Ministero dello Sviluppo Economico

Ricevuta di presentazione

per

Brevetto per invenzione industriale

Domanda numero: 102019000007290

Data di presentazione: 27/05/2019

DATI IDENTIFICATIVI DEL DEPOSITO

Ruolo	Mandatario
Depositante	Filippo Ferroni
Data di compilazione	27/05/2019
Riferimento depositante	PLT055
Titolo	Apparato d'utente e metodo di protezione di dati riservati
Carattere domanda	Ordinaria
Esenzione	NO
Accessibilità al pubblico	NO
Numero rivendicazioni	13
Autorità depositaria	

PRIVACY

Autorizzo il trattamento dei dati personali, inseriti all'interno del deposito, ai sensi del GDPR (Regolamento UE 2016/679) e del Decreto Legislativo 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali"

RICHIEDENTE/I

Natura giuridica	Persona giuridica
Denominazione	POLITECNICO DI TORINO
Partita IVA	00518460019
Tipo Società	le universita'
Nazione sede legale	Italia
Comune sede legale	Torino (TO)
Indirizzo	Corso Duca degli Abruzzi
Civico	24
CAP	10129
Telefono	
Fax	
Email	
Pec	

Quota percentuale	50.0%
Natura giuridica	Persona giuridica
Denominazione	TOOTHPIC S.r.l.
Partita IVA	03686180047
Tipo Società	societa' a responsabilita' limitata
Nazione sede legale	Italia
Comune sede legale	Torino (TO)
Indirizzo	Corso Castelfidardo
Civico	30/a
CAP	10129
Telefono	
Fax	
Email	
Pec	
Quota percentuale	50.0%

DOMICILIO ELETTIVO

Cognome/R.sociale	Metroconsult Milano S.r.l.
Indirizzo	via Palestro 5/6
Cap	16122
Nazione	Italia
Comune	Genova (GE)
Telefono	010 - 8196592
Fax	010 - 813268
Email\PEC	genova@pec.metroconsult.it

MANDATARI/RAPPRESENTANTI

Cognome	Nome
Bianco	Mirco
Pancot	Gian Antonio
Ferroni	Filippo

INVENTORI

Cognome	Nome	Nazione residenza
MAGLI	Enrico	Italia
COLUCCIA	Giulio	Italia
VALSESIA	Diego	Italia
BIANCHI	Tiziano	Italia

CLASSIFICAZIONI

Sezione	Classe	Sottoclasse	Gruppo	Sottogruppo

NUMERO DOMANDE COLLEGATE

DOCUMENTAZIONE ALLEGATA

Tipo documento	Riserva	Documento
Descrizione in italiano*	NO	PLT055_DESCRIZIONE firmata.pdf hash: 58916e345a57f51762ec37507fb642dd
Disegni	NO	PLT055_DISEGNI firmati.pdf hash: 262ab82b7cb16292fb2780c871fc2b60
Riassunto	NO	PLT055_RIASSUNTO firmato.pdf hash: 425333dc08344cd4ef96dd721daeb501
Rivendicazioni	NO	PLT055_RIVENDICAZIONI firmate.pdf hash: c81e6aaf34f23a1ce0ec72f0569a1b71
Lettera di Incarico	SI	hash:
Lettera di Incarico	SI	hash:
Rivendicazioni in inglese	SI	hash:

PAGAMENTI

Tipo	Identificativo	Data
Bollo	01171640362017	09/08/2018

DOVUTO

Gli importi indicati non tengono conto delle eventuali esenzioni applicabili

Importo Tasse:	€ 185,00
Importo Imposta Bollo:	€ 40,00

NOTE

RIASSUNTO

L'invenzione consiste in un metodo ed in un apparato d’utente (1) per la protezione di dati riservati, dove detto apparato comprende un sensore di immagini (14) e mezzi di elaborazione (11) configurati per acquisire una pluralità di immagini mediante detto sensore di immagini (14), generare un’impronta sensore sulla base di detta pluralità di immagini, codificare almeno una porzione di detta impronta sensore utilizzando un algoritmo di proiezioni casuali in modo da generare un’impronta compressa (W), cifrare e/o decifrare detti dati riservati utilizzando detta impronta compressa (W) come chiave.

(figure 2 e 5)

PLT055

Descrizione dell'Invenzione Industriale dal titolo:

"APPARATO D'UTENTE E METODO DI PROTEZIONE DI DATI RISERVATI"

A nome di

- POLITECNICO DI TORINO (titolare al 50% dell'invenzione), di nazionalità italiana, con sede in Corso Duca degli Abruzzi 24, 10129 Torino;
- TOOTHPIC S.r.l. (titolare al 50% dell'invenzione) di nazionalità italiana, con sede in Corso Castelfidardo 30/a, 10129 Torino;

ed elettivamente domiciliati, ai fini del presente incarico, presso i Mandatari Mirco BIANCO (No. Iscr. Albo 1639B), Filippo FERRONI (No. Iscr. Albo 530BM), Marco CAMOLESE (No. Iscr. Albo 882BM), Giancarlo REPOSIO (No. Iscr. Albo 1168BM), Corrado BORSANO (No. Iscr. Albo 446 BM) e Matteo BARONI (No. Iscr. Albo 1064 BM) c/o Metroconsult Milano S.r.l., Via Palestro 5/2, 16122 GENOVA (GE).

Inventori designati:

- **MAGLI Enrico**, di nazionalità italiana, residente in Via Ferrante Aporti 28, 10131 Torino, Italia;
- **COLUCCIA Giulio**, di nazionalità italiana, residente in Via Leonardo da Vinci, 9/1, 10095 Grugliasco, Torino, Italia;
- **VALSESIA Diego**, di nazionalità italiana, residente in Via Bogogno 8, 28021 Borgomanero, Novara, Italia;
- **BIANCHI Tiziano**, di nazionalità italiana, residente in Viale Alcide De Gasperi 63, 59100 Prato, Italia.

DESCRIZIONE

La presente invenzione si riferisce ad un apparato d'utente (user equipment; come uno smartphone, un tablet, un personal computer, un laptop, o altro) e ad un metodo per la protezione di dati riservati; in particolare per cifrare/decifrare una chiave crittografica privata.

Come è noto, i sistemi di autenticazione elettronica secondo lo stato dell'arte si basano su tecniche di crittografia asimmetrica. L'utilizzo di queste tecniche richiede che a ciascun utente/dispositivo venga assegnata una coppia di stringhe generate in maniera (pseudo)casuale dette chiavi, ossia una 'chiave pubblica' ed una 'chiave privata'. La chiave privata è il segreto (non condiviso) che consente di autenticare l'utente/dispositivo. Essa deve essere custodita dall'utente/dispositivo e mai condivisa pubblicamente. Al contrario, la chiave pubblica è l'informazione che l'utente può e deve divulgare per consentire il funzionamento dei sistemi basati su questo tipo di crittografia. Ad esempio, nel caso in cui l'utente A vuole inviare all'utente B un messaggio criptato, l'utente A deve essere in possesso della chiave pubblica di B, con la quale cripta il messaggio e lo invia all'utente B. L'utente B, essendo l'unico soggetto in possesso della sua chiave privata, è l'unico soggetto in grado di decodificare il messaggio; infatti, la decodifica del messaggio cifrato con la chiave pubblica di B può avvenire solo tramite la chiave privata dell'utente B.

Un altro esempio in cui sono utilizzate le tecniche di crittografia asimmetrica per l'autenticazione è quello in cui si utilizza la cosiddetta 'firma digitale', che permette ad un utente A di verificare l'identità dell'utente B. In questo scenario, l'utente A invia all'utente B un messaggio, detto challenge, dopodiché l'utente B firma il challenge usando la propria chiave privata, e invia il messaggio firmato

all'utente A. L'utente A, in possesso della chiave pubblica dell'utente B, può verificarne l'identità verificando con la chiave pubblica la firma dell'utente B e la consistenza del messaggio.

Esistono diverse soluzioni secondo lo stato dell'arte per custodire la chiave privata, come la memorizzazione su hardware dedicato rimovibile (ad esempio un token USB, una smart card, un hardware ledger per criptomonete o altro), la memorizzazione su memoria non volatile (in chiaro o cifrata), l'esecuzione delle applicazioni che possono accedere a tale chiave in un ambiente di esecuzione sicuro (*Trusted Execution Environment*), la memorizzazione in un chip crittografico dedicato (noto anche con il termine di *Secure Element*) contenuto all'interno di uno smartphone, e la memorizzazione in cloud.

Ciascuno di questi sistemi appena elencati presenta però dei problemi e/o delle vulnerabilità. Infatti, la memorizzazione su hardware dedicato esterno presenta lo svantaggio che l'utente deve portare con sé tutto l'hardware necessario (il token per accedere al servizio, il token per firmare, la smartcard, il lettore di smartcard, ecc.). Inoltre, l'hardware dedicato potrebbe non essere di uso generico (*general purpose*), potrebbe cioè consentire solo determinate operazioni, o solo con le chiavi precaricate in fase di fabbricazione. Potrebbe, inoltre, presentare problemi di interfaccia; infatti, risulta molto spesso impossibile collegare un token USB ad uno smartphone.

La memorizzazione nella memoria locale del dispositivo in chiaro risulta, invece, essere vulnerabile ad un qualsiasi utente malintenzionato (*malicious user*) in possesso delle credenziali di accesso al device.

La memorizzazione criptata su memoria locale non volatile è vulnerabile a un qualsiasi utente malintenzionato in possesso

delle credenziali di accesso al device ed in grado di effettuare una copia della memoria e di decriptare (offline) il contenuto della memoria.

L'esecuzione delle applicazioni che possono accedere a tale chiave in un ambiente di esecuzione sicuro (*Trusted Execution Environment*), ossia in un'area virtualizzata del processore e della memoria RAM del dispositivo, non accessibile a tutte le applicazioni del sistema, ma solo a quelle appositamente realizzate, presenta una minore flessibilità nella realizzazione delle applicazioni, poiché una maggiore sicurezza corrisponde a minori possibilità da parte di applicazioni terze e ad una maggior richiesta di memoria e di potenza di calcolo per realizzare l'ambiente virtuale; inoltre, l'ambiente di esecuzione sicuro offre una maggiore "superficie di attacco", poiché, essendo basato su un'implementazione software, può essere modificato (in modo malevolo) disponendo dei privilegi adatti.

La memorizzazione in un chip crittografico dedicato presenta lo svantaggio di essere poco flessibile come già descritto per l'hardware dedicato esterno. Le versioni aggiornabili di tali chip crittografici presentano, invece, delle vulnerabilità. Infatti, i dati al loro interno sono scritti su memoria riscrivibile, rendendo comunque possibile la creazione di cloni (come è possibile per gli ambienti di esecuzione sicuri).

La memorizzazione dei dati in cloud richiede la connessione a Internet e richiede inoltre che i server su cui sono custodite le chiavi siano sicuri (livello di sicurezza di cui ci si deve fidare, poiché gli apparati in cui avviene fisicamente la memorizzazione non sono sotto il diretto controllo dell'utente proprietario delle chiavi).

Risulta evidente come queste vulnerabilità permettano ad una terza persona di effettuare il cosiddetto furto di identità

elettronica (*electronic identity theft*), consentendo a detta terza persona di mettere in atto i suoi intenti criminali, come trasferire i soldi dal conto bancario di un utente verso un altro conto, inviare messaggi di posta elettronica dall'account dell'utente verso tutti gli altri indirizzi presenti nella rubrica dell'utente minimizzando gli effetti dei filtri anti-spam, vendere l'identità rubata ad un'altra persona, o altro.

La presente invenzione si propone di risolvere questi ed altri problemi mettendo a disposizione un metodo per la protezione di dati riservati come da rivendicazioni allegate.

Inoltre, la presente invenzione mette anche a disposizione un apparato d’utente per la protezione di dati riservati come da rivendicazioni allegate.

L’idea alla base della presente invenzione è di configurare un apparato d’utente in modo da acquisire una pluralità di immagini mediante un sensore di immagini compreso in detto apparato, generare un’impronta sensore sulla base di detta pluralità di immagini, codificare almeno una porzione di detta impronta sensore utilizzando un algoritmo di proiezioni casuali in modo da generare un’impronta compressa, e cifrare e/o decifrare detti dati riservati utilizzando detta impronta compressa come chiave.

In questo modo, è possibile aumentare la sicurezza di un sistema di autenticazione; infatti, risulta essere particolarmente complesso (se non impossibile) compiere un furto d'identità rubando una chiave privata cifrata utilizzando un’impronta compressa come chiave, poiché per decifrare detta chiave privata cifrata è necessario possedere l’impronta del sensore di immagini che, per essere determinata richiede di aver accesso al terminale d’utente con i diritti di accesso sufficienti ad utilizzare il sensore di immagini di detto apparato d’utente.

Inoltre, nel caso in cui una terza persona (l'attaccante) riuscisse a generare un'impronta del sensore di immagini in maniera fraudolenta (ad esempio acquisendo delle foto scattate mediante detto sensore direttamente dal terminale d'utente o da Internet), sarebbe comunque possibile riportare il sistema di autenticazione nuovamente in uno stato sicuro utilizzando un nuovo seme per generare una nuova impronta compressa mediante l'algoritmo di proiezioni casuali, e cifrando una nuova chiave privata utilizzando detta nuova impronta compressa come chiave.

Si evidenzia anche che, memorizzando in maniera sicura le chiavi negli apparati d'utente, è possibile utilizzare vantaggiosamente apparati già in possesso degli utenti, evitando così il costo di acquisto e gestione di hardware dedicato; inoltre, questa soluzione tecnica risulta essere molto flessibile, poiché consente l'offuscamento di chiavi già in possesso degli utenti ed un utilizzo universale in sistemi di autenticazione già funzionanti. Infatti, tale soluzione può essere utilizzata come un livello aggiuntivo di sicurezza, in grado di rendere possibile l'utilizzo di una chiave soltanto se è disponibile l'impronta del sensore della camera.

Ulteriori caratteristiche vantaggiose della presente invenzione sono oggetto delle allegate rivendicazioni.

Queste caratteristiche ed ulteriori vantaggi della presente invenzione risulteranno maggiormente chiari dalla descrizione di una sua forma di attuazione mostrata nei disegni annessi, forniti a puro titolo esemplificativo e non limitativo, in cui:

- fig. 1 illustra un sistema di autenticazione comprendente un apparato d'utente secondo l'invenzione;
- fig. 2 illustra uno schema a blocchi dell'apparato d'utente di fig. 1;
- fig. 3 illustra un diagramma di flusso che rappresenta il

funzionamento del sistema di fig. 1 durante una sessione di registrazione;

- fig. 4 illustra un diagramma di flusso che rappresenta il funzionamento del sistema di fig. 1 durante una sessione di autenticazione;
- fig. 5 illustra un diagramma di flusso che rappresenta un metodo di protezione di dati riservati secondo l'invenzione.

Il riferimento ad "una forma di attuazione" all'interno di questa descrizione sta ad indicare che una particolare configurazione, struttura o caratteristica è compresa in almeno una forma di attuazione dell'invenzione. Quindi, i termini "in una forma di attuazione" e simili, presenti in diverse parti all'interno di questa descrizione, non sono necessariamente tutti riferiti alla stessa forma di attuazione. Inoltre, le particolari configurazioni, strutture o caratteristiche possono essere combinate in ogni modo adeguato in una o più forme di attuazione. I riferimenti utilizzati nel seguito sono soltanto per comodità e non limitano l'ambito di tutela o la portata delle forme di attuazione.

Con riferimento a fig. 1, verrà ora descritto un sistema di autenticazione S, ad esempio operante secondo lo standard WebAuthn (promosso dalla FiDO Alliance), in un tipico scenario di utilizzo; tale sistema di autenticazione S comprende le seguenti parti:

- un apparato d'utente 1 secondo l’invenzione, come ad esempio uno smartphone, un tablet o altro;
- un server applicativo 2 atto ad erogare almeno un servizio (come ad esempio un servizio di rete sociale, di posta elettronica, di trading, di home banking, di e-commerce, di banking online, di scambio (exchange) per criptovalute, o altro) che richiede l'autenticazione dell'apparato d'utente

1, ossia che necessita di accertare che l'apparato d’utente 1 sia lo stesso apparato d'utente a cui è stato associato un particolare account nel corso di una fase di registrazione (meglio descritta nel seguito di questa descrizione) e a cui sono associati dei servizi privati e/o personali (ad esempio l'accesso al proprio conto corrente o a quello di una società, l'accesso al proprio profilo o quello di una società su un servizio di rete sociale come Facebook, o altro).

L'apparato d'utente 1 ed il server applicativo 2 sono in comunicazione di segnale tra loro mediante una rete dati, preferibilmente una rete dati di tipo pubblico (come ad esempio Internet).

Il server applicativo 2 può essere costituito da uno o più server opportunamente configurati per formare un cluster, ed è preferibilmente configurato per inviare all’apparato d’utente almeno una richiesta di autenticazione dopo che l’apparato d’utente 1 ha richiesto a detto server applicativo 2 l’accesso a servizi privati e/o personali, ossia a servizi che richiedono l’autenticazione di detto apparato d’utente 1; tale richiesta di autenticazione comprende preferibilmente una stringa di caratteri (che rappresenta ad esempio l’orario di tale richiesta) che l’apparato d’utente 1 deve ritornare firmata utilizzando la sua firma privata, così che il server applicativo 2 possa autenticare detto apparato d’utente 1 utilizzando la chiave pubblica associata a detta chiave privata.

L'apparato d'utente 1 comprende un sensore di immagini 14 (come ad esempio un sensore fotografico, un sensore per la visione notturna, o altro); tale apparato d'utente 1 può anche essere costituito alternativamente da un personal computer, da un laptop, o da un altro dispositivo elettronico in comunicazione di segnale con un sensore di immagini (come ad

esempio una webcam), preferibilmente compreso (integrato) all'interno di detto dispositivo.

Il server applicativo 2 comprende alcuni elementi funzionalmente simili a quelli dell'apparato d'utente 1 (ossia mezzi di controllo ed elaborazione, mezzi di memoria volatile, mezzi di memoria di massa, i mezzi di comunicazione e i mezzi di ingresso/uscita) in comunicazione di segnale tra loro e configurati per eseguire delle differenti funzioni che verranno meglio descritte nel seguito di questa descrizione; inoltre, tale server applicativo 2 può anche coincidere con l'apparato d'utente 1 nel caso in cui il servizio che richiede l'autenticazione dell'apparato d'utente 1 sia eseguito direttamente da detto apparato d'utente 1.

Con riferimento anche a fig. 2, l'apparato d'utente 1 (come ad esempio uno smartphone, un tablet o altro) secondo l'invenzione comprende i seguenti componenti:

- mezzi di controllo ed elaborazione 11 (detti anche mezzi di elaborazione), come ad esempio una o più CPU, che governano il funzionamento del dispositivo 1, preferibilmente in modo programmabile, mediante l'esecuzione di apposite istruzioni;
- mezzi di memoria volatile 12, come ad esempio una memoria ad accesso casuale RAM, che è in comunicazione di segnale con i mezzi di controllo ed elaborazione 11, e dove in detti mezzi di memoria volatile 12 possono essere memorizzate almeno le istruzioni che implementano il metodo secondo l'invenzione e che possono essere lette dai mezzi di controllo ed elaborazione 11 quando il dispositivo 1 è in una condizione di funzionamento;
- mezzi di memoria di massa 13, preferibilmente uno più dischi magnetici (hard disk) o una memoria di tipo Flash o altro tipo, che sono in comunicazione di segnale con i mezzi di controllo ed elaborazione 11 e con i mezzi di

memoria volatile 12;

- il sensore di immagini 14, come ad esempio un sensore fotografico, un sensore per la visione notturna, ad infrarossi o altro;
- mezzi di comunicazione 15, preferibilmente un'interfaccia di rete che opera secondo uno standard della famiglia 802.11 (noto con il nome di WiFi), 802.16 (noto con il nome di WiMax), IEEE 803.2 (noto anche con il nome di Ethernet) o un'interfaccia ad una rete dati di tipo GSM/GPRS/UMTS/LTE, TETRA o altro, che permettono al dispositivo 1 di comunicare con altri dispositivi attraverso una rete dati, dove questi ultimi saranno meglio descritti nel seguito di questa descrizione;
- mezzi di ingresso/uscita (I/O) 16 che possono ad esempio essere utilizzati per collegare a detto dispositivo 1 delle periferiche (come ad esempio una o più interfacce che consentano l'accesso ad altri mezzi di memoria di massa in modo da permettere preferibilmente la copiatura delle informazioni da questi ai mezzi di memoria di massa 13) oppure ad un terminale di programmazione configurato per scrivere delle istruzioni (che i mezzi di elaborazione e controllo 11 dovranno eseguire) nei mezzi di memoria 12,13; tali mezzi di ingresso/uscita 16 possono ad esempio comprendere un adattatore USB, Firewire, RS232, IEEE 1284 o altro;
- un bus di comunicazione 17 che permette lo scambio di informazioni tra i mezzi di controllo ed elaborazione 11, i mezzi di memoria volatile 12, i mezzi di memoria di massa 13, il sensore di immagini 14, i mezzi di comunicazione 15, ed i mezzi di ingresso/uscita 16.

