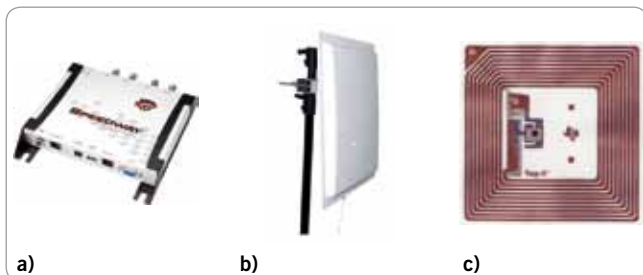


Přístupové systémy (2)

Relativně novou je metoda RFID identifikace v UHF pásmu. Využívá se především v průmyslových aplikacích, logistice, skladovém managementu, řízení budov apod. Obecně všude tam, kde je třeba na velkou vzdálenost, typicky jednotky až desítky metrů, identifikovat objekty. Snímače pro UHF RFID pracují v pásmech 865 – 956 MHz (vyjíměčně 2,4 GHz), umožňují připojení i několika externích antén (dvojitá polarizace) a disponují celou řadou komunikačních rozhraní (Wiegand, RS-485/232, ethernet). Identifikátory mají různé tvary a velikosti, nejčastěji existují ve formě potisknutelných samolepek se zabudovanou anténou a čipem – obr. 14.



Obr. 14 RFID identifikace v UHF pásmu UHF:

a) RFID snímač (Speedway R420), b) monostatická UHF anténa, c) transpondér v podobě nálepkového štítku

Kombinované identifikační čipy

Jedná se o spojení kontaktního a bezkontaktního principu v jedné kartě, přívěšku nebo klíči.

Magnetická identifikační média

Jedná se o karty, které mají na svém povrchu umístěn magnetický proužek, na kterém jsou zaznamenány informace. Magnetický proužek obsahuje dvě nebo tři datové stopy. První dvě stopy slouží pouze pro čtení informací a na třetí stopu lze informace i zapisovat. Tuto třetí stopu využívají např. banky pro zaznamenání různých údajů (finanční limit klienta, apod.) [7]. Fotografie vybavení pro magnetickou identifikační média jsou na obr. 15.



Obr. 15 Magnetická identifikační média: a) Karta s magnetickým proužkem, b) průtažná čtečka IEI 233, c) elektromotorická čtečka.

Optická identifikační média

Pro optické identifikační prvky se používá čárový kód, data matrix (2D) nebo kruhový kód. Pro čtení tohoto kódu slouží laserové nebo CCD čtečky – obr. 16.



Obr. 16 Optická identifikační média: a) příklad optického kódu data matrix, b) QR kód, c) EAN-13, d) čtečka MK-7120 Orbit (Honeywell.)

Biometrická identifikační média

Biometrická identifikace vychází z předpokladu, že některé fyziologické (anatomické) a behaviorální vlastnosti člověka jsou jedinečné a časem neměnné. Z fyziologických znaků jsou nejpoužívanější:

- **Otisk prstů** – papilární linie prstů, v daktyloskopii porovnávání charakteristických vzorů a markantů
- **Oční sítnice** – Optický systém sejmě část sítnice, obraz tvoří krevní cévky osvětlené koherentním zdrojem světla. Systém uživatelsky nepřívětivý, je nutná velmi přesná pozice vůči skeneru.
- **Oční duhovka** – Oko je snímáno kamerou ve viditelném nebo infračerveném spektru, analýzou kontrastu je „vyseknuta“ oblast duhovky, a pouze ta je navzorkována, normována a zaznamenána. K porovnání jsou použity sofistikované matematické metody. Není nutná nehybnost ani tak přesná pozice uživatele vůči čtečce.
- **Obličej** – porovnávána je geometrie, resp. 3D model tváře. Snímání je prováděno 1 nebo 2 kamerami většinou v IR spektru, porovnávají se charakteristické vzdálenosti a proporce očí, nosu, uší, lícních kostí, čelisti apod. Při dnešních algoritmech je spolehlivost značná ($FAR < 0,0001\%$), problém nebývá ani u jednovaječných dvojčat.
- **Další** – tvar ruky, ušnice, pach, rozložení cév, DNA apod.

