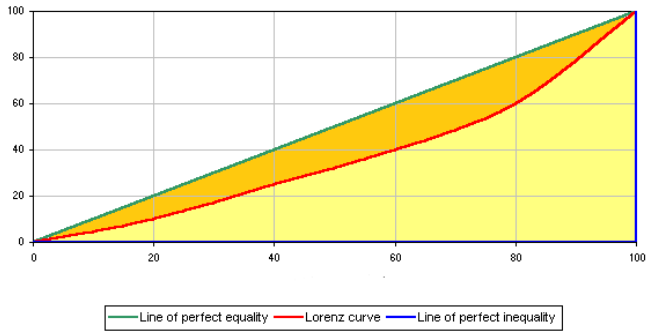


Figura 52: Casi della curva di Lorenz

Inoltre succederà che, all'aumentare della sovrapposizione della spezzata nei confronti della retta, diminuirà via via l'indice di Gini essendo l'area che si trova tra le due curve. Infatti esistono principalmente due modi per calcolare matematicamente il coefficiente:

- **Metodo semplice** (quello poi utilizzato per l'elaborazione dei dati): Si andrà a svolgere il rapporto tra la differenza puntuale tra la retta e la spezzata con la somma dei valori della linea di equidistribuzione. La formula è la seguente:

$$g = \frac{\sum_{i=1}^{n-1}(p_i - q_i)}{\sum_{i=1}^{n-1} p_i}$$

$$Gini = \frac{[(0.1429 + 0.2857 + 0.4286 + 0.5714 + 0.7143 + 0.8571) - (0.0169 + 0.0773 + 0.1492 + 0.2542 + 0.4054 + 036549)]}{(0.1429 + 0.2857 + 0.4286 + 0.5714 + 0.7143 + 0.8571)}$$

- **Metodo del trapezio**: si va a calcolare l'area di concentrazione effettuando la differenza tra l'area di metà quadrato lato 1, quindi 1/2, con l'area del trapezio al di sotto della spezzata (si hanno basi Qi e Qi+1). Quindi si ha la seguente formula:

$$S = \frac{1}{2} - \frac{1}{2}\sum_{i=0}^{n-1}(q_i + q_{i+1})(p_{i+1} - p_i)$$

L'indice di Gini andrà quindi a rapportarsi al caso di massima concentrazione cioè pari all'area di metà quadrato, quindi 1/2.

$$R = \frac{\frac{1}{2} - \frac{1}{2}\sum_{i=0}^{n-1}(q_i + q_{i+1})(p_{i+1} - p_i)}{\frac{1}{2}}$$

Arrivando quindi ad avere la formula finale con il metodo del trapezio:

$$R = 1 - \sum_{i=0}^{n-1}(q_i + q_{i+1})(p_{i+1} - p_i)$$

Si avranno con i due metodo valori non esattamente uguali, ma comunque molto vicini.

In realtà esistono altri indici di concentrazione possibili, come quello di Herfindahl, ma l'indice di Gini tiene maggiormente in considerazione, rispetto ad HHI, le aziende con livelli bassi di finanziamento. Poichè ci sono molte imprese che hanno ricevuto un basso ammontare di denaro si ritiene che l'indice di Gini possa rappresentare meglio questo contesto.

3.2 Il Database

Qui di seguito vengono riportate le suddivisioni per ogni incrocio tecnologia-applicazione andando a mostrare i vari finanziamenti in milioni di dollari (1999-2020) ricevuti dalle aziende considerate.

Controllo accessi edifici/ Controllo presenze		Identificazione criminali Controlli di sicurezza (es. aeroporto)		Avviamento veicoli/ macchine industriali	Accesso PC/ Telefono		Autenticazione remota su internet (es. Servizi bancari, account streaming)	
Biosec	0,15	BI2 Technologies	0,28		Biosec	0,15	Crayonic	0,18
Chipsailing	0,50	Warwick Warp Ltd	0,95		Crayonic	0,18	Fortress Identity	0,75
ievo	0,76	Identification International, Inc – i3	1,72		Chipsailing	0,50	Touch Biometix	1,01
Warwick Warp Ltd	0,95	IDmission	2,60		Touch Biometix	1,01	Diamond Fortress Technologies	1,26
QuardLock	0,97	Integrated Biometrics	4,75		Precise Biometrics	1,75	Bio-Key International	1,85
BIODIT GLOBAL TECHNOLOGY	1,00	Isorg	8,95		Nymi	4,54	Nymi	4,54
Bioconnect	1,95	Tascent	12,67		Isorg	8,95	Facephi	5,72
Eyecool	2,51				Delta ID	41,53	Validity Sensors	54,60
BioSITE Systems	2,73				Validity Sensors	54,60		
INVIXIUM	3,32				AuthenTec	502,00		
Isorg	4,47							
Nymi	4,54							
FINGER CRYSTAL	5,11							
Dessmann	30,50							
Delta ID	41,53							
	100,99		31,91			615,21		69,90

Transazioni online/ bancomat		Firma digitale/ protezione e scambio sicuro di documenti		Verifica documenti		Esami		Controllo presenze		Call Center
Biosec	0,15	Crayonic	0,18	Chipsailing	0,50	Eyecool	2,51	BIODIT GLOBAL TECHNOLOGY	1,00	
Chipsailing	0,50	Veri5Digital	0,67	Haijing Yun Pingtai	1,01			INVIXIUM	3,32	
QuardLock	0,97	Nymi	4,54	Diamond Fortress Technologies	1,26			Easy Clocking	3,33	
Touch Biometix	1,01			Incode	6,05			Isorg	4,47	
A3BC	1,53									
Precise Biometrics	1,75									
Case	2,30									
Fingpay	3,50									
Veridium	5,55									
CardLab	8,40									
Isorg	8,95									
IDEX Biometrics	10,83									
Net1 UEPS Technologies, Inc	31,20									
Delta ID	41,53									
Zwipe	42,05									
Validity Sensors	54,60									
	214,83		5,38		8,81		2,51		12,12	

Tabella 2: Finanziamenti complessivi ricevuti per applicazioni delle aziende che sfruttano la biometria dell'**impronta digitale**

Controllo accessi edifici/ Controllo presenze		Identificazione criminali Controlli di sicurezza (es. aeroporto)		Avviamento veicoli/ macchine industriali	Accesso PC/ Telefono		Autenticazione remota su internet (es. Servizi bancari, account streaming)	
J2C	0,06	TECH5	-		J2C	0,06	Eyecool	1,26
Iristar	0,45	BI2 Technologies	0,28		IrisKing	6,43		
CMI TECH	0,53	Iristar	0,89					
Eyecool	1,26	Tascent	6,33					
Princeton Identity	2,00	Homsh Tech	13,90					
EyeLock	3,00							
IrisKing	3,22							
Iridian Technologies	5,00							
Tascent	6,33							
Homsh Tech	13,90							
Clear	17,50							
	53,24		21,40			6,49		1,26

Transazioni online/ bancomat		Firma digitale/ protezione e scambio sicuro di documenti		Verifica documenti	Esami		Controllo presenze		Call Center
J2C	0,06	Veri5Digital	0,67		Eyecool	1,26	Iristar	0,45	
Eyecool	1,26						CMI TECH	0,53	
FacePhi	5,72						IrisKing	3,22	
IrisKing	6,43						Easy Clocking	3,33	
	13,46		0,67			1,26		7,52	

Tabella 3: Finanziamenti complessivi ricevuti per applicazioni delle aziende che sfruttano la biometria dell'**iride**

Controllo accessi edifici/ Controllo presenze		Identificazione criminali Controlli di sicurezza (es. aeroporto)	Avviamento veicoli/ macchine industriali		Accesso PC/ Telefono	Autenticazione remota su internet (es. Servizi bancari, account streaming)	
Normee Limited	0,71		Normee Limited	0,71		Q5id	5,15
						Bio-Key International	1,85
						Normee Limited	0,71
	0,71			0,71			7,71

Transazioni online/ bancomat		Firma digitale/ protezione e scambio sicuro di documenti	Verifica documenti	Esami	Controllo presenze	Call Center
Normee Limited	0,71					
	0,71					

Tabella 4: Finanziamenti complessivi ricevuti per applicazioni delle aziende che sfruttano la biometria della **geometria della mano**

Controllo accessi edifici/ Controllo presenze		Identificazione criminali Controlli di sicurezza (es. aeroporto)		Avviamento veicoli/ macchine industriali		Accesso PC/ Telefono		Autenticazione remota su internet (es. Servizi bancari, account streaming)	
Normee Limited	0,71	Weidun Keji	3,07	Normee Limited	0,71	Biowatch	0,91	Normee Limited	0,71
Biowatch	0,91								
Weidun Keji	3,07								
	4,68		3,07		0,71		0,91		0,71

Transazioni online/ bancomat		Firma digitale/ protezione e scambio sicuro di documenti	Verifica documenti	Esami	Controllo presenze	Call Center
Normee Limited	0,71					
Biowatch	0,91					
	1,62					

Tabella 5: Finanziamenti complessivi ricevuti per applicazioni delle aziende che sfruttano la biometria delle **vene della mano**

Controllo accessi edifici/ Controllo presenze		Identificazione criminali Controlli di sicurezza (es. aeroporto)		Avviamento veicoli/ macchine industriali	Accesso PC/ Telefono		Autenticazione remota su internet (es. Servizi bancari, account streaming)	
Nymi	4,54				Nymi	4,54	Nymi	4,54
	4,54					4,54		4,54

Transazioni online/ bancomat	Firma digitale/ protezione e scambio sicuro di documenti		Verifica documenti	Esami	Controllo presenze	Call Center
	Nymi	4,54				
		4,54				

Tabella 6: Finanziamenti complessivi ricevuti per applicazioni delle aziende che sfruttano la biometria del **battito**

Controllo accessi edifici/ Controllo presenze		Identificazione criminali Controlli di sicurezza (es. aeroporto)		Avviamento veicoli/ macchine industriali	Accesso PC/ Telefono		Autenticazione remota su internet (es. Servizi bancari, account streaming)	
Saffe	0,03	Customer Clever	0,10		Sensory Inc.	0,20	Faceki	0,01
Customer Clever	0,10	HongJian Technology	0,15		Securlinx	0,43	Saffe	0,03
OneVisage	0,15	Facebox	0,23		Keyless	1,03	OneVisage	0,15
HongJian Technology	0,15	CyberExtruder	0,25		Keylemon	1,53	Veri5Digital	0,33
CyberExtruder	0,25	Facewatch	0,33		Veridium	2,78	Fortress Identity	0,38
unike.TECH	0,28	Biometrica	0,40				Eyecool	0,84
Facewatch	0,33	Securlinx	0,43				ID R&D	0,95
Securlinx	0,43	Haijing Yun Pingtai	0,50				Keyless	1,03
Iristar	0,45	3D Face	0,67				Smart Eye Technology	1,75
CMI TECH	0,53	Eyecool	0,84				FacePhi	1,91
Clockster	0,55	Iristar	0,89				Smile Identity	2,05
3D Face	0,67	3DiVi, Inc.	0,90				Veridium	2,78
GTRIIP	0,75	Deepsense	1,01				Trust Stamp	5,15
Eyecool	0,84	eConnect	2,00				Q5id	5,15
3DiVi, Inc.	0,90	Travizory	2,35				authID.ai	9,87
ID R&D	0,95	Corsight	2,50					
Deepsense	1,01	Trueface	2,50					
FaceOS	1,55	IntelliVision	3,00					
Qigu Technolgy	1,55	FaceFirst	4,78					
Blink Identity	1,62	Ntechlab	5,50					
Bioconnect	1,95	VisionLabs B.V.	5,50					
Princeton Identity	2,00	Tascent	6,33					
PopID	2,50	Paravision	7,25					
Trueface	2,50	Watrix	7,25					
Corsight	2,50	Clearview	8,60					
BioSITE Systems	2,73	Kairos AR	10,95					
IntelliVision	3,00	BriefCam	16,50					
INVIXIUM	3,32	Faceter	28,60					
Precise Biometrics	3,50	AnyVision	58,50					
Moredian	4,45	Intellifusion	93,20					
FaceFirst	4,78	Digital signal	109,90					
Oloid AI	5,00							
Ntechlab	5,50							
Tascent	6,33							
Paravision	7,25							
StoneLock	7,45							
Alcatraz	13,80							
Clear	17,50							
Intellifusion	46,60							
AnyVision	58,50							
	214,23		381,92			5,97		32,37

