Dipartimento di Scienze

Scuola Dottorale EDEMOM

European **D**octorate in **E**lectronic Materials, **O**ptoelectronics and **M**icrosystems

XXVII Ciclo dottorale

Tecniche Hylemetriche per l'autenticazione:

Metodologie biometriche applicate ad oggetti inanimati

Ing. Giuseppe MAKARY

Tutor

Prof. Giuseppe Schirripa Spagnolo

Coordinatore

Prof. Giuseppe Schirripa Spagnolo

13 Aprile 2015

Ringraziamenti

Un sentito ringraziamento al Professor Schirripa per avermi “accompagnato” in questo lungo percorso di ricerca, per avermi sostenuto e dato fiducia dai tempi della tesi di Laurea sino ad oggi, permettendomi di poter fare interessanti esperienze professionali e pratiche. Un ringraziamento perché grazie alla sua disponibilità oggi faccio ciò che per anni ho sognato; un grazie infine per essersi dimostrato un professionista e un vero docente come pochi, sostenendomi anche quando io stesso pensavo di non farcela.

Ringrazio, inoltre, immensamente la mia famiglia per non avermi mai fatto mancare il proprio sostegno morale, per avermi dato l’incoraggiamento e la forza d’animo necessaria a concludere questo lavoro, che si è dimostrato più tortuoso del previsto.

Ringrazio la mia ragazza per avermi sostenuto, supportato e sopportato in questi anni di fatica e privazioni.

Infine un grazie agli amici, che vicini e lontani, ognuno a modo suo è stato presente in quest’esperienza di vita.

1 Abstract

Negli ultimi anni si è assistito alla crescita costante dell'esigenza, da parte delle autorità così come dei singoli individui, di incrementare la sicurezza contro le frodi; in particolare per quanto riguarda quella legata all'autenticità e alla provenienza garantita degli oggetti.

I sistemi di sicurezza tradizionali sono realizzati, quasi esclusivamente, con delle tecnologie che con il tempo possono diventare semplici ed economiche, ciò grazie agli sviluppi tecnologici dei mercati; pertanto quello che ora potrebbe essere considerato come antieconomico e complesso può divenire con il tempo oggetto d'interesse per eventuali frodi; inoltre un bene durevole, col trascorrere del tempo, potrebbe acquistare un valore tale per cui l'utilizzo di tecnologie di duplicazione, inizialmente costose, diventano economicamente convenienti.

Affinché una tecnologia possa essere considerata utile all'anti-contraffazione deve avere anche una durata paragonabile a quella del bene da proteggere; questa condizione, per le tecnologie attualmente in uso, non sempre è rispettata.

L'elevata concorrenza effettuata, specialmente dai paesi emergenti, sfrutta gli investimenti e l'inventiva delle aziende leader per sottrarre loro quote di mercato con prodotti palesemente contraffatti o realizzati in modo molto simile al brand che intendono "attaccare". Sul mercato si rilevano quotidianamente situazioni di contraffazione e di mercato parallelo; il brand subisce gravi danni di immagine, mentre i mercati paralleli danneggiano mercati consolidati a maggiore marginalità, oltre a creare conflittualità con la rete vendita ufficiale. Non tutti i fenomeni di contraffazione puntano allo stesso scopo. Talvolta il prodotto è contraffatto in modo palese e veicolato attraverso canali di vendita chiaramente non ufficiali, una situazione che paradossalmente crea un effetto positivo; diffonde il brand (e il desiderio di possederlo) attraverso una clientela che non potrebbe accederne e consapevole di possedere un falso (ciò al di là della legislazione). Talvolta il brand viene invece contraffatto in modo molto accurato e veicolato attraverso canali plausibili, in questo caso si creano contemporaneamente due danni: l'utente crede di acquistare un prodotto originale a un prezzo vantaggioso e il brand perde una vendita. L'unico modo per contrastare questi fenomeni è consentire l'identificazione certa del prodotto e la sua tracciabilità durante tutti i passaggi della catena di distribuzione.

Le industrie del fashion si propongono sul mercato come aziende consolidate, fortemente strutturate e organizzate, capaci di gestire logiche di filiera produttiva e di mercato a livello internazionale. Un mercato globale caratterizzato da una forte delocalizzazione della produzione e dalla decentralizzazione delle attività, nell'ottica della crescita di competitività, ha tuttavia comportato numerose problematiche, causate soprattutto dall'impossibilità, per l'azienda, di monitorare con certezza attività, risorse, prodotti. Le criticità sono trasversali a tutti gli stadi della filiera, e sono in gran parte riconducibili a un problema fondamentale: l'impossibilità di accertare l'identità univoca del singolo prodotto. Oggigiorno, vista la delocalizzazione della produzione, è oneroso assegnare un nome o un numero di serie univoco e non "clonabile" al singolo prodotto. L'assenza del riconoscimento "unico" non consente una tracciabilità del prodotto lungo tutta la filiera, nonostante le numerosissime tecnologie presenti sul mercato.

La quasi totalità dei metodi utilizzati per l'anticontraffazione, si basano su caratteristiche aggiunte all'oggetto. La filosofia finora adottata, prevede di inserire dei "marchi/caratteristiche" utilizzando tecniche complesse e costose. In questo modo, si rende economicamente sconveniente duplicarle. La semplice commercializzazione di oggetti senza il corretto marchio/caratteristica consente l'individuazione della frode. L'inserimento di marchi e caratteristiche "complessi" ed economicamente onerosi, fa sì che tali sistemi possano essere utilizzati solo su oggetti di valore economico "considerevole". Inoltre, con il progredire della tecnologia, la clonazione delle caratteristiche aggiunte diventa sempre più semplice e compatibile economicamente.

Oggetto del lavoro presentato in questa tesi è stato quello di cercare di contrastare la clonazione di un oggetto mediante la ricerca di caratteristiche "instinseche", alla stregua della biometria, che consentissero di identificare univocamente l'oggetto stesso. La teoria che permette un'identificazione di un oggetto in maniera univoca va con il nome di Hylemetria; questa richiede che la caratteristica utilizzata per l'identificazione debba avere le seguenti proprietà: essere unica, numerabile, non-invasiva, coerente, concisa, robusta, resistente alla contraffazione. Qualunque caratteristica che sia randomica e difficile/impossibile da riprodurre può potenzialmente essere una caratteristica Hylemetrica.

Nel settore della moda, gli attuali sistemi sono basati quasi esclusivamente sul riconoscimento visivo di dettagli.

Scopo quindi della tesi è stata quella di cercare e proporre un sistema che consentisse al singolo capo di moda di essere identificato come unico ed essere totalmente verificabile come tale.

Lo studio inizia con l'analisi di tutte le tecnologie anticontraffazione oggi presenti sul mercato, sia per mercati globali che di nicchia, ciò al fine di avere un quadro completo di tutte le soluzioni esistenti, con la definizione dei vantaggi e svantaggi nell'applicazione delle stesse agli oggetti e le relative tutele in termini di sicurezza. Le tecnologie anti-contraffazione possono quindi essere divise in quattro categorie analizzate approfonditamente: visibili (overt), progettate in modo da permettere all'utente finale di verificare l'autenticità di un oggetto su cui è posto (es. ODV, ologrammi, inchiostri a colorazione variabile), invisibili (covert), anche se sono invisibili ad occhio nudo (stampa invisibile, filigrane), permettono al proprietario del marchio di fabbrica di identificare i prodotti contraffatti; tecniche forensi, soluzioni ad alta-tecnologia che richiedono test di laboratorio o kit per test elaborati per valutare la loro l'autenticità; "Segui e traccia" (Track and Trace) che consiste nell'assegnare, durante la produzione, un'unica identità ad ogni stock o al singolo pezzo, che poi rimane per tutta la catena di distribuzione sino al consumatore, tracciandone il percorso completo. La tecnologia segui/traccia presenta molte funzioni distinte: traccia un singolo oggetto attraverso tutta la catena di distribuzione, in ogni suo punto, conserva il percorso ed i passaggi eseguiti a seconda dei punti di controllo decisi a priori, permette l'autenticazione della data e dell'ora del pacco o dell'unità in cui sono applicati. Tale soluzione rappresenta quindi una soluzione migliore rispetto alle precedenti in relazione alla ricerca effettuata nella tesi.

La tecnica fornisce anche altri importanti vantaggi quale un'elevata capacità di memorizzazione un elevato livello di sicurezza. Le soluzioni, all'interno di questa tecnica, che consentirebbero l'incorporazione dei dati in un capo di abbigliamento, sono due: "Codici a barre" e RFID. I primi, in particolare i più evoluti 2D (datamatrix, Qcode, VSCode, VIsual Code, Shotcode, Colorcode), pur incorporando l'identità del prodotto presentano una scarsa capacità di memorizzazione e salvo alcune soluzioni anche una scarsa sicurezza.

Gli RFID forniscono un controllo totale, pur necessitando comunque di ulteriori definizioni degli standard. Inoltre, consentono un pieno automatismo, la possibilità di scambio di dati in maniera bidirezionale fra il lettore ed il tag e come detto pocanzi una capacità di memorizzazione potenzialmente elevata, campo fisico di lettura ampio da pochi centimetri ad alcuni metri. Ed infine, uno

dei fattori più importanti elevata sicurezza sui tag (password e/o crittografia); condizioni che ne hanno fatto la soluzione ideale per un impiego nel lavoro qui proposto.

Il passaggio successivo è stato quello di studiare i sistemi biometrici, semplici e complessi; cercando di sviluppare un metodo analogo applicabile agli oggetti e che consentisse di fornire uno strumento per combattere la contraffazione; si sono cercate soluzioni che potessero tener conto delle caratteristiche intrinseche dei singoli prodotti, alla stregua quindi delle impronte digitali, iride, retina, geometria della mano, etc. per l'uomo; conseguenza logica è stata quella di trovare delle caratteristiche che potessero essere misurate con metodi non distruttivi, e che permettessero la verifica circa la veridicità ed unicità dell'oggetto stesso, rendendo questi complessi alla contraffazione.

Per quanto introdotto pocanzi, la soluzione al problema è stato trovato nell'hylemetria (e nelle PUF), che come indicato in precedenza ha lo scopo di identificare delle caratteristiche, alla stregua della biometria, che rendano un "entità" fisica unica e randomica al fine di identificarla univocamente.

Nel quadro di una lotta alla contraffazione, ciò che è stato importante capire, è stato quale fosse il legame tra un oggetto, e gli elementi di certificazione "indissolubili". Nello specifico se fosse sviluppare dei sistemi anti-contraffazione che leghino le caratteristiche intrinseche di un oggetto ai moderni sistemi di riconoscimento.

A questo punto ci si è interessati a ricercare sistemi che tutelassero i dati Hylemetrici.

Per fare questo era necessario comprendere quali fossero le classificazioni in termini di sicurezza e i limiti degli attuali sistemi.

I sistemi tradizionali spesso pur fornendo una risposta non consentono livelli di sicurezza adeguati, spesso addirittura fallimentari, come per l'ispezione visiva, utile quando si trattano dei documenti protetti con tecniche di stampa particolari (come nel caso delle banconote) ma ad esempio non applicabile ad altri casi. In aiuto a questi metodi viene utilizzata la crittografia

In particolare è risultata molto utile ed idonea la funzione Hash. La funzione Hash è una funzione che "tritura" l'ingresso rendendolo non riconoscibile; quindi le caratteristiche uniche vengono "triturate" in modo "univoco". Per avere la certezza che la funzione Hash non venga sostituita,

(clonazione di un opera per esempio e sostituzione dell'Hash) è indispensabile che venga firmato digitalmente dall'autore o dall'ente certificatore.

A questo punto si è stati in grado di proporre un sistema che consentisse l'acquisizione di strutture random casuali e non duplicabili, già presenti nell'oggetto o introdotti artificialmente, e la loro codifica attraverso procedure di firma digitale asimmetrica, per garantirne la non duplicabilità e la non ripudiabilità.

La procedura d'identificazione "sicura" proposta prevede che il "realizzatore" (designer) di moda una volta realizzato il singolo capo di abbigliamento, parte di una collezione/lotto, estragga una caratteristica Hylemetrica (presente sul capo stesso o opportunamente introdotta), e la invii alla funzione Hash. L'uscita di tale funzione, attraverso la chiave privata del designer viene crittografata; inoltre il designer firma digitalmente il singolo oggetto.

Le informazioni per la decodifica, le informazioni per estrarre l'Hash e il link alla maison, vengono memorizzati su un RFID inserito nel capo; l'inserimento deve essere fatto in modo che il RFID non possa essere rimosso senza distruggerlo e/o senza danneggiare il capo. Ovviamente invece di un RFID è possibile utilizzare un codice a barre bidimensionale, comunque da tener presente, che le informazioni presenti su un codice a barre sono limitate rispetto a quelle memorizzabili su un RFID.

A questo punto il comparatore attraverso un apposito software (APP) ed un semplice smartphone in grado di leggere RFID (o codice a barre 2D) accede alle informazioni presenti sul RFID e qualora non tutte le informazioni fossero presenti sul RFID (scelta discrezionale della casa di moda), si collega alla maison. A questo punto l'app, con opportune indicazioni, chiede all'utente l'acquisizione di un particolare "unico" (caratteristica Hylemetrica) da catturare. Acquisito il particolare d'identificazione (ad esempio un specifico ricamo), l'app provvede ad estrarre l'Hash. Viene effettuato il controllo tra l'Hash memorizzato e l'Hash estratto; e se le due informazioni "coincidono" si ha la "certezza" che il capo è stato realizzato dal Designer "A" fornendo quindi l'informazione sull'originalità del capo.

Il sistema proposto (procedura di autenticazione) consente quindi l'integrazione fra più tecnologie fornendo maggior sicurezza sulla provenienza e autenticità dell'oggetto, e proponendo una

metodologia accessibile ad un largo numero di utenti; la sicurezza alla contraffazione è garantita dall'acquisizione di strutture random casuali e non duplicabili (teoria Hylemetrica) già presenti nell'oggetto o introdotti artificialmente (caratteristiche microscopiche che rendono l'oggetto unico), e la codifica attraverso procedure di firma digitale asimmetrica per garantirne la non duplicabilità e la non ripudiabilità; in altre parole si realizza una sorta di passaporto (Fashion-passport) del capo di moda verificabile sia direttamente che da remoto, nulla ne vieta anche una versione cartacea.

Nella parte finale della tesi si sono quindi analizzati ed effettuate delle proposte concrete di sistemi che permettessero di tutelare la non duplicabilità dei sistemi commercializzati in particolare nel campo della moda (alcuni esempi sono comunque non settoriali); evitando tutti gli inconvenienti dovuti ai metodi tradizionali, puntando essenzialmente sul basso costo di produzione e sulla semplicità.

In particolare si è mostrato il processo che porta al dato hylemetrico (prima del Hash). Sono state quindi proposte alcune tecniche Hylemetriche, naturali o artificiali; a riscontro della validità e dell'efficienza del tecnica scelta. Per quanto concerne tecniche hylemetriche naturali implementabili, sono state considerate le tipiche trame "randomiche" dei tessuti, la Sfumatura di colori presenti nei fili delle cuciture, la marcatura del pellame; in relazione a questo ultimo caso è stato poi mostrato in maniera esaustiva il procedimento di riconoscimento Hylemetrico.

Esempi di tecniche Hylemetriche artificiali sono l'inserimento di fibrille fluorescenti presenti nelle banconote; un'etichetta con presenza di fibrille fluorescenti a cui è possibile per altro stampare, ad esempio, il bordo di un barcode 2D Datamatrix.

Nello specifico è stata studiata dettagliatamente una tecnica Hylemetrica artificiale applicabile su un'etichetta, o su una parte dell'oggetto, mediante l'uso di una tintura/vernice fluorescente sotto illuminazione UV; la cui nebulizzazione produce delle minuscole goccioline che si disperdono in modo "randomico".

Sono stati in conclusione mostrati altri due ultimi esempi, entrambi legati all'inserimento all'interno dei capi di moda di strutture che possano interagire con campi elettromagnetici "esterni", possibilità offerta dall'inserimento di strutture metalliche distribuite casualmente. Nel primo

caso si sono inserite delle strutture sensibili ai campi elettromagnetici all'interno di cuciture (sei "piccoli" frammenti di ferrite). Questi frammenti, se investiti da microonde si scaldano e il calore può facilmente essere rivelato da una termocamera, divenendo un dato hylemetrico. L'altro esperimento proposto in tale contesto propone l'uso di piccole pagliuzze di rame distribuite in modo casuale. Queste pagliuzze possono essere presenti tra la pelle esterna e la fodera di una borsa, così come tra i due strati di una cintura e/o di un portafoglio. Queste strutture possono essere visualizzare "tramite" telecamere operanti nei THz e considerati come dati Hylemetrici.

In conclusione si sono quindi proposte nuove caratteristiche Hylemetriche impiegabili per la lotta alla contraffazione, impiegabili in un ambito tecnologico che ne consente un impiego vasto e diversificato con costi che si ritengono bassi e che possono garantire per un lungo tempo un buon livello di sicurezza.

SOMMARIO

1 ABSTRACT I

2 LISTA DELLE FIGURE XII

3 ELENCO DELLE TABELLE XIV

4 ACRONIMI XV

5 TECNOLOGIE ANTI-CONTRAFFAZIONE 1

5.1 INTRODUZIONE 1
5.2 TECNOLOGIE 2
5.2.1 Caratteristiche visibili – Overt 2
5.2.1.1 Dispositivi ottici variabili – ODV 2
5.2.1.2 Ologrammi 5
5.2.1.2.1 Dot Matrix 6
5.2.1.2.2 Ologrammi 2D/3D 6
5.2.1.2.3 Ologrammi 3D 7
5.2.1.2.4 Ologramma ad immagini combinate 7
5.2.1.2.5 Ologramma Ebeam – Ologramma a fascio di elettroni 7
5.2.1.3 Stampa a caldo 10
5.2.1.4 Inchiostri e pellicole a colorazione variabile 11
5.2.1.5 Grafica di sicurezza 12
5.2.1.6 Numeri di serie sequenziali 13
5.2.1.7 Marcatura del prodotto 13
5.2.1.8 Schema riassuntivo delle tecniche di sicurezza visibili 14
5.2.2 Caratteristiche invisibili – Covert 15
5.2.2.1 Stampa invisibile 15
5.2.2.2 Immagine integrata 16
5.2.2.3 Filigrana – watermarking 16
5.2.2.4 Filigrana e impronte digitali – watermarking/ fingerprinting 18
5.2.2.4.1 Filigrane infrarosse ed ultraviolette 18
5.2.2.5 Marchio e stampa nascoste 19
5.2.2.6 Disegni anti-copia e anti-scansione 19
5.2.2.7 Codice inciso con il Laser 19
5.2.2.8 Substrato 20
5.2.2.9 Odore 20
5.2.2.10 Schema riassuntivo delle tecniche di sicurezza invisibili 21
5.2.3 Marcatori Forensi 21
5.2.3.1 Etichettatura chimica 21
5.2.3.2 Etichettatura Biologica 22
5.2.3.3 Etichettatura tramite DNA 22
5.2.3.4 Percentuale di Isotopi 22
5.2.3.5 Micro-etichette 23
5.2.3.6 Schema riassuntivo delle tecniche che impiegano tecnologie Forensi 24
5.2.4 Segui e traccia 24
5.2.4.1 Serializzazione 26
5.2.4.2 Codici a barre 27
5.2.4.2.1 Tipologie di codici a barre 27
5.2.4.3 Identità in Radio Frequenza (Radio Frequency Identity) – RFID 32

5.2.4.3.1 Tag passivo ... 33
5.2.4.3.2 Tag attivi ... 34
5.2.4.3.3 Tag Semi Passivi ... 34
5.2.4.3.4 Tag – Modalità di funzionamento della memoria interna ... 34
5.2.4.3.4.1 Read Only ... 34
5.2.4.3.4.2 Read & Write ... 34
5.2.4.3.4.3 Write Once – Read Many ... 35
5.2.4.3.5 Tag - Classificazione ... 35
5.2.4.3.6 Reader ... 36
5.2.4.3.7 Applicazioni d'uso ... 37
5.2.4.3.8 Il problema della Privacy ... 38
5.2.4.3.8.1 Contraffazione ... 39
5.2.4.3.8.2 Replay ... 39
5.2.4.3.8.3 Eavesdropping – "Origliare" ... 39
5.2.4.4 Schema riassuntivo delle tecniche di Serializzazione/Segui e Traccia ... 40

6 PRINCIPI DI BIOMETRIA ... 41

6.1 INTRODUZIONE ... 41
6.1.1 Parametri Biometrici ... 42
6.1.2 Struttura di un sistema di riconoscimento biometrico ... 43
6.2 FASI DI RICONOSCIMENTO DI UN SISTEMA BIOMETRICO ... 44
6.2.1 Registrazione ... 45
6.2.2 Verifica ... 45
6.2.3 Autenticazione ... 46
6.3 RENDIMENTO DI UN SISTEMA BIOMETRICO ... 47
6.3.1 Tipologie di errore ... 47
6.3.2 Metriche per la valutazione del rendimento ... 48
6.4 APPLICAZIONI DEI SISTEMI BIOMETRICI ... 50
6.5 TIPOLOGIE DI SISTEMI BIOMETRICI ... 51
6.5.1 Impronte digitali ... 51
6.5.1.1 Acquisizione ... 53
6.5.2 Viso ... 54
6.5.3 Orecchio ... 56
6.5.4 Lingua ... 57
6.5.5 Denti ... 58
6.5.6 Geometria della mano ... 58
6.5.7 Impronta Palmare ... 58
6.5.8 Iride ... 59
6.5.9 Retina ... 60
6.5.10 Battitura ... 61
6.5.11 Firma ... 61
6.5.12 Voce ... 62
6.5.13 Andatura ... 65
6.5.14 Confronto Biometrico ... 66
6.6 CONCLUSIONI ... 67

7 HYLEMETRIA ... 68

7.1 INTRODUZIONE ... 68

7.2 DEFINIZIONE 68
7.3 HYLEMETRIA, PRINCIPALI CARATTERISTICHE 69
7.4 HYLEMETRIA, APPLICAZIONI 70
7.5 LEGAME TRA UN OGGETTO ED ELEMENTI DI CERTIFICAZIONE "INDISSOLUBILI" 71
7.5.1 Archivio sicuro. 72
7.5.2 Uso di funzione one-way (funzione hash). 72
7.6 FUNZIONI FISICHE NON CLONABILI - PHYSICAL UNCLONABLE FUNCTIONS (PUF) 73
7.6.1 Misura delle Inter ed Intra-distanze 75
7.6.2 Effetti ambientali 76
7.6.3 Proprietà delle PUF 77
7.6.3.1 Descrizione delle proprietà 77
7.6.4 Applicazioni PUF 80
7.6.4.1 Puf "non-elettroniche" 80
7.6.4.1.1 PUF ottiche 80
7.6.4.1.2 PUF della carta 82
7.6.4.1.3 CD PUF 82
7.6.4.1.4 RF-DNA 83
7.6.4.1.5 PUF magnetiche" 83
7.6.4.1.6 PUF Acustiche 83
7.6.4.2 PUF Analogiche-Elettroniche 84
7.6.4.2.1 PUF V_T 84
7.6.4.2.2 Distribuzione di Potenza PUF 84
7.6.4.2.3 Rivestimento PUF 84
7.6.4.2.4 LC PUF 85
7.6.4.3 Sistemi basati su ritardi intrinsechi delle PUF 86
7.6.4.3.1 PUF ad arbitraggio 87
7.6.4.3.2 Oscillatore ad anello PUF 90
7.6.4.4 Memorie basate su PUF 92
7.6.4.4.1 SRAM PUF 93
7.6.4.4.2 Butterfly PUF 94
7.6.4.4.3 Latch PUF 95
7.6.4.4.4 Flip-flop PUF 95
7.6.4.5 PUF – Sistemi integrativi, Prospettive e studi in atto 96
7.6.4.5.1 Chiavi offuscate fisicamente (POK - Physically Obfuscated Keys) 96
7.6.4.5.2 Puf controllata – CPUF 96
7.6.4.5.3 PUF riconfigurabili 97
7.6.4.5.4 PUF a lettura quantica 98
7.6.4.5.5 Sistemi SIMPL 98
7.6.4.5.6 PPUF 99
7.6.5 Schema riepilogativo delle PUF 99
7.6.6 Proprietà comuni alle PUF 100
7.6.7 PUF - Considerazioni 103

8 CRITTOGRAFIA 104

8.1 INTRODUZIONE 104
8.2 ALGORITMI DI CIFRATURA 105
8.2.1 Chiave Privata (Crittografia simmetrica) 105
8.2.2 Chiave Pubblica (Crittografia asimmetrica) 106
8.3 FUNZIONAMENTO DEI SISTEMI CRITTOGRAFICI ASIMMETRICI 107

8.4 REQUISITI DELLA CRITTOGRAFIA A CHIAVE PUBBLICA 110
8.5 VULNERABILITÀ DELLA CHIAVE PUBBLICA 112
8.6 LA FIRMA DIGITALE 112
8.7 L'ALGORITMO RSA 113
8.7.1 Algoritmo di Euclide 116
8.7.1.1 Sviluppo dell'algoritmo di Euclide: 116
8.7.2 Generazione delle chiavi 117
8.7.3 Uso dell'algoritmo RSA 118
8.7.4 Sicurezza dell'algoritmo RSA 119
8.8 LA FUNZIONE HASH 120

9 INTEGRAZIONE FRA TECNICHE DI INDUPLICABILITÀ 122

9.1 INTRODUZIONE 122
9.2 PROTEZIONE HYLEMETRICA DEGLI OGGETTI DI MODA 125
9.3 TECNICHE IMPLEMENTATE 127
9.3.1 Introduzione 127
9.3.2 Tecniche 128
9.3.3 Procedura di autenticazione " 131
9.3.4 Esempi di tecniche Hylemetriche utilizzabili 133
9.3.4.1 Caratteristiche randomiche "naturali" 134
9.3.4.1.1 Esempio di procedura di riconoscimento Hylemetrico 135
9.3.4.2 Caratteristiche randomiche "artificiali" 137
9.3.4.2.1 Fibrille fluorescenti 137
9.3.4.2.2 Inserimento di "verniciatura randomica" fluorescente. 139

10 CONCLUSIONI 144

11 BIBLIOGRAFIA E SITOGRAFIA 145

2 Lista delle Figure

Figura 1 – Esempio di etichetta antimanomissione....4
Figura 2 – Esempio di ologramma Tamper Evident su scotch da imballaggio....5
Figura 3 – Esempio di ologramma 2D/3D (Suzhou Image Laser Technology Co., ltd)....6
Figura 4 – Ologramma ad immagini combinate....7
Figura 5 – Esempio di Ologramma Ebeam....8
Figura 6 – Generazione olografica di un fascio di elettroni di Airy....9
Figura 7 – Passaggi della stampa a caldo....10
Figura 8 – Esempio di inchiostro a colorazione variabile presente sulle banconote da 50 Euro....11
Figura 9 – Stampa di fondo/di sicurezza con vari elementi....12
Figura 10 – Dettaglio della nuova carta d'identità elettronica, a sinistra la carta in condizioni di luce naturale, a destra la carta sotto un illuminazione UV....15
Figura 11 – Rullo "Mollette"....16
Figura 12 - Esempio di macchina dandy roll usata per la stampa di filigrane chiare nella carta....17
Figura 13 – Esempi di filigrane....17
Figura 14 – Esempio di watermarking....18
Figura 15 – Banconota da 100 Euro esposta ai raggi ultravioletti....19
Figura 16 – Linea di preparazione agli imballaggi....26
Figura 17 – Esempio di struttura QR code....28
Figura 18 – Esempi di codici a barre bidimensionali....32
Figura 19 – Esempi di RFID....32
Figura 20 – Esempi di RFID applicati ad etichette....38
Figura 21 – Struttura di un sistema di riconoscimento biometrico....43
Figura 22 – Composizione di un sistema biometrico....44
Figura 23 – Metriche del rendimento di un sistema biometrico....49
Figura 24 – Micro-caratteristiche delle impronte: Minuzie....53
Figura 25 – Micro-caratteristiche delle impronte: Pori, Profili delle linee e delle creste....53
Figura 26 – Caratteristiche biometriche dell'orecchio....57
Figura 27 – Esempio di immagini dell'iride acquisite da diversi sensori, si può notare la differenze dei modelli dell'iride....60
Figura 28 – Crittografia a chiave pubblica....72
Figura 29 – Rappresentazione di un'implementazione base, con le operazioni di una PUF ottica .81
Figura 30 – Operazioni base di un rivestimento PUF....85
Figura 31 – Operazioni base di una PUF ad arbitraggio....88
Figura 32 – Operazioni base di una oscillatore ad anello PUF....90
Figura 33 – Oscillatore PUF ad anello con compensazione a divisione....91
Figura 34 – Oscillatore PUF ad anello con compensazione a comparatore....92
Figura 35 – Circuito Logico di una SRAM (PUF)....93
Figura 36 – Circuito elettrico di una cella SRAM (PUF) in tecnologia CMOS....93

Figura 37 – Circuito di una cella Butterfly PUF 94
Figura 38 – Crittografia simmetrica 106
Figura 39 – Crittografia asimmetrica 107
Figura 40 – Autenticazione 110
Figura 41 – Firma digitale con algoritmo RSA 113
Figura 42 – Pinze chirurgiche con "marcatura" del metallo. 122
Figura 43 – Tecniche biometriche vs. tecniche Hylemetriche. 123
Figura 44 – Particolari di oggetti originali vs. falsi 123
Figura 45 – Etichetta con all'interno un RFID. 124
Figura 46 – Lettura di un RFID con Smartphone dotato di tecnologia NFC. 124
Figura 47 – Schema di principio per la realizzazione di una infrastruttura per la certificazione dell'autenticità di un oggetto. 127
Figura 48 – Funzione Hash applicata alle impronte digitali 129
Figura 49 – Funzione Hash applicata a una cucitura a mano 130
Figura 50 – Capo di moda legato in modo "indissolubile" ad informazioni che lo rendono unico e non-duplicabile (Fashion passport) 131
Figura 51 – Procedura di identificazione "sicura" 132
Figura 52 – Tipica trama "randomica" dei tessuti 134
Figura 53 – Sfumatura di colori presenti nei fili delle cuciture 134
Figura 54 – Tipica marcatura del pellame 135
Figura 55 – Caratteristica Hylemetrica estratta da un ricamo fatto a mano 135
Figura 56 – Procedimento di riconoscimento Hylemetrico 137
Figura 57 – Fibrille fluorescenti presenti in una banconota da 10 Euro 138
Figura 58 – Etichetta con presenza di fibrille fluorescenti 138
Figura 59 – Etichetta con presenza di fibrille fluorescenti; estrazione dell'Hash 139
Figura 60 – Texture randomica fluorescente presente sulla spiaggia di Leucadia in California. ..140
Figura 61 – Un nebulizzatore d'inchiostro/vernice produce delle minuscolo goccioline che si disperdono in modo "randomico" sia spazialmente sia come dimensione geometrica. 140
Figura 62 – Immagine di una etichetta, dove è presente una vernice fluorescente "spruzzata" casualmente" illuminata con luce bianca e con radiazione UV. 141
Figura 63 – Statistica estratta da uno dei blocchi ricavati dall'immagine a speckle. 142
Figura 64 – Statistica estratta da uno dei blocchi ricavati dall'immagine a speckle. 142
Figura 65 – Pattern di temperatura attenuti irraginado con microonde dei "piccoli" frammenti di ferrite. 143

3 Elenco delle Tabelle

Tabella 1 Schema riepilogativo dei vantaggi/svantaggi delle tecnologie visibili 14
Tabella 2 Schema riepilogativo dei vantaggi/svantaggi delle tecnologie invisibili 21
Tabella 3 Schema riepilogativo dei vantaggi/svantaggi delle tecnologie Forensi 24
Tabella 4 Classificazione dei tag in virtù della Classe.....35
Tabella 5 Classificazione dei tag in virtù della frequenza.....36
Tabella 6 Schema riepilogativo dei vantaggi/svantaggi delle tecnologie invisibili 40
Tabella 7 Comparazione delle principali caratteristiche biometriche. 66
Tabella 8 Comparazione fra le principali caratteristiche delle PUF. 100
Tabella 9 Tabella riassuntiva delle proprietà delle PUF. 102
Tabella 10 Algoritmo RSA.....119

4 Acronimi

AFIS	Automatic Fingerprint Identification System
ANSI	American National Standards Institute
ASIC	Application specific integrated circuit
CPUF	Controlled PUF – PUF controllata
CRP	Challenge–response pair - Interrogazione-response pair
CTW	Context Tree Weighting
DOVID	Diffractive Optically Variable Image Devices - Elementi di diffrazione ottica di immagini variabili
EER	Equal Error Rate - valore con uguale errore
FAR	False Accept Rate - Falsa soglia di accettazione
FFT	Fast Fourier Transform – Trasformata veloce di Fourier
FRR	False Rejection Rate - Falsa soglia di rifiuto
FTC	Failure To Capture - fallimento in acquisizione
FTE	Failure to Enroll - fallimento in registrazione
ICID	Integrated circuit identification – Circuito integrato di identificazione
ISO	International Organization for Standardization - Organizzazione internazionale per la normazione
NFC	Near Field Communication – Comunicazione a “campo vicino”
NIST	National Institute of Standards and Technology
ODV	Optical variable device o optically variable device-Dispositivi ottici variabili
POK	Physically obfuscated key – Chiavi fisicamente offuscate
PPUF	Public Physical Unclonable Functions - funzioni pubbliche fisiche inclonabili
PUF	Physical Unclonable Functions - funzioni fisiche inclonabili
RFID	Radio Frequency Identity
ROC	Receiver Operating Characteristic - Caratteristica Operativa Ricevuta
SIMPL	SIMulation Possible but Laborious – Simulazione possibile ma laboriosa
SRAM	Static random access-memory – Memoria statica ad accesso casuale

5 Tecnologie anti-contraffazione

5.1 Introduzione

I produttori oggi hanno a disposizione un gran numero di tecnologie per l'anti-contraffazione e marchi di proprietà, dai più semplici ma di effetto, ai più sofisticati ed estremamente sicuri; la maggior parte di dette tecnologie può essere implementata su uno o più componenti degli imballi, ma alcune caratteristiche possono essere applicate in fase di produzione, contrassegnando direttamente ciascun prodotto mediante l'uso sia di marcature sia fisiche che chimiche.

Lo scopo di una caratteristica anti-contraffattiva è principalmente di permettere la verifica dell'autenticità di un oggetto da parte di un organo governativo o industriale e da parte di un acquirente, e consentire l'individuazione di un oggetto non originale.

Il secondo possibile scopo è quello di generare un effetto deterrente a possibili malintenzionati, ciò mediante l'uso di sistemi anti-contraffattivi che introducono difficoltà alla riproduzione e aumentando i costi legati alla produzione.

Deve essere sottolineato che i dispositivi di sicurezza presenti negli imballi non assicurano l'autenticità del contenuto, il quale potrebbe essere sostituito o alterato.

I dispositivi di sicurezza da soli non riducono la contraffazione, ma vengono concepiti per consentirne la scoperta.

Le attuali tecnologie anti-contraffattive impiegate possono essere divise in quattro categorie (World Health Organization, 2014)

- Caratteristiche visibili (Overt)
- Marcature invisibili (Covert)
- Tecniche forensi
- Tecniche di serializzazione/ segui e traccia

Di seguito verranno analizzate in dettaglio le categorie di cui sopra, al fine di avere un quadro completo delle tecniche anti-contraffattive attualmente disponibili.

5.2 Tecnologie

5.2.1 Caratteristiche visibili – Overt

Le caratteristiche visibili (overt) sono progettate in modo da permettere all'utente finale di verificare l'autenticità di un oggetto su cui è posto; tali caratteristiche sono normalmente ben visibili, inizialmente difficili o costose da riprodurre, oggi più semplici da riprodurre, ed economiche.

Queste caratteristiche permettono all'utente una verifica veloce sull'originalità del bene in osservazione; infatti un oggetto falso è una semplice copia, che ne richiama una caratteristica originale; tuttavia spesso i falsi sono sufficientemente ben fatti e confondono persino gli utenti più attenti.

Le caratteristiche di tipo visibile richiedono estrema attenzione in termini di sicurezza nella fornitura, nella manipolazione e nel controllo delle procedure per evitare manomissioni o diversivi di personale non autorizzato. Le caratteristiche visibili, infatti, dovrebbero essere applicate in maniera da non poter essere ri-usate o rimosse senza causare danni alla confezione; altrimenti, un loro riutilizzo comporterebbe che una confezione può essere scambiata per un'originale, dando così una falsa impressione di autenticità; per questo motivo una caratteristica visibile dovrebbe essere incorporata all'interno di una caratteristica con evidenza di manomissione per aumentarne la sicurezza.

5.2.1.1 Dispositivi ottici variabili – ODV

I dispositivi ottici variabili includono una vasta gamma di dispositivi, spesso senza componenti in tre dimensioni; generalmente includono immagini a scatti o a transazione, spesso includono trasformazioni di colore o contrasti monocromatici. Fanno parte di questi dispositivi anche gli ologrammi, che verranno trattati a parte in maniera esaustiva.

I dispositivi ottici variabili sono generalmente fatti di un film trasparente che serve come trasportatore dell'immagine, uno strato riflessivo posto alle spalle del film che è normalmente molto sottile, ed infine di uno strato di alluminio. In alcune applicazioni con particolare livello di sicurezza vengono impiegati nei processi produttivi altre tipologie di metallo, quale il rame che consente di in alcune applicazioni di dare una caratteristica tinta contraddistintiva.

Un miglioramento della sicurezza può essere inoltre dato dal processo di parziale de-metallizzazione di alcuni strati riflessivi effettuato per via chimica, che genera nell'immagine un contorno "intricato" (alcune banconote presentano detta tecnica). La parziale rimozione dello strato metallico è un processo però più restrittivo perché se è vero che aumenta sotto alcuni aspetti il livello di sicurezza, è anche vero che aumenta il costo di produzione.

In alternativa lo strato riflessivo può essere talmente fino da apparire quasi trasparente, risultando un film chiaro con più immagini "fantasma" riflesse; visibile solo sotto alcune angolazioni ed illuminazioni.

I fornitori spesso, decidono di produrre etichette che combinano più ODV, ciò al fine di migliorare le prestazioni dei loro prodotti e per migliorare il livello di sicurezza, consentendo all'utente finale di eseguire una semplice verifica del marchio del prodotto. La combinazione di stampa e di ODV consente di ottenere anche, rispetto all'uso di un solo ODV, un prodotto esteticamente più piacevole. Lo scenario risulta molto variegato infatti si noti che le etichette possono anche essere composte con inchiostri indelebili, numerate, e quelle di dimensioni maggiori possono disporre di codici a barre o sistemi più complessi.

Le tecnologie di ODV più diffuse sono sotto riportate:

- Effetti-Void: Effetto che appare su una superficie inizialmente di colore uniforme (Figura 1), quando questa viene forzata, evidenziandone irreversibilmente l'apertura. Tale scritta o logo può essere personalizzabile.
- Die-Cutting: Etichette di protezione pre-forate secondo pattern specifici e personalizzabili, tali che, ad ogni tentativo di rimozione si rompono, e non possono più essere ricomposte.
- Adesivi: dalla combinazione di diversi adesivi e materiali è possibile ottenere soluzioni flessibili in grado di adeguarsi a diversi requisiti.

Figura 1 – Esempio di etichetta antimanomissione

Il ODV può essere fornito quindi come etichetta sensibile alla pressione (autoadesiva) o come un foglio adatto per stampa a caldo o a freddo. Le immagini ODV possono anche essere fornite come pellicola adatta ad applicazioni di imballaggio.

Nella maggior parte dei casi, sono stati prodotti degli ODV che possono essere usati su carte di credito, banconote, biglietti, documenti stampati, i più famosi e diffusi ODV sono gli ologrammi discussi nel paragrafo successivo.

Come accennato in antecedenza i produttori tendono ad usare più tecniche ODV per migliorare la sicurezza pertanto ciò avviene anche con gli ologrammi, che sono resi più efficaci quando incorporati con caratteristiche ad evidente manomissione o integrati in un pacco principale mediante incorporazione in bande a strappo, o l'inserimento all'interno di un substrato di carta.

Nell'immagine sotto (Figura 2) vi è un esempio di tecnica mista; l'ologramma può quindi essere prodotto su materiale tamper-evident[1], tamper-evident **VOID**, ed essere numerato progressivamente e fornito in piste o bobine. (Diavy S.r.l., s.d.)

[1] Materiale tamper-evident alias materiale ad "evidente manomissione" ottenuta con la de-metallizzazione selettiva

Figura 2 – Esempio di ologramma Tamper Evident su scotch da imballaggio

5.2.1.2 Ologrammi

Probabilmente la più familiare delle caratteristiche visibili è l'ologramma, tale tipologia di tecnica è stata usata per proteggere le carte di credito per molti anni in maniera efficace. Un ologramma normalmente incorpora immagini aventi costruzioni in tre-dimensioni ed illusioni ottiche, o un'apparente profondità ed una separazione speciale.

L'ologramma, o DOVIDs (Diffractive Optically Variable Image Devices) è forse il più famoso degli ODV, ed è costituito da una microstruttura creata con l'uso di un dispositivo laser, che dà origine ad immagini animate o semplici pattern.

Tale tecnica rappresenta sicuramente un deterrente alla contraffazione, poiché rende più difficile la copia anche con avanzate tecnologie o la riproduzione anche mediante l'uso di scanner ad alta definizione, fotocopie a colori, o qualsiasi dispositivo di stampa; oggi non è inviolabile come in passato, ma sicuramente richiede uno sforzo maggiore da parte di malintenzionati.

Gli ologrammi possono incorporati, come mostrato nel paragrafo precedente, in molteplici livelli di sicurezza:

1° livello: ha visibilità immediata dall'occhio

2° livello: l'autenticazione è verificata dall'uso di un dispositivo ottico minore

3° livello: presuppone l'uso di un microscopio per l'autenticazione,

4° livello: è appositamente progettato su richiesta, integrando altri sistemi di sicurezza

Dei paragrafi successivi verranno mostrati i principali tipi di ologrammi esistenti.

5.2.1.2.1 Dot Matrix

Ologramma generalmente piatto e monodimensionale, presenta una elevata percezione cinetica dell'immagine olografica.

La tecnica dot-matrix consiste nella realizzazione di una matrice di reticoli diffrattivi, delle dimensioni dell'ordine di decine di micron, registrati in successione con fasci laser focalizzati.

Il controllo automatizzato delle orientazioni dei reticoli permette di ottenere svariati effetti cinetici come espansioni e contrazioni, rotazioni, sfumature. (Istituto Poligrafico e Zecca dello Stato S.p.A, s.d.)