In alternativa al bus di comunicazione 17, è possibile collegare con un'architettura a stella i mezzi di controllo ed elaborazione 11, i mezzi di memoria volatile 12, i mezzi di

memoria di massa 13, il sensore di immagini 14, i mezzi di comunicazione 15 e i mezzi di ingresso/uscita 16.

Con riferimento anche a fig. 3, verrà ora descritto con maggior dettaglio uno scenario tipico di utilizzo del metodo e dell'apparato d'utente 1 secondo l'invenzione in cui vengono eseguite le fasi di un metodo per registrare detto apparato d'utente 1 in modo da rendere successivamente possibile l'autenticazione di detto apparato d'utente 1 presso detto dispositivo 1. Il metodo di registrazione, che viene preferibilmente eseguito da detto apparato d'utente 1, comprende le seguenti fasi:

- una fase di acquisizione immagini E1, in cui una pluralità di immagini (preferibilmente un numero compatibile con la potenza di calcolo messa a disposizione dai mezzi di elaborazione 11, ad esempio un numero compreso tra 10 e 30 immagini) viene acquisita mediante il sensore di immagini 14, preferibilmente in formato grezzo (RAW) in modo da rendere maggiormente evidenti i difetti del sensore di immagini 14 dovuti alle impurità delle porzioni di silicio che lo compongono;
- una fase di calcolo impronta di registrazione E2, in cui un'impronta sensore di registrazione è generata, mediante i mezzi di elaborazione 11 dell'apparato d'utente 1, sulla base di detta pluralità di immagini acquisita nel corso di detta fase E1, e dove detta almeno una porzione di detta impronta sensore di registrazione viene codificata (compressa), mediante i mezzi di elaborazione e controllo dell'apparato d'utente 1, utilizzando un algoritmo di proiezioni casuali, in modo da generare un'impronta compressa W di detta almeno una porzione di detta impronta sensore di registrazione. Ad esempio, i mezzi di elaborazione e controllo dell'apparato d'utente 1 sono configurati per eseguire un insieme di istruzioni che

implementa detto algoritmo di proiezioni casuali (che verrà meglio descritto nel seguito di questa descrizione);

- una fase di preparazione chiavi E3, in cui viene generata una coppia di chiavi, ossia una chiave pubblica ed una chiave privata, e viene trasmessa al server applicativo 2 la chiave pubblica, mentre la chiave privata viene cifrata, preferibilmente mediante un algoritmo di crittografia simmetrico, utilizzando come chiave detta impronta compressa W, così da generare una chiave privata cifrata (detta anche 'sketch') che viene memorizzata nei mezzi di memoria 12,13;
- una fase di trasmissione chiave pubblica E4, in cui la chiave pubblica generata nel corso della fase E3 è trasmessa al server applicativo 2 mediante i mezzi di comunicazione 15 di detto apparato d'utente 1, preferibilmente attraverso un canale protetto (come ad esempio una connessione SSL o altro).

Con riferimento anche a fig. 4, verrà ora descritto un metodo per autenticare detto apparato d'utente 1 presso detto server applicativo 2. Il metodo di autenticazione, che viene preferibilmente eseguito da detto apparato d'utente 1, comprende le seguenti fasi:

- una fase di acquisizione immagini V1, in cui almeno un'immagine (preferibilmente un numero di immagini compatibile con la potenza di calcolo messa a disposizione dai mezzi di elaborazione 11, ad esempio un numero compreso tra cinque e dieci immagini) viene acquisita mediante il sensore di immagini 14, preferibilmente in formato grezzo (RAW) per le stesse ragioni già sopra enunciate;
- una fase di calcolo impronta di autenticazione V2, in cui un'impronta sensore di autenticazione è generata, mediante i mezzi di elaborazione 11 apparato d'utente 1, sulla base di detta pluralità di immagini acquisita nel corso di detta

fase V1 in maniera simile o uguale alla fase E2 sopra descritta, così da generare un'impronta compressa W di almeno una porzione di detta impronta sensore di autenticazione;

- una fase di recupero chiave privata V3, in cui, mediante i mezzi di elaborazione 11, la chiave privata cifrata (detta anche 'sketch') viene letta dai mezzi di memoria 12,13 e decifrata, preferibilmente mediante un algoritmo di crittografia simmetrico omologo o identico a quello utilizzato nel corso della fase E3, utilizzando detta impronta compressa W come chiave, così da recuperare la chiave privata, ossia ottenere una copia in chiaro di detta chiave privata;
- una fase di firma V4, in cui viene ricevuta dal server applicativo 2 una richiesta di autenticazione (ossia un messaggio detto anche 'challenge'), ed i mezzi di elaborazione 11 eseguono i seguenti passi:
  - generare una firma elettronica sulla base della richiesta di autenticazione eseguendo un algoritmo di firma digitale (come ad esempio DSA, ECDSA, o altro, ossia un algoritmo di crittografia asimmetrico) che utilizza la chiave privata come chiave;
  - trasmettere, mediante i mezzi di comunicazione 15, detta firma elettronica al server applicativo 2.

Quando il sistema S è in una condizione di funzionamento, gli elementi 1,2,3 di detto sistema eseguono preferibilmente i seguenti passi:

- l'apparato d'utente genera una coppia di chiavi, ossia una chiave pubblica ed una chiave privata, e si registra presso il server applicativo 2 trasmettendogli la propria chiave pubblica e memorizzando la propria chiave privata nei mezzi di memoria 12,13;
- l'apparato d'utente 1 accede ai servizi pubblici erogati

dal server applicativo 2 (ad esempio accedendo alla “landing page” del servizio erogato da detto server 2) e trasmette le proprie informazioni d’utente richiedendo l’accesso a detto almeno un servizio che necessita l'autenticazione di detto apparato d’utente 1;

- il server applicativo 2 genera una richiesta di autenticazione (il ‘challenge’) sulla base delle informazioni d’utente ricevute dall’apparato d’utente (ad esempio creando un messaggio che include almeno dette informazioni d’utente) e trasmette detta richiesta d’autenticazione al dispositivo 1;
- l’apparato d’utente 1 compie i seguenti sottopassi:
  - generare una firma elettronica sulla base della richiesta di autenticazione eseguendo un algoritmo di firma digitale (come ad esempio il DSA, il ECDSA, o altro, ossia un algoritmo di crittografia asimmetrico) che utilizza (dopo aver eseguito il metodo secondo l’invenzione come di seguito descritto) la chiave privata come chiave;
  - trasmettere detta firma elettronica al server applicativo 2;
- il server applicativo 2 verifica l’autenticità della firma elettronica ricevuta da detto apparato d’utente 1 eseguendo un algoritmo di verifica di firma digitale (come ad esempio il DSA, il ECDSA, o altro, ossia un algoritmo di crittografia asimmetrico) che utilizza la chiave pubblica come chiave.

Con riferimento anche a fig. 5, verrà ora descritto, nello specifico, il metodo secondo l’invenzione che è eseguito nel corso dei metodi di registrazione ed autenticazione sopra descritti e che può essere generalizzato come un metodo per la protezione di dati privati (come ad esempio una o più chiavi private) comprendente i seguenti passi:

- una fase di acquisizione immagini P1, in cui una pluralità di immagini vengono acquisite mediante un sensore di immagini 14;
- una fase di calcolo impronta P2, in cui un'impronta sensore è generata, mediante mezzi di elaborazione 11, sulla base di detta pluralità di immagini acquisita nel corso della fase di acquisizione immagini P1;
- una fase di compressione P3, in cui almeno una porzione di detta impronta sensore di codifica viene codificata, mediante detti mezzi di elaborazione 11, utilizzando un algoritmo di proiezioni casuali, in modo da generare un'impronta compressa W;
- una fase di elaborazione P4, in cui si cifrano e/o decifrano detti dati riservati utilizzando detta impronta compressa W come chiave.

In questo modo, è possibile aumentare la sicurezza di un sistema di autenticazione.

Nel corso della fase di elaborazione P4, le operazioni di cifratura e/o decifratura di detti dati riservati possono essere preferibilmente effettuate compiendo un'operazione di OR esclusivo bit a bit (bitwise-XOR) tra detta impronta compressa W ed una stringa composta da almeno detti dati riservati.

Nel corso della fase di compressione P3, vengono compresse le impronte sensore calcolate nel corso della fase di calcolo impronta P2, utilizzando la tecnica delle proiezioni casuali (Random Projections - RP). In altre parole, durante ciascuna la fase P3, i mezzi di elaborazione e controllo dell'apparato d'utente 1 sono configurati per eseguire un insieme di istruzioni che implementa un algoritmo di compressione che sfrutta la tecnica delle proiezioni casuali.

Questo algoritmo prevede di comprimere le impronte sensore di registrazione e di autenticazione con pochissima o

idealmente nessuna perdita di informazione. Più nel dettaglio, la tecnica delle proiezioni casuali è un potente e poco complesso metodo di riduzione dimensionale che si basa sull'idea di proiettare i dati *n*-dimensionali originali su un sottospazio *m*-dimensionale, con $m < n$, utilizzando una matrice casuale $\Phi \in \mathbb{R}^{m \times n}$. Di conseguenza, un'impronta del sensore *n*-dimensionale $k \in \mathbb{R}^n$ viene ridotta a un sottospazio *m*-dimensionale $y \in \mathbb{R}^m$ mediante la seguente formula:

$$y = \Phi k \tag{8}$$

La proprietà chiave che soggiace alla tecnica RP è il lemma di Johnson-Lindenstrauss (che si considera parte integrante di questa descrizione), riguardante l'incorporazione (embedding) a bassa distorsione di punti da spazi euclidei alto-dimensionali a spazi euclidei basso-dimensionali. Il lemma stabilisce che un piccolo insieme di punti in uno spazio alto-dimensionale può essere incorporato in uno spazio di dimensioni molto inferiori in maniera tale da (quasi) preservare le distanze tra i punti.

Basandosi su tale presupposto, l'apparato d'utente 1 può essere configurato per calcolare una versione compressa di ciascuna delle impronte sensore da lui calcolate mediante proiezioni casuali, vale a dire mediante una moltiplicazione (prodotto matriciale) tra una matrice di compressione e una matrice che rappresenta detta impronta sensore (o viceversa), dove detta matrice di compressione ha un numero di righe (o colonne) inferiore a quello della matrice che rappresenta l'impronta sensore.

Il risultato di detto prodotto può essere quantizzato, ovvero rappresentato su un numero finito di bit, al fine di ottenere una rappresentazione più compatta della versione compressa dell'impronta sensore. Ad esempio, una versione binaria dell'impronta sensore compressa può essere ottenuta

mediante la seguente formula:

$$w = sign(y)$$

In altre parole, nel corso della fase di compressione P3, detta almeno una porzione di detta impronta sensore di codifica viene codificata utilizzando un algoritmo di proiezioni casuali, così da generare una impronta sensore codificata; dopodiché, detta impronta sensore codificata viene quantizzata mediante i mezzi di elaborazione 11, generando detta l'impronta compressa W.

Così facendo è possibile generare una versione compressa dell'impronta sensore (di registrazione o di autenticazione) memorizzando e processando meno dati e, soprattutto, non richiedendo al dispositivo 1 di eseguire la decifratura dei dati sensibili senza che le proprietà di sicurezza del sistema di autenticazione S subiscano un degrado. In questo modo, la riduzione della complessità in spazio permette all'apparato d'utente 1 un impiego limitato di risorse, così che tale sistema di autenticazione S possa essere impiegato su di un largo numero di terminali d'utente. Questo permette di aumentare il livello di sicurezza globale, poiché è possibile realizzare un sistema di autenticazione S utilizzando terminali d'utente non necessariamente di ultima generazione.

In alternativa o in combinazione a quanto sopra descritto, la sicurezza del sistema può essere ulteriormente aumentata dal metodo di generazione delle proiezioni casuali in quanto esso si basa sull'uso di un generatore di numeri pseudo-casuali che è inizializzato da un seme mantenuto segreto sul dispositivo dell'utente.

Più nel dettaglio, il metodo secondo l'invenzione può anche comprendere una fase di generazione casuale, in cui si genera, mediante i mezzi di elaborazione, una stringa casuale di bit, e dove nel corso della fase di compressione P3, detto algoritmo di proiezioni casuali genera un insieme di

proiezioni casuali, preferibilmente una matrice di tipo BCCB (Block circulant with circulant blocks), sulla base di detta stringa casuale di bit, così che nel corso della fase di elaborazione P4, quando si cifrano i dati riservati, è possibile vantaggiosamente utilizzare un impronta compressa generata con una nuova stringa casuale di bit (seme).

La stringa casuale di bit è preferibilmente memorizzata nei mezzi di memoria 12,13 per consentire un successivo riuso quando è necessario decifrare i dati riservati. A tale scopo, il metodo secondo l'invenzione può anche comprendere una fase di lettura stringa casuale, in cui si legge, mediante i mezzi di elaborazione 11, la stringa casuale di bit memorizzata nei mezzi di memoria 12,13, e dove nel corso della fase di compressione P3, i mezzi di elaborazione 11 generano un insieme di proiezioni casuali sulla base di detta stringa casuale di bit, così che nel corso della fase di elaborazione P4, quando si decifrano i dati riservati, è possibile ricostruire l'impronta compressa utilizzata in precedenza (per la cifratura dei dati riservati).

In questo modo, è possibile aumentare la sicurezza del sistema di autenticazione, rendendo possibile gestire la situazione in cui un attaccante riesce a generare un'impronta del sensore di immagini in maniera fraudolenta; infatti, generando una nuova stringa casuale di bit e utilizzandola per cifrare una nuova chiave privata (e ripetendo la procedura di registrazione) è possibile riportare il sistema di autenticazione S in uno stato sicuro.

Si evidenzia che l'impronta calcolata nel corso della fase P2 e utilizzata dall'apparato d'utente 1 per registrarsi presso il server applicativo 2 è (molto probabilmente) differente da quella che verrà utilizzata per l'autenticazione. Infatti, si evidenzia anche che, essendo l'impronta sensore di fatto una misura di una caratteristica

del sensore, due impronte distinte determinate in istanti di tempo distinti tra loro saranno difficilmente uguali tra loro, poiché saranno affette da rumore come avviene per ogni altra misura; infatti, l'impronta generate nel corso della fase P2 è dipendente dalla quantità di luce che raggiunge il sensore di immagini 14 quando, nel corso della fase di acquisizione immagini P1, vengono acquisite le immagini.

Per evitare che questo rumore comprometta il funzionamento del sistema di autenticazione S (con evidenti problemi per la sicurezza), i mezzi di elaborazione 11 possono essere configurati per eseguire un insieme di istruzioni che implementa un algoritmo di codifica/decodifica polare (come ad esempio quello descritto da Mahdavifar et al. in "Achieving the secrecy capacity of wiretap channels using polar codes," *IEEE Transactions on Information Theory*, vol. 57, no. 10, pp. 6428–6443, Oct 2011) nel corso della fase di elaborazione P4.

In particolare, quando si devono cifrare dei dati riservati nel corso della fase di elaborazione P4, si codifica, mediante i mezzi di elaborazione 11, la stringa di dati riservati utilizzando una codifica polare, in modo da ottenere una stringa di dati riservati codificati, e si cifrano detti dati riservati codificati utilizzando l'impronta compressa W come chiave. Invece, quando è necessario decifrare dei dati riservati nel corso della fase di elaborazione P4, si decifrano detti dati riservati ottenendo dati riservati codificati, e si decodificano detti dati riservati codificati utilizzando una codifica polare.

Una codifica/decodifica polare consente di correggere le differenze (errori) che sono presenti tra la versione dei dati riservati prima della cifratura e la versione di detti dati riservati dopo la decifratura con un margine di probabilità che può essere provato, e che sono dovuti alle differenze che possono essere presenti tra l'impronta sensore compressa

utilizzata per cifrare i dati riservati e l'impronta sensore compressa utilizzata per decifrare detti dati riservati. Questo consente di autenticare un apparato d'utente 1 utilizzando poche immagini (anche una sola) con una probabilità superiore all'ottanta percento, mentre rende praticamente impossibile autenticare un altro apparato d'utente avente un sensore di immagini differente oppure utilizzare immagini pubblicamente disponibili scattate dallo stesso sensore e compresse con metodi a perdita di informazione (lossy), come ad esempio il JPEG o altro formato.

In questo modo, è possibile migliorare la sicurezza del sistema di autenticazione S.

Nelle corso della fase P2, l'impronta sensore (di registrazione e di autenticazione) è estratta eseguendo una insieme di istruzioni che implementano un algoritmo di regressione. Più nel dettaglio, l'uscita del sensore è preferibilmente modellata come di seguito:

$$\mathbf{o} = g^{\gamma} \cdot \left[(1+\mathbf{k}) \cdot \mathbf{i} + \mathbf{e}\right]^{\gamma} + \mathbf{q} \ , \qquad (1)$$

dove g^{γ} è la correzione di gamma (g è differente per ciascun canale di colore e γ è normalmente prossimo a 0.45), e modella le sorgenti di rumore interne al sensore, q modella il rumore esterno a detto sensore (ad esempio il rumore di quantizzazione), mentre k modella l'impronta sensore (una matrice delle dimensioni delle immagini prodotte dal sensore di immagini 14) che si vuole estrarre, i è l'intensità della luce che colpisce il sensore. Al fine di estrarre k, la formula (1) può essere approssimata al primo termine della serie di Taylor:

$$\mathbf{o} = \mathbf{o}^{\mathrm{id}} + \mathbf{o}^{\mathrm{id}} \cdot \mathbf{k} + \tilde{\mathbf{e}} \qquad (2)$$

dove $o^{\mathrm{id}} = (\mathrm{gi})^{\gamma}$ è l'output ideale del sensore di immagini, $o^{\mathrm{id}} \cdot k$ è la risposta fotografica non uniforme (photo-response non-uniformity - PRNU) del sensore di immagini di cui si vuole

estrarre l'impronta k, ed $\tilde{e} = \gamma o^{\mathrm{id}} \cdot e/i + q$ raggruppa tutte le altre sorgenti di rumore.

Assumendo che è possibile produrre una versione senza rumore o^{dn} mediante un opportuno processo di filtraggio e che tale versione senza rumore può essere utilizzata al posto dell'output ideale o^{id}, allora è possibile scrivere

$$\mathbf{w} = \mathbf{o} - \mathbf{o}^{\mathsf{dn}} = \mathbf{o} \cdot \mathbf{k} + \tilde{\mathbf{q}} \tag{3}$$

dove q raggruppa tutti gli errori del modello. Supponendo che un numero di immagini $C \geq 1$ è disponibile e considerando $\tilde{q}$ come un rumore Gaussiano indipendente dal segnale $o \cdot k$ e avente media zero e varianza σ^2, è possibile scrivere per ciascuna immagine $\ell, \ell = 1, \ldots, C$ la seguente relazione:

$$\mathbf{w}^{(\ell)}/\mathbf{o}^{(\ell)} = \mathbf{k} + \tilde{\mathbf{q}}/\mathbf{o}^{(\ell)} \ , \quad \text{dove} \quad \mathbf{w}^{(\ell)} = \mathbf{o}^{(\ell)} - \mathbf{o}^{(\ell)\mathsf{dn}} \tag{4}$$

Pertanto, la stima di k, ossia la stima di massima verosimiglianza $\hat{k}$ (maximum likelihood estimate), può essere ottenuta come

$$\hat{\mathbf{k}} = \sum_{\ell=1}^{C} \left(\mathbf{w}^{(\ell)} \cdot \mathbf{o}^{(\ell)} \right) \Bigg/ \sum_{\ell=1}^{C} (\mathbf{o}^{(\ell)})^2 \tag{5}$$

E la varianza di questa stima è data da

$$\sigma_{\hat{\mathbf{k}}}^2 = \sigma^2 \Bigg/ \sum_{\ell=1}^{C} (\mathbf{o}^{(\ell)})^2 \tag{6}$$

dalla quale è possibile notare che le immagini dalle quali si riescono ad estrarre le migliori impronte sensore sono le immagini aventi elevata luminanza (ma non sature) e contenuto regolare (in modo da abbassare la varianza σ^2 del rumore $\tilde{q}$). Per migliorare ulteriormente la qualità della stima $\hat{k}$, gli

artefatti in comune tra i sensori di immagini della stessa marca e/o modello possono essere rimossi sottraendo i valori medi delle righe e delle colonne ai valori della stima $\hat{k}$.

