

SPÔSOBY PREKONANIA ELEKTRONICKÉHO SYSTÉMU KONTROLY VSTUPOV

Jakub Ďurica
Žilinská univerzita v Žiline
Univerzitná 8215/1, 010 26 Žilina, Slovenská republika
jakub.durica@fbi.uniza.sk

Abstract: This article focus on overcoming electronic access control system working on optical sensor which scanning fingerprint. The tests were accomplish by non - destructive method with use fake flat and bulky fingerprint. Results of tests were rate by false rejection rate – FRR, false acceptance rate – FAR and shown to ROC curve. Mechanical barrier devices as door, barriers are important part of electronic access control system, because they help perform their function, but mechanical barrier devices can be overcoming too.

Key words: *electronic access control system, mechanical barrier devices, testing*

Abstrakt: Článok sa zameriava na prekonanie elektronického systému kontroly vstupu, pracujúcim na optickom snímaní odtlačku prsta. Boli vykonané testy, nedeštruktúrnou metódou, za použitia falošných plošných i objemových odtlačkov. Výsledky testov boli hodnotené prostredníctvom pravdepodobnosti chybného odmietnutia - FRR, pravdepodobnosti chybného prijatia – FAR, a taktiež boli znázornené v ROC krivke. Dôležitou súčasťou elektronického systému kontroly vstupu sú mechanické zábranné prostriedky ako dvere, závary a pod., ktoré napomáhajú plniť elektronickým systémom kontroly vstupu ich základnú funkciu, ale takisto môžu byť prekonané.

Kľúčové slová: *elektronický systém kontroly vstupu, mechanicky zábranný systém, testovanie*

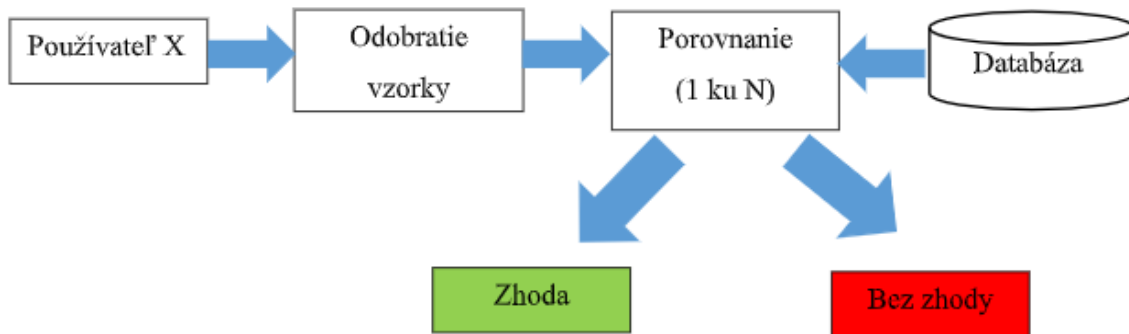
1 Úvod

Elektronické systémy kontroly vstupov patria k dôležitej súčasti celkovej bezpečnosti v organizácií, avšak bez mechanického zábranného prostriedku nedokážu plniť svoju základnú funkciu a to zabrániť vstupu alebo výstupu neoprávneným osobám a naopak oprávneným osobám umožniť vstup alebo výstup zo zabezpečeného priestoru. Práve mechanické zábranné prostriedky tvoria bariéru medzi zabezpečeným priestorom a priestorom s voľným pohybom [1]. Podobne elektronické systémy kontroly vstupov definuje Duarte, ktorý hovorí, že “kontrola vstupu za pomoci elektronického systému kontroly vstupu spočíva v priradení prístupových práv/údajov k používateľovi, čo umožňuje používateľovi prístup do zabezpečeného priestoru len v prípade, že má spravené prístupové práva/údaje” [2].

Elektronické kontroly vstupov sú rozdelené do 4 stupňov zabezpečenia. Pre prvý stupeň je definované nízke riziko, chránený záujem nízkej hodnoty a páchateľ, ktorý nemá znalosť o elektronických systémov kontroly vstupov. Druhý stupeň je definovaný nízkym až stredným rizikom, chránený záujem vyššej hodnoty a páchateľ má malé znalosti o ESKV a disponujú bežnými nástrojmi a presnými prístrojmi. Tretí stupeň je definovaný stredným až vysokým rizikom, chránený záujem má vysokú hodnotu a páchateľ disponuje znalosťami o ESKV, a má dostatočný počet nástroj a prenosných prístrojov. Štvrtý stupeň je definovaný vysokým rizikom, chránený záujem má vysokú hodnotu páchateľ má schopnosti, prostriedky a prenosné prístroje na napadnutie systému, vrátane prostriedkov pre nahradenie jednotlivých častí elektronického systému kontroly vstupov [3].