Z behaviorálních znaků lze jmenovat hlas, podpis, stisk kláves, chůzi. Tyto technologie však nejsou příliš rozšířené.

V biometrických systémech se vždy zpracovává mnohem větší objem dat než např. u systémů čipových. Terminály pro oční nebo obličejovou identifikaci jsou vybaveny výkonným procesorem na bázi ARM nebo průmyslovým PC, s integrovaným „embedded“ operačním systémem (Windows, Linux...). Proces ověřování pro velké množství uživatelů je tedy náročnou procedurou. Proto se v praxi u biometrických systémů setkáme s metodou ověřování „1:N“ nebo „1:1“. První z jmenovaných metod prohledává celou databázi uložených identit, zatímco druhá metoda vyžaduje před samotnou biometrickou identifikací ještě identifikaci jiným způsobem (kód, RFID apod.), poté dojde jen k porovnání konkrétní identity s právě pořízeným vzorkem.

Čtečky otisků prstů nabízejí uživatelský komfort, vysokou míru zabezpečení a v posledních letech také nízkou cenu. Z pohledu snímacího elementu je dělíme na tyto nejpoužívanější druhy:

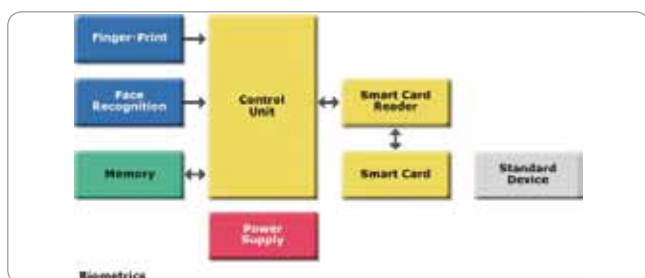
- **Optické** – Prst položený na dotykovou vrstvu (sklo) je osvětlen zdrojem viditelného světla (LED), které po odrazu na CCD/CMOS čip vytváří obraz papilárních linií. Nevýhodou je nutný velký kontrast linií, náchylnost k zašpinění, poškrábání, možnost opticky napodobit otisk a velké rozměry senzoru. Výhodou pak především ESD odolnost.
- **Kapacitní (CMOS)** – Zvrásnění papilárních linií je v podstatě kombinací 2 dielektrik (vzduchu a tkáně). Kapacitní senzory mohou být pasivní nebo aktivní. Pasivní senzory pouze měří kapacitu záhybů dermální vrstvy pokožky (ta se jeví jako vodivá) vůči mikroelektrodám matice kapacitorů, zatímco aktivní kapacitní (někdy označované jako RF) budí elektrody matice vysokofrekvenčním signálem a tak jsou schopny měřit kapacitu včetně epidermálních vrstev. Z toho vyplývá, že jsou odolnější vůči vnějšímu zašpinění nebo poškození pokožky.
- **Ultrazvukové** – Podobně jako aktivní kapacitní senzory pronikají vysokofrekvenčním ultrazvukovým signálem až do dermální vrstvy, proto je odolnost vůči zašpinění nebo poškrábání velmi dobrá, cena je však nejvyšší ze zde uvedených senzorů. Senzor je tvořen maticí piezoelektrických měničů.
- **Teplotní** – Matice pyroelektrického materiálu snímá na povrchu teplotní rozdíly, způsobené vrcholky a prohlubněmi linií. Funkce je značně ovlivněna okolní teplotou, setrvačností apod.

Podle způsobu aplikace prstu na senzor dělíme čtečky, resp. jejich senzory, na dotykové (touch) a posuvné (swipe). U dotykových je obraz pap. linií nasnímán najednou, zatímco u posuvných dochází ke složení výsledného obrazu z několika proužků získaných z užší matice senzoru. Přirozené, uživatelsky příjemnější je typ dotykový.