In caso le immagini acquisite dal sensore di immagini 14 siano a colori, la stima deve essere effettuate separatamente per ciascun canale di colore (rosso, verde, blu), cioè si devono ottenere una stima di massima verosimiglianza per ciascun canale, ossia $\hat{k}_R$ per il canale del rosso, $\hat{k}_G$ per il canale del verde, e $\hat{k}_B$ per il canale del blu. Dopodiché, un'impronta "globale" può essere ottenuta applicando una qualunque conversione da RGB a scala di grigi, come ad esempio quella di seguito riportata:

$$\hat{\mathrm{k}} = 0.3\hat{\mathrm{k}}_{\mathrm{R}} + 0.6\hat{\mathrm{k}}_{\mathrm{G}} + 0.1\hat{\mathrm{k}}_{\mathrm{B}} \qquad (7)$$

È comunque possibile per il tecnico del ramo utilizzare un algoritmo di regressione differente da quello appena sopra descritto, senza comunque allontanarsi dagli insegnamenti della presente invenzione.

Al fine di migliorare ulteriormente la qualità delle impronte sensore estratte nel corso della fase di calcolo impronta P2, ciascuna delle immagini, che viene acquisita mediante il sensore di immagini 14, può essere filtrata mediante un filtro di Wiener atto a rimuovere tutti gli artefatti periodici, prima che le impronte sensore vengano estratte (calcolate). In altre parole, i mezzi di elaborazione e controllo dell'apparato d'utente 1 possono anche essere configurati per eseguire, all'inizio della fase di calcolo impronta P2, un insieme di istruzioni che applica l'algoritmo di filtraggio di Wiener alle immagini acquisite nel corso della fase di acquisizione immagini P1 prima che l'impronta sensore di autenticazione sia generata, in modo da rimuovere tutti gli artefatti periodici da dette immagini. In questo

modo, si migliora la capacità del sistema S di distinguere tra due impronte provenienti da due sensori di immagini distinti, aumentando così il livello di sicurezza del sistema di autenticazione S.

In combinazione o in alternativa a quanto sopra descritto, nel corso della fase di compressione P3 è anche possibile effettuare una selezione delle parti dell'impronta (calcolata nel corso della fase di calcolo impronta P2) che hanno una frequenza spaziale (orizzontale e/o verticale) superiore ad un valore di soglia.

In particolare, durante la fase di compressione P3, i mezzi di elaborazione e controllo dell'apparato d'utente 1 sono configurati per eseguire i seguenti passi:

- trasformare l'impronta calcolata nel corso della fase P2 in un dominio trasformato, in modo da ottenere un'impronta trasformata; ad esempio eseguendo un insieme di istruzioni che implementa un algoritmo di trasformazione, come la trasformata discreta del coseno (Discrete Cosine Transform - DCT) oppure la trasformata veloce di Fourier bidimensionale (2D Fast Fourier Transform - 2D FFT), o altro;
- selezionare i punti dell'impronta trasformata che hanno una frequenza spaziale orizzontale e/o verticale superiore ad un valore di soglia prestabilito;
- antitrasformare detti punti dell'impronta trasformata selezionati, ad esempio eseguendo un insieme di istruzioni che implementa un algoritmo di antitrasformazione, come la trasformata discreta del coseno inversa (Inverse Discrete Cosine Transform - DCT) oppure la trasformata veloce di Fourier inversa bidimensionale (2D Inverse Fast Fourier Transform - 2D IFFT), o altro.

Così facendo si ottiene un'impronta sensore (di registrazione e di autenticazione) contenente solamente le

componenti di "elevata" frequenza. Questo diventa particolarmente vantaggioso quando queste componenti frequenziali sono superiori alle frequenze massime che sono contenute nelle immagini compresse utilizzando i formati di compressione di largo impiego (come ad esempio il JPEG o altro) e che vengono spesso utilizzati per pubblicare dei contenuti autoprodotti su Internet. In questo modo, si rende impossibile generare un'impronta sensore di autenticazione valida partendo da un insieme di immagini che sono state scattate da uno stesso terminale utente e che sono state poi pubblicate su Internet (ed essendo anche a conoscenza del seme utilizzato dall'algoritmo di proiezioni casuali), poiché le componenti frequenziali dell'impronta che vengono utilizzate dal sistema S per autenticare l'apparato d'utente 1 non sono presenti nelle immagini compresse, aumentando così il livello di sicurezza del sistema di autenticazione S.

In combinazione o in alternativa a quanto sopra descritto, l'apparato d'utente 1 può comprendere mezzi di ostruzione (come ad esempio un tappo, un'aletta traslabile o altro) che, se azionati dall'utilizzatore di detto apparato d'utente 1, possono impedire che il sensore di immagini 14 possa essere illuminato, ossia che la luce raggiunga il sensore di immagini 14. Questo permette di impedire che i mezzi di elaborazione 11 generino (nel corso della fase P2) un'impronta sensore valida, poiché nel corso della fase di acquisizione immagini P1, l'assenza di luce impedisce di acquisire delle immagini con un'entropia sufficiente a permettere l'estrazione dell'impronta del sensore di immagini 14.

In questo modo, si aumenta la sicurezza del sistema di autenticazione S impedendo (fisicamente) che un attaccante riesca a generare un'impronta valida per decifrare i dati riservati anche prendendo (da remoto) il controllo dell'apparato d'utente 1.

In una variante dell'invenzione sopra descritta, un sensore di immagini simile a quello della forma esecutiva preferita comprende mezzi di elaborazione (come ad esempio una CPU, un microcontrollore o altro) configurati per eseguire le fasi del metodo secondo l'invenzione.

In questo modo, si aumenta la sicurezza del sistema di autenticazione S, poiché si semplifica l'integrazione del metodo secondo l'invenzione in apparati d'utente già esistenti o in progetti di apparati d'utente già completati (ad esempio mediante la sostituzione del sensore di immagini o la sua riprogrammazione).

Alcune delle possibili varianti sono state descritte sopra, ma è chiaro al tecnico del ramo che, nell'attuazione pratica, esistono anche altre forme di realizzazione, con diversi elementi che possono essere sostituiti da altri tecnicamente equivalenti. La presente invenzione non è dunque limitata agli esempi illustrativi descritti, ma è suscettibile di varie modifiche, perfezionamenti, sostituzioni di parti e di elementi equivalenti senza comportare scostamenti dall'idea inventiva di base, come specificato nelle seguenti rivendicazioni.

RIVENDICAZIONI

1. Metodo per la protezione di dati riservati,

caratterizzato dal fatto di comprendere

- una fase di acquisizione immagini (P1), in cui una pluralità di immagini vengono acquisite mediante un sensore di immagini (14),
- una fase di calcolo impronta (P2), in cui un'impronta sensore è generata, mediante mezzi di elaborazione (11), sulla base di detta pluralità di immagini acquisita nel corso della fase di acquisizione immagini (P1),
- una fase di compressione (P3), in cui almeno una porzione di detta impronta sensore di codifica viene codificata, mediante detti mezzi di elaborazione (11), utilizzando un algoritmo di proiezioni casuali, in modo da generare un'impronta compressa (W),
- una fase di elaborazione (P4), in cui si cifrano e/o decifrano detti dati riservati utilizzando detta impronta compressa (W) come chiave.

2. Metodo secondo la rivendicazione 1, in cui, nel corso della fase di elaborazione (P4), si cifrano i dati riservati, dove detto metodo comprende anche

- una fase di generazione casuale, in cui si genera, mediante detti mezzi di elaborazione (11), una stringa casuale di bit,

e dove nel corso della fase di compressione (P3), detto algoritmo di proiezioni casuali genera un insieme di proiezioni casuali sulla base di detta stringa casuale di bit.

3. Metodo secondo le rivendicazioni 1 o 2, in cui nel corso della fase di elaborazione (P4) si decifrano i dati riservati, dove detto metodo comprende anche

- una fase di lettura stringa casuale, in cui si legge, mediante detti mezzi di elaborazione (11), una stringa casuale di bit memorizzata in mezzi di memoria (12,13),

e dove nel corso della fase di compressione (P3), i mezzi di elaborazione (11) generano un insieme di proiezioni casuali sulla base di detta stringa casuale di bit.

4. Metodo secondo una qualunque delle rivendicazioni da 1 a 3, in cui, nel corso della fase di elaborazione (P4), si codifica, mediante detti mezzi di elaborazione (11), la stringa di dati riservati utilizzando una codifica polare, in modo da ottenere una stringa di dati riservati codificati, e si cifrano detti dati riservati codificati utilizzando detta impronta compressa (W) come chiave.

5. Metodo secondo una qualunque delle rivendicazioni da 1 e 4, in cui nel corso della fase di elaborazione, si decifrano detti dati riservati ottenendo dati riservati codificati, e si decodificano detti dati riservati codificati utilizzando una codifica polare.

6. Metodo secondo una qualunque delle rivendicazioni da 1 a 5, in cui, nel corso della fase di compressione (P3), detta almeno una porzione di detta impronta sensore viene codificata utilizzando un algoritmo di proiezioni casuali, generando una impronta sensore codificata, e dove detta impronta sensore codificata viene quantizzata mediante i mezzi di elaborazione (11), generando detta impronta compressa (W).

7. Metodo secondo una qualunque delle rivendicazioni da 1 a 6, in cui, nel corso della fase di compressione (P3), si eseguono, mediante i mezzi di elaborazione (11), i passi di

- trasformare in un dominio trasformato l'impronta sensore generata nel corso della fase di calcolo impronta (P2), in modo da ottenere un'impronta trasformata,
- selezionare i punti dell'impronta trasformata che hanno una frequenza spaziale orizzontale e/o verticale superiore ad un valore di soglia, e
- antitrasformare detti punti dell'impronta trasformata selezionati.

8. Metodo secondo una qualunque delle rivendicazioni da 1 a 7, in cui nel corso della una fase di calcolo impronta (P2) viene eseguito un insieme di istruzioni che, prima che l'impronta sensore sia generata, applica l'algoritmo di filtraggio di Wiener a ciascuna immagine acquisita nel corso della fase di acquisizione immagini (P1), in modo da rimuovere tutti gli artefatti periodici da detta pluralità di immagini.

9. Metodo secondo una qualunque delle rivendicazioni da 1 a 8, in cui i dati riservati comprendono una chiave privata.

10. Apparato d'utente (1) per la protezione di dati riservati, comprendente

- un sensore di immagini (14) atto ad acquisire immagini,
- mezzi di elaborazione (11) in comunicazione con detto sensore di immagini (14),

caratterizzato dal fatto che

i mezzi di elaborazione (11) sono anche configurati per

- acquisire una pluralità di immagini mediante detto sensore di immagini (14),
- generare un'impronta sensore sulla base di detta pluralità di immagini,
- codificare almeno una porzione di detta impronta sensore utilizzando un algoritmo di proiezioni casuali, in modo da generare un'impronta compressa (W),
- cifrare e/o decifrare detti dati riservati utilizzando detta impronta compressa (W) come chiave.

11. Apparato d'utente (1) comprendente mezzi di ostruzione atti ad impedire che il sensore di immagini (14) possa essere illuminato.

12. Sensore di immagini per apparato d'utente,

caratterizzato dal fatto di comprendere

mezzi di elaborazione configurati per eseguire le fasi del metodo secondo una qualsiasi delle rivendicazioni da 1 a 9.

13. Prodotto informatico (computer program product)

caricabile nella memoria di un elaboratore elettronico e comprendente porzione di codice software per attuare le fasi del metodo secondo una qualsiasi delle rivendicazioni da 1 a 9.

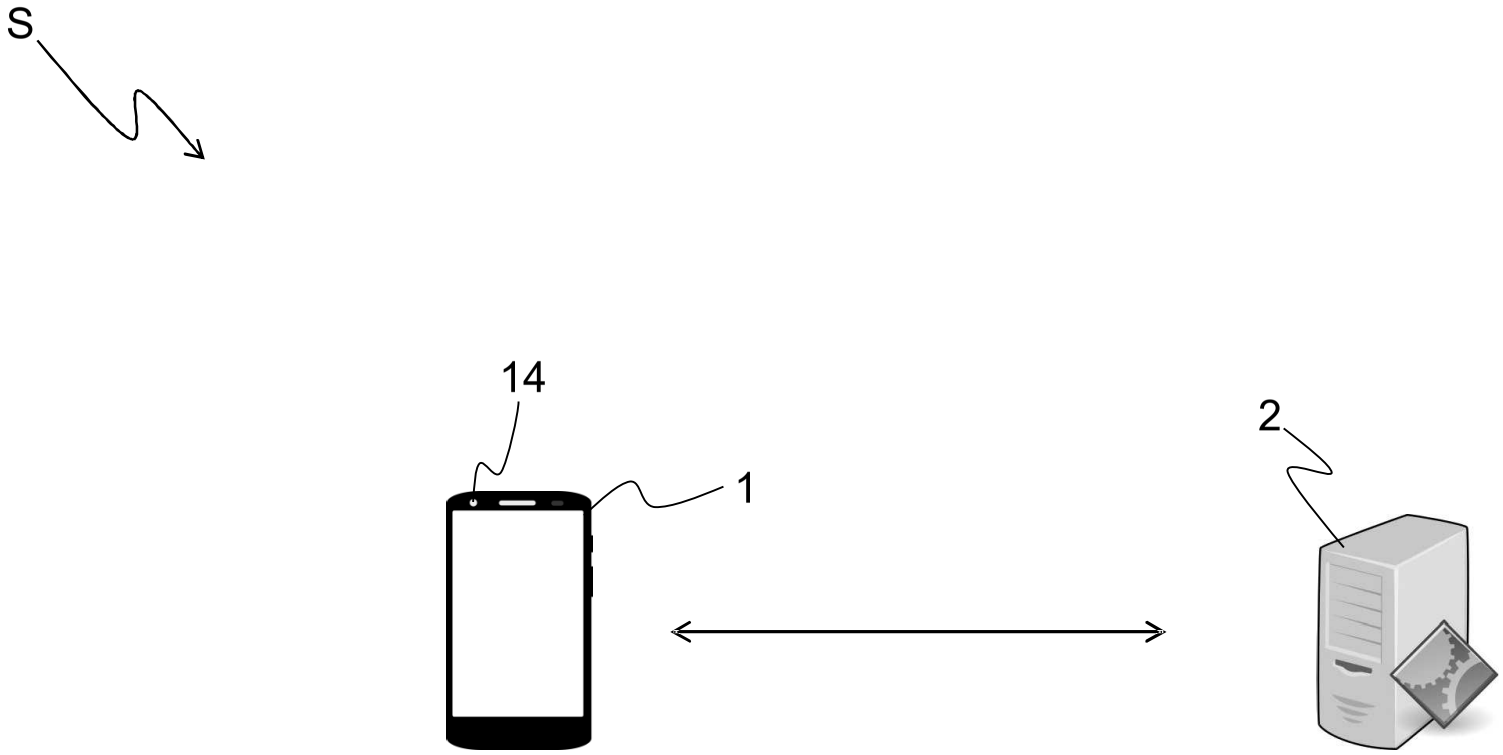

Fig. 1

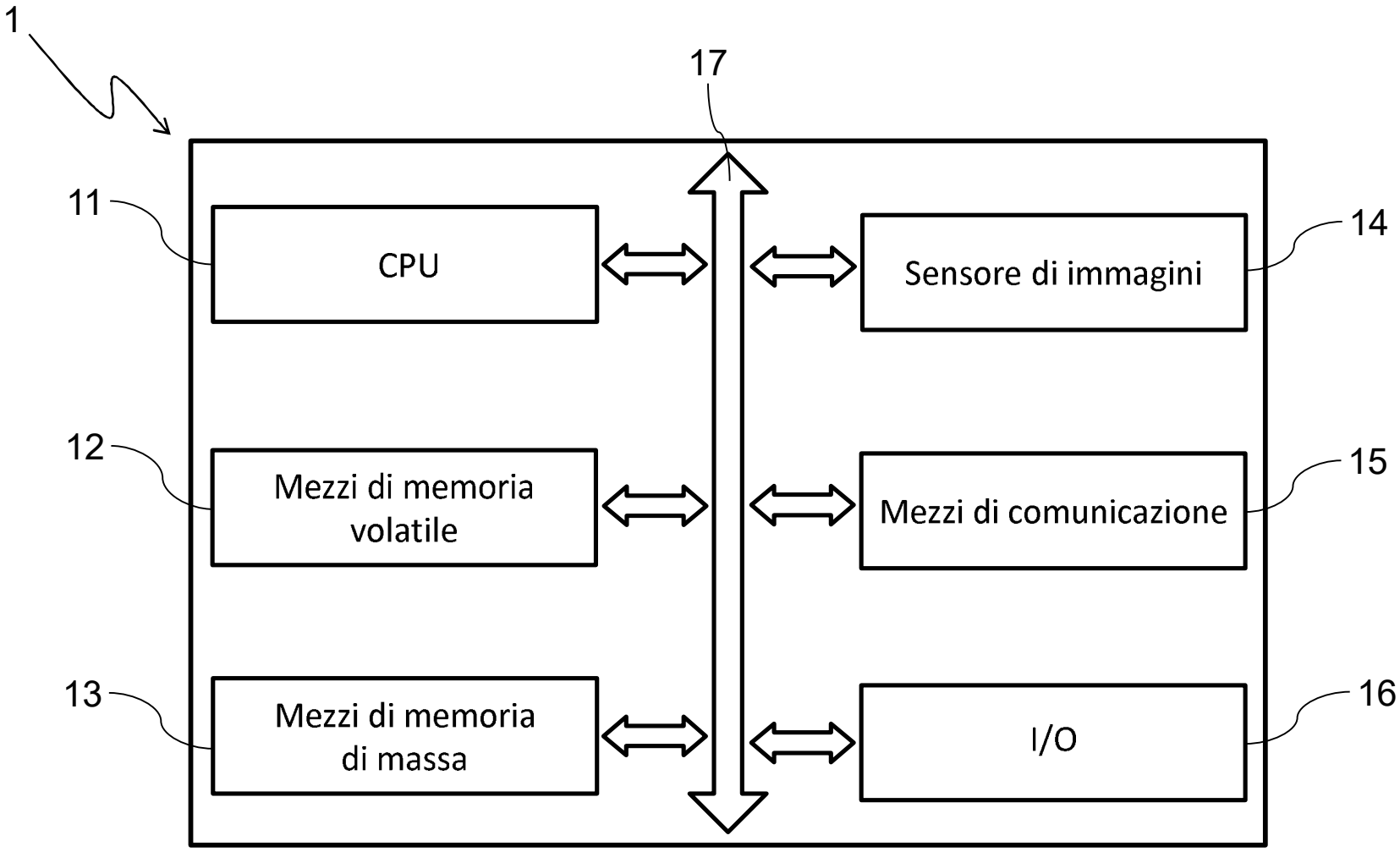
1
17
11
CPU
14
Sensore di immagini
12
Mezzi di memoria volatile
15
Mezzi di comunicazione
13
Mezzi di memoria di massa
16
I/O