2 Možnosti identifikácie

Osoba, používateľ, ktorý sa chce dostať z/do zabezpečeného priestoru sa musí identifikovať, na základe identifikačných prostriedkov. Údaje z identifikačných prostriedkov sú načítané, porovnané s údajmi z databázy, a v prípade zhody je osobe umožnený prístup, v opačnom prípade zamietnutý [3].



Obrázok 1 Proces identifikácie [4].

Používateľ sa môže identifikovať na základe 3 prístup:

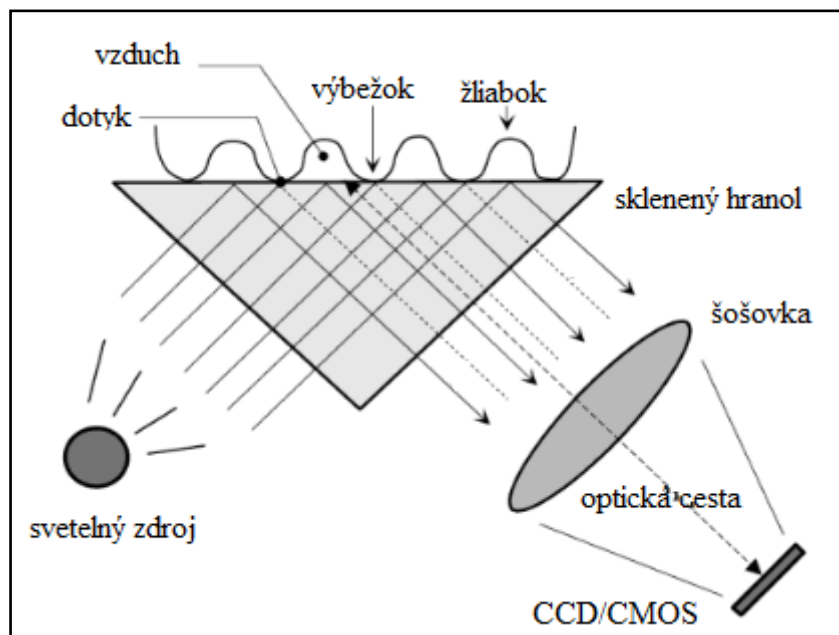
- dokázaním znalosti,
- dokázaním vlastníctva,
- dokázaním vlastnosti [5].

Pre potreby článku bol použitý prístup dokázaním vlastnosti, biometria, teda akékoľvek fyziologické charakteristiky alebo vlastností človeka, ktoré sa dajú použiť na overenie totožnosti jednotlivca [6]. Biometria je bezpečnejšia alternatíva ku klasickým identifikačným metódam elektronického systému kontroly vstupov [4].

Ako biometrickú identifikáciu je možné použiť viacero fyziologických charakteristík alebo vlastností človeka, ako napríklad rozpoznávanie odtlačkov prstov, rozpoznávanie očných vzorov, rozpoznávanie tváre, rozpoznávanie hlasových vzorov, rozpoznávanie žíl a ďalšie. Rozpoznávanie vzorov odtlačkov prstov však zostáva najpoužívanejšou technikou pre ich jednoduché použitie a nákladovo efektívne [7,8,9].