Typické rozlišení dnešních čteček otisků prstů bývá 500 dpi, zpracování vlastní informace ze senzoru se provádí výkonným DSP procesory. Všechny sensory musí vykazovat velkou ESD ochranu a odolnou kontaktní vrstvu. Příklady systémů pro biometrickou identifikaci jsou uvedeny na obr. 17. a na obr. 18 je uveden příklad přístupového systému s biometrickými prvky od firmy STMicroelectronics [8].



Obr. 17 Systémy pro biometrickou identifikaci: a) Optický snímač otisku prstů, b) kapacitní snímač otisků prstů, c) snímač oční duhovky, d) terminál s rozeznáváním modelu obličeje (Suprema BioEntry, Aktion AXR-500, LG IrisAccess 3000, Aktion AFT-500)



Obr. 18 Příklad přístupového systému s biometrickými prvky od firmy STMicroelectronics [8].

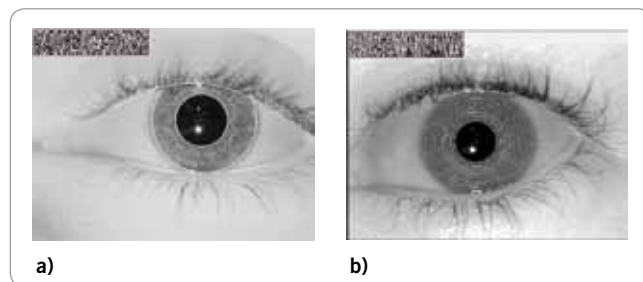
Mezi základní identifikační oblasti náleží oko – duhovka, oko – sítnice, obličej, otisk prstu, geometrie ruky, podpis, barva hlasu apod. Tab. 2 porovnává vlastnosti používaných biometrických systémů [9].

Charakteristika	Otisk prstu	Geometrie ruky	Sítnice	Duhovka	Obličej	Podpis	Hlas
Snadnost použití	Vysoká	Vysoká	Nizká	Střední	Střední	Vysoká	Vysoká
Výsoký chyb	Pocení, špína, věk	Úrazy, věk	Brýle	Slabé osvětlení	Osvětlení, věk, brýle, vlasy	Změny podpisu	Hluk, nachlazení, počasí
Přesnost porovnání	Vysoká	Vysoká	Velmi vysoká	Velmi vysoká	Vysoká	Vysoká	Vysoká
Akceptovatelnost	Střední	Střední	Střední	Střední	Střední	Střední	Vysoká
Úroveň zabezpečení	Vysoká	Střední	Vysoká	Velmi vysoká	Střední	Střední	Střední
Dlouhodobá stabilita	Vysoká	Střední	vysoká	vysoká	Střední	Střední	Střední

Tab. 2 Porovnání základních vlastností biometrických systémů

Oko-duhovka

Základem této metody je převod obrazu duhovky do elektronické podoby. V podstatě se jedná o „obyčejné“ fotografování očí, které se osvětí infračerveným světlem nízké intenzity. Širokoúhlý objektiv nejprve zachytí celý obličej, zjistí pozici očí a vybere jedno z nich. Dougmanův postup vyhodnocuje asi 250 znaků duhovky, jako jsou žilky, pigmentové skvrny, proužky, body, vyvýšeniny a další. Fotografováním je vytvořen černobílý obraz s rozlišením 640x480 pixelů. Softwarově se odstraní různé kazy a reflexy, ale i půlkruh duhovky se transformuje na obdélník. Při analýze je kontrolován bit po bitu, zjistí-li se shoda v 67 % znaků, považují se oba vzory za totožné. Shodnost v 67 % odpovídá pravděpodobnosti 1:1,2 milionu. Protože je struktura duhovky symetrická, lze různé deformace matematicky korigovat. Vzorek duhovky je jedinečný, ale některá onemocnění snižují možnost tohoto rozpoznávání. Na obr. 19 je provedeno porovnání obrazu duhovky s její elektronickou podobou [10].



Obr. 19 Duhovka oka: a) obraz duhovky, b) elektronická podoba obrazu.