Fig. 2

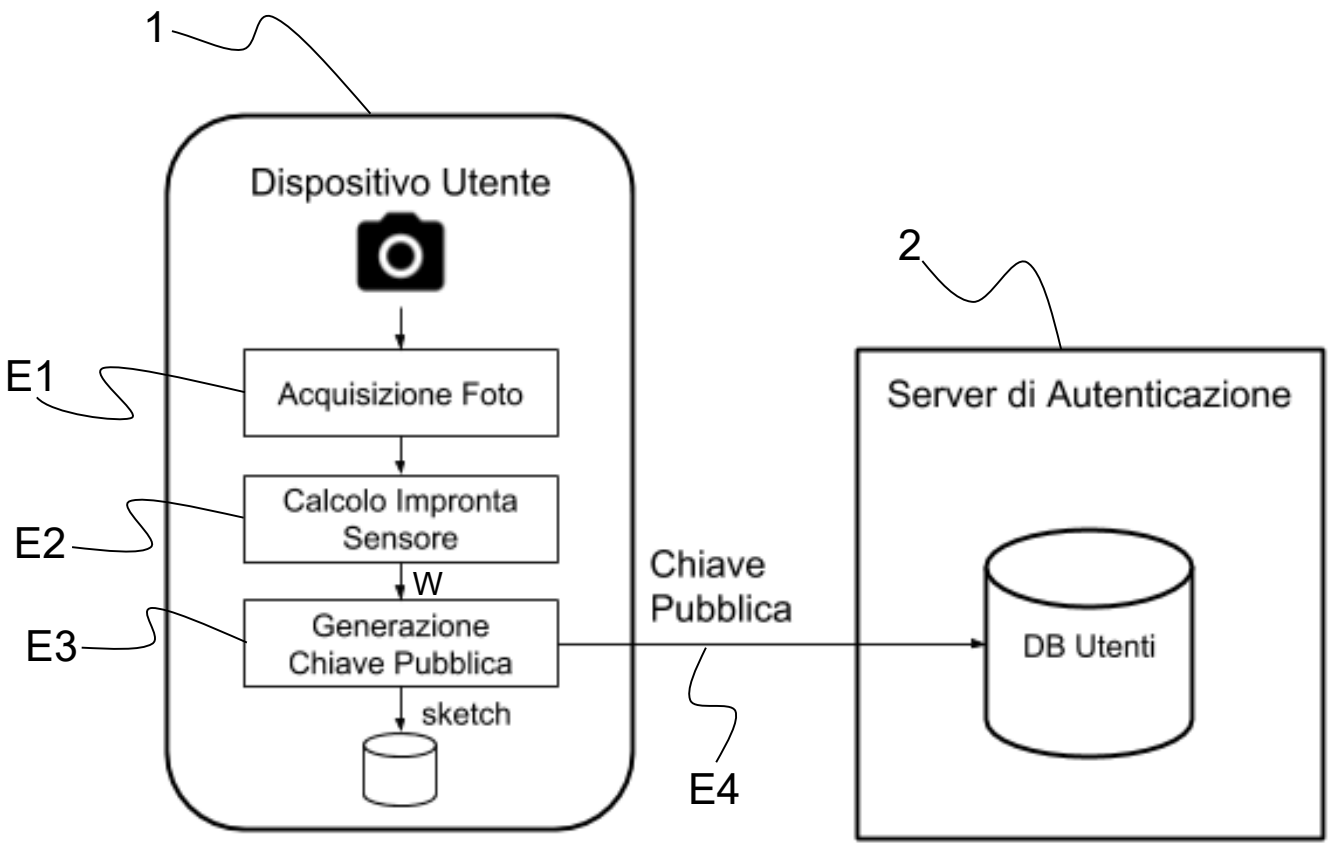
1
Dispositivo Utente
2
Server di Autenticazione
E1
Acquisizione Foto
E2
Calcolo Impronta Sensore
W
E3
Generazione Chiave Pubblica
sketch
Chiave Pubblica
E4
DB Utenti

Fig. 3

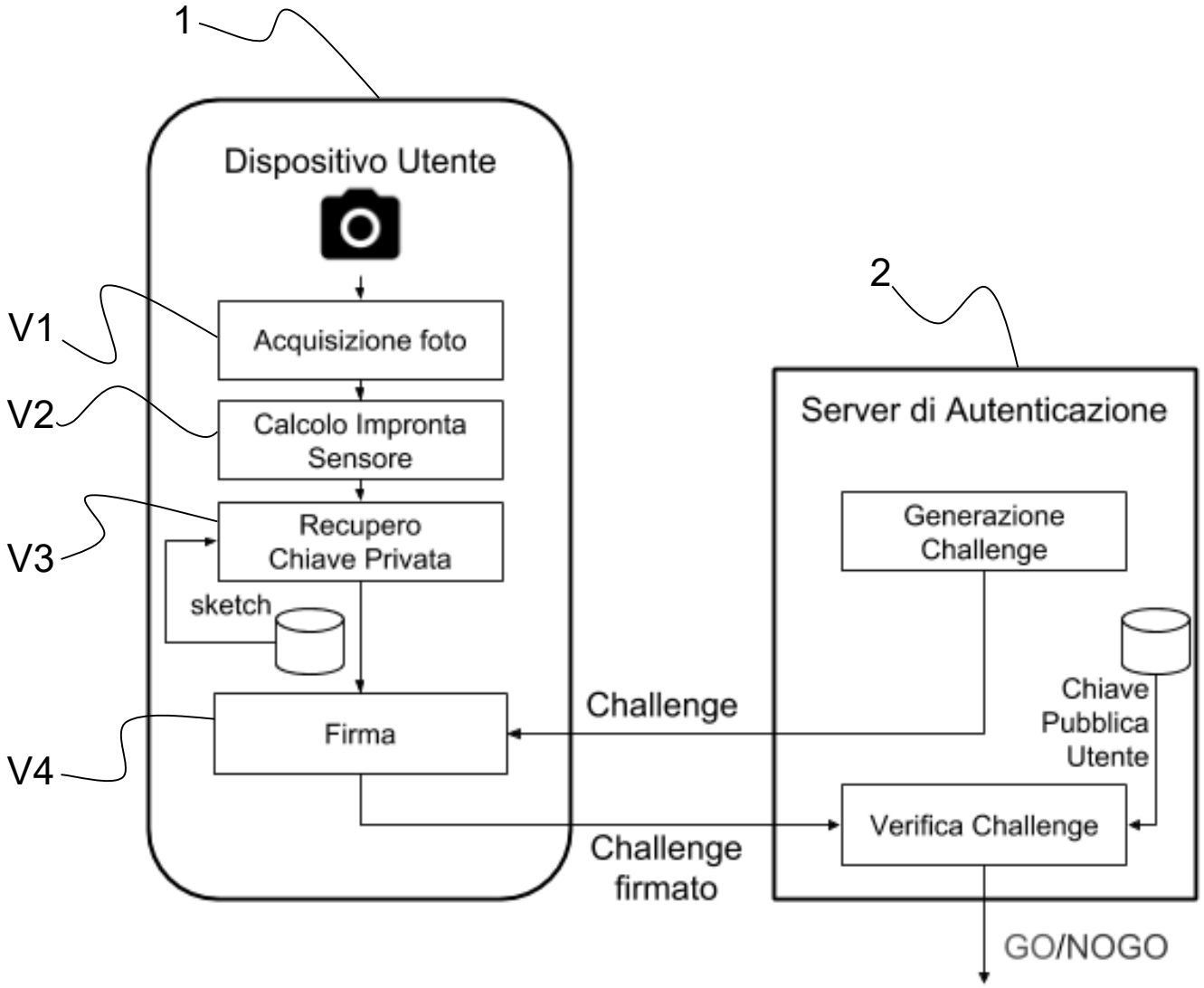
1
Dispositivo Utente
V1
Acquisizione foto
V2
Calcolo Impronta Sensore
V3
Recupero Chiave Privata
sketch
V4
Firma
2
Server di Autenticazione
Generazione Challenge
Chiave Pubblica Utente
Verifica Challenge
Challenge
Challenge firmato
GO/NOGO

Fig. 4

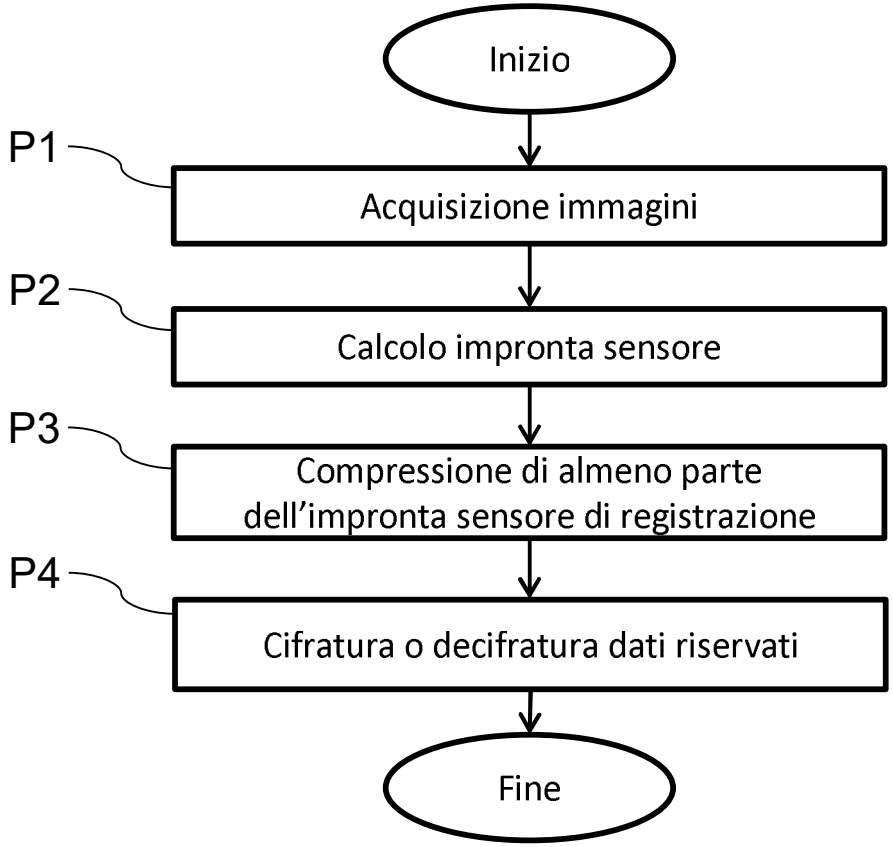
Inizio
P1
Acquisizione immagini
P2
Calcolo impronta sensore
P3
Compressione di almeno parte dell'impronta sensore di registrazione
P4
Cifratura o decifratura dati riservati
Fine

Fig. 5

Ministero dello Sviluppo Economico
DIREZIONE GENERALE SVILUPPO PRODUTTIVO E COMPETITIVITA'-
UFFICIO ITALIANO BREVETTI E MARCHI

RAPPORTO DI RICERCA

Numero della domanda
IO 90947
IT 201900007290

DOCUMENTI CONSIDERATI DI RILIEVO

Categoria	Citazione del documento con indicazione, se appropriata, delle parti rilevanti	Rivendicazioni rilevanti	CLASSIFICAZIONE DELLA DOMANDA (IPC)
X	WO 2018/073681 A1 (TORINO POLITECNICO [IT]) 26 April 2018 (2018-04-26) * page 1, line 5 - page 1, line 7 * * page 3, line 1 - page 3, line 11 * * page 8, line 13 - page 10, line 31 * * page 13, line 9 - page 14, line 19 * * page 16, line 7 - page 16, line 11 * * page 19, line 14 - page 20, line 23 * * figures 3, 5 * -----	1-13	INV. H04L9/32 H04L9/08 G06F21/73
X	VALSESIA DIEGO ET AL: "User Authentication via PRNU-Based Physical Unclonable Functions", IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, IEEE, PISCATAWAY, NJ, US, vol. 12, no. 8, 24 April 2017 (2017-04-24), pages 1941-1956, XP011648722, ISSN: 1556-6013, DOI: 10.1109/TIFS.2017.2697402 [retrieved on 2017-05-09] * abstract * * Sections: I, II.B, II.C, II.E, III * -----	1-13	
A	DIEGO VALSESIA ET AL: "Compressed Fingerprint Matching and Camera Identification via Random Projections", IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, vol. 10, no. 7, 2 June 2015 (2015-06-02), pages 1472-1485, XP055253084, US ISSN: 1556-6013, DOI: 10.1109/TIFS.2015.2415461 * abstract * * Sections: I, II.C * -----	1-13	

CAMPI TECNICI RICERCATI (IPC)
G06F
H04L

-/--

Questo rapporto di ricerca è stato redatto sulla base di tutte le rivendicazioni

Munich	Data di completamento della ricerca 17 January 2020	Esaminatore Volpato, Gian Luca

CATEGORIA DEI DOCUMENTI CITATI

X : di particolare rilevanza se considerato singolarmente
Y : di particolare rilevanza se combinato con un altro documento della stessa categoria
A : informazione generica
O : divulgazione orale
P : documento intermedio

T : teoria o principio alla base dell'invenzione
E : documento brevettuale antecedente, ma pubblicato dopo o alla data di deposito
D : documento citato nella domanda
L : documento citato per altre ragioni
.....
& : membro della stessa famiglia di brevetti, documento corrispondente

1

EPO FORM 1503 07.08 (P04C74)

Ministero dello Sviluppo Economico
DIREZIONE GENERALE SVILUPPO PRODUTTIVO E COMPETITIVITA'-
UFFICIO ITALIANO BREVETTI E MARCHI

RAPPORTO DI RICERCA

Numero della domanda
IO 90947
IT 201900007290

DOCUMENTI CONSIDERATI DI RILIEVO

Categoria	Citazione del documento con indicazione, se appropriata, delle parti rilevanti	Rivendicazioni rilevanti	CLASSIFICAZIONE DELLA DOMANDA (IPC)
A	US 2015/143130 A1 (DUCHARME PAUL D [CA] ET AL) 21 May 2015 (2015-05-21) * paragraphs [0011] - [0012], [0017] - [0018], [0021] - [0022] * * figure 1 * -----	1-13	

CAMPI TECNICI RICERCATI (IPC)

Questo rapporto di ricerca è stato redatto sulla base di tutte le rivendicazioni

1

Munich	Data di completamento della ricerca 17 January 2020	Esaminatore Volpato, Gian Luca

CATEGORIA DEI DOCUMENTI CITATI

X : di particolare rilevanza se considerato singolarmente
Y : di particolare rilevanza se combinato con un altro documento della stessa categoria
A : informazione generica
O : divulgazione orale
P : documento intermedio

T : teoria o principio alla base dell'invenzione
E : documento brevettuale antecedente, ma pubblicato dopo o alla data di deposito
D : documento citato nella domanda
L : documento citato per altre ragioni
.....
& : membro della stessa famiglia di brevetti, documento corrispondente

EPO FORM 1503 07.08 (P04C74)

ALLEGATO AL RAPPORTO DI RICERCA SULLA DOMANDA DI BREVETTO ITALIANO N.

IO 90947
IT 201900007290

Questo allegato enumera i membri della famiglia di brevetti relativi a documenti brevettuali citati nel summenzionato rapporto di ricerca.
I membri sono indicati come da database dell'Ufficio Europeo dei Brevetti al 17-01-2020
L'Ufficio Europeo dei Brevetti non si assume alcuna responsabilità per queste indicazioni, che vengono fornite a solo scopo informativo.

Documenti brevettuali citati nel rapporto di ricerca	Data di pubblicazione	Membri della famiglia di brevetti	Data di pubblicazione
WO 2018073681 A1	26-04-2018	CN 109997137 A	09-07-2019
		EP 3529728 A1	28-08-2019
		JP 2019536127 A	12-12-2019
		US 2019260739 A1	22-08-2019
		WO 2018073681 A1	26-04-2018
US 2015143130 A1	21-05-2015	CN 104657630 A	27-05-2015
		EP 2874135 A2	20-05-2015
		US 2015143130 A1	21-05-2015

Ministero dello Sviluppo Economico

DIREZIONE GENERALE SVILUPPO PRODUTTIVO E COMPETITIVITA' -
UFFICIO ITALIANO BREVETTI E MARCHI

OPINIONE SCRITTA

N. dossier	Data di deposito *(gg/mm/aa)*	Data di priorità *(gg/mm/aa)*	N. domanda
IO90947	27.05.2019		IT201900007290

Classificazione Internazionale dei Brevetti (IPC)
INV. H04L9/32 H04L9/08 G06F21/73

Richiedente
TOOTHPIC S.R.L., et al

Questa opinione fornisce indicazioni riguardanti i seguenti elementi:

- ☒ Riquadro N. I — Base dell'opinione
- ☐ Riquadro N. II — Priorità
- ☐ Riquadro N. III — Non-redazione di un'opinione a riguardo di novità, attività inventiva e applicazione industriale
- ☐ Riquadro N. IV — Violazione del requisito d'unità dell'invenzione
- ☒ Riquadro N. V — Dichiarazione motivata a riguardo di novità, attività inventiva o applicazione industriale; citazioni e spiegazioni giustificative della dichiarazione
- ☐ Riquadro N. VI — Particolari documenti citati
- ☐ Riquadro N. VII — Difetti particolari nella domanda
- ☐ Riquadro N. VIII — Osservazioni particolari a riguardo della domanda

	Esaminatore
	Volpato, Gian Luca

N. domanda

OPINIONE SCRITTA

IT201900007290

Riquadro N. I Base dell'opinione

1. Questa opinione è stata redatta sulla base delle ultime rivendicazioni depositate prima dell'inizio della ricerca nella tecnica anteriore.

2. Per quanto concerne eventuali sequenze di nucleotidi e/o amminoacidi descritte nella domanda e necessarie per l'invenzione di cui oggetto nelle rivendicazioni, questa opinione è stata redatta sulla base di:

   a. tipo di materiale:

   ☐ una sequenza di DNA

   ☐ una o più tabelle relative alla sequenza di DNA

   b. formato del materiale:

   ☐ cartaceo

   ☐ elettronico

   c. momento di deposito o presentazione:

   ☐ depositato insieme alla domanda al momento del deposito della medesima

   ☐ depositato insieme alla domanda in formato elettronico

   ☐ presentato successivamente al fine della ricerca d'anteriorità

3. ☐ Inoltre, ove sia stata depositata o presentata più di una versione o copia di una sequenza di DNA e/o tabella ad essa relativa, è stata presentata anche la dichiarazione obbligatoria che le informazioni contenute nelle copie successive o addizionali sono identiche a quelle nella domanda come depositata o che, in ogni caso, non vanno oltre il contenuto della domanda depositata originariamente.

4. Note aggiuntive:

N. domanda

OPINIONE SCRITTA

IT201900007290

Riquadro N. VDichiarazione motivata a riguardo di novità, attività inventiva o applicazione industriale; citazioni e spiegazioni giustificative della dichiarazione

1. 1. Dichiarazione

Novità (N)	Sì:	Rivendicazioni	1-13
	No:	Rivendicazioni	
Attività inventiva (IS)	Sì:	Rivendicazioni	
	No:	Rivendicazioni	1-13
Applicazione industriale (IA)	Sì:	Rivendicazioni	1-13
	No:	Rivendicazioni	

2. 2. Citazioni e spiegazioni

si veda l'allegato

Item V

1 **Prior art**

Reference is made to the following documents:

D1 WO 2018/073681 A1 (TORINO POLITECNICO [IT])
26 April 2018 (2018-04-26)

D4 US 2015/143130 A1 (DUCHARME PAUL D [CA] ET AL)
21 May 2015 (2015-05-21)

2 **Independent claims 1, 10, 12, 13**

The present application does not meet the criteria of patentability, because the subject-matter of independent claims 1, 10, 12, 13 does not involve an inventive step.