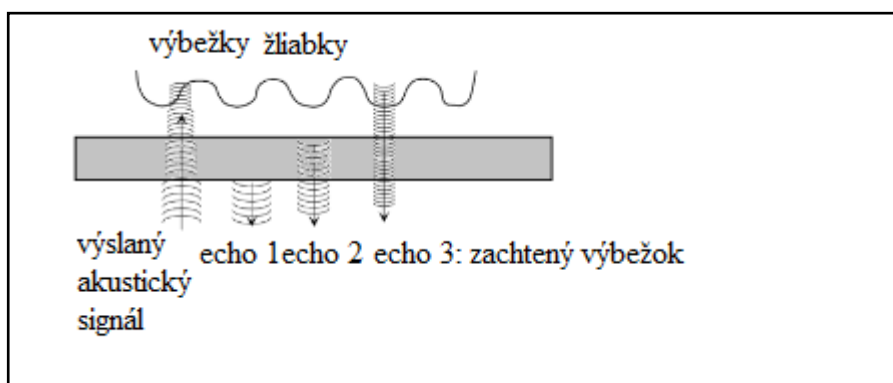
Rozpoznávanie tváre sa tiež považuje za dobrú alternatívu k odtlačkom prsta, pretože nie je potrebná žiadna fyzická interakcia s používateľom a výsledky zhody sú presné, ak je obraz dobre zachytený [10]. Biometrická čítačka, ktorá bola použitá pri testoch, využíva optický princíp.

Pri čítačke na odtlačok prsta, pracujúcej na optickom princípe je prst, konkrétne jeho posledný článok, priložený na sklenenú časť čítacieho zariadenia, následne je osvetlený svetlom dopadajúcim na prst pod definovaným uhlom. Na prste sa nachádzajú papilárne línie, o ktorých platia 3 zákonitosti, a to že neexistujú 2 osoby s rovnakými obrazcami papilárnych línií, markantov. Papilárne línie sú nemenné počas života človeka a papilárne línie sú neodstrániteľné, pokiaľ nie je odstránená zárodočná vrstva kože. Odraz svetla od týchto papilárnych línií, ktoré vytvárajú výbežky a žliabky, pričom od žliabkov je svetlo odrazené do šošovky a pokračuje do CCD/CMOS čipu [1,11].



Obrázok 2 Princíp fungovania optickej čítačky odtlačku prsta [1]

Kapacitná čítačka odtlačku prsta využíva kapacitný senzor, ktorý vytvára dvojrozmerné pole mikro-kondenzátorovej platne zabudovanej do čipu. Druhou doskou každého mikro-kondenzátora je samotná koža prsta. Pri umiestnení prsta na čip sa medzi povrchom prsta a kapacitným senzorom čítacieho zariadenia vytvárajú malé elektrické náboje. Veľkosť týchto nábojov závisí od vzdialenosti medzi prstom a kapacitným senzorom. Výbežky a žliabky odtlačku prstu tak vedú rôzne kapacitné odpory. Presné meranie kapacity je pomerne ťažko urobiť a upraviť a každý výrobca má svoju vlastnú metódu, aby dostal dostatok citlivosti na rozlíšenie medzi výbežkami a žliabkami [1,12].



Obrázok 3 Ultrazvukové čítacie zariadenie [1]

Teplotné čítačky sú vyrobené z pyro-elektrického materiálu, ktorý vytvára prúd na základe teplotných rozdielov. Výbežky odtlačkov prstov, ktoré sú v kontakte s povrchom čítačky vytvárajú odlišný teplotný rozdiel ako žliabky, ktoré sa nedotýkajú povrchu čítačky. Teplotný rozdiel vytvorí obraz prstu, ktorý po vyrovnaní teploty medzi prstom a povrchom čítačky zmizne. Okrem tejto nevýhody má tepelné snímanie aj výhody napr.

nie je citlivé na elektrostatické výboje, odtlačok prstu nasníma, aj cez povlak (10-20 μm), pretože tepelné informácie sa môžu ľahko šíriť prostredníctvom povlaku [1,12].

3 Testovanie

Pri testovaní elektrického systému kontroly vstupov, fungujúcom na optickom princípe skenovania odtlačku prsta, bolo vykonaných celkovo 500 testov, 250 krát simulácia oprávnenej žiadosti a 250 simulácia neoprávnenej žiadosti. Za neoprávnené žiadosti sú považované umelé odtlačky, ktoré majú rovnaké papilárne línie ako registrovaný prst, a tak isto živý prst s odlišnými papilárnymi líniami. Ako umelé odtlačky boli použité objemné odtlačky vyrobené zo želatíny, latexu a silikónu, tak isto bol vyrobený aj plochý odtlačok z grafitovej tuhy.