Geometrie obličeje

Podobně jako při skenování duhovky se i při rozpoznávání obličeje stanoví charakteristické ukazatele a porovnají se s uloženou šablonou. Používají se především znaky málo ovlivněné mimikou, jako horní okraje očních, oblasti kolem lícních kostí, postranní partie úst. Software nejprve vyhledá oči jako temné body a poté další významné body obličeje. Při výpočtu charakteristických dat se vytvoří na obličeji mřížka spojující významné body, její velikost bývá kolem 1 MB až 1,3 MB. Shoda obrazu s vzorem je ovlivněna správným natočením obličeje. K eliminaci této chyby se stále více využívají speciální kamery schopné zaznamenat 3D obraz obličeje. Na obličej se promítne obraz složený z barevných proužků, které se na nosu, čele, uších a bradě různě zformují a vytvoří charakteristický vzor. Tato metoda odstraňuje rušivé faktory, umožňuje identifikaci osoby i uprostřed davu. Na obr. 20 je zobrazen skenovaný obličej a elektronická podoba geometrie obličeje [11], [12].

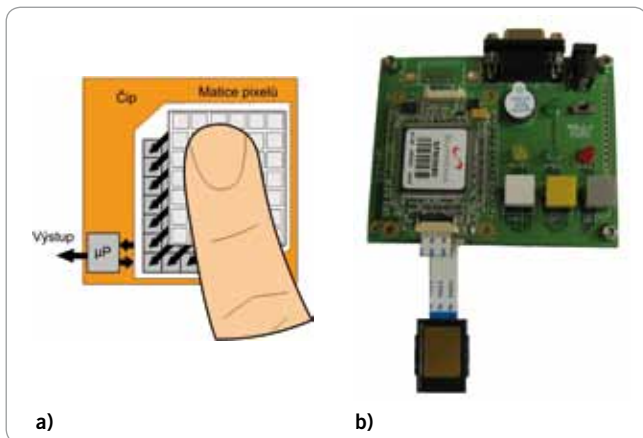


Obr. 20 Identifikace podle geometrie obličeje.

Otisk prstu

Systém pracuje na základě porovnávání papilárních linií. Mikro počítač porovnává charakteristické body, tzv. minucie s uloženým vzorem. K vytvoření obrazu povrchu prstu se používají senzory využívající různé fyzikální principy (tepelný, kapacitní, optický atd.), které zajišťují přípravu černobílých vzorů linií. Vzorky se považují za shodné, souhlasí-li 12% znaků. Nejrozšířenější jsou optické senzory, při nichž se prst osvětí a vyfotografuje. U kapacitního snímání tvoří povrch senzoru spolu s povrchem prstu kondenzátor, jehož

kapacita se mění s reliéfem prstu. Další metody měří elektrické pole nebo teplotní obraz. Aby se zamezilo použití napodobenin (např. silikonových), mnohé systémy navíc měří puls, průtok krve, obsah kyslíku v krvi a teplotu prstu. Základní princip kapacitního senzoru otisků lze prezentovat na obr. 21, kde je uvedeno blokové zapojení jednoduchého čipu realizovaného v 0,5 μm CMOS LSI technologii [13]. Čip senzoru obsahuje mikrokondenzátory uspořádané do matice. Počít kondenzátorů určuje rozlišení (rozečť článků je až 65 μm). Po přiložení prstu se měří kapacita jednotlivých článků, z hodnot se vytváří mapa rozložení kapacity (obraz otisku). Každý článek představuje jeden pixel obrazu. Jednotlivé pixely jsou zpracovány digitálně s paralelním zpracováním informace ze všech pixelů. Na čipu je mikrokontroler pro řízení paralelního zpracování signálu v jednotlivých pixelech a pro řízení komunikace mezi senzorem a vnějším počítačem. Na obr. 21b) je fotografie systému snímáče otisku prstu s kapacitním senzorem otisků [14]. Rozlišení je 508 dpi, snímací plocha 12,8 mm x 18 mm a obrazová velikost je 256 x 360 pixelů.