Transazioni online/ bancomat		Firma digitale/ protezione e scambio sicuro di documenti		Verifica documenti		Esami		Controllo presenze		Call Center
Saffe	0,03	Keyless	1,03	Faceki	0,01	Faceki	0,01	Iristar	0,45	
Passid	0,04	Smart Eye Technology	1,75	Saffe	0,03	HongJian Technology	0,15	CMI TECH	0,53	
OneVisage	0,15	Trust Stamp	5,15	Passid	0,04	Clockster	0,55	PayrollHero	1,00	
unike.TECH	0,28	Post-Quantum	5,60	Facebox	0,23	Eyecool	0,84	INVIXIUM	3,32	
Payface	0,49	Yoti	11,17	Veri5Digital	0,33	Ntechlab	5,50	Easy Clocking	3,33	
Eyecool	0,84			Preventor	0,35			Moredian	4,45	
IDmission	1,30			iDenfy	0,37			Intellifusion	46,60	
FacePhi	1,91			Fortress Identity	0,38					
PopID	2,50			Haijing Yun Pingtai	0,50					
SWIP	2,70			Biometric Signature ID	0,65					
Weixuanke	3,25			3D Face	0,67					
Paravision	7,25			GTRIIP	0,75					
Element	9,03			Eyecool	0,84					
authID.ai	9,87			RapidID.com	0,88					
				3DiVi, Inc.	0,90					
				ID R&D	0,95					
				IDmission	1,30					
				Sensity	1,41					
				Ariadnext	1,70					
				Truora	1,73					
				Youverify	1,85					
				FacePhi	1,91					
				Smile Identity	2,05					
				Polygon	2,20					
				Ondato	2,64					
				Blinking	2,82					
				Thirdfort	3,33					
				Passbase	4,20					
				Voatz	4,64					
				Trust Stamp	5,15					
				Incode	6,05					
				Paravision	7,25					
				Authenteq	7,34					
				Vouched	7,40					
				Sumsub	7,50					
				Element	9,03					
				authID.ai	9,87					
				ID checker	10,60					
				Yoti	11,17					
				Berbix	11,62					
				Signzy	12,60					
				Icar	15,00					
				Mitek System	15,80					
				Mati	16,50					
				Persona	17,50					
				Fourthline	19,50					
				Veriff	23,30					
				ID.me	55,27					
				Jumio	55,40					
				AU10TIX	80,00					
				Advance.AI	136,00					
				Onfido	193,21					
	39,62		24,70		772,69		7,05		59,67	

Tabella 7: Finanziamenti complessivi ricevuti per applicazioni delle aziende che sfruttano la biometria del **volto**

Controllo accessi edifici/ Controllo presenze		Identificazione criminali Controlli di sicurezza (es. aeroporto)		Avviamento veicoli/ macchine industriali		Accesso PC/ Telefono		Autenticazione remota su internet (es. Servizi bancari, account streaming)	
Biometricvox	0,59	VoiceAI	0,52	MyVoice	2,19	Crayonic	0,18	Crayonic	0,18
ID R&D	0,95	AGNITiO	10,49			Sensory Inc.	0,20	V2verify	0,50
MyVoice	2,19							VoiceAI	0,52
								Fortress Identity	0,75
								ValidSoft	0,95
								ID R&D	0,95
								VoiceVault	1,79
	3,73		11,00		2,19		0,38		5,63

Transazioni online/ bancomat		Firma digitale/ protezione e scambio sicuro di documenti		Verifica documenti		Esami	Controllo presenze	Call Center	
ValidSoft	0,95	Crayonic	0,18	Truora	1,73			VoiceAI	0,52
MyVoice	2,19	Biometricvox	0,59					ID R&D	0,95
FacePhi	2,86	Post-Quantum	5,60					IDmission	2,60
								FacePhi	2,86
								Voatz	4,64
								Omilia	20,00
								Validity Sensors	163,80
								Pindrop	212,80
	5,99		6,37		1,73				408,16

Tabella 8: Finanziamenti complessivi ricevuti per applicazioni delle aziende che sfruttano la biometria della **voce**

Controllo accessi edifici/ Controllo presenze	Identificazione criminali Controlli di sicurezza (es. aeroporto)	Avviamento veicoli/ macchine industriali	Accesso PC/ Telefono		Autenticazione remota su internet (es. Servizi bancari, account streaming)	
			Crayonic	0,18	Crayonic	0,18
			Biometric Signature ID	0,32	Biometric Signature ID	0,32
					Verifyoo	2,18
				0,50		2,68

Transazioni online/ bancomat	Firma digitale/ protezione e scambio sicuro di documenti		Verifica documenti	Esami	Controllo presenze	Call Center
	Crayonic	0,18				
		6,54				

Tabella 9: Finanziamenti complessivi ricevuti per applicazioni delle aziende che sfruttano la biometria della **scrittura - firma**

Controllo accessi edifici/ Controllo presenze	Identificazione criminali Controlli di sicurezza (es. aeroporto)		Avviamento veicoli/ macchine industriali	Accesso PC/ Telefono	Autenticazione remota su internet (es. Servizi bancari, account streaming)
	Watrix	7,25			
		7,25			

Tabella 10: Finanziamenti complessivi ricevuti per applicazioni delle aziende che sfruttano la biometria della **camminata** (restanti voci pari a zero)

Controllo accessi edifici/ Controllo presenze	Identificazione criminali Controlli di sicurezza (es. aeroporto)	Avviamento veicoli/ macchine industriali	Accesso PC/ Telefono		Autenticazione remota su internet (es. Servizi bancari, account streaming)	
			TWOSENSE.AI	1,8	Fortress Identity	0,75
					Zighra	1
					TWOSENSE.AI	1,8
					Digital fingerprints	2
					Cybertonica	2,415
					Keyless	3,1
					ThreatMark	3,56083
					Nethone	3,9
					Veridium	5,55
					Plurilock	6,503
					Intensity Analytics	8,5
					Typingdna	8,92
					SecuredTouch	11,5
					Revelock	14,55
					Appmobi	15,4
					UnifyID	20
					BehavioSec	25,052
					AimBrain	26,19795
					Callsign	38,75
					Featurespace	113,5
					BioCatch	213,7
				1,80		526,65

Tabella 11: Finanziamenti complessivi ricevuti per applicazioni delle aziende che sfruttano la biometria del **comportamento digitale** (restanti voci pari a zero)

La suddivisione geografica delle aziende considerate è la seguente:

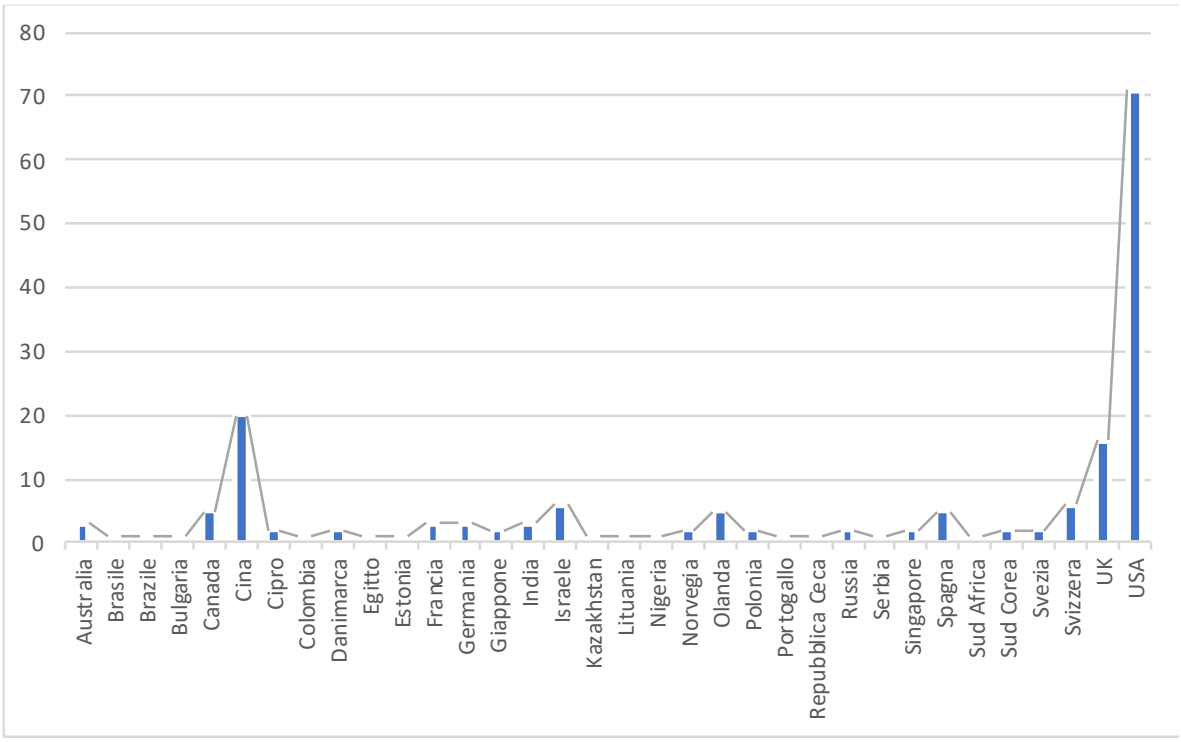


Figura 53: Disposizione geografica delle aziende considerate

3.3 L'analisi dei risultati

Nei paragrafi che seguono si presentano i vari risultati ottenuti dalla ricerca brevettuale e dalla creazione del database, in base alla metodologia sopra esposta.
In particolare, per esprimere meglio il concetto basato sull'analisi dei finanziamenti, si procede a suddividere la trattazione in due parti.
Nella prima si va a visionare i dati di insieme, cioè si guardano quelli complessivi dal nascere delle iniziali osservazioni fino al 2020, sia per i brevetti sia per l'ammontare dei finanziamenti.
In seguito, si suddividono le considerazioni spezzando in due periodi temporali la matrice finanziaria (fino al 2014 compreso e poi fino al 2020) e parallelamente si analizza il comportamento dell'indice di Gini.

3.3.1 I brevetti

Prima di iniziare con l'analisi brevettuale, bisogna spiegare che, contrariamente a quanto viene esposto nel prossimo paragrafo, qui non si entra nel dettaglio dei vari ambiti applicativi esposti in precedenza, in quanto gli stessi brevetti non rientrano specificatamente in un campo piuttosto che in un altro.
Anzi, già nell'introduzione alla documentazione si cita questo fatto di multi-disciplinarietà della tecnologia, garantendo che la stessa possa esser usata parallelamente per diversi scopi.
Inoltre, non si può neanche ragionare come con i finanziamenti, dato che non è possibile "suddividere l'ammontare" in diversi ambiti, poiché fare questo implicherebbe una distorsione delle varie considerazioni fatte.
Non è stata percorsa neanche la strada di considerare tutti i brevetti indistintamente, in quanto si sarebbe andati nella direzione di avere un numero eccessivamente sovradimensionato dei brevetti.
Quindi, evidenziata la possibilità di "condivisione" delle informazioni, non sono state fatte analisi localizzate per incrocio tecnologia-applicazione, ma solo per tecnologia.