5.2.1.2.2 Ologrammi 2D/3D

Gli ologrammi 2D-3D hanno la peculiarità dell'effetto tridimensionale; l'immagazzinamento cioè dell'informazione della profondità. In questo tipo di ologramma quest'effetto è ottenuto con la collocazione spaziale differenziata d'oggetti bidimensionali, riprodotti a profondità diverse. La tecnologia 2D - 3D offre la possibilità di originare effetti multicanali e cinematismi, e di registrare una sequenza di immagini che viene riprodotta ruotando l'ologramma lungo l'asse verticale. La difficoltà in un eventuale riproduzione di questo tipo d'ologramma consiste, oltre che nel generare un disegno identico all'originale, anche nel riprodurre la stessa combinazione di colori, profondità ed effetti cinetici.

Figura 3 – Esempio di ologramma 2D/3D (Suzhou Image Laser Technology Co., ltd)

5.2.1.2.3 Ologrammi 3D

Tale tipo di ologrammi sono creati con l'utilizzo di un laser che riproduce un modello 3D dell'oggetto, sviluppato al computer o con un micro-modello. Nell'ologramma di tipo 3D, la tridimensionalità è data dall'inserimento di un modello fisico in tre dimensioni, che esce dal piano olografico. L'immagine olografica è un'informazione completa del fronte d'onda emesso da un oggetto illuminato. La percezione visiva di un oggetto ripreso nell'ologramma è dunque la stessa che si ha osservandolo nella realtà, con la possibilità di ruotarlo per cambiare la proiezione delle ombre o la visione prospettica. La riproduzione di un ologramma 3D presuppone la realizzazione di un modello identico all'originale, la stessa geometria d'illuminazione ed uguale combinazione cromatica.

5.2.1.2.4 Ologramma ad immagini combinate

Questo particolare ologramma consiste in una combinazione delle tecnologie sopra menzionate, nata per aumentarne la sicurezza. L'ologramma nella Figura 4, mostra un esempio di ologramma ad immagini combinate, realizzato presentando diverse apparenze secondo le condizioni di osservazione, tale ologramma è realizzato da tanti reticoli di diffrazione, che disperdono la luce visibile incidente con angoli diversi; in particolare l'ologramma in figura è realizzato con tecnica mista Dot-Matrix e ologramma 2D/3D ed è presente sulla carta d'identità elettronica

Figura 4 – Ologramma ad immagini combinate

5.2.1.2.5 Ologramma Ebeam – Ologramma a fascio di elettroni

Ologramma generato senza l'ausilio del laser, fu inventato da Gabor (Gabor, 1948) già nel 1948 durante uno studio di perfezionamento del microscopio elettronico. La struttura di base dell'immagine è scritta a livello microscopico, mediante l'uso di un generatore di un fascio di elettroni, che

mostrano un elevata coerenza temporale e spaziale. Questo tipo di immagine può includere elementi tridimensionali ed altamente cinetici. Tale sistema di generazione dell'ologramma è altamente sicuro, ma ha un elevato costo di produzione. Viene di seguito mostrato un esempio di un ologramma di questo tipo (Security Hologram, 2015).

Figura 5 – Esempio di Ologramma Ebeam

A titolo di esempio, si riporta un nuovo sistema di generazione olografica che usa un fascio di elettroni di Airy (Voloch-Bloch, et al., 2013)

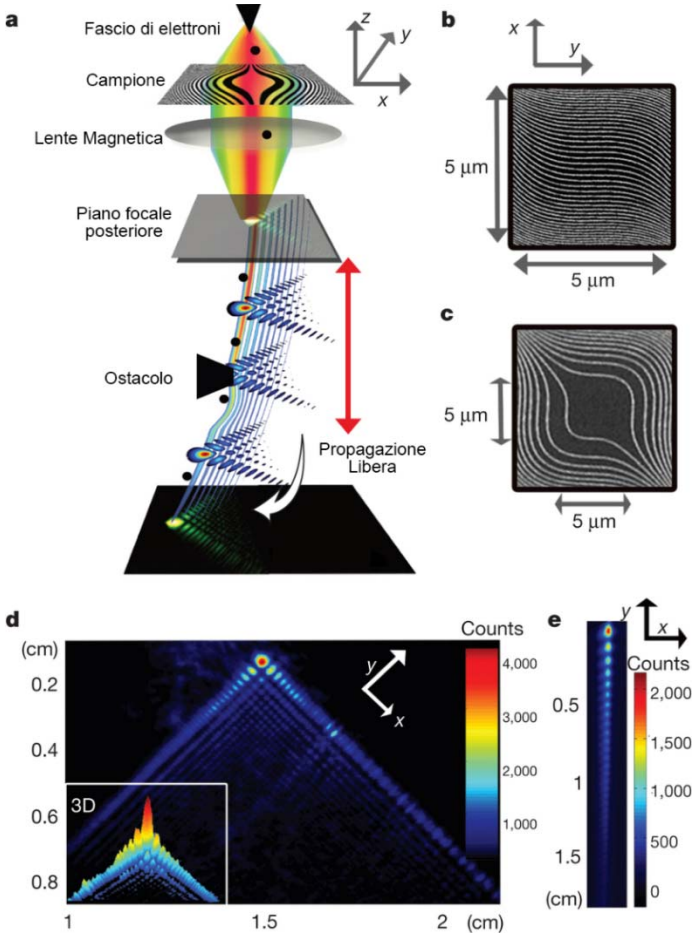


Figura 6 – Generazione olografica di un fascio di elettroni di Airy

Nella figura sopra è mostrata la generazione olografica mediante l'ausilio di un fascio di elettroni di Airy; il fascio di elettroni viene trasmesso attraverso un ologramma fabbricato con nanotecnologie, con una modulazione di fase cubica. Nella parte (a) è mostrata la propagazione del fascio dalla sorgente, il fascio viene quindi focalizzato con l'ausilio di una lente magnetica. L'onda di Airy si formata in corrispondenza del piano focale posteriore e ne viene registrata la propagazione. Il fascio di elettroni dell'onda di Airy è un fascio che tende a conservare la forma durante la propagazione lungo la traiettoria curva, e qualora trovi un ostacolo superato torna alla sua traiettoria precedente.

In figura nei punti b), c) sono illustrate delle micrografie TEM degli ologrammi in nanoscala: la prima immagine è un'immagine bidimensionale di Airy su una frequenza portante di tipo spaziale; la seconda è un'immagine bidimensionale di Airy senza portante

Nel punto d) è possibile vedere al microscopio il pacchetto d'onda in due dimensioni; nell'immagine e) una vista del fascio di elettroni di Airy monodimensionale.

5.2.1.3 Stampa a caldo

Tale tecnica presenta specifiche elevate ed è applicata usando attrezzature specialistiche impiegate solo per la produzione di prodotti in fabbrica. Le principali stampanti a caldo, usate in ambito sicurezza, usano un foglio con stampa a caldo. In generale, il foglio menzionato è usato nella giunzione della carta o dei substrati di polimeri plastici. Viene quindi inserito un materiale prestampato ed un ODV che è applicato all'interno delle superfici dei materiali, il tutto è sigillato usando una pressa ad alta velocità.

Questo processo consente l'inserimento di un ODV in un assegno, in etichette, biglietti e documenti finanziari. Il processo di applicazione ha di solito una precisione di +/- 0,25 millimetri e garantisce la coerenza in tutto il ciclo di produzione. L'impiego di un sistema di questo tipo rappresenta comunque un applicazione limitata.

a) Stemma originale

b) Lamina per stampa a caldo

c) Prodotto finale

Figura 7 – Passaggi della stampa a caldo

5.2.1.4 Inchiostri e pellicole a colorazione variabile

Questa tipologia di inchiostri cambiano colore a seconda dell'angolo di osservazione e possono risultare efficaci sia se utilizzati come elementi di grafica visibile che come sistemi di sicurezza grafica, venendo incorporati in sigilli di sicurezza.

I pigmenti dei colori variabili sono finemente macinati in lamine metalliche; necessitano di essere posati in un film opaco fino, per fissare l'effetto ottico e soddisfare meglio le tecniche di stampa, come la fotoincisione e la litografia.

La sicurezza che offrono è legata alla specificità e al cambiamento dinamico del colore, combinato con le difficoltà e la spesa della produzione.

Tali sistemi sono ottenibili con un numero limitato di pigmenti, attraverso l'utilizzo di pochi inchiostri prodotti da specialisti. E' quindi possibile un'autenticazione di tipo forense mediante l'uso del microscopio e marcatori impressi.

Pellicole a colorazione variabile sono usate in applicazioni di sicurezza; richiedendo un deposito multistrato di pellicole per costruire una struttura unica con proprietà diffrattive e con transazioni oscillanti di colore. Tali pellicole possono essere applicate come sigillo di sicurezza o come timbro all'etichetta visibile

Figura 8 – Esempio d'inchiostro a colorazione variabile presente sulle banconote da 50 Euro

5.2.1.5 Grafica di sicurezza

Tale tecnica usa linee di colore stampate in maniera molto sottile, simile alla stampa di banconote, incorporando elementi visibili e invisibili come Ghiglioscé[2], modulazione di linee e linee a rilievo; tali elementi grafici possono essere usati come sfondo in una zona specifica, come un area di sovrastampa, oppure come grafica completa dell'imballo; può inoltre essere stampata come normale offset, oppure per aumentare la sicurezza della stampa a intaglio. L'uso sottile di colori a pastello distribuiti a chiazze genera una grafica più difficile da scansionare e riprodurre, la sicurezza può essere poi aumentata incorporando uno spettro di disegni nascosti, come immagini latenti o micro-testi.

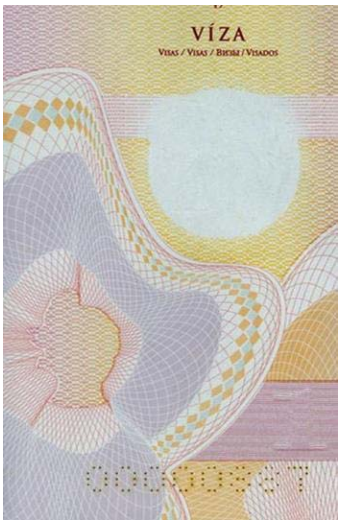


Figura 9 – Stampa di fondo/di sicurezza con vari elementi

Nell'immagine sopra è possibile notare alcune peculiarità di questo tipo di stampa come le rabescature o i motivi a linee sottili, il motivo a griglia, la micro stampa, le zone di colore uniforme e linee sottili in rilievo.

[2] Indica una caratteristica lavorazione ornamentale, di superfici generalmente metalliche, ottenuta con apposite macchine che, guidate manualmente, generano un disegno ripetitivo di righe incise, lineari oppure ondulate. Con accessori dedicati è possibile anche disegnare cerchi concentrici o ghiglioscinare forme cilindriche e di rivoluzione, come penne stilografiche.

5.2.1.6 Numeri di serie sequenziali

L'utilizzo di un numero seriale unico per ogni imballaggio o di un'etichetta può rendere più semplice l'identificazione nella catena di fornitura. Se stampata in maniera visibile, può essere assimilata ad un sistema misto cioè visibile e invisibile; la parte visibile è ovviamente il codice seriale mentre la parte invisibile permette l'autenticazione mediante la verifica in un database, i duplicati o i numeri invalidati vengono infatti verificati e rigettati dal sistema.

Il principale svantaggio di questa tecnica è che la sequenzialità può essere predetta e facilmente replicabile ed inoltre, l'utente finale dovrebbe aver accesso al database; i sistemi più sicuri consentono una serializzazione con una sequenza pseudo-randomica non ripetibile che verrà discussa nei paragrafi successivi.

5.2.1.7 Marcatura del prodotto

La tecnologia di marcatura del prodotto permette l'inserimento di speciali immagini o codici su forme convenzionali; queste tecnologie visibili possono essere difficilmente riproducibili ed offrono tecnologie di sicurezza a piccolissimi livelli.

Questa caratteristica di sicurezza risulta utile qualora i prodotti e gli imballaggi vengano separati.

5.2.1.8 Schema riassuntivo delle tecniche di sicurezza visibili

Di seguito viene riportato uno schema a carattere generale che riassume i vantaggi e svantaggi delle tecnologie visibili:

Caratteristiche visibili	
Vantaggi	Svantaggi
Verificabile dall'utente	Richiedono conoscenza da parte dell'utente – non sempre sono riconoscibili o interpretabili da parte di questi
Tecnologie con un livello di sicurezza maggiore	Possono essere facilmente imitati
Possono apparire esteticamente gradevoli in quanto decorative	Aggiungono un costo significativo
Possono fungere da deterrente alla contraffazione	Potrebbero aver bisogno di caratteristiche nascoste per l'autenticazione
	Potrebbe essere ri-usata
	Potrebbero fornire false assicurazioni di sicurezza

Tabella 1 – Schema riepilogativo dei vantaggi/svantaggi delle tecnologie visibili

5.2.2 Caratteristiche invisibili – Covert

Lo scopo di una caratteristica invisibile è di permettere al proprietario del marchio di fabbrica di identificare i prodotti contraffatti, rendendoli però invisibili ad occhio nudo.

Il pubblico generalmente non si accorge della presenza e non è in grado di verificarli; una caratteristica invisibile non dovrebbe essere semplice da rilevare o copiare, i dettagli inerenti questi elementi dovrebbero essere controllati solo con conoscenze "need to know", ovvero con le sole informazioni strettamente necessarie; il loro controllo richiede quindi una conoscenza compartimentale da parte di chi opera.

Se compromesse o pubblicizzate, molte caratteristiche invisibili perderebbero in parte o totalmente la sicurezza che forniscono.

5.2.2.1 Stampa invisibile

Gli inchiostri speciali utilizzati come marcatori invisibili, possono essere stampati su qualunque substrato e possono essere visti e verificati solo in alcune condizioni come l'illuminazione IR e UV; tali inchiostri vengono inseriti per aggiungere alcuni aspetti peculiari, mostrando infatti diversi colori a seconda delle lunghezze d'onda e della differente illuminazione che le colpisce.

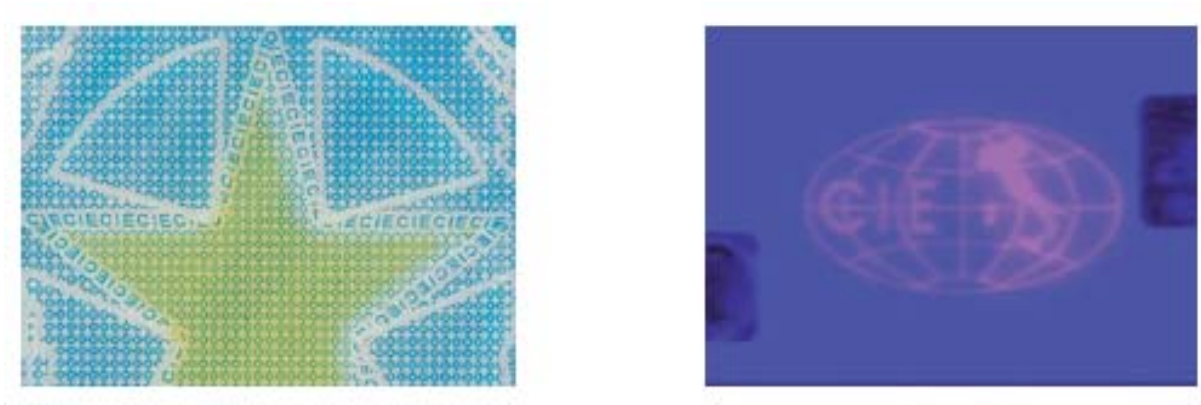


Figura 10 – Dettaglio della nuova carta d'identità elettronica, a sinistra la carta in condizioni di luce naturale, a destra la carta sotto un illuminazione UV.

5.2.2.2 Immagine integrata

Tale tecnologia consiste in un'immagine invisibile integrata all'interno di un'altra immagine o in un marchio noto e presente sull'imballo; visibile mediante l'uso di speciali filtri e non riproducibile dai comuni scanner.

5.2.2.3 Filigrana – watermarking

La filigrana è il marchio di fabbrica della cartiera produttrice, rappresenta uno dei riferimenti più importanti per la datazione e la localizzazione della carta (Wikipedia, 2015); in pratica vengono integrate nella carta delle particolari immagini o scritte, che possono assumere la connotazione di un ritratto, un disegno, un sigillo. Un'altra definizione più tecnica identifica la filigrana come una serie di zone d'ombra e zone chiaroscuro, visibili quando il foglio è illuminato in riflessione o trasmissione (Biermann, 1996).

E' possibile distinguere tre tipi di filigrana:

- Filigrana nera (opaca)
- Filigrana chiara
- Filigrana ombrata

La filigrana nera, chiamata filigrana "Molette", è ottenuta passando sulla carta a fine ciclo di produzione ma ancora umida su un particolare rullo detto "Molette".

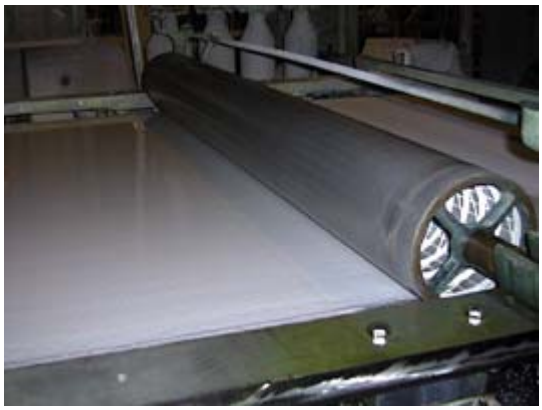


Figura 11 – Rullo "Mollette".

La filigrana Chiara, detta anche ombrata, è creata inserendo (filigrane che generano ombre) o togliendo (effetto della filigrana più chiaro) della carta ancora pastosa dalla sezione della cinghia di produzione della macchina; generando una filigrana con vergature "egoutteur" (machine anche dette dandy-roll). E' possibile realizzare filigrane mezzo-tono, usando stampi a cilindro, il cui motivo è situato direttamente sullo stampo del cilindro.

Figura 12 - Esempio di macchina dandy roll usata per la stampa di filigrane chiare nella carta.

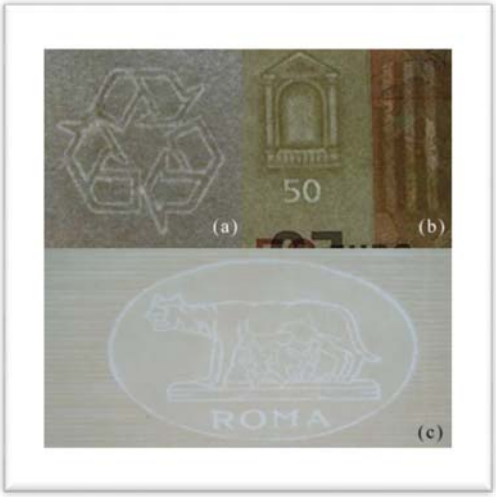


Figura 13 – Esempi di filigrane

Nell'immagine sopra è possibile vedere nel punto a) e c) un esempio di filigrana nella carta, nel punto b) la Filigrana in una banconota da 50 Euro.

5.2.2.4 Filigrana e impronte digitali – watermarking/ fingerprinting

Trattasi di dati invisibili digitalmente codificati all'interno di elementi grafici verificabili con lettori e software dedicati. I dati possono essere catturati mediante l'uso di una semplice webcam, cellulare o scanner; le informazioni non sono ovviamente visibili ad occhio nudo o interpretabili; inoltre una duplicazione potrebbe comportare la degradazione dei dati invisibili integrati e conseguentemente rendere non verificabile l'oggetto e non consentire l'accettabilità dello stesso. Di seguito nella Figura 14 viene mostrato un esempio di watermarking che consente la pubblicazione di stampe (Mills & CNET, 2011), nell'esempio l'obiettivo non è quello della tutela dei dati ma di consentire un accesso veloce all'utente.

Figura 14 – Esempio di watermarking

5.2.2.4.1 Filigrane infrarosse ed ultraviolette

Se esposte ai raggi infrarossi le zone in cui sono presenti filigrane di questo tipo mostrano aree più scure in zone differenti a seconda del valore nominale. Se esposte invece ai raggi ultravioletti, la zona con la filigrana viene messa in risalto con un forte contrasto, così come alcune zone che appaiono fluorescenti.

Sotto un immagine in cui è integrata la filigrana digitale usata dalla EURion constellation, per scoraggiare la contraffazione, nel disegno delle banconote.

Figura 15 – Banconota da 100 Euro esposta ai raggi ultravioletti.

5.2.2.5 Marchio e stampa nascoste

Speciali marchi e stampe invisibili possono essere applicati in modo tale da essere posti in maniera che non destino attenzione e non siano semplici da copiare. La loro efficacia è legata ad una combinazione di segretezza e sottigliezza nell'utilizzo; non offrono però maggiori garanzie rispetto alle tecniche precedenti

5.2.2.6 Disegni anti-copia e anti-scansione

Questi disegni di sfondo aventi linee fini risultano avere una tonalità uniforme, ma quando scansionati o copiati essi rivelano un'immagine latente che inizialmente non risultava visibile; usati comunemente per l'autenticità dei documenti, possono essere impiegati sugli imballi come sfondo.

5.2.2.7 Codice inciso con il Laser

Consiste nell'applicazione di una serie di dettagli variabili mediante un codice effettuato con il laser; per essere elaborata questa tecnica richiede speciali apparecchiature abbastanza costose; il risultato è un artefatto riconoscibile ma difficilmente riproducibile. I codici laser possono essere applicati su cartoni ed etichette, sia su componenti plastiche che metalliche.

5.2.2.8 Substrato

Esistono numerosi modi per incorporare marcatori nascosti all'interno di un substrato, ad esempio fibre fluorescenti, reagenti chimici nelle tavole di cartoni o nella carta; i marcatori possono essere incorporati in volantini di carta, oppure in pagliuzze metalliche mischiate nel materiale di base, è inoltre possibile introdurre in detta tecnica anche ODV nascosti.; questi ultimi richiedono una sorgente di alimentazione dedicata e una produzione su larga scala che garantisce un risultato molto efficace.

5.2.2.9 Odore

Un'ulteriore tecnica consiste nell' inserire determinati "odori" micro-incapsulati in un inchiostro o in un rivestimento per fornire una nuova caratteristica nascosta o semi-nascosta.

Questa tecnica presenta ovviamente alcune difficoltà intrinseche legate alle condizioni di trasporto, metereologiche ed ai sistemi di riconoscimento e spesso possono essere riprodotti anche sinteticamente da un malintenzionato.

5.2.2.10 Schema riassuntivo delle tecniche di sicurezza invisibili

Di seguito viene riportato uno schema a carattere generale che riassume i vantaggi e svantaggi delle tecnologie invisibili:

Caratteristiche visibili	
Vantaggi	Svantaggi
Semplici e poco costose da implementare	Richiedono di non essere divulgate e va seguito il principio "need to know"
Non necessitano di approvazione ufficiale	Se largamente conosciuti o usati, possono essere semplicemente copiati
Possono essere aggiunti semplicemente o modificati	Opzioni più sicure aggiungono un ulteriore livello di complessità e un maggior costo
Possono essere applicati in fase di immagazzinamento o mediante l'aggiunta di componenti addizionali	Se applicati a componenti aggiuntivi, aumentano il rischio di compromissione

Tabella 2 – Schema riepilogativo dei vantaggi/svantaggi delle tecnologie invisibili

5.2.3 Marcatori Forensi

C'è una vasta gamma di soluzioni ad alta-tecnologia che richiedono test di laboratorio o kit per test elaborati per valutare la loro l'autenticità; queste sono una ristretta sotto-categoria di tecnologie non-visibili, ma la differenza è nel metodo scientifico richiesto per l'autentificazione; l'impiego di queste tecnologia rappresenta una soluzione molto di nicchia.

Sotto sono riportate alcuni esempi di tecniche di questa categoria:

5.2.3.1 Etichettatura chimica

Traccianti chimici possono essere rilevati solo con specifici reagenti di sistemi molto sofisticati, non sono infatti rilevabili con analisi convenzionali; per tale ragione difficilmente applicabili su scala commerciale.

5.2.3.2 Etichettatura Biologica

Un marcatore biologico può essere incorporato a livelli molto elevati nelle formulazioni dei prodotti o nei rivestimenti, e può essere applicato all'interno degli imballi in maniera invisibile. Ovviamente non rilevabili dai normali metodi di analisi, richiede l'uso di kit di reagenti detti "lock e key[3]" molto specifici necessari per garantire l'autenticità.

5.2.3.3 Etichettatura tramite DNA

Anche in questo caso come nel caso di marcature biologiche si usano specifici kit di reagenti "lock e key" per l'applicazione (e verifica) sugli imballi attraverso una varietà di metodi di stampa; richiedono un'immagine a specchio per poter effettuare una ricombinazione e stabilire la parità, questa reazione è rilevabile da un apparato dedicato. Attualmente questa è tecnica è molto particolare e costosa ma l'interesse per questo settore è in forte crescita.

Lo studio del DNA quale discriminante è stato oggetto di particolare attenzione proprio quest'anno da parte del parlamento Europeo, ciò per porre fine alle frodi in campo alimentare dalla Carne equina venduta come carne bovina, sale per disgelo stradale come sale alimentare, alcol al metanolo utilizzato nei superalcolici, grasso contaminato da diossina nella produzione di alimenti per animali e scorretta etichettatura delle specie ittiche e dei prodotti del mare. Il Parlamento Europeo, ha approvato una risoluzione, non vincolante, per rivedere il funzionamento della catena di produzione e la legislazione che riguarda l'etichettatura degli alimenti, valutando la creazione di una rete europea contro la frode alimentare attraverso un uso più ampio dei test del DNA (Giuntella, 2014).

5.2.3.4 Percentuale di Isotopi

L'individuazione di isotopi quale marcatore, dà come risultato un'alta caratterizzazione della sorgente di un composto, ed è accuratamente determinato da un laser a fluorescenza o da una riso-

[3] Tecnica con cui i reagenti si legano transitoriamente all'enzima che li convertirà nei prodotti della reazione; spesso paragonato al meccanismo della chiave e della serratura. In effetti però l'interazione fra i substrati e l'enzima è di tipo più complesso e coinvolge spesso una cambiamento conformazionale dell'enzima stesso nel momento in cui i substrati, gli si legano.

nanza magnetica; possono fornire un'impronta di uno o più prodotti costituenti, o in alternativa possono essere impiegati quali marcatori unici.

Tale sistema attualmente è oggetto di grande interesse, di seguito vengono presentati alcuni studi effettuati su questa tecnica, atti ad ottenere la discriminazione della tipologia produttiva di alcune specie di pesci (allevamento vs pesca) e dell'origine geografica del latte. L'obiettivo degli studi è ovviamente migliorare l'etichettatura dei prodotti della pesca e dell'acquacoltura e conseguentemente la tracciabilità con la tutela del consumatore nel caso dei prodotti lattiero-caseari a marchio, dove l'origine del latte è stabilita da apposito disciplinare. Nel caso del latte, i peculiari meccanismi biochimici e fisiologici della lattifera fanno sì che una quota significativa dei solidi idrosolubili ingeriti con la dieta (mangime, foraggio, insilati, acqua, ecc.) venga poi secreto nel latte. Particolarmente significativo è il contributo dell'acqua di bevanda soprattutto per H^2 e O^{18} la cui abbondanza nell'ambiente segue precise regole conformi con la latitudine, l'altitudine, la distanza dal mare.

Analogamente l'abbondanza dell'isotopo C^{13} in alcune fonti vegetali (mais e canna da zucchero) risulta significativa per la discriminazione della tipologia produttiva nel caso dei prodotti della pesca. L'analisi dei rapporti tra isotopi stabili (H, C, N, O, S) mediante Spettrometria di Massa Isotopica (IRMS) ha dimostrato la potenzialità di differenziare prodotti animali quali carne, latte, burro e formaggio di diversa origine geografica e di diversa tipologia produttiva nel caso della spigola.

Tale discriminazione fa leva sul fatto che i rapporti isotopici nei prodotti di origine animale sono correlati alla composizione della dieta (impiego del mais) e posizione geografica delle risorse alimentari compresa l'acqua di bevanda. (Novelli, et al., 2011)

Ovviamente la determinazione della loro presenza può essere effettuata solo con tecniche di laboratorio.

5.2.3.5 Micro-etichette

Le Micro-etichette sono microscopiche particelle contenenti informazioni in codice per identificare unicamente ogni variante attraverso l'uso di microscopi; la loro unicità è rappresentata su piccole scaglie o filetti o su frammenti di lamine multicolore e multistrato con la "firma". Questa tec-

nica è al contrario della precedente, usata ad esempio nelle banconote, integrata in adesivi o applicata direttamente nei componenti degli imballi.

Tali micro-etichette possono supportare un elevatissimo numero d'informazioni: da 2667 caratteri in quelle da 1x1 mm a 256 mila caratteri in quelle da 12x8 mm. Costano al massimo 1 euro, hanno lunga durata e si prestano a essere utilizzate come un bollino tecnologico di certificazione, ma necessitano un elevata elaborazione e conoscenza per essere elaborate.

5.2.3.6 Schema riassuntivo delle tecniche che impiegano tecnologie Forensi

Di seguito viene riportato uno schema a carattere generale che riassume i vantaggi e svantaggi delle tecnologie forensi:

Caratteristiche	
Vantaggi	Svantaggi
Alta tecnologia e sicurezza contro la copia	Tecnologie normalmente con licenze che sono limitate a pochi utenti
Permette autenticazione positiva	Costi rilevanti
Può essere rivelato e reso visibile	Difficoltà nell'implementazione e del controllo di più mercati
	Improbabile disponibilità alle autorità o al pubblico

Tabella 3 – Schema riepilogativo dei vantaggi/svantaggi delle tecnologie Forensi

5.2.4 Segui e traccia

La tecnica "Segui e Traccia" (Track and Trace) consiste nell'assegnare, durante la produzione, un'unica identità ad ogni stock, che poi rimane per tutta la catena di distribuzione sino al consumatore, tracciandone il percorso completo. L'identità associata allo stock include normalmente tutti i

dettagli inerenti il nome del produttore, numero di serie del prodotto, data di produzione; può semplicemente assumere la forma di un unico codice in cui sono memorizzate tutte le informazioni. Quest'ultima situazione trova alcuni problemi di privacy dove i dati sono codificati e possono essere letti a distanza da dispositivi radio, una violazione comporterebbe la conoscenza di tutte le informazioni.

Si noti che tale tecnologia presenta molte funzioni distinte:

- Traccia un singolo oggetto attraverso tutta la catena di distribuzione, in ogni suo punto
- Conserva il percorso ed i passaggi eseguiti a seconda dei punti di controllo decisi a priori
- Permette l'autenticazione della data e dell'ora del pacco o dell'unità in cui sono applicati

I vantaggi più importanti possono essere apprezzati nella catena logistica, dove la trasparenza dell'inventario e dei modelli richiesti possono portare un aumento di efficienza e una diminuzione dei costi. Un altro beneficio è legato alla capacità di identificare il prodotto attraverso la distribuzione, permettendo l'eliminazione di eventuali errori nella filiera distributiva, permettendo l'aumento della velocità di richiamare prodotti fallati o con errori nella distribuzione. La capacità di controllare e autenticare tutti i prodotti attraverso tutta la filiera riduce le possibilità di contraffazione, furto, deviazione di prodotti che entrino nel sistema senza essere rilevati.

Si noti che le etichette "segui e traccia" non necessariamente sono poste a livello di pacco unitario, ma possono essere posti su un unico o alcuni pallet, avendo un beneficio logistico ma non aumentando in questo caso la sicurezza.

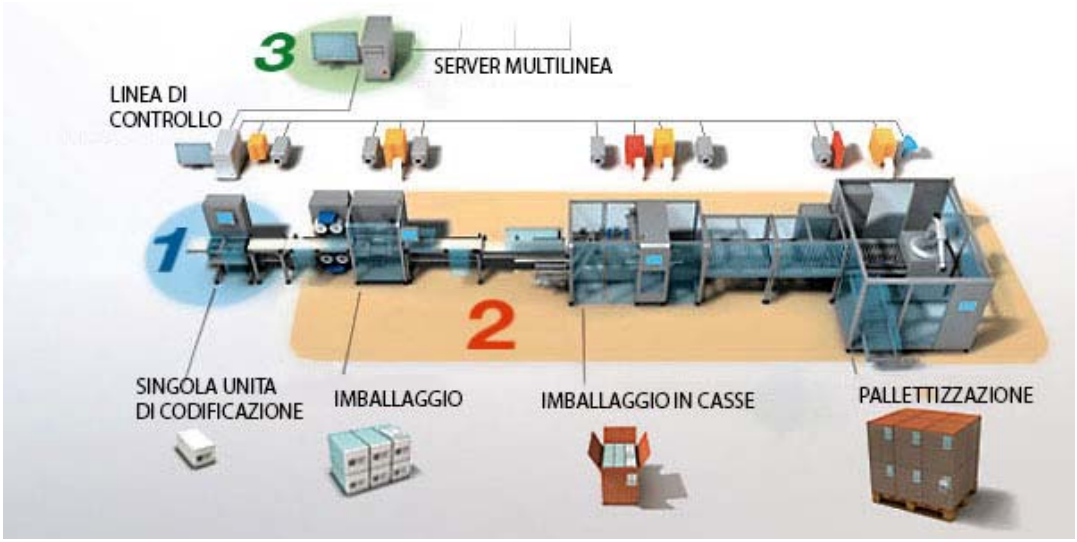


Figura 16 – Linea di preparazione agli imballaggi.

Esistono due modalità per l'incorporazione dei dati in un unico pacco per facilitare processi automatici che verranno mostrati in seguito: "Codici a barre" e RFID.

5.2.4.1 Serializzazione

La stessa etichetta "Segui e traccia" non è immune da copie o falsificazioni, ma la sua sicurezza è grande se legata a l'inclusione di serializzazioni uniche e apparentemente randomiche, numeri non-sequenziali, attribuiti sino al livello del singolo oggetto

Se la serializzazione fosse sequenziale, il livello di sicurezza sarebbe molto basso in quanto violabile mediante una semplice predizione, al contrario la serializzazione randomica usa algoritmi altamente sicuri oppure metodi di criptaggio. Pacchi sinoli potrebbero essere copiati, ma il database identifica le copie o i numeri seriali, cosi come quelli cancellati o scaduti, o che appaiono in un mercato sbagliato, o con dettagli del prodotto errato.

Qualora la serializzazione è applicata visibilmente su un pacco, questo deve essere autenticato tramite operatore telefonico o database – esempio tipico sono i software dei computer.

5.2.4.2 Codici a barre

I codici a barre sono uno tra i sistemi di verifica di un prodotto più diffusi al mondo e forse più vecchi, risalendo al 1948, questi sono un insieme di elementi grafici a contrasto elevato disposti in modo da poter essere letti da un sensore a scansione e decodificati per restituire l'informazione contenuta. Sono nati per esigenze di automatismo nel settore alimentare per poi diffondersi comunemente in tutti i settori. Il primo prodotto venduto con un codice a barre lineare risale al 1978.

I codici a barre sono di varia tipologia: lineari ad alta densità o codici a barre a due dimensioni che incorporano l'identità del prodotto a livello unità, sono scansionati e si interfacciano con il database centrale.

Tra i tipi più diffusi in Italia, senz'altro troviamo il codice EAN (European Article Number) che viene utilizzato nella grande distribuzione, seguito dal Farmacode, adottato per l'identificazione dei farmaci e delle specialità vendibili al banco nelle farmacie. Nell'ambito industriale hanno trovato grande diffusione il codice 128, il codice 39 (alfanumerico) e il 2/5 interlacciato. A seconda del tipo di codice adottato vi sono dei limiti nel ridimensionamento, nel numero e nel tipo di caratteri rappresentabili. Ad esempio, il già citato codice EAN13 può rappresentare solo dodici caratteri numerici, il codice UCC/EAN-128, utilizzato nel settore medico, può rappresentare l'intero set di caratteri ASCII.

La maggior parte dei codici ha un codice di controllo (check digit) che l'unità di lettura è in grado di ricalcolare e verificare per assicurare la corretta lettura e l'integrità dei dati.

5.2.4.2.1 Tipologie di codici a barre

I Codici a barre bidimensionali (detti anche Matrix): Sono codici a barre a due dimensioni, adatti per essere letti con apparecchi fotografici e smartphone. Le implementazioni più popolari dei codici a barre 2D sono il datamatrix 2D (Figura 18 a) ed il Qcode (Figura 18 b), che tipicamente assumono la dimensione di 1 cm quadrato o poco meno, e contiene più di un 1kb di dati con alcune ridondanze per prevenire gli errori. Composti da moduli disposti all'interno di uno schema di forma quadrata. Entrambi le tipologie di codice a barre registrano una quantità di informazioni di gran lunga superiore ai codici a barre tradizionali.

Vengono impiegati per memorizzare informazioni generalmente destinate a essere lette tramite un telefono cellulare o uno smartphone.

Il Datamatrix può contenere sino a 2.335 caratteri alfanumerici; il QR Code più di 4.296 caratteri alfanumerici. Data Matrix è considerato meno attaccabile e quindi più sicuro e favorito in contesti in cui è richiesta maggior sicurezza.

Per quanto sopra, ed almeno all'inizio dello sviluppo di questa tecnologia, il Datamatrix sembrava essere divenuto uno standard almeno nel Nord America con un vasto impiego da parte di numerose aziende. Tuttavia il Data Matrix non era stato progettato per supportare i caratteri Giapponesi Kainji mentre il QR Code lo era, essendo stato sviluppato nel 1994 dalla compagnia giapponese Denso Wave, allo scopo di tracciare i pezzi di automobili nelle fabbriche di Toyota.

Il QR code visto la maggiore versatilità nel contempo si è quindi esteso anche fuori dal Giappone divenendo il codice a barre 2D maggiormente usato.

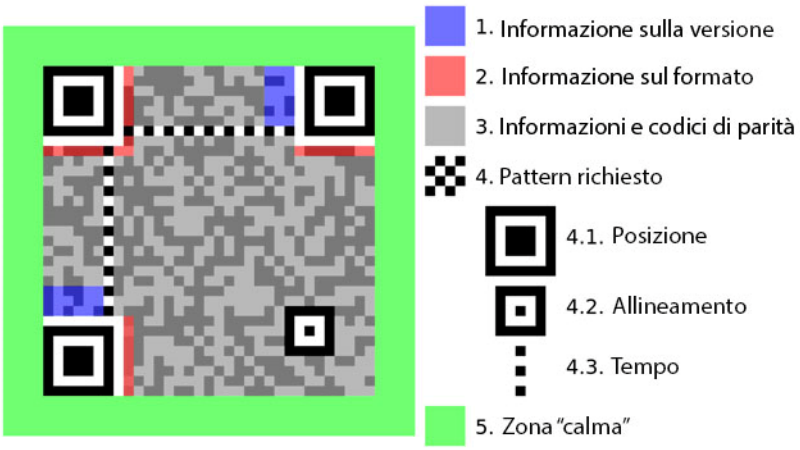


Figura 17 – Esempio di struttura QR code

Si noti che l'impiego dei codici a barre 2D può essere associato anche a codici a barre lineari qualora non vi siano problemi di spazio, detti codici sono stampabili mediante un interrogazione del database con semplice stampanti inkjet o stampanti digitali.

Esistono inoltre altre forme di codici a barre 2D: il VSCode, VIsual Code, Shotcode, Colorcode; attualmente ancora poco diffusi in Italia, ma molto usati all'estero:

- VSCode (originariamente Vericode) si pone sul mercato come codice capace di rendere le applicazioni mobili più sicure (Veritec, s.d.). Una caratteristica distintiva di VSCode è la sua elevata capacità di immagazzinamento dei dati, che gli permette di memorizzare dati di tipo biometrico, utile per le applicazioni di controllo degli accessi. Tale codice a barre offre maggiore sicurezza attraverso progetti personalizzati che utilizzano tecniche di crittografia. VSCode si presta quindi all'impiego integrato con altri supporti elettronici, come ad esempio un tag RFID o un chip intelligente.

  Come mostra la Figura 18c, VSCode presenta due bordi completi e continui, uno marcato e uno "invisibile" detto quiet, ed una zona centrale contenente i dati. Questo codice a barre è in grado di memorizzare fino a 4.151 byte, la sua dimensione è regolabile in virtù dello spazio di stampa, e presenta forma quadrata o rettangolare. Utilizzando il codice di Reed-Solomon[4], VSCode ha un'elevata percentuale (15 a 25 percento) di rilevamento e correzione degli errori. Questo gli permette di ripristinare tutti i dati codificati, anche con un danneggiamento rilevante fino al 35 per cento dell'immagine.
- Il VIsual Code (Figura 18d) è stato sviluppato per migliorare l'impiego della tecnologia HCI[5] (Human Computer Interface) nell'uso di telefoni cellulari con fotocamera.

  Questo codice a barre ha un sistema di coordinate che mappa i punti arbitrari in un piano dell'immagine e li correla a punti corrispondenti ad un piano "codice". L'algoritmo di rilevazione del movimento permette di abilitare il funzionamento del telefono cellulare come mouse ottico. VIsual Code aggiunge informazioni ad un'acquisizione inerenti l'angolo di rotazione e l'inclinazione. Ciò consente alle applicazioni che supportano interazioni in

4 Il codice Reed-Solomon è un tipo di codice lineare (ciclico) non binario di rilevazione e correzione d'errore, inventato da Irving S. Reed e Gustave Solomon. L'idea chiave dietro il codice Reed-Solomon è di vedere i dati da "proteggere" come un polinomio. L'algebra lineare dice che un numero k di punti distinti determinano univocamente un polinomio di grado al massimo k-1. Il polinomio è quindi "codificato" tramite il calcolo di diversi suoi punti e i valori di questi punti sono ciò che viene effettivamente trasmesso. Durante la trasmissione, alcuni di questi punti possono essere corrotti. Per questo motivo sono trasmessi k+n punti, con n che sono i dati aggiunti per la protezione dell'informazione. Il ricevitore analizza i punti ricevuti e determina il polinomio di grado k-1 che meglio approssima la sequenza di punti ricevuti. Finché "non troppi" punti sono ricevuti corrotti, il ricevitore può ricostruire quale fosse il polinomio originario e quindi decodificare i dati. Nel caso di un numero eccessivo di errori comunque il decodificatore ricostruisce un polinomio "simile" a quello di partenza. Quindi l'algoritmo mostra una dipendenza debole dal numero di errori, non vi è un numero di errori oltre la quale la ricostruzione fallisce, ma l'algoritmo ricostruisce sempre un polinomio verosimile, la verosimiglianza del polinomio ricostruito dipende dal numero di errori ricevuti.