2.1 Document D1 is regarded as being the prior art closest to the subject-matter of claim 1 and discloses:

- a method (method for authenticating a user equipment by using a fingerprint of an image sensor, in D1: page 1 lines 5-8) ~~for the protection of confidential data~~,

characterised in that it comprises

- an image acquisition phase, wherein a plurality of images are captured by means of an image sensor (image acquisition phase E1, wherein a plurality of images are acquired, in D1: page 9 lines 12-16),

- an fingerprint calculation phase, wherein a sensor fingerprint is generated, by means of processing means, on the basis of said plurality of images captured during the image acquisition phase (registration fingerprint computation phase E2, wherein a registration fingerprint is generated, in D1: page 9 lines 17-21),

- a compression phase, wherein at least a portion of said encoding sensor fingerprint is encoded, by means of said processing means, using an algorithm of random projections, in such a way as to generate a compressed fingerprint (a registration fingerprint compression phase E4, wherein said registration sensor fingerprint is coded by using a random projection algorithm, in D1: page 9 lines 22-27),

~~- a processing phase, wherein said confidential data are encrypted and/or decrypted using said compressed fingerprint as a key.~~

2.2 The subject-matter of claim 1 differs from this known method in that:

- the compressed fingerprint is used as a key to encrypt and/or decrypt confidential data.

2.3 The technical effect of said difference is to achieve protection of confidential data.

The objective technical problem to be solved may therefore be regarded as: how to protect confidential data of the user and/or of the user equipment.

2.4 The solution proposed by the present invention is to use the compressed fingerprint is used as a key to encrypt and/or decrypt confidential data.

Said solution cannot be considered inventive, because, at the time of filing of the present application, it was well-known to a skilled person to use the output of a physical unclonable function (PUF) of an integrated circuit (e.g. a fingerprint of an image sensor) as a cryptographic key. For example, document D4 discloses an integrated circuit that generated PUF data, which are unique to the integrated circuit, and uses said PUF data to encrypt security information (D4: [0011],[0017],[0018],[0021]).

It would thus be straightforward for the skilled person to combine documents D1 and D4, thereby obtaining the subject-matter of claim 1 without involving any inventive step activity.

2.5 The subject-matter of claims 10, 12, 13 corresponds to a user apparatus, respectively an image sensor and a computer program product, adapted to perform the method of claim 1. Consequently, the lack of inventive step objection raised for claim 1 applies mutatis mutandis to claims 10, 12, 13.

3 **Dependent claims 2 - 9 and 11**

Dependent claims 2-9 and 11 do not appear to contain any additional features which, in combination with the features of any claim to which they refer, meet the requirements of inventive step.

Their subject-matter is either disclosed or directly derivable from the prior art document D1.

3.1 Claims 2-3 deal with details of the random projections. These features are disclosed in document D1 (D1: page 13 line 9 to page 14 line 19).

Claims 4-5 deal with the use of polar coding. These features are disclosed in document D1 (D1: page 10 lines 22-31, page 16 lines 7-11).

Claim 6 deals with quantization of the compressed fingerprint. These features are disclosed in document D1 (D1: page 13 line 33 to page 14 line 5).

Claim 7 deals with the filtering of signal frequency of the sensor fingerprint. These features are disclosed in document D1 (D1: page 20 lines 1-23).

Claim 8 deals with the filtering of period artifacts from the images. These features are disclosed in document D1 (D1: page 19 lines 14-25).

Claim 9 deals with the nature of the confidential data. This feature is not disclosed in document D1, however it is not evident what inventive technical contribution could be obtained by the confidential data comprising a private key.

Claim 11 deals with construction details of the user apparatus. These features are not disclosed in document D1, however they are considered as normal and straightforward solutions for blocking functionality of the image sensor.

Metroconsult

CONSULENTI IN PROPRIETA' INDUSTRIALE E INTELLETTUALE
INTELLECTUAL PROPERTY CONSULTANTS

UNA PROTEZIONE SU MISURA PER LE TUE IDEE
DEFENDING CREATIVITY WITH TAILORED PROTECTION

Matteo Baroni • Mirco Bianco • Corrado Borsano • Diego Borsetti • Marco Camolese
Filippo Ferroni • Raffaella Previtera • Giancarlo Reposio • Carmela Rotundo • Monica Serrau

SPETT.LE
MINISTERO SVILUPPO ECONOMICO
DIPARTIMENTO PER L'IMPRESA E L'INTERNAZIONALIZZAZIONE
DIREZIONE GENERALE PER LA LOTTA ALLA CONTRAFFAZIONE
UIBM – UFFICIO ITALIANO BREVETTI E MARCHI DIVISIONE XI
VIA MOLISE N. 19
00187 ROMA

OGGETTO: Domanda di brevetto italiana No. 102019000007290 depositata il 27.05.2019 dal titolo: "APPARATO D'UTENTE E METODO DI PROTEZIONE DI DATI RISERVATI"
Titolari: Toothpic S.r.l;
Politecnico di Torino

Vs. Rif.: PROT. IO 90947
Ns. Rif.: PLT055

Egregi Signori,

con riferimento alla Comunicazione Ministeriale del 31.01.2020 relativa alla domanda di brevetto sopra indicata, la Titolare deposita, con la presente, le proprie argomentazioni in replica alle obiezioni contenute nel Riquadro V della Ricerca di Anteriorità ricevuta in precedenza dall'Ufficio Italiano Brevetti e Marchi (UIBM).

Nel riquadro V, l'Esaminatore afferma che le rivendicazioni 1-13 come depositate sono nuove, ma non inventive e, quindi, non soddisfano i requisiti di brevettabilità ex Art. 45, comma 1, del Codice della Proprietà Industriale (C.P.I.).

1. Novità

a) L'oggetto della rivendicazione 1 si differenzia rispetto a ciascuno dei documenti di arte nota D1 e D4 citati dall'esaminatore per il fatto che nessuno di tali documenti descriva *"una fase di elaborazione, in cui si cifrano e/o decifrano detti dati riservati utilizzando detta impronta compressa come chiave"*, dove detta impronta compressa è stata compressa utilizzando un algoritmo di proiezioni casuali.

In particolare, il documento D4 descrive un metodo per cifrare/decifrare delle informazioni crittografiche utilizzando come chiave l'uscita prodotta da una funzione fisica non-clonabile (Physical unclonable function – PUF) eseguita da un circuito integrato (vedere par. 11, 17, 19, 21 di D4). È evidente come una chiave crittografica generata da una funzione fisica non-clonabile è differente da una chiave crittografica generata comprimendo un'impronta di un sensore di immagini mediante un algoritmo di proiezioni casuali.

Pertanto, l'oggetto della rivendicazione 1 è nuovo rispetto a ciascuno dei documenti D1 e D4.

b) La Titolare ritiene che le argomentazioni al punto *a)* riguardanti la novità della rivendicazione 1 si applichino, *mutatis mutandis*, anche alle rivendicazioni indipendenti 10, 12, 13 come depositate.

2. Attività inventiva

c) Rivendicazione 1:

Come stato della tecnica più vicino all'invenzione è stato considerato il contenuto del documento D1, in quanto D1 è l'arte nota che costituisce il punto di partenza più promettente per il tecnico del ramo, poiché D1 proviene da un ambito tecnico vicino a quello della presente invenzione.

L'effetto tecnico prodotto dalle caratteristiche tecniche distintive presenti nella parte caratterizzante della nuova prima rivendicazione è di consentire di proteggere chiavi crittografiche in un qualsiasi istante del ciclo di vita di un dispositivo mobile (vedere pag. 6, righe 1-10 della descrizione come depositata).

Questo effetto tecnico consente di risolvere il problema tecnico oggettivo di *come proteggere chiavi crittografiche in un qualsiasi istante del ciclo di vita di un dispositivo*.

L'oggetto della rivendicazione 1 risolve questo problema tecnico utilizzando come chiave crittografica un'impronta di un sensore di immagini compressa mediante un algoritmo di proiezioni casuali (Random Projection), così che se ci fosse una violazione della sicurezza (ad esempio se una terza persona riuscisse a generare un'impronta del sensore di immagini in maniera fraudolenta) sarebbe comunque possibile riportare un sistema di autenticazione nuovamente in uno stato sicuro utilizzando un nuovo seme per generare una nuova impronta compressa mediante l'algoritmo di proiezioni casuali.

D1 da solo e in combinazione con le conoscenze del tecnico del ramo:

Il documento D1 da solo non consentirebbe di risolvere il problema tecnico oggettivo, poiché D1 non contiene insegnamenti riguardo a come proteggere chiavi, ma bensì solo su come autenticare un terminale mobile sfruttando l'unicità dell'impronta del suo sensore di immagini. Pertanto, è evidente che l'insegnamento fornito da D1 è completamente differente dall'insegnamento della presente invenzione.

Inoltre, partendo dal documento D1, è opinione che il tecnico del ramo non svilupperebbe una soluzione come quella oggetto della rivendicazione 1 utilizzando le proprie conoscenze; infatti, per risolvere il problema tecnico oggettivo, il tecnico del ramo svilupperebbe una soluzione che cifrerebbe/decifrerebbe

le chiavi crittografiche mediante un algoritmo di crittografia simmetrica (come ad esempio il 3DES, l'AES o altro) utilizzando una password come chiave, in modo che per garantire la protezione delle chiavi crittografiche in un qualsiasi istante del ciclo di vita di un dispositivo (ad esempio dopo il furto di detta password) basterebbe utilizzare una nuova password per cifrare/decifrare le chiavi crittografiche.

Si ritiene, pertanto, che il documento D1 da solo o in combinazione con le conoscenze del tecnico del ramo non renda ovvio l'oggetto della prima rivendicazione come depositata.

D1 in combinazione con D4:

Come già discusso per la novità, il documento D4 insegna ad utilizzare come chiave l'uscita prodotta da una funzione fisica non-clonabile (Physical unclonable function – PUF) eseguita da un circuito integrato (vedere par. 11, 17, 19, 21 di D4). È opinione che questo insegnamento non risolva il problema tecnico oggettivo di *come proteggere chiavi crittografiche in un qualsiasi istante del ciclo di vita di un dispositivo*, poiché le funzioni fisiche non-clonabili producono un'uscita stabile, ossia ad un certo ingresso producono sempre una certa uscita. Per questo motivo, il tecnico del ramo considererebbe inadatta una funzione fisica non-clonabile al fine di proteggere chiavi crittografiche in un qualsiasi istante del ciclo di vita di un dispositivo; infatti, nel caso il dispositivo venisse violato, si dovrebbe procedere a sostituire il circuito integrato che implementa detta funzione fisica non-clonabile.

Nel caso il tecnico del ramo combinasse tra loro D1 e D4, si otterrebbe una chiave crittografica generata da una funzione fisica non-clonabile (Physical unclonable function – PUF) eseguita da un circuito integrato, dove detta funzione fisica non-clonabile riceverebbe in ingresso un'impronta di un sensore di immagini non compresso, producendo così un'uscita difficilmente ripetibile poiché l'impronta del sensore di immagine è affetta da rumore e, quindi, tale uscita non sarebbe utilizzabile come chiave crittografica. Pertanto, la soluzione generata dalla combinazione degli insegnamenti di D1 e D4 non risolverebbe il problema tecnico oggettivo.

È, quindi, opinione che il tecnico del ramo non consulterebbe il documento D4 per risolvere il problema tecnico oggettivo.

Si ritiene, pertanto, che il tecnico del ramo non combinerebbe gli insegnamenti di D4 con quanto descritto in D1 al fine di risolvere il problema tecnico oggettivo, rendendogli così impossibile sviluppare, senza compiere attività inventiva, una soluzione compresa nell'ambito di protezione della prima rivendicazione come depositata.

È, quindi, opinione che né il documento D1 preso singolarmente né la combinazione del documento D1 con le conoscenze del tecnico del ramo o con il documento D4 consenta al tecnico del ramo di sviluppare la soluzione oggetto della rivendicazione 1 come depositata, poiché è opinione che il tecnico del ramo risolverebbe il problema tecnico oggettivo sopra formulato sviluppando una soluzione differente da quella oggetto della prima rivendicazione.

Quindi l'oggetto della rivendicazione 1 è, oltre che nuovo, anche inventivo.

d) La Titolare ritiene che le argomentazioni al punto *c)* riguardanti l'attività inventiva della rivendicazione 1 si applichino, *mutatis mutandis*, anche alle rivendicazioni indipendenti 10, 12, 13 come depositate.

e) Le rimanenti rivendicazioni 2-9 e 11 come depositate risultano, alla luce delle argomentazioni sopra riportate, nuove ed inventive.

La Titolare richiede che il brevetto sia rilasciato il prima possibile, con facoltà di presentare ricorso alla Commissione dei Ricorsi, ai sensi dell'Art. 135 CPI, in caso di rifiuto del medesimo.

Un Mandatario

Allegati:
- N/A.

RIASSUNTO

L'invenzione consiste in un metodo ed in un apparato d’utente (1) per la protezione di dati riservati, dove detto apparato comprende un sensore di immagini (14) e mezzi di elaborazione (11) configurati per acquisire una pluralità di immagini mediante detto sensore di immagini (14), generare un’impronta sensore sulla base di detta pluralità di immagini, codificare almeno una porzione di detta impronta sensore utilizzando un algoritmo di proiezioni casuali in modo da generare un’impronta compressa (W), cifrare e/o decifrare detti dati riservati utilizzando detta impronta compressa (W) come chiave.

(figure 2 e 5)

PLT055

Descrizione dell'Invenzione Industriale dal titolo:

"APPARATO D'UTENTE E METODO DI PROTEZIONE DI DATI RISERVATI"

A nome di

- POLITECNICO DI TORINO (titolare al 50% dell'invenzione), di nazionalità italiana, con sede in Corso Duca degli Abruzzi 24, 10129 Torino;
- TOOTHPIC S.r.l. (titolare al 50% dell'invenzione) di nazionalità italiana, con sede in Corso Castelfidardo 30/a, 10129 Torino;

ed elettivamente domiciliati, ai fini del presente incarico, presso i Mandatari Mirco BIANCO (No. Iscr. Albo 1639B), Filippo FERRONI (No. Iscr. Albo 530BM), Marco CAMOLESE (No. Iscr. Albo 882BM), Giancarlo REPOSIO (No. Iscr. Albo 1168BM), Corrado BORSANO (No. Iscr. Albo 446 BM) e Matteo BARONI (No. Iscr. Albo 1064 BM) c/o Metroconsult Milano S.r.l., Via Palestro 5/2, 16122 GENOVA (GE).

Inventori designati:

- **MAGLI Enrico**, di nazionalità italiana, residente in Via Ferrante Aporti 28, 10131 Torino, Italia;
- **COLUCCIA Giulio**, di nazionalità italiana, residente in Via Leonardo da Vinci, 9/1, 10095 Grugliasco, Torino, Italia;
- **VALSESIA Diego**, di nazionalità italiana, residente in Via Bogogno 8, 28021 Borgomanero, Novara, Italia;
- **BIANCHI Tiziano**, di nazionalità italiana, residente in Viale Alcide De Gasperi 63, 59100 Prato, Italia.

DESCRIZIONE

La presente invenzione si riferisce ad un apparato d'utente (user equipment; come uno smartphone, un tablet, un personal computer, un laptop, o altro) e ad un metodo per la protezione di dati riservati; in particolare per cifrare/decifrare una chiave crittografica privata.

Come è noto, i sistemi di autenticazione elettronica secondo lo stato dell'arte si basano su tecniche di crittografia asimmetrica. L'utilizzo di queste tecniche richiede che a ciascun utente/dispositivo venga assegnata una coppia di stringhe generate in maniera (pseudo)casuale dette chiavi, ossia una 'chiave pubblica' ed una 'chiave privata'. La chiave privata è il segreto (non condiviso) che consente di autenticare l'utente/dispositivo. Essa deve essere custodita dall'utente/dispositivo e mai condivisa pubblicamente. Al contrario, la chiave pubblica è l'informazione che l'utente può e deve divulgare per consentire il funzionamento dei sistemi basati su questo tipo di crittografia. Ad esempio, nel caso in cui l'utente A vuole inviare all'utente B un messaggio criptato, l'utente A deve essere in possesso della chiave pubblica di B, con la quale cripta il messaggio e lo invia all'utente B. L'utente B, essendo l'unico soggetto in possesso della sua chiave privata, è l'unico soggetto in grado di decodificare il messaggio; infatti, la decodifica del messaggio cifrato con la chiave pubblica di B può avvenire solo tramite la chiave privata dell'utente B.

Un altro esempio in cui sono utilizzate le tecniche di crittografia asimmetrica per l'autenticazione è quello in cui si utilizza la cosiddetta 'firma digitale', che permette ad un utente A di verificare l'identità dell'utente B. In questo scenario, l'utente A invia all'utente B un messaggio, detto challenge, dopodiché l'utente B firma il challenge usando la propria chiave privata, e invia il messaggio firmato

all'utente A. L'utente A, in possesso della chiave pubblica dell'utente B, può verificarne l'identità verificando con la chiave pubblica la firma dell'utente B e la consistenza del messaggio.

Esistono diverse soluzioni secondo lo stato dell'arte per custodire la chiave privata, come la memorizzazione su hardware dedicato rimovibile (ad esempio un token USB, una smart card, un hardware ledger per criptomonete o altro), la memorizzazione su memoria non volatile (in chiaro o cifrata), l'esecuzione delle applicazioni che possono accedere a tale chiave in un ambiente di esecuzione sicuro (*Trusted Execution Environment*), la memorizzazione in un chip crittografico dedicato (noto anche con il termine di *Secure Element*) contenuto all'interno di uno smartphone, e la memorizzazione in cloud.

Ciascuno di questi sistemi appena elencati presenta però dei problemi e/o delle vulnerabilità. Infatti, la memorizzazione su hardware dedicato esterno presenta lo svantaggio che l'utente deve portare con sé tutto l'hardware necessario (il token per accedere al servizio, il token per firmare, la smartcard, il lettore di smartcard, ecc.). Inoltre, l'hardware dedicato potrebbe non essere di uso generico (*general purpose*), potrebbe cioè consentire solo determinate operazioni, o solo con le chiavi precaricate in fase di fabbricazione. Potrebbe, inoltre, presentare problemi di interfaccia; infatti, risulta molto spesso impossibile collegare un token USB ad uno smartphone.

La memorizzazione nella memoria locale del dispositivo in chiaro risulta, invece, essere vulnerabile ad un qualsiasi utente malintenzionato (*malicious user*) in possesso delle credenziali di accesso al device.

La memorizzazione criptata su memoria locale non volatile è vulnerabile a un qualsiasi utente malintenzionato in possesso

delle credenziali di accesso al device ed in grado di effettuare una copia della memoria e di decriptare (offline) il contenuto della memoria.

L'esecuzione delle applicazioni che possono accedere a tale chiave in un ambiente di esecuzione sicuro (*Trusted Execution Environment*), ossia in un'area virtualizzata del processore e della memoria RAM del dispositivo, non accessibile a tutte le applicazioni del sistema, ma solo a quelle appositamente realizzate, presenta una minore flessibilità nella realizzazione delle applicazioni, poiché una maggiore sicurezza corrisponde a minori possibilità da parte di applicazioni terze e ad una maggior richiesta di memoria e di potenza di calcolo per realizzare l'ambiente virtuale; inoltre, l'ambiente di esecuzione sicuro offre una maggiore "superficie di attacco", poiché, essendo basato su un'implementazione software, può essere modificato (in modo malevolo) disponendo dei privilegi adatti.

La memorizzazione in un chip crittografico dedicato presenta lo svantaggio di essere poco flessibile come già descritto per l'hardware dedicato esterno. Le versioni aggiornabili di tali chip crittografici presentano, invece, delle vulnerabilità. Infatti, i dati al loro interno sono scritti su memoria riscrivibile, rendendo comunque possibile la creazione di cloni (come è possibile per gli ambienti di esecuzione sicuri).

La memorizzazione dei dati in cloud richiede la connessione a Internet e richiede inoltre che i server su cui sono custodite le chiavi siano sicuri (livello di sicurezza di cui ci si deve fidare, poiché gli apparati in cui avviene fisicamente la memorizzazione non sono sotto il diretto controllo dell'utente proprietario delle chiavi).

Risulta evidente come queste vulnerabilità permettano ad una terza persona di effettuare il cosiddetto furto di identità

elettronica (*electronic identity theft*), consentendo a detta terza persona di mettere in atto i suoi intenti criminali, come trasferire i soldi dal conto bancario di un utente verso un altro conto, inviare messaggi di posta elettronica dall'account dell'utente verso tutti gli altri indirizzi presenti nella rubrica dell'utente minimizzando gli effetti dei filtri anti-spam, vendere l'identità rubata ad un'altra persona, o altro.

La presente invenzione si propone di risolvere questi ed altri problemi mettendo a disposizione un metodo per la protezione di dati riservati come da rivendicazioni allegate.

