

BIOMETRIC SYSTEM PERFORMANCE TESTING - FINGERPRINT TECHNOLOGY

Matej Šuta

Bachelor Degree Programme (3), FIT BUT

E-mail: xsutam00@stud.fit.vutbr.cz

Supervised by: Dana Lodrová

E-mail: ilodrova@fit.vutbr.cz

ABSTRACT

This document deals with several technologies currently used by fingerprint sensors. It is also aimed at testing spoof-resistance of sensors and their ability to be employed in many extreme situations such as humid environment. Couple of procedures are introduced and described to test these properties of fingerprint sensors.

1 ÚVOD

Nedávno sa v médiách objavil článok o tom, že kórejskí cestujúci boli schopní prejsť hranicami napriek tomu, že boli snímané ich odtlačky prstov. Preto vznikajú znepokojivé otázky týkajúce sa odolnosti biometrických senzorov voči útokom.

Testy odolnosti voči týmto útokom boli naposledy vykonané v roku 2002 (vid' práca L. Thalheimovej [2]). Od toho času však boli uvedené nové technológie. Zároveň vzrastajú požiadavky na bezpečnosť vo všeobecnosti. Preto je vhodné vykonať testy momentálne používaných snímačov odtlačkov prstov.

2 POUŽÍVANÉ TECHNOLOGIE

V súčasnosti sa v senzorech pre snímanie odtlačkov prstov používa niekoľko technológií. V nasledujúcej časti uvedieme princípy použité v senzorech, s ktorými sme pracovali v laboratóriu biometrických systémov na FIT VUT v Brne [1]:

- **FTIR** (*frustrated total internal reflection*). Známy aj ako optický senzor. Pri skenovaní sa prst dotýka skleneného hranola, na ktorý zospodu pod určitým uhlom dopadá svetlo emitované diódou. Reliéf bruška prstu zaisťuje to, že časť svetla je náhodne rozptýlená, prípadne pohltaná a časť svetla sa odrazí späť do CCD/CMOS obrazového snímača.
- **Multispektrálny** (*multispectral imaging*). Diódami emitované svetlo o rôznych vlnových dĺžkach preniká do rôznych úrovní kože prsta. Nasnímaním odrazených spektier získava senzor informácie o podpovrchových štruktúrach ako je hrúbka kože, jej morfológia, kapilárna hustota, úroveň okysličenia krvi a pod. Tento systém používa vo svojich senzorech firma Lumidigm.

- **Kapacitný** (*capacitive*). Senzor je realizovaný ako dvojrozmerné pole mikro-kondenzátorov zložených len z jednej platne. Druhá platňa je reprezentovaná pritlačeným prstom. Po pritlačení prsta na plochu senzora sa medzi týmito platňami tvoria malé elektrické náboje.
- **Termický** (*thermal*). V tomto prípade je senzor vytvorený z materiálu, ktorý generuje prúd pri zmene teploty. Pri kontakte prsta so senzorom produkujú vyvýšeniny povrchu prsta inú teplotu ako drážky. V prvej časti sa prst nahrieva, a následný teplotný rozdiel senzora a povrchu prsta vytvára obraz povrchu prsta.
- **Senzor s elektrickým poľom** (*e-field*). Senzor obsahuje okruh, ktorý generuje sínusový signál a maticu antén, ktoré prijímajú signál vyslaný týmto okruhom a upravený prechodom cez pokožku prsta. Prst sa musí súčasne dotýkať okruhu i matice.

3 NÁVRH TESTOV

V prvej kategórii sa snažíme uviesť biometrický systém do takého stavu, že systém prijme neoprávneného užívateľa pod falošnou identitou bez toho, aby o tom sám vedel. Takéto testy môžeme vykonať štyrmi rôznymi spôsobmi:

- **Živý prst – živý prst.** Ide o klasické porovnanie, keď je v systéme zaregistrovaný živý prst užívateľa a tým istým prstom sa užívateľ snaží verifikovať svoju identitu.
- **Umelý prst – živý prst.** V systéme je uložený obraz umelého prstu a užívateľ sa snaží verifikovať svojím živým prstom, z ktorého bol vytvorený umelý prst.
- **Živý prst – umelý prst.** Užívateľ použije na verifikáciu umelú repliku živého prsta, ktorý už je v systéme zaregistrovaný. Tento spôsob testovania je najdôležitejší z hľadiska narušenia bezpečnosti biometrického systému.
- **Umelý prst – umelý prst.** V tomto prípade sa užívateľ snaží o verifikáciu identity pomocou umelého prstu, ktorého obraz je už uložený v systéme. Tento test určuje schopnosť biometrického systému určiť živosť subjektu tak pri registrácii, ako aj pri verifikácii.