5 Per Human Computer Interface – indicata anche come Interfaccia uomo macchina IUM, si intende lo strato che separa un essere umano che sta utilizzando una macchina dalla macchina stessa

tempo reale, il collegamento tra il telefono cellulare e display attivi nelle vicinanze. La capacità di immagazzinamento dati è limitato a 83 bit ma VIsualCode può funzionare sia da database portatile che come tag per accedere ad un database remoto.

- Lo Shotcode (Figura 18e) ha la caratteristica distintiva di presentare una forma rotonda. Anche questo barcode è nato per migliorare la funzione HCI, consentendo una migliore acquisizione da parte dell'utente. Lo Shotcode si presenta come un cerchio simile ad bersaglio, con al centro "un occhio di bue" e delle zone contenenti dati che lo circondano. La tecnologia legge le zone centrali misurando l'angolo e la distanza dal centro.

  ShotCode differisce dai codici a barre a matrice in quanto non contiene dati regolari ma piuttosto un numero composto di 40 bit. Questo numero viene riconosciuto in un server che contiene le informazioni relative ad un URL mappato, a questo punto il dispositivo ottenuto l'URL si connette a questo per la lettura del dato.
- Il ColorCode (Figura 18f), nacque nel 2000, da parte di Tack-Don Han presso l'università di Yonsei (Kato & Tan, 2007). Questo tag si presenta nettamente più accattivante, con una flessibilità nel design e la forma. Un ColorCode tag codifica 10 digits, quindi poco più di 1 byte, e comprende una matrice 5x5 composta da una combinazione di quattro colori diversi; nero, blu, verde e rosso.

  Le celle non presentano forma rigorosamente quadrata ma possono presentare forme diverse quali cerchi, ovali o poligoni (attualmente esistono un'immensa variante di opzioni, pur non essendo ancora molto diffuso al piccolo consumatore italiano)

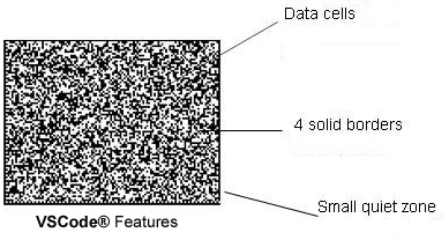
  ColorCode utilizza delle celle di riferimento, che garantiscono un colore standard e una tonalità scelta per distinguere correttamente ogni cella riprodotta. Il valore del colore e tonalità di ciascuna cella è riportato in una area "dati" e viene determinato rispetto al valore del colore standard registrato in una cella di riferimento. ColorCode include un controllo di errore di parità che rileva qualsiasi colore errato, riconoscendolo ed effettuandone la correzione.

  Le uniche operazioni effettuate su ogni colonna e riga sono il controllo di parità; il codificatore quindi converte ogni cella (tenendo conto della rispettiva riga e colonna) nel corri-

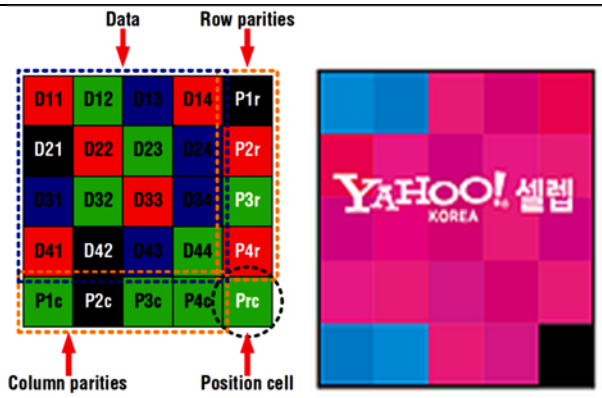
spondente valore di colore della zona di parità del simbolo (vedi Figura 18f – immagine di sinistra).

Un errore di lettura del colore da parte del codificatore viene rilevato dalla non corrispondenza nell'area di parità. La decodifica del ColorCode richiede la visibilità solo del 40 per cento di una singola cella. Ciò consente l'incorporazione di questo codice a barre in un logo aziendale o in qualsivoglia grafica, lasciando infatti il 60% dello spazio al brand dell'azienda.

Un'azienda giapponese "ColorZip" (Colorzip, s.d.) ha poi introdotto un nuovo tipo di codice a barre ColorCode che integra più codici a barre e più simboli (vedi Figura 18 f – immagine di destra).

a) Data Matrix	b) QR code
	
c) VScode	d) VIsualCode

e) Shotcode



f) Colorcode

Figura 18 – Esempi di codici a barre bidimensionali

5.2.4.3 Identità in Radio Frequenza (Radio Frequency Identity) – RFID

Radio frequency identification (RFID) indica una tecnologia che, sfruttando la radiofrequenza, permette l'identificazione univoca, di un oggetto. Alla base degli RFID ci sono i tag, anche detti transponder, ossia dei chip con memoria ed annessa antenna.

Il tipo di RFID più usato per l'anti-contraffazione opera semplicemente attraverso la codifica di un numero seriale nel microchip, collegando quest'ultimo all'antenna radio, e ponendo il tutto in un imballo di un prodotto.

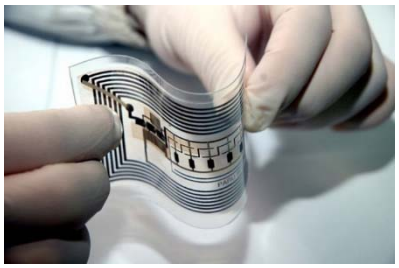


Figura 19 – Esempi di RFID

Il tag comunica il suo identificativo ad un "reader" alias un dispositivo in grado di effettuare un riconoscimento, questo a sua volta si interfaccia con un server che effettua un interrogazione nei

database in possesso e restituisce una risposta al reader, a questo punto il reader invierà le informazioni necessarie o richieste al tag.

Il tag ovviamente possiede una sua memoria interna tipo EEPROM, tale tipo di memoria identifica la modalità d'uso del tag e ne condiziona l'impiego.

La radiofrequenza usata determina lo spettro e la sensibilità, ma non l'applicazione scelta ovviamente. Alcuni sistemi sono capaci di catturare più informazioni da impiegarsi anche contemporaneamente, ma vi sono delle limitazioni legate all'orientamento dei tag e all'assorbimento dei segnali radio nei liquidi o fogli di alluminio. I vantaggi di questa tecnologia sono numerosi di seguito verranno enunciati i principali:

- Il pieno automatismo e controllo della filiera distributiva.
- I dati possono essere scambiati in maniera bidirezionale fra il lettore ed il tag
- Capacità di memorizzazione potenzialmente elevata, legata ovviamente alla scelta dei tag
- Campo fisico di lettura ampio da pochi centimetri ad alcuni metri
- Sistemi di sicurezza sui tag (password e/o crittografia)

I costi dei tag RFID rimangono elevati per l'impiego di pacchi singoli, anche se consente l'impiego in una vastissima varietà di applicazione e possibilità di verifica.

Ci sono principalmente tre tipi di "tag" RFID, passivo e attivo e semi-passivo, di seguito alcune caratteristiche peculiari.

5.2.4.3.1 Tag passivo

Il tag passivo, non è dotato di una sorgente di alimentazione indipendente; il tag prende la potenza necessaria dalle onde elettromagnetiche trasmesse dal lettore di tag. Le onde elettromagnetiche inducono una corrente all'interno dell'antenna attraverso il tag, fornendo un piccolo impulso, necessario all'invio di un segnale al lettore RFID attraverso le onde elettromagnetiche. Tale tag passivo lavora al massimo sino a una distanza di 6 m. e pertanto una capacità molto limitata.

I tag passivi hanno, anche solo la capacità di avere una limitata capacità computazionale, che rende impossibile l'utilizzo di crittografia o protocolli di sicurezza complessi.

5.2.4.3.2 Tag attivi

Tag attivi hanno una sorgente di alimentazione interna, di solito una batteria al litio, che alimenta l'antenna con un elevato range di comunicazione (dieci o più metri) e il microchip interno con una memoria RAM dell'ordine di qualche KB; ciò consente l'uso della crittografia e algoritmi di encryption and decryption.

I tag passivi sono più economici, quelli attivi dieci volte di più.

L'infrastruttura richiesta dal RFID è minima. Un Tag RFID deve essere introdotto all'interno dei prodotti e/o confezioni, ed essere registrato in un database di un computer. Sarà sufficiente per la verifica dell'autenticità che un lettore RFID legga il tag contenuto all'interno delle confezioni, ciò senza che il pacco debba essere aperto o senza che sia necessario un contatto visivo. (Johnson, et al., 2011)

5.2.4.3.3 Tag Semi Passivi

I tag semi-passivi sono una tipologia intermedia fra le soluzioni presentate sopra, hanno una batteria interna che permette loro di eseguire alcune operazioni (controllo potenza, operazioni logiche avanzate); possono avviare una comunicazione con il reader oppure, nella maggior parte dei casi, essere silenti in attesa di un segnale.

5.2.4.3.4 Tag – Modalità di funzionamento della memoria interna

La RAM dei tag determina e condiziona il tipo di impiego ed ovviamente la quantità di memoria contenuta, definiscono quindi la modalità di utilizzo:

5.2.4.3.4.1 Read Only

Il tag può essere interrogato in sola lettura. La capacità di memoria è minima. I tag passivi sono di solito read only

5.2.4.3.4.2 Read & Write

La memoria del tag può essere sia letta che scritta. La dimensione è dell'ordine di qualche kB ed il loro costo è maggiore.

5.2.4.3.4.3 Write Once – Read Many

E' consentito scrivere all'interno del tag una sola volta, dopodiché la sua memoria è accessibile solo in lettura.

5.2.4.3.5 Tag - Classificazione

Una classificazione ufficiale di tale tecnologia non c'è, ma la EPCGlobal Network, un'organizzazione dedita anche allo studio di applicazioni RFID, ha sviluppato una classificazione dei tag in base alle loro caratteristiche, che per completezza si riporta di seguito:

Classe	Caratteristiche
Classe 0	Tag passivi Read-only
Classe I	Tag passivi con memoria utente e accesso con password
Classe II	Tag passivi con funzionalità aggiuntive (memoria Secondaria, crittografia)
Classe III	Tag semi-passivi
Classe IV	Tag attivi

Tabella 4 – Classificazione dei tag in virtù della Classe

La frequenza di impiego dei tag, come detto in precedenza, determina il raggio d'azione e l'uso, di seguito uno schema riassuntivo:

Intervallo	Raggio	Uso
125-134 kHz (LF)	Corto	Identificazione, sistema accezione autovettura
13,533 – 13,567 MHz (HF)	Corto/medio	Smart card, biblioteche
860 – 960 MHz (UHF)	Medio/Lungo	Monitoraggio della catena di ap-provvigionamento

2400 – 2483 GHz (VHF)	Lungo	Telepass

Tabella 5 – Classificazione dei tag in virtù della frequenza

5.2.4.3.6 Reader

E' il dispositivo preposto sia alla lettura del tag che alla sua scrittura, ove questo sia possibile. Il reader (anche "interrogator" o "lettore") si interfaccia anche con il database del sistema per recuperare le informazioni sul prodotto identificato dal tag.

La struttura base del reader è così costituito:

- Il Controller che gestisce la comunicazione con l'host, traducendo i comandi interni in segnali captabili dalle antenne dei tag.
- Network Interface: insieme di porte di comunicazione che permettono di collegare il reader all'host.
- Apparato ricetrasmettitore: permette di interfacciarsi in radiofrequenza con le antenne secondo una banda di frequenza prestabilita.

La potenza di trasmissione del reader è legata alla potenza effettivamente trasmissibile via radio. La limitazione posta è legato alle normative vigenti nel paese di impiego in genere, comunque è possibile affermare che va da alcune **centinaia di mW** fino a oltre **4 W**.

Lo spazio in cui reader e tag possono comunicare è definito zona di interrogazione o "range".

La comunicazione reader - tag deve essere libera da interferenze esterne che potrebbero alterare o anche annullare la connettività.

All'interno di un range possono esistere più tag ma anche più reader. Per evitare sovrapposizioni di comunicazioni, occorre usare degli algoritmi di *anti-collisione*.

Si acquisiscono i codici identificativi di tutti i tag presenti nel sistema e si fa in modo di organizzarli in maniera selettiva.

A seconda della presenza di tag e reader in un ambiente, è possibile definire quattro tipologie di sistemi:

- **One-to-Many**

Ossia un solo lettore per più tag (un piccolo negozio al dettaglio)

- **One-to-One**

Un solo reader per un solo tag (la chiave di accensione di un'auto)

- **Many-to-One**

Più reader per un solo tag (Telepass).

- **Many-to-Many**

Più reader per più tag. (Biblioteche, magazzini, grandi negozi)

5.2.4.3.7 Applicazioni d'uso

Magazzini e punti vendita: Ogni prodotto può essere identificato univocamente da un tag, permettendo un miglior controllo delle merci e dei loro spostamenti.

Trasporti: i tag possono essere applicati anche sui mezzi di trasporto così come sul conducente. Altre applicazioni sono tag sui bagagli negli aeroporti o sulle chiavi di accensione delle auto

Tracciamento pratiche: tale applicazione non è diffusa ma consentirebbe uno snellimento della burocrazia aiutando ad automatizzare la ricerca in archivi cartacei e a gestire meglio gli spostamenti delle pratiche dentro gli uffici.

Biblioteche: i tag sono posti su libri, video, CD, consentono un controllo ed una gestione più accurata dei beni, sostituendo la lamina metallica che ne controlla solo l'eventuale uscita dalla biblioteca

Antitaccheggio: interagiscono con una barriera posta all'uscita di un magazzino o di un negozio accertando che nessuna marce abbia varcato la soglia in maniera illecita.

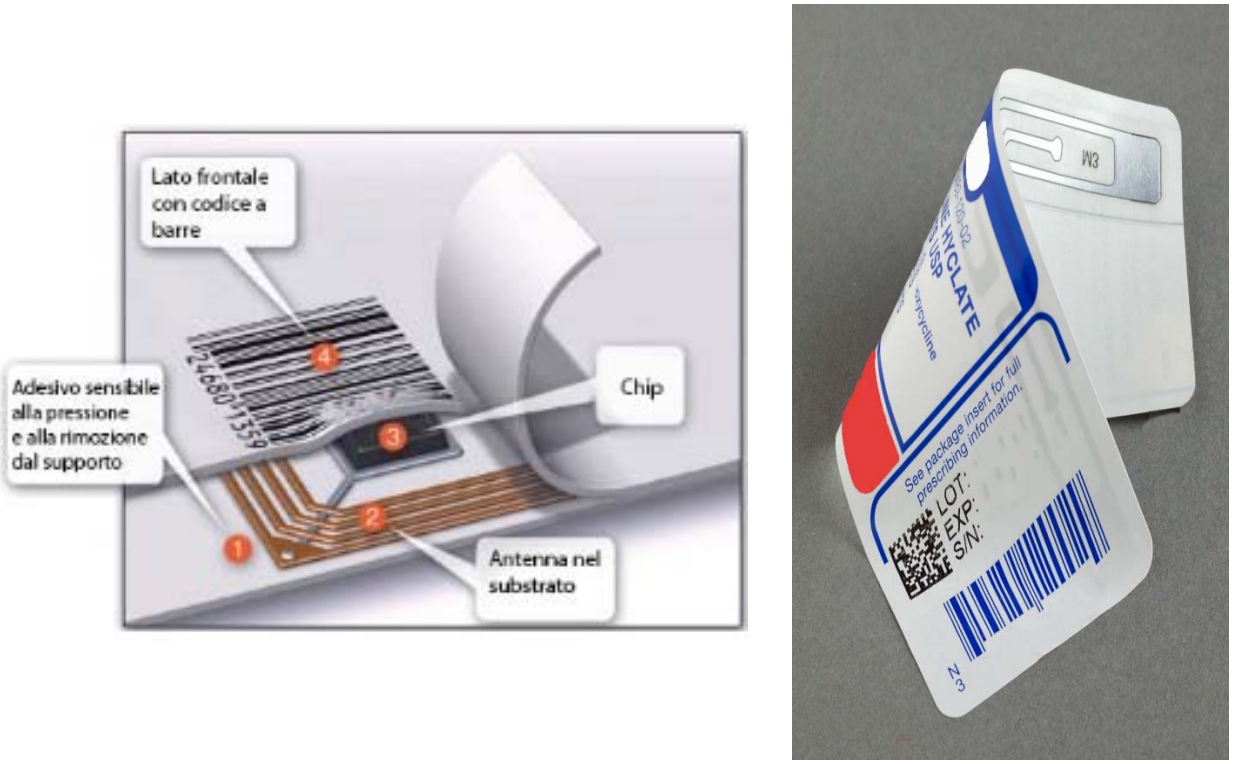


Figura 20 - Esempi di RFID applicati ad etichette

5.2.4.3.8 Il problema della Privacy

Gli RFID risultano molto applicati e relativamente economici, ogni individuo però in possesso di prodotti "taggati" rischia di essere anch'esso "taggato". I tag permetto di sapere dove si trova una persona in un dato momento (se è in prossimità di un reader), quali sono le sue abitudini (cosa ha comprato). In pratica è possibile tracciare una persona e controllarla come se avesse un occhio piazzato sopra di essa.

I sistemi RFID, originariamente, erano sistemi promiscui, cioè rispondevano a qualsiasi lettore che li interrogasse.

Per quanto sopra si è verificata la possibilità che la tecnologia potesse essere utilizzata per violare la privacy del possessore degli oggetti "taggati"

In origine non vi erano grosse preoccupazioni da questo punto di vista. Ma la possibilità di crescita dei sistemi RFID ha posto tale problematica al centro dell'attenzione.

Per fare in modo che la privacy di una persona non venga lesa, sono stati inseriti sistemi di sicurezza, al fine di garantire che solo reader e solo personale autorizzati possano avere accesso alle informazioni contenute nei tag e nei database.

Ciò non basta. Esistono altri problemi legati agli attacchi che alcuni individui possono effettuare sui tag:

5.2.4.3.8.1 Contraffazione

Falsificare o imitare un tag. Problema legato principalmente ai transponder

5.2.4.3.8.2 Replay

Una trasmissione valida tra tag e reader viene ripetuta da un avversario che intercetta i dati e li ritrasmette.

5.2.4.3.8.3 Eavesdropping – "Origliare"

Capacità di "origliare" una trasmissione tra tag e reader. Spesso alla base del replay vi sono essenzialmente due grandi problemi: il tracciamento clandestino e l'immagazzinamento.

Il primo è definibile come la possibilità di seguire il segnale emesso da un tag e di collegarlo al suo possessore. Il secondo consiste nel riconoscimento di oggetti all'interno di uno magazzino, ed è ottenibile tramite la lettura dei tag posti sugli oggetti.

Il problema diventa sempre più serio quando le informazioni sui tag sono facilmente collegabili ai dati personali delle persone che li posseggono

La duplicazione di dispositivi non protetti è piuttosto semplice e richiede solo lo scanning del tag e poi la duplicazione.

Una soluzione per ridurre i rischi è quella di crittografare i dati nei tag. L'approccio più generico e sicuro, però, è l'uso di protocolli standard di autenticazione già largamente usati nelle reti o nelle smart cards. Tuttavia gran parte delle aziende preferiscono usare dei loro sistemi di autenticazione e non quelli consentiti dagli standard.

5.2.4.4 Schema riassuntivo delle tecniche di Serializzazione/Segui e Traccia

La serializzazione di un unico pacco ha il potenziale di essere una soluzione robusta alle frodi e deterrente, i costi risultano non proibitivi ma alcune soluzioni ancora troppo alti. I codici a barre sono largamente usati ed economicissimi, ma non garantiscono un controllo totale. Gli RFID forniscono un controllo totale ma non sono ancora cosi robusti, e necessitano ulteriori definizioni degli standard, sono ancora vulnerabili ad alterazioni invisibili o manomissioni.

In generale è possibile riassumere che tale tecnologia ha i seguenti vantaggi e svantaggi:

Caratteristiche Serializzazione/Segui e traccia	
Vantaggi	Svantaggi
Alta tecnologia e sicurezza contro la copia	Costi significanti per l'implementazione e il monitoraggio
Autenticazione remota, via telefono o internet	Difficoltà di implementazione delle tecnologie su più mercati
Accessibilità alle autorità investigative senza compromissione	Vulnerabilità ad attacchi hacker
Elimina la dispersione degli errori	Etichette danneggiate sono illeggibili
Facilità di richiamo dei prodotti difettosi	Robustezza dei RFID non provata
Potrebbe combattere i furti e le frodi	Necessari armonizzazioni degli standard
	Non accessibile al pubblico
	Problemi di privacy legati a letture remote

Tabella 6 – Schema riepilogativo dei vantaggi/svantaggi delle tecnologie invisibili

6 Principi di Biometria

6.1 Introduzione

Il termine biometria deriva dalle parole greche "*bios*" e "*metron*". In un contesto legato alla gestione dell'identità, il termine biometria è contemporaneamente associato a due significati: usualmente indica il processo di misurazione e analisi di caratteristiche fisiche e comportamentali degli esseri umani, realizzata per il riconoscimento degli individui; ma può essere anche usata per valutare le caratteristiche medesime, a seconda del contesto d'interesse.

L'uso di specifici tratti per il riconoscimento di persone è il metodo più impiegato da migliaia di anni dagli esseri umani per riconoscersi, la biometria pertanto pur non avendo la connotazione che ha oggi, ha un origine antica.

Il primo vero sistema di riconoscimento biometrico fu implementato da Bertillon, capo della divisione di identificazione criminale del dipartimento di polizia parigina; egli usò, per le analisi indirizzate all'identificazione dei criminali, alcune caratteristiche fisiche (altezza, peso, lunghezza delle braccia, delle gambe).

Nel tardo 1800, l'utilizzo delle misure del corpo descritte poc'anzi fu sostituita dalla valutazione delle impronte digitali.

L'uso delle impronte per l'identificazione dei criminali divenne in poco tempo un sistema consolidato.

Durante l'ultimo secolo, infatti, il dipartimento di giustizia degli Stati Uniti adottò le impronte digitali come uno dei principali sistemi di riconoscimento dei criminali; il numero delle impronte memorizzato in un database ebbe un notevole incremento con la generazione di un sistema di identificazione automatico di impronte noto tutt'ora con nome di AFIS.

Sebbene la biometria sia emersa per il suo intenso impiego in ambito legale e delle applicazioni forensi, è attualmente la branca più promettente per il riconoscimento in ambito civile (es. accessi ad edifici, caveau banca, aree militari sensibili, ecc.) essa pertanto non è connessa all'ambito legale in maniera restrittiva.

Esempi di tratti fisici che sono stati studiati al fine di avere un riconoscimento dell'individuo sono: il viso, le impronte digitali, l'occhio, la retina, la geometria della mano e del palmo, forma dell'orecchio, DNA, pattern delle vene.

Vi sono poi tutta una serie di caratteristiche comportamentali che pur non essendo strettamente biometriche sono fortemente legate a queste, come ad esempio la firma, il tratto della scrittura, la pressione dei tasti (nelle vecchie macchine dattilografiche), il movimento delle labbra (Faraj & Bigun, 2007). La voce è considerata sia una caratteristica fisica che comportamentale, poiché legata alla conformazione anatomica del tratto oro-faringeo della persona con conseguenti caratteristiche peculiari dello stesso, sia perché soggetto a variazioni legate allo stato psico/fisico dell'individuo.

Molte delle caratteristiche biometriche o comportamentali sin qui citate sono uniche e consentono l'identificazione di un individuo, permettendo tra l'altro l'impiego in tecnologie come documenti d'identità digitale e le chiavi digitali.

Il vantaggio nell'uso di sistemi biometrici è il fatto che i dati ad essi connessi non possono essere dimenticati, persi, rubati e copiati (almeno non con tecniche semplici), come potrebbe essere per i sistemi tradizionali.

6.1.1 Parametri Biometrici

Ogni tecnologia ha i suoi vantaggi e le sue limitazioni ed una sola caratteristica potrebbe non essere sufficiente ad incontrare tutte le esigenze biometriche delle varie applicazioni.

Specificatamente, una data caratteristica biometrica può essere descritta in accordo ai seguenti parametri:

- Universalità: ogni persona deve avere il carattere biometrico considerato
- Distinguibilità: a seconda del sistema biometrico prescelto deve essere possibile distinguere due persone
- Invarianza: un tratto biometrico o al massimo l'informazione che può essere estratta da essa, deve essere invariante nel tempo

Inoltre, la capacità di un dato sistema di essere usato in una specifica applicazione è tipicamente misurata nel rispetto delle seguenti specifiche:

- Prestazione: il tempo necessario all'elaborazione del processo biometrico e l'accuratezza del processo di riconoscimento può essere archiviato e deve soddisfare i requisiti dati dai fattori operazionali e ambientali dell'applicazione considerata.
- Accettabilità: questa specifica si riferisce alla disponibilità di un individuo ad accettare che il proprio tratto biometrico sia utilizzato per una specifica applicazione.
- Incontraffabilità: la specifica biometrica desiderata deve essere difficile da copiare, contraffare, o sottrarre; ciò rende l'applicazione più sicura da metodi fraudolenti.

6.1.2 Struttura di un sistema di riconoscimento biometrico

I sistemi biometrici sono essenzialmente delle applicazioni che riconoscono determinati modelli ("pattern"), dove i modelli considerati sono dati dalle caratteristiche psicofisiche o comportamentali; viene di seguito schematizzato uno schema classico di un sistema di riconoscimento dei pattern

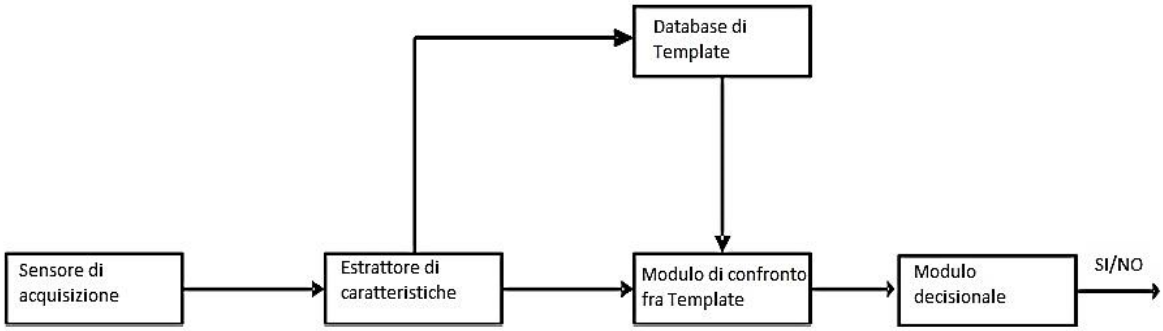


Figura 21 – Struttura di un sistema di riconoscimento biometrico

Il primo modulo è il sensore di acquisizione che cattura le caratteristiche biometriche. Questo modulo deve dapprima acquisire le caratteristiche degli utenti del sistema mediante un dato algoritmo valutando la qualità di dette caratteristiche; se la qualità è bassa l'ingresso deve essere reacquisito.

Il secondo modulo è l'estrattore di caratteristiche. Questo modulo effettua un'elaborazione dei dati acquisiti con l'obiettivo di estrarre un set di caratteristiche importanti e discriminanti (per esempio nel caso delle impronte digitali le minuzie).

La generazione del set di caratteri è comunemente chiamata "template biometrico", considerata come una nuova rappresentazione di una data caratteristica. Il template utilizzato dovrebbe essere generato in modo da contenere le informazioni biometriche che siano utili al riconoscimento individuale. I template estratti da dati biometrici di un dato utente, ottenuti attraverso diverse acquisizioni, devono mostrare una variabilità molto bassa. Template di diversi utenti dovranno essere abbastanza diversi, al fine di poter distinguere il singolo soggetto. I template di un utente, estratti, possono essere memorizzati in un apposito database, cioè inviati al modulo detto "Database di template", oppure inviati ad un modulo che effettua un confronto e valuta il grado di somiglianza rispetto ad un altro template di riferimento.

La misura ottenuta, generalmente indicata come valore di somiglianza ("similarity score"), viene in seguito inviata ad un apposito modulo che effettua la decisione circa la probabilità che il campione appartenga alla persona in esame o se al contrario appartenga ad un impostore.

I template generati dal modulo di estrazione sono memorizzati e inviati al modulo di confronto fra template, ciò è legato ovviamente allo schema di funzionamento del sistema; alcuni moduli potrebbero infatti avere ordine diverso.

6.2 Fasi di riconoscimento di un sistema biometrico

Sistemi biometrici di autenticazione effettuano sempre due procedimenti: registrazione ("enrollment") e autenticazione.

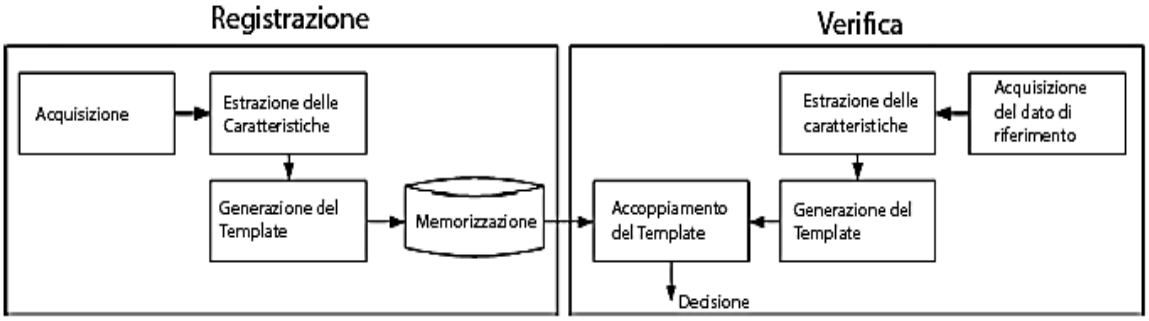


Figura 22 – Composizione di un sistema biometrico

6.2.1 Registrazione

Durante la prima fase i dati biometrici sono catturati dal soggetto e se ne verificano le qualità; vengono estratte solo le informazioni rilevanti e viene conseguentemente generato un template, tali informazioni vengono memorizzate in un database e successivamente inviate al sistema di verifica.

6.2.2 Verifica

Successivamente vi è un operazione di verifica; partendo dal presupposto che il soggetto che necessita di essere identificato è in possesso di alcuni modelli di identificazione memorizzati nel sistema (per esempio carta d'identità o username) ed una data caratteristica biometrica; il sistema estrae alcune caratteristiche dai dati acquisiti e confronta i dati corrispondenti ai modelli di identificazione, archiviati nel database del sistema, con quelli in ingresso oggetto dell'analisi.

Questa modalità è tipicamente utilizzata per il cosiddetto "riconoscimento positivo", dove lo scopo è quello di evitare che più persone possano utilizzare la stessa identità. In tale modalità il confronto è fra il singolo tratto in ingresso al sistema e quello memorizzato nel database centrale centralizzato alias un confronto 1:1.

Il problema della verifica può quindi essere analiticamente rappresentato come segue:

Data una rappresentazione biometrica di query[6] F_Q ed un identità I; deve essere determinato che F_Q è un dato biometrico estratto da I

Tale processo è effettuato comparando F_Q con un template biometrico F_T registrato in un database durante la fase di registrazione dell'identità I.

Se il valore ottenuto all'uscita del template del modulo di accoppiamento, indicato come (F_Q, FT) è più alto di una soglia t predeterminata, allora la caratteristica F_Q è considerata appartenere alla persona con identità I. Al contrario se si ha (F_Q, FT) < t allora la query ha come origine dati contraffatti ed è rifiutata dal sistema.

Va considerato che molti template durante la fase di accoppiamento e confronto presentano soglie vicine ma producono distanze dissimili, vediamo nel dettaglio cosa si intende:

[6] Query: indica l'interrogazione da parte di un utente di un database, strutturato tipicamente secondo il modello relazionale, per compiere determinate operazioni sui dati quali selezione, inserimento, cancellazione dati, aggiornamento ecc.

Si consideri che più le due funzioni F_Q, FT sono simili più piccola sarà la distanza $d(F_Q, FT)$.

Avremo $d(F_Q, FT) \leq t_d$ se un utente è riconosciuto dal sistema come reale possessore dell'identità, oppure $d(F_Q, FT) > t_d$ se il sistema rifiuta l'utente; pertanto è possibile affermare che t_d è una soglia impiegata per valutare una decisione che il sistema deve effettuare.

6.2.3 Autenticazione

Il sistema acquisisce un campione biometrico del soggetto, estrae alcune caratteristiche da una misura effettuata nelle precedenti fasi e ricerca degli accoppiamenti in tutto il database.

Quando il sistema di autenticazione opera in modalità di identificazione vengono effettuati dei confronti 1:n.

Un'identificazione, a differenza del processo di verifica, è normalmente sviluppata su applicazioni di "riconoscimento con esito negativo", cioè è necessario che il sistema verifichi anche se l'individuo è chi "dichiara" di essere. Lo scopo di un "riconoscimento al negativo" è quello di evitare che una persona possa assumere più identità.

Un processo di identificazione può essere comunque sviluppato in un conteso di "riconoscimento positivo", ove cioè non è necessaria la verifica dell'identità bensì il solo riconoscimento.

Si noti che il "riconoscimento positivo" ha un uso più comune in quanto si esplica ad esempio mediante l'utilizzo di password mentre quello al "negativo" si stabilisce esclusivamente mediante la biometria.

E' chiaro che effettuando un elevato numero di confronti i tempi di elaborazione si allungano; per ovviare a tale problematica viene di solito impiegato un sistema scalare. Tale sistema tipicamente analizza e rileva solo le caratteristiche peculiari.

Informazioni riguardanti genere, anni, cicatrici, tatuaggi ecc., sono presi in considerazione nello sviluppo dei sistemi di riconoscimento; tali peculiarità non permettono, almeno da sole, di individuare univocamente l'individuo, ma possono essere discriminati se associate ad altri elementi; queste caratteristiche sono quindi definite "caratteristiche biometriche leggere".

6.3 Rendimento di un sistema biometrico

La qualità di un sistema di riconoscimento può essere valutata sulla base dell'accettabilità, delle circostanze e delle caratteristiche intrinseche del dato biometrico.

Il sistema dovrebbe essere in grado di gestire le eccezioni che possono verificarsi quando un utente non vuole utilizzare un sistema biometrico o quando non è possibile rilevare tali dati, anche per condizioni transitorie.

In uno scenario in cui è concesso l'uso di accessi fisiologici, la sicurezza inerte dei sistemi biometrici diventa di estrema importanza al fine di evitare truffe o ingressi non autorizzati al sistema.

Altro fattore da considerare è il parametro della "velocità computazionale", legato al sistema che effettua la decisione, pertanto tale sistema deve essere dimensionato alle esigenze di utilizzo e rapportato agli altri moduli.

Il sistema automatico di verifica deve in primis essere **accurato**, deve riconoscere tutte le persone autorizzate e al contrario rendere minima la possibilità che possano accedere al sistema persone prive di autorizzazione.

Vi è un'ulteriore considerazione da fare, qualunque caratteristica biometrica di un individuo presenta una certa variabilità detta intra-utente. Anche per i tratti che sono tempo-invarianti (come gli occhi per esempio), vi è nella generazione di un template una subordinazione tra i tratti biometrici ed i moduli di acquisizione (rumore, sensibilità, posizione, ecc.). Questa interazione è necessariamente differente quando si effettuano due acquisizioni, ciò è dovuto per esempio a cambiamenti fisiologici o comportamentali di un determinato utente, oppure a variazioni legate alle condizioni ambientali, va pertanto introdotto un elemento di variabilità anche qualora la caratteristica biometrica non vari con il tempo.

6.3.1 Tipologie di errore

I sistemi biometrici di verifica possono presentare due tipologie di errore:

- Errore di tipo I: errore nella fase di misurazione biometrica di due persone differenti acquisite come se fossero la medesima, tipicamente dovuto a una significante somiglianza inter-utente; in questo caso si parla comunemente di "falso accoppiamento" (false-match) e quando ciò avviene il sistema commette una "falsa accettazione".

- Errore di tipo II: errore di misurazione di una caratteristica biometrica della stessa persona che acquisita viene poi rilevata in modi diversi, come se gli individui fossero due; tipicamente ciò è dovuto ad una grande variabilità inter-utente. Comunemente si parla di "falso non-accoppiamento" (false non-matching) e quando ciò avviene il sistema commette un "falso rifiuto" (false reject).

6.3.2 Metriche per la valutazione del rendimento

Le metriche più comunemente usate per definire il rendimento di un sistema di riconoscimento di una caratteristica biometrica sono:

- Falsa soglia di rifiuto – FRR (False Rejection Rate): definita come il rapporto fra i falsi rifiuti stimati ed il numero totale di accessi al sistema effettuati da un individuo autorizzato ad accedere al sistema tramite riconoscimento dell'identità
- Falsa soglia di accettazione – FAR (False Acceptance Rate): definita come il rapporto tra le false accettazioni ed il numero totale di tentativi di accesso al sistema tramite identificazione di identità di utenti autorizzati ed accessi effettuati da un impostore.

Ovviamente vi è un compromesso nella scelta di un sistema in funzione dei due parametri FRR e FAR; sia FRR che FAR possono essere espresse come una funzione di una soglia t del sistema.

Se la soglia t decresce, il sistema può essere più tollerante alle variazioni e al rumore in ingresso, producendo così una peggiore qualità in termini di FAR a differenza del parametro FRR.

Al contrario se t viene posta crescente, sarà migliore la qualità del parametro FRR e peggiore la qualità del parametro FAR.

Il rendimento del sistema in tutti i punti in cui opera è normalmente descritto da una singola funzione, essa mostra come opposti siano nell'andamento FAR e FRR per i valori della soglia t.

Questa funzione rappresenta la "caratteristica operativa ricevuta" ed è detta ROC, mostrata nella figura sotto riportata.

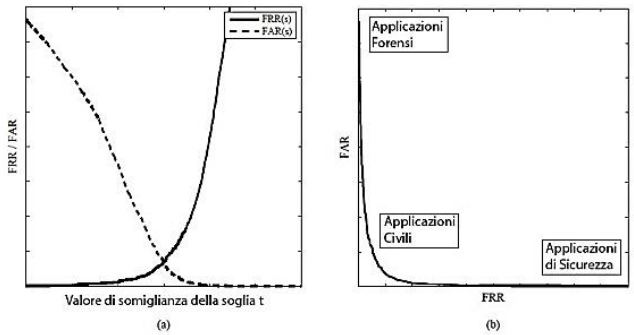


Figura 23 – Metriche del rendimento di un sistema biometrico.

(a): FRR e FAR rispetto a t; (b): curva ROC

In particolari applicazioni ove è richiesto un alto valore di sicurezza, l'obiettivo principale è quello di proteggere il sistema da un ingresso indesiderato di un malintenzionato, pertanto è auspicabile avere un alto valore di FRR ed accettare un basso valore di FAR. Applicazioni forensi, legate ad esempio alla sola identificazione di un criminale richiedono un basso FRR ed un alto valore di FAR, pertanto è preferibile "perdere" l'identificazione di un criminale a dispetto di un gran numero di dati non corretti. Le applicazioni civili (per esempio accesso presso edifici) lavorano con un punto operativo che varia fra i due estremi dove FAR e FRR assumono lo stesso valore, tale valore è detto EER – valore con uguale errore.

Il punto di intersezione fra le funzioni FAR e FRR è comunemente chiamato EER ed è considerato come la misura più rappresentativa della qualità di un sistema biometrico: più basso è il valore di EER, più alta è l'accuratezza del sistema.

L'accuratezza del sistema può essere valutata da altri due parametri FTC –fallimento in acquisizione e FTE – fallimento in registrazione. Il parametro FTC è applicabile solo quando l'apparato ha un sistema automatico di acquisizione e mostra una percentuale di tempo di insuccesso nell'acquisizione di una caratteristica biometrica in ingresso, ciò è legato all'incapacità del dispositivo di avere in ingresso un segnale di qualità sufficiente. Il FTE, mostra la percentuale di utenti che non sono in grado di essere registrati nel sistema di riconoscimento; errori FTE avvengono tipicamente quando un sistema in fase di registrazione rifiuta ingressi di bassa qualità. Vi è una correlazione fra FTE e l'accuratezza delle misurazione (FRR e FAR): se solamente i template di buo-

na qualità possono essere memorizzati nel sistema, allora l'accuratezza è ovviamente maggiore. Tutte le metriche sopra menzionate costituiscono le specifiche di un sistema biometrico e devono essere riportate durante la valutazione del rendimento.

6.4 Applicazioni dei sistemi biometrici

I sistemi di riconoscimento biometrico sono oggi impiegati in molti settori, con lo scopo di effettuare la verifica o l'identificazione automatica di una persona.

Le applicazioni in cui è richiesto l'uso di sistemi biometrici sono principalmente di tre tipi:

- *Applicazioni commerciali:* accesso remoto su internet o su applicazione di altri computer, sicurezza dei dati, controllo fisico di ingressi ad edifici, gestione medica, studi a distanza, ecc.
- *Applicazioni governative:* carte d'identità, patenti (altri stati), sicurezza sociale, controlli alle frontiere.
- *Applicazioni forensi:* identificazione di corpi, investigazioni su criminali, determinazione di parentela, ricerca di bambini scomparsi.

Nonostante il grande interesse mostrato in relazione alle tecniche biometriche, ed il crescente impiego nelle applicazioni pratiche che sono state sviluppate, i possibili impieghi e sviluppi sono ancora notevoli rispetto a quanto sarebbe possibile ottenere.

I limiti ancora presenti sono di diversa natura, per fare un esempio possiamo prendere in esame la **scalabilità**, legata alle tecnologie e agli impieghi del sistema, per la quale va tenuto conto delle dimensioni del database che rispetto ad alcuni anni fa risulta essersi ridimensionato viste le dimensioni raggiunte dalle memorie di massa che però vanno considerate come fattore limitante.

Va inoltre aggiunto che non risulta esservi criticità nei sistemi di verifica che richiedono l'autenticazione mediante un accoppiamento ("matching") di una query biometrica ed un singolo template registrato, questo elemento diventa di elevatissima importanza quando si tratta di sistemi di identificazione in cui i dati biometrici in ingresso devono essere confrontati in sequenza con tutti i modelli registrati nel sistema. Il processo necessità di tempo per effettuare alcune operazioni in maniera lineare con la dimensione del database e diviene rapidamente insostenibile quando la di-

mensione dei soggetti da registrare è nell'ordine del milione, condizione possibile in ambito governativo e forense.

Questa problematica è stata in realtà in parte risolta da qualche anno mediante lo sviluppo di processi come il filtraggio o l'indicizzazione; il database viene prima analizzato sulla base delle informazioni accessorie connesse all'oggetto, oppure considerando informazioni di alto livello connesse con i dati biometrici considerati ed impiegandoli direttamente. La ricerca è quindi limitata ad un database la cui dimensione è più piccola di quella originale.