Prima di entrare nel merito dei vari risultati trovati, sussiste la necessità di evidenziare quali filtri sono stati inseriti all'interno del motore di ricerca dei brevetti, *PatentInspiration,* affinché venga spiegata il più esaustivamente la metodologia utilizzata.
Le voci inserite per ogni tecnologia sono le seguenti:

- Per l'**impronta digitale**: "*fingerprint authentication*" or "*fingerprint recognition*" or "*fingerprint identity*" or "*fingerprint biometric*";
- Per l'**iride**: "*iris authentication*" or "*iris recognition*" or "*iris identity*" or "*iris biometric*";
- Per la **retina**: "*retina authentication*" or "*retina recognition*" or "*retina* identity" or "*retina biometric*";
- Per la **geometria della mano**: "*hand geometry*";

- Per le **vene**: "*vein authentication*" or "*vein recognition*" or "*vein identity*" or "*vein biometric*" or "*vein pattern authentication*" or "*vein pattern recognition*" or "*vein pattern identity*" or "*vein pattern biometric*";

- Per il **battito**: "*ecg authentication*" or "*ecg recognition*" or "*ecg identity*" or "*ecg biometric*";

- Per il **volto**: "*face authentication*" or "*face recognition*" or "*face biometric*" or "*facial authentication*" or "*facial recognition*" or "*facial identity*" or "*facial biometric*" (contrariamente ad altri non è stato considerate il filto "*face identity*", in quanto alcuni brevetti presi a campione non riguardavano propriamente la biometria per l'identità);

- Per la **voce**: "*speaker authentication*" or "*speaker recognition*" or "*speaker identity*" or "*speaker biometric*";

- Per la **scrittura – firma**: "*signature authentication*" or "*signature recognition*" or "*signature identity*" or "*signature biometric*" or "*handwriting authentication*" or "*handwriting recognition*" or "*handwriting* identity" or "*handwriting biometric*";

- Per la **camminata**: "*gait authentication*" or "*gait recognition*" or "*gait identity*" or "*gait biometric*";

- Per il **comportamentale digitale**: "*keystroke dynamics*" or "*mouse dynamics*".

In seguito all'apposizione di queste parole chiave è stato trovato il seguente ammontare di brevetti pubblicati, suddiviso per tecnologia e loro andamento storico.

	TOTALI
Impronta digitale	10433
Riconoscimento iride	2665
Riconoscimento retina	47
Riconoscimento geometria della mano	57
Riconoscimento vene mano (vascolarizzazione)	1321
Riconoscimento ECG	23
Riconoscimento volto	23145
Riconoscimento voce	1246
Riconoscimento scrittura - firma	2113
Riconoscimento della camminata	371
Comportamentale digitale (es. movimento mouse, pressione dati su tastiera)	71

Figura 54: Brevetti totali negli anni

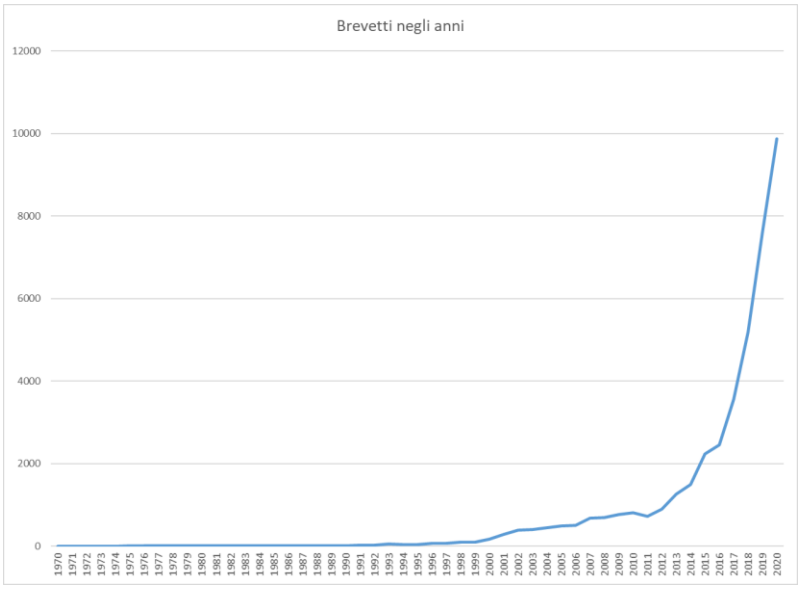


Figura 55: Numero di brevetti pubblicati negli anni

	1970	1971	1972	1973	1974	1975	1976	1977	1978	1979	1980	1981	1982	1983	1984	1985	1986	1987	1988	1989	1990	1991	1992	1993	1994	1995
Impronta digitale	1	1	0	0	0	3	2	0	1	0	0	0	0	0	0	0	0	4	2	4	3	8	4	4	6	6
Riconoscimento iride	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	2	1	1	0	0	0	0	0	0
Riconoscimento retina	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Riconoscimento geometria della mano	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	1	0	0	0	0	0	0	0	0
Riconoscimento vene mano (vascolarizzazione)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Riconoscimento ECG	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Riconoscimento volto	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	0	0	0	0	3	3	0	3
Riconoscimento voce	0	0	0	1	0	0	1	1	0	1	1	0	3	2	2	2	2	3	4	5	10	8	15	12	10	8
Riconoscimento scrittura - firma	0	0	1	0	0	1	1	1	1	3	2	5	1	3	0	2	0	3	0	1	1	6	8	27	22	26
Riconoscimento della camminata	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Comportamentale digitale (es. movimento mouse, pressione dati su tastiera)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	2	1	0	0	0	0	0	0
TOTALE	1	1	1	1	0	4	4	2	2	4	3	5	4	6	3	5	6	15	9	12	14	22	30	46	38	43

	1996	1997	1998	1999	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020
Impronta digitale	5	12	15	15	53	132	154	191	166	189	156	194	143	149	175	131	184	236	415	702	811	1186	1371	1587	2012
Riconoscimento iride	4	4	8	9	12	32	49	59	57	40	57	57	52	57	74	39	39	80	85	156	267	372	389	355	307
Riconoscimento retina	0	0	0	0	0	2	1	0	0	1	2	0	0	0	0	2	0	0	6	10	5	8	4	4	2
Riconoscimento geometria della mano	0	0	2	0	3	2	3	1	9	1	5	1	5	2	4	1	1	1	1	4	2	0	4	0	2
Riconoscimento vene mano (vascolarizzazione)	0	0	0	0	0	0	3	1	2	4	7	29	50	57	71	38	45	53	56	81	82	133	136	237	236
Riconoscimento ECG	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	4	2	7	5	3	2
Riconoscimento volto	6	10	13	13	18	26	67	75	100	130	166	258	308	363	357	398	503	762	766	1073	1137	1638	3021	5051	6871
Riconoscimento voce	12	11	27	32	36	27	26	20	36	35	28	45	47	34	37	26	34	38	52	67	48	56	91	130	160
Riconoscimento scrittura - firma	36	26	25	24	45	62	86	58	75	85	79	93	81	90	77	71	72	77	92	112	83	119	127	147	156
Riconoscimento della camminata	0	0	0	0	0	0	0	0	2	0	0	1	4	6	5	5	7	11	16	19	18	38	44	82	113
Comportamentale digitale (es. movimento mouse, pressione dati su tastiera)	0	0	0	0	2	0	3	0	2	1	1	2	0	8	3	5	5	4	3	7	0	1	4	9	7
TOTALE	63	63	90	93	169	283	392	405	449	486	501	680	690	766	803	716	890	1262	1492	2235	2455	3558	5196	7605	9868

Tabella 12: Suddivisione annuale per ogni singola tecnologia

Dai suddetti grafici si nota principalmente un aumento progressivo dell'attività brevettuale nell'ambito della biometria per l'identità.

In particolare, si evidenzia il fatto di trovare, specialmente negli anni più addietro (risalendo fino agli anni '90), singole tecnologie con brevetti sporadici. Infatti, su un totale di circa 46 mila brevetti nell'arco di cinquanta anni, in una ventina d'anni se ne trovano circa 20, quindi un'attività brevettuale decisamente irrisoria nell'ultimo periodo storico. Si può dire, quindi, senza ombra di dubbio, che ci si trovi attualmente in una fase totalmente divergente, dato che si è effettuato solo un minimo sforzo verso poche, o addirittura una sola, tecnologia, lasciando così le altre prive di brevetti.

Via via che si procede negli anni, ci sono tecnologie che “scompaiono” dal mondo dei brevetti, perché ad esempio non ci sono aziende che licenziano conoscenza o perché il mondo, non essendo ancora pronto per questo passo tecnologico importante per la vita quotidiana, non è interessato a che sia effettuata sempre più ricerca in quel particolare ambito.
Si hanno però ambienti in cui l’attività brevettuale continua ad essere viva nel tempo, come nel caso del riconoscimento della scrittura-firma e della voce. Potrebbero rientrare anche i metodi che fanno affidamento sulle impronte digitali e sul volto anche se, soprattutto negli anni iniziali dei primi brevetti nell’ambito della biometria per l’identità, non vi è notizia documentata di alcuna attività di ricerca.

Ci sono poi tecnologie, come il riconoscimento dell’ECG (corrispondente al battito cardiaco), che sono state prese in considerazione solo da pochi anni, seppure lievemente, attività soprattutto con il probabile aumento di affidamento, e di ricerca, del mondo dei wearable. Si sfrutta la tecnologia dietro l’orologio intelligente affinché si implementi questo metodo di riconoscimento, avendo già una base sostanziosa di hardware e software.

Caso “speciale” va attribuito al comportamentale digitale in cui l’attività brevettuale inizia a cavallo degli anni 2000 proprio con l’avvento di Internet, fattore che il metodo utilizza specialmente per i suoi relativi ambiti applicativi dell’autenticazione per gli account online.

Come curiosità si può notare che, nonostante ci sia stata la famosa bolla di Internet nei primi anni del 2000 e successivo “scoppio” e apprezzamento diffuso di questo nuovo utile strumento, non è stata abbandonata la tecnologia biometrica per l’identità, sebbene si sia perso molto affidamento e fiducia nei confronti di tutta la componentistica digitale che, invece, stava caratterizzando quel particolare momento storico.

In conclusione, quest’analisi grafica mostra che si parte da una fase in cui si hanno poche tecnologie studiate per avere negli anni sempre più attività brevettuale arrivando fino ai giorni nostri in cui tutte queste sono analizzate.

