DOI: 10.26314/GARR-Conf18-proceedings-23

Interoperabilità e accesso a dati e servizi: sistema di protezione di documenti elettronici mediante accesso biometrico

Pierluigi Tuveri, Marco Micheletto, Giulia Orrù, Luca Ghiani, Gian Luca Marcialis

Università degli studi di Cagliari, Dipartimento di Ingegneria Elettrica ed Elettronica

Abstract. Al giorno d'oggi, milioni di documenti attraversano ogni secondo le reti di telecomunicazione. In questo contesto la protezione dei dati e in particolare la crittografia rappresenta uno strumento fondamentale per la difesa di informazioni sensibili e/o personali.In questo articolo verrà presentato un prototipo di sistema di protezione di documenti digitali basato sull'utilizzo di tecniche crittografiche tradizionali rafforzate da un sistema di verifica personale biometrica. Il prototipo è stato sviluppato nell'ambito del progetto "Protezione di documenti elettronici mediante accesso biometrico", finanziato dalla Regione Lombardia tramite il bando InnoDriver3 per attività di trasferimento tecnologico con l'azienda CSAMed-Net4Market srl.

Keywords. impronte digitali, biometria, autenticazione

Introduzione

Oggigiorno, gran parte della popolazione mondiale ha accesso a Internet e miliardi di informazioni sensibili o personali sono quotidianamente esposte al rischio di essere intercettate, manipolate, divulgate o utilizzate per scopi diversi da quelli per cui sono state concepite. Se consideriamo anche tutte le informazioni memorizzate localmente che necessitano anch'esse di essere preservate con un certo grado di riservatezza, abbiamo un quadro chiaro di quanto sia importante e necessario sviluppare algoritmi sofisticati in grado di garantire un elevato livello di sicurezza dei dati.

Negli ultimi decenni, numerose ricerche si sono basate sullo studio dell'interazione tra crittografia e biometria, due tecnologie di sicurezza potenzialmente complementari. La crittografia è la scienza che si occupa di trovare metodi e algoritmi per rendere dei simboli o del testo, in un primo momento chiari e leggibili, del tutto incomprensibili a chiunque non fosse a conoscenza dei procedimenti utilizzati per codificarli (Stallings 2006). Attualmente gli algoritmi di criptaggio, basano l'identificazione della persona che deve accedere alla risorsa criptata, sui classici paradigmi basati su "qualcosa che si possiede" come smart card, o su "qualcosa che si conosce", come pin o password. Questi metodi hanno però il grande svantaggio di essere facili da violare in quanto una smart card può essere rubata o smarrita, pin o password dimenticati.Per questo motivo negli ultimi anni si sta sempre più diffondendo il paradigma che permette di riconoscere un individuo sulla basa di "ciò che si è", utilizzando quindi parametri biometrici, come le impronte digitali o il volto. La

Cagliari, 3-5 ottobre 2018 - ISBN: 978-88-905077-8-6

biometria, infatti, è la scienza che studia e analizza i metodi per riconoscere in maniera univoca l'identità di un individuo sulla base delle sue caratteristiche fisiche o comportamentali (Jain et al. 2007). L'uso di metodi di autenticazione biometrica in sistemi di protezione dei dati tramite crittografia aumenta considerevolmente il livello di sicurezza sfruttando i vantaggi dei tratti biometrici, che non possono essere dimenticati, rubati o persi. In questo articolo presentiamo un prototipo di sistema di protezione di documenti elettronici mediante accesso biometrico, in particolare tramite l'utilizzo dell'impronta digitale. Il progetto è nato dalla collaborazione tra il Dipartimento di Ingegneria Elettrica ed Elettronica dell'Università di Cagliari e l'azienda Net4Market-CSAMed s.r.l.. Il suo scopo è quello di indagare la possibilità di sfruttare la tecnologia relativa ai tratti biometrici, nello specifico relativa alle impronte digitali, per incrementare il livello di protezione nei documenti elettronici dato dal semplice utilizzo di metodi crittografici. Il prototipo è stato sviluppato nell'ambito del progetto "Protezione di documenti elettronici mediante accesso biometrico", finanziato dalla Regione Lombardia tramite il bando InnoDriver3.