Un'altra condizione da considerare è quando un sistema di riconoscimento biometrico è assente di standardizzazione anche se ampiamente accettata.

I comitati NIST e ANSI (American National Standards Institute) hanno negli anni effettuato lunghi lavori per avere degli standard comunemente accettati di definizioni biometriche e di procedure. La maggior parte di queste attività è stata effettuata dal comitato tecnico ISO/IEC Joint Technical Committee dal Luglio 2002.

Tuttavia, la questione più importante che doveva essere risolta per la diffusione dei sistemi di riconoscimento biometrico riguarda la loro **usabilità**. In particolare, l'usabilità di un sistema di riconoscimento biometrico è determinata dalla facilità di utilizzo del sistema da parte di un individuo ed è strettamente collegata con la sicurezza e la riservatezza nonché ai problemi che ne potrebbero seguire, ciò comporta quindi un analisi profonda nel processo di elaborazione dei dati biometrici.

6.5 Tipologie di sistemi Biometrici

Di seguito verranno mostrati i principali sistemi biometrici. Tenendo conto di quanto sin qui esposto in maniera puramente accademica, è possibile affermare che non esiste un sistema biometrico perfetto, a seconda dell'impiego esistono sistemi più appropriati e con risultati accettabili.

6.5.1 Impronte digitali

Le impronte digitali sono usate per l'identificazione da più di un secolo. La capacità di verifica dell'identità di una persona mediante l'uso di questa tecnica risulta molto elevata (Wilson, et al., 2004).

La formazione delle impronte digitali è completa già al settimo mese dello sviluppo fetale e la configurazione delle creste su ciascun dito è costante durante l'intero ciclo vitale, essa segue una modalità di crescita comune a quella dei capillari o dei vasi sanguigni durante l'angiogenesi. I fattori rilevanti che influenzano il microambiente circostante il feto sono il flusso dei liquidi amniotici e la sua posizione durante il processo di differenziazione.

Le micro diversità delle condizioni ambientali nelle immediate vicinanze di ciascun polpastrello caratterizza la formazione dei più minuti dettagli della loro superficie. Poiché il punto di partenza del processo di differenziazione è lo stesso per ogni impronta in quanto determinato dagli stessi geni, i pattern risultanti non sono totalmente casuali. Nel caso di gemelli omozigoti, i dettagli minuti delle impronte digitali sono differenti, ma la maggior parte degli studi ha mostrato significative similitudini nella classificazione delle configurazioni relative agli altri attributi generali. La massima diversità fra le impronte digitali è quella riscontrabile tra individui appartenenti a razze diverse. Seguono in ordine decrescente di diversità le impronte di:

- *soggetti della stessa razza ma senza alcuna parentela,*
- *padre e figlio (che hanno in comune metà dei geni),*
- *fratelli e/o sorelle,*
- *gemelli omozigoti.*

I sistemi di riconoscimento delle impronte digitali hanno il vantaggio della facilità di utilizzo e del basso costo. La maggior parte dei sistemi di riconoscimento delle impronte digitali sono basati su l'uso di una minuzia impostata in precedenza.

Al fine di poter valutare attentamente le peculiarità di un'impronta si deve tener conto che vi sono macro-caratteristiche e micro-caratteristiche. La prima considera l'impronta come un insieme di linee (ridge line) che scorrono principalmente in maniera parallela, creando un pattern (ridge pattern).

Le seconde sono note con il nome di minuzie o caratteristiche di Galton e sono determinate a partire dalle terminazioni o dalle biforcazioni delle linee di cresta (Boyanapally, 2008)

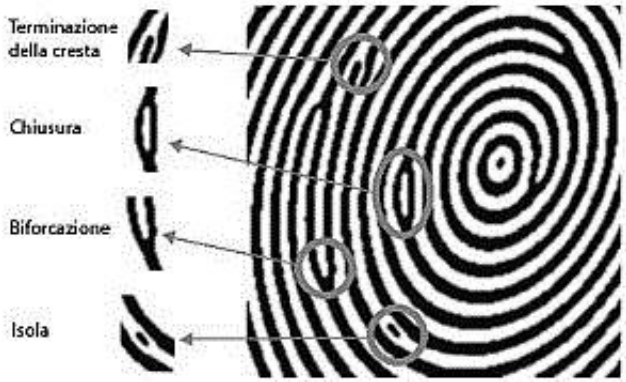


Figura 24 – Micro-caratteristiche delle impronte: Minuzie

Altre micro-caratteristiche più complesse nel loro impiego sono illustrate nella figura seguente

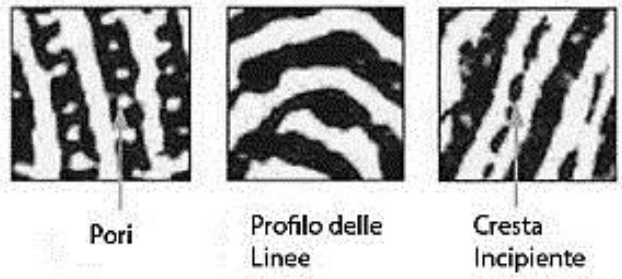


Figura 25 – Micro-caratteristiche delle impronte: Pori, Profili delle linee e delle creste

6.5.1.1 Acquisizione

Storicamente, l'acquisizione delle impronte digitali in ambito forense avveniva mediante la "tecnica ink": il soggetto poneva il dito su un tampone con inchiostro nero e premeva su una carta, la stessa veniva poi analizzato mediante una comune scanner producendo l'immagine digitale finale.

Questo tipo di processo è denominato acquisizione off -line fingerprint o off -line sensing. Un caso particolare di "off -line sensing" è l'acquisizione di un'impronta digitale latente da una scena del crimine. L'acquisizione di impronte digitali può essere classificato in tecniche di scansione diretta oppure off-line.

Una delle tecniche più comuni è la tecnica ad inchiostrazione in cui il dito è posto su un tampone con inchiostro e successivamente premuto su carta, la quale viene semplicemente scansionata per produrre un'immagine digitale; un'inchiostrazione eccessiva o una carenza determina immagini di cattiva qualità.

La tecnica di scansione in tempo reale è facile da usare e presenta un basso costo oltre ad essere affidabile, caratteristiche che la rendono utile anche per applicazioni civili e commerciali; tali benefici non sono sufficienti per un impiego AFIS. Il vantaggio di utilizzare la tecnica di scansione offline è che produce un modello equivalente ruotato mentre la tecnica di scansione diretta richiede un tecnico specializzato che effettui il rotolamento del dito in modo sincronizzato con la scansione. Per l'identificazione, la scansione diretta utilizza un'impressionamento su un piano che è generato premendo il dito contro la superficie dello scanner. In tecniche di scansione diretta, il dito è premuto contro la superficie dello scanner che viene rilevato da un sensore, producendo un'immagine digitale dell'impronta. In un sistema scanner diretto, il sensore che produce l'immagine dell'impronta digitale è la parte più importante. In base al tipo di sensore utilizzato, è possibile classificare le tecniche di scansione diretta come ottiche, allo stato solido e agli ultrasuoni, tecniche ancora in fase di studio e perfezionamento. (Boyanapally, 2008)

L'accuratezza offerta ha favorito l'uso di questa tecnica per l'autorizzazione e identificazione di un sistema soprattutto in ambito forense. In particolare sistemi multi-dita permettono l'acquisizione di tutte e 10 le dita, con un elevato livello di unicità ed elevato livello di identificazione oltre che di autenticazione.

6.5.2 Viso

Il viso è stato, per i ricercatori, oggetto di grande attenzione in quanto risulta essere il tratto biometrico più naturale ed utilizzato per riconoscere un individuo (Jain & Kumar, 2012). Sebbene sia la caratteristica più naturale, il viso è una struttura non lineare, pertanto rende il problema complesso del riconoscimento del Pattern, nonché la determinazione di un'area di ricerca in applicazioni di gestione grafica. Per le promettenti promesse si sono investiti notevoli sforzi nello sviluppo di sistemi automatici di riconoscimento del viso che fossero robusti. Un sistema automatizzato

per il riconoscimento facciale, stabilisce l'identità di un individuo basandosi sul calcolo di funzioni 2D o 3D (Abate, et al., 2007), (Zhang & Gao, 2009).

Tali sistemi per lavorare in maniera corretta, devono effettuare automaticamente le seguenti operazioni:

- Identificazione di una faccia all'interno di un'immagine;
- Localizzazione, se presente, della posizione della faccia.
- Riconoscimento di una faccia, in ogni condizione ambientale, rispetto a un generico punto di riferimento.

I principali approcci di riconoscimento facciale sono (Jain & Anil, 2005):

- Determinazione della forma e posizione delle caratteristiche facciali, quali occhi, naso, bocca, distanza inter-pupillare, distanza naso-bocca.
- Analisi globale del volto effettuata su un set normalizzato di volti (es. Eigenfaces).

Le prestazioni dei sistemi di riconoscimento facciale sono adatti ad usi per fini commerciali (Kumar & Prathyusha, 2009), anche se sono molto influenzati da fattori ambientali (ad esempio illuminazione) e da fattori di acquisizione (ad esempio la rotazione, la distanza di acquisizione); va notato che questi sistemi biometrici possono avere difficoltà a controllare le immagini del volto acquisite con diverse angolazioni. L'analisi comparativa delle regioni facciali rileva i vantaggi di non essere invasiva e di poter acquisire le immagini senza contatto, ottenendo un buon livello di tolleranza dell'opinione pubblica.

Vi sono però chiaramente dei fattori limitativi associati alla sensibilità e alle condizioni di illuminazione, in presenza di parziali o totali occlusioni infatti vi è una bassa accuratezza nel riconoscimento; ed in generale a causa di alcuni problemi quali un livello medio di carattere distintivo, i sistemi di riconoscimento facciale, sono quindi molto inclini ad errori di riconoscimento. (Unar, et al., 2014). Al fine di superare dette condizioni la comunità scientifica ha effettuato ricerche utilizzando caratteristiche 3D anziché 2D (Yuan & Mu, 2012) (Theoharisa, et al., 2008).

Il riconoscimento facciale 3D ha rappresentato un'evoluzione; esso è nato per correggere i problemi fondamentali connessi con il riconoscimento facciale 2D come la degradazione dell'immagine, lo scarso allineamento, il movimento delle orecchie e delle espressioni facciali. Questi sistemi non possono tuttavia garantire un'identificazione affidabile in presenza di artefatti, presentano inoltre problemi con particolari tipologie di cosmetici e qualora vengano effettuati interventi di chirurgia plastica di notevole entità.

Si consideri inoltre che il viso di una persona subisce variazioni col il trascorrere del tempo e ciò può influire sulla precisione di tali sistemi, tale problematica può essere superata con l'applicazione di sistemi predittivi ma richiedono un'elevata elaborazione e campionamenti duranti gli anni; inoltre, l'hardware di elaborazione delle immagini rappresenta un limite nell'uso del sistema.

6.5.3 Orecchio

Un sistema automatico riconosce la forma dell'orecchio umano mediante l'uso di caratteristiche 2D e 3D (Ramesh & Rao, 2009) (Yuan & Mu, 2012). Sono pertanto richieste differenti tecniche di gestione dell'immagine che richiedono l'acquisizione di una fotografia dell'orecchio; avendo un calco dell'orecchio ottenuto spingendolo su una superficie piana ed acquisendo l'orecchio con un termografo è possibile acquisire la misura della funzione di trasferimento acustica di un un'onda inviata sull'orecchio (Yuan & Mu, 2012) (Purkait & Singh, 2008).

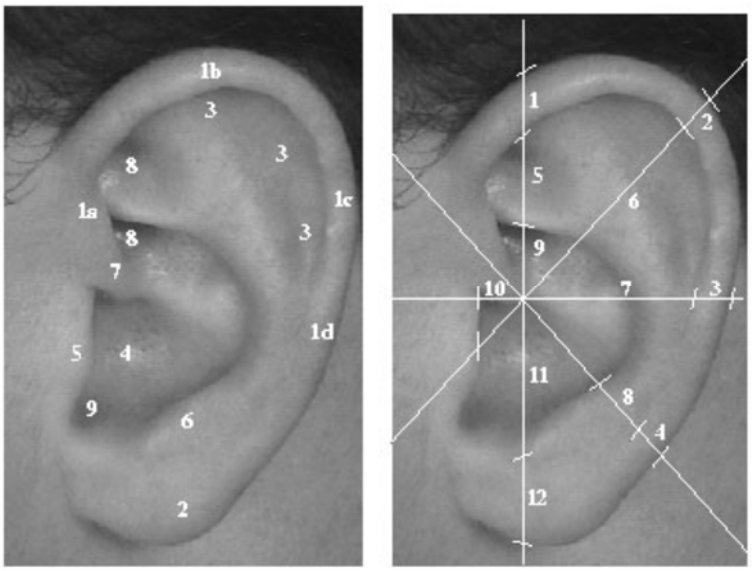


Figura 26 – Caratteristiche biometriche dell'orecchio

Immagine di Sinistra: Anatomia – 1 Elice, 2 Lobo, 3 Canale auricolare, 4 Conca, 5 Trago, 6 Antitrago, 7. Crus di elica, 8 Fossa triangolare, 9 Incisura Intertragica. Immagine a destra: Misure - Punto di misura antropometrico usato nel "Sistema Iannarelli" (Iannarelli, 1989).

6.5.4 Lingua

L'identificazione basata sull'uso della lingua è una modalità relativamente recente per altro non molto diffusa. I principali vantaggi associati all'uso biometrico della lingua includono la protezione dall'ambiente esterno e la forma intrinseca che consente di verificare che il soggetto è vivo.

Un sistema di identificazione che impiega la lingua come caratteristica biometrica verifica caratteristiche geometriche come la larghezza, lo spessore, la curvatura della lingua, il contorno, le crepe, le caratteristiche delle "crepe" e le caratteristiche della struttura della stessa. (Zhanga, et al., 2010).

La conformità nell'uso delle tecniche biometriche legate alla lingue richiede ad oggi ancora numerosi approfondimenti ed uno studio su larga scala.

6.5.5 Denti

Il riconoscimento biometrico mediante l'uso dei denti, risulta del tutto sconosciuto al pubblico; inoltre l'impiego primario è effettuato in applicazioni forensi o in casi di analisi post-morte, pertanto attualmente il suo impiego è rarissimo.

6.5.6 Geometria della mano

La biometria della mano è basata sull'acquisizione di una serie di misure geometriche che si basano sulla mano stessa, inclusa anche la lunghezza e larghezza di ogni dito.

Questa tecnica è molto semplice, non ha subito molte variazioni dalla sua introduzione ed è accettata così come è stata concepita. Non presenta problemi ambientali di umidità o di sudorazione della pelle.

Tale tecnica presenta però un basso carattere distintivo fra esseri umani ed è usato esclusivamente per l'autenticazione e non per l'identificazione. Un'altra limitazione è che l'acquisizione è soggetta a variazioni con il passare del tempo, ciò è legato ovviamente all'avanzare dell'età e quindi a patologie come ad esempio l'artrosi.

6.5.7 Impronta Palmare

Il palmo umano contiene un enorme quantità di informazioni utilizzabili per identificare una persona in maniera simile ad un'impronta digitale.

Il palmo infatti contiene un pattern di creste e valli che lo può far identificare. Grazie alla grande area che può essere acquisita, presenta maggiori caratteri distintivi rispetto alle impronte digitali (Zhang, et al., 2003).

L'impronta palmare presenta anche altre caratteristiche peculiari di tipo geometrico; fra le caratteristiche del punto di delta è possibile distinguere linee principali (linea del cuore, linea della testa, linea della vita), minuzie, creste e pieghe.

L'acquisizione del palmo è anche una delle modalità più affidabili in quanto possiede più funzioni rispetto ad altri sistemi di analisi delle caratteristiche biometriche, si possono distinguere in-

fatti le linee principali, l'orientamento, le minuzie, punti singolari ecc. Considerata la somiglianza delle caratteristiche peculiari, è possibile affermare che il riconoscimento dell'impronta palmare è alla stregua delle impronte digitali una risorsa importantissima; utilizzata sia in applicazioni civili che in applicazioni delle forze dell'ordine, e da molte applicazioni in cui il controllo degli accessi è considerato di elevata importanza. Dalle caratteristiche di cui sopra si può ovviamente rilevare un'unica impronta associandola ad un unico individuo.

Le tecniche di riconoscimento dell'impronta palmare sono state raggruppate in due categorie principali; il primo approccio si basa sulle caratteristiche a bassa risoluzione mentre il secondo si basa sulle caratteristiche ad alta risoluzione.

Il primo approccio fa uso di immagini a bassa risoluzione (ad esempio 75 o 150 ppi), dove vengono estratte solo le linee principali, le strutture e le rughe. Il secondo approccio utilizza immagini ad alta risoluzione (ad esempio 450 o 500 ppi), dove oltre alle principali linee e alle rughe, si acquisiscono le caratteristiche più discriminanti come le creste, i punti singolari e le minuzie.

Gli scanner del palmo presentano la difficoltà nell'acquisizione vista l'elevata area da acquisire, limitandone in parte l'uso. In ogni caso questa tecnica biometria, se aggiunta alla geometria della mano, risolve le limitazioni di quest'ultima. (Sumalatha & Harsha, 2014).

6.5.8 Iride

L'iride è una regione anulare dell'occhio, compresa fra la pupilla e la sclera (in anatomia, la parte non trasparente della tunica esterna dell'occhio). La struttura dell'iride si forma durante la fase fetale e si stabilizza intorno al secondo anno di vita, anche se può subire variazioni durante i primi anni di vita in relazione ai pigmenti in essa contenuti.

La complessità fisiologica della struttura dell'iride si presta per essere utilizzata in ambito biometrico, presentando per altro caratteristiche altamente distintive che ne consentono un impiego sia a livello di autenticazione sia di identificazione (Daugman, 2004).

Tale tratto è infatti considerato uno dei più accurati e precisi, ciò consente un impiego in numerosi settori in cui è richiesto un altissimo livello di sicurezza; può essere infatti impiegato in aeroporti, per il controllo dei rifugiati, nei sistemi per autovetture, ecc. Non vi sono iridi uguali, nean-

che fra gemelli, inoltre l'iride destra non è uguale a quella sinistra. Il numero di informazioni richieste è però, durante una misurazione, molto più grande rispetto a quella di un impronta digitale. (SANGEETHA & KARNAN, 2014).

Il sistema biometrico dell'iride ha un FAR molto inferiore rispetto ai FAR di altri sistemi biometrici, tuttavia presenta un valore FRR che è ancora troppo elevato.

Si noti che un eventuale intervento chirurgico che provi ad alterare l'iride risulta estremamente complesso; risulta inoltre piuttosto facile rilevare iridi artificiali (Sharma, et al., 2012) mediante l'analisi della riflessione della luce in più punti dell'iride (Puhan, et al., 2011) (Daugman, 1998).

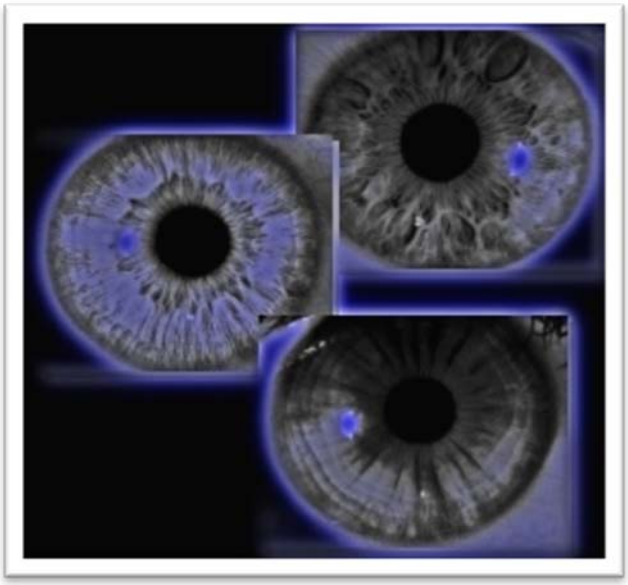


Figura 27 – Esempio di immagini dell'iride acquisite da diversi sensori, si può notare la differenze dei modelli dell'iride.

6.5.9 Retina

La retina è la membrana più interna del bulbo oculare ed è la componente fondamentale per la visione; le strutture della retina sono ricche di informazioni che le rendono una diversa dall'altra, mostrando caratteristiche distintive e consentendo in sostanza l'identificazione del singolo soggetto.

La biometria della retina, è da considerarsi fra le più sicure, ma anche la più invasiva.

Gli scanner della Retina offrono valori di FRR (false rejection rate) e di FAR (false acceptance rate) bassissimi, pari a circa uno su un milione (Woittennek, et al., 2014). Gli scanner si basano infatti sull'acquisizione della struttura vascolare della retina mediante un sistema di verifica della sagoma oculare; si ha quindi l'inconveniente di rivelare problemi collaterali come l'ipertensione (ecc.) con conseguenti problemi di privacy, inoltre l'utente medio ritiene tale sistema come fortemente invasivo, tenuto conto delle modalità di acquisizione, con conseguenti applicazioni solo in particolarissimi settori.

6.5.10 Battitura

La battitura di tasti è la prima delle biometrie legata ad una caratteristica non strettamente fisica ma comportamentale e psicologia; la dinamica della battuta dei tasti è iniziata con le vecchie macchine da scrivere dove la battuta demarcava la modalità con la quale un utente premeva un tasto sulla macchina da scrivere; oggi, con l'impiego dei computer, le considerazioni inerenti lo studio di questa biometria è profondamente cambiata, inoltre l'analisi può essere accompagnata anche da tecniche più avanzate come la tecnica del "tracciamento del mouse" (Freeman & Ambady, 2010) o la tecnica degli "Registrazione degli ingressi" di un pc (Kukreja, et al., 2005).

La ricerca di applicazioni che effettuano la registrazione della scrittura dei tasti include numerosi settori di studio: studi sui processi di scrittura, cognitivi, analisi della strategia di scrittura in ambito professionale o di scrittura creativa, lo sviluppo della scrittura di un bambino– con e senza problemi a imparare a scrivere, analisi della scrittura di una prima e di una seconda lingua, ecc. (Mariëlle Leijten, 2013). In sostanza tale tecnica non ha un valore fortemente distintivo, ma consente un basso FRR (Rubin & A., 1997) ed anche dopo la completa identificazione di un operatore, si ha un monitoraggio completo.

6.5.11 Firma

Il metodo di analisi connesso all'apposizione della firma è universalmente riconosciuto come caratteristico e distintivo di un particolare individuo (Lee, et al., 1996) (Nalwa, 1997) (Schirripa Spagnolo, et al., 2004).

Anche se questa tecnica biometrica richiede ovviamente un supporto sul quale è apposta la firma e quindi un'azione attiva da parte di un utente, tale tecnica è riconosciuta sia in ambito giuridico che governativo come metodo di autenticazione. L'analisi della veridicità della firma mediante l'uso di PDA e di tavolette grafiche consente la verifica in tempo reale e lo studio del profilo dinamico di pressione. L'analisi della firma può essere fatta anche off-line o tradizionalmente senza l'ausilio di apparecchiature di verifica diretta (Schirripa Spagnolo, et al., 2004). La firma è considerata un tratto biometrico comportamentale in quanto soggetta a variazioni legate all'evoluzione della vita, agli atteggiamenti, allo stato fisico o mentale, o al supporto impiegato. L'analisi di questo tratto richiede ampia conoscenza ed esperienza inerenti alcune caratteristiche intrinseche nell'apposizione della firma

6.5.12 Voce

La voce è la combinazione di più caratteristiche fisiche e comportamentali (Campbell, 1997). La ricerca delle caratteristiche di un segnale vocale richiede metodi di analisi e teorie specifiche, spesso ben distinte da quelle della ricerca di un discorso scritto. Lo studio del parlato deve coniugare una trattazione puramente linguistica con una di natura psicologica e pragmatica. Rilevanti infatti sono le condizioni sociali, la provenienza geografica, che caratterizzano il segnale vocale emesso da un essere umano.

In maniera più rigorosa è possibile affermare che l'energia aereodinamica prodotta dal sistema respiratorio è trasformata attraverso il passaggio del tratto orofaringeo, che funge da trasduttore, in energia acustica. Tale energia che è modulata dalla trachea viene poi irradiata attraverso le labbra ed è definita comunemente voce. Il segnale vocale può essere quindi interpretato come segnale che attraversa un filtro complesso variabile nel tempo. A causa dell'imprecisione e della notevole varietà nel modo di articolare i suoni un segnale vocale abbastanza fluido è normalmente non stazionario. Esistono però piccole porzioni di segnale in cui anche se per poco tempo rimangono costanti alcune frequenze, frequenze dette formanti. Tali frequenze permettono di modellizzare l'apparato vocale come una successione di cavità risonanti con frequenza propria, stimolate da un generatore d'impulsi. Si ipotizza quindi che il segnale sia considerato quasi-stazionario in ristretti intervalli di tempo e che quindi possa essere segmentato in base a fonemi. Il fonema è la più piccola parte di

segnale dotata di significato distinguibile per un determinato linguaggio, è chiaro che questo sono diversi in base alle varie lingue. Dal punto di vista spettrale un fonema presenta una forte concentrazione alle basse frequenze quando vi è una nasalizzazione del fonema stesso. Si tenga che non sempre si è in grado di distinguere i fonemi ciò perché durante una conversazione vi è una preparazione da parte del cavo orale alla pronuncia di un fonema successivo. Si è posto particolare attenzione ai fonemi poiché esistono sistemi semi-automatici che impiegano proprio i fonemi per l'identificazione di un oratore. In ambito forense e scientifico dagli anni 60 ad oggi vi è stato un notevole interesse sulle caratteristiche di un segnale vocale anche a causa di eventi criminosi di natura terroristica ed intimidatoria, a man forte dell'aera forense si sono però aggiunti col tempo strumentazioni "hardware" e "software" di supporto. Il riconoscimento di un parlatore non è un operazione semplice poiché oltre alle caratteristiche di variabilità della voce si deve tener conto delle condizioni in cui sono effettuate le registrazioni quali ad esempio il rumore ambientale o il rumore del canale. Vi è un ulteriore fattore di cui bisogna tener conto la voce è soggetta ad un intrinseca variabilità dovuta ad alterazioni legate all'aumentare dell'età o dell'insorgere di patologie, cause queste di medio-lungo periodo, esistono però cause di breve periodo come l'assunzione di sostanze stupefacenti o l'assunzione di alcool o più semplicemente lo stato emotivo del soggetto.

Tali variazioni influiscono alterando la frequenza di vibrazione delle corde stesse. Bisogna pertanto tener presente della componente a breve termine e quella a lungo. In aggiunta la voce non è considerata estremamente distintiva, pertanto non utilizzabile, da sola, per l'identificazione.

Un sistema di riconoscimento delle parole si basa sulla lettura predeterminata di frasi usate durante la fase di "registrazione", o in un'identificazione libera. Questa seconda possibilità è molto più complessa e richiede una robustezza maggiore, incluso un archivio molto grande.

I principali svantaggi di questo sistema sono la sensibilità al rumore di fondo. Per questa ragione si preferisce usare questa tecnica mediante l'impiego di apparati di telefonia. E' chiaro che durante un intercettazione ambientale la componente a lungo termine non è rilevante, a meno di non volere un confronto con un campione di non recente acquisizione. Oltre alle variazioni appena menzionate e note col nome di intrinseche, si devono considerare distorsione introdotta dal sistema strumentale di registrazione del suono in tutte le sue componenti, microfono, canale di trasmissione, apparecchio di registrazione; le variazioni sono legate alla qualità degli strumenti che si impie-

gano e dalle configurazioni in cui è posto il sistema di registrazione, la qualità finale è pertanto determinata dal peggior componente impiegato nel sistema di acquisizione audio. Tali limiti devono essere considerati nella fase precedente l'acquisizione anche nel rispetto del likelihood ratio, tenendo conto delle conoscenze "a priori" e quelle "a posteriori". L'analisi di una voce ha quindi due modalità quella linguistica e quella acustico-strumentale.

L'analisi fonetico-linguistica tiene conto di aspetti peculiari di un soggetto in esame, tale analisi viene eseguita da un operatore che tiene conto di diversi fattori, fattori come detto di tipo fonetico, fattori inerenti l'educazione posseduta dall'oratore ed anche aspetti salienti della personalità del soggetto, lo studio fonetico mostra modalità di articolazione e collegamento dei suoni ed è un fattore semi-conscio, non variabile nel medio periodo. I fonemi base sono le vocali e le consonanti. I dittonghi sono anch'essi considerati fonemi ma inscindibili poiché le caratteristiche spettrali delle vocali si susseguono così rapidamente che non sono osservabili individualmente. A livello spettrale le vocali le vocali possono essere distinte in base alle prime due formanti. La PRIMA formante varia da 300 Hz a circa 700 Hz, la seconda da 800 Hz a 2,5 kHz tali valori presentano chiaramente variabilità legato al singolo parlatore. Altri aspetti fonetici linguistici sono quelli semantico letterari legati alla scelta dei vocaboli operata, socio-linguistica, accenti o inflessioni legate alla zona di appartenenza o particolarità legate alla cultura dell'oratore, ulteriore aspetto è quello prosodico che riguarda l'andamento espositivo, le intonazioni che però possono essere legate allo stato emotivo al contrario della velocità di articolazione; infine caratteristiche foniatriche che sono caratteristiche legate a condizioni morfo-fisiologiche del singolo oratore.

L'analisi sopra menzionata nei suoi vari aspetti non può essere condotta da un sistema automatico poiché prevede l'analisi di peculiarità che un sistema non è in grado di rilevare e distinguere. Esistono quindi sistemi semi-automatici che con l'ausilio di un operatore consentono l'identificazione di alcuni tratti di un segnale vocale attraverso spettrogrammi; o sistemi totalmente automatici in cui una volta introdotti file audio il database effettua confronti e fornisce risultato fornendo il rapporto di vero somiglianza. Il sistema automatico non tiene conto di peculiarità linguistiche, si tende pertanto ad impiegare più metodi in modo da poter rilevare tratti caratteristici ed effettuare verifiche nella maniera più veloce ma con ragionevole certezza dei dati ottenuti, i soli sistemi automatici o semi-automatici non sono in grado come già detto ad esempio di rilevare la

pronuncia di una parola tipo “casa” da parte di un fiorentino, inoltre i sistemi semi-automatici lavorano solo sulle vocali poiché è più il riconoscimento delle stesse.

L’analisi delle onde acustiche da parte dei software avviene tramite scomposizione dell’onda complessa nelle sue onde componenti, l’analisi è condotta nel dominio di Fourier attraverso l’impiego della FFT, per l’analisi linguistica l’onda viene divisa nella parte periodica e aperiodica, è chiaro che siamo interessati ad ampiezza e frequenza dell’onda complessa che viene quindi visualizzata nel piano spettrale, la frequenza fondamentale mostra invece il numero di oscillazioni delle corde vocali nell’unità di tempo, questa viene percepita come tono vocale detto timbro vocalico; la fondamentale è legata alle caratteristiche anatomiche dell’oratore, più spesse e lunghe sono le pliche, più bassa è la frequenza di vibrazione. Nel dominio del tempo come detto in antecedenza si impiegano gli spettrogrammi che sull’asse delle ascisse hanno come riferimento il tempo, sulle ordinate gli aumenti di frequenza ed hanno un piano perpendicolare all’asse del tempo in cui vi sono le ampiezze. Con tali grafici è possibile studiare la durata vocalica e consonantica, il timbro delle vocali, le caratteristiche del modo e l’articolazione dei suoni, la realizzazione dei suoni, la variazione intra e interlinguistica. Tali grafici permettono attraverso la rappresentazione con l’ausilio di un computer di sovrapporre eventi acustici e quindi spettri del segnale.

6.5.13 Andatura

Il parametro biometrico dell’andatura della camminata di una persona è riconosciuta e spesso impiegata in ambito di sicurezza nei sistemi di videosorveglianza. Questa caratteristica biometrica presenta una notevole variabilità, pertanto esistono numerosi algoritmi basati sulla definizione della fisionomia di una persona, lo scopo è quello di determinare caratteristiche spazio-temporali legate all’andatura di un soggetto; pertanto al fine di effettuare un’analisi significativa di una persona è necessario avere la massima conoscenza di un modello del corpo della persona.

Alcuni algoritmi si basano sull’estrazione dinamica delle variazioni di un predeterminato punto, come l’alterazione destra o sinistra dei piedi durante una camminata (Nixon, et al., 1999). Questo tratto biometrico è altamente soggetto a variazioni di fattori esterni come le scarpe impiegate, i vestiti, problemi reumatici, superfici di camminamento; in sostanza si ritiene che da solo non possa contraddistinguere una persona ma possa fornire in alcuni casi informazioni discriminanti.

6.5.14 Confronto Biometrico

La tabella sotto-riportata confronta le caratteristiche biometriche principali in virtù di alcune peculiarità, sia tecniche che sociali; risulta chiaro che ogni tecnica presenta livelli di accettabilità diversi a seconda dell'utilità finale. Si noti che nei paragrafi precedenti non sono state affrontate/discusse tutte le tecniche biometriche riportate in tabella; ci si è soffermati soltano su quelle con interesse biometrico di ricerca che posso portare a nuove scoperte e applicazioni.

Indicatore Biometrico	**Universalità**	**Distintività**	**Permanenza**	**Collezionabilità**	**Prestazioni**	**Accettabilità**	**Circonvenzione**
Impronte Digitali	M	A	A	M	A	M	M
Volto	A	B	M	A	B	A	A
Iride	A	A	A	M	A	B	B
Retina	A	A	M	B	A	B	B
Geometria della Mano	M	M	M	A	M	M	M
Palmo	M	A	A	M	A	M	M
Andatura	M	B	B	A	A	A	M
Battitura	B	B	B	M	B	M	M
Firma	B	B	B	A	B	A	A
Voce	M	B	B	M	B	A	A
Orecchio	M	M	A	M	M	A	M
Pattern venoso della mano	M	M	M	M	M	M	B
Termografia del Volto	A	A	B	A	M	A	B
DNA	A	A	A	B	A	B	B
Odore	A	A	A	B	B	M	B

Tabella 7 – Comparazione delle principali caratteristiche biometriche

In Tabella 7, basandosi sul “American standard scale”, ad ogni tipologia è indicato il livello in riferimento al parametro di interesse: A (alto), M (medio), B (basso).

6.6 Conclusioni

E’ possibile concludere che non sempre è vero che soluzioni più sicure e realizzabili sono quelle più accettabili dall’utente o attagliate le finalità previste. Si pensi per esempio alla retina, questa offre livelli altissimi di distintività ed universalità ma un bassissimo livello di accettabilità, legato al metodo invasivo; d’altro canto il DNA presenta valori di accuratezza simile alla retina ma un impatto nella collettività limitato.

Pertanto, è possibile affermare che non esiste una tecnica perfetta, ma tecniche da scegliere in funzione delle applicazioni; inoltre potrebbe essere necessario l’impiego di più tecniche biometriche per il raggiungimento dello scopo prefissato.

7 Hylemetria

7.1 Introduzione

Nei capitoli precedenti è stata fatta una lunga panoramica sulle peculiarità di sistemi biometrici, semplici e complessi; ed un excursus sulle principali tecnologie anticontraffazione. Questi capitoli introducono il presente; l'idea è quella di sviluppare un metodo che consenta una diminuzione della contraffazione, inserendo dei sistemi che tengono conto delle caratteristiche intrinseche dei singoli prodotti; alla stregua delle impronte digitali, iride, retina, geometria della mano, etc. per l'uomo. Esistono delle caratteristiche differenti a seconda dell'oggetto in esame, che possono essere misurate con metodi non distruttivi, e che permettono l'identificazione in maniera univoca di ogni oggetto, rendendo gli oggetti quasi impossibili da contraffare.

Obiettivo di questo capitolo è introdurre tutti quei concetti e conoscenze che hanno condotto e condurranno a dimostrare e mostrare l'unicità, l'induplicabilità di molti oggetti.

7.2 Definizione

L'unicità di un oggetto trae la propria origine nella filosofia della biometria, lo studio delle caratteristiche intrinseche degli oggetti va con il nome di Hylemetria, dalle parole greche ὕλη (hyle), oggetti inanimati e μετρον (metros) misura.

I primi studi sull'argomento pur non passando con questo nome risalgono al 1990, ma solo nel luglio 2005 (Buchanan, et al., 2005), sulla rivista Nature venivano identificate delle imperfezioni sulla superficie della carta; come imperfezioni uniche; la rivista propone queste imperfezioni come caratteristica di identificazione per poter combattere le frodi. Secondo quanto riportato nella rivista tutti i documenti, carte plastificate e confezioni dei prodotti contengono un codice fisico che li rende unici ed identificabili. L'origine di queste unicità sono alcune caratteristiche fisiche randomiche che consentono di identificatore univocamente documenti e oggetti (Smith, 1999) (Renesse, 1995) (Indeck & E., 1993) (Pappu, et al., 2002) (Goodman, 1984).

7.3 Hylemetria, principali caratteristiche

Per quanto introdotto è possibile asserire che l'hylemetria, ha lo scopo di identificare delle caratteristiche, alla stregua della biometria (paradigma biometrico su oggetti inanimati), che siano uniche e randomiche al fine di identificare univocamente un oggetto.

Vi è un gran numero di applicazioni che potrebbe beneficiare delle capacità di identificare univocamente un oggetto, si pensi ai soldi, biglietti, sistemi di protezione delle opere d'arte.

La verifica è solo una delle possibili applicazioni in cui si possano sfruttare le caratteristiche intrinseche degli oggetti.

Teoricamente, qualunque caratteristica che sia randomica e irriproducibile può essere usata nell'identificazione hylemetrica. Una caratteristica deve comunque rispettare i seguenti requisiti, cioè essere:

- **Unica:** ogni oggetto deve essere identificabile e distinguibile da tutti gli altri;
- **Numerabile**: la caratteristica deve poter essere misurata quantitativamente;
- **Non-invasiva:** la caratteristica deve poter essere misurabile senza essere modificata in alcun modo.
- **Coerente:** funzione di vettore e deve essere verificabile da più parti per tutta la durata dell'oggetto;
- **Concisa**: funzione di vettore deve essere breve e facilmente calcolabile
- **Robusta:** dovrebbe essere possibile verificare il vettore funzione, anche se l'oggetto è stato sottoposto a un trattamento duro;
- **Resistente alla contraffazione:** dovrebbe essere molto difficile e costoso, o impossibile per un malintenzionato esprimere lo stesso vettore di un secondo oggetto in funzione di quello originale

Qualunque caratteristica che sia randomica e difficile/impossibile da riprodurre può potenzialmente essere una caratteristica Hylemetrica. Vi sono però dei requisiti che detta caratteristica, dovrà però ulteriormente soddisfare:

- Consentire l'implementazione di un vettore (template) e ciò sia ripetibile;

- Il costo della creazione e la “firma” del vettore della caratteristica deve essere piccolo, e proporzionato al livello di sicurezza desiderato;
- Il costo della riproduzione delle strutture fisiche uniche e randomiche usate come caratteristiche Hylemetriche deve essere più grande della soglia che indica un falso;
- Il costo di verifica di autenticità di una caratteristica firmata digitalmente deve essere più piccola, se comparata con il livello di sicurezza desiderato.

Partendo da queste condizioni, si è verificata la possibilità di applicare il metodo hylemetrico ad altri ambiti, l'obiettivo è quello di far rispettare il processo di autenticazione e anti-contraffazione con una soluzione innovativa. Per fare questo, il primo passo è quello dell'identificazione, per ciascun caso di studio, delle caratteristiche imposte dall’approccio Hylemetrico. Per qualsiasi studio del caso analizzato, deve essere possibile identificare caratteristiche che hanno le proprietà descritte in precedenza. Le particolarità intrinseche che si vanno a verificare sono diverse a seconda degli oggetti, ma il metodo e l’approccio di verifica è simile per tutti quelli analizzati.

Solo a titolo di esempio è possibile oramai affermare che le fibre di sicurezza metalliche presenti nelle banconote, possono generare una caratteristica Hylemetrica. (Schirripa Spagnolo, et al., 2010)

Esse hanno la proprietà fisica di brillare nello spettro visibile quando illuminate da luce ultravioletta a una precisa lunghezza d'onda. La distribuzione delle fibre del tutto casuale, crea un modello di identificazione che rende ogni banconota unica.

7.4 Hylemetria, applicazioni

L’Hylemetria può essere usata, per le premesse sin qui espresse, in numerosi campi e in numerose applicazioni, esistono infatti già studi di caratteristiche Hylemetriche in numerosi settori: dall’arte, alla sicurezza. Nel campo delle opere d'arte per esempio, sono già stati eseguiti esperimenti per aumentare la sicurezza delle stesse, l’idea di base usa il certificato di garanzia tradizionale apportandone un ulteriore livello di sicurezza. Il certificato di garanzia presente su tutte le opere d’arte, può essere copiato o sostituito da una copia falsificata ad opera d’arte essendo comunemente un foglio apposto dietro la tela, con al massimo dei sistemi di sicurezza tradizionali come i watermarking o ologrammi; l’idea introdotta è stata quella di unire alla soluzione tradizionale

nominata pocanzi, forme più avanzate di codici di sicurezza come ad esempio i qcode in cui immagazzinare un dettaglio dell'opera d'arte, presupponendo che ogni opera è unica e rispetta i criteri Hylemetrici.

Un altro caso di studio già effettuato è legato alla litografia, l'impressionamento dovuto alla pressione della pietra, processo intrinseco della produzione, genera delle venature uniche, acquisibili con una semplice fotocamera digitale ed elaborabile per renderle uniche.

Per dipinti e le statue è possibile usare una particolare tecnica di image processing e di filtraggio che fornisce dalla struttura dell'oggetto acquisisce l'immagine mostrando un pattern di speckle.

Un ulteriore studio effettuato in precedenza è legato alle confezioni di farmaci, su di esse è possibile trovare caratteristiche, questa volta mediante l'uso di una tecnica nota come "White Light Speckle". Una particolare zona veniva spruzzata mediante uno spray con componenti nell'ultravioletto, il risultato è stato che ogni confezione era stata stampata un cono Speckle Pattern differente.

Per quanto sopra il metodo di studio legato alla generazione di un Template Hylemetrico è da considerarsi consolidato; questo consente quindi di autenticare un oggetto, sia essa opera d'arte, documento ecc., che si sta analizzando; le modalità verranno esplicate nei capitoli successivi.

7.5 Legame tra un oggetto ed elementi di certificazione "indissolubili"

Per quanto si qui esposto, nel quadro di una lotta alla contraffazione, ciò che è importante capire, è quale sia il legame tra un oggetto, e gli elementi di certificazione "indissolubili".