Entrando maggiormente nel dettaglio dello studio della concentrazione, si può ricavare il seguente grafico ottenuto con il metodo semplice:

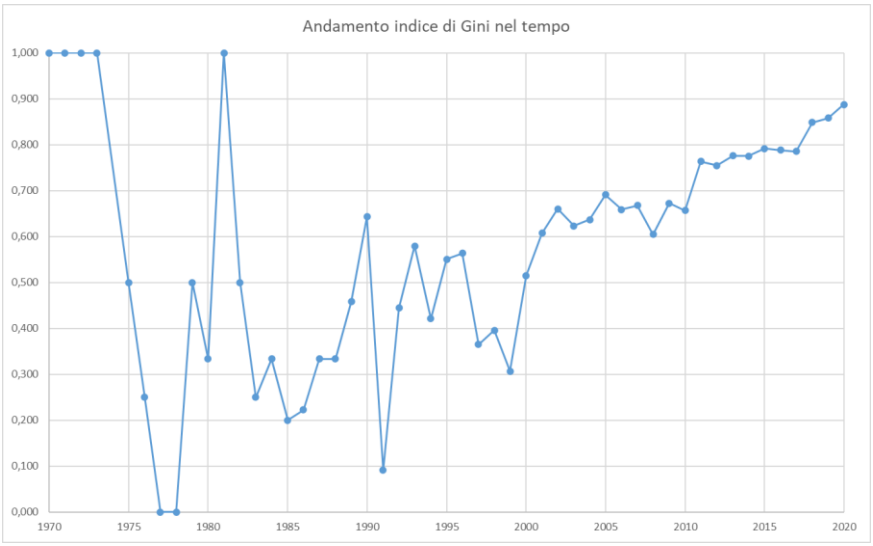


Figura 56: Andamento annuale dell'indice di Gini

Analizzando l'andamento, si può notare che si ha un trend crescente del coefficiente di Gini.
In particolare, non considerando gli anni iniziali che distorcono le considerazioni (valori massimi di concentrazione perché si ha una sola tecnologia o minimi avendo due tecnologie con pari numero di brevetti), si evidenzia una tendenza verso valori elevati.
Una volta stabilizzato l'andamento, quindi con l'inizio vero e proprio dell'attività di brevettazione (si inizia ad avere un certo numero di documenti scientifici tali da poter cominciare ad essere consistenti), si può evidenziare come il trend sia via via in aumento.
Si ha una sorta di "indecisione" iniziale, annotabile tra il 1991 e 1999, in cui si verifica un innalzamento vertiginoso di concentrazione dei brevetti, soprattutto per i metodi di riconoscimento che sfruttano la voce e la scrittura-firma, per poi scendere.
In seguito, l'indice di Gini inizia ad aumentare sempre più in concomitanza all'aumento evidente di brevetti per l'impronta digitale e il volto.

Analizzando tutti i periodi si vede che le tecnologie con attività brevettuale maggiormente attiva è quella relativa le impronte digitali e il volto. Fattore che si ripresenta sempre più "ricalcato" ogni anno dai primi del 2000.

i	Xi	Fi	Qi
1	23	0,09091	0,00055
2	47	0,18182	0,00169
3	57	0,27273	0,00306
4	71	0,36364	0,00477
5	371	0,45455	0,01371
6	1246	0,54545	0,04374
7	1321	0,63636	0,07558
8	2113	0,72727	0,12651
9	2665	0,81818	0,19074
10	10433	0,90909	0,44218
11	23145	1,00000	1,00000
	41492		

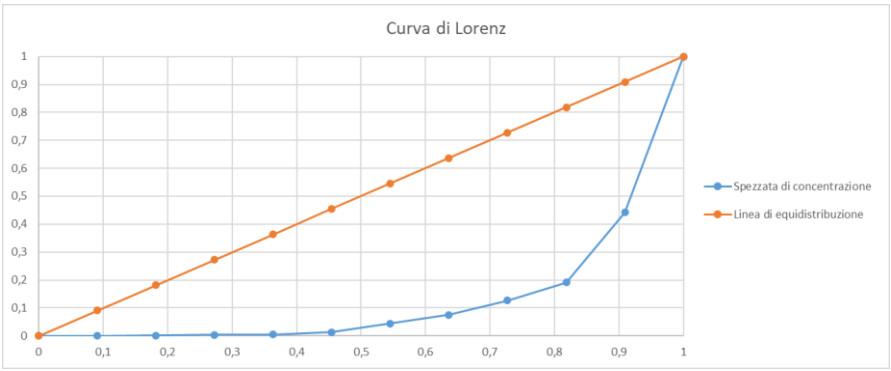


Figura 57: Curva di Lorenz considerando l'intero arco temporale dei brevetti (1970-2020)

Si nota che, considerando l'intero periodo temporale, si ha la spezzata che accentua la forma a L citata prima cioè verso valori di alta concentrazione. Infatti, calcolando l'indice di Gini (rappresenta l'area tra le due curve), si ha un valore pari a 0.819 caratterizzato dall'elevata attività brevettuale specificatamente con il metodo di riconoscimento delle impronte digitali e della fisionomia del volto.

Per concludere si nota che si ha un andamento inizialmente divergente per poi convergere e parallelamente un fenomeno di concentrazione verso pochi metodi specifici.
Fenomeno che va anche ad indicare quale può essere il dominant design sfruttando i brevetti come iniziale indicatore di evoluzione.

3.3.2 I finanziamenti

3.3.2.1 I finanziamenti complessivi (1999-2020)

In questa sezione vengono effettuate delle considerazioni sulla matrice dei finanziamenti ricevuti, nel periodo 1999-2020, dalle aziende considerate che lavorano nel mondo della biometria per l'identità.

MATRICE FINANZIAMENTI 1999-2020		APPLICAZIONI												
		Controllo accessi edifici	Identificazione criminali Controlli di sicurezza (es. aeroporto)	Avviamento veicoli/ macchine industriali	Accesso PC/ Telefono	Autenticazione remota su internet (es. Servizi bancari, account streaming)	Transazioni online/ bancomat	Firma digitale/ protezione e scambio sicuro di documenti	Verifica documenti	Esami	Controllo presenze	Assistenza clienti		
TECNOLOGIE	Impronta digitale	100,99	31,91	0,00	615,21	69,90	214,83	5,38	8,81	2,51	12,12	0,00	1061,67	28,47%
	Riconoscimento iride	53,24	21,40	0,00	6,49	1,26	13,46	0,67	0,00	1,26	7,52	0,00	105,29	2,82%
	Riconoscimento retina	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00%
	Riconoscimento geometria mano	0,71	0,00	0,71	0,00	7,71	0,71	0,00	0,00	0,00	0,00	0,00	9,86	0,26%
	Riconoscimento vene mano (vascolarizzazione)	4,68	3,07	0,71	0,91	0,71	1,62	0,00	0,00	0,00	0,00	0,00	11,70	0,31%
	Riconoscimento battito	4,54	0,00	0,00	4,54	4,54	0,00	4,54	0,00	0,00	0,00	0,00	18,15	0,49%
	Riconoscimento volto	214,23	381,92	0,00	5,97	32,37	39,62	24,70	772,69	7,05	59,67	0,00	1538,20	41,25%
	Riconoscimento voce	3,73	11,00	2,19	0,38	5,63	5,99	6,37	1,73	0,00	0,00	408,16	445,17	11,94%
	Riconoscimento scrittura - firma	0,00	0,00	0,00	0,50	2,68	0,00	0,18	0,00	0,00	0,00	0,00	3,36	0,09%
	Riconoscimento camminata	0,00	7,25	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	7,25	0,19%
	Comportamentale digitale (es. movimento mouse, pressione dati su tastiera)	0,00	0,00	0,00	1,80	526,65	0,00	0,00	0,00	0,00	0,00	0,00	528,45	14,17%
		382,11	456,54	3,61	635,80	651,45	276,24	41,83	783,22	10,81	79,31	408,16	3729,10	
		10,25%	12,24%	0,10%	17,05%	17,47%	7,41%	1,12%	21,00%	0,29%	2,13%	10,95%		

Tabella 13: Curva di Lorenz considerando l'intero arco temporale dei brevetti (1970-2020)

La suddetta immagine mostra l'ammontare complessivo di denaro per ogni incrocio tecnologia-applicazione.
Analizzando in prima battuta le varie tecnologie (quindi le linee orizzontali della matrice) si notano diversi fattori molto interessanti. Innanzitutto si ha evidenza che tra le circa 180 aziende visionate, nessuna effettivamente utilizza il metodo di riconoscimento basato sulla retina. Questo va a supporto dei punti citati nel capitolo precedente, cioè che si sta sempre parlando di una tecnologia poco matura e poco presa in considerazione, e parallelamente molto costosa. In particolare quest'ultimo punto poi rende l'applicazione abbastanza complessa, in quanto il denaro investito per la ricerca non sarebbe ripagato non essendoci successivamente un relativo mercato per potersi espandere e sfruttare fattori molto importanti come le economie di scala e di scopo.

Ci sono inoltre altri metodi che hanno riscontrato un basso livello di finanziamento: geometria della mano, vascolarizzazione, battito, scrittura e camminata. Le motivazioni per quanto successo, a parità di metodologia utilizzata per la creazione del database, possono essere diverse:

- Relativamente basso grado di sicurezza: può non essere considerato un metodo a causa di errori di prima e seconda specie moderati (considerazione ricavata in seguito ad elaborazioni svolte su determinati database sfruttati per ricavare il FRR e il FAR di ogni singola tecnologia

di riconoscimento biometrico). Questi livelli, che per alcune applicazioni possono essere eccessivamente alti (come, ad esempio, la cassetta di sicurezza in banca) portano al mancato utilizzo del metodo in questione, anche se tendenzialmente possiede un'elevata semplicità relativamente alla sua fruizione per riconoscere l'identità dell'individuo.

- Difficoltà nell'utilizzo: caso particolare di tecnologie che soffrono particolarmente in condizioni non ottimali di luce e che, conseguentemente, portano ad un mancato riconoscimento o errore nella sua sequenza.
  Oppure possono verificarsi anche dei casi concernenti il dispositivo di riconoscimento, dato che una difficoltà durante il suo impiego potrebbe comportare anche il mal posizionamento della caratteristica dell'individuo, causando dei problemi nella verificazione o identificazione dell'utente. Questo fattore crea dei disagi a valle della "filiera", cioè nei confronti dell'utilizzatore finale. Infatti, se questo non avrà una sensazione positiva o un'esperienza soddisfacente e semplice, allora si creerà un processo a catena che terminerà con il mancato utilizzo della tecnologia biometrica in questione.

- Online: specialmente negli ultimi anni, in seguito alla pandemia, si ha uno spostamento degli individui verso il mondo digitale. Questo fattore porta con sé anche la difficoltà di modificare i processi di riconoscimento, traslandoli verso altri dispositivi, come ad esempio il cellulare. Questo, unito eventualmente al basso grado di maturità della tecnologia, porta ad un irrisorio finanziamento da parte di soggetti terzi.

Le tecnologie che, al contrario, presentano alti investimenti e finanziamenti sono, in ordine: riconoscimento della fisionomia del volto, dell'impronta digitale, del comportamento sulle piattaforme digitali, della voce e dell'iride.

Per quanto riguarda i campi applicativi, invece, si hanno alcuni che sono particolarmente finanziati mentre altri meno. Ad esempio per l'avviamento dei motori si è davanti ad un'applicazione ancora molto giovane e di basso interesse dato che manca essenzialmente la tecnologia complementare nell'auto. Stesso discorso si può fare per l'ambito degli esami anche se, grazie allo spostamento verso il mondo online, si sta ampliando il campo.

Prendendo in esame i suddetti metodi di identificazione, ora si passa ad analizzare i verticali cioè i diversi campi applicativi. Si evince che le tecnologie dominanti non sussistono sulle stesse applicazioni. In particolare, gli incroci predominanti, in ordine decrescente, sono:

1. Volto – Verifica documenti;
2. Impronta Digitale– Accesso PC/Telefono;
3. Comportamentale Digitale– Identificazione online;
4. Voce – Assistenza alla clientela;
5. Volto – Controlli di sicurezza;
6. Impronta Digitale – Transazioni;

7. Volto – Controllo accessi;
8. Impronta Digitale – Controllo accessi.

Da queste combinazioni di tecnologia-applicazione si possono effettuare alcune considerazioni. Si nota, innanzitutto, che ci sono dei verticali che "vivono" grazie unicamente ad una particolare tecnologia come, ad esempio, l'assistenza alla clientela, che trova solamente applicazione con la biometria della voce, proprio a causa della sua intrinseca natura.
Un'altra osservazione mostra che, invece, il campo applicativo del controllo degli accessi verte su diverse tecnologie. Questo è un caso particolare, perché dipende principalmente dalle caratteristiche proprie di ogni biometria, essendo che per ambienti che richiedono un maggior grado di protezione è meglio usare la biometria dell'impronta digitale oppure in contesti di lavoro manuale è altamente sconsigliato usufruire di tale tecnologia, in quanto il riconoscimento ne risentirebbe per via di eventuali condizioni non ottimali del dito dell'individuo.