Inoltre, la presente invenzione mette anche a disposizione un apparato d’utente per la protezione di dati riservati come da rivendicazioni allegate.

L’idea alla base della presente invenzione è di configurare un apparato d’utente in modo da acquisire una pluralità di immagini mediante un sensore di immagini compreso in detto apparato, generare un’impronta sensore sulla base di detta pluralità di immagini, codificare almeno una porzione di detta impronta sensore utilizzando un algoritmo di proiezioni casuali in modo da generare un’impronta compressa, e cifrare e/o decifrare detti dati riservati utilizzando detta impronta compressa come chiave.

In questo modo, è possibile aumentare la sicurezza di un sistema di autenticazione; infatti, risulta essere particolarmente complesso (se non impossibile) compiere un furto d'identità rubando una chiave privata cifrata utilizzando un’impronta compressa come chiave, poiché per decifrare detta chiave privata cifrata è necessario possedere l’impronta del sensore di immagini che, per essere determinata richiede di aver accesso al terminale d’utente con i diritti di accesso sufficienti ad utilizzare il sensore di immagini di detto apparato d’utente.

Inoltre, nel caso in cui una terza persona (l'attaccante) riuscisse a generare un'impronta del sensore di immagini in maniera fraudolenta (ad esempio acquisendo delle foto scattate mediante detto sensore direttamente dal terminale d'utente o da Internet), sarebbe comunque possibile riportare il sistema di autenticazione nuovamente in uno stato sicuro utilizzando un nuovo seme per generare una nuova impronta compressa mediante l'algoritmo di proiezioni casuali, e cifrando una nuova chiave privata utilizzando detta nuova impronta compressa come chiave.

Si evidenzia anche che, memorizzando in maniera sicura le chiavi negli apparati d'utente, è possibile utilizzare vantaggiosamente apparati già in possesso degli utenti, evitando così il costo di acquisto e gestione di hardware dedicato; inoltre, questa soluzione tecnica risulta essere molto flessibile, poiché consente l'offuscamento di chiavi già in possesso degli utenti ed un utilizzo universale in sistemi di autenticazione già funzionanti. Infatti, tale soluzione può essere utilizzata come un livello aggiuntivo di sicurezza, in grado di rendere possibile l'utilizzo di una chiave soltanto se è disponibile l'impronta del sensore della camera.

Ulteriori caratteristiche vantaggiose della presente invenzione sono oggetto delle allegate rivendicazioni.

Queste caratteristiche ed ulteriori vantaggi della presente invenzione risulteranno maggiormente chiari dalla descrizione di una sua forma di attuazione mostrata nei disegni annessi, forniti a puro titolo esemplificativo e non limitativo, in cui:

- fig. 1 illustra un sistema di autenticazione comprendente un apparato d'utente secondo l'invenzione;
- fig. 2 illustra uno schema a blocchi dell'apparato d'utente di fig. 1;
- fig. 3 illustra un diagramma di flusso che rappresenta il

funzionamento del sistema di fig. 1 durante una sessione di registrazione;

- fig. 4 illustra un diagramma di flusso che rappresenta il funzionamento del sistema di fig. 1 durante una sessione di autenticazione;
- fig. 5 illustra un diagramma di flusso che rappresenta un metodo di protezione di dati riservati secondo l'invenzione.

Il riferimento ad "una forma di attuazione" all'interno di questa descrizione sta ad indicare che una particolare configurazione, struttura o caratteristica è compresa in almeno una forma di attuazione dell'invenzione. Quindi, i termini "in una forma di attuazione" e simili, presenti in diverse parti all'interno di questa descrizione, non sono necessariamente tutti riferiti alla stessa forma di attuazione. Inoltre, le particolari configurazioni, strutture o caratteristiche possono essere combinate in ogni modo adeguato in una o più forme di attuazione. I riferimenti utilizzati nel seguito sono soltanto per comodità e non limitano l'ambito di tutela o la portata delle forme di attuazione.

Con riferimento a fig. 1, verrà ora descritto un sistema di autenticazione S, ad esempio operante secondo lo standard WebAuthn (promosso dalla FiDO Alliance), in un tipico scenario di utilizzo; tale sistema di autenticazione S comprende le seguenti parti:

- un apparato d'utente 1 secondo l’invenzione, come ad esempio uno smartphone, un tablet o altro;
- un server applicativo 2 atto ad erogare almeno un servizio (come ad esempio un servizio di rete sociale, di posta elettronica, di trading, di home banking, di e-commerce, di banking online, di scambio (exchange) per criptovalute, o altro) che richiede l'autenticazione dell'apparato d'utente

1, ossia che necessita di accertare che l'apparato d’utente 1 sia lo stesso apparato d'utente a cui è stato associato un particolare account nel corso di una fase di registrazione (meglio descritta nel seguito di questa descrizione) e a cui sono associati dei servizi privati e/o personali (ad esempio l'accesso al proprio conto corrente o a quello di una società, l'accesso al proprio profilo o quello di una società su un servizio di rete sociale come Facebook, o altro).

L'apparato d'utente 1 ed il server applicativo 2 sono in comunicazione di segnale tra loro mediante una rete dati, preferibilmente una rete dati di tipo pubblico (come ad esempio Internet).

Il server applicativo 2 può essere costituito da uno o più server opportunamente configurati per formare un cluster, ed è preferibilmente configurato per inviare all’apparato d’utente almeno una richiesta di autenticazione dopo che l’apparato d’utente 1 ha richiesto a detto server applicativo 2 l’accesso a servizi privati e/o personali, ossia a servizi che richiedono l’autenticazione di detto apparato d’utente 1; tale richiesta di autenticazione comprende preferibilmente una stringa di caratteri (che rappresenta ad esempio l’orario di tale richiesta) che l’apparato d’utente 1 deve ritornare firmata utilizzando la sua firma privata, così che il server applicativo 2 possa autenticare detto apparato d’utente 1 utilizzando la chiave pubblica associata a detta chiave privata.

L'apparato d'utente 1 comprende un sensore di immagini 14 (come ad esempio un sensore fotografico, un sensore per la visione notturna, o altro); tale apparato d'utente 1 può anche essere costituito alternativamente da un personal computer, da un laptop, o da un altro dispositivo elettronico in comunicazione di segnale con un sensore di immagini (come ad

esempio una webcam), preferibilmente compreso (integrato) all'interno di detto dispositivo.

Il server applicativo 2 comprende alcuni elementi funzionalmente simili a quelli dell'apparato d'utente 1 (ossia mezzi di controllo ed elaborazione, mezzi di memoria volatile, mezzi di memoria di massa, i mezzi di comunicazione e i mezzi di ingresso/uscita) in comunicazione di segnale tra loro e configurati per eseguire delle differenti funzioni che verranno meglio descritte nel seguito di questa descrizione; inoltre, tale server applicativo 2 può anche coincidere con l'apparato d'utente 1 nel caso in cui il servizio che richiede l'autenticazione dell'apparato d'utente 1 sia eseguito direttamente da detto apparato d'utente 1.

Con riferimento anche a fig. 2, l'apparato d'utente 1 (come ad esempio uno smartphone, un tablet o altro) secondo l'invenzione comprende i seguenti componenti:

- mezzi di controllo ed elaborazione 11 (detti anche mezzi di elaborazione), come ad esempio una o più CPU, che governano il funzionamento del dispositivo 1, preferibilmente in modo programmabile, mediante l'esecuzione di apposite istruzioni;
- mezzi di memoria volatile 12, come ad esempio una memoria ad accesso casuale RAM, che è in comunicazione di segnale con i mezzi di controllo ed elaborazione 11, e dove in detti mezzi di memoria volatile 12 possono essere memorizzate almeno le istruzioni che implementano il metodo secondo l'invenzione e che possono essere lette dai mezzi di controllo ed elaborazione 11 quando il dispositivo 1 è in una condizione di funzionamento;
- mezzi di memoria di massa 13, preferibilmente uno più dischi magnetici (hard disk) o una memoria di tipo Flash o altro tipo, che sono in comunicazione di segnale con i mezzi di controllo ed elaborazione 11 e con i mezzi di

memoria volatile 12;

- il sensore di immagini 14, come ad esempio un sensore fotografico, un sensore per la visione notturna, ad infrarossi o altro;
- mezzi di comunicazione 15, preferibilmente un'interfaccia di rete che opera secondo uno standard della famiglia 802.11 (noto con il nome di WiFi), 802.16 (noto con il nome di WiMax), IEEE 803.2 (noto anche con il nome di Ethernet) o un'interfaccia ad una rete dati di tipo GSM/GPRS/UMTS/LTE, TETRA o altro, che permettono al dispositivo 1 di comunicare con altri dispositivi attraverso una rete dati, dove questi ultimi saranno meglio descritti nel seguito di questa descrizione;
- mezzi di ingresso/uscita (I/O) 16 che possono ad esempio essere utilizzati per collegare a detto dispositivo 1 delle periferiche (come ad esempio una o più interfacce che consentano l'accesso ad altri mezzi di memoria di massa in modo da permettere preferibilmente la copiatura delle informazioni da questi ai mezzi di memoria di massa 13) oppure ad un terminale di programmazione configurato per scrivere delle istruzioni (che i mezzi di elaborazione e controllo 11 dovranno eseguire) nei mezzi di memoria 12,13; tali mezzi di ingresso/uscita 16 possono ad esempio comprendere un adattatore USB, Firewire, RS232, IEEE 1284 o altro;
- un bus di comunicazione 17 che permette lo scambio di informazioni tra i mezzi di controllo ed elaborazione 11, i mezzi di memoria volatile 12, i mezzi di memoria di massa 13, il sensore di immagini 14, i mezzi di comunicazione 15, ed i mezzi di ingresso/uscita 16.

In alternativa al bus di comunicazione 17, è possibile collegare con un'architettura a stella i mezzi di controllo ed elaborazione 11, i mezzi di memoria volatile 12, i mezzi di

memoria di massa 13, il sensore di immagini 14, i mezzi di comunicazione 15 e i mezzi di ingresso/uscita 16.

Con riferimento anche a fig. 3, verrà ora descritto con maggior dettaglio uno scenario tipico di utilizzo del metodo e dell'apparato d'utente 1 secondo l'invenzione in cui vengono eseguite le fasi di un metodo per registrare detto apparato d'utente 1 in modo da rendere successivamente possibile l'autenticazione di detto apparato d'utente 1 presso detto dispositivo 1. Il metodo di registrazione, che viene preferibilmente eseguito da detto apparato d'utente 1, comprende le seguenti fasi:

- una fase di acquisizione immagini E1, in cui una pluralità di immagini (preferibilmente un numero compatibile con la potenza di calcolo messa a disposizione dai mezzi di elaborazione 11, ad esempio un numero compreso tra 10 e 30 immagini) viene acquisita mediante il sensore di immagini 14, preferibilmente in formato grezzo (RAW) in modo da rendere maggiormente evidenti i difetti del sensore di immagini 14 dovuti alle impurità delle porzioni di silicio che lo compongono;
- una fase di calcolo impronta di registrazione E2, in cui un'impronta sensore di registrazione è generata, mediante i mezzi di elaborazione 11 dell'apparato d'utente 1, sulla base di detta pluralità di immagini acquisita nel corso di detta fase E1, e dove detta almeno una porzione di detta impronta sensore di registrazione viene codificata (compressa), mediante i mezzi di elaborazione e controllo dell'apparato d'utente 1, utilizzando un algoritmo di proiezioni casuali, in modo da generare un'impronta compressa W di detta almeno una porzione di detta impronta sensore di registrazione. Ad esempio, i mezzi di elaborazione e controllo dell'apparato d'utente 1 sono configurati per eseguire un insieme di istruzioni che

implementa detto algoritmo di proiezioni casuali (che verrà meglio descritto nel seguito di questa descrizione);

- una fase di preparazione chiavi E3, in cui viene generata una coppia di chiavi, ossia una chiave pubblica ed una chiave privata, e viene trasmessa al server applicativo 2 la chiave pubblica, mentre la chiave privata viene cifrata, preferibilmente mediante un algoritmo di crittografia simmetrico, utilizzando come chiave detta impronta compressa W, così da generare una chiave privata cifrata (detta anche 'sketch') che viene memorizzata nei mezzi di memoria 12,13;
- una fase di trasmissione chiave pubblica E4, in cui la chiave pubblica generata nel corso della fase E3 è trasmessa al server applicativo 2 mediante i mezzi di comunicazione 15 di detto apparato d'utente 1, preferibilmente attraverso un canale protetto (come ad esempio una connessione SSL o altro).

Con riferimento anche a fig. 4, verrà ora descritto un metodo per autenticare detto apparato d'utente 1 presso detto server applicativo 2. Il metodo di autenticazione, che viene preferibilmente eseguito da detto apparato d'utente 1, comprende le seguenti fasi:

- una fase di acquisizione immagini V1, in cui almeno un'immagine (preferibilmente un numero di immagini compatibile con la potenza di calcolo messa a disposizione dai mezzi di elaborazione 11, ad esempio un numero compreso tra cinque e dieci immagini) viene acquisita mediante il sensore di immagini 14, preferibilmente in formato grezzo (RAW) per le stesse ragioni già sopra enunciate;
- una fase di calcolo impronta di autenticazione V2, in cui un'impronta sensore di autenticazione è generata, mediante i mezzi di elaborazione 11 apparato d'utente 1, sulla base di detta pluralità di immagini acquisita nel corso di detta

fase V1 in maniera simile o uguale alla fase E2 sopra descritta, così da generare un'impronta compressa W di almeno una porzione di detta impronta sensore di autenticazione;

- una fase di recupero chiave privata V3, in cui, mediante i mezzi di elaborazione 11, la chiave privata cifrata (detta anche 'sketch') viene letta dai mezzi di memoria 12,13 e decifrata, preferibilmente mediante un algoritmo di crittografia simmetrico omologo o identico a quello utilizzato nel corso della fase E3, utilizzando detta impronta compressa W come chiave, così da recuperare la chiave privata, ossia ottenere una copia in chiaro di detta chiave privata;
- una fase di firma V4, in cui viene ricevuta dal server applicativo 2 una richiesta di autenticazione (ossia un messaggio detto anche 'challenge'), ed i mezzi di elaborazione 11 eseguono i seguenti passi:
  - generare una firma elettronica sulla base della richiesta di autenticazione eseguendo un algoritmo di firma digitale (come ad esempio DSA, ECDSA, o altro, ossia un algoritmo di crittografia asimmetrico) che utilizza la chiave privata come chiave;
  - trasmettere, mediante i mezzi di comunicazione 15, detta firma elettronica al server applicativo 2.

Quando il sistema S è in una condizione di funzionamento, gli elementi 1,2,3 di detto sistema eseguono preferibilmente i seguenti passi:

- l'apparato d'utente genera una coppia di chiavi, ossia una chiave pubblica ed una chiave privata, e si registra presso il server applicativo 2 trasmettendogli la propria chiave pubblica e memorizzando la propria chiave privata nei mezzi di memoria 12,13;
- l'apparato d'utente 1 accede ai servizi pubblici erogati

dal server applicativo 2 (ad esempio accedendo alla “landing page” del servizio erogato da detto server 2) e trasmette le proprie informazioni d’utente richiedendo l’accesso a detto almeno un servizio che necessita l'autenticazione di detto apparato d’utente 1;

- il server applicativo 2 genera una richiesta di autenticazione (il ‘challenge’) sulla base delle informazioni d’utente ricevute dall’apparato d’utente (ad esempio creando un messaggio che include almeno dette informazioni d’utente) e trasmette detta richiesta d’autenticazione al dispositivo 1;
- l’apparato d’utente 1 compie i seguenti sottopassi:
  - generare una firma elettronica sulla base della richiesta di autenticazione eseguendo un algoritmo di firma digitale (come ad esempio il DSA, il ECDSA, o altro, ossia un algoritmo di crittografia asimmetrico) che utilizza (dopo aver eseguito il metodo secondo l’invenzione come di seguito descritto) la chiave privata come chiave;
  - trasmettere detta firma elettronica al server applicativo 2;
- il server applicativo 2 verifica l’autenticità della firma elettronica ricevuta da detto apparato d’utente 1 eseguendo un algoritmo di verifica di firma digitale (come ad esempio il DSA, il ECDSA, o altro, ossia un algoritmo di crittografia asimmetrico) che utilizza la chiave pubblica come chiave.

Con riferimento anche a fig. 5, verrà ora descritto, nello specifico, il metodo secondo l’invenzione che è eseguito nel corso dei metodi di registrazione ed autenticazione sopra descritti e che può essere generalizzato come un metodo per la protezione di dati privati (come ad esempio una o più chiavi private) comprendente i seguenti passi:

- una fase di acquisizione immagini P1, in cui una pluralità di immagini vengono acquisite mediante un sensore di immagini 14;
- una fase di calcolo impronta P2, in cui un'impronta sensore è generata, mediante mezzi di elaborazione 11, sulla base di detta pluralità di immagini acquisita nel corso della fase di acquisizione immagini P1;
- una fase di compressione P3, in cui almeno una porzione di detta impronta sensore di codifica viene codificata, mediante detti mezzi di elaborazione 11, utilizzando un algoritmo di proiezioni casuali, in modo da generare un'impronta compressa W;
- una fase di elaborazione P4, in cui si cifrano e/o decifrano detti dati riservati utilizzando detta impronta compressa W come chiave.

In questo modo, è possibile aumentare la sicurezza di un sistema di autenticazione.

Nel corso della fase di elaborazione P4, le operazioni di cifratura e/o decifratura di detti dati riservati possono essere preferibilmente effettuate compiendo un'operazione di OR esclusivo bit a bit (bitwise-XOR) tra detta impronta compressa W ed una stringa composta da almeno detti dati riservati.

Nel corso della fase di compressione P3, vengono compresse le impronte sensore calcolate nel corso della fase di calcolo impronta P2, utilizzando la tecnica delle proiezioni casuali (Random Projections - RP). In altre parole, durante ciascuna la fase P3, i mezzi di elaborazione e controllo dell'apparato d'utente 1 sono configurati per eseguire un insieme di istruzioni che implementa un algoritmo di compressione che sfrutta la tecnica delle proiezioni casuali.

Questo algoritmo prevede di comprimere le impronte sensore di registrazione e di autenticazione con pochissima o

idealmente nessuna perdita di informazione. Più nel dettaglio, la tecnica delle proiezioni casuali è un potente e poco complesso metodo di riduzione dimensionale che si basa sull'idea di proiettare i dati *n*-dimensionali originali su un sottospazio *m*-dimensionale, con $m < n$, utilizzando una matrice casuale $\Phi \in \mathbb{R}^{m \times n}$. Di conseguenza, un'impronta del sensore *n*-dimensionale $k \in \mathbb{R}^n$ viene ridotta a un sottospazio *m*-dimensionale $y \in \mathbb{R}^m$ mediante la seguente formula:

$$y = \Phi k \tag{8}$$

La proprietà chiave che soggiace alla tecnica RP è il lemma di Johnson-Lindenstrauss (che si considera parte integrante di questa descrizione), riguardante l'incorporazione (embedding) a bassa distorsione di punti da spazi euclidei alto-dimensionali a spazi euclidei basso-dimensionali. Il lemma stabilisce che un piccolo insieme di punti in uno spazio alto-dimensionale può essere incorporato in uno spazio di dimensioni molto inferiori in maniera tale da (quasi) preservare le distanze tra i punti.

Basandosi su tale presupposto, l'apparato d'utente 1 può essere configurato per calcolare una versione compressa di ciascuna delle impronte sensore da lui calcolate mediante proiezioni casuali, vale a dire mediante una moltiplicazione (prodotto matriciale) tra una matrice di compressione e una matrice che rappresenta detta impronta sensore (o viceversa), dove detta matrice di compressione ha un numero di righe (o colonne) inferiore a quello della matrice che rappresenta l'impronta sensore.

Il risultato di detto prodotto può essere quantizzato, ovvero rappresentato su un numero finito di bit, al fine di ottenere una rappresentazione più compatta della versione compressa dell'impronta sensore. Ad esempio, una versione binaria dell'impronta sensore compressa può essere ottenuta

mediante la seguente formula:

$$w = sign(y)$$

In altre parole, nel corso della fase di compressione P3, detta almeno una porzione di detta impronta sensore di codifica viene codificata utilizzando un algoritmo di proiezioni casuali, così da generare una impronta sensore codificata; dopodiché, detta impronta sensore codificata viene quantizzata mediante i mezzi di elaborazione 11, generando detta l'impronta compressa W.