Nello specifico è possibile sviluppare dei sistemi anti-contraffazione che leghino le caratteristiche intrinseche di un oggetto con moderni sistemi di riconoscimento. Il legame che lega un oggetto con gli elementi di certificazione può prevedere nello specifico due soluzioni che si accenneranno (per completezza di trattazione) nei paragrafi di seguito riportati, ma che saranno ampiamente discussi nel Capitolo 8 inerente la Crittografica.

7.5.1 Archivio sicuro.

Per archivio sicuro si intende un'archivio che è di sola lettura e in cui possono essere memorizzate le caratteristiche "uniche" dell'oggetto. L'archivio a sola lettura può essere implementato tramite crittografia asimmetrica (chiave segreta per criptare e chiave pubblica per decriptare). In questo caso, la sicurezza dell'archivio risiede nella sicurezza/robustezza delle chiavi (su questo argomento si rimanda al capitolo 8).

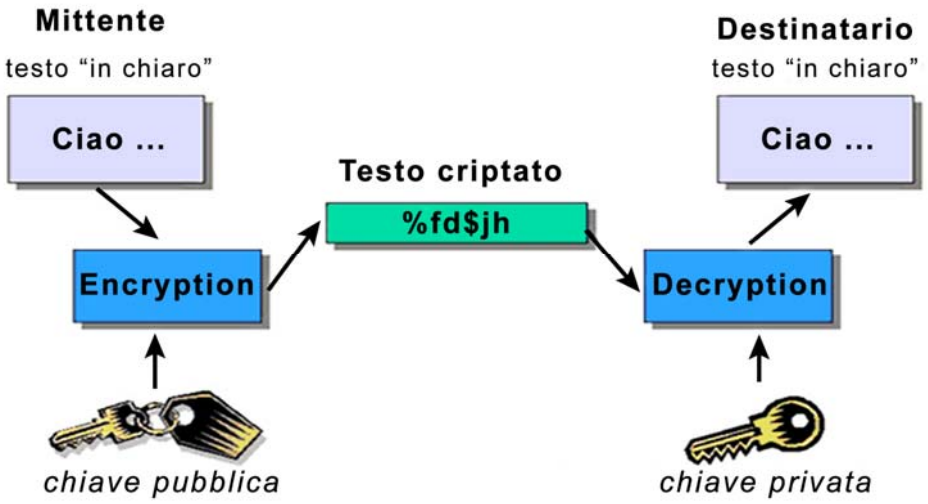


Figura 28 – Crittografia a chiave pubblica

Per questo approccio vi sono due punti deboli. Il primo risiede nel fatto che si ha a disposizione, per lungo tempo, informazione in chiaro (la chiave pubblica) e il risultato della crittografia. Questo consente di poter accedere, avendo un lasso di tempo lungo, alla chiave segreta. Una possibile soluzione per irrobustire il sistema sarebbe quella di cambiare le chiavi periodicamente.

Tale soluzione è possibile però solo su un archivio remoto (ad esempio WEB) non su un sistema RFID. Cambiare le chiavi di crittografia comporta infatti la modifica del contenuto dell'archivio a sola lettura (in altre parole l'archivio non può essere "fisicamente" a sola lettura).

7.5.2 Uso di funzione one-way (funzione hash).

Questa funzione agisce sulle caratteristiche uniche, "triturandole" in modo "univoco". Due oggetti "leggermente" differenti restituiscono Hash "significativamente" diversi. Dal Hash non è

possibile ricostruire la caratteristica di partenza (informazione in chiaro). La funzione Hash è pubblica così come è pubblica la caratteristica che la determina. Per avere la certezza che la funzione Hash non venga sostituita, (clonazione di un opera per esempio e sostituzione dell'Hash) è indispensabile che venga firmato digitalmente dall'autore o dall'ente certificatore. In questo caso, la robustezza si sposta sulla robustezza della firma digitale.

Il problema, di questo approccio, risiede nella tecnologia della firma digitale. Le tecnologie possono facilmente diventare obsolete. La firma digitale di un'opera d'arte, potrebbe essere soggetta ad obsolescenza delle tecnologie di certificazione e ciò non è accettabile.

Avendo a disposizione l'opera originale, il risultato della crittografia e della chiave pubblica è sempre possibile ottenere (anche se con tempi di calcolo lunghi – che si accorciano con l'aumento di potenzialità di calcolo degli elaboratori elettronici) la chiave privata. Se la funzione hash lavora su oggetto/immagine con dimensione/risoluzione non nota, non si ha l'informazione dell'oggetto/immagine originale e pertanto vi è l'impossibilità fisica di risalire alla chiave privata. (Si rimanda inoltre al Para. 8.8 -La funzione HASH)

7.6 Funzioni fisiche non clonabili - Physical Unclonable Functions (PUF)

Oltre ai sopra menzionati sistemi di riconoscimento dei materiali vi è una forte attenzione alla verifica dell'originalità di componenti tecnologicamente avanzati e la verifica di ogni componente o scheda; gli impieghi spesso di nicchia o in cui sia richiesto un livello di elevatissima affidabilità hanno richiesto di innalzare il livello di attenzione rispetto alla contraffazione di componenti tecnologicamente avanzati.

Solo per menzionare qualche esempio, le applicazioni per le Smart card, i tag per RFID ed i sensori senza filo sono divenuti di impiego quasi comune e la sicurezza nella comunicazione tra i vari dispositivi è divenuta di fondamentale importanza, soprattutto in alcuni settori di impiego.

Nella maggior parte dei circuiti attualmente in commercio la maggior limitazione è legata alle limitate risorse e alle dimensioni dell'area in cui viene inserito il circuito integrato che hanno imposto ai progettisti un'attenzione anche sul consumo di energia da parte delle applicazioni all'interno degli integrati, limitando la scelta dei protocolli crittografici. I metodi convenzionali si

basano pertanto sull'immagazzinamento digitale di chiavi segrete in memorie volatili che sono vulnerabili a tecniche "reverse engineering"[7] e attacchi "side channel"[8].

Attualmente in alternativa sono in forte fase di studio delle funzioni denominate "PUF" - **Physical Unclonable Functions alias funzioni fisiche inclonabili**; che sfruttano unicità o variazioni intrinseche nei processi di produzione per creare codici identificativi (ID) inclonabili e chiavi segrete.

È opportuno considerare una PUF come una funzione in senso "ingegneristico", vale a dire una procedura eseguita da o su un particolare sistema (fisico).

L'ingresso di una PUF è chiamata "challenge" alias "interrogazione" e l'uscita "risposta". Data un'interrogazione e la risposta misurata, la relazione che le lega è nota come "coppia interrogazione-risposta" (challenge-response pair) CRP e la relazione che lega un'interrogazione e la risposta di una particolare PUF è detta comportamento CRP (behavior CRP).

In un'applicazione tipo, una PUF è usata in due distinte fasi. Nella prima fase detta "enrollment" un numero di CRP è estratto da una particolare PUF e registrato in un database di CRP. In una seconda fase detta di verifica, viene presa un'interrogazione avente come origine il database CRP e viene applicata alla PUF, la risposta viene quindi confrontata con quella contenuta nello stesso database.

La caratteristica distintiva di una PUF è che anche una fusione non sicura, genera una funzione unica che non può essere copiata; inoltre essendo legate alle variazioni del processo produttivo non sono controllabili o modificabili. Le PUF generano quindi una funzione di tipo operazionale, nella maggior parte dei casi non di tipo logico, dato un ingresso si potrebbero avere più uscite.

---

[7] Attacco di "reverse engineering" – attacco di reingegnerizzazione è un attacco che punta ad effettuare una stima delle caratteristiche dei componenti di un sistema (esempio ritardo del gate), cosi che il malintenzionato possa clonare il sistema oppure possa contraffare lo sviluppo di un software. Finché la clonazione di un sistema è tecnologicamente irrealizzabile (o poco conveniente), gli attacchi di questo tipo sono rivolti all'emulazione del comportamento delle strutture dei modelli del sistema. Un effettivo tentativo di "reverse-engineering" si modella il sistema con N componenti, in un tempo polinomiale rispetto a questi. Aumentando però linearmente N, è possibile fornire facilmente una contromisura contro questi attacchi che hanno complessità esponenziale.

[8] Attacchi Side channel: Categoria di attacchi che, utilizzando varie tecniche di inferenza statistica, producono una stima del valore dei segreti (P. es. password, chiave di codifica) utilizzati in una funzione di sicurezza sulla base dell'osservazione di grandezze fisiche.

Tali funzioni garantiscono quindi un funzionamento affidabile in presenza di variazioni di tensione e temperatura anche se non sono esenti da rumori (Srivathsa, 2012).

7.6.1 Misura delle Inter ed Intra-distanze

La fondamentale applicazione di una PUF è quella di consentire che il sistema in cui è inserita sia identificato e ciò avviene con debiti accorgimenti. Queste funzioni consentono quindi l'identificazione ma al contempo una protezione. A questo scopo, si ritiene opportuno per completezza introdurre dei cenni sulla "teoria della classificazione e identificazione" sui concetti di inter-distanza o intra-distanza legati alle PUF.

Per una data istanza di una PUF, l'inter ed intra-distanza è calcolata nel seguente modo:

- L'inter-distanza tra due differenti PUF è la distanza tra due risposte risultanti l'applicazione dell'interrogazione, una volta a tutte le due PUF.
- L'intra-distanza tra due risultati aventi come origine una singola PUF è data dalla distanza tra le due risposte risultanti l'applicazione dell'interrogazione due volte su una sola PUF.

Sia l'inter-distanza che l'intra-distanza sono misurate su un paio di risposte derivanti dalla stessa interrogazione.

La misura della distanza può variare a seconda della natura della risposta. In molti casi in cui la risposta è una stringa di bit, si utilizza distanza di Hamming. Spesso la distanza di Hamming è espressa come una frazione della lunghezza delle stringhe considerate, e in tal caso si chiama distanza di Hamming relativa o frazionata.

Il valore sia dell'inter che dell'intra-distanza può variare a seconda dell'interrogazione e delle PUF coinvolte.

Per un particolare tipo di PUF, le caratteristiche delle distanze di cui sopra sono spesso riassunte attraverso l'uso di istogrammi che mostrano la distanza che intercorre su entrambe le distanze, osservate su un numero differente di interrogazioni, e su coppie differenti di PUF.

In molti casi, entrambi gli istogrammi possono essere approssimati ad una distribuzione gaussiana ed essere schematizzati attraverso il valore medio, rispettivamente μ_{inter} ed μ_{intra} e quando possibile con la loro deviazione standard σ_{inter} e σ_{intra}.

Si noti che μ_{intra} esprime il rumore medio delle risposte, e pertanto tale valore deve essere reso il più piccolo possibile al fine di avere una risposta PUF affidabile.

D'altro canto μ_{inter} esprime il valore dell'unicità. Per esempio può infatti misurare il valore migliore per distinguibilità di due sistemi che si basano sulle rispettive risposte PUF.

7.6.2 Effetti ambientali

La generazione di una risposta PUF richiede generalmente delle misurazioni fisiche, vi sono quindi da considerare un numero di effetti non voluti che possono interferire sulla misura.

Come descritto in precedenza, la stessa interrogazione applicata alla stessa PUF non necessariamente produce la stessa risposta, bensì una intra-distanza fra due risposte PUF.

Le cause di questo fenomeno si ritengono essere dovute a rumore randomico e incertezza nella misurazione, che causano un'inevitabile disturbo nella misura. In aggiunta alle cause menzionate pocanzi, vi sono alcuni fattori ambientali che hanno effetti sistematici sulla misura; per esempio la temperatura o la tensione di alimentazione di un circuito integrato.

Il valore medio della intra-distanza aumenta in misurazioni in cui vi sono grandi variazioni ambientali. Considerando gli effetti come sistematici, è possibile ridurre la loro influenza secondo le seguenti opzioni:

- Se gli effetti sono parzialmente lineari e interessano l'intero dispositivo in maniera più o meno omogenea, è possibile applicare un approccio differenziale. Si considera una relazione (differenza o rapporto) tra due misurazioni simultanee invece di una singola misurazione; la misura ottenuta sarà molto più robusta. Questa tecnica è nota come compensazione (Gassend, et al., 2002) (Gassend, 2003).
- L'importanza degli effetti ambientali dipende principalmente dalla modalità di implementazione delle PUF (Vivekraja, 2009). E' possibile pertanto scegliere un'implementazione che riduca o sia poco sensibile a fattori ambientali, o in alternativa selezionare in anticipo risposte che siano robuste e poco legate all'ambiente ed ignorare quelle instabili (Suh & Devadas, 2007)
- Se le risposte PUF variano fortemente su tutto il range per un determinato fattore ambientale, è possibile effettuare una misurazione con un sensore esterno ed introdurre differenti

operazioni nei diversi intervalli, scelti abbastanza stretti, da consentire di ridurre gli effetti ambientali negli stessi (Yin & Qu, 2009).

7.6.3 Proprietà delle PUF

La nozione di funzione fisica non clonabile non è racchiudibile in una singola definizione, inoltre non descriverebbe a pieno le caratteristiche delle PUF. Di seguito verranno mostrate le caratteristiche delle PUF anche in virtù di una più ampia valutazione all'interno dell'Hylemetria. Si noterà che pur non essendo conosciute in letteratura con tale nome, le PUF rispecchiano in pieno le caratteristiche da noi definite come Hylemetriche, mostrando per altro, date le applicazioni PUF, l'ampiezza dell'applicabilità della teoria Hylemetrica.

7.6.3.1 Descrizione delle proprietà

Di seguito vengono mostrate le proprietà principali; si parte da una classificazione di una PUF come una procedura fisica di un interrogazione e relativa risposta. Si noti che implicitamente si sono già formulate due proprietà, ossia un'istanza di una PUF non può essere semplicemente un concetto astratto ma è sempre un'entità fisica (o parte della stessa), ed una PUF è una procedura (non strettamente una funzione) con alcune funzionalità di ingresso-uscita. Dal momento che queste proprietà sono fondamentali e sono immediatamente chiare vengono subito mostrate. Per brevità, si usa la notazione: Π: $X \rightarrow Y$, $\Pi(x) = y \rightarrow \Pi$ denota la funzione interrogazione-risposta di una PUF

Elencheremo di seguito le sette proprietà che sono sempre identificabili definendo una PUF, dandone una descrizione sintetica ma precisa.

- Valutabilità: data Π e x, è semplice valutare $y = \Pi(x)$.

  Da un punto di vista teorico, la semplicità della valutazione si traduce nella possibilità di esaurire il ciclo di valutabilità in un "tempo" polinomiale e in unica prova.

  Dal punto di vista pratico, la valutazione si traduce nell'impiego di risorse il più piccole possibile, ad esempio, nella temporizzazione, nell'area, nella potenza e nell'energia di un chip integrato.

Si noti inoltre che se una PUF è valutabile, è già implicitamente costruibile; chiaramente la valutabilità e fattibilità sono legate all'applicazione della stessa.

- Unicità: $\Pi(x)$ contiene alcune informazioni dell'identità dell'entità fisica Π che rappresenta.

  In senso teorico, se si considera una partizione di informazioni di un'istanza (o una classe di informazioni ben definita), l'informazione contenuta in una risposta PUF $\Pi(x)$ si lega alla partizione sulla base di questa risposta. Risposte consecutive consentono di avere partizioni sempre più piccole fino al raggiungimento di una partizione ottimale per una singola istanza, in questo caso il set di CRP considerato è identificato univocamente nella risposta PUF, come identificazione "possibile" o "non possibile"

  Si noti infatti che in base alla dimensione della partizione e delle caratteristiche delle risposte PUF, l'identificazione può essere possibile o non possibile.

  Una possibile misurazione dell'unicità che è eseguita nella maggior parte dei risultati è l'istogramma dell'inter-distanza, riassunta nel suo valore medio μinter.

- Riproducibilità: $y = \Pi(x)$ è riproducibile, con un margine di un piccolo errore.

  Le risposte alla stessa "interrogazione" x, della stessa PUF Π, devono essere vicine rispetto alla distanza metrica considerata. Per risultati sperimentali, la misura maggiormente usata è l'istogramma dell'intra-distanza, che può essere riassunto nella valutazione di μ_{intra}, a cui è anche legato il margine di accettabilità dell'errore.

- Inclonabilità: data Π, risulta difficile costruire una procedura Γ I= Π, tale che $\forall x \in X$: $\Gamma(x) \approx \Pi(x)$ a meno di un piccolo errore.

  E' la proprietà fondamentale delle PUF. In primis, quando si parla di clonazione Γ ci si riferisce ad una procedura, non necessariamente esclusivamente fisica, bensì anche matematica.

  Se è difficile trovare un'entità fisica che possa contenere un'altra PUF allora $\Pi\Gamma \neq \Pi$ (ove $\Pi\Gamma$ e Π sono due entità distinte anche se parti integranti di sistemi diversi) tale che $\forall x$ allora $\Pi\Gamma(x) \approx \Pi(x)$, ne segue che Π è fisicamente inclonabile. La difficoltà di produrre un clone fisico vale anche però per il produttore della PUF originale ed è per questa ragione che

si parla di resistenza di produzione.

Si noti che l'inclonabilità fisica e quella matematica sono proprietà fondamentalmente differenti, anche qualora si effettui una clonazione fisica non detto che sia possibile una matematica o viceversa.

Teoricamente affinché una PUF sia veramente inclonabile, Π deve essere necessariamente sia fisicamente che matematicamente inclonabile.

Praticamente, la clonazione pur essendo molto difficile non è impossibile, e la dimostrazione dell'inclonabilità è altrettanto complessa. L'unico sistema che può essere dimostrato è quello che usa la fisica quantistica (illustrato al Par. 7.6.4.5.4).

- Non-Predizione: dato solo un set Q = {(xi, yi = Π(xi))}, risulta difficile predire yc≈Π(xc) con un piccolo errore, per un interrogazione x_c randomica, cosi che $(x_c,\cdot) \notin$ Q. L'incapacità di riuscire a predire il comportamento di una PUF è legata all'inclonabilità. Se si è in grado di predire correttamente l'uscita di un'interrogazione randomica di una PUF solo dall'osservazione di un set di CRP, avendone accesso completo si riesce, in maniera più semplice a costruire un clone matematico.

  Ne segue che la prevedibilità implica clonabilità matematica e quindi clonabilità.

- Unidirezionalità: dati solo y and Π, è difficile trovare x cosi che Π(x) = y.
- Evidenza della contraffazione: alterando l'entità fisica inclusa in Π vi è la variazione di Π → Π' cosi che con molta probabilità ∃x ∈ X: Π(x) ≠ Π'(x).

  All'interno dei sistemi a "prova di manomissione", è possibile identificare sistemi per il quale la manomissione non mostra alcuna informazione e sistemi per cui la manomissione è possibile ma lascia un evidente traccia. Chiamiamo PUF ad evidente manomissione, quel sistema in cui in presenza di manomissione fra un entità fisica e un sistema integrato, si ha che il comportamento della CRP della PUF è modificato.

7.6.4 Applicazioni PUF

Di seguito vengono mostrate tutte le applicazioni assimilabili a strutture randomiche PUF presenti in letteratura. La lista di applicazioni PUF è suddivisa in una serie di categorie, basate principalmente sui principi costruttivi e di funzionamento.

Si riportano per completezza di informazione tutte le strutture note, alcune verranno descritte in maniera più accurata poiché più note e con maggiore documentazione, altre ancora in fase di studio da parte della comunità scientifica.

7.6.4.1 Puf "non-elettroniche"

Vengono analizzate le PUF con proprietà costruttive e/o operative non strettamente elettroniche. Si noti che comunque non vengono esclusi alcuni passaggi che impieghino tecniche digitali o elettroniche (es. memorizzazione dei dati). Pertanto per PUF non elettroniche si intendono tutte quelle PUF che hanno come natura dei componenti del sistema non-elettronici che contribuiscono a rendere la struttura randomica della PUF unica.

Alcune Puf sono già state citate in precedenza e vengono indicate in questa trattazione per mera completezza di informazioni.

7.6.4.1.1 PUF ottiche

Una prima versione di un sistema di identificazione non clonabile basata su un modello di riflessione ottico casuale, chiamato "Reflective Particle Tag", fu proposto prima dell'introduzione del concetto di PUF (Tolk, 1992). Tale sistema fu proposto per il conteggio di missili nucleari mobili atto alla riduzione delle armi strategiche nei trattati sul controllo degli armamenti. Tale sistema non ha poi trovato seguito a causa di uno mancato sviluppo hardware.

In seguito sono state proposte delle funzioni fisiche unidirezionali (POWF) (Pappu, et al., 2002), ancora in uso su supporti trasparenti. L'elemento centrale del progetto fu un reticolo ottico (optical token) che contiene una microstruttura ottica, costruita miscelando microscopiche (500μm) sfere di vetro rifrattivo in una piccola (10 × 10 × 2,54 mm) piastra epossidica trasparente. Il reticolo è quindi irradiato da un laser e il fronte d'onda emergente diviene molto irregolare a causa dello scattering multiplo del fascio con le particelle rifrattive; il pattern di speckle che ne de-

riva è catturato da una fotocamera CCD per un elaborazione digitale. A questo punto viene eseguito al pattern speckle osservato, un hash ottenuto con filtro di Gabor, alla stregua della procedura di estrazione delle caratteristiche biometriche. Il risultato è una stringa di bit che rappresentano il valore di hash. Si noti che, anche piccole variazioni nell'orientamento del fascio laser, portano ad un risultato del pattern di Speckle diverso e conseguentemente anche ad un hash diverso.

L'attuale PUF ottica non è altro quindi che un'interrogazione che descrive l'esatta orientazione del laser ed il hash ottenuto con filtro di Gabor del pattern di speckle registrato in uscita dal reticolo ottico (Optical token).

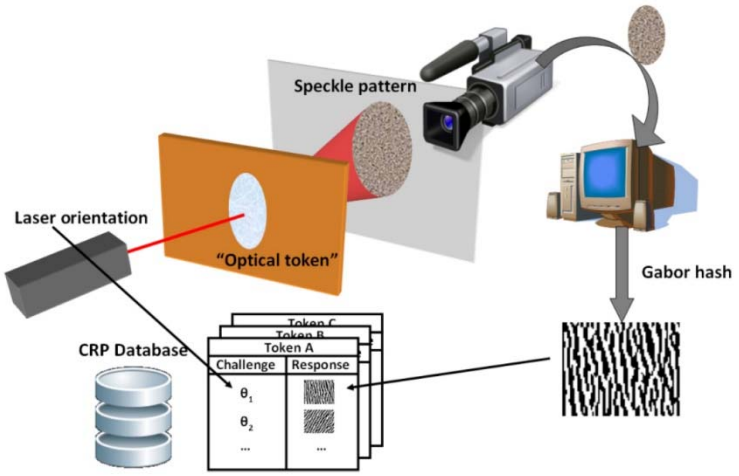


Figura 29 – Rappresentazione di un'implementazione base, con le operazioni di una PUF ottica

In letteratura sono presenti i risultati di un numero di esperimenti, eseguiti per verificare la performance di queste PUF (Pappu, et al., 2002).

La metodica eseguita è di seguito riportata: sono stati testati quattro reticoli mediante l'uso di 575 interrogazioni distinte. L'inter-distanza e l'intra-distanza misurate erano valutate dopo il hash con filtro di Gabor, ottenuto in uscita dal sistema. Il risultato è stato di un inter-distanza media pari a μ_{inter}=49.79% (σ_{inter}=3.3%) e un intra-distanza media di μ_{intra}=25.25% (σ_{intra} = 6.9%).

Mediante l'uso di un algoritmo CTW (Willems F.M.J., 1995), è stato stimato che mediamente in un hash con filtro di Gabor vi è un contenuto di entropia pari a 0,3 bit per pixel.

L'uso di una PUF ottica è in conclusione molto laborioso e richiede molto lavoro nella predisposizione del sistema laser e nel suo posizionamento.

7.6.4.1.2 PUF della carta

Come accennato nel paragrafo iniziale vi sono numerose proposte in letteratura inerenti lo studio di PUF nella carta. Sostanzialmente consistono semplicemente nella scansione della struttura della fibra della carta verificando l'unicità e la casualità sia di carte ad uso comune che più trattate. Le prime proposte (Bauder, 1983) (Commission on Engineering and Technical Systems (CETS), 1993) sono note in letteratura ben prima dell'introduzione del concetto PUF, anche se il primo vero articolo che introduce lo studio di alcune caratteristiche risale ai primi del 2000 (Buchanan, et al., 2005); principalmente le caratteristiche della carta, erano considerate come una strategia anti-contraffazione per banconote. In sostanza la riflessione di un raggio laser focalizzato sulla struttura della fibra irregolare di un documento cartaceo, viene utilizzato come impronta digitale di tale documento, rendendolo identificabile e non falsificabile.

Un approccio simile è usato (Bulens, et al., 2010) introducendo delle fibre sensibili all'ultravioletto nella carta durante il processo di fabbricazione, ciò ha consentito la misura e l'elaborazione mediante l'uso di uno scanner normale. L'acquisizione ottenuta collegata con una firma forte viene così posto sul documento, generando un'impronta digitale non modificabile.

7.6.4.1.3 CD PUF

Pur essendo un'applicazione non commerciale, ma più di tipo forense, in letteratura è presente uno studio effettuato sui CD che verifica la presenza della possibilità di ricavare una funzione PUF.

Le lunghezze delle "land" e delle "pit" di un cd contengono una deviazione casuale dalle loro lunghezze dovute variazioni intrinseche del processo di fabbricazione e registrazione da parte del masterizzatore. Inoltre, questa deviazione è abbastanza grande da essere osservata verificando il segnale elettrico del fotorivelatore in un normale lettore CD.

Dopo una procedura di quantizzazione, è presente in letteratura una misurazione che dà come risultato un inter-distanza media μ_{inter} = 8% e un intra-distanza media di μ_{intra} = 54% sulle stringhe di bit archiviate. Usando un metodo CTW, si stima che l'entropia contenuta nei bit estratti sia pari a 0.83 bit. (Hammouri, 2009).

7.6.4.1.4 RF-DNA

Dato un sistema che potrebbe essere assimilato ad un RFID, o più in generale un sistema con segnale in radio frequenza, si verifica la dispersione del campo vicino EM su dei filamenti di rame rispetto ad una banda di lunghezze d'onda diversa, in particolare nel 5 – 6 GHz. Gli effetti di scattering casuali sono misurati da uno scanner costituito da una matrice di antenne RF. L'entropia stimata per un sistema del genere è in almeno 50000 bit (Hammouri, 2009).

7.6.4.1.5 PUF magnetiche"

Le PUF magnetiche (Indeck & Muller, 1994) usano l'unicità intrinseca delle strutture e posizioni delle particelle nei supporti magnetici, ad esempio nelle tessere magnetiche. L'interesse per questa PUF è stato ampio sino a che la diffusione di carte con bande magnetiche era in espansione, gli studi sembravano poter prevenire le frodi con carta di credito (Magneprint, s.d.) o debito; oggi tale ricerche hanno assunto importanza minore visto l'evolversi tecnologico dei sistemi che prima utilizzavano sistemi magnetici.

7.6.4.1.6 PUF Acustiche

Le linee acustiche sono spesso delle componenti usate per ritardare il segnale elettrico. Consentono infatti la conversione di un segnale elettrico alternato in una vibrazione e viceversa. Le PUF acustiche sono costruite osservando lo spettro di frequenza di una linea acustica e sfruttandone i ritardi conseguenti (Vrijaldenhoven, 2005), in tal caso si parla di "linea di ritardo acustica". Dalla linea di ritardo viene estratta una stringa di bit e ne viene effettuata l'analisi di una componente principale, con una stima risultante di 160 bit di entropia. Il sistema sopra riportato presenta un FRR pari a 10^{-4} e un FAR di 10^{-5}

7.6.4.2 PUF Analogiche-Elettroniche

Verranno ora mostrate le PUF costruite su operazioni con misure analogiche di quantità elettriche o elettroniche.

7.6.4.2.1 PUF V_T

La prima tecnica che assegnava un unico identificativo ad ogni singolo passo di un circuito integrato, senza particolari processi o programmazione dopo la fabbricazione, fu chiamato ICID. Il sistema era composto da un numero di transistor con le medesime specifiche progettuali, i transistor venivano disposti in modo da formare una matrice indirizzabile.

Il transistor selezionato sulla matrice pilota un carico resistivo e a causa dei processi produttivi intrinsechi, le tensioni di soglia (threshold voltages) V_T risultano lievemente differenti; cosicché anche le correnti attraverso il carico risultano parzialmente randomiche. La corrente misurata sul carico viene convertita in una stringa binaria mediante un comparatore ad autoazzeramento.

Tale tecnica verificata su 55 chip prodotti in tecnologia CMOS (Lofstrom, et al., 2000) ha fornito una intra-distanza media μ_{intra} = 1,3%, mentre il valore medio di μ_{inter} risulta molto vicino al 50%.

7.6.4.2.2 Distribuzione di Potenza PUF

Un'altra proposta presente in letteratura si basa sulla variazione della resistenza del circuito elettrico di un chip. Furono misurate infatti le cadute di tensione e le resistenze equivalenti nel sistema di distribuzione di energia dei chip e si constatò che processi produttivi dei chip introducevano delle variabili non prevedibili. I risultati sperimentali delle resistenze equivalenti dei chip realizzati in tecnologia CMOS di 65 nm fornirono un valore di $\mu_{inter} \approx 1.5\Omega$ e un valore di $\mu_{intra} \approx 0.04\Omega$ (Helinski, et al., 2009).

7.6.4.2.3 Rivestimento PUF

Questo tipo di PUF considera le misurazioni randomiche della capacitanza nei sensori con sagoma a pettine posti nello strato metallico superiore di un circuito integrato.

Fu la prima PUF ad introdurre oltre alle variabilità intrinseche legate alla fabbricazione, elementi casuali esplicitamente introdotti mediante l'uso di rivestimenti dielettrici passivi posti diret-

tamente sulla parte superiore dei sensori. Il rivestimento inoltre era opaco e chimicamente inerte, offrendo quindi anche una protezione del sottostante rivestimento da agenti fisici esterni.

I test effettuati su 35 chip prodotti, cadauno con 31 sensori, hanno mostrato dopo la quantizzazione un elevato livello di casualità pari a $\mu_{inter} \approx 50\%$ e un basso rumore pari $\mu_{intra}<5\%$.

Valutazioni sperimentali hanno mostrato che tale tipologia di PUF evidenzia una notevole riduzione delle manomissioni, è stato eseguito infatti, nei confronti di questa PUF un tentativo di manomissione mediante l'uso di un fascio ionico focalizzato[9], il risultato è che a seguito di questo "attacco" le risposte PUF venivano significativamente modificate, mostrando il tentativo di manomissione.

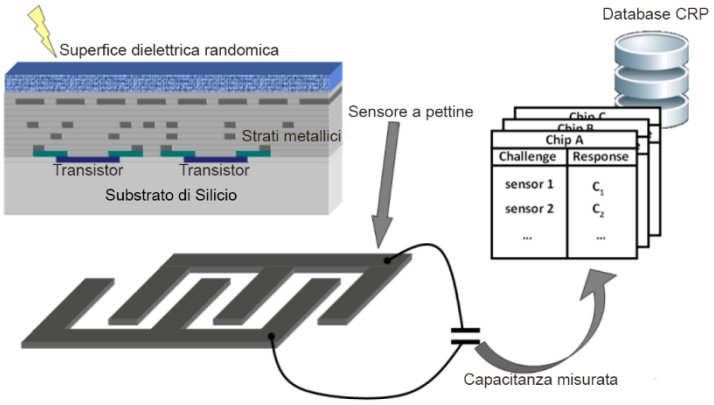


Figura 30 – Operazioni base di un rivestimento PUF.

A sinistra della figura è mostrata una sezione trasversale di un circuito CMOS integrato, a destra l'elaborazione del circuito come PUF.

7.6.4.2.4 LC PUF

Una PUF LC può essere costituita fisicamente da due lamine metalliche al cui centro vi è una lamina di vetro, formando quindi una capacità di dimensioni pari a 1 mm^2, connessa in serie ad una bobina metallica che funge da induttanza. Il sistema cosi formato è un circuito LC passivo che, se immerso in un campo RF, è in grado di assorbire una determinata quantità di energia (la quantità è ovviamente legata alla progettazione dei componenti).

[9] Noto pure come FIB, dall'inglese Focused Ion Beam è una tecnica usata particolarmente nei campi dei semiconduttori e delle scienze dei materiali per analisi puntualizzate, deposizioni, e ablazioni di materiali.

La frequenza di risonanza è legata ovviamente come accennato in precedenza alla scelta dei componenti ed intrinsecamente dei materiali stessi e dei processi di lavorazione, il picco di risonanza sarà pertanto differente anche con la scelta di componenti simili (impossibile avere componenti identici).

A questo punto è possibile delineare un analogia con le "PUF nel rivestimento" (Par. 7.6.4.2.3) nel modo procedurale ovviamente, e analogamente anche con la RF-DNA PUF (Par. 7.6.4.1.4) infatti anche per quest'ultima vi era la scansione del campo RF e rilevamento dell'assorbimento wireless.

Contrariamente alla RF-DNA PUF, la costruzione di una LC PUF è intrinsecamente una costruzione precisa e determinata di un circuito elettrico passivo e non di un posizionamento casuale di fili di rame.

Dati sperimentali presenti in letteratura hanno mostrano per i circuiti LC PUF una riproducibilità, ad una temperatura costante, del picco di risonanza sotto a 1 MHz ed un valore di entropia compresa fra 9-11 bit per circuito (Guajardo, et al., 2009).

7.6.4.3 Sistemi basati su ritardi intrinsechi delle PUF

Nei paragrafi precedenti (PUF "non-elettroniche e PUF Analogiche-Elettroniche) ci si basava su sistemi con parametri fisici randomici misurati analogicamente, che venivano poi quantizzati e che potevano essere usati per l'identificazione del sistema.

Di seguito verranno mostrati sistemi che assumono caratteristiche intrinsecamente PUF. Sebbene non esistano definizioni formali di PUF intrinseche, vi sono due requisiti che consentono di considerare una PUF tale:

- La PUF, inclusa la strumentazione di misura, dovrebbe essere completamente integrata nel dispositivo di cui fa parte.
- La costruzione di una PUF dovrebbe consistere in strutture basilari definite "primitive" che dovrebbero essere disponibili durante il processo di produzione del dispositivo in cui dovrà essere integrata.

La prima condizione implica che il dispositivo possa interrogare e leggere la PUF senza l'ausilio di strumentazione esterna e senza la necessità di usare "interrogazioni" e relative risposte al di fuori del dispositivo stesso. Si noti che questa condizione potrebbe essere verificata anche per le PUF mostrate nei paragrafi, un esempio sono le PUF del rivestimento o le PUF ottiche integrate.

La seconda condizione implica che la costruzione completa di una PUF avvenga senza ulteriori aumenti dello spazio fisico, se non quelli necessari alla costruzione della PUF medesima; per esempio non dovranno essere necessari altri processi produttivi o essere necessari componenti specializzati. Questa seconda condizione esclude quindi le PUF rivestimento e le PUF ottiche integrate dalle PUF intrinseche, in quanto entrambe necessitano di fasi di lavorazione altamente specializzate.

In letteratura vi sono già un consistente numero di PUF intrinseche, il tutto su circuiti integrati digitali. Il grande vantaggio di una PUF integrata su un chip digitale è che le risposte PUF possono essere usate direttamente da altre applicazioni in esecuzione sullo stesso dispositivo.

Si distinguono quindi due classi diverse di PUF intrinseche, PUF intrinseche basate sulla misurazione del ritardo digitale e PUF intrinseche basate sulla stabilizzazione di elementi di memoria (più avanti discussi).

7.6.4.3.1 PUF ad arbitraggio

La prima idea di una PUF che sfruttasse l'arbitraggio, introduceva delle condizioni di collegamento su due piste di un chip e creava un circuito detto di arbitraggio che sceglieva quale dei due circuiti doveva essere impiegato. Se le due piste sono progettate simmetricamente in teoria dovrebbero presentare ritardi uguali, l'uscita non dovrebbe in teoria presentare anticipo/ritardo fisso. Durante la produzione del chip, vi sono però delle variazioni rispetto al processo di fabbricazione che avranno un effetto sui parametri fisici, e che quindi consentiranno di determinare l'esatto ritardo di ciascun percorso, provocando quindi un piccola deviazione casuale tra i due ritardi.

Se la deviazione è molto piccola, il tempo di settaggio del circuito di arbitraggio potrebbe essere violato, e la relativa uscita potrebbe non essere più legata alle "regole" legate alla conduzione sulle piste. La causa di questo fenomeno è presumibilmente imputabile al rumore randomico pre-

sente nel sistema. Questo fenomeno è chiamato metastabilità dell'arbitraggio e introduce il rumore nelle risposte delle PUF.

Il primo progetto di PUF ad arbitraggio (Lee, et al., 2004) (Lim, 2004) usava due blocchi per la commutazione, al fine di creare due percorsi simmetrici, ed un latch (o un flip-flop) per implementare il circuito di arbitraggio. I blocchi di commutazione presentavano ognuno due ingressi e due uscite, collegate direttamente o commutate, e si basavano su un numero predeterminato di bit.

Il collegamento in serie fra più blocchi di commutazione crea due linee di ritardo parametrizzabili che si immettono nel sistema di arbitraggio. In questo caso è possibile asserire che il settaggio dei blocchi di commutazione rappresenta l'interrogazione della PUF e la risposta della PUF l'uscita dal sistema di arbitraggio.

Si consideri che il numero delle possibili "interrogazioni" è esponenziale al numero di blocchi che si decide di usare.

La costruzione base di una PUF di questo tipo è riportata nell'immagine sottostante

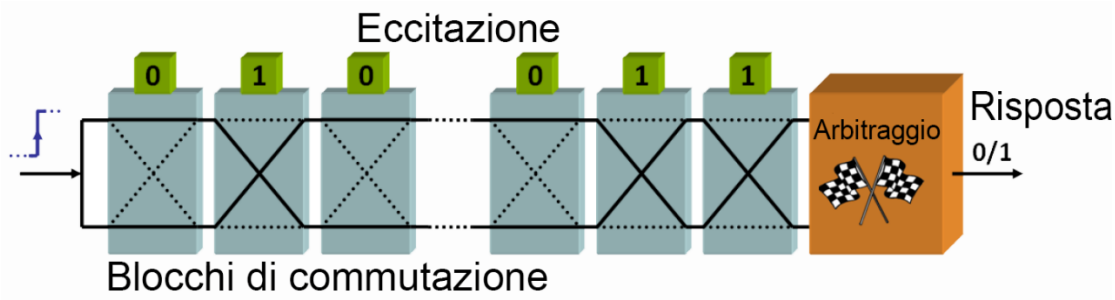


Figura 31 – Operazioni base di una PUF ad arbitraggio

Questa implementazione fu eseguita successivamente sui ASIC[10], collegando 64 blocchi di commutazione. L'esperimento, presente in letteratura, fu effettuato su 37 chip mostrando un valore di μ_{inter}=23% ed un valore di μ_{intra}<5%, anche con considerevoli variazioni di tensione di alimentazione e temperatura. Test equivalenti effettuati sulle FPGA hanno mostrato un livello di caratteristiche randomiche notevolmente minori (μ_{inter}=1,05% e μ_{intra}=0,3%), ciò è dovuto presumibilmente ai vincoli di instradamento dei dati intrinsechi nell'architettura delle FPGA.

[10] ASIC: application specific integrated circuit - è un circuito integrato creato appositamente per risolvere un'applicazione di calcolo ben precisa (specific purpose).

Considerando l'introduzione di un ritardo base delle PUF, tenuto conto che il ritardo digitale è additivo per natura; il ritardo di blocchi di commutazione sarà quindi la somma dei ritardi dei singoli blocchi.

Questa osservazione ha portato a verificare, che data l'osservazione di predeterminato numero di query CRP, si è in grado di predire la risposta ad un interrogazione, con una precisione relativamente alta. Questa condizione ha portato a consentire un "attacco" a questa tipo di PUF, condotto su una PUF ad arbitraggio di tipo basico, usando una tecnica di apprendimento automatico, ed ottenendo un errore di predizione del 3,55% con un'osservazione di 5000 CRP su un sistema ASIC, ed un errore di predizione del 0,6% per un campione di 90000 CRP per le FPGA.

Il successivo lavoro sulle PUF ad arbitraggio è fondamentalmente un tentativo di creare un modello che fosse più difficile e resistente agli attacchi; il cuore della ricerca è indirizzata all'introduzione di non linearità nei ritardi e processi di controllo e/o limitazione degli ingressi e delle uscite delle PUF.

Le PUF ad arbitraggio Feed-forward (Lim, 2004) sono state un primo tentativo di introdurre delle non linearità nelle linee di ritardo delle PUF. Tale tipologia di PUF sono un estensione delle PUF ad arbitraggio, alcuni bit dell'ingresso non sono impostati a priori ma sono il risultato di arbitraggi intermedi valutati con la stessa distanza e con stessi ritardi. Le PUF Feed-forward sono state testate su sistemi ASIC con risultati pari a μ_{inter}=38% e μ_{intra}=9,8%.

Si noti che le risposte ottenute sono molto rumorose, ciò è dovuto probabilmente ad un aumento della metastabilità dovuta dalla presenza di più arbitraggi.

Attacchi effettuati a PUF con arbitraggi semplici, non sono risultati efficaci per PUF con arbitraggi "non-lineari".

Tuttavia, risultati successivi (Majzoobi, et al., 2008) (Ruhrmair, et al., 2009) mostrano che con tecniche di modellazione più avanzate è possibile costruire un modello di PUF ad arbitraggio feed-forward ancora più accurato, con un errore di predizione su singolo progetto pari a meno del 5% per un valore superiore di 49000 CRP.

Ulteriori studi sono stati condotti per la costruzione di una PUF ad arbitraggio che sia sicura su una FPGA (Majzoobi, et al., 2009) (Ruhrmair, et al., 2009), tali studi si basano su uno stato inizia-

le che consiste in una caratterizzazione del sistema mediante l'uso della riconfigurabilità delle FPGA.

Per aumentare la randomicità e impedire la costruzione di un modello con cui effettuare gli attacchi, il sistema usa una rete con ingressi ed uscite difficilmente invertibili e ingressi e uscite delle PUF controllabili, con un aumento della sicurezza attraverso l'uso della crittografia. La predizione d'errore per il sistema di cui sopra assume un valore del 1,3% su 50000 CRP osservate durante le simulazioni.