Se prendessimo solamente i due casi più cospicui di finanziamenti, cioè la biometria del volto e dell'impronta digitale, si nota ancora di più questa differenziazione relativa ai campi applicativi. Questa considerazione ripercorre quanto già citato nel primo capitolo in occasione dei limiti del modello di Abernathy e Utterback, cioè che per il dominant design non bisogna considerare solo la tecnologia che presenti un successo tecnico, ma anche un successo applicativo. In sostanza, bisogna non solo guardare i livelli orizzontali della matrice per scoprire quale sia l'architettura dominante, ma rivolgere la propria attenzione in special modo anche ai vari verticali, così da andare a considerare limitatamente i vari incroci.
Ciò mette in evidenza che, oltre ad essere il volto la tecnologia predominante, per via del maggior ammontare di finanziamenti ricevuti, trova anche successo all'interno delle applicazioni. In particolare, l'incrocio tra la biometria del volto e la verifica dei documenti è quello che ha ricevuto il maggior ammontare di denaro negli anni rispetto alle altre combinazioni.

Collegando anche i concetti ricavati prima con l'analisi dell'attività brevettuale, il dominio della fisionomia del volto come metodo di riconoscimento dell'identità dell'utente è anche confermato dall'andamento di ricerca.

Attenzione alla lettura della matrice perché potrebbe risultare che l'incrocio del riconoscimento facciale per i controlli di sicurezza non sia abbastanza importante. In realtà intervengono aziende importanti a livello globale come *SenseTime*, *Avigilon Corp* e *Veritone* che investono grossi capitali anche in questo campo applicativo in quanto intervengono fattori legati l'interesse collettivo. Però vista la natura multidisciplinare di queste, ed altre, aziende non sono state considerate nell'analisi in quanto non coerenti con la metodologia di analisi.

MATRICE INDICE DI GINI 1999-2020		APPLICAZIONI										
		Controllo accessi edifici	Identificazione criminali Controlli di sicurezza (es. aeroporto)	Avviamento veicoli/ macchine industriali	Accesso PC/ Telefono	Autenticazione remota su internet (es. Servizi bancari, account streaming)	Transazioni online/ bancomat	Firma digitale/ protezione e scambio sicuro di documenti	Verifica documenti	Esami	Controllo presenze	Assistenza clienti
TECNOLOGIE	Impronta digitale	0,738	0,587		0,926	0,852	0,681	0,810	0,639	1,000	0,287	
	Riconoscimento iride	0,628	0,722		0,982	1,000	0,584	1,000		1,000	0,503	
	Riconoscimento retina											
	Riconoscimento geometria mano	1,000		1,000		0,575	1,000					
	Riconoscimento vene mano (vascolarizzazione)	0,502	1,000	1,000	1,000	1,000	0,118					
	Riconoscimento battito	1,000			1,000	1,000		1,000				
	Riconoscimento volto	0,743	0,802		0,523	0,629	0,637	0,488	0,781	0,828	0,830	
	Riconoscimento voce	0,428	0,906	1,000	0,059	0,365	0,318	0,851	1,000			0,824
	Riconoscimento scrittura - firma				0,291	0,746		1,000				
	Riconoscimento camminata		1,000									
	Comportamentale digitale (es. movimento mouse, pressione dati su tastiera)				1,000	0,745						

Tabella 14: Matrice dell'indice di Gini per la matrice complessiva (1999-2020)

In questa matrice è stato analizzato l'indice di Gini per i vari incroci di tecnologia-applicazione. Innanzitutto, non verranno considerati i valori unitari del coefficiente in quanto manifesta unicamente il caso di singola azienda presente all'interno dell'intersezione in esame.

Valutando gli otto incroci sopra citati, i quali rappresentano quelli maggiormente finanziati, si nota che i valori del coefficiente assumono diverse connotazioni. Nella totalità si ha una tendenza ad avere un mercato prettamente concentrato, essendo elevati i vari indici. Si hanno poi delle situazioni, come l'impronta digitale per l'accesso al PC/Telefono, che trova quasi il caso di massima concentrazione dovuta all'importante presenza di una particolare azienda la quale, in occasione dell'inizio di interessamento da parte della collettività di avere una maggiore sicurezza, ha venduto le sue quote ad *Apple* che, grazie alla sua tecnologia, ha potuto implementare la biometria del dito negli IPhone di nuova generazione.

Studiando anche gli altri incroci, non vi è un particolare andamento dell'indice di Gini trovandosi davanti a valori sia tendenti alla massima concentrazione sia tendenti all'equi distribuzione del capitale investito.

i	Xi	fi	qi		
1	3,36	0,10	0,00	Gini	0,750
2	7,25	0,20	0,00		
3	9,86	0,30	0,01		
4	11,70	0,40	0,01		
5	18,15	0,50	0,01		
6	105,29	0,60	0,04		
7	445,17	0,70	0,16		
8	528,45	0,80	0,30		
9	1061,67	0,90	0,59		
10	1538,20	1,00	1,00		
	3729,096				

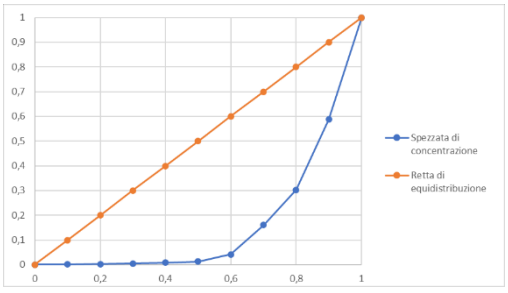


Figura 58: Analisi grafica della concentrazione dei finanziamenti complessivi delle tecnologie con la Curva di Lorenz (1999-2020)

Dalle suddette curve si nota che per le tecnologie (valori nella colonna Xi) si ha un cospicuo livello di concentrazione dei finanziamenti dovuta principalmente ai rinomati metodi di riconoscimento basati sull'impronta digitale e sulla fisionomia del volto.

i	Xi	fi	qi		
1	3,61	0,09	0,00	Gini	0,4896
2	10,81	0,18	0,00		
3	41,83	0,27	0,02		
4	79,31	0,36	0,04		
5	276,24	0,45	0,11		
6	382,11	0,55	0,21		
7	408,16	0,64	0,32		
8	456,54	0,73	0,44		
9	635,80	0,82	0,62		
10	651,45	0,91	0,79		
11	783,22	1,00	1,00		
	3729,096				

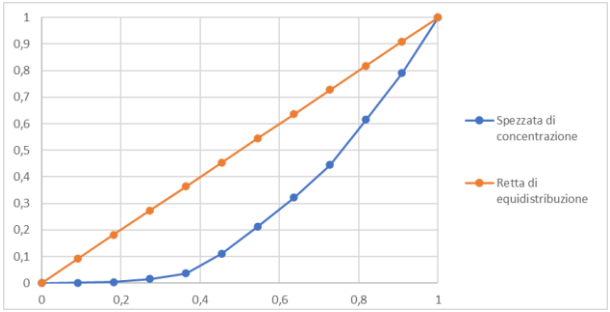


Figura 59: Analisi grafica della concentrazione dei finanziamenti complessivi delle applicazioni con la Curva di Lorenz (1999-2020)

Invece, per le applicazioni (valori nella colonna Xi), si ha un discreto livello di concentrazione in quanto non è presente in maniera così netta la predominanza di un manipolo ristretto di campi applicativi. Si ha quindi una minor area di concentrazione (cioè l'area presente tra la retta di equa distribuzione e la curva di Lorenz) rispetto al caso delle tecnologie.

3.3.2.2 I finanziamenti divisi in periodi

In questa parte dell'elaborato verrà analizzato l'andamento storico. In particolare, verranno studiate due matrici date dalla suddivisione in due periodi storici della tabella complessiva sopra esposta. I due archi temporali vanno dal 1999 al 2014 (compreso) e dal 2015 al 2020 (compreso).

3.3.2.2.1 I finanziamenti nel periodo 1999-2014

Iniziando con il primo intervallo si evidenziano i seguenti livelli di finanziamento:

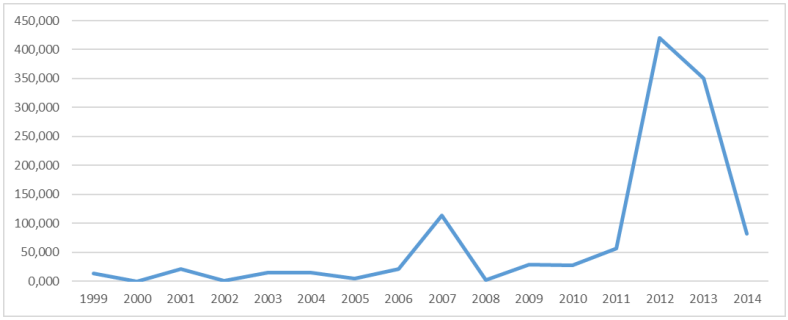


Figura 60: Livello di finanziamenti complessivi 1999-2014

MATRICE FINANZIAMENTI 1999-2014		APPLICAZIONI												
		Controllo accessi edifici	Identificazione criminali Controlli di sicurezza (es. aeroporto)	Avviamento veicoli/ macchine industriali	Accesso PC/ Telefono	Autenticazione remota su internet (es. Servizi bancari, account streaming)	Transazioni online/ bancomat	Firma digitale/ protezione e scambio sicuro di documenti	Verifica documenti	Esami	Controllo presenze	Assistenza clienti		
TECNOLOGIE	Impronta digitale	7,77	8,56	0,00	563,61	59,38	63,18	1,93	1,24	0,00	0,94	0,00	706,60	60,38%
	Riconoscimento iride	10,70	1,05	0,00	3,86	0,00	3,86	0,00	0,00	0,00	1,93	0,00	21,41	1,83%
	Riconoscimento retina	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00%
	Riconoscimento geometria mano	0,11	0,00	0,11	0,00	1,96	0,11	0,00	0,00	0,00	0,00	0,00	2,31	0,20%
	Riconoscimento vene mano (vascolarizzazione)	0,11	0,00	0,11	0,00	0,11	0,11	0,00	0,00	0,00	0,00	0,00	0,46	0,04%
	Riconoscimento battito	1,93	0,00	0,00	1,93	1,93	0,00	1,93	0,00	0,00	0,00	0,00	7,70	0,66%
	Riconoscimento volto	2,81	109,39	0,00	2,17	0,00	3,69	0,00	81,60	0,00	1,00	0,00	200,66	17,15%
	Riconoscimento voce	0,00	10,49	0,00	0,20	1,79	0,00	0,00	0,00	0,00	0,00	177,13	189,61	16,20%
	Riconoscimento scrittura - firma	0,00	0,00	0,00	0,32	0,32	0,00	0,00	0,00	0,00	0,00	0,00	0,65	0,06%
	Riconoscimento camminata	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00%
	Comportamentale digitale (es. movimento mouse, pressione dati su tastiera)	0,00	0,00	0,00	0,00	40,94	0,00	0,00	0,00	0,00	0,00	0,00	40,94	3,50%
		23,44 2,00%	129,47 11,06%	0,23 0,02%	572,09 48,88%	106,43 9,09%	70,97 6,06%	3,85 0,33%	82,84 7,08%	0,00 0,00%	3,87 0,33%	177,13 15,14%	1170,32	

Tabella 15: Matrice dei finanziamenti 1999-2014

Da questa tabella si evince subito che la tecnologia biometrica dell'impronta digitale presenta il più elevato ammontare di finanziamento, corrispondente a circa il 60% del livello complessivo del periodo storico, rendendo quindi questa caratteristica quella vincente per il mercato dell'identificazione per raggiungere livelli maggiori di sicurezza, e diventando di conseguenza il dominant design.