Così facendo è possibile generare una versione compressa dell'impronta sensore (di registrazione o di autenticazione) memorizzando e processando meno dati e, soprattutto, non richiedendo al dispositivo 1 di eseguire la decifratura dei dati sensibili senza che le proprietà di sicurezza del sistema di autenticazione S subiscano un degrado. In questo modo, la riduzione della complessità in spazio permette all'apparato d'utente 1 un impiego limitato di risorse, così che tale sistema di autenticazione S possa essere impiegato su di un largo numero di terminali d'utente. Questo permette di aumentare il livello di sicurezza globale, poiché è possibile realizzare un sistema di autenticazione S utilizzando terminali d'utente non necessariamente di ultima generazione.

In alternativa o in combinazione a quanto sopra descritto, la sicurezza del sistema può essere ulteriormente aumentata dal metodo di generazione delle proiezioni casuali in quanto esso si basa sull'uso di un generatore di numeri pseudo-casuali che è inizializzato da un seme mantenuto segreto sul dispositivo dell'utente.

Più nel dettaglio, il metodo secondo l'invenzione può anche comprendere una fase di generazione casuale, in cui si genera, mediante i mezzi di elaborazione, una stringa casuale di bit, e dove nel corso della fase di compressione P3, detto algoritmo di proiezioni casuali genera un insieme di

proiezioni casuali, preferibilmente una matrice di tipo BCCB (Block circulant with circulant blocks), sulla base di detta stringa casuale di bit, così che nel corso della fase di elaborazione P4, quando si cifrano i dati riservati, è possibile vantaggiosamente utilizzare un impronta compressa generata con una nuova stringa casuale di bit (seme).

La stringa casuale di bit è preferibilmente memorizzata nei mezzi di memoria 12,13 per consentire un successivo riuso quando è necessario decifrare i dati riservati. A tale scopo, il metodo secondo l'invenzione può anche comprendere una fase di lettura stringa casuale, in cui si legge, mediante i mezzi di elaborazione 11, la stringa casuale di bit memorizzata nei mezzi di memoria 12,13, e dove nel corso della fase di compressione P3, i mezzi di elaborazione 11 generano un insieme di proiezioni casuali sulla base di detta stringa casuale di bit, così che nel corso della fase di elaborazione P4, quando si decifrano i dati riservati, è possibile ricostruire l'impronta compressa utilizzata in precedenza (per la cifratura dei dati riservati).

In questo modo, è possibile aumentare la sicurezza del sistema di autenticazione, rendendo possibile gestire la situazione in cui un attaccante riesce a generare un'impronta del sensore di immagini in maniera fraudolenta; infatti, generando una nuova stringa casuale di bit e utilizzandola per cifrare una nuova chiave privata (e ripetendo la procedura di registrazione) è possibile riportare il sistema di autenticazione S in uno stato sicuro.

Si evidenzia che l'impronta calcolata nel corso della fase P2 e utilizzata dall'apparato d'utente 1 per registrarsi presso il server applicativo 2 è (molto probabilmente) differente da quella che verrà utilizzata per l'autenticazione. Infatti, si evidenzia anche che, essendo l'impronta sensore di fatto una misura di una caratteristica

del sensore, due impronte distinte determinate in istanti di tempo distinti tra loro saranno difficilmente uguali tra loro, poiché saranno affette da rumore come avviene per ogni altra misura; infatti, l'impronta generate nel corso della fase P2 è dipendente dalla quantità di luce che raggiunge il sensore di immagini 14 quando, nel corso della fase di acquisizione immagini P1, vengono acquisite le immagini.

Per evitare che questo rumore comprometta il funzionamento del sistema di autenticazione S (con evidenti problemi per la sicurezza), i mezzi di elaborazione 11 possono essere configurati per eseguire un insieme di istruzioni che implementa un algoritmo di codifica/decodifica polare (come ad esempio quello descritto da Mahdavifar et al. in "Achieving the secrecy capacity of wiretap channels using polar codes," *IEEE Transactions on Information Theory*, vol. 57, no. 10, pp. 6428–6443, Oct 2011) nel corso della fase di elaborazione P4.

In particolare, quando si devono cifrare dei dati riservati nel corso della fase di elaborazione P4, si codifica, mediante i mezzi di elaborazione 11, la stringa di dati riservati utilizzando una codifica polare, in modo da ottenere una stringa di dati riservati codificati, e si cifrano detti dati riservati codificati utilizzando l'impronta compressa W come chiave. Invece, quando è necessario decifrare dei dati riservati nel corso della fase di elaborazione P4, si decifrano detti dati riservati ottenendo dati riservati codificati, e si decodificano detti dati riservati codificati utilizzando una codifica polare.

Una codifica/decodifica polare consente di correggere le differenze (errori) che sono presenti tra la versione dei dati riservati prima della cifratura e la versione di detti dati riservati dopo la decifratura con un margine di probabilità che può essere provato, e che sono dovuti alle differenze che possono essere presenti tra l'impronta sensore compressa

utilizzata per cifrare i dati riservati e l'impronta sensore compressa utilizzata per decifrare detti dati riservati. Questo consente di autenticare un apparato d'utente 1 utilizzando poche immagini (anche una sola) con una probabilità superiore all'ottanta percento, mentre rende praticamente impossibile autenticare un altro apparato d'utente avente un sensore di immagini differente oppure utilizzare immagini pubblicamente disponibili scattate dallo stesso sensore e compresse con metodi a perdita di informazione (lossy), come ad esempio il JPEG o altro formato.

In questo modo, è possibile migliorare la sicurezza del sistema di autenticazione S.

Nelle corso della fase P2, l'impronta sensore (di registrazione e di autenticazione) è estratta eseguendo una insieme di istruzioni che implementano un algoritmo di regressione. Più nel dettaglio, l'uscita del sensore è preferibilmente modellata come di seguito:

$$\mathbf{o} = g^{\gamma} \cdot \left[(1+\mathbf{k}) \cdot \mathbf{i} + \mathbf{e}\right]^{\gamma} + \mathbf{q} \ , \qquad (1)$$

dove g^{γ} è la correzione di gamma (g è differente per ciascun canale di colore e γ è normalmente prossimo a 0.45), e modella le sorgenti di rumore interne al sensore, q modella il rumore esterno a detto sensore (ad esempio il rumore di quantizzazione), mentre k modella l'impronta sensore (una matrice delle dimensioni delle immagini prodotte dal sensore di immagini 14) che si vuole estrarre, i è l'intensità della luce che colpisce il sensore. Al fine di estrarre k, la formula (1) può essere approssimata al primo termine della serie di Taylor:

$$\mathbf{o} = \mathbf{o}^{\mathrm{id}} + \mathbf{o}^{\mathrm{id}} \cdot \mathbf{k} + \tilde{\mathbf{e}} \qquad (2)$$

dove $o^{\mathrm{id}} = (\mathrm{gi})^{\gamma}$ è l'output ideale del sensore di immagini, $o^{\mathrm{id}} \cdot k$ è la risposta fotografica non uniforme (photo-response non-uniformity - PRNU) del sensore di immagini di cui si vuole

estrarre l'impronta k, ed $\tilde{e} = \gamma o^{\mathrm{id}} \cdot e/i + q$ raggruppa tutte le altre sorgenti di rumore.

Assumendo che è possibile produrre una versione senza rumore o^{dn} mediante un opportuno processo di filtraggio e che tale versione senza rumore può essere utilizzata al posto dell'output ideale o^{id}, allora è possibile scrivere

$$\mathbf{w} = \mathbf{o} - \mathbf{o}^{\mathsf{dn}} = \mathbf{o} \cdot \mathbf{k} + \tilde{\mathbf{q}} \tag{3}$$

dove q raggruppa tutti gli errori del modello. Supponendo che un numero di immagini $C \geq 1$ è disponibile e considerando $\tilde{q}$ come un rumore Gaussiano indipendente dal segnale $o \cdot k$ e avente media zero e varianza σ^2, è possibile scrivere per ciascuna immagine $\ell, \ell = 1, \ldots, C$ la seguente relazione:

$$\mathbf{w}^{(\ell)}/\mathbf{o}^{(\ell)} = \mathbf{k} + \tilde{\mathbf{q}}/\mathbf{o}^{(\ell)} \ , \quad \text{dove} \quad \mathbf{w}^{(\ell)} = \mathbf{o}^{(\ell)} - \mathbf{o}^{(\ell)\mathsf{dn}} \tag{4}$$

Pertanto, la stima di k, ossia la stima di massima verosimiglianza $\hat{k}$ (maximum likelihood estimate), può essere ottenuta come

$$\hat{\mathbf{k}} = \sum_{\ell=1}^{C} \left(\mathbf{w}^{(\ell)} \cdot \mathbf{o}^{(\ell)} \right) \Bigg/ \sum_{\ell=1}^{C} (\mathbf{o}^{(\ell)})^2 \tag{5}$$

E la varianza di questa stima è data da

$$\sigma_{\hat{\mathbf{k}}}^2 = \sigma^2 \Bigg/ \sum_{\ell=1}^{C} (\mathbf{o}^{(\ell)})^2 \tag{6}$$

dalla quale è possibile notare che le immagini dalle quali si riescono ad estrarre le migliori impronte sensore sono le immagini aventi elevata luminanza (ma non sature) e contenuto regolare (in modo da abbassare la varianza σ^2 del rumore $\tilde{q}$). Per migliorare ulteriormente la qualità della stima $\hat{k}$, gli

artefatti in comune tra i sensori di immagini della stessa marca e/o modello possono essere rimossi sottraendo i valori medi delle righe e delle colonne ai valori della stima $\hat{k}$.

In caso le immagini acquisite dal sensore di immagini 14 siano a colori, la stima deve essere effettuate separatamente per ciascun canale di colore (rosso, verde, blu), cioè si devono ottenere una stima di massima verosimiglianza per ciascun canale, ossia $\hat{k}_R$ per il canale del rosso, $\hat{k}_G$ per il canale del verde, e $\hat{k}_B$ per il canale del blu. Dopodiché, un'impronta "globale" può essere ottenuta applicando una qualunque conversione da RGB a scala di grigi, come ad esempio quella di seguito riportata:

$$\hat{\mathrm{k}} = 0.3\hat{\mathrm{k}}_{\mathrm{R}} + 0.6\hat{\mathrm{k}}_{\mathrm{G}} + 0.1\hat{\mathrm{k}}_{\mathrm{B}} \qquad (7)$$

È comunque possibile per il tecnico del ramo utilizzare un algoritmo di regressione differente da quello appena sopra descritto, senza comunque allontanarsi dagli insegnamenti della presente invenzione.

Al fine di migliorare ulteriormente la qualità delle impronte sensore estratte nel corso della fase di calcolo impronta P2, ciascuna delle immagini, che viene acquisita mediante il sensore di immagini 14, può essere filtrata mediante un filtro di Wiener atto a rimuovere tutti gli artefatti periodici, prima che le impronte sensore vengano estratte (calcolate). In altre parole, i mezzi di elaborazione e controllo dell'apparato d'utente 1 possono anche essere configurati per eseguire, all'inizio della fase di calcolo impronta P2, un insieme di istruzioni che applica l'algoritmo di filtraggio di Wiener alle immagini acquisite nel corso della fase di acquisizione immagini P1 prima che l'impronta sensore di autenticazione sia generata, in modo da rimuovere tutti gli artefatti periodici da dette immagini. In questo

modo, si migliora la capacità del sistema S di distinguere tra due impronte provenienti da due sensori di immagini distinti, aumentando così il livello di sicurezza del sistema di autenticazione S.

In combinazione o in alternativa a quanto sopra descritto, nel corso della fase di compressione P3 è anche possibile effettuare una selezione delle parti dell'impronta (calcolata nel corso della fase di calcolo impronta P2) che hanno una frequenza spaziale (orizzontale e/o verticale) superiore ad un valore di soglia.

In particolare, durante la fase di compressione P3, i mezzi di elaborazione e controllo dell'apparato d'utente 1 sono configurati per eseguire i seguenti passi:

- trasformare l'impronta calcolata nel corso della fase P2 in un dominio trasformato, in modo da ottenere un'impronta trasformata; ad esempio eseguendo un insieme di istruzioni che implementa un algoritmo di trasformazione, come la trasformata discreta del coseno (Discrete Cosine Transform - DCT) oppure la trasformata veloce di Fourier bidimensionale (2D Fast Fourier Transform - 2D FFT), o altro;
- selezionare i punti dell'impronta trasformata che hanno una frequenza spaziale orizzontale e/o verticale superiore ad un valore di soglia prestabilito;
- antitrasformare detti punti dell'impronta trasformata selezionati, ad esempio eseguendo un insieme di istruzioni che implementa un algoritmo di antitrasformazione, come la trasformata discreta del coseno inversa (Inverse Discrete Cosine Transform - DCT) oppure la trasformata veloce di Fourier inversa bidimensionale (2D Inverse Fast Fourier Transform - 2D IFFT), o altro.

Così facendo si ottiene un'impronta sensore (di registrazione e di autenticazione) contenente solamente le

componenti di "elevata" frequenza. Questo diventa particolarmente vantaggioso quando queste componenti frequenziali sono superiori alle frequenze massime che sono contenute nelle immagini compresse utilizzando i formati di compressione di largo impiego (come ad esempio il JPEG o altro) e che vengono spesso utilizzati per pubblicare dei contenuti autoprodotti su Internet. In questo modo, si rende impossibile generare un'impronta sensore di autenticazione valida partendo da un insieme di immagini che sono state scattate da uno stesso terminale utente e che sono state poi pubblicate su Internet (ed essendo anche a conoscenza del seme utilizzato dall'algoritmo di proiezioni casuali), poiché le componenti frequenziali dell'impronta che vengono utilizzate dal sistema S per autenticare l'apparato d'utente 1 non sono presenti nelle immagini compresse, aumentando così il livello di sicurezza del sistema di autenticazione S.

In combinazione o in alternativa a quanto sopra descritto, l'apparato d'utente 1 può comprendere mezzi di ostruzione (come ad esempio un tappo, un'aletta traslabile o altro) che, se azionati dall'utilizzatore di detto apparato d'utente 1, possono impedire che il sensore di immagini 14 possa essere illuminato, ossia che la luce raggiunga il sensore di immagini 14. Questo permette di impedire che i mezzi di elaborazione 11 generino (nel corso della fase P2) un'impronta sensore valida, poiché nel corso della fase di acquisizione immagini P1, l'assenza di luce impedisce di acquisire delle immagini con un'entropia sufficiente a permettere l'estrazione dell'impronta del sensore di immagini 14.

In questo modo, si aumenta la sicurezza del sistema di autenticazione S impedendo (fisicamente) che un attaccante riesca a generare un'impronta valida per decifrare i dati riservati anche prendendo (da remoto) il controllo dell'apparato d'utente 1.

In una variante dell'invenzione sopra descritta, un sensore di immagini simile a quello della forma esecutiva preferita comprende mezzi di elaborazione (come ad esempio una CPU, un microcontrollore o altro) configurati per eseguire le fasi del metodo secondo l'invenzione.

In questo modo, si aumenta la sicurezza del sistema di autenticazione S, poiché si semplifica l'integrazione del metodo secondo l'invenzione in apparati d'utente già esistenti o in progetti di apparati d'utente già completati (ad esempio mediante la sostituzione del sensore di immagini o la sua riprogrammazione).

Alcune delle possibili varianti sono state descritte sopra, ma è chiaro al tecnico del ramo che, nell'attuazione pratica, esistono anche altre forme di realizzazione, con diversi elementi che possono essere sostituiti da altri tecnicamente equivalenti. La presente invenzione non è dunque limitata agli esempi illustrativi descritti, ma è suscettibile di varie modifiche, perfezionamenti, sostituzioni di parti e di elementi equivalenti senza comportare scostamenti dall'idea inventiva di base, come specificato nelle seguenti rivendicazioni.

RIVENDICAZIONI

1. Metodo per la protezione di dati riservati,

caratterizzato dal fatto di comprendere

- una fase di acquisizione immagini (P1), in cui una pluralità di immagini vengono acquisite mediante un sensore di immagini (14),
- una fase di calcolo impronta (P2), in cui un'impronta sensore è generata, mediante mezzi di elaborazione (11), sulla base di detta pluralità di immagini acquisita nel corso della fase di acquisizione immagini (P1),
- una fase di compressione (P3), in cui almeno una porzione di detta impronta sensore di codifica viene codificata, mediante detti mezzi di elaborazione (11), utilizzando un algoritmo di proiezioni casuali, in modo da generare un'impronta compressa (W),
- una fase di elaborazione (P4), in cui si cifrano e/o decifrano detti dati riservati utilizzando detta impronta compressa (W) come chiave.

2. Metodo secondo la rivendicazione 1, in cui, nel corso della fase di elaborazione (P4), si cifrano i dati riservati, dove detto metodo comprende anche

- una fase di generazione casuale, in cui si genera, mediante detti mezzi di elaborazione (11), una stringa casuale di bit,

e dove nel corso della fase di compressione (P3), detto algoritmo di proiezioni casuali genera un insieme di proiezioni casuali sulla base di detta stringa casuale di bit.

3. Metodo secondo le rivendicazioni 1 o 2, in cui nel corso della fase di elaborazione (P4) si decifrano i dati riservati, dove detto metodo comprende anche

- una fase di lettura stringa casuale, in cui si legge, mediante detti mezzi di elaborazione (11), una stringa casuale di bit memorizzata in mezzi di memoria (12,13),

e dove nel corso della fase di compressione (P3), i mezzi di elaborazione (11) generano un insieme di proiezioni casuali sulla base di detta stringa casuale di bit.

4. Metodo secondo una qualunque delle rivendicazioni da 1 a 3, in cui, nel corso della fase di elaborazione (P4), si codifica, mediante detti mezzi di elaborazione (11), la stringa di dati riservati utilizzando una codifica polare, in modo da ottenere una stringa di dati riservati codificati, e si cifrano detti dati riservati codificati utilizzando detta impronta compressa (W) come chiave.

5. Metodo secondo una qualunque delle rivendicazioni da 1 e 4, in cui nel corso della fase di elaborazione, si decifrano detti dati riservati ottenendo dati riservati codificati, e si decodificano detti dati riservati codificati utilizzando una codifica polare.

6. Metodo secondo una qualunque delle rivendicazioni da 1 a 5, in cui, nel corso della fase di compressione (P3), detta almeno una porzione di detta impronta sensore viene codificata utilizzando un algoritmo di proiezioni casuali, generando una impronta sensore codificata, e dove detta impronta sensore codificata viene quantizzata mediante i mezzi di elaborazione (11), generando detta impronta compressa (W).

7. Metodo secondo una qualunque delle rivendicazioni da 1 a 6, in cui, nel corso della fase di compressione (P3), si eseguono, mediante i mezzi di elaborazione (11), i passi di

- trasformare in un dominio trasformato l'impronta sensore generata nel corso della fase di calcolo impronta (P2), in modo da ottenere un'impronta trasformata,
- selezionare i punti dell'impronta trasformata che hanno una frequenza spaziale orizzontale e/o verticale superiore ad un valore di soglia, e
- antitrasformare detti punti dell'impronta trasformata selezionati.

8. Metodo secondo una qualunque delle rivendicazioni da 1 a 7, in cui nel corso della una fase di calcolo impronta (P2) viene eseguito un insieme di istruzioni che, prima che l'impronta sensore sia generata, applica l'algoritmo di filtraggio di Wiener a ciascuna immagine acquisita nel corso della fase di acquisizione immagini (P1), in modo da rimuovere tutti gli artefatti periodici da detta pluralità di immagini.

9. Metodo secondo una qualunque delle rivendicazioni da 1 a 8, in cui i dati riservati comprendono una chiave privata.

10. Apparato d'utente (1) per la protezione di dati riservati, comprendente

- un sensore di immagini (14) atto ad acquisire immagini,
- mezzi di elaborazione (11) in comunicazione con detto sensore di immagini (14),

caratterizzato dal fatto che

i mezzi di elaborazione (11) sono anche configurati per

- acquisire una pluralità di immagini mediante detto sensore di immagini (14),
- generare un'impronta sensore sulla base di detta pluralità di immagini,
- codificare almeno una porzione di detta impronta sensore utilizzando un algoritmo di proiezioni casuali, in modo da generare un'impronta compressa (W),
- cifrare e/o decifrare detti dati riservati utilizzando detta impronta compressa (W) come chiave.