7.6.4.3.2 Oscillatore ad anello PUF

L'oscillatore ad anello PUF (Gassend, et al., 2002) (Gassend, 2003) usa un differente approccio nella misurazione della deviazione del ritardo randomico causato dalle variabilità dei processi produttivi. L'uscita di una linea digitale con ritardo viene invertita e retroazionata al suo ingresso, creando così un ciclo asincrono oscillante, chiamato anche anello oscillatore. La frequenza di questo oscillatore è determinata proprio dal ritardo della linea digitale. Misurare la frequenza è dunque equivalente a misurare il ritardo; a causa dei processi produttivi i ritardi risultano variabili, l'esatta frequenza sarà parzialmente randomica e dipendente dal dispositivo.

La misurazione della frequenza viene effettuata abbastanza semplicemente mediante l'ausilio di componenti digitali: un rilevatore d'onda verifica la salita dell'onda in un oscillazione periodica e un contatore digitale verifica il numero di onde in un periodo di tempo. Il contatore pertanto contiene tutti i dettagli della misurazione effettuata ed è considerata come la risposta PUF. Se la linea di ritardo è parametrizzabile come per una PUF ad arbitraggio semplice, il settaggio di un particolare ritardo è considerata l'interrogazione della PUF.

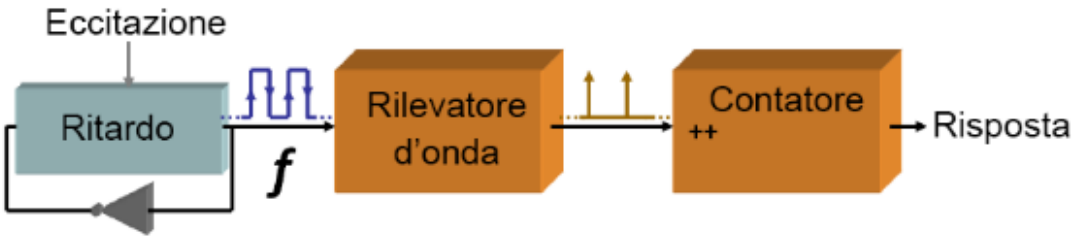


Figura 32 – Operazioni base di un oscillatore ad anello PUF

Come già accennato in precedenza alcuni parametri ambientali possono modificare le risposte PUF (Par.7.6.2). Durante di misurazioni di ritardi su un circuito integrato, la temperatura di giunzione e la tensione di alimentazione influenzano fortemente il valore del ritardo. Nel caso delle PUF ad arbitraggio, questo effetto non è così grande, poiché vi è una misura differenziale fra i due percorsi paralleli del ritardo. Per gli oscillatori ad anello PUF, questo effetto è reso più grande a causa della compensazione necessaria. Per ovviare a questa problematica, vi sono due soluzioni (Gassend, et al., 2002) (Gassend, 2003) che consistono nel dividere il valore del contatore in due misurazioni simultanee, che portano a risposte più robuste.

La prima tecnica sotto riportata mostra un oscillatore ad anello PUF con compensazione a divisione su 4 dispositivi FPGA; a 25°C si ottiene un valore di $\mu_{inter} \approx 10*10^{-3}$ e $\mu_{intra} \approx 10*10^{-3}$. La variazione della tensione di alimentazione aumenta il valore di μ_{intra} di $0{,}003*10^{-3}$ per ogni mV.

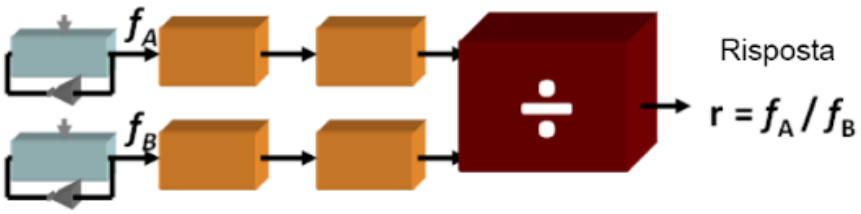


Figura 33 – Oscillatore PUF ad anello con compensazione a divisione

Come si può notare il circuito di ritardo è uguale alle PUF ad arbitraggio "semplici" pertanto suscettibili ad attacchi di tipo "model-building". Inoltre esiste un elevata correlazione, sia tra la risposta proveniente dalla stessa interrogazione di differenti FPGA che risposte provenienti dalla stessa FPGA ma con differenti interrogazioni.

La seconda tecnica applicata (Suh & Devadas, 2007), pur mantenendo la stessa tecnica di misurazione dei fronti di risalita delle onde, usa un circuito diverso con ritardo fisso.

Un numero di oscillatori con lo stessa frequenza prevista, sono implementati in parallelo. L'interrogazione inviata alla PUF seleziona una coppia di oscillatori e la risposta è il prodotto. Questa soluzione risulta semplice e poco costosa

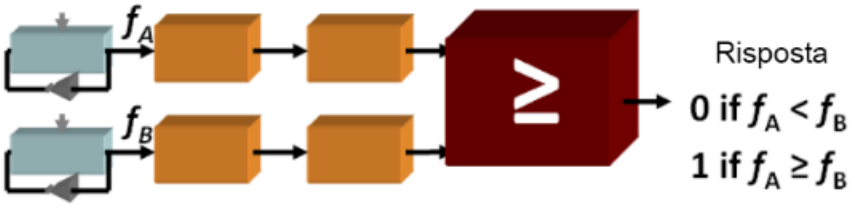


Figura 34 – Oscillatore PUF ad anello con compensazione a comparatore

Valori sperimentali (Suh & Devadas, 2007) effettuati su 15 FPGA con 1024 loop per FPGA, mostrano valori di μ_{inter} = 46.15% ed un valore μ_{intra} = 0.48%. Si noti che tali valori sono stati ottenuti con una tecnica chiamata "1-out-of-8 masking", che considera solo le risposte stabili di 8 coppie di loop.

7.6.4.4 Memorie basate su PUF

Di seguito verrà illustrato un altro tipo di PUF intrinseca, che si basa sullo stato di stabilizzazione della memoria digitale.

Una cella di memoria è tipicamente un circuito digitale con uno o più stati logici stabili. Restando in uno degli stati stabili è possibile registrare le informazioni; non è noto a priori invece il comportamento se il sistema va in uno stato instabile; è possibile in questo caso che inizi una oscillazione fra stati instabili o che converga su uno stato stabile. In quest'ultima condizione si è osservato che alcune celle preferiscono fortemente alcuni stati stabili rispetto ad altri. Inoltre, questo effetto non può essere spesso spiegato con l'implementazione logica di una cella, ma risulta legato a difetti nella fisica intrinseca, ad esempio causata da variazioni durante i processi produttivi, che svolgono quindi in questo caso un ruolo importante.

Per questa ragione, la durata di uno stato stabile in una cella di memoria instabile è un fattore che la rende una buona candidata in qualità di risposta PUF.

Di seguito verranno mostrate differenti proposte presenti in letteratura che si basano su basano su celle di memoria quali celle SRAM, latch dati e flip-flop

7.6.4.4.1 SRAM PUF

La SRAM PUF fu proposta quasi simultaneamente da due gruppi di ricercatori (Guajardo, et al., 2007) (Holcomb, et al., 2007), anche se con modalità differenti. La SRAM (Static random-access memory) è un tipo di memoria digitale che consiste di celle ognuna capace di memorizzare un numero binario.

Una cella SRAM, è costituita da un circuito retroazionato formato da due invertitori logici le cui uscite sono collegate alle due estremità alle linee dei dati tramite due transistor detti porte di trasmissione, come noto una SRAM presenta due stati stabili.

La tecnologia CMOS, implementa una cella SRAM con 4 MOSFET, e ulteriori 2 MOSFET per la lettura/scrittura.

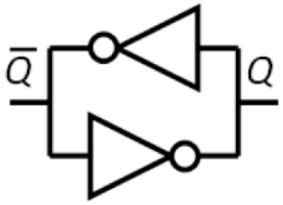


Figura 35 – Circuito Logico di una SRAM (PUF)

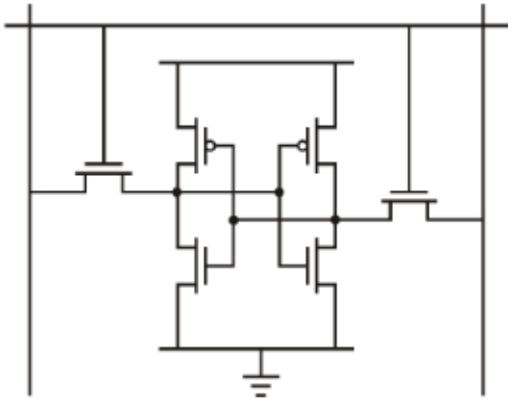


Figura 36 – Circuito elettrico di una cella SRAM (PUF) in tecnologia CMOS

Per ragioni di prestazione, i disallineamenti fisici tra le due metà simmetriche del circuito (ciascuna implementa un inverter) viene mantenuto il più piccolo possibile. Non è chiaro in che stato la cella si troverà subito dopo l'accensione del circuito e l'attivazione della stessa in qualità di memoria. Alcune celle "preferiscono" all'atto dell'attivazione memorizzare uno zero, altre un uno, alcune non hanno una reale preferenza, ma la distribuzione di queste tre tipi di cella di memoria è completamente casuale.

Come si è visto, la mancata corrispondenza fisica nella cella, causato dalla variabilità dei processi di produzione della stessa, determina il comportamento durante l'accensione della cella. Si

impone ad una cella lo zero od un uno durante l'accensione a seconda del segno del disallineamenti. Se lo squilibrio è molto piccolo, lo stato di accensione è determinato dal rumore stocastico.

Esperimenti su questa PUF, hanno dimostrato che l'accensione di 8190 byte di SRAM di differenti blocchi di memoria FPGA, danno un inter-distanza media tra due blocchi pari a μ_{inter} = 49,97% e intra-distanza media entro misurazioni multiple di un singolo blocco pari μ_{intra} = 3,57% con temperatura costante e μ_{intra} <12% per grandi variazioni di temperatura. La stima pertanto dell'entropia degli stati di accensione di una SRAM è 0,76 bit per cella SRAM.

Il comportamento dell'accensione delle celle SRAM di due sistemi composti da 5120 blocchi di celle da 64 SRAM misurati su 8 chip SRAM commerciali, hanno dato un valore di μ_{inter}=43,16% and μ_{intra}=3,8%; per 15 blocchi di celle SRAM incorporati in microcontrollori di chip i valori misurati sono stati di μ_{inter} = 49.34% and μ_{intra} = 6.5%.

In generale però poiché sulle FPGA più comuni, tutte le celle SRAM sono difficilmente resettabili a zero subito dopo l'accensione, la casualità è di difficile realizzabilità.

Un altro inconveniente delle SRAM PUF è che è necessaria la presenza di un dispositivo di accensione per consentire la generazione della risposta e ciò potrebbe non essere sempre possibile.

7.6.4.4.2 Butterfly PUF

Il comportamento di una cella SRAM è simulato da una FPGA a logica riconfigurabile fatta da latch ad accoppiamento incrociato.

Sotto viene riportata una rappresentazione schematica di una cella Butterfly PUF.

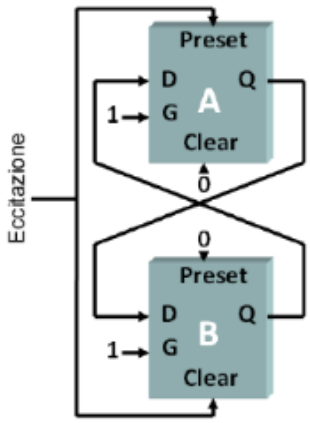


Figura 37 – Circuito di una cella Butterfly PUF

Anche in questo caso il circuito è dotato di due stati logici stabili. Tuttavia, utilizzando le funzionalità clear/preset dei latch, è possibile indurre uno stato instabile dopo che il circuito converge ad uno dei due stati stabili, condizione questa comparabile all'avvio di una cella SRAM ma senza la necessità di avviare la stessa realmente.

Lo stato si stabilizzazione di una cella butterfly PUF è determinata dalla mancanza di corrispondenza fra i latch e le interconnessioni dell'accoppiamento incrociato.

A causa delle opzioni di instradamento delle FPGA, non è semplice però implementare una cella con un disallineamento in fase di progettazione piccolo, che non generi un instabilità tale da rendere inutilizzabile il circuito.

Inoltre la condizione di disallineamento è una condizione necessaria all'impiego delle caratteristiche di variabilità; questo se si vuole che la mancanza di corrispondenza delle interconnessioni, dovute alla variabilità dei processi di fabbricazione, abbia effetto.

I risultati delle misurazioni in condizioni di grande variazioni di temperatura di 64 celle Butterfly PUF in 36 FPGA danno un rendimento pari a $\mu_{inter}\approx 50\%$ e $\mu_{intra}<5\%$. (Kumar, et al., 2008)

7.6.4.4.3 Latch PUF

Con latch PUF si identifica una tecnica di identificazione (Su, et al., 2007), che usa due porte NOR ad accoppiamento incrociato, come mostrato in figura sotto, che costituiscono un latch NOR.

Per impostare un segnale di reset, il latch diventa instabile e ancora converge ad uno stato stabile a seconda del disallineamento interno tra i componenti elettronici.

Equivalentemente alla SRAM PUF e alla butterfly PUF, questa struttura può essere usata per costruire una PUF. Esperimenti su 128 NOR latch implementati su 19 ASIC prodotti in tecnologia CMOS a 0.130μm con un rendimento di $\mu_{inter} = 50.55\%$ e $\mu_{intra} = 3{,}04\%$.

7.6.4.4.4 Flip-flop PUF

Equivalentemente alla SRAM PUF, il comportamento della regolarità di accensione dei flip-flop può essere studiato e per 4096 flip-flop di 3 FPGA si ha $\mu_{inter} \approx 11\%$ e $\mu intra < 1\%$.

7.6.4.5 PUF – Sistemi integrativi, Prospettive e studi in atto

Di seguito, verranno illustrate una serie di concetti proposti in letteratura, che sono strettamente legati alle PUF. Vi sono delle proposte concrete di PUF prive di implementazione e su cui non vi è ancora conferma di fattibilità.

7.6.4.5.1 Chiavi offuscate fisicamente (POK - Physically Obfuscated Keys)

Il concetto di chiave offuscate fisicamente o POK è stato introdotto da Gassend (Gassend, 2003) ed è stato generalizzato per tutti gli algoritmi offuscati fisicamente da Bringer (Bringer, et al., 2009).

Il concetto di base di una POK è che una chiave è memorizzata in modo permanente in un modo fisico anziché digitale, ciò rende difficile per un malintenzionato forzare la chiave con un "attacco". Inoltre, un attacco invasivo sul dispositivo atto a memorizzare una nuova chiave dovrebbe distruggere la precedente rendendo però impossibile l'uso del dispositivo, fornendo quindi una chiara indicazione di manomissione. POK e PUF sono concetti molto simili, le POK possono essere costruite a partire da una PUF e viceversa.

7.6.4.5.2 Puf controllata – CPUF

Una PUF controllata - CPUF, è di fatto una modalità di operare di una PUF combinata con altre operazioni base (per esempio la crittografia) Una PUF è detta controllata se è possibile accedervi solo mediante l'uso di un algoritmo, ed è fisicamente legata in modo inseparabile a questo. Un tentativo di rompere il legame fra la PUF e l'algoritmo di accesso deve condurre alla distruzione della PUF con conseguente segnale di tentativo di infrazione al sistema.

Avere una CPUF rispetto ad una Puf normale ha dei vantaggi:

- Una funzione crittografica hash, scelta con accuratezza, usata per generare le risposte PUF può prevenire un attacco chosen-challenge[11].

[11] Attacco chosen-challenge: Attacco che si focalizza sulla generazione dei flussi di un algoritmo crittografico (per esempio nelle SIM card). L'attacco usa il flusso della funzione di Hash per dedurre la chiave segreta; l'attacco costruisce un numero di chosen-challenge speciali e le invia al sistema, che le applica alla chiave segreta e alla chosen-challenge, dandone una risposta. Dall'analisi della risposta, è possibile che si possa risalire al valore della chiave segreta.

- Algoritmi di correzione degli errori attuati sulle PUF portano a misure delle risposte finali molto più affidabili, riducendo la probabilità di errori in risposta virtualmente a zero.
- Una funzione hash applicata alle uscite con errore corretto spezza efficacemente il legame tra le risposte ed le caratteristiche fisiche associate alla misura PUF. Questo rende gli attacchi model-building molto più difficile.

La funzione Hash che genera un'interrogazione PUF può assumere più ingressi, per esempio permette l'associazione di una PUF a più persone, questa condizione potrebbe essere di interesse in impieghi in cui è richiesto un livello adeguato di privacy, consentendo quindi di non essere tracciati.

Risulta quindi chiaro che avere una CPUF anziché una PUF aumenta la sicurezza, ciò ovviamente è legato all'uso dei protocolli scelti.

La maggiore sicurezza di un CPUF dipende fortemente dal collegamento fisico della PUF con gli algoritmi di accesso che possono essere molto arbitrari ciò costituisce un punto debole di una CPUF.

7.6.4.5.3 PUF riconfigurabili

Le PUF riconfigurabili o rPUFs (Kursawe, et al., 2009) hanno come idea di base quella di estendere il comportamento di una CRP regolare di una PUF base con un'operazione aggiuntiva denominata riconfigurazione. Questa riconfigurazione ha come effetto che il comportamento CRP della PUF risulta casuale ed irreversibilmente cambiato; quindi porta ad un nuova PUF.

Sono quindi state proposte dagli ideatori della rPUF, due possibili implementazioni legate al meccanismo di riconfigurazione fisico della casualità nel PUF.

La prima implementazione è un'estensione delle PUF ottiche; un fascio laser ad alta intensità scioglie in breve tempo il supporto ottico, causando un riallineamento dei diffusori ottici, che portano ad un nuovo comportamento casuale della CRP.

La seconda implementazione si basa su una tecnica di archiviazione non-volatile chiamata "memoria a cambiamento di fase". La fase di scrittura su tale tipologia di memoria consiste in un'alterazione fisica della fase di una piccola cella da cristallina ad amorfa o fasi intermedie, memoria che viene letta misurando la resistenza della cella. Poiché le misurazioni finali della resi-

stenza sono più accurate rispetto all'accuratezza della scrittura, il valore delle resistenze misurate possono essere utilizzate come risposte PUF; la riscrittura delle celle pertanto le cambierà in modo casuale.

Entrambe le proposte non sono ancora state testate sono pertanto state riportate per completezza.

7.6.4.5.4 PUF a lettura quantica

Le PUF a lettura quantica (Skoric, 2009) rappresenta un estensione quantica di una PUF regolare.

Viene proposta la sostituzione dell'interrogazione e delle risposte di una PUF con stati quantici.

Viste le proprietà degli stati quantici, un malintenzionato non può intercettare le interrogazioni senza cambiare le relative risposte. Questa cosa ha il vantaggio di consentire al meccanismo di lettura della PUF di non essere più prevedibile, che è il problema della maggior parte delle PUF non quantiche.

Fino ad ora, la fattibilità di questa proposta non è stata verificata. Inoltre, non è chiaro se PUF attualmente esistenti possano essere facilmente estese e sia possibile accettare e produrre stati quantistici.

7.6.4.5.5 Sistemi SIMPL

Questo tipo di PUF, di cui vi è pochissima letteratura ha come idea l'utilizzo delle PUF come parte dell'algoritmo della chiave pubblica. E' detto SIMPL (SIMulation Possible but Laborious) fu proposto da Ruhrmair (Ruhrmain, 2009).

In pratica un sistema S è chiamato SIMPL se rispetta le seguenti condizioni:

1. È possibile elaborare numericamente, quindi, prevedere, il comportamento fisico di S con una precisione molto elevata. La base della simulazione è una funzione descrittiva D(S), e un generico algoritmo di simulazione Sim, entrambi noti pubblicamente.
2. Qualunque simulazione numerica sufficientemente accurata, nonché qualsiasi emulazione fisica arbitraria di S, è più lenta rispetto al comportamento in tempo-reale di S.

3. Riprodurre fisicamente o clonare S deve essere difficile.

Associando il concetto della crittografia a quanto affermato, è possibile considerare la funzione D(S) come chiave pubblica, mentre il sistema fisico S chiave privata.

La chiave privata, è una struttura fisica irriproducibile, che non contiene informazioni segrete al suo interno. L'utilizzo di chiavi crittografiche irriproducibili porta ad un significante vantaggio in termini di sicurezza.

Esistono due proposte per l'implementazione di un sistema SIMPL basate su circuiti elettrici integrati

La prima, una memoria SRAM basata su nuovo sistema "skew", che sfrutta celle di memoria fuzzy con operazionali ad alta variazione di tensione

La seconda proposta è una rete analogica non lineare cellulare (Cellular NonLinear Networks - CNN), che si sviluppa nel tempo in un convertitore analogico, altamente parallelo.

Questo può permettere ad architetture classiche ad avere performance migliori su operazioni computazioni, come richiesto dai sistemi SIMPL.

7.6.4.5.6 PPUF

Un concetto similare al SIMPL è la Public PUF – PPUF (Beckmann & Potkonjak, 2009). Una PPUF è una PUF che è creata in modo che, la simulazione è fattibile, ma richiede un alto tempo di elaborazione anche in presenza di un'ampia risorsa computazionale. La PPUF, sviluppa concettualmente un nuovo scambio di chiavi segrete e protocolli di chiave pubblica che è resistente contro attacchi di tipo fisico e "side channel" e non richiede ipotesi matematiche non dimostrate.

Sia i sistemi SIMPL che i sistemi PPUF si affidano a sistemi (PUF) che possono essere modellati, ma per i quali la valutazione del modello è molto laboriosa e richiede inoltre una quantità di tempo per la valutazione del sistema base alias la PUF di base.

7.6.5 Schema riepilogativo delle PUF

Vengono mostrate nella tabella sottostante le principali peculiarità delle PUF nei sistemi sin qui analizzati.

PUF	Randomicità	Interrogazione	Risposta	μ_{inter}	μ_{intra}	Entropia
PUF Ottiche	Introdotta esternamente	Orientamento Laser	Da Hash Gabor Pattern Speckle	49.79%	25.25%	0.3 bit/pixel
PUF Superficiale	Introdotta esternamente	Selezione del Sensore	Misura della capacità quantizzata	≈ 50%	< 5%	6.6 bit/sensor
Arbitraggio a PUF	Variazione legata ai processi produttivi.	Settaggio linee di ritardo	Decisione arbitraggio	23%	< 5%	Non nota
Arbitraggio PUF Feed-forward	Variazione legata ai processi produttivi.	Settaggio linee di ritardo	Decisione arbitraggio	38%	9.8%	Non nota
Oscillatore PUF ad anello	Variazione legata ai processi produttivi.	Settaggio linee di ritardo	Contatore a divisione compensato	≈ 1%	≈0.01%	Non nota
Oscillatore PUF ad anello con comparatore	Variazione legata ai processi produttivi.	Selezione coppie di Loop	Contatore a comparatore	46.14%	0.48%	Non nota
SRAM PUF	Variazione legata ai processi produttivi.	Indirizzi della SRAM	Stato di accensione di una cella SRAM	49.97%	< 12%	0.76 bit/cell
Latch PUF	Variazione legata ai processi produttivi.	Selezione del Latch	Stato di stabilizzazione di un latch NOR instabile	50.55%	3.04%	Non nota
Butterfly PUF	Variazione legata ai processi produttivi.	Selezione della cella Butterfly	Stato di stabilizzazione di una cella instabile	≈ 50%	< 6%	Non nota

Tabella 8 − Comparazione fra le principali caratteristiche delle PUF.

7.6.6 Proprietà comuni alle PUF

Nella tabella sottostante, sono riportate e tabellate schematicamente tutte le proprietà di una PUF

	PUF Ottiche	PUF Superficiale	Arbitraggio a PUF	Arbitraggio PUF Feed-forward	Oscillatore PUF ad anello	Oscillatore PUF ad anello con comparatore	SRAM PUF	Latch PUF	Butterfly PUF	TRNG[12]	Protocollo ID	Chiave Pubblica
Valutabilità	√[1]	√[1]	√	√	√	√	√[2]	√	√	√	√	√
Unicità	√	√	√	√	√	√	√	√	√	√	√[3]	√[3]
Riproducibilità	√	√	√	√	√	√	√	√	√	×	√	√
Inclonabilità Fisica	√	√	√	√	√	√	√	√	√	√	×[4]	×[4]
Inclonabilità Matematica	√	×[5]	×[6]	×[6]	×[5]	×[5]	×[5]	×[5]	×[5]	√	×[7]	×[7]
Non-Predizione	√	√	![8]	![8]	![8]	√	√	√	√	√[9]	×	√
Unidirezionalità	?	×[10]	×[11]	×[11]	?	×[11]	×[11]	×[11]	×[11]	×	×	×
Evidenza della contraffazione	√	√	?	?	?	?	?	?	?	?	×[12]	×[12]

√ si indica che viene riscontrata la singola proprietà; × proprietà non applicabile;

! proprietà applicabile sotto alcune condizioni; ? proprietà non ancora verificata

[12] TRNG: True Random Number Generators, è un generatore di numeri casuali realizzato da un dispositivo di calcolo ed ha come fonte di generazione un fenomeno fisico, è progettato quindi per generare in maniera indipendente una sequenza di numeri o simboli senza alcun modello.

1. Richiede ulteriori processi produttivi e/o apparati di misurazione esterni.
2. Richiede accensione dell'apparato.
3. Richiede la programmazione di una identificazione forte o una chiave.
4. La clonazione fisica di una identificazione forte o una chiave è più semplice.
5. Per queste PUF, è possibile creare un clone matematico con la lettura esaustiva di tutte le CRP in uscita.
6. Per queste PUF, è possibile creare con un attacco model-building un clone matematico
7. Un malintenzionato che è in possesso dell'identità/chiave privata può semplicemente forzare un identificazione/firma valida
8. Queste PUF divengono sempre più semplice al crescere delle CRP note.
9. Imprevedibilità è un requisito fondamentale per una buona TRNG.
10. Poiché queste PUF presentano un numero ridotto di "interrogazioni" con probabilità non da escludere sarà possibile invertire la risposta
11. Poiché l'uscita di queste PUF è basilarmente pari a 1 bit, un'interrogazione randomica potrà essere invertita dà una risposta PUF, con una probabilità ≈ 50%.
12. Se non vi sono ulteriori protezioni anti-manomissione, identificazioni programmate e chiavi forti non sono evidenti alla manomissione.

Tabella 9 – Tabella riassuntiva delle proprietà delle PUF.

Guardando la tabella sopra è possibile notare che la valutabilità e l'unicità, è riscontrata in tutte le applicazioni. Ciò significa che sono proprietà PUF necessarie seppur non sufficienti, poiché permettono un identificazione programmata, la firma con chiave pubblica e il TRNG. La terza proprietà, la riproducibilità, esclude il TRNG.

La proprietà principale, l'inclonabilità fisica differenzia completamente le PUF in virtù di quelle basate sull'identificazione unica programmata o identificazione a chiave.

Unidirezionalità non sembra essere una buona proprietà PUF, nessuna PUF raggiunge a pieno questa proprietà.

Anche per le PUF ottiche, che sono considerate unidirezionali, l'invertibilità non è teoricamente impossibile.

L'inclonabilità matematica è una proprietà irraggiungibile per la maggior parte delle PUF. Tuttavia, tale proprietà può essere notevolmente migliorata trasformando le PUF base in PUF controllate, per esempio per prevenire attacchi read-out e attacchi model-building.

In finale, anche quella che si credeva essere il principale vantaggio della tecnologia PUF, l'evidenza di manomissione è stata verificata sperimentalmente per le (non-intrinseche) PUF ottiche e il rivestimenti PUF.

7.6.7 PUF - Considerazioni

In questa parte, si è cercato di esporre in modo completo le peculiarità delle PUF. Come emerso nella trattazione le PUF sono funzioni fisiche non clonabili; funzioni non in modo rigorosamente definito. Le PUF sono da considerarsi come una raccolta di costruzioni funzionali che soddisfano una serie di qualità; qualità comparabili che portano ad un sottoinsieme comune incentrato sulla proprietà di inclonabilità fisica.

Per le loro proprietà, sono da considerarsi come parte integrante dell'Hylemetria. Il loro impiego si è dimostrato in forte aumento e con studi da parte dell'intera comunità scientifica sempre crescenti, ciò grazie ai risvolti che sembrano poter offrire, pur con i limiti che tutt'ora vi sono.

Da un punto di vista teorico, sarebbe necessaria un ulteriore formalizzazione delle proprietà identificate per consentire lo sviluppo di una base PUF forte basata su primitive sicure; in particolare hardware che implichi l'uso della crittografia.

Da un punto di vista pratico dovrebbero essere adottate e verificate, caratteristiche più concrete e standardizzate, ciò al fine di prendere decisioni obiettive, sia nella progettazione di nuove PUF che nelle loro applicazioni.

8 Crittografia

8.1 Introduzione

La sicurezza, nella sua forma più semplice, si occupa di impedire a terzi di accedere a servizi senza autorizzazione, di identificare le fonti che emettono documenti o che inviano e-mail, ma anche di impedire l'intercettazione dei messaggi ed evitarne la modifica. I problemi di sicurezza possono quindi essere raggruppati in quattro aree d'interesse: segretezza, autenticazione, non-ripudio e controllo dell'integrità. La segretezza, detta anche confidenzialità, si occupa di mantenere le informazioni lontane dalla portata di utenti non autorizzati; l'autenticazione, invece stabilisce l'identità del soggetto con cui si sta scambiando l'informazione, come nel caso di un ente con cui si sta concludendo una trattazione commerciale; il non-ripudio consente l'attestazione dell'invio dei dati da parte di un utente, riguarda di solito le firme; controllo dell'integrità, verifica che i dati non vengano alterati.

Tutti questi problemi possono essere affrontati nei sistemi tradizionali, in maniera non sempre utile, come l'ispezione visiva, utile quando si trattano dei documenti protetti con tecniche di stampa particolari (come nel caso delle banconote) ma ad esempio non applicabile in altri casi. In aiuto a questi metodi viene utilizzata la crittografia (Katz & Lindell, 2007).

L'etimologia della parola crittografia ne spiega il significato. Essa deriva dall'unione di due parole greche: κρυπτός (*kryptós*) che significa "nascosto", e γραφία (*graphía*) che significa "scrittura". Crittografia è l'insieme delle teorie e delle tecniche che permettono di rendere un messaggio "offuscato" in modo da non essere comprensibile/intellegibile a persone non autorizzate a leggerlo.

Per capire a fondo il meccanismo di funzionamento è necessario distinguere tra due concetti, il cifrario ed il codice. Con cifrario s'intende una trasformazione bit per bit (o carattere per carattere) senza considerare la struttura linguistica del messaggio. Al contrario invece, per "codice" invece si intende una sostituzione di una parola con un'altra parola o con un simbolo.

I messaggi in chiaro da cifrare, detti "testi in chiaro", vengono trasformati, secondo il cifrario o il codice, tramite una funzione parametrizzata da una chiave. L'output del processo di cifratura, noto come testo cifrato, viene poi trasmesso.

Una volta giunto a destinazione questo deve essere decifrato, e ciò suppone che il criptoanalista conosca l'algoritmo usato per la cifratura; questo significa che non è possibile pensare di mantenere segreto il metodo, bensì ciò si può fare con le chiavi.

La chiave crittografica è una stringa che identifica una particolare cifratura fra molte possibilità. Al contrario dell'algoritmo, la chiave può essere cambiata ogni volta che si ritiene necessario, quindi la sicurezza sta proprio in questa caratteristica e nella sua lunghezza.

8.2 Algoritmi di cifratura

Fondamentalmente gli algoritmi di cifratura possono essere distinti in due grandi gruppi proprio in base alle caratteristiche della chiave: *algoritmi a chiave privata (crittografia simmetrica)* o *a chiave pubblica (crittografia asimmetrica)*.

8.2.1 Chiave Privata (Crittografia simmetrica)

La prima classe di algoritmi che si affronta è quella degli algoritmi a chiave privata (crittografia simmetrica), chiamati così in quanto usano la stessa chiave o chiavi diverse ma in stretta relazione tra di loro per cifrare e decifrare i messaggi. La robustezza di questi algoritmi è legata alla lunghezza della chiave che può essere di 40 bit (4 caratteri) e in questo caso si parla di chiave debole, oppure 128 bit (13 caratteri) detta chiave forte; tali chiavi diventano però poco applicabili quando la comunicazione avviene tra un numero consistente di utenti.

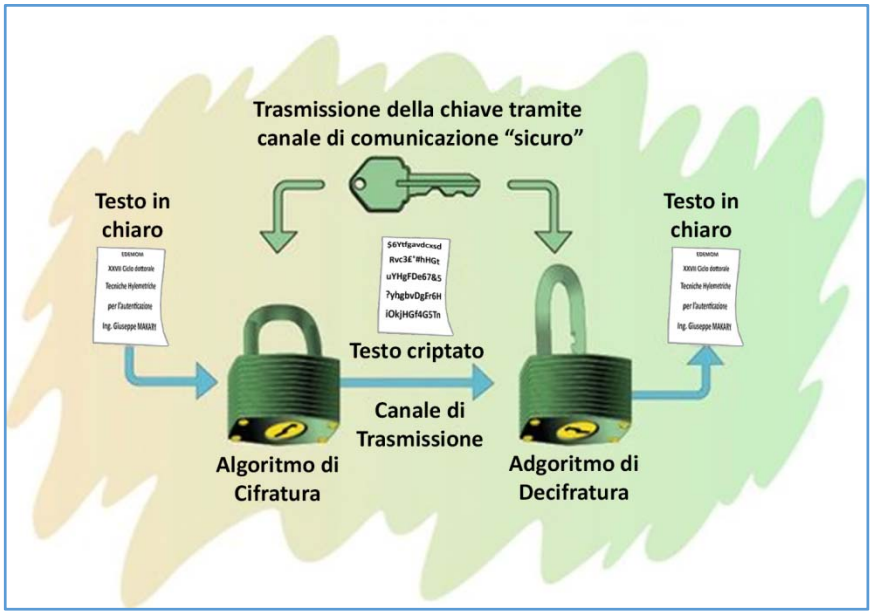


Figura 38 – Crittografia simmetrica

8.2.2 Chiave Pubblica (Crittografia asimmetrica)

La seconda classe, che verrà trattata più in dettaglio, è quella degli algoritmi a chiave pubblica (crittografia asimmetrica). Si tratta di un tipo di crittografia che utilizza due chiavi differenti, una per la codifica e una per la decodifica: se una chiave viene usata per la cifratura, l'altra viene usata per la decifratura, e viceversa. Inoltre, si basa su funzioni matematiche e non su operazioni di sostituzione e permutazione. Il punto fondamentale è che le due chiavi devono essere indipendenti; ossia la conoscenza di una delle due non deve fornire alcuna informazione utile per costruire l'altra. L'uso di due chiavi ha conseguenze rilevanti nel campo della segretezza, della distribuzione di queste e dell'autenticazione.

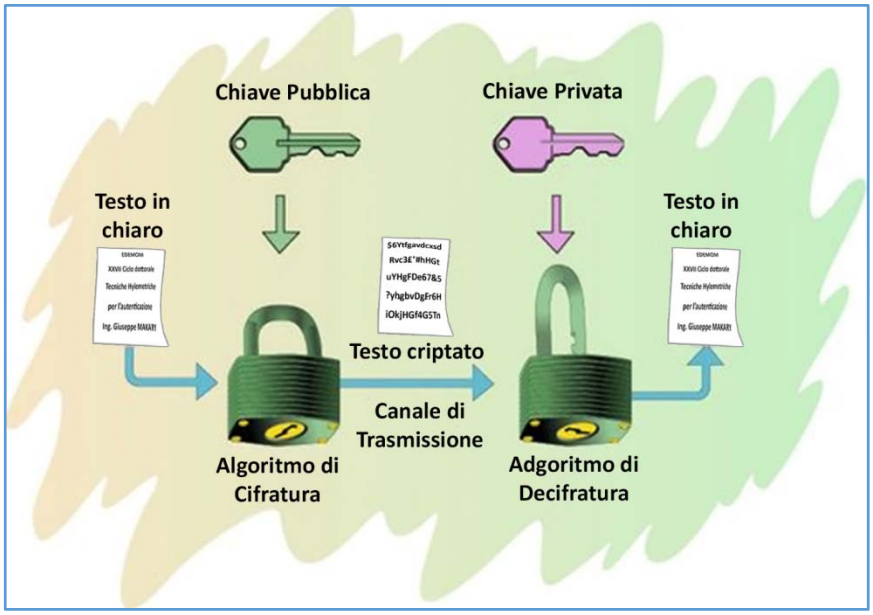


Figura 39 – Crittografia asimmetrica

Si tende a pensare che la chiave asimmetrica come più sicura ed efficiente, cosa non del tutto vera in quanto spesso, viene sfruttata la crittografia simmetrica per lo scambio delle chiavi.

Molti degli algoritmi con cui si ha a che fare sono quindi più adatti, o alla codifica (ad esempio attraverso un'estesa distribuzione delle chiavi) o per la firma digitale[13]. Soltanto tre di questi lavorano bene in entrambi i campi: RSA, Rabin e ElGamal (Rivest, et al., 1978) (Rabin, 1979) (ElGamal, 1985). In generale gli algoritmi a chiave pubblica sono molto più lenti a criptare e decriptare rispetto agli algoritmi simmetrici, questo perché supportano una grande quantità di dati da elaborare. Una soluzione più rapida è quella di usare i sistemi ibridi che sono più veloci e sfruttano le caratteristiche degli algoritmi simmetrici e asimmetrici alternandoli casualmente.

8.3 Funzionamento dei sistemi crittografici asimmetrici

Come detto in precedenza il meccanismo si basa sulla presenza di due chiavi differenti ma correlate tra loro; utilizzate una per la crittografia e una per la decrittografia. Questi algoritmi sono costruiti in modo tale da rendere impossibile la determinazione della chiave per la decrittografia

[13] La firma digitale è una informazione che viene aggiunta al fine di garantirne integrità e provenienza. Essa può essere utilizzata per autenticare una qualunque sequenza di simboli binari, indipendentemente dal loro significato.

anche se è nota quella usata per crittografare e l'algoritmo utilizzato. Inoltre alcuni algoritmi come RSA presentano un'ulteriore caratteristica che permette di usare una qualsiasi delle due chiavi correlate per la codifica a patto che si usi l'altra per la decodifica (Diffe, 1988).

Uno schema di crittografia asimmetrica prevede sei componenti (si veda Figura 39)

- **Testo in chiaro:** il messaggio o i dati leggibili inviati come input all'algoritmo.
- **Algoritmo di crittografia:** l'algoritmo di crittografia che opera varie trasformazioni sul testo in chiaro.
- **Chiavi pubblica e privata:** la coppia di chiavi scelte in modo che l'utilizzo di una nella crittografia comporti l'utilizzo dell'altra nella decrittografia. Le informazioni dettagliate riguardo alle trasformazioni che effettua l'algoritmo dipendono dalla chiave pubblica o privata fornita come input.
- **Testo cifrato:** il messaggio cifrato prodotto come output e che dipende dal testo in chiaro e dalla chiave. Per un determinato messaggio due chiavi diverse producono due diversi testi cifrati.
- **Algoritmo di decrittografia:** accetta il testo cifrato e la chiave corrispondente per restituire il testo in chiaro.

Il meccanismo si basa quindi su quattro operazioni:

1. Ciascun utente genera una coppia di chiavi da usare nella crittografia e decrittografia dei messaggi.
2. Una delle due chiavi viene inserita in un registro pubblico o in un file accessibile e l'altra viene mantenuta segreta (privata). Questo permette a ciascun utente di gestire un "mazzo" di chiavi pubbliche appartenenti a tutti gli altri utenti
3. La chiave pubblica del destinatario viene utilizzata per crittografare un messaggio confidenziale
4. La chiave privata del ricevente, essendo segreta, viene utilizzata per decrittografare il messaggio.

Seguendo questi passi, le chiavi pubbliche potranno essere distribuite liberamente e quelle private saranno generate localmente da ogni partecipante e non dovranno essere mai distribuite. Finché questa segretezza viene mantenuta, tutte le comunicazioni resteranno sicure.

Si supponga che una sorgente *A* produca un messaggio in chiaro, $X = [X_1, X_2, ..., X_M]$ che deve essere inviato a *B*. Questi genera una coppia di chiavi correlate: una pubblica PU_b, e una privata PR_b. Quest'ultima è nota solo a *B*, mentre l'altra è accessibile anche ad *A*.

Utilizzando come input il messaggio X e la chiave PU_b, *A* genera il testo cifrato $Y = [Y_1, Y_2, ..., Y_M]$.

$$Y = E(PU_b, X)$$

Il destinatario, in possesso della chiave privata corrispondente, potrà invertire la trasformazione:

$$X = D(PU_b, Y)$$

Uno schema crittografico di questo tipo garantisce la segretezza, ma non l'autenticazione. Viene quindi utilizzato un altro tipo di schema in cui *A* prepara il messaggio per *B* e lo codifica utilizzando la propria chiave privata prima di trasmetterlo.

Le funzioni saranno quindi:

$$Y = E(PU_a, X)$$

$$X = D(PU_a, Y)$$

quindi *B* potrà decrittografarlo usando la chiave pubblica di *A*.

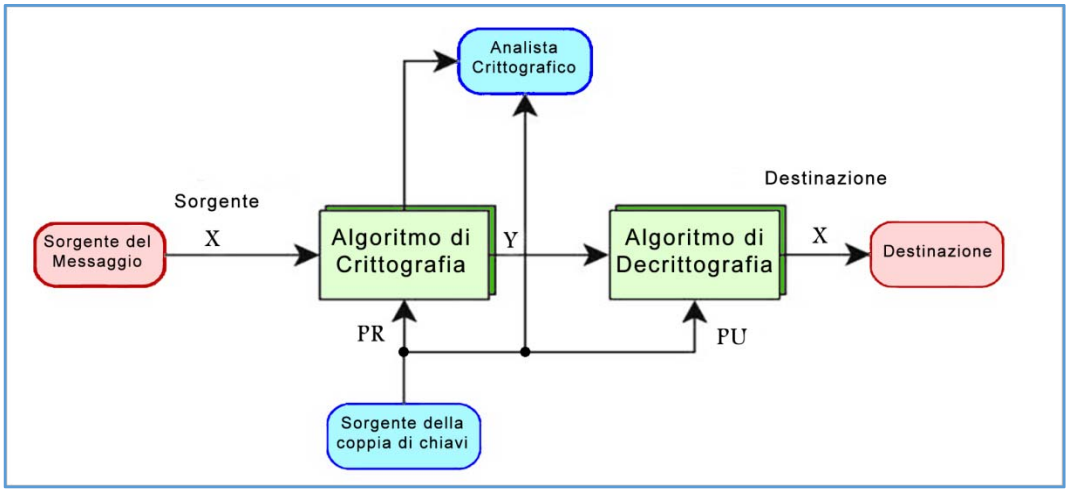


Figura 40 – Autenticazione

Poiché il messaggio è stato crittografato con la chiave privata di A si ha la certezza del mittente. In questo modo il messaggio crittografato in sostanza funge da firma digitale, quindi sono protette sia l'autenticità che l'integrità dei dati.