Prendendo quindi in esame questo metodo di riconoscimento, si va ad osservare la riga corrispondente per analizzare se ci sia una qualche particolare correlazione verso un campo

applicativo. Si nota che si ha un elevato ammontare di finanziamento per l'applicazione relativo l'accesso al PC/Telefono. Incrocio che rende la biometria considerata quella dominante sul mercato.

Questo fenomeno di preferenza dell'impronta da parte del target di riferimento va sicuramente di pari passo con il mercato, sebbene anche la tecnologia che si basa sulla fisionomia del volto ha riscosso altrettanto successo nel mondo della ricerca. Questo a manifestare, magari, anche gli anni di gloria dell'impronta digitale come prima tecnologia di successo oltre che come prima tecnologia ad essere sviluppata in ambito biometrico, come è stato citato nella storia.

Analizzando anche gli altri metodi si evidenzia che anche la fisionomia del volto e della voce hanno raggiunto dei buoni livelli nei rispettivi campi dei controlli di sicurezza e dell'assistenza alla clientela. Gli altri incroci invece non presentano ancora un sufficiente ammontare di finanziamento tale da essere considerato come consistente (> 100 milioni di dollari).

MATRICE INDICE DI GINI 1999-2014		APPLICAZIONI										
		Controllo accessi edifici	Identificazione criminali Controlli di sicurezza (es. aeroporto)	Avviamento veicoli/ macchine industriali	Accesso PC/ Telefono	Autenticazione remota su internet (es. Servizi bancari, account streaming)	Transazioni online/ bancomat	Firma digitale/ protezione e scambio sicuro di documenti	Verifica documenti	Esami	Controllo presenze	Assistenza clienti
TECNOLOGIE	Impronta digitale	0,38	0,32		0,93	0,86	0,84	1,00	0,63		1,00	
	Riconoscimento iride	0,43	0,47		1,00		1,00				1,00	
	Riconoscimento retina											
	Riconoscimento geometria mano	1,00		1,00		0,88	1,00					
	Riconoscimento vene mano (vascolarizzazione)	1,00		1,00		1,00	1,00					
	Riconoscimento battito	1,00			1,00	1,00		1,00				
	Riconoscimento volto	0,44	0,92		0,62		0,64		0,78		1,00	
	Riconoscimento voce				1,00	1,00						0,92
	Riconoscimento scrittura - firma				1,00	1,00						
	Riconoscimento camminata											
	Comportamentale digitale (es. movimento mouse, pressione dati su tastiera)					0,38						

Tabella 16: Matrice dell'indice di Gini per il periodo 1999-2014

Studiando, in prima battuta, il coefficiente per questo intervallo storico relativo ai tre incroci dominanti per livello dei finanziamenti si nota una elevata concentrazione quasi tendente all'unità. Anche per le altre combinazioni di tecnologia-applicazione si evidenzia un alto livello dell'indice. Questo, unitamente al basso numero di aziende operanti su questo particolare settore per la sicurezza biometrica e al basso ammontare di finanziamenti ricevuti, simboleggia un mercato ancora poco sviluppato e con una mancata equa distribuzione del denaro investito da terze parti.

i	Xi	fi	qi		
1	0,455	0,111	0,000	Gini	0,819
2	0,6475	0,222	0,001		
3	2,305	0,333	0,003		
4	7,7	0,444	0,009		
5	21,405	0,556	0,028		
6	40,935	0,667	0,063		
7	189,60833	0,778	0,225		
8	200,67195	0,889	0,396		
9	706,60033	1,000	1,000		
	1170,3281				

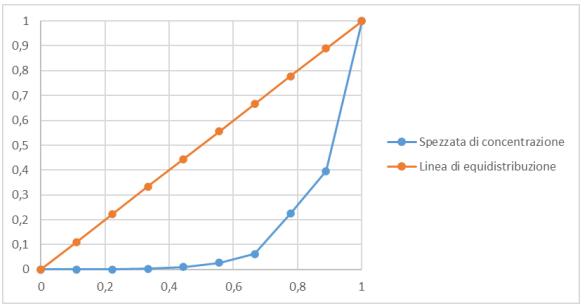


Figura 61: Analisi grafica della concentrazione dei finanziamenti del 1999-2014 delle tecnologie con la Curva di Lorenz

Il suddetto grafico va ad analizzare la concentrazione delle varie tecnologie (valori nella colonna Xi) nella loro totalità, quindi prendendo i dati relativi a tutte le applicazioni. Si nota che la spezzata, ossia la curva di Lorenz, tende ad avere un andamento ad L sottintendendo così un'ampia area di concentrazione racchiusa tra le due curve, cioè un elevato valore dell'indice di Gini.

i	Xi	fi	qi		
1	0,23	0,10	0,00	Gini	0,6881795
2	3,85	0,20	0,00		
3	3,87	0,30	0,01		
4	23,44	0,40	0,03		
5	70,97	0,50	0,09		
6	82,84	0,60	0,16		
7	106,43	0,70	0,25		
8	129,47	0,80	0,36		
9	177,13	0,90	0,51		
10	572,09	1,00	1,00		
	1170,33				

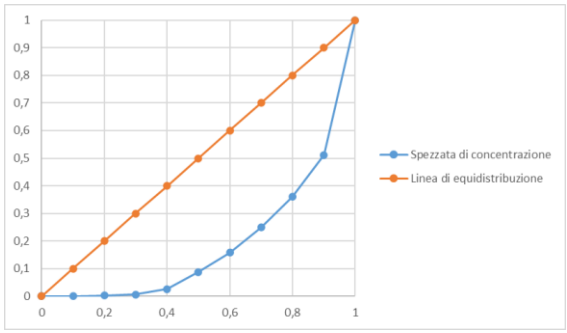


Figura 62: Analisi grafica della concentrazione delle applicazioni del 1999-2014 delle tecnologie con la Curva di Lorenz

Invece, per le applicazioni (valori nella colonna Xi), si ha una spezzata meno tendente alla forma a L, come sopra. Infatti, si ha un coefficiente di Gini alto, ma non come per le tecnologie. Questo dipende dal fatto che c'è un'applicazione, quella dell'accesso al PC/Telefono, che ha ricevuto un ampio finanziamento, ma ci sono comunque altri campi applicativi che hanno riscosso abbastanza fiducia negli investitori.

3.3.2.2.1 I finanziamenti nel periodo 2015-2020

Per quanto riguarda il secondo intervallo di tempo, cioè 2015-2020, si ha:

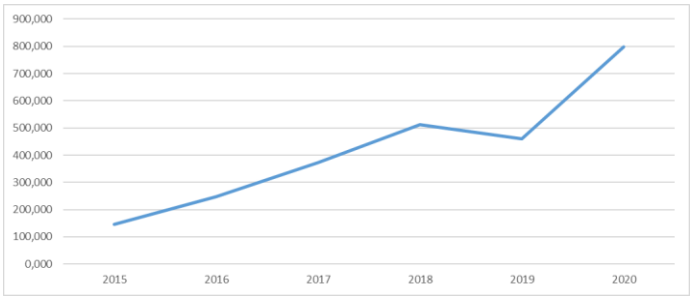


Figura 63: Livello di finanziamenti complessivi 2015-2020

MATRICE FINANZIAMENTI 2015-2020		APPLICAZIONI												
		Controllo accessi edifici	Identificazione criminali Controlli di sicurezza (es. aeroporto)	Avviamento veicoli/ macchine industriali	Accesso PC/ Telefono	Autenticazione remota su internet (es. Servizi bancari, account streaming)	Transazioni online/ bancomat	Firma digitale/ protezione e scambio sicuro di documenti	Verifica documenti	Esami	Controllo presenze	Assistenza clienti		
TECNOLOGIE	Impronta digitale	93,22	23,35	0,00	51,61	10,52	151,65	3,46	7,58	2,51	11,18	0,00	355,07	14,02%
	Riconoscimento iride	42,53	20,35	0,00	2,63	1,26	9,60	0,67	0,00	1,26	5,59	0,00	83,89	3,31%
	Riconoscimento retina	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00%
	Riconoscimento geometria mano	0,60	0,00	0,60	0,00	5,75	0,60	0,00	0,00	0,00	0,00	0,00	7,55	0,30%
	Riconoscimento vene mano (vascolarizzazione)	4,57	3,07	0,60	0,91	0,60	1,51	0,00	0,00	0,00	0,00	0,00	11,25	0,44%
	Riconoscimento battito	2,61	0,00	0,00	2,61	2,61	0,00	2,61	0,00	0,00	0,00	0,00	10,45	0,41%
	Riconoscimento volto	211,41	272,53	0,00	3,81	32,36	35,92	24,70	691,08	7,05	58,67	0,00	1337,53	52,81%
	Riconoscimento voce	3,73	0,52	2,19	0,18	3,84	5,99	6,37	1,73	0,00	0,00	231,03	255,56	10,09%
	Riconoscimento scrittura - firma	0,00	0,00	0,00	0,18	2,35	0,00	0,18	0,00	0,00	0,00	0,00	2,71	0,11%
	Riconoscimento camminata	0,00	7,25	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	7,25	0,29%
	Comportamentale digitale (es. movimento mouse, pressione dati su tastiera)	0,00	0,00	0,00	1,80	459,71	0,00	0,00	0,00	0,00	0,00	0,00	461,51	18,22%
		358,67	327,07	3,39	63,72	519,01	205,27	37,98	700,38	10,81	75,43	231,03	2532,77	
		14,16%	12,91%	0,13%	2,52%	20,49%	8,10%	1,50%	27,65%	0,43%	2,98%	9,12%		

Tabella 17: Matrice dei finanziamenti 2015-2020

Andando ora ad analizzare l'altro periodo storico, quello che si avvicina di più a noi oggi, si nota subito che la tecnologia che ha raccolto la maggior quantità di finanziamenti da parte di attori esterni è quella concernente il metodo basato sulla fisionomia del volto. Rendendo quindi tale tecnologia l'architettura dominante.
Studiando, poi, più dettagliatamente i vari campi applicativi, si va ad evidenziare che il riconoscimento sussiste principalmente per le applicazioni maggiormente importanti per l'arco temporale considerato: controllo accessi, controlli di sicurezza e verifica dei documenti. In special modo, l'ultimo tra questi, raccoglie un maggior bacino di denaro ricevuto dagli investitori.

Ci sono poi altri incroci importanti, come la tecnologia del comportamento digitale per l'autenticazione online, quella della voce per l'assistenza alla clientela, … Queste combinazioni fanno risaltare limitatamente l'architettura specifica, anche se non dominanti rispetto allo studio della fisionomia del volto per la verifica dei documenti.