Obrázok 4 Umelé odtlačky

Test pozostával z 250 krát simulovanej žiadosti neoprávneným odtlačkom (N_{II}). Z 250 simulácií neoprávneného pokusu boli jednotlivé neoprávnené odtlačky rozdelené rovnomerné, teda každý druh bol testovaný 50 krát, vid' tabuľka

Druh	Počet pokusov	Správne odmietnutie	Chybné prijatie (N_{FA})
Neregistrovaný	50	50	0
Silikónový	50	33	17
Latexový	50	24	26
Želatinový	50	12	38
Tuha	50	50	0
Σ	250	169	81

Tabuľka 1 Výsledky pri pokuse o prekonanie

Z tabuľky 1 vyčítame, že N_{FA} je 81 a hodnota N_{II} je 250.

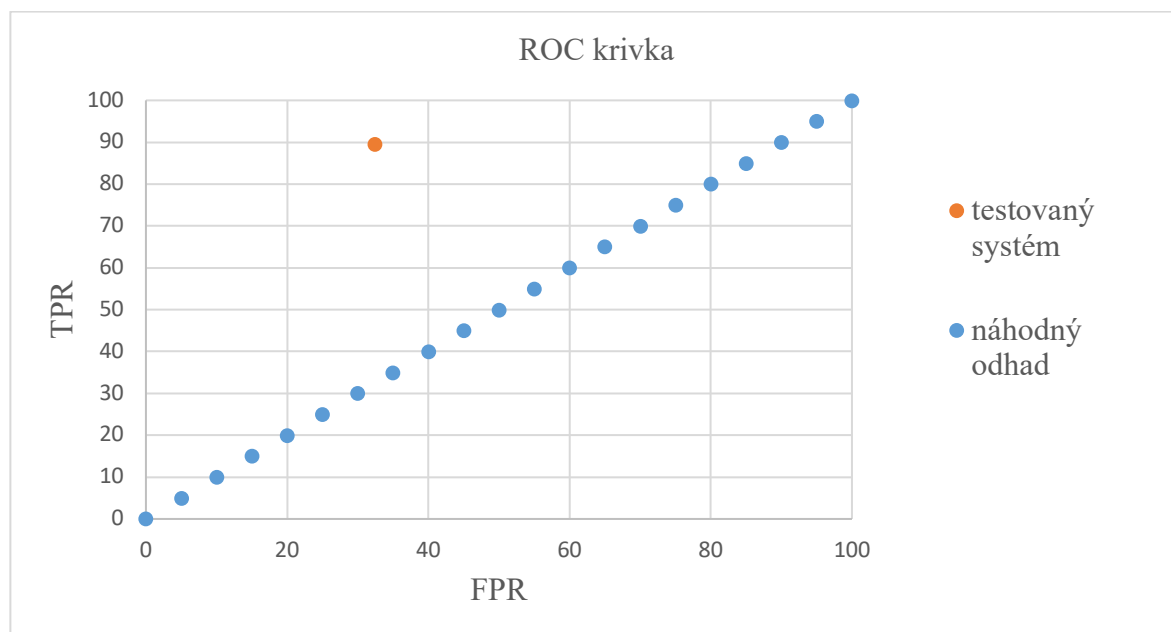
$$FAR = \frac{N_{FA}}{N_{II}} = \frac{81}{250} = 0,324 = 32,4 \% \quad (1)$$

Pravdepodobnosť chybného prijatie – FAR pri použití metódy identifikácie na základe odtlačku prstu je v testovanom systéme je 32,4 %.

Po vypočítaní hodnoty FAR, môžeme prejsť k znázorneniu ROC krivky, na ktorej znázornenie potrebujeme poznať hodnoty FPR a TPR. Keďže $FPR = FAR = 32,4\%$ je potrebné vypočítať už len hodnotu TPR, teda aké percento zo všetkých oprávnených pokusov bolo správne klasifikovaných.

$$TPR = \frac{TP}{N_{FTA}} = \frac{224}{250} = 0,896 = 89,6\% \quad (2)$$

Z výsledkov vyplýva, že bod, ktorý bude prezentovať testovaný systém bude mať súradnice (32,4;89,6).