8.4 Requisiti della crittografia a chiave pubblica

Il sistema crittografico a chiave pubblica dipende da un algoritmo crittografico che deve rispettare delle caratteristiche imposte da Diffie e Hellman (Diffie & Hellman, 1976) (Hellman, 1978).

1. Deve essere computazionalmente facile per il destinatario generare una coppia di chiavi pubblica PUb e privata PRb.
2. Deve essere facile per il mittente, conoscendo la chiave pubblica e il messaggio da crittografare, M, generare un testo cifrato corrispondente:

   $$C = E\left(PU_b, M\right)$$

3. Deve essere facile per il destinatario decrittografare il testo cifrato utilizzando la chiave privata:

   $$M = D\left(PR_B, C\right) = D\left[PR_b, E\left(PU_b, M\right)\right]$$

4. Deve essere impossibile per un estraneo, conoscendo la chiave pubblica PU_b, determinare la chiave privata PR_b.

5. Deve essere impossibile per un estraneo, conoscendo la chiave pubblica e il messaggio cifrato C, ricostruire il messaggio originale M.
6. Le due chiavi possono essere applicate in qualsiasi ordine:
7. $M = D\left[PU_b, E\left(PR_b, M\right)\right] = D\left[PR_b, E\left(PU_b, M\right)\right]$

Solo pochi algoritmi (Rivest, et al., 1978) (Hellman, 1978) (Koblitz, 1987) (NIST, 2013) (Menezes, et al., 1996), hanno ricevuto un'ampia accettazione da quando è stata proposta la crittografia a chiave pubblica, questo perché si ha l'esigenza di avere una funzione monodirezionale che mappi un dominio in un codominio tale che ogni valore della funzione abbia un verso univoco, con la condizione che il calcolo dell'inverso sia impossibile:

$$Y = f(X) \qquad \text{facile}$$

$$X = f^{-1}(Y) \qquad \text{impossibile}$$

Con "facile" s'intende un problema risolvibile in un tempo polinomiale rispetto la lunghezza dell'input. Alla luce di questo quindi se n bit è la lunghezza dell'input, il tempo necessario a calcolare la funzione deve essere proporzionale a n^a dove a è una costante fissa.

Il termine "impossibile" è più difficile da definire: un problema si può definire tale se l'impegno per risolverlo cresce più rapidamente di un polinomio in funzione delle dimensioni dell'input. Nell'esempio precedente quindi se n è la lunghezza dell'input e il tempo necessario a calcolare la funzione è proporzionale a 2^n, il problema è considerato impossibile. Purtroppo la crittografia richiede l'impossibilità di invertire una funzione per tutti gli input, quindi non risulta possibile riferirsi a queste funzioni per calcolare i tempi, vengono introdotte quindi delle informazioni aggiuntive.

Una funzione monodirezionale di questo tipo è una famiglia di funzioni invertibili f_k tali che:

$$Y = f_k\left(X\right) \quad \text{facile se } k \text{ e } X \text{ sono noti}$$

$$X = f_k^{-1}(Y) \quad \text{facile se } k \text{ e } Y \text{ sono noti}$$

$$X = f_k^{-1}(Y) \quad \text{impossibile se } Y \text{ è noto ma } k \text{ sconosciuto}$$

8.5 Vulnerabilità della chiave pubblica

Come per la crittografia simmetrica, anche quella a chiave pubblica risulta vulnerabile agli attacchi, ma una contromisura possibile per fronteggiarli può essere quella della scelta di chiavi di grandi dimensioni, tenendo conto però della dipendenza di tale sistema, dall'uso di una funzione matematica invertibile.

La complessità del calcolo può essere non lineare rispetto al numero di bit della chiave ma può crescere più rapidamente. Le dimensioni della chiave devono quindi essere sufficientemente grandi da rendere impossibile un attacco, ma abbastanza piccole da consentire l'esecuzione pratica di crittografia e decrittografia. In pratica le dimensioni delle chiavi che renderebbero impossibili gli attacchi generano velocità di crittografia/decrittografia troppo lente per gli utilizzi generali. La crittografia a chiave pubblica è però usata quasi esclusivamente nelle sole applicazioni di gestione delle chiavi e firma digitale. L'algoritmo più utilizzato tra quelli che si occupano di questo tipo di crittografia è l'RSA.

8.6 La Firma Digitale

Le caratteristiche su cui la firma digitale si basa sono molto simili a quelle della firma autografa; infatti come per questa, è necessario che possa essere emessa solo da una persona, ma che chiunque ne possa verificare la paternità. Trattandosi di una firma digitale, se il mittente A volesse spedire un messaggio M firmato, dovrà prima applicare ad M la sua chiave privata PR_a, nota solo a lui, e poi pubblicare il messaggio firmato con $PR_a(M)$ insieme al messaggio in chiaro M.

Il destinatario B può verificare a questo punto l'autenticità della firma digitale utilizzando la chiave pubblica di A PU_a e vedendo se M e $PR_a(M)$ convivono bene.

Nel caso venga utilizzato l'algoritmo RSA la verifica viene fatta applicando PU_a alla firma $PR_a(M)$ e vedendo se è valida l'uguaglianza:

$PU_a\left[PR_a\left(M\right)\right] = M$ in questo modo chiunque può verificare la paternità del messaggio.

La differenza fondamentale che c'è con la firma autografa è che la firma digitale $PR_a(M)$ è inscindibile dal messaggio, mentre la firma autografa viene aggiunta al messaggio ed è sempre la stessa. Conseguentemente, non si può alterare il messaggio firmato $PR_a(M)$ senza che nessun al-

tro capisca che è stato cambiato: alterando $PR_a(M)$ anche di un solo bit, l'applicazione della chiave pubblica restituisce un messaggio $PR_a(M')$ da cui si ottiene un messaggio in chiaro totalmente diverso e casuale.

La Figura 41 mostra, in forma schematica, la procedura di firma digitale tramite algoritmo RSA.

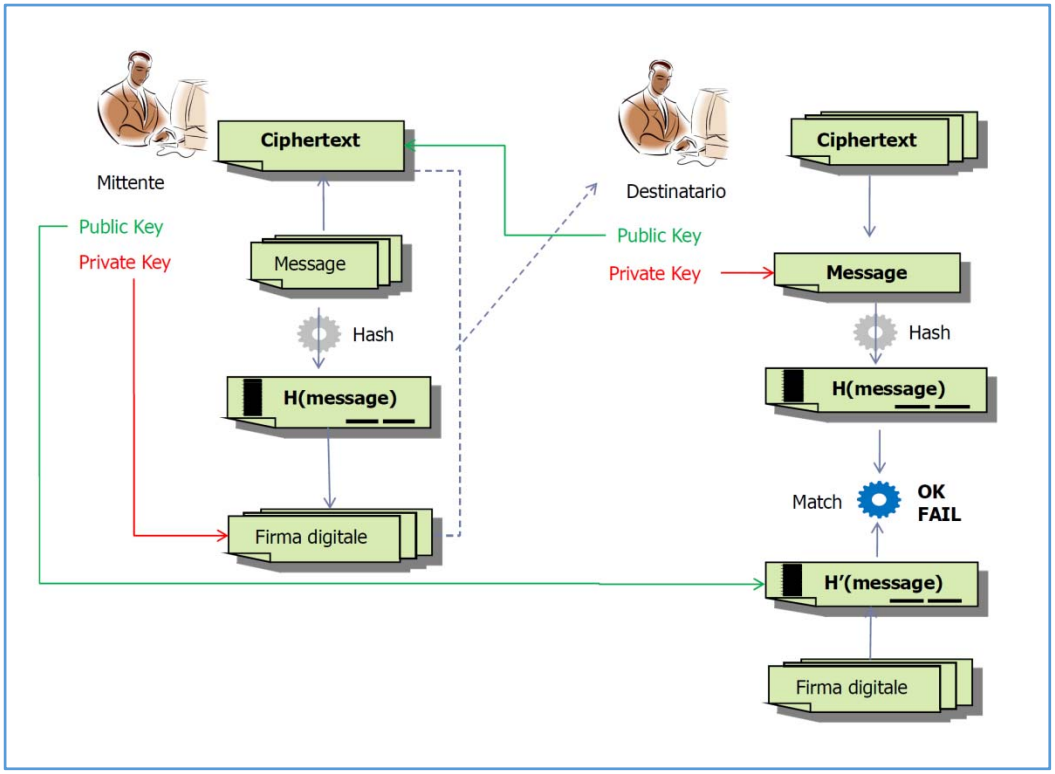


Figura 41 – Firma digitale con algoritmo RSA

8.7 L'algoritmo RSA

Lo schema ideato da Rivest, Shamir e Adleman (Rivest, et al., 1978), indicato come RSA, è una cifratura a blocchi in cui il testo in chiaro e il cifrato sono interi compresi tra 0 e n-1 per un dato valore di n. Se n è pari a 1024 bit, ovvero 309 cifre decimali si ha $n < 2^{1024}$. Ogni blocco è un valore binario minore di un certo numero n, ovvero deve avere dimensioni minori o uguali di $\ln(n)$, quindi di k bit dove $2^k < n \leq 2^{k+1}$. La crittografia e la decrittografia di un determinato testo in chiaro M e del corrispondente blocco cifrato C hanno la seguente forma:

$$C = M^e \bmod n$$
$$M = C^d \bmod n = \left(M^e\right)^d \bmod n = M^{e \cdot d} \bmod n$$

Il valore di n deve essere noto sia al mittente che al destinatario. Il mittente conosce anche il valore di e mentre solo il destinatario conosce il valore d. Questo è quindi un algoritmo con una chiave pubblica $PU = \{e, n\}$ e una chiave privata $PR = \{d, n\}$ e affinché sia soddisfacente per la crittografia a chiave pubblica deve soddisfare i seguenti requisiti:

1. E' possibile trovare i valori di e, d, n tali che $M = M^{e \cdot d} \bmod n$ per ogni $M < n$.
2. E' relativamente facile calcolare $M^e \bmod n$ e $C^d \bmod n$ per tutti i valori $M < n$.
3. E' impossibile determinare d sulla base di e e n.

Per giustificare i tre punti precedentemente elencati è necessario ricorrere al ***teorema di Eulero***; l'algoritmo RSA è una diretta applicazione del teorema di Eulero (Berardi & Beutelspacher, 1996).

Si definisce $\phi(n)$ *indicatore di Eulero* di un numero naturale n il numero dei numeri naturali minori o uguali a n che non hanno nessun fattore, tranne 1, in comune con n. In altre parole $\phi(n)$ è il numero dei numeri naturali minori di n e primi con n, cioè aventi con n massimo comune divisore 1. Valgono quindi le seguenti proprietà:

a. Se p è un numero primo, allora:

   $\phi(p) = p - 1$

b. Se p e q sono due primi distinti, allora:

   $\phi(p \cdot q) = (p-1)(q-1)$.

Ora è possibile enunciare il **teorema di Eulero** (Davenport, 1994) **:**

Siano M ed n due naturali primi tra loro e k un numero intero non negativo. Allora:

$$M^{k\phi(n+1)} \bmod n = M$$

Interessa in modo particolare il caso in cui n è il prodotto di due primi distinti; in tal caso il teorema può essere enunciato come segue.

Sia M un naturale, p e q due primi distinti e k un intero non negativo. Allora

$$M^{k(p-1)(q-1)} \bmod (p \cdot q) = M$$

In altre parole dividendo il numero $M^{k(p-1)(q-1)+1}$ per $p \cdot q$, otteniamo come resto $\boldsymbol{M}$.

Tornando ora alla relazione $M^{e \cdot d} \bmod n = M$, essa è valida quando e e d sono inversi moltiplicativi del modulo $\phi(n)$. Il legame fra e e d può essere espresso come:

$$e \cdot d \bmod \phi(n) = 1$$

Che equivale a dire:

$$e \cdot d = 1 \cdot \bmod \phi(n)$$
$$d = e^{-1} \cdot \bmod \phi(n)$$

In pratica, e e d sono inversi moltiplicativi $\bmod \phi(n)$. Si noti che secondo le regole dell'aritmetica modulare, questo vale solo se d (e pertanto e) è primo relativo di $\phi(n)$.

Definiamo alla luce di questo lo schema RSA con i seguenti elementi:

p, q sono due numeri primi	(privati e scelti)
$n = p \cdot q$	(pubblico, calcolato)
$d \equiv e^{-1} \cdot \bmod \phi(n)$	(privato , calcolato)
e, con $\gcd[\phi(n), e] = 1$; $1 < e < \phi(n)$	(pubblico, scelto)

(la funzione gcd, restituisce il massimo comun divisore usando l'algoritmo di Euclide)

la chiave privata risulta costituita da $\{d, n\}$ e la chiave pubblica da $\{e, n\}$.

Si supponga che A abbia reso nota la propria chiave pubblica e che l'utente B voglia inviare ad A un messaggio m. Quindi B calcola $C = M^e \bmod n$ e trasmette C. Dopo aver ricevuto il testo cifrato C, l'utente A esegue la crittografia calcolando $M = C^d \bmod n$.

8.7.1 Algoritmo di Euclide

Si ricorre all'uso dell'*algoritmo di Euclide* per generare sia la chiave pubblica che privata di ogni partecipante. Esso serve per calcolare il massimo comun divisore $MCD(a,b)$ (funzione di due naturali a e b $(a \geq b)$, anche molto grandi.

8.7.1.1 Sviluppo dell'algoritmo di Euclide:

$$
\begin{array}{ll}
r_0 = a & \\
r_1 = b & \\
r_0 = q_1 r_1 + r_2 & 0 < r_2 < r_1 \\
r_1 = q_2 r_2 + r_3 & 0 < r_3 < r_2 \\
\vdots & \vdots \\
r_{i-1} = q_i r_i + r_{i+1} & 0 < r_{i+1} < r_i \\
\vdots & \vdots \\
r_{n-2} = q_{n-1} r_{n-1} + r_n & 0 < r_n < r_{n-1} \\
r_n = q_n r_n &
\end{array}
$$

Il numero r_n definito dall'algoritmo di Euclide è il massimo comun divisore tra a e b. Per provarlo si faccia riferimento alle seguenti affermazioni:

* r_n divide a e b (ovvero r_n è un divisore comune);
* ogni numero z che divide a e b divide anche r_n (r_n è il più grande tra i divisori comuni).

Entrambe le due affermazioni possono essere scritte attraverso l'aritmetica modulare; infatti:
dati due naturali a e b, sia $d = MCD(a,b)$. Allora esistono due interi x e y tali che: $d = x \cdot a + y \cdot b$

Per calcolare x e y si ricorre all'algoritmo di Euclide e applicandole si giunge a:

$$
\begin{aligned}
d = r_n &= r_{n-2} - q_{n-1} r_{n-1} = r_{n-2} + \left(-q_{n-1}\right) r_{n-1} \\
&= r_{n-2} - q_{n-1}\left(r_{n-3} - q_{n-2} r_{n-2}\right) \\
&= \left(-q_{n-1}\right) r_{n-3} + \left[1 + q_{n-2} q_{n-1}\right] r_{n-2} \\
&= [\ldots] r_{n-4} + [\ldots] r_{n-3} \\
&\vdots \\
&= x r_0 + y r_1 = xa + yb
\end{aligned}
$$

Se a e b sono due numeri interi tra loro (cioè il loro MCD è 1), allora esiste un intero c tale che

$$b \cdot c \bmod a = 1$$

Ovvero, c è l'inverso di $b \bmod a$.

Se abbiamo $d = r_n = 1$; esistono due numeri x e y tali che:

$$1 = d = ax + by$$

Poiché ax è multiplo di a, dividendo $b \cdot y$ per a, si ottiene necessariamente come resto 1. In altre parole

$$b \cdot y \bmod a = 1$$

8.7.2 Generazione delle chiavi

E' necessario quindi che ogni partecipante sia provvisto di due chiavi; allo scopo vengono scelti due numeri primi distinti p e q grandi. Si ottiene: $n = p \cdot q$.

Successivamente viene calcolato: $\phi(n) = \phi(p \cdot q) = (p-1)(q-1)$.

Il passo successivo è quello di scegliere un naturale e primo con $\phi(n)$ e si calcola d tale che: $e \cdot d \bmod \phi(n) = 1$.

In altre parole: $d = e^{-1} \bmod \left[(p-1)(q-1)\right]$.

Le chiavi sono cosi calcolate: e ed n come chiave pubblica e d come chiave privata. I parametri segreti p, q e $\phi(n)$ possono restare segreti, questo perché a partire da questi è possibile ricostruire le chiavi private senza difficoltà.

Analizzando il criterio con cui vengono scelti i parametri, si nota che:

- e è scelto in maniera da rendere semplice il calcolo di $M^e \bmod n$, in cui naturalmente gli n assegnati sono distinti. Ciò garantisce che le chiavi segrete siano diverse.
- Il calcolo di d invece è legato a e, oppure ad un numero primo che non divida $\phi(n)$. Si scelga quindi e si calcola il suo *MCD* e $\phi(n)$ usando l'algoritmo di Euclide precedentemente illustrato, a questo punto si divida e per questo *MCD*. Si applichi poi l'algoritmo di Euclide per calcolare il corrispondente valore di d.

I numeri primi utilizzati da RSA devono avere una lunghezza che va dalle 100 alle 200 cifre decimali per restare sufficientemente robusto. La questione è superata in quanto si ha bisogno di numeri non propriamente primi, ma di pseudoprimi per poter soddisfare i criteri precedentemente elencati.

8.7.3 Uso dell'algoritmo RSA

Per criptare un messaggio è necessario che questo sia trasformato in una sequenza di uno o più interi positivi in modo che risulti $M \leq n$. Si considerino p e q di 100 digits, n sarà appena sotto i 200 digits; quindi ogni blocco in cui è diviso il messaggio sarà lungo almeno 200 digit. Nel caso si avesse bisogno di criptare un numero di blocchi fissato, è possibile estenderli con l'aggiunta di una serie di zeri a sinistra per garantire che siano sempre inferiori a n. Il messaggio criptato, c sarà quindi di lunghezza simile a quella dei blocchi, o addirittura della stessa lunghezza. La formula per ricavare il messaggio c, corrispondente al testo in chiaro m, è:

$$C = M^e \bmod n \quad .$$

Dovendo a questo punto decifrare il messaggio, si prenda ogni blocco criptato C e si applichi la chiave privata:

$$M' = C^d \bmod n$$

per ottenere però il messaggio originale e non qualunque messaggio M' si ricorra ad un teorema che afferma la validità dell'algoritmo applicato se per ogni intero positivo $M \leq n$ si ha $M' = M$.

La scelta di criptare con d e decriptare con e è arbitraria, i due numeri potrebbero essere tranquillamente invertiti senza causare alcun problema.

Generazione della chiave	
Selezione di p e q	p e q entrambi primi e $p \neq q$
Calcolare $n = p \cdot q$	
Calcolare $\phi(n) = (p-1)(q-1)$	
Selezionare l'intero e	$\gcd[\phi(n), e] = 1$; $1 < e < \phi(n)$
Calcolare d	$d \equiv e^{-1}(mod\, \phi(n))$
Chiave pubblica	$PU = \{e.n\}$
Chiave privata	$PR = \{d, n\}$
Nota: la funzione gcd, restituisce il massimo comun divisore usando l'algoritmo di Euclide	

Crittografia	
Testo in chiaro	$M < n$
Testo cifrato	$C = M^e \bmod n$

Decrittografia	
Testo cifrato	C
Testo in chiaro	$M = C^d \bmod n$

Tabella 10 – Algoritmo RSA

8.7.4 Sicurezza dell'algoritmo RSA

L'algoritmo RSA basa la sua forza sul problema della fattorizzazione dei grandi numeri. La conoscenza della scomposizione di n nei suoi fattori primi p e q ; ma è valido anche il viceversa, noti

n e $\phi(n)$ permette di risalire alla fattorizzazione di n. Infatti sotto queste ipotesi si hanno le due equazioni: $p \cdot q = n$ e $(p-1)(q-1) = \phi(n)$ nelle due incognite p e q; il che rende possibile ricavarle.

Ricapitolando, se n è il prodotto di due numeri primi distinti, computare $\phi(n)$ è equivalente a fattorizzare n. Tenendo conto che l'intero n che compare nell'RSA ha una lunghezza di circa 200 cifre decimali, ci si imbatte in un problema estremamente difficile.

L'impiego così diffuso dell'RSA si deve al fatto che gli altri algoritmi impiegati per l'implementazione della firma digitale sono molto lenti (impiegano in genere 1 secondo per una firma elettronica formata da 1024 bits).

8.8 La funzione HASH

Quando si ha a che fare con file di grandi dimensioni per creare la firma digitale spesso si ricorre all'uso di funzioni **hash**: infatti è a livello computazionale più conveniente eseguire con rapidità un hashing del testo da firmare e poi autenticare solo quello, evitando così di eseguire i complessi algoritmi di crittografia asimmetrica su moli troppo grandi di dati. La lunghezza dei valori di hash varia a seconda degli algoritmi utilizzati. Il valore più comunemente adottato è di 128 bit, che offre una buona affidabilità in uno spazio relativamente ridotto. Tuttavia va registrata la possibilità d'uso di hash di dimensione maggiore.

In generale hash significa "sintetizzare", ovvero trasformare un testo di lunghezza arbitraria in una stringa di lunghezza fissa relativamente limitata. Tale stringa rappresenta una sorta di impronta digitale del testo in chiaro (*message digest*).

Sono quindi funzioni che svolgono un ruolo essenziale nella crittografia: sono utili per verificare l'integrità di un messaggio, poiché l'esecuzione dell'algoritmo su un testo anche minimamente modificato fornisce un *message digest* completamente differente rispetto a quello calcolato sul testo originale, rivelando la tentata modifica.

Una funzione di questo tipo soddisfa dei requisiti fondamentali:

1. L’algoritmo restituisce una stringa di numeri e lettere a partire da un qualsiasi flusso di bit di qualsiasi dimensione (può essere un file ma anche una stringa). L'output è detto Digest.
2. La stringa di output è univoca per ogni documento e ne è un identificatore. Perciò, l'algoritmo è utilizzabile per la firma digitale.
3. L’algoritmo non è invertibile, ossia non è possibile ricostruire il documento originale a partire dalla stringa che viene restituita in output.

9 Integrazione fra tecniche di induplicabilità

9.1 Introduzione

Negli ultimi anni si è assistito alla crescita costante dell'esigenza, da parte delle autorità così come dei singoli individui, di incrementare la sicurezza contro le frodi; in particolare per quanto riguarda quella legata all'autenticità e alla provenienza garantita degli oggetti.

Come già visto in precedenza (Capitolo 5), vi sono molti sistemi che offrono protezione contro la contraffazione. La quasi totalità però dei metodi utilizzati per l'anticontraffazione si basano su caratteristiche aggiunte all'oggetto. La filosofia finora adottata, si veda il caso emblematico delle banconote, prevede quindi l'inserimento di "marchi/caratteristiche" utilizzando tecniche complesse e costose, rendendo economicamente sconveniente duplicarle. La semplice commercializzazione di oggetti senza il corretto marchio/caratteristica consente l'individuazione della frode.

Figura 42 – Pinze chirurgiche con "marcatura" del metallo.

L'inserimento di marchi e caratteristiche "complesse" ed economicamente onerose, fa sì che tali sistemi possano essere utilizzati solo su oggetti di valore economico "considerevole". Inoltre, con il progredire della tecnologia, la clonazione delle caratteristiche aggiunte è divenuto sempre più semplice e compatibile economicamente.

Così come per le tecniche biometriche, sarebbe utile riuscire a trovare per ogni oggetto un sistema basato su caratteristiche intrinseche e non clonabili. Alla stregua per esempio delle nostre impronte digitali, che sono proprie ed uniche.

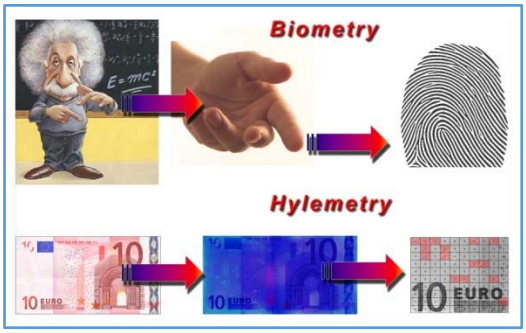


Figura 43 – Tecniche biometriche vs. tecniche Hylemetriche.

Come già detto in precedenza, oggigiorno si duplica di tutto. Uno dei mercati del falso più fiorente è il mercato della moda. In questo ambito, gli oggetti contraffatti, molto spesso, non hanno un elevato valore economico tale da giustificare sistemi di sicurezza sofisticati e complessi. Inoltre, l'autenticazione dovrebbe poter essere fatta con metodi semplici, economici e accessibili al comune acquirente.

In questo settore quindi, gli attuali sistemi sono basati quasi esclusivamente sul riconoscimento visivo di dettagli. Nel caso di "copie" ben fatte, il comune acquirente ha difficoltà notevoli a riconosce un originale da un falso; in alcuni casi è impossibile; inoltre durante l'acquisto non è possibile un controllo visivo comparativo tra originale e copia.

Figura 44 – Particolari di oggetti originali vs. falsi

Nell'immagine sopra si può facilmente notare la difficoltà, con un semplice esame visivo, di individuare l'autenticità o meno dell'oggetto.

Attualmente, in qualche capo, comincia ad essere presente, all'interno dell'etichetta un RFID (Par. 5.2.4.3) in grado di fornire una maggior sicurezza sulla provenienza ed autenticità dell'oggetto.

Figura 45 – Etichetta con all'interno un RFID.

Questa metodologia, considerando che vi sono sistemi di lettura degli RFID che possono essere accoppiati con telefoni con tecnologia NFC (Near Field Communication), potenzialmente, rende la metodologia accessibile ad un largo numero di utenti.

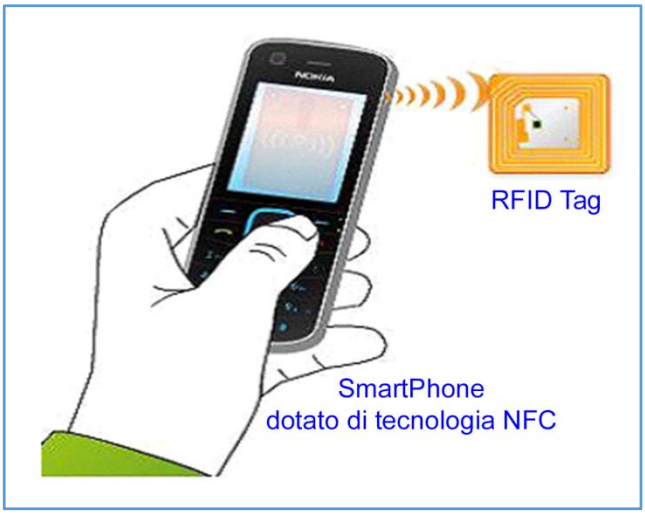


Figura 46 – Lettura di un RFID con Smartphone dotato di tecnologia NFC.

Per un corretto utilizzo di sistemi di autenticazione basati su RFID o similari, per garantire la sicurezza del dispositivo in questione, è indispensabile utilizzare tecniche crittografiche. In questo modo, ognuno può controllarne la autenticità, ma solo una persona autorizzata può immagazzinare le informazioni che lo caratterizzano.

Gli algoritmi crittografici sono molto utilizzati in internet in quanto vi è la necessità di assicurare segretezza, autenticazione e integrità al messaggio. Gli utenti in fase di interazione con altre persone, sentono il bisogno di sapere ed avere la conferma che il loro interlocutore sia esattamente la persona con cui vogliono interloquire; che quindi il loro messaggio arrivi integro a destinazione e che nessun altro oltre al destinatario stia ascoltando. In questo contesto si parla più che altro di segretezza e il tipo di frode da fronteggiare non è la duplicazione, ma la contraffazione; assistiamo infatti a dati che vengono "sniffati" attraverso la rete, a carte di credito che vengono utilizzate da truffatori all'insaputa dei proprietari e a informazioni che vengono modificate; problematiche risolte in modo esauriente dalla crittografia.

In questo lavoro, abbiamo analizzato invece dei sistemi che permettono di tutelare la non duplicabilità dei sistemi di "marcatura" degli oggetti commercializzati nel campo della moda; evitando tutti gli inconvenienti dovuti ai metodi già esistenti, puntando essenzialmente sul basso costo di produzione e sulla semplicità.

I sistemi proposti consisteranno nell'acquisizione di strutture random casuali e non duplicabili già presenti nell'oggetto o introdotti artificialmente. Queste caratteristiche microscopiche rendono l'oggetto unico. Si procederà poi con la loro codifica attraverso procedure di firma digitale asimmetrica per garantirne la non duplicabilità e la non ripudiabilità.

9.2 Protezione Hylemetrica degli oggetti di moda

Al fine di poter verificare l'autenticità di un oggetto che appartiene al mercato della moda, come già detto, è possibile applicare tecniche di origine hylemetriche alle stesse.

Il primo passo consiste quindi nell'individuare/inserire una caratteristica fisica stabile e non clonabile, che lo identifichi in modo univoco. Qualora la caratteristica (marcatura) debba essere aggiunta artificialmente, l'inserimento deve rispettare la peculiarità dell'oggetto ed evitare, in maniera assoluta, di alterarla.

Successivamente, si dovrà prevedere un sistema di acquisizione "non a contatto", per catturare tale caratteristica (es. macchina fotografica dotata di opportuni filtri, luce laser strutturata, ecc.). Una volta acquisita la caratteristica, dalla stessa si dovrà creare un template, sulla falsariga di

quanto avviene in ambito biometrico. Tale template potrà essere, se necessario codificato tramite opportuno sistema crittografico.

Tutte le informazioni del prodotto, con il template, realizzano una sorta di passaporto, legato in modo indissolubile all'articolo stesso. Le informazioni sull'oggetto, il sistema di marcatura, il template, le informazioni crittografiche saranno depositate all'interno di una base di dati centralizzata, a cui sarà possibile accedere in forma remota al fine di effettuare verifiche certificate.

Per rendere fruibile un tale sistema di autenticazione bisogna affrontare:

1) ***Scelta delle caratteristiche***: si deve verificare se sia possibile sempre estrarre una o più caratteristiche (stabili e non clonabili) dall'oggetto (es. particolari macchie di colore, puntinatura, rugosità superficiale, ecc.) in maniera non invasiva, tali da poter identificare univocamente il singolo articolo, anche in caso di deterioramento dello stesso. In assenza di tale possibilità si deve verificare la possibilità dell'aggiunta di una caratteristica in modo artificiale, che sia unica, stabile e non clonabile; senza "modificare" il valore estetico e la qualità del prodotto.
2) ***Creazione del template***: si deve definire come creare il template, che sia standard e quindi adeguato a ogni possibile prodotto ed adattabile quindi, a differenti caratteristiche. E' necessario definire a questo punto il tipo di crittografia da utilizzare e l'elenco delle entità autorizzate a rilasciare le chiavi per la creazione e verifica di ogni singolo template.
3) ***Apposizione del template***: per maggior sicurezza si può apporre il template codificato direttamente sull'oggetto, permettendo quindi, sia verifiche remote, che locali, sull'originalità dell'opera. In tal caso si dovrà verificare che tecnologia utilizzare, RFID, chip miniaturizzato, barcode, ecc. In fase di verifica tale supporto sarà letto, in maniera diretta o indiretta, e utilizzando i dati in esso contenuto sarà possibile completare il processo di verifica dell'opera o ottenerne informazioni sulla stessa. D'altra parte la sua assenza permetterebbe di identificare il prodotto come contraffatto.
4) ***Creazione e manutenzione di una base dati centralizzata***: si dovrà creare un database centralizzato, accessibile da remoto, in maniera sia diretta (pagina web), che indiretta (ricerca da app certificata), contenente tutti i template, in formato standard, con le relative informazioni sia di carattere generale (stilista, fabbrica di produzione, provenienza della materia

prima, controllo qualità, ecc.), che informazioni necessarie alla corretta verifica (chiave di decodifica, ecc.).

Figura 47 – Schema di principio per la realizzazione di una infrastruttura per la certificazione dell'autenticità di un oggetto.

9.3 Tecniche implementate

9.3.1 Introduzione

L'elevata concorrenza effettuata, specialmente dai paesi emergenti, sfrutta gli investimenti e l'inventiva delle aziende leader per sottrarre loro quote di mercato con prodotti palesemente contraffatti o realizzati in modo molto simile al brand che intendono "attaccare". Sul mercato si rilevano quotidianamente situazioni di contraffazione e di mercato parallelo: il brand subisce gravi danni di immagine, mentre i mercati paralleli danneggiano mercati consolidati a maggiore marginalità, oltre a creare conflittualità con la rete vendita ufficiale. Non tutti i fenomeni di contraffa-

zione puntano allo stesso scopo: talvolta il prodotto è contraffatto in modo palese e veicolato attraverso canali di vendita chiaramente non ufficiali, una situazione che comunque paradossalmente crea un effetto positivo: veicola il brand (e il desiderio di possederlo) attraverso una clientela che non potrebbe accedere comunque al brand stesso e consapevole di possedere un falso. Talvolta il brand viene invece contraffatto in modo molto accurato e veicolato attraverso canali plausibili, in questo caso si creano contemporaneamente due danni: l'utente crede di acquistare un prodotto originale a un prezzo vantaggioso e il brand perde una vendita. L'unico modo per contrastare questi fenomeni è l'identificazione certa del prodotto e la sua tracciatura durante tutti i passaggi della catena di distribuzione (supply chain). (Par. 5.2.4)

Le industrie del fashion si propongono sul mercato come aziende consolidate, fortemente strutturate e organizzate, capaci di gestire logiche di filiera produttiva e di mercato a livello internazionale. Un mercato globale caratterizzato da una forte delocalizzazione della produzione e dalla decentralizzazione delle attività, nell'ottica della crescita di competitività, ha tuttavia comportato numerose problematiche, causate soprattutto dall'impossibilità, per l'azienda, di monitorare con certezza attività, risorse, prodotti. Le criticità sono trasversali a tutti gli stadi della filiera, e sono in gran parte riconducibili a un problema fondamentale: l'impossibilità di accertare l'identità univoca del singolo prodotto. Oggigiorno, vista la delocalizzazione della produzione, è oneroso assegnare un nome o un numero di serie univoco e non "clonabile" al singolo prodotto. L'assenza del riconoscimento "unico" non consente una tracciabilità del prodotto lungo tutta la filiera. Non essendo i prodotti identificabili in modo univoco e certo, s'introducono problematiche fortemente sentite, quali:

- ✓ difficoltà e talvolta impossibilità di identificare un capo originale (contraffazione);
- ✓ prolificazione del mercato "parallelo e grigio" (grey market);
- ✓ errori nelle fasi di produzione, stoccaggio e movimentazione delle merci, sia in fase di ricezione che di spedizione.

9.3.2 Tecniche

La tecnologia RFID, accoppiata con sistemi di firma digitale e caratteristiche "uniche" (caratteristiche Hylemetriche) estratte dall'oggetto consente di soddisfare con successo tali esigenze.

In fase di produzione del capo di moda può essere individuato o inserito un qualche “particolare non duplicabile” (caratteristica Hylemetrica). Questo particolare viene “catturato”, ad esempio come immagine ad alta risoluzione, e inviato ad un algoritmo Hash. L’algoritmo fornisce un risultato non invertibile, e si ricorda che dal Hash è impossibile ricostruire la caratteristica di partenza. Questo dato ad esempio, può in seguito essere impiegato con l’ausilio della tecnologia RFID per la verifica del capo di moda.

Viene qui mostrato un esempio di applicazione della funzione hash, in ambito Biometrico. L’esempio tipico è l’utilizzo della funzione hash nelle minuzie delle impronte digitali usate nell’identificazione biometrica (si veda più sotto)

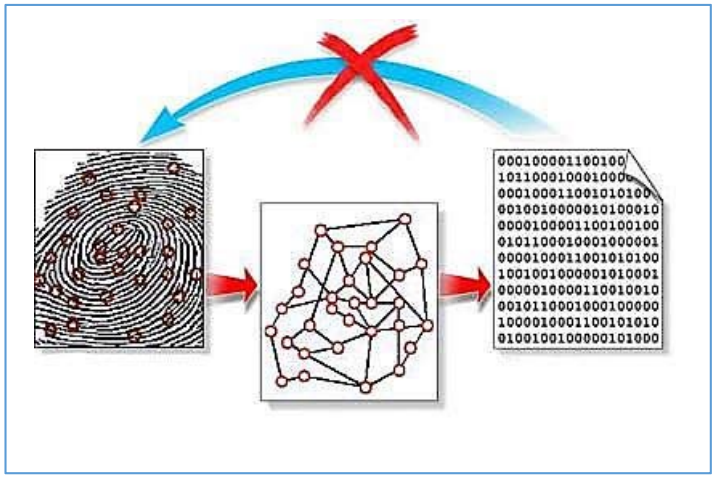


Figura 48 – Funzione Hash applicata alle impronte digitali

Alla stregua del caso mostrato pocanzi è possibile applicare la modalità sopra in ambito Hylemetrico. Nel campo della moda, ad esempio, si può prendere come “caratteristica Hylemetrica” una particolare cucitura eseguita a mano. Questa cucitura può essere binarizzatata, calcolata la lunghezza media dei singoli punti e realizzata una stringa binaria dove al singolo punto viene associato uno “0” o un “1” a seconda se è più corto o più lungo della lunghezza media (si veda immaginepiù sotto)

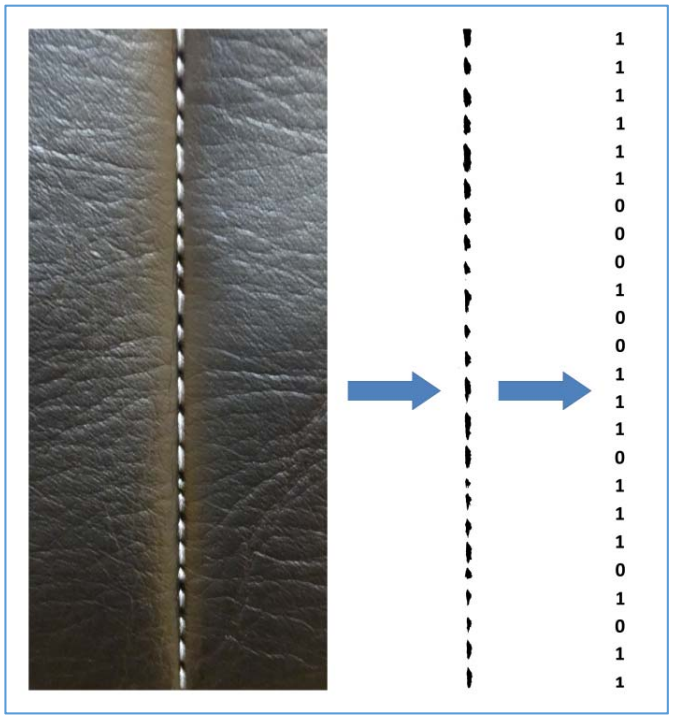


Figura 49 – Funzione Hash applicata a una cucitura a mano

Riepilogando quindi, al singolo capo di moda può essere associato un RFID che al proprio interno contiene memorizzati:

- ✓ i dati della casa di moda che ideato il capo;
- ✓ chi materialmente lo ha realizzato;
- ✓ i dati Hylemetrici (le caratteristiche uniche estratte dall'oggetto);
- ✓ la firma digitale di chi certifica l'originalità del capo;
- ✓ la scansione digitale del particolare da cui estrarre i dati Hylemetrici;
- ✓ link alla banca dati della maison; questo link consente di associare al prodotto informazioni, quale numero di lotto, stabilimento di produzione, data d'immissione sul mercato, ossia tutte le informazioni utili per il tracciamento della storia del prodotto.

Ovviamente, al capo di moda, soprattutto se di pregio elevato, può essere associato una sorta di passaporto (libretto cartaceo) che contiene tutte le informazioni che sono contenute nel RFID e nella banca dati della maison. In altre parole, le caratteristiche Hylemetriche estratte dal singolo

capo lo rendono unico e non “clonabile”, si realizza quindi una sorta di passaporto (Fashion-passport) del capo di moda.

Figura 50 – Capo di moda legato in modo “indissolubile” ad informazioni che lo rendono unico e non-duplicabile (Fashion passport)

9.3.3 Procedura di autenticazione “

Di seguito viene proposta, in virtù di quanto sin qui esposto, una procedura d’identificazione “sicura”. Nella figura più sotto viene quindi schematizzata tale procedura

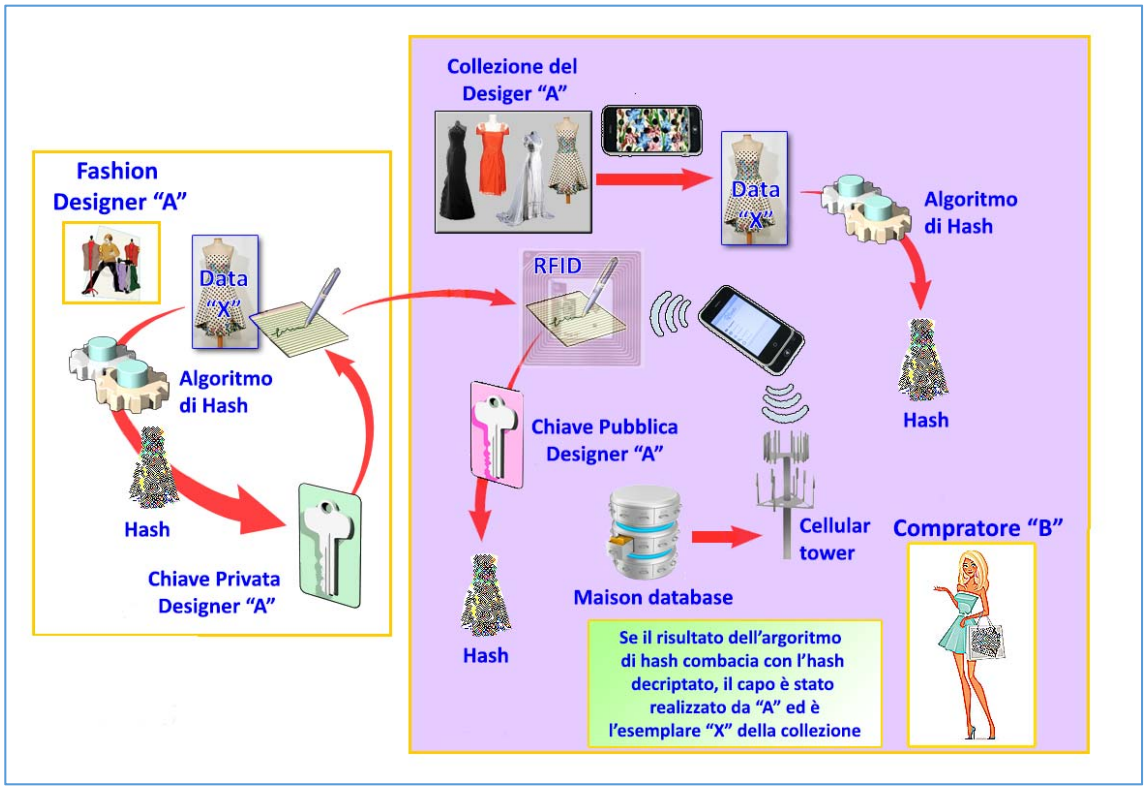


Figura 51 – Procedura di identificazione "sicura"

Il "realizzatore" (designer) di moda "A", disegna e fa realizzare il suo capo, che ovviamente fa parte di una collezione/lotto.