MATRICE INDICE DI GINI 2015-2020		APPLICAZIONI										
		Controllo accessi edifici	Identificazione criminali Controlli di sicurezza (es. aeroporto)	Avviamento veicoli/ macchine industriali	Accesso PC/ Telefono	Autenticazione remota su internet (es. Servizi bancari, account streaming)	Transazioni online/ bancomat	Firma digitale/ protezione e scambio sicuro di documenti	Verifica documenti	Esami	Controllo presenze	Assistenza clienti
TECNOLOGIE	Impronta digitale	0,73	0,56		0,85	0,67	0,68	0,70	0,78	1,00	0,23	
	Riconoscimento iride	0,71	0,60		0,95	1,00	0,63	1,00		1,00	0,56	
	Riconoscimento retina											
	Riconoscimento geometria mano	1,00		1,00		0,79	1,00					
	Riconoscimento vene mano (vascolarizzazione)	0,54	1,00	1,00	1,00	1,00	0,20					
	Riconoscimento battito	1,00			1,00	1,00		1,00				
	Riconoscimento volto	0,74	0,77		0,46	0,63	0,64	0,49	0,78	0,83	0,83	
	Riconoscimento voce	0,43	1,00	1,00	1,00	0,28	0,32	0,85	1,00			0,93
	Riconoscimento scrittura - firma				1,00	0,85		1,00				
	Riconoscimento camminata		1,00									
	Comportamentale digitale (es. movimento mouse, pressione dati su tastiera)				1,00	0,78						

Tabella 18: Matrice dell'indice di Gini per il periodo 2015-2020

Analizzando inizialmente l'indice di Gini per gli incroci con una considerevole quantità di denaro ricevuto, si evince che è presente un livello medio alto di concentrazione. Caratteristica che viene ripresa anche per le altre combinazioni di tecnologia-applicazione.

Il maggiore ammontare di denaro presente nel mercato della sicurezza biometrica, e relativa concentrazione, porta con sé il fatto di avere un settore via via più sviluppato, con l'aumento del numero delle aziende operanti nel settore e una tendenza ad evidenziare un'architettura.

i	Xi	fi	qi		
1	2,708333333	0,100	0,001	Gini	0,778
2	7,25	0,200	0,004		
3	7,55	0,300	0,007		
4	10,45	0,400	0,011		
5	11,246	0,500	0,015		
6	83,88558333	0,600	0,049		
7	255,56425	0,700	0,150		
8	355,0696833	0,800	0,290		
9	461,51378	0,900	0,472		
10	1337,53025	1,000	1,000		
	2532,76788				

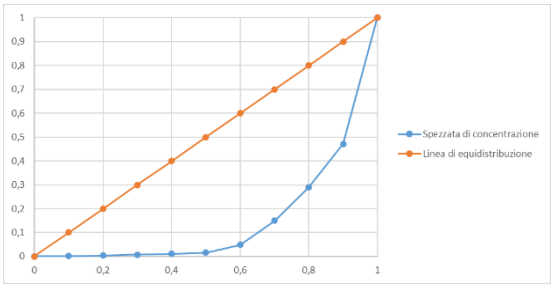


Figura 64: Analisi grafica della concentrazione dei finanziamenti del 2015-2020 delle tecnologie con la Curva di Lorenz

Questo grafico ha l'intenzione di sottolineare il livello di concentrazione presente per ogni singola tecnologia (valori nella colonna Xi), considerando i dati per tutte le applicazioni. In particolare, vi è la presenza di una curva spezzata, tendente la forma ad L che sottintende un alto valore del coefficiente di Gini. Tale è spiegato principalmente dall'intervento della tecnologia della fisionomia del volto che, su un totale di quasi due miliardi e mezzo di dollari, partecipa per circa metà del finanziamento.

i	Xi	fi	qi		
1	3,386666667	0,091	0,001	Gini	0,566
2	10,81402778	0,182	0,006		
3	37,983	0,273	0,021		
4	63,71766667	0,364	0,046		
5	75,43275	0,455	0,076		
6	205,2709944	0,545	0,157		
7	231,0259583	0,636	0,248		
8	327,0684444	0,727	0,377		
9	358,6717861	0,818	0,519		
10	519,0119328	0,909	0,723		
11	700,3846528	1,000	1,000		
	2532,76788				

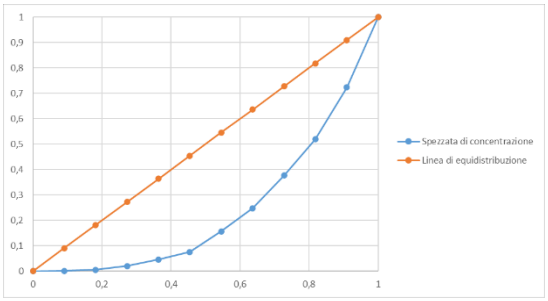


Figura 65: Analisi grafica della concentrazione delle applicazioni del 2015-2020 delle tecnologie con la Curva di Lorenz

Invece, per le applicazioni (valori nella colonna Xi), si ha una concentrazione media del mercato biometrico in quanto ci sono diverse applicazioni che partecipano molto attivamente alla totalità del finanziamento.

3.3.3 Le considerazioni complessive

Analizzando l'andamento storico dei finanziamenti e dell'indice di Gini correlato, si possono ricavare delle considerazioni.
In particolare, viene evidenziato come molte tecnologie e molte applicazioni non fossero ancora esistenti all'inizio del periodo di espansione dei metodi di riconoscimento biometrici.
Con l'avanzamento della ricerca, e con il bisogno sempre più impellente di aumentare i livelli di sicurezza collettivi, si cominciò ad introdurre le varie biometrie, con lo scopo principale di verificare e/o identificare l'individuo con un livello di accertamento ben superiore a quanto si era abituati all'epoca. In questo modo, la matrice negli anni iniziò a complicarsi sempre più, andando ad aggiungere righe e colonne. Si passa così da periodi di alta divergenza a periodi di alta convergenza quindi dal lavorare su una o poche tecnologie-applicazioni ad elaborare versioni di quasi tutti gli incroci possibili nel mercato.

Parallelamente a ciò ci sono stati dei diversi fenomeni di concentrazione negli anni, passando, ad esempio, da valori quasi unitari dell'indice di Gini a valori minori. Questa costante modifica del coefficiente, unitamente ai vari movimenti del mercato, in cui prima vi è la preferenza verso un determinato incrocio e successivamente verso un altro, porta alla continua modifica dell'ammontare di aziende facendo conseguentemente variare i livelli di finanziamenti presenti nel mercato.
Si andò via via ad aumentare l'intensità dei capitali degli investitori verso tecnologie ben precise, orientate verso applicazioni altrettanto puntuali, facendo risaltare diversi incroci nel tempo. Tale andamento ha la caratteristica di far emergere l'architettura dominante verso specifici incroci in base alle necessità.
Anche lo stesso dominant design è mutato negli anni passando dallo studio dell'impronta digitale per l'accesso al PC/Telefono allo studio della fisionomia del volto per la verifica dei documenti.

Negli anni le condizioni al contorno cambiano e, con essi, anche gli equilibri. Pertanto non è soltanto più una storia di aumento considerevole dell'ammontare di denaro immesso nel mercato della sicurezza biometrica, ma si tratta proprio di un altro tipo di evoluzione.

3.3.4 L'analisi parziale del 2021

In seguito al lavoro appena mostrato, è stata fatta una elaborazione risalente all'anno in corso. Sia per tenere una sorta di parallelismo con i brevetti, sia per via di un mercato in continua evoluzione, non è stato considerata l'annualità 2021 nello studio delle matrici dei finanziamenti. È però interessante analizzarlo, con lo scopo di cercare di capire se il trend annuale è in linea con quanto appena esposto.

Essendo un continuo divenire, vengono considerati i dati aggiornati al 01/10/2021.

MATRICE FINANZIAMENTI 2021		APPLICAZIONI												
		Controllo accessi edifici	Identificazione criminali Controlli di sicurezza (es. aeroporto)	Avviamento veicoli/ macchine industriali	Accesso PC/ Telefono	Autenticazione remota su internet (es. Servizi bancari, account streaming)	Transazioni online/ bancomat	Firma digitale/ protezione e scambio sicuro di documenti	Verifica documenti	Esami	Controllo presenze	Assistenza clienti		
TECNOLOGIE	Impronta digitale	4,02	8,21	0,00	6,37	1,67	7,71	0,00	12,50	0,00	2,35	0,00	42,83	2,45%
	Riconoscimento iride	254,60	3,50	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	258,10	14,78%
	Riconoscimento retina	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00%
	Riconoscimento geometria mano	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00%
	Riconoscimento vene mano (vascolarizzazione)	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00%
	Riconoscimento battito	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00%
	Riconoscimento volto	415,89	165,57	0,00	1,80	18,63	14,58	1,94	758,00	0,61	0,00	0,00	1377,03	78,85%
	Riconoscimento voce	9,83	0,00	0,00	1,67	14,53	4,70	0,00	0,00	0,00	0,00	21,42	52,15	2,99%
	Riconoscimento scrittura - firma	0,00	0,00	0,00	0,00	0,00	0,00	0,30	0,00	0,00	0,00	0,00	0,30	0,02%
	Riconoscimento camminata	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00%
	Comportamentale digitale (es. movimento mouse, pressione dati su tastiera)	0,00	0,00	0,00	1,50	14,46	0,00	0,00	0,00	0,00	0,00	0,00	15,96	0,91%
		684,34 39,19%	177,28 10,15%	0,00 0,00%	11,34 0,65%	49,30 2,82%	26,99 1,55%	2,25 0,13%	770,50 44,12%	0,61 0,03%	2,35 0,13%	21,42 1,23%	1746,37	

Tabella 19: Matrice dei finanziamenti 2021

I finanziamenti ricevuti nel periodo dell'anno considerato sono pari a quanto è risultato nell'arco temporale che spazia dall'anno 1999 fino al 2014. Questo sicuramente porta ad affermare con certezza che si sta procedendo verso un continuo apporto di capitale, utilizzato per necessità di ricerca, dato che la volontà del mercato sta andando in questa direzione. Sicuramente la pandemia ha dato un impulso senza precedenti a questo settore, ma certamente grazie allo sviluppo dei sistemi informativi si possono raggiungere livelli ben superiori di sicurezza.

In linea con il periodo 2015-2020, la biometria del volto è nettamente dominante rispetto alle altre tecnologie. Specialmente con l'applicazione della verifica dei documenti trova più seguito. Esattamente l'incrocio già presente nell'altro arco temporale, convalidando l'andamento.

Particolarità aggiuntiva è il palesarsi, in maniera molto consistente, della tecnologia dell'iride specialmente riguardante il campo del controllo degli accessi. Biometria che garantisce livelli elevati di sicurezza, confermati anche dai bassi livelli di errori da parte dei test eseguiti sui database di ricerca, e un'alta semplicità di utilizzo. Va quindi ad unire la sicurezza dell'impronta digitale e la naturalità del riconoscimento facciale.

MATRICE INDICE DI GINI 2021		APPLICAZIONI										
		Controllo accessi edifici	Identificazione criminali Controlli di sicurezza (es. aeroporto)	Avviamento veicoli/ macchine industriali	Accesso PC/ Telefono	Autenticazione remota su internet (es. Servizi bancari, account streaming)	Transazioni online/ bancomat	Firma digitale/ protezione e scambio sicuro di documenti	Verifica documenti	Esami	Controllo presenze	Assistenza clienti
TECNOLOGIE	Impronta digitale	0,17	0,15		0,48	1,00	0,22		1,00		1,00	
	Riconoscimento iride	1,00	1,00									
	Riconoscimento retina											
	Riconoscimento geometria mano											
	Riconoscimento vene mano (vascolarizzazione)											
	Riconoscimento battito											
	Riconoscimento volto	0,89	0,86		0,39	0,52	0,13	0,66	0,79	0,15		
	Riconoscimento voce	0,66			1,00	0,45	1,00					0,37
	Riconoscimento scrittura - firma							1,00				
	Riconoscimento camminata											
	Comportamentale digitale (es. movimento mouse, pressione dati su tastiera)				1,00	0,54						

Tabella 20: Matrice dell'indice di Gini per il 2021

Analizzando l'indice di Gini, si notano coefficienti molto bassi, quasi tendenti verso la equa distribuzione del finanziamento. Al contrario, proprio in occasione dei tre incroci predominanti della tecnologia della fisionomia del volto, si osserva una concentrazione elevata. Questo a manifestazione del fatto che si sta convergendo verso un manipolo sempre più ristretto di aziende operanti in un determinato campo.
Valori che sono in linea con il periodo 2015-2020.