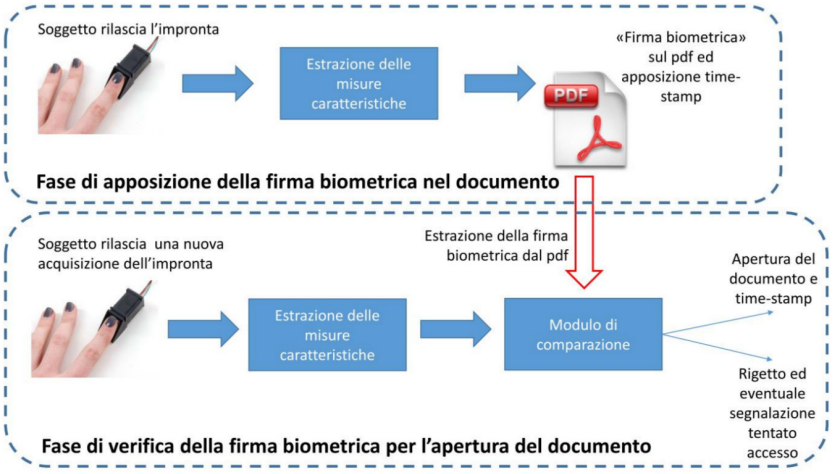


Fig. 1
Fasi funzionali del sistema di protezione di file pdf mediante accesso tramite impronta digitale

1. Il prototipo

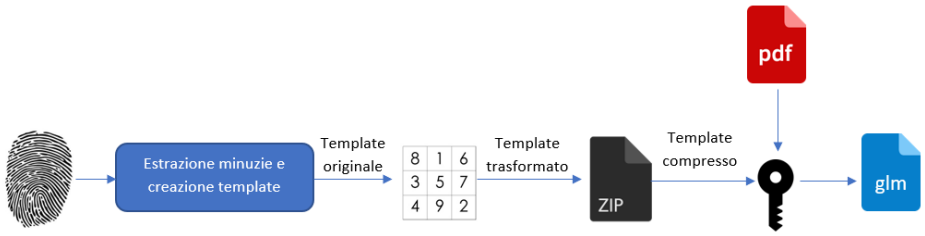
Il sistema realizzato (Figura 1) utilizza congiuntamente un tratto biometrico, in particolare l'impronta digitale, e un metodo di sicurezza tradizionale, la password, per proteggere un documento elettronico. Usando questa due informazioni il sistema è in grado di criptare il file e di salvarlo in un altro formato con estensione proprietaria (.glm). In questo modo il nuovo file risulta illeggibile e può essere decriptato solo dalla stessa persona che l'ha criptato, cioè da chi conosce la password e possiede l'impronta digitale. In particolare, il sistema schematizzato in Figura 2 è suddiviso in tre moduli:

- modulo di estrazione delle minuzie, ossia le caratteristiche distintive dell'impronta digitale;
- modulo di protezione del template, necessario al fine di garantire la privatezza e la rinnovabilità della biometria;
- modulo di criptaggio, all'interno del quale vengono criptati sia il template che il file.

Nel modulo di estrazione delle minuzie, l'applicazione acquisisce l'impronta digitale e e-

strae i punti salienti (biforcazioni, termini, uncini, laghi, isole delle creste papillari). L'insieme delle coordinate e degli angoli di allineamento delle minuzie costituiscono il template dell'impronta digitale.

Fig. 2
Schema di funzionamento del prototipo



Il template descrive in maniera puntuale un'impronta digitale e poiché da esso è possibile ricreare l'impronta digitale da cui è stato estratto (Cao, Jain 2015) , esso deve essere protetto. Come primo passo del modulo di protezione del template viene applicata una trasformazione cartesiana al template che permette di modificare la posizione delle minuzie (Nalini et al. 2007). Per implementare la trasformazione si utilizza una matrice che cambia periodicamente (aggiornando di conseguenza i file coinvolti), come si può vedere nella Figura 3. Il template trasformato viene successivamente compresso e inserito all'interno del file pdf.

Il documento risultante viene a questo punto criptato ed esportato in formato (.glm). Alcuni dettagli delle procedure adottate non possono essere inseriti per via dell'accordo di riservatezza vigente tra il DIEE e l'azienda. Per poter accedere al file è necessario conoscere la password e superare il sistema di verifica biometrica.
Infatti, l'inserimento della password permette di decriptare ed estrarre il template trasformato.

Il template ottenuto verrà quindi decompresso e verrà applicata la trasformazione inversa tramite la stessa matrice utilizzata in fase di criptaggio ottenendo il template relativo all'impronta digitale memorizzata.

L'accesso effettivo al pdf sarà consentito solo in caso di corrispondenza (matching) tra l'impronta digitale memorizzata e quella in input al sistema.