Obr. 21 Kapacitní senzor otisku: a) blokové zapojení jednoduchého čipu v 0,5 μm CMOS LSI technologii, b) fotografie kapacitního senzoru s elektronickým vybavením

Geometrie ruky

Metoda proměřuje geometrii celé ruky, charakteristická data obsahují délku prstů, šířku kloubů, tvar ruky. Data ke zpracování se snímají čtecím zařízením na obr. 22 [15].



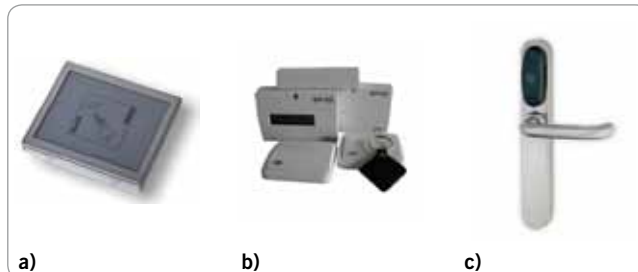
Obr. 22 Snímání dat o geometrii ruky.

Rozsah přístupových systémů, topologie

Autonomní systémy

Autonomní systém je tvořen max. 2 (oboustranný přístup) snímáči zařízeními (klávesnice, RFID, biometrie), který má zároveň funkci kontroléru, nebo je řídicí jednotka oddělena. Přístupová práva se programují pomocí specifického postupu (master kód/karta, speciální HW mód, popř. připojení k PC) a jsou uložena v paměti samotného kontroléru. Bezpečnější variantou je samozřejmě oddělená řídicí jednotka. V tomto uspořádání je

obvykle identifikační zařízení propojeno s řídicí jednotkou pomocí proudové smyčky, jednoduché sériové linky nebo sběrnici RS-485. Obvykle paměť umožňuje uložení jen několik desítek uživatelů, s tím, že záznam událostí na přístupovém místě není vůbec prováděn nebo jen ve velmi omezené míře. Připojení řídicího PC buď není vůbec možné, nebo slouží jen pro servisní programování uživatelů a stažení logu (např. v případě škodní události). Systém je vhodný pro jeden nebo několik samostatných prostupů, s menší četností pohybu osob, obecně pro instalace s nízkými nároky na bezpečnost apod. Do této kategorie patří také autonomní dveřní zámky s integrovanou čtečkou. Příklady autonomních přístupových systémů jsou uvedeny na obr.23.



Obr. 23 Autonomní přístupové systémy: a) VIDEX 4850, b) Jablocb RP-02, c) EVVA Salto Prox.

Poděkování

Obsah článku vznikl v souvislosti s řešením projektu Centrum bezpečnostních technologií (CEBET II) podporovaného MŠMT ČR, částečně v souvislosti s řešením projektu MV ČR VG 2010 2015 015 „Miniaturní inteligentní analyzační systém koncentrací plynů a škodlivých látek, zejména toxických“.

Literatura

- [7] Karty s magnetickým proužkem http://pandatron.cz/?535&karty_s_magnetickym_pruhem
- [8] (www.st.com)
- [9] Teplý, T., Přístupové systémy, přednáška, ČVUT, 2008
- [10] <http://www.cl.cam.ac.uk>
- [11] http://www.bundesregierung.de/Content/EN/Artikel/2007/11/Bilder/hightech-serie-sicherheit-3d-objekterfassung_layoutVariant=Poster.html
- [12] <http://www.3dface.org/media/images.html>
- [13] Husák, M., Mikrosenzory a mikroaktuátory, Academia 2008
- [14] Meghdadi, Majid; Jalilzadeh, Saeed (29 October 2005). „Validity and Acceptability of Results in Fingerprint Scanners“. Proceedings of the 7th WSEAS International Conference on Mathematical Methods and Computational Techniques In Electrical Engineering. Retrieved 4 November 2010.
- [15] <http://www.sandiacontrolsystems.com/page3.html>

Pokračovanie v budúcom čísle.

Prof. Ing. Miroslav Husák, CSc.

Ing. Tomáš Vítek

Ing. Tomáš Teplý

Katedra mikroelektroniky, Elektrotechnická fakulta ČVUT v Praze