L'incrocio corrispondente al riconoscimento dell'iride per il controllo degli accessi ha la particolarità di trovare il lavoro di un'unica impresa, *Clear*, concentratasi su questo e che ha avuto uno sbocco sostanziale per evitare gli assembramenti di persone negli aeroporti (correlato alla tecnologia "touch-free" per non causare il contagio dal tocco del dispositivo).

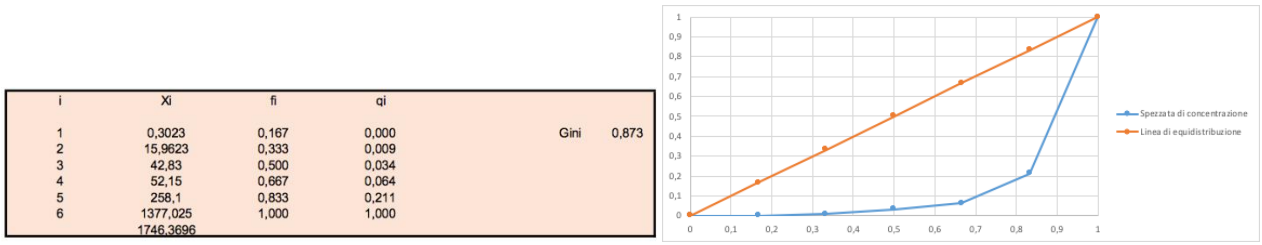


Figura 66: Analisi grafica della concentrazione dei finanziamenti del 2021 delle tecnologie con la Curva di Lorenz

Analizzando il complessivo di tecnologie (valori nella colonna Xi), si nota l'evidente forma ad L della spezzata, sottintendendo un valore elevato del coefficiente di concentrazione. Questo comportamento è dovuto in maniera preminente all'ingente ammontare della tecnologia di riconoscimento facciale.

i	Xi	fi	qi		
1	0,61	0,100	0,000	Gini	0,808
2	2,245633333	0,200	0,002		
3	2,35375	0,300	0,003		
4	11,34083333	0,400	0,009		
5	21,41666667	0,500	0,022		
6	26,99083333	0,600	0,037		
7	49,29563333	0,700	0,065		
8	177,2758333	0,800	0,167		
9	684,33875	0,900	0,559		
10	770,5016667	1,000	1,000		
	1746,3696				

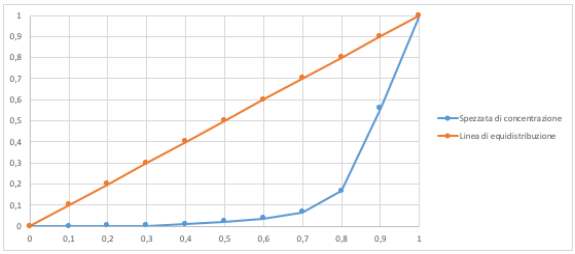


Figura 67: Analisi grafica della concentrazione delle applicazioni del 2021 delle tecnologie con la Curva di Lorenz

Stesso andamento si evidenzia studiando le applicazioni (valori nella colonna Xi), soprattutto per i finanziamenti ricevuti per la verifica dei documenti e per il controllo degli accessi.

Rapportando queste analisi dell'indice di Gini con quelle svolte per il periodo 2015-2020, è possibile notare un aumento consistente della concentrazione, soprattutto per quanto riguarda i campi applicativi.

4. BIBLIOGRAFIA

G. Moore (1991) "*Crossing the chasm*"

E. Rogers (1962) "*Diffusion of innovations*"

W. Abernathy, J.M. Utterback (1975) *"A Dynamic Model of Process and Product Innovation"*

W. Abernathy, J.M. Utterback (1978) *"Patterns of Industrial Innovation"*

W. Abernathy (1978) *"The Productivity Dilemma: roadblock to innovation in automobile industry"*

P. Anderson, **M. Tushman** (1990) *"Technological Discontinuities and Dominant Designs:* A Cycl*ical Model of Technological Change"*

J. Utterback (1996) *"Mastering the Dynamics of Innovation"*

J. Utterback, F. Suarez (1993) *"Patterns of Industrial Evolution,* Dominant Designs, *and Firms' Survival*", Sloan School of Management, 1993

J. Funk (2003) *"Standards, dominant designs and preferential acq*uisition of *complementary assets through slight information advantages"*

F. Suarez (2003) *"Battles for technological dominance: an integrative framework"*

P. Cebon, O. Hauptman (2008) "*Product modularity and the product lifecycle: New dynamics in the interactions of product and process technologies"*

L. Bigelow, N. Argyres (2007) "*Competitive positioning, dominant design and vertical integration over the industry lifecycle"*

P. Cebon, O. Hauptman (2002) "*Industries in the making: Product modularity, technological innovation and the product lifecycle"*

D. O'Leary (2008) "*Gartner's hype cycle and information system research issues"*

M. Cantamessa, F. Montagna (2016) "*Management of Innovation and Product Development*"

5. SITOGRAFIA

https://www.sciencedirect.com/

https://www.researchgate.net/

https://www.mdpi.com/

https://www.gartner.com/

https://www.treccani.it/

https://link.springer.com/

https://www.mdpi.com/

https://www.cambridge.org/core/

https://www.cgdev.org/

https://www.biometricupdate.com/

https://www.intechopen.com/

http://archive.ceciis.foi.hr/app/index.php/ceciis/archive

https://www.semanticscholar.org/

https://www.hitachi.com/

https://www.nojitter.com/

https://www.xyzmo.com/

http://www.aispeech.com/

https://ieeexplore.ieee.org/Xplore/home.jsp

https://www.raconteur.net/

https://medcraveonline.com/

https://itif.org/

https://www.m2sys.com/blog/

https://platform.keesingtechnologies.com/

https://resources.infosecinstitute.com/

https://www.bayometric.com/

https://www.privacyend.com/

https://www.mofiria.com/en/

https://home.keyo.co/

https://scialert.net/

http://way2benefits.com/

https://techxplore.com/

https://recfaces.com/

https://www.hindawi.com/

https://www.ijstr.org/

https://www.crunchbase.com/

https://dealroom.co/

https://www.statista.com/

https://iquii.com/

https://www.marketsandmarkets.com/

https://www.cybersecurity360.it/

http://mondodigitale.aicanet.net/

http://archivio-mondodigitale.aicanet.net/

https://heimdalsecurity.com/blog/

https://www.paymentsjournal.com/

https://www.biometricsinstitute.org/

https://www.safetysecuritymagazine.com/

https://www.intechopen.com/

https://www.dw.com/

https://www.1kosmos.com/

http://www.3dface.com.cn/

http://www.3divi.com/

https://www.a3bc.org/

https://www.advance.ai/

http://www.agnitio-corp.com/

https://aimbrain.com/

http://www.alcatraz.ai/

https://www.anyvision.co/

https://appmobi.com/

https://www.ariadnext.com/

http://www.au10tix.com/

http://authentec.com/

http://authenteq.com/

https://www.authid.ai/

http://www.ayonix.com/

http://www.behaviosec.com/

https://www.berbix.com/

http://bi2technologies.com/

http://www.biocatch.com/

https://www.bioconnect.com/

https://www.biodit.com/

http://bio-key.com/

https://biosig-id.com/

http://www.biometrica.com/

http://www.biometricvox.com/

http://www.biosec.com.cn/

https://www.biositesystems.com/

https://biowatchid.com/

https://www.blinkidentity.com/

https://blinking.id/

http://www.briefcam.com/

http://www.callsign.com/

https://www.cardlab.com/

http://www.choosecase.com/

http://www.chipsailing.com/

http://www.clearme.com/

https://clearview.ai/

https://clockster.com/

http://www.cmi-tech.com/

https://corsight.ai/

http://www.crayonic.com/

http://cursorinsight.com/

http://customerclever.co.uk/

http://cyberextruder.com/

https://www.cybertonica.com/

http://deepsense.cn/

http://deltaid.com/

http://dessmann.com.sg/

http://diamondfortress.com/

http://fingerprints.digital/

http://www.digitalsignalcorp.com/

https://easyclocking.com/

http://www.econnectglobal.com/

http://www.discoverelement.com/

https://www.eyecool.cn/

http://eyelock.com/

http://hebsckj.com/

http://facefirst.com/

https://faceki.com/

https://facenote.me/

http://www.faceos.com/

http://www.facephi.com/

https://fog.faceter.cam/

https://www.facewatch.co.uk/

https://www.featurespace.com/

http://www.fingercrystal.com/

http://www.fingpay.co.in/

https://fortress-identity.com/

http://www.fourthline.com/

http://www.gtriip.com/

http://www.fzhjkj.com/

http://www.hongshi-tech.com/

http://www.hjzn.com.cn/

http://icarvision.com/

http://idchecker.com/

https://www.idrnd.ai/

https://www.id.me/

https://www.idenfy.com/

http://www.idintl.com/

https://www.idexbiometrics.com/

http://idmission.com/

http://www.ievoreader.com/

http://www.incode.com/

http://integratedbiometrics.com/

http://www.intellif.com/

http://intelli-vision.com/

http://www.intensityanalytics.com/

https://www.invixium.com/

http://www.iridiantech.com/

http://www.irisking.com/

http://www.iristar.com.cn/

http://www.isorg.fr/

http://www.jtwoc.com/

http://www.jumio.com/

https://www.kairos.com/

https://www.keylemon.com/

https://keyless.io/

https://www.getmati.com/

https://www.miteksystems.com/

http://www.moredian.com/index.html

https://www.myvoice.ai/

http://www.net1.com/

http://www.nethone.com/

http://www.normee.co.jp/index.html

http://ntechlab.com/

http://nymi.com/

http://ocrlabs.com/

https://www.oloid.ai/

https://omilia.com/

https://ondato.com/

http://onevisage.com/

http://www.onfido.com/

https://paravision.ai/

https://passbase.com/

https://www.getpassid.com/

http://payface.co/

http://www.payrollhero.com/

https://withpersona.com/

http://pindrop.com/

http://www.plurilock.com/

https://polygon.pt/

https://www.popid.com/

https://www.post-quantum.com/

http://precisebiometrics.com/

http://preventor.com/

http://princetonidentity.com/

https://q5id.com/

http://qigurl.com/

https://www.quardlock.com/

https://www.rapidid.com/

https://www.revelock.com/

http://www.saffe.co/

http://www.securedtouch.com/

http://securlinx.com/

https://www.sensity.ai/

http://www.sensory.com/

https://sentryhealth.life/

https://www.signzy.com/

http://www.smarteyetechnology.com/

http://www.smileidentity.com/

https://spitch.ai/

https://www.stonelock.com/

https://sumsub.com/

https://swip.one/en/

http://www.tascent.com/

https://www.tech5.ai/

http://www.thirdfort.com/

https://www.threatmark.com/

https://www.touchbiometrix.com/

https://www.travizory.com/

https://www.trueface.ai/

https://www.truora.com/

https://www.truststamp.ai/

https://www.twosense.ai/

https://www.typingdna.com/

https://unify.id/

https://unike.tech/

https://www.v2verify.com/

http://www.validityinc.com/

https://www.validsoft.com/

https://veri5digital.com/

https://www.veridiumid.com/

https://veriff.com/

http://www.verifyoo.com/

http://www.visionlabs.ai/

https://voatz.com/

http://www.voiceaitech.com/

http://www.voicevault.com/

https://www.vouched.id/

http://www.warwickwarp.co.uk/

http://www.watrix.ai/

http://www.wedonetech.com/

https://www.vicmob.com/

https://www.yoti.com/

https://www.youverify.co/

https://zighra.com/

https://zwipe.com/