Fig. 3
L'impronta a sinistra riporta le minuzie trovate, al centro la matrice M che permette di trasformare le minuzie, a destra le minuzie trasformate sovrapposte all'immagine originale. Come si può vedere le minuzie trasformate sono scorrelate dall'impronta.

Nel caso preso in considerazione il matching è basato sulle minuzie (Maltoni et al. 2009): le minuzie estratte dalle immagini da confrontare sotto forma di coordinate di un punto sul piano e di orientamento corrispondente.

In questo tipo di matching si cerca di raggiungere il migliore allineamento tra le due immagini in modo da ottenere una corrispondenza tra il maggior numero possibile di minuzie. Per compensare le variazioni causate del rumore e della distorsione è definita una regione di tolleranza attorno alla posizione di ogni minuzia.

2. Conclusioni

Il prototipo sviluppato nell'ambito del progetto "Protezione di documenti elettronici mediante accesso biometrico", finanziato dalla Regione Lombardia tramite il bando Inno-Driver3 per attività di trasferimento tecnologico con l'azienda CSAMed-Net4Market srl, utilizza un sistema di verifica biometrica tramite impronta digitale per proteggere ulteriormente un file pdf criptato tramite password.

Un futuro miglioramento del prototipo presentato si baserà sull'eliminazione della necessità di richiedere una password per accedere al documento, utilizzando il tratto biometrico stesso come chiave di criptaggio.

Riferimenti bibliografici

Cao K. and Jain A. K., (January 2015), Learning Fingerprint Reconstruction: From Minutiae to Image, EEE Trans. on Information Forensics and Security, vol.10, no.1, pp.104-117.

Jain A. K., Flynn P., Ross A. A., (2007), Handbook of biometrics. Springer Science & Business Media.

Maltoni D., Maio D., Jain A. K., Prabhakar S., (2009), Handbook of fingerprint recognition. Springer Science & Business Media.

Nalini K. R, Sharat C., Jonathan H. Connell, and R. M. Bolle, (April 2007), Generating Cancelable Fingerprint Templates. IEEE Trans. PAMI 29, 4 , pp 561-572.

Stallings W, (2006). Cryptography and Network Security, 4/E. Pearson Education India.

Autori

Pierluigi Tuveri - pierluigi.tuveri@diee.unica.it
Pierluigi Tuveri si è laureato nel marzo del 2014 in ingegneria elettronica presso l'Università degli Studi di Cagliari discutendo la tesi dal titolo "A user-specific approach to fingerprint liveness detecton". Dal marzo 2014 collabora con il PRA Lab, su tematiche biometriche come sviluppatore software.

Marco Micheletto - michelettomarco@gmail.com
Ha conseguito la laurea in Ingegneria Biomedica nel luglio 2017 presso l'università degli Studi di Cagliari discutendo la tesi intitolata: "Riconoscimento personale mediante le vene del palmo". Attualmente laureando in ingegneria elettronica, collabora col PRA Lab su tematiche inerenti le impronte digitali.

Giulia Orrù - giulia.orru@diee.unica.it
Dottoranda in Ingegneria Elettronica e Informatica dell'Università di Cagliari, dal 2014 collabora

con il PRA Lab nell'ambito del riconoscimento di volti, fingerprint liveness detection e sistemi biometrici adattivi.

Luca Ghiani - luca.ghiani@diee.unica.it
Luca Ghiani si è laureato nel Dicembre del 2011 in Ingegneria Elettronica con votazione 110/110 presso l'Università degli studi di Cagliari, discutendo una tesi dal titolo "Multimodal Fingerprint Liveness Detection by Local Phase Quantization and Wavelet Transforms".
Da Marzo 2012 collabora col PRA Lab, prima come dottorando di ricerca, attualmente come ricercatore post-doc.

Gian Luca Marcialis - marcialis@diee.unica.it
Dirige le attività relative alla Divisione "Biometria" del PRA Lab. Le sue attività di ricerca sono incentrate sulla biometria. Sulla base di queste attività è responsabile delle attività svolte in diversi progetti internazionali e nazionali (MAVEN, FP7 Tabula Rasa, PRIN su “Guardie biometriche”, RAS Legge 7 su “Sistemi biometrici adattativi”), commesse di aziende nazionali ed internazionali (Crossmatch, Greenbit, CSAMed) ed è organizzatore della “International Fingerprint Liveness Detection Competition” (LivDet) giunta alla sua sesta edizione.