Obrázok 5 ROC krivka pri identifikácii na základe odtlačku prsta

Z ROC krivky, uvedenej v obrázku 4 vyplýva, že identifikácia na základe odtlačku prsta, testovaného systému sa dá považovať za kvalitnú, pretože čím je krivka, v našom prípade bod bližšie k ľavému hornému rohu, tým je systém kvalitnejší. Krivku nie je možné znázorniť, pretože na testovacom zariadení, nie je možné nastaviť citlivosť čítacieho zariadenia, a tak, nie je možné vypočítať hodnoty TPR a FPR pre rôzne citlivosti, znázorniť ich na grafe a prepojiť ich krivkou.

4 Záver

Článok bol zameraný na nedeštrukčné prekonanie elektronického systému kontroly vstupov, pracujúcom na identifikácii používateľa prostredníctvom biometrie – odtlačku prsta. Odtlačok prsta bol skenovaný optickou čítačkou, ktorá zaznamenáva odrazené svetelné lúče od papilárnych línií a na základe nich dokáže identifikovať osobu. Na testovanie sme použili umelé odtlačky prsta, ktorý je registrovaný v pamäti systému. Plošný umelý odtlačok s rovnakými papilárnymi líniami ako registrovaný prst a neregistrovaný živý prst bol v 100% prípadoch odmietnutý. Umelé odtlačky zo silikónu, latexu a želatíny boli objemné, na ktorých papilárne línie ako výbežky a žliabky, teda tak, ako na reálnom prste. Rovnako bol použitý aj plošný odtlačok, ktorý bol jednoducho vyrobený z odtlačku prsta, na ktorom bola nanosená tuha a následne bol prst odtlačený na biely kancelársky papier. A taktiež, bol použitý aj živý prst, ktorý nie je registrovaný. Výsledky testov preukázali, že systém nerozoznal umelý objemný odtlačok a v 32,4% nesprávne prijala takýto odtlačok ako pravý a umožnila vstup. Preto by som z môjho pohľadu odporúčal vybaviť takýto systém, ktorý pracuje s optickou čítačkou na odtlačok prsta, senzorom na zisťovanie teploty prsta, resp. doplnením o viac násobné overenie používateľa.

Literatura

- [1] - MALTONI, D., et al., 2003. Hand book of fingerpritrn recognition. Druhé vydanie. Londýn: Springer-Verlag. ISBN 978-1-84882-253-5.
- [2] - DOURTE, T., et al., 2016. Biometric access control systems: A review on technologies to improsve their efficiency. In Power Electronics and Motion Control Conference (PEMC), 2016 IEEE International
- [3] - EN 60839-11-1, Poplachové a elektronické bezpečnostní systémy – Část 11-1: Elektronické systémy kontroly vstupu – Požadavky na systém a komponenty.
- [4] - LODERER, M., J., PAVLOVIČOVÁ. 2016. Biometria. Prvé vydanie. Bratislava: Felia s.r.o. ISBN 978-80-89824-06-9.
- [5] - RAK, R., et al., 2008. Biometrie a identita člověka ve forenzních a komerčních aplikacích. Prvé vydanie. Praha: Grada. ISBN 8024723655.
- [6] - KO, T., 2005. Multimodal biometric identification for large user population using fingerprint, face and iris recognition”. In Applied Imagery and Pattern Recognition Workshop, Proceedings. 34th, IEEE
- [7] - RAHIM, M., R., 2016. Implementation of biometric authentication methods for home based systems (dizertačná práca), Cardiff Metropolitan University
- [8] - PINTO, A., et al., 2019. Counteracting Presentation Attacks in Face, Fingerprint, and Iris ecognition. In Deep Learning in Biometrics, CRC Press
- [9] - SANJEKAR, P. S., J. B. PATIL, 2019. Multimodal biometrics with serial, parallel and hierarchical mode at decision level fusion,” Indonesian Journal of Electrical Engineering and Computer Science
- [10] - JAHROMI, M., et al., 2018. Automatic Access Control Based on Face and Hand Biometrics in A Non-Cooperative Context. In Computer Vision Workshops (WACVW), 2018 IEEE Winter Applications of, IEEE
- [11] – ŠIMOVICEK, I., at all, 2011. Kriminalistika. Prvé vydanie. Plzeň: Aleš Čeněk. ISBN 978-80-7380-343-8.
- [12] - LUKÁŠ, L., et all, 2011. Bezpečnostní technologie, systémy a management I. Zlín: Verbum. ISBN 978-80-87500-05-7