11. Apparato d'utente (1) comprendente mezzi di ostruzione atti ad impedire che il sensore di immagini (14) possa essere illuminato.

12. Sensore di immagini per apparato d'utente,

caratterizzato dal fatto di comprendere

mezzi di elaborazione configurati per eseguire le fasi del metodo secondo una qualsiasi delle rivendicazioni da 1 a 9.

13. Prodotto informatico (computer program product)

caricabile nella memoria di un elaboratore elettronico e comprendente porzione di codice software per attuare le fasi del metodo secondo una qualsiasi delle rivendicazioni da 1 a 9.

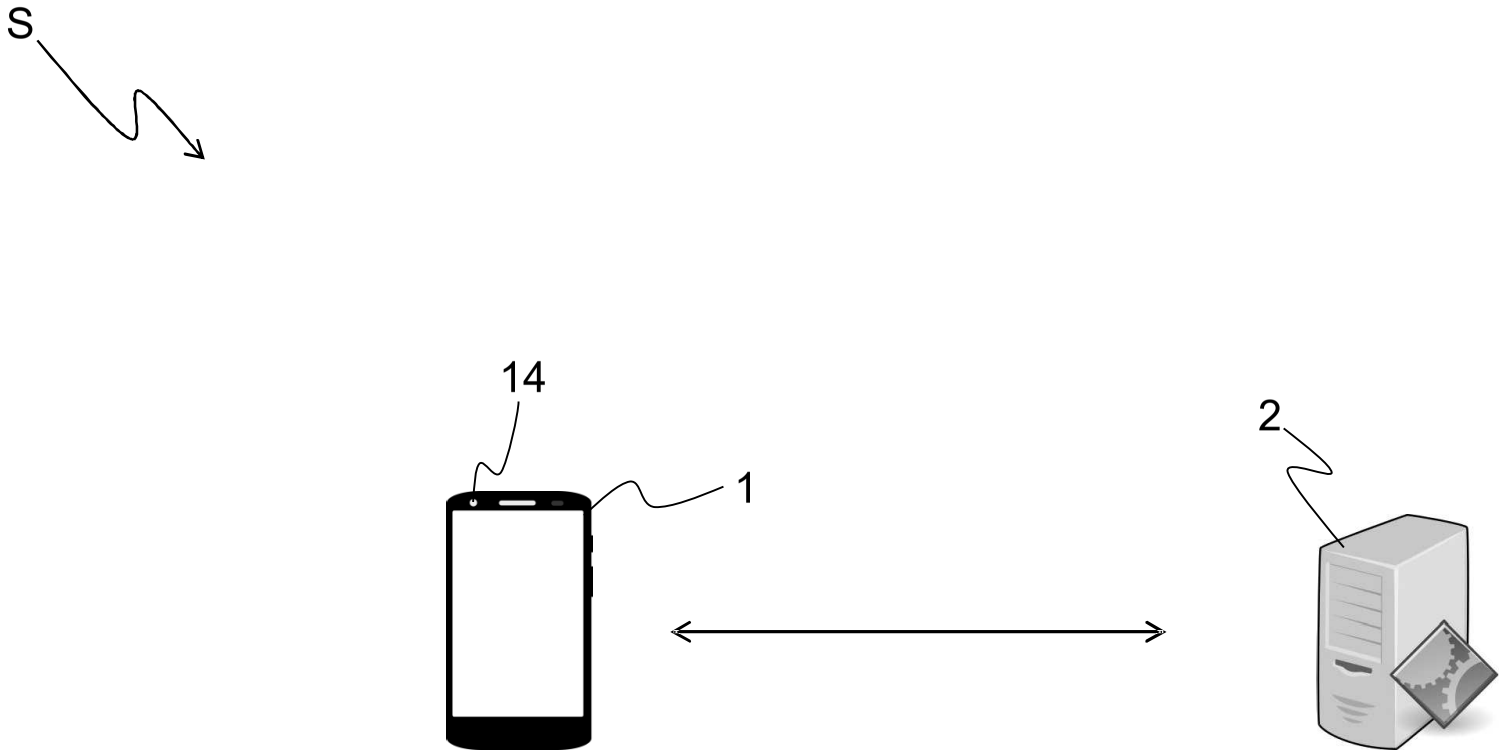

Fig. 1

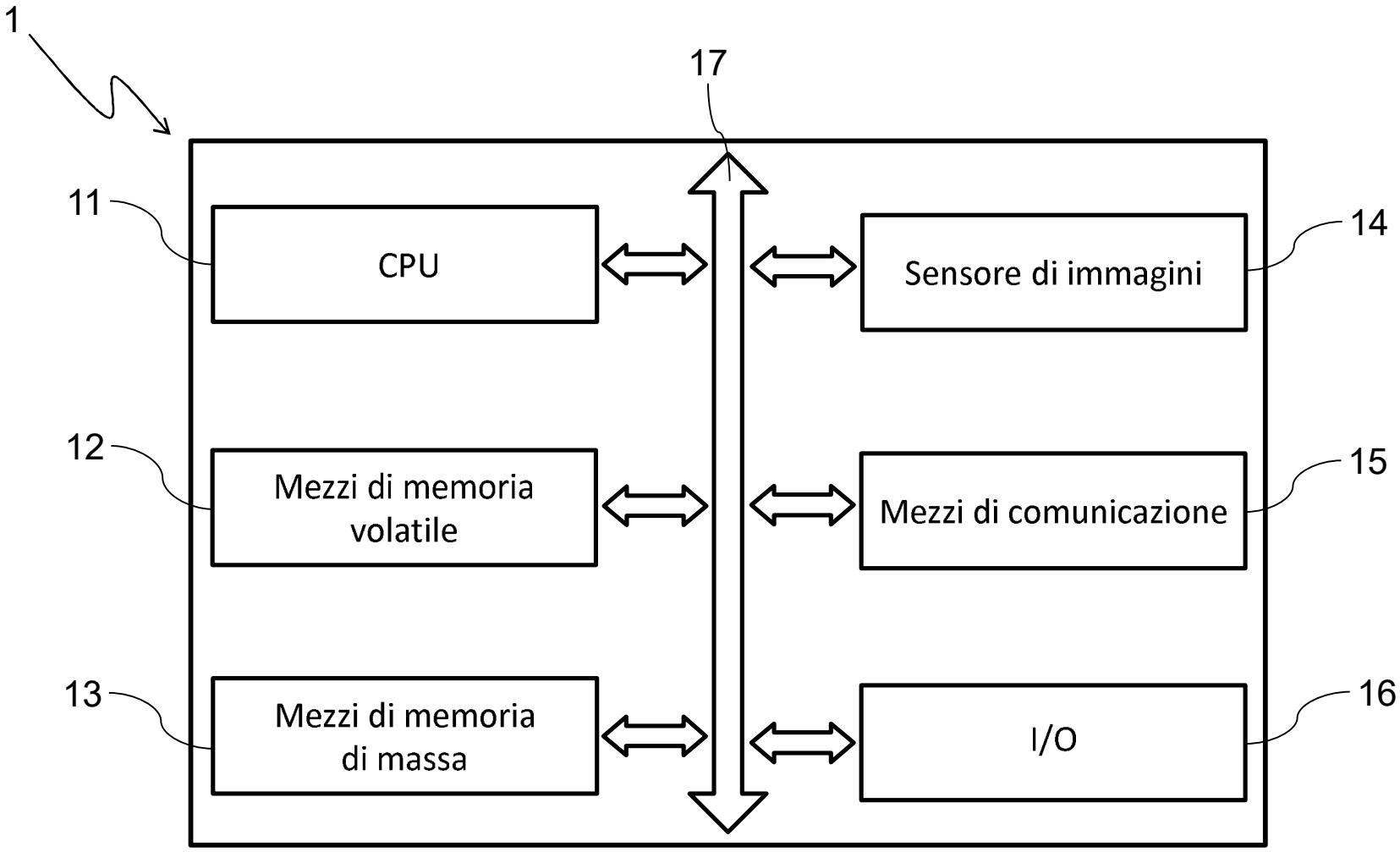
1
17
11
CPU
14
Sensore di immagini
12
Mezzi di memoria volatile
15
Mezzi di comunicazione
13
Mezzi di memoria di massa
16
I/O

Fig. 2

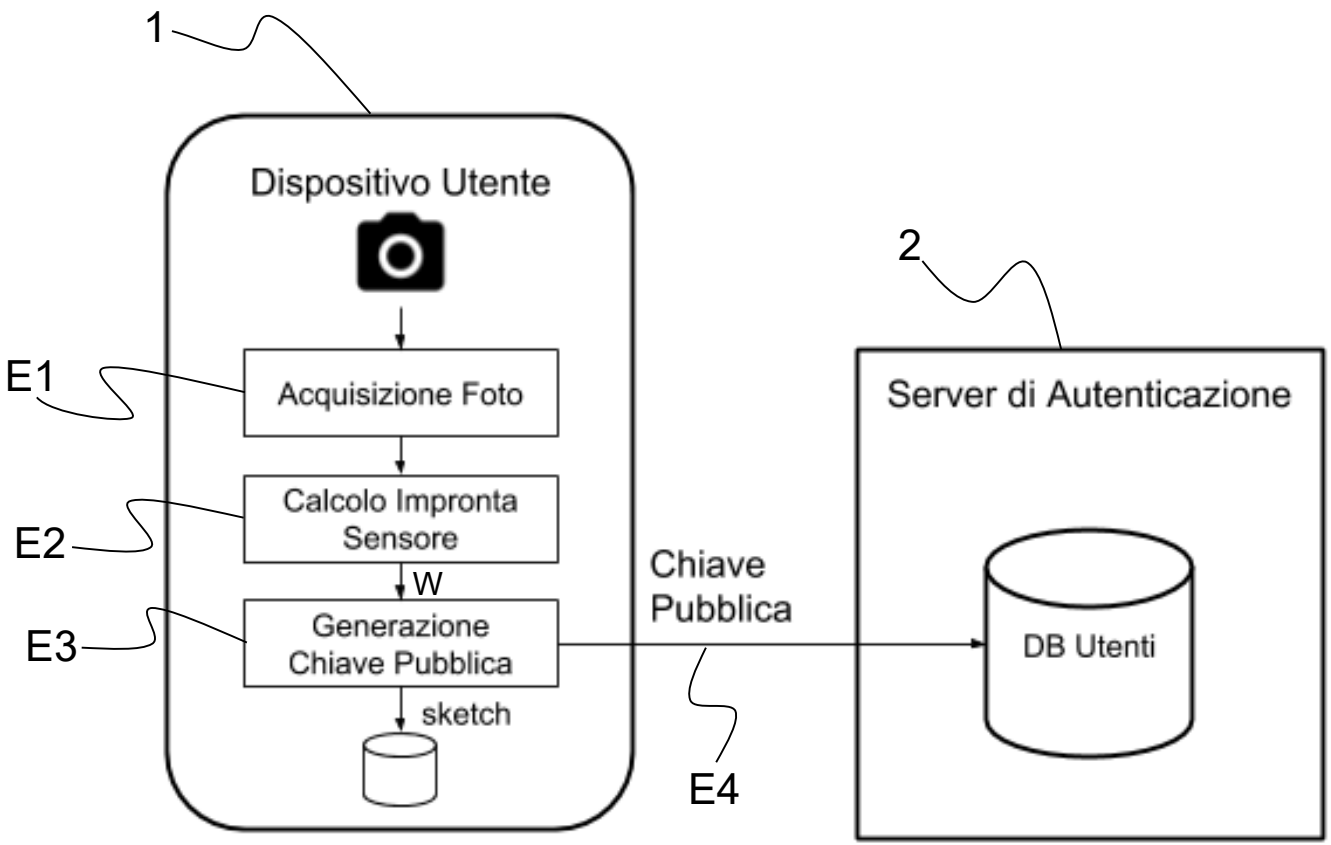
1
Dispositivo Utente
2
Server di Autenticazione
E1
Acquisizione Foto
E2
Calcolo Impronta Sensore
W
E3
Generazione Chiave Pubblica
sketch
Chiave Pubblica
E4
DB Utenti

Fig. 3

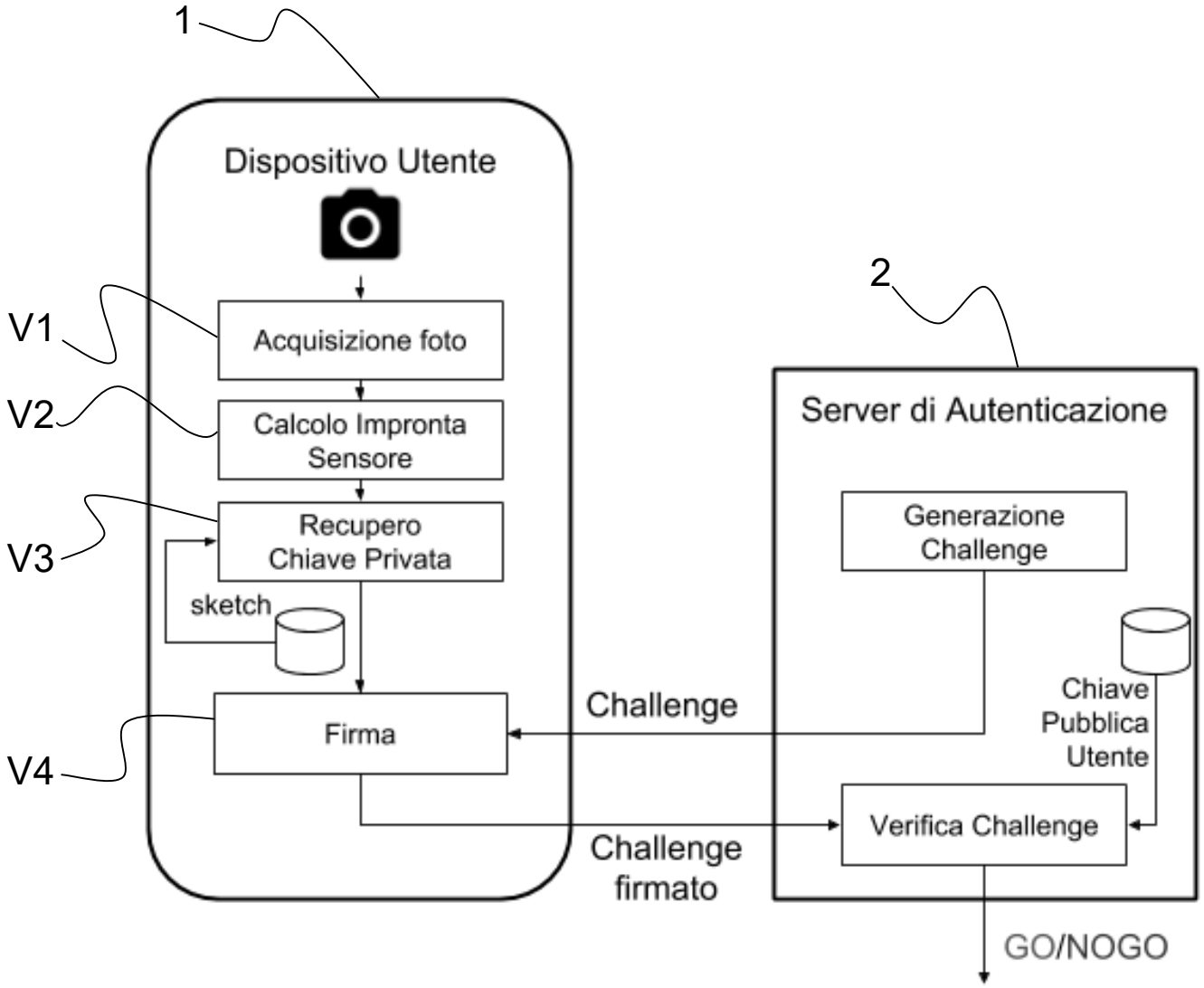
1
Dispositivo Utente
V1
Acquisizione foto
V2
Calcolo Impronta Sensore
V3
Recupero Chiave Privata
sketch
V4
Firma
2
Server di Autenticazione
Generazione Challenge
Chiave Pubblica Utente
Verifica Challenge
Challenge
Challenge firmato
GO/NOGO

Fig. 4

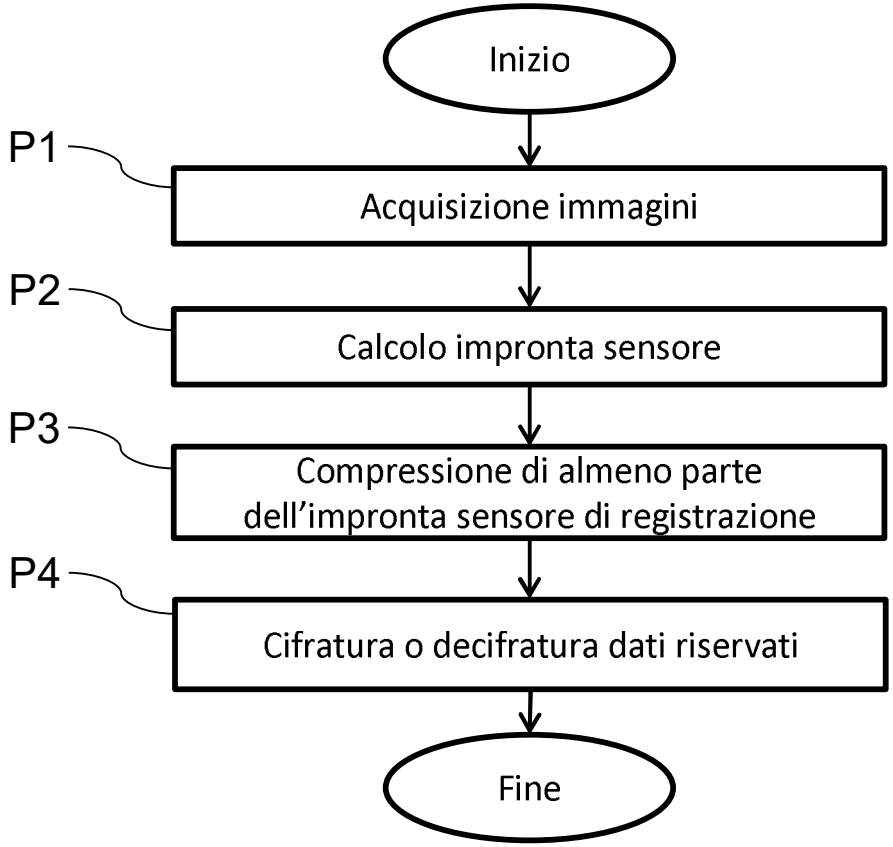
Inizio
P1
Acquisizione immagini
P2
Calcolo impronta sensore
P3
Compressione di almeno parte dell'impronta sensore di registrazione
P4
Cifratura o decifratura dati riservati
Fine

Fig. 5

Ministero dello Sviluppo Economico

Direzione generale per la tutela della proprietà industriale

Ufficio Italiano Brevetti e Marchi

ATTESTATO DI BREVETTO PER INVENZIONE INDUSTRIALE

Il presente brevetto viene concesso per l'invenzione oggetto della domanda:

N. 102019000007290

TITOLARE/I:	• TOOTHPIC S.r.l. 50.0% • POLITECNICO DI TORINO 50.0%
	Ferroni Filippo
DOMICILIO:	Metroconsult Genova S.r.l. via Palestro 5/6 16122 Genova
INVENTORE/I:	• MAGLI Enrico • COLUCCIA Giulio • VALSESIA Diego • BIANCHI Tiziano
TITOLO:	Apparato d'utente e metodo di protezione di dati riservati
CLASSIFICA:	H04L
DATA DEPOSITO:	27/05/2019

Roma, 25/06/2021

Il Dirigente della Divisione VII
Loredana Guglielmetti

Via Molise 19 - 00187 Roma
tel. +39 06 4705 5800 - e-mail contactcenteruibm@mise.gov.it - www.mise.gov.it