Pre získanie odtlačku prsta je potrebné zvoliť vhodný materiál pre formu – ako dobré alternatívy sa javia plastelína, vosk, sádra alebo tmel. Pre naše experimenty použijeme voskové formy, kvôli ich stálosti a jednoduchej manipulácii s nimi.

Na umelé repliky odtlačkov prstov môžeme použiť niektoré z nasledujúcich materiálov: plastelína, vosk, želatína, Durocast, latex, silikón, či lepidlo na drevo. V laboratóriu bolo už predtým pripravené gumené razítko so štruktúrou papilárnych línií.

V druhej kategórii sa snažíme uviesť biometrický systém do takého stavu, že systém neprijme oprávneného užívateľa, teda systém zlyhá pri porovnaní biometrických charakteristík zo vstupu so šablónou registrovanou v systéme. Tu môžeme zaradiť vplyvy nečistôt alebo prostredia na funkčnosť systému.

Ako nečistoty môžeme použiť napríklad kriedu, prach, masť i tuhu od pera. Je možné sledovať aj vplyv teplotných zmien alebo vplyv zmeny vlhkosti povrchu prsta. Najmä v systémoch s testovaním živosti bude zaujímavé sledovať vplyv fyzickej aktivity. Tieto faktory menia fyzikálne vlastnosti prsta (absorbciu resp. reflexiu žiarenia, vodivosť, teplotu, úroveň okysličenia krvi apod.) a preto môžeme dostať rôzne výsledky.

4 VÝSLEDKY PREDBEŽNÝCH TESTOV

Zatiaľ sme sa zamerali na prvú skupinu testov pre neoprávnený prístup. V týchto testoch zatiaľ nebudeme určovať úspešnosť pokusov. Vytvorili sme nasledujúce umelé repliky ukazováka a palca pravej ruky: želatínové prsty, voskové odtlačky, Durocastové odtlačky, odtlačky z plastelíny a gumené razítko. Testovali sme schopnosť načítať umelý odtlačok z daného materiálu senzorom. Výsledky môžeme zhrnúť do tabuľky 1.

| | FTIR | Multispektrálny | Kapacitný | Termický | E-field |
|------------|------|-----------------|-----------|----------|---------|
| Želatína | A | N | A | A | A |
| Vosk | N | N | N | A | N |
| Durocast | A | A | N | A | N |
| Plastelína | A | A | N | N | N |
| Guma | A | N* | A | A | N** |

Tabuľka 1: Schopnosť senzoru načítať umelý odtlačok, kde A – senzor je schopný načítať odtlačok a N – senzor nie je schopný načítať odtlačok.

Pri hodnote N* sa domnievame, že plocha gumeného razítka nebola dostatočne veľká na to, aby senzor úspešne načítal odtlačok. Naopak, v prípade N** malo zase razítko príliš veľkú plochu na to, aby sa celé zmestilo na plochu senzora s elektrickým poľom a preto nedošlo k vedeniu prúdu a načítaniu odtlačku. V prípade, že tieto predpoklady sú správne, sa javí gumené razítko zatiaľ ako najúspešnejší umelý materiál, jeho kladom je aj jednoduché použitie. Podobne, umelé odtlačky z Durocastu sa ukazujú ako celkom dobrá možnosť, ale neposkytujú dostatočne vodivé vlastnosti pre e-field a kapacitný senzor. Zaujímavé výsledky sú so želatínovými prstami, kde ich okrem multispektrálneho načítali všetky senzory, avšak kvalita výsledného obrazu je vždy nízka. Navyše, práca so želatínovými prstami nie je jednoduchá a ich trvanlivosť je približne dve hodiny až jeden deň. Umelé odtlačky z plastelíny sú schopné prekonať opticky založené senzory. Nevýhodou je ľahké poškodenie takýchto odtlačkov. Najmenej úspešné boli odtlačky z vosku.

5 ZÁVER

V nasledujúcej fáze tejto práce sa pokúsím o dôkladnejšie testovanie neoprávneného prístupu, pokúsím sa otestovať ďalšie materiály a určím presnejšie štatisticky dosiahnuté výsledky. Zároveň sa zamerám na testy neoprávneného zamietnutia, ktoré sa budem snažiť vykonať na dostatočnom množstve dobrovoľníkov.

REFERENCIE

- [1] Maltoni, D., Maio, D., Jain, A.K., Prabhakar, S.: Handbook of Fingerprint Recognition, Springer, 2003, ISBN 0-387-95431-7
- [2] Thalheim, L., Krissler, J., Ziegler, P.-M.: Body Check – Biometric Access Protection Devices and their Programs Put to the Test, c't 11/2002, s. 104 – Biometric