Una volta realizzato il capo su di esso si estrare una caratteristica Hylemetrica (presente sul capo stesso o opportunamente introdotta). Questa caratteristica viene inviata ad una funzione Hash. L'uscita di tale funzione, attraverso la chiave privata del designer "A" viene crittografata. In altre parole, il designer "A" firma digitalmente il singolo articolo (così come un'artista firma "materialmente" la sua singola opera – si pensi di acquistare un abito di Valentino e all'interno vi sia un'etichetta con la firma autografa dello stilista – in realtà il nostro metodo è più sicuro della firma autografa in quanto con gli attuali mezzi tecnologici è possibile clonare, quasi fedelmente, una qualunque firma).

Le informazioni per decodificarla, le informazioni per estrarre l'Hash e il link alla maison, vengono memorizzati su un RFID inserito nel capo; possibilmente, l'inserimento deve essere fatto in

modo che il RFID non possa essere rimosso senza distruggerlo e/o senza danneggiare il capo. Oltre ad essere memorizzate sul RFID, le informazioni vengono trascritte sul Fashion-passport. Ovviamente invece di un RFID si può utilizzare un codice a barre bidimensionale (Kato & Tan, 2007) (si rimanda al par. 5.2.4.2.1 - Tipologie di codici a barre), comunque da tener presente, che le informazioni presenti su un codice a barre sono limitate rispetto a quelle memorizzabili su un RFID.

Un compratore, tramite un opportuno smartphone (oggi sono moltissimi i cellulari dotati di tecnologia in grado di leggere gli RFID) e un'opportuna applicazione software (App) accede alle informazioni presenti sul RFID. Se non tutte fossero presenti sul RFID (scelta discrezionale della casa di moda), lo smartphone si collega alla maison e procede alla consultazione.

L'app quindi chiederebbe all'utente l'acquisizione del particolare "unico" (caratteristica Hylemetrica) da catturare mediante opportune indicazioni. Successivamente, l'acquirente acquisisce il particolare d'identificazione (ad esempio un specifico ricamo), a questo punto l'app provvede ad estrarre l'Hash. Si effettua il controllo tra l'Hash memorizzata e l'Hash estratto; e se le due informazioni "coincidono" si ha la "certezza" che il capo è stato realizzato dal Designer "A" (informazione ricavata dalla corretta decodifica tramite dell'Hash criptato e che il capo è effettivamente quello che si dichiara di essere) fornendo quindi l'informazione sull'originalità del capo.

9.3.4 Esempi di tecniche Hylemetriche utilizzabili

Per poter essere certi della autenticità di un capo di moda, è indispensabile, così come nell'autenticazione biometrica, estrarre le caratteristiche "peculiari" che lo contraddistinguono, così come spiegato in antecedenza.

Tutte le procedure devono prevedere l'individuazione di caratteristiche "uniche" (diverse a seconda del campo di applicazione), non duplicabili (caratteristiche "naturali" non replicabili artificialmente) e stabili (non devono variare durante l'uso e devono avere vita comparabile con quella dell'oggetto).

Ovviamente, se i capi non possiedono, intrinsecamente, una qualche qualità che rispecchia l'unicità, la non-duplicabilità e la stabilità, questa può essere aggiunta artificialmente.

Iniziamo con l'esaminare dei casi dove le caratteristiche "randomiche" sono già presenti. Successivamente vedremo dei casi dove le caratteristiche "uniche" vengono aggiunte artificialmente.

9.3.4.1 Caratteristiche randomiche "naturali"

Osserviamo che in molti materiali naturali esistono delle texture randomiche impossibili da duplicare. Tipici esempi sono la trama di un tessuto; si osservi nella figura sotto dove si nota che la trama dei tessiti, di fatto cambia da zona a zona.

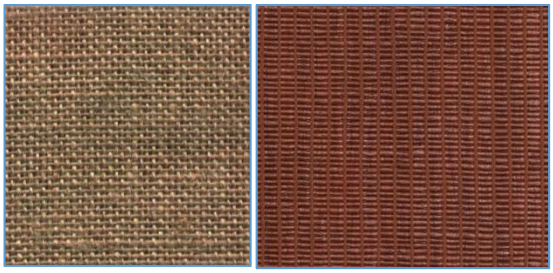


Figura 52 – Tipica trama "randomica" dei tessuti

Altra struttura randomica utilizzabile sono le diverse sfumature di colore che possono essere presenti nei fili delle cuciture (si veda più sotto)

Figura 53 – Sfumatura di colori presenti nei fili delle cuciture

Altro tipico esempio di struttura randomica naturale è la marcatura del pellame. Poiché abbiamo a che fare con un prodotto naturale (la pelle), ogni incisione/marcatura (anche se effettuata con il più sofisticati sistemi tecnologici) sarà differente da un'altra. Sfruttando queste "microscopiche" differenze è possibile identificare in modo univoco l'oggetto.

Figura 54 – Tipica marcatura del pellame

Simile al caso caso precedente, è la struttura di un ricamo manuale. Anche in questo caso, tra due ricami apparentemente identici (se realizzati manualmente) vi sono delle differenze che possono essere utilizzate come cararatteristica Hylemetrica (Figura 55).

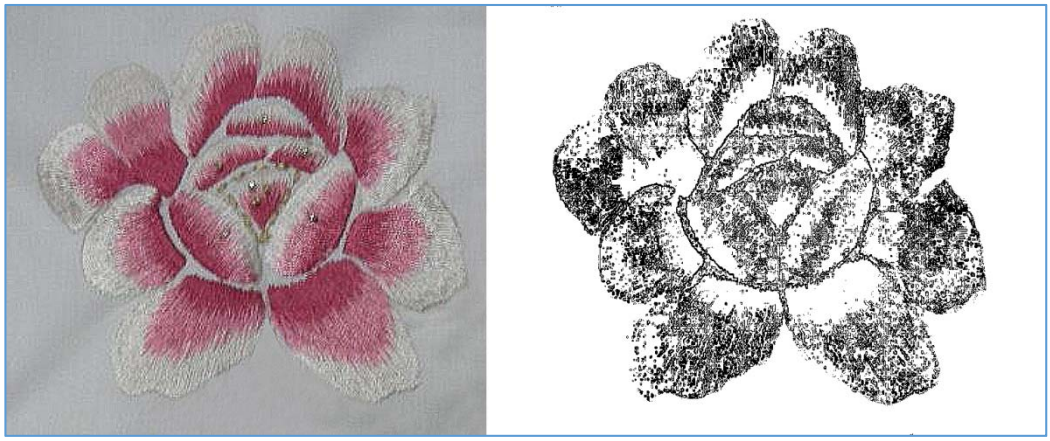


Figura 55 – Caratteristica Hylemetrica estratta da un ricamo fatto a mano

9.3.4.1.1 Esempio di procedura di riconoscimento Hylemetrico

In relazione al caso della marcatura del pellame (Figura 54), vediamo come funziona la nostra procedura d'identificazione (Par 9.3.3)

Il Database (su RFID e/o sul sito della maison) contiene le informazioni relative alla procedura necessaria per la corretta autenticazione. In particolare contiene l'Hash criptato e le informazioni

sulla chiave pubblica del "designer". Inoltre contiene le informazioni sulla zona da acquisire. Acquisita la zona indicata (I_S), da questa viene estratto l'Hash (HP_S); HP_S è ricavato seguendo le procedure e gli algoritmi estratti dal Database (in questo esempi, l'Hash è ottenuto applicando un filtro passa banda e un'opportuna binarizzazione). E' chiaro che Hash memorizzato nel Database "sicuramente" proviene da una zona "lievemente" differente rispetto a quella "catturata". Inoltre, in fase di acquisizione si possono introdurre distorsioni prospettiche e variazioni di scala. Per tali motivi, è indispensabile avere una procedura di registrazione dell'immagine dell'Hash.

Tale registrazione (correzione geometrica) viene realizzata utilizzando dei punti fiduciari memorizzati, come tutto il resto nel Database. Ottenuto l'Hash "registrato" (HP_R – Hash corretto in distorsione, traslazione, rotazione e scala) questo viene confrontato con quello recuperato dal Database dopo la decriptazione con la chiave pubblica del Designer (HP_D). La comparazione viene effettuata utilizzando una correlazione di fase:

$$C_\alpha(\Delta x, \Delta y) = F^{-1}\left[\frac{F^*(HP_D)F(HP_R)}{\left|F^*(HP_D)F(HP_R)\right|^\alpha}\right].$$

Nell'equazione scritta sopra (Δx, Δy) sono le coordinate del picco di correlazione, F e F^{-1} sono, rispettivamente, la trasformata di Fourier diretta e inversa; * indica il complesso coniugato. Il coefficiente α controlla l'ampiezza del picco di correlazione. I valori ottimali vanno da $\alpha = 0$ per un'immagine caratterizzata da un elevato contenuto di frequenze spaziali e alto livello di rumore, a $\alpha = 0.5$ immagine a basso rumore e presenza di bassa frequenza spaziale. Nei nostri esperimenti abbiamo sempre utilizzato $\alpha = 0.5$ valori.

Dobbiamo prendere in considerazione che la registrazione delle immagini non sempre è perfetta. Inoltre, in fase di acquisizione, a causa di polvere o imperfezioni sopravvenute dopo la memorizzazione del Hash nel Database, vi possono essere degli artefatti "posticci". Per queste ragioni, il confronto tra i due Hash viene fatto utilizzando una opportuna soglia. La soglia, così come viene fatto nell'identificazione biometrica, viene scelta minimizzando sia il FRR (*False Rejection Rate*) sia il FAR (*False Acceptance Rate*).

La Figura 56 illustra, in forma schematica, il procedimento di riconoscimento Hylemetrico descritto sopra.

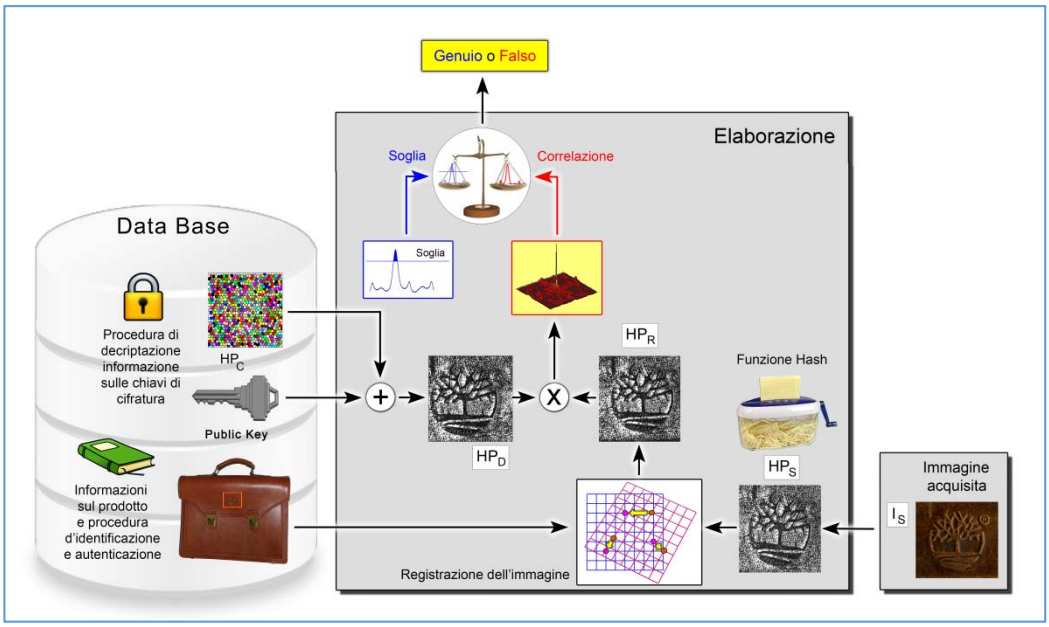


Figura 56 – Procedimento di riconoscimento Hylemetrico

9.3.4.2 Caratteristiche randomiche "artificiali"

Quando le caratteristiche "random" naturali non sono presenti o quando non danno risultato "affidabile" è bene ricorrere all'introduzione artificiale delle caratteristiche Hylemetriche.

9.3.4.2.1 Fibrille fluorescenti

Tutti i capi di moda, possiedono una qualche "etichetta". Questa etichetta può essere realizzata inserendovi delle fibrille metalliche fluorescenti (simili a quelle presenti nella carta moneta e nei passaporti (si veda Figura 0 più sotto).

Figura 57 – Fibrille fluorescenti presenti in una banconota da 10 Euro

Se la “targhetta” è realizzata con queste fibrille, posizionate in modo casuale durante la fase di tessitura della “stoffa” utilizzata per l’etichetta, si ha un ottima caratteristica Hylemetrica (sui veda figura sotto).

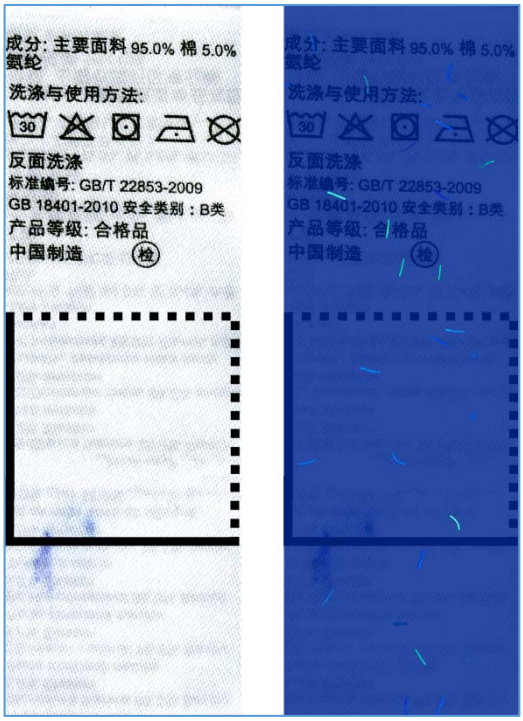


Figura 58 – Etichetta con presenza di fibrille fluorescenti

Sull'etichetta può essere stampato, ad esempio, il bordo di un barcode 2D Datamatrix. Questo bordo risulta utile per effettuare tutte le opportune correzioni geometriche (registrazione) necessarie per la fase di verifica della caratteristica Hylemetrica utilizzata.

In questo esempio, l'Hash può essere ricavato suddividendo "opportunamente" l'area contrassegnata dal bordo del Datamatrix ed assegnando un "1" alle zone dove è presente almeno una fibrilla e uno "0" alle zone prive di "fibrille" (si veda figura di seguito)

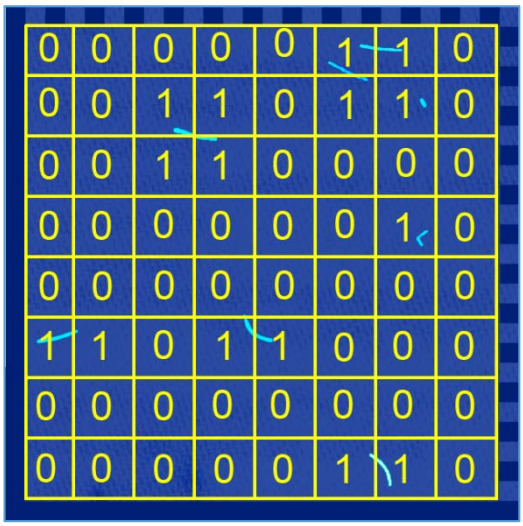


Figura 59 – Etichetta con presenza di fibrille fluorescenti; estrazione dell'Hash

9.3.4.2.2 Inserimento di "verniciatura randomica" fluorescente.

Un'altra tecnica applicabile è quella di utilizzare sull'etichetta, o su una parte dell'oggetto, una tintura/vernice fluorescente sotto illuminazione UV. Quest'inchiostro deve essere spruzzato così da generare a un pattern casuale, simile al campo di speckle che si genera in ottica quando una superficie rugosa viene "illuminata" con luce coerente.

Molte strutture fluorescenti "randomiche" naturali sono presenti in natura. La Figura 60 mostra la spiaggia di Leucadia in California dove dei residui di alghe presenti sulla spiaggia emanano dei bagliori luminosi blu creando una texture molto simile a un pattern "randomico" di speckle.

Figura 60 – Texture randomica fluorescente presente sulla spiaggia di Leucadia in California.

Una struttura “randomica” simile a quella della spiaggia di Leucadia in California, può essere ottenuta spruzzando, ad esempio, su di una etichetta, dell’inchiostro fluorescente.

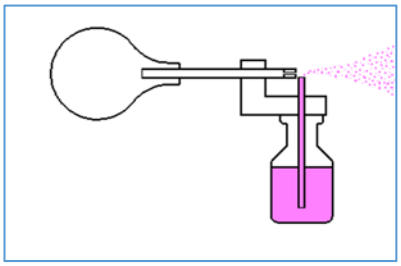


Figura 61 – Un nebulizzatore d’inchiostro/vernice produce delle minuscolo goccioline che si disperdono in modo “randomico” sia spazialmente sia come dimensione geometrica.

La Figura 62 mostra un pattern “randomico” fluorescente ottenuto sull’etichetta di un indumento.

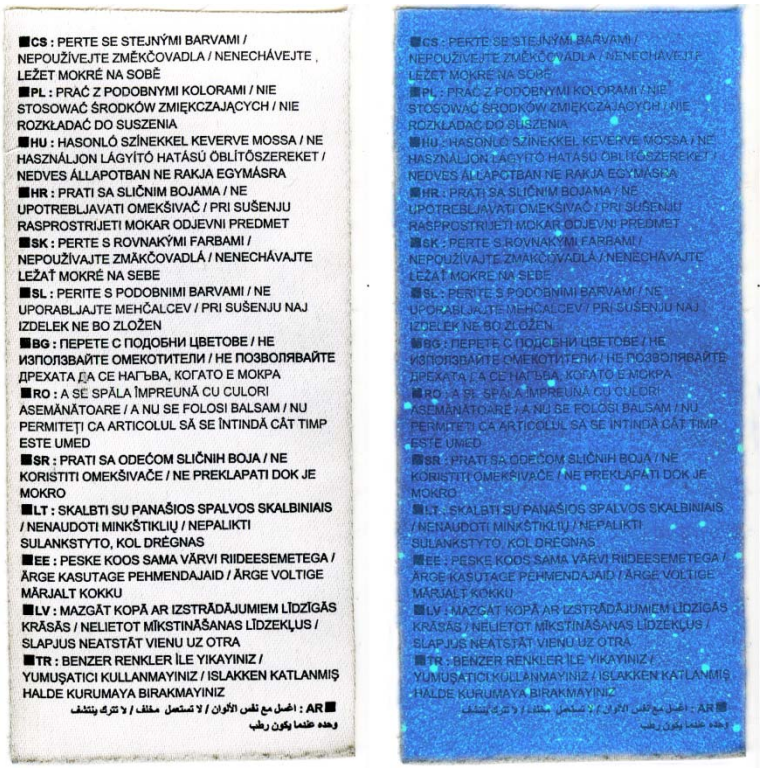


Figura 62 – Immagine di un'etichetta, dove è presente una vernice fluorescente "spruzzata" casualmente" illuminata con luce bianca e con radiazione UV.

Questo pattern ha tutte le proprietà necessarie per essere considerato una caratteristica Hylemetrica. Infatti, qualsiasi etichetta, inchiostrata spruzzando la tintura ha un nebulizzatore, a causa della casualità della generazione delle "goccioline", presenta un campo di speckle differente. Acquisendo l'immagine del pattern fluorescente e suddividendo l'immagine acquisita in blocchi, si può realizzare la funzione Hash attraverso la statistica della dimensione degli speckle. La suddivisione in blocchi garantisce la robustezza del sistema ad eventuali artefatti che possono nascere dopo la realizzazione del Hash memorizzato.

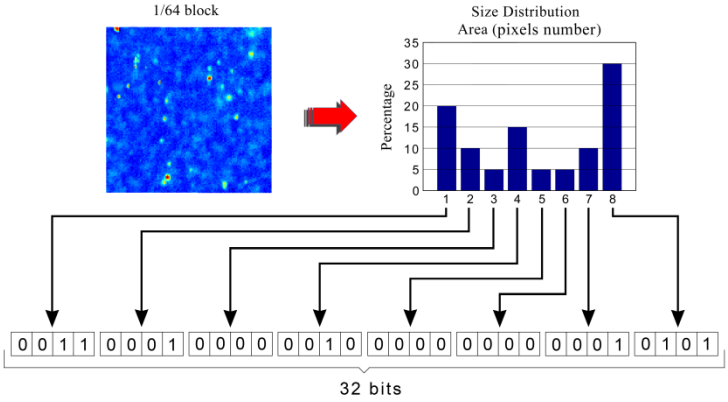


Figura 63 – Statistica estratta da uno dei blocchi ricavati dall'immagine a speckle.

Di seguito sono proposti altri due esempi; all'interno dei capi di moda vengono inserite delle strutture che possono interagire con campi elettromagnetici "esterni".

Una possibilità viene offerta dell'inserimento di strutture metalliche distribuite casualmente. La Figura 64 mostra delle piccole pagliuzze di rame distribuite in modo casuale. Queste pagliuzze possono essere presenti tra la pelle esterna e la fodera di una borsa, così come tra i due strati di una cintura e/o di un portafoglio.

Queste strutture possono essere visualizzare "tramite" telecamere operanti nei THz.

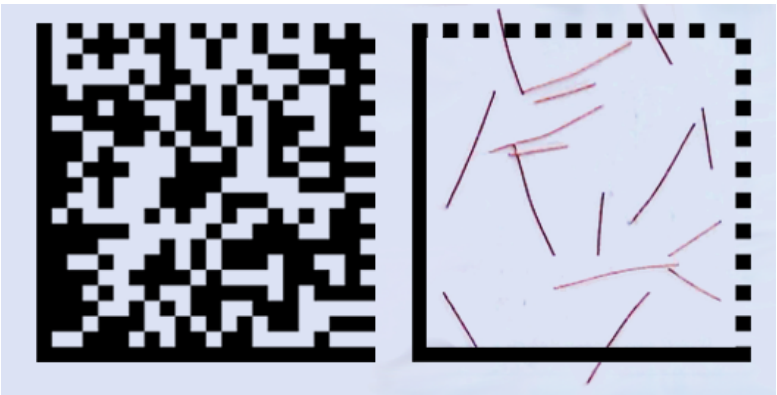


Figura 64 – Statistica estratta da uno dei blocchi ricavati dall'immagine a speckle.

Infine, sempre all'interno di cuciture, possono essere distribuiti sei "piccoli" frammenti di ferrite. Questi frammenti, se investiti da microonde si scaldano e il calore può facilmente essere rivelato da una termocamera. La Figura 65 mostre dei pattern ottenuti con delle etichette di dimensioni di 2 cm x 2 cm scaldate con radiazione da 1 GHz per 1 s.

I pattern ottenuti possono essere trattati come delle caratteristiche Hylemetriche e possono essere elaborati in modo simile ai pattern termici utilizzati per il riconoscimento biometrico facciale (Akhloufi, et al., 2008) (Guzman, 2011) (Guzman, et al., 2013)

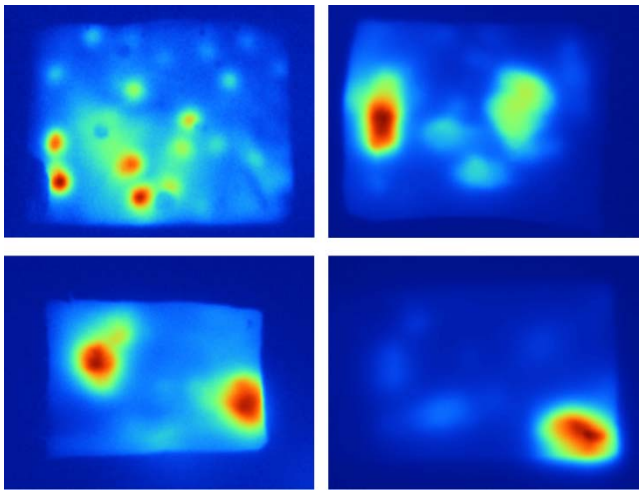


Figura 65 – Pattern di temperatura attenuti irradiando con microonde dei "piccoli" frammenti di ferrite.

10 Conclusioni

In questo lavoro di tesi sono state presentate nuove tecniche che consentono l'autenticazione di oggetti mediante l'utilizzo del paradigma biometrico negli oggetti inanimati (Hylemetria), l'impiego industriale delle tecniche proposte è realizzabile con costi di produzione bassi e livelli di sicurezza, in generale, elevati. I vantaggi mostrati da queste tecniche, rispetto ai sistemi tradizionali sono stati innumerevoli, consentono infatti la salvaguardia e la durata di dati e dei sistemi di protezione posti sugli oggetti, garantendoli da furti, perdite, copie; alla stregua dei dati biometrici.

L'applicabilità della teoria Hylemetria si è dimostrata vasta e diversificata e gli impieghi che consentono un'innovazione sono innumerevoli. Le caratteristiche che consentono ad un oggetto di rispettare la teoria Hylemetrica sono sì rigide ma non restrittive, inoltre come proposto nella tesi è possibile anche introdurre in maniera artificiosa alcune caratteristiche mancanti.

Oggetto della tesi è stata anche la ricerca di una "procedura di autenticazione" atta a consentire la verifica sull'autenticità di un oggetto, fornendo quindi una nuova proposta per combattere la contraffazione. Tale proposta consente l'integrazione fra più tecnologie e fornisce maggior sicurezza sulla provenienza e originalità dell'oggetto, con una metodologia accessibile ad un largo numero di utenti anche con accesso da remoto; il tutto con un elevato livello di sicurezza garantito dall'acquisizione delle strutture random casuali e non duplicabili, alias strutture Hylemetriche, e le ulteriori garanzie offerte dall'impiego della crittografica.

11 Bibliografia e sitografia

Abate, A. F., Nappi, M., Riccio, D. & Sabatino, G., 2007. 2D and 3D face recognition: A survey. *Elsevier,* pp. 1885-1906.

Akhloufi, M., Bendada, A. & Batsale, J., 2008. State of the art in infrared face recognition. *Quantitative InfraRed Thermography Journal,* 5(1), pp. 3-26.

Bauder, D., 1983. *An anti-counterfeiting concept for currency systems,* Albuquerque, NM: Sandia National Labs.

Beckmann, N. & Potkonjak, M., 2009. Hardware-Based Public-Key Cryptography with Public Physically Unclonable Functions. In: *Information Hiding.* s.l.:Springer Berlin Heidelberg, pp. 206-220.

Berardi, L. & Beutelspacher, A., 1996. *Crittologia: Come protegere le informazioni riservate.* Milano: Franco Angeli.

Biermann, J., 1996. *Handbook of Pulping and Papermaking.* II a cura di San Diego, California, USA: Academic Press.

Boyanapally, D., 2008. *Merging of fingerprint scans obtained from multiple cameras in 3d fingerprint scanner system.* s.l.:s.n.

Bringer, J., Chabanne, H. & Icart, T., 2009. *On physical obfuscation of cryptographic algorithms.* India, Springer-Verlag, pp. 88-103.

Buchanan, J. D. R. et al., 2005. 'Fingerprinting' documents and packaging. *Nature,* 28 July.Volume 436.

Bulens, P., Standaert, F.-X. & Quisquater , J.-J., 2010. How to strongly link data and its medium: the paper case. *IET Information Security,* 4(3), pp. 125-136.

Campbell, J. P., 1997. Speker Recognition: a Tutorial. *IEEE - Proceedings of the IEEE,* 85(9), p. 1437–1462.

Colorzip, s.d. *Colorzip.* [Online]
Available at: http://www.colorzip.co.kr/
[Consultato il giorno 14 Marzo 2015].

Commission on Engineering and Technical Systems (CETS), 1993. *Counterfeit Deterrent Features for the Next-Generation Currency Design,* s.l.: The National Academic Press.

Daugman, J., 1998. Recognizing people by their iris patterns. *Elsevier,* 3(1), pp. 33-39.

Daugman, J., 2004. How Iris Recognition Works. *IEEE,* 14(1), pp. 21-30.

Davenport, H., 1994. *Aritmetica superiore.* Bologna: Zanichelli.

Diavy S.r.l., s.d. s.l.:s.n.

Diffe, W., 1988. The First Ten Years of Public-Key Cryptography,. *Proceedings of the IEEE,* 76(5), pp. 560-577.

Diffie, W. & Hellman, M. E., 1976. New directions in cryptography. *IEEE Transactions on Information Theory,* Volume 22, pp. 644-654.

ElGamal, T., 1985. A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms. *IEEE Transactions on Information Theory,* IT-31(4), pp. 469-472.

Faraj, M. & Bigun, J., 2007. *"Audiovisual person authentication using lip-motion from orientation maps", Pattern Recognition Letters.* s.l.:s.n.

Freeman, J. B. & Ambady, N., 2010. MouseTracker: Software for studying real-time mental processing using a computer mouse-tracking method.. *Behavior Research Methods,* 42(1), pp. 226-241.

Gabor, D., 1948. A new microscopic principle. *Nature,* 15 May, 4098(161), pp. 777-778.

Gassend, B., 2003. *Physical Random Functions.* Massachusetts: Massachusetts Institute of Technology.

Gassend, B., Clarke, D., van Dijk, M. & Devadas, S., 2002. *Silicon physical random functions..* New York, NY, USA, ACM - Press, pp. 148 - 160.

Giuntella, I., 2014. *ilsole24ore.* [Online]
Available at: http://www.ilsole24ore.com/art/notizie/2014-01-15/il-parlamento-ue-mette-freno-frodi-alimentari-arrivo-etichettatura-test-dna-e-sanzioni-191039.shtml?uuid=AB60lyp

Goodman, J. W., 1984. Topics in Applied Physics: Laser Speckle and Related Phenomena. In: Berlino: Springer.

Guajardo, J., Kumar, S. S., Schrijen, G. J. & Tuyls, P., 2007. *FPGA intrinsic PUFs and their use for IP protection..* s.l., s.n., pp. 63-80.

Guajardo, J. et al., 2009. Anti-counterfeiting, key distribution, and key storage in an ambient world via physical unclonable functions. *Journal Information Systems Frontiers,* 11(1), pp. 19-41.

Guzman, A. M., 2011. *Thermal Imaging As A Biometrics Approach To Facial Signature Authentication.* s.l.: FIU Electronic Theses and Dissertations.

Guzman, A. M. et al., 2013. Thermal Imaging as a Biometrics Approach to Facial Signature Authentication. *IEEE Journal of Biomedical and Health Informatics,* 17(1), pp. 214-222.

Hammouri, G. D. A. S. B., 2009. *CDs Have Fingerprints Too.* Berlin, Heidelberg, Springer-Verlag, p. 348–362.

Helinski, R., Acharyya, D. & Plusquellic, J., 2009. *A physical unclonable function defined using power distribution system equivalent resistance variations.* New York, NY, s.n., p. 676–681.

Hellman, M. E., 1978. An Overview of Public Key Cryptography. *IEEE Communications Society Magazine,* Novembre, Volume 16, pp. 24-32 (Invited Paper).

Holcomb, D., Burleson, W. P. & Fu, K., 2007. *Initial SRAM state as a fingerprint and source of true random numbers for RFID tags..* s.l., s.n.

Huby, P., 1974. *"Review: Matter in Aristotle", The Classical Review.* s.l.:s.n.

Iannarelli, A., 1989. *Ear Identification (Forensic Identification Series).* s.l.:Paramont Pub.

Indeck, R. & Muller, M., 1994. *Method and apparatus for fingerprinting magnetic media.* s.l. Brevetto n. US Patent No. 5365586.

Indeck, R. S. & E., G., 1993. Fingerprinting magnetic media. *IEEE transactions on magnetics,* 29(6), pp. 4095 - 4097.

Istituto Poligrafico e Zecca dello Stato S.p.A, s.d. [Online]
Available at: http://www.ipzs.it/

Jain, A. K. & Kumar, A., 2012. Biometric recognition: an overview. In: *Second Generation Biometrics: The Ethical, Legal and Social Context.* s.l.:Springer, pp. 49-79.

Jain, S. Z. L. & Anil, K., 2005. *Handbook of Face Recognition.* New York: Springer-Verlag.

Johnson, D. P., Dobbs, R. & Ge, C., 2011. *Anti-Counterfeiting Technology in product design and manufacturing: an opportunity for engineering technology programs.* [Online].

Kato, H. & Tan, K., 2007. Pervasive 2D Barcodes for Camera Phone Applications. *IEEE Pervasive Computing,* 6(4), pp. 76-85.

Katz, J. & Lindell, Y., 2007. *Introduction to Modern Cryptography: Principles and Protocols.* s.l.:CRC Press - Taylor&Francis Group.

Koblitz, N., 1987. Elliptic Curve Cryptosystems. *Mathematics of Computation,* 48(17), pp. 203-209.

Kukreja, U., Stevenson, W. E. & Ritter, 2005. RUI - Recording User Input from interfaces under Windows and Mac OS X. p. 656–659.

Kumar, A. & Prathyusha, . K. V., 2009. Personal authentication using hand vein triangulation and knuckleshape. *IEEE Trans,* p. 2127–2136.

Kumar, S. et al., 2008. *Extended abstract: The buttery PUF protecting IP on every FPGA..* s.l., IEEE, pp. 67-70.

Kursawe, K., Sadeghi, A., Schellekens, D. & Skoric, B., 2009. *Reconfigurable Physical Unclonable Functions - Enabling technology for tamper-resistant storage.* s.l., s.n., pp. 22 - 29.

Lee, J. et al., 2004. *A technique to build a secret key in integrated circuits for identification and authentication application.* s.l., IEEE, pp. 176 - 179.

Lee, L., Berger, T. & Aviczer, E., 1996. Reliable On-Line Human Signature Verification Systems. *IEEE,* 18(6), pp. 643-647.

Lim, D., 2004. *Extracting Secret Keys from Integrated Circuits.* MIT, MA, USA: s.n.

Lofstrom, K., Daasch, W. & Taylor, D., 2000. *IC Identification Circuit Using Device Mismatch..* San Francisco, CA, USA, IEEE, p. 372–373.

Magneprint, s.d. [Online]
Available at: http://www.magneprint.com/

Majzoobi, M., Koushanfar, F. & Potkonjak, M., 2008. *Testing techniques for hardware security..* s.l., s.n., pp. 1-10.

Majzoobi, M., Koushanfar, F. & Potkonjak, M., 2009. Techniques for design and implementation of secure reconfigurable PUFs. *ACM Transactions on Reconfigurable Technology and Systems (TRETS)*, 1 3, 2(1), p. 5.

Mariëlle Leijten, L. V. W., 2013. Keystroke Logging in Writing Research: Using Inputlog to Analyze and Visualize Writing Processes. *SAGE,* 30(3), pp. 358-392.

Menezes, A. J., van Oorschot, P. C. & Vanstone, S., 1996. *Handbook of Applied Cryptography.* ISBN 9781439821916 a cura di FL- USA: CRC Press - Taylor&Francis Group Boca Raton.

Mills, E. & CNET, 2011. *cnet.com.* [Online]
Available at: http://www.cnet.com/news/watermarks-tap-old-trick-for-mobile-media/

Nalwa, V., 1997. Automatic On-Line Signature Verification. *IEEE,* 85(2), p. 215–239.

NIST, 2013. *Digital Signature Standard (DSS),* Gaithersburg: National Institute of Standards and Technology.

Nixon, M. S. et al., 1999. Automatic Gait Recognition, Biometrics: Personal Identification in Networked Society. *Kluwer Academic Publishers,* p. 231–249.

Novelli, E. et al., 2011. Utilizzo a scopo analitico degli isotopi stabili di carbonio, azoto, ossigeno e idrogeno per la descrizione dell'autenticità di prodotto. *Italian Journal of Food Safety*, 1(1).

Pappu, R., Recht, B., Taylor, J. & Gershenfeld, 2002. Physical one-way functions. *Nature,* September, 297(5589), p. 2026–2030.

Puhan, N., Sudha, N. & Hegde, S. A., 2011. *A new iris liveness detection method against contact lens spoofing.* Singapore, IEEE, pp. 71-74.

Purkait, R. & Singh, P., 2008. A test of individuality of human external ear pattern: Its application in the field of personal identification. *Elsevier,* Volume 178(2–3), p. 112–118.

Rabin, M., 1979. Digitalized signatures and public-key functions as intractable as factorization. *MIT Laboratory for Computer Science.*

Ramesh, K. P. & Rao, K. N., 2009. *Pattern extraction methods for ear biometrics.* s.l., s.n., p. 1657–1660.

Renesse, v., 1995. *European Convention on Security and Detection.* London, s.n., pp. 45-49.

Rivest, R. L., Shamir, A. & Adleman, L., 1978. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. *Communications of the ACM ,* 21(2), pp. 120-126.

Rubin, F. & A., M., 1997. *Authentication Via Keystroke Dynamics.* Zurich, Switzerland, s.n., p. 48–56 .

Ruhrmain, U., 2009. *Simpl systems: On a public key variant of physical unclonable functions.,* s.l.: Cryptology ePrint Archive.

Ruhrmair, U., Solter, J. & Sehnke, F., 2009. *On the foundations of physical unclonable functions.,* s.l.: Cryptology ePrint Archive.

SANGEETHA, S. P. & KARNAN, M., 2014. Survey of biometric systems using iris recognition. *International Journal of Engineering Science and Technology,* 6(2), p. 40–44.

Schirripa Spagnolo, G., Cozzella, L. & Simonetti, C., 2010. Banknote security using a biometric-like technique: a hylemetric approach. *Measurement Science and Technology,* 26 Marzo.21(5).

Schirripa Spagnolo, G., Simonetti, C. & Cozzella, L., 2004. Superposed strokes analysis by conoscopic holography as an aid for a handwriting expert. *J. Opt. A: Pure Appl. Opt.,* Volume 6, pp. 869-874.

Security Hologram, 2015. *http://www.hologramsindia.net/.* [Online]
Available at: http://www.hologramsindia.net/e-beam-security-holograms.html
[Consultato il giorno 10 March 2015].

Sharma, G., Sharma, R. & Nigam, P., 2012. Recognition of Human Iris Patterns for Biometric Identification. *VSRD International Journal of Electrical, Electronics & Communication & Engineering,* 2(6), pp. 353-358.

Skoric, B., 2009. *Quantum readout of physical unclonable functions: Remote authentication without trusted readers and authenti-cated quantum key exchange without initial shared secrets.,* s.l.: Cryptology ePrint Archive.

Smith, J. R. &. S., 1999. New York, IEEE, p. 79–83.

Srivathsa, S., 2012. *Secure and Energy Efficient Physical Unclonable Functions.* s.l.:s.n.

Suh, G. E. & Devadas, S., 2007. *Physical unclonable functions for device authentication and secret key generation..* New York, NY, USA, ACM press, p. 9.

Sumalatha, K. A. & Harsha, H., 2014. Biometric Palmprint Recognition System: A Review. *International Journal of Advanced Research in Computer Science and Software Engineering,* 4(1), pp. 429-433.

Su, Y., Holleman, J. & Otis, B., 2007. *A 1.6pj/bit 96% stable chip-id generating circuit using process variations.* s.l., IEEE International, pp. 406-611.

Theoharisa, T., Passalisa, G., Todericib, G. & Kakadiarisb, I. A., 2008. Unified 3D face and ear recognition using wavelets on geometry images. *Elsevier,* Volume 41(3), pp. 796-804.

Tolk, K., 1992. *Reflective particle technology for identification of critical components.* Orlando, FL (United States), s.n., pp. 19-22 .

Unar, J., Seng, W. C. & Abbasi, A., 2014. A review of biometric technology along with trends and prospects – Elsevier, Febbraio 2014]. *Pattern Recognition Society, Elsevier,* 08, 47(8), p. 2673–2688.

Veritec, s.d. [Online]
Available at: www.veritecinc.com/vericode

Vivekraja, V. N. L., 2009. *Circuit-level techniques for reliable physically uncloneable functions.* s.l., Proceedings of the 2009 IEEE International Workshop on Hardware-Oriented Security and Trust,, p. 30.

Voloch-Bloch, N. et al., 2013. Generation of electron Airy beams. *Nature,* 21 Febbraio, 494(7437), pp. 331-335.

Vrijaldenhoven, S., 2005. *Acoustical Physical Uncloneable Functions.* Eindhoven, the Netherlands: s.n.

Wikipedia, 2015. *Wikipedia.* [Online]
Available at: http://it.wikipedia.org/wiki/Filigrana_(codicologia)],

Willems F.M.J., S. Y. T. T., 1995. The context tree weighting method: Basic properties. *IEEE Transactions on Information Theory*, Volume 41, p. 653–664.

Wilson, C. et al., 2004. *Fingerprint Vendor Technology Evaluation 2003: Summary of Results and Analysis Report,* s.l.: s.n.

Woittennek, F. et al., 2014. Design of a MEMS-based retina scanning system for biometric authentication. *SPIE,* Volume 9130, p. 10.

World Health Organization, 2014. *Anti-counterfeit Technologies for the protection of Medicines,* Ginevra, Svizzera: s.n.

Yin, C. & Qu, G., 2009. *Temperature-aware cooperative ring oscillator PUF.* Washington, DC, USA, IEEE Computer Society, p. 36.

Yuan, L. & Mu, Z. c., 2012. Ear recognition based on local information fusion. *Elsevier,* Volume 33(2), p. Pages 182–190.

Zhanga, D., Liub, Z. & Yanc, J.-q., 2010. Dynamic tongueprint: A novel biometric identifier. *Elsevier,* Volume 43(3), p. 1071–1082.

Zhang, D., Kong, W.-K., You, J. & Wong, M., 2003. Online palmprint identification. *IEEE,* 25(9), pp. 1041 - 1050.

Zhang, X. & Gao, Y., 2009. Face recognition across pose: A review. *Elsevier,* pp. 2876 - 2896.