Jihočeská univerzita v Českých Budějovicích
Přírodovědecká fakulta

Biometrie a její využití v kriminalistice

Bakalářská práce

Ivona Váchová

Vedoucí práce: Mgr. Jakub Kothánek, LL. M.

České Budějovice 2019

Jihočeská univerzita v Českých Budějovicích
Přírodovědecká fakulta

ZADÁVACÍ PROTOKOL BAKALÁŘSKÉ PRÁCE

Student: Ivona Váchová
(jméno, příjmení, tituly)

Obor – zaměření studia: Aplikovaná informatika

Katedra/ústav PřF JU, kde bude práce vypracována a obhájena:
UAI

Školitel: Mgr. Jakub Kothánek LL.M.
(jméno, příjmení, tituly, u externího š. název a adresa pracoviště, telefon, fax, e-mail)

Garant z PřF JU: .....
(jméno, příjmení, tituly, katedra – jen v případě externího školitele)

Školitel – specialista, konzultant: .....
(jméno, příjmení, tituly, u externího š. název a adresa pracoviště, telefon, fax, e-mail)

Téma bakalářské práce: Biometrie a její využití v kriminalistice

Cíle práce:
- Provedení rešerše na dané téma
- Vysvětlení pojmů problematiky, její historie a vývoje
- Seznámení s biometrickými metodami identifikace
- Vysvětlení nejvyužívanějších metod
- Uvedení dokladů ~~využívané~~ využívajících biometrické vlastnosti a jejich vývoje
- Zpracování vztahu biometrie ke kriminalistice

Základní doporučená literatura:

Financování práce .....

Školitel práce .....podpis: .....

U externích vedoucích fakultní garant práce .....podpis: .....

Garant oboru bak. studia (nepožaduje se u oboru biologie) .....podpis: .....

Vedoucí katedry/ústavu PřF JU, kde proběhne obhajoba.....podpis:

.....

Případný souhlas vedoucího ústavu AV .....podpis: .....

V Českých Budějovicích dne .....Podpis studenta ....Váchová

Bibliografické údaje:

Váchová Ivona, 2019: Biometrie a její využití v kriminalistice

[Biometry and its use in forensic science Bc. Thesis, in Czech], Faculty of Science, The University of South Bohemia, České Budějovice, Czech Republic.

Anotace:

Bakalářská práce je zaměřena na podání aktuálních a srozumitelných informací o biometrii. Cílem je srozumitelně seznámit veřejnost s možnostmi biometrické identifikace, jejich technologiemi a využitím v kriminalistice. V práci jsou vysvětleny důležité pojmy, historie oboru a dělení biometrických vlastností a identifikace. Dále práce seznamuje s biometrickými systémy, jejich kritérii a chybami. Hlavní část tvoří zpracování jednotlivých vybraných identifikačních metod. Na závěr je také uvedeno využití biometrických vlastností v osobních dokladech a kriminalistice.

Klíčová slova:

biometrie; biometrické systémy; ePas; identifikace; kriminalistika; verifikace

Abstract:

The bachelor thesis is focused on submitting actual and understandable information about biometrics. The aim is to acquaint the public with the possibilities of biometric identification, their technologies and utilization in forensic science. The thesis explains important terms, history of the branch and division of biometric characteristics and identification. The thesis also introduces biometric systems, their criteria and errors. The main part consists of processing of selected identification methods. At the end there is also a possibility of using biometric characteristics in identity papers and forensic science.

Keywords:

biometrics; biometric systems; ePassport; forensic science; identification; verification

Prohlášení

Prohlašuji, že svoji bakalářskou práci jsem vypracovala samostatně pouze s použitím pramenů a literatury uvedených v seznamu citované literatury.

Prohlašuji, že v souladu s § 47b zákona č. 111/1998 Sb. v platném znění souhlasím se zveřejněním své bakalářské práce, a to v nezkrácené podobě elektronickou cestou ve veřejně přístupné části databáze STAG provozované Jihočeskou univerzitou v Českých Budějovicích na jejích internetových stránkách, a to se zachováním mého autorského práva k odevzdanému textu této kvalifikační práce. Souhlasím dále s tím, aby toutéž elektronickou cestou byly v souladu s uvedeným ustanovením zákona č. 111/1998 Sb. zveřejněny posudky školitele a oponentů práce i záznam o průběhu a výsledků obhajoby kvalifikační práce. Rovněž souhlasím s porovnáním textu mé kvalifikační práce s databází kvalifikačních prací Theses.cz provozovanou Národním registrem vysokoškolských kvalifikačních prací a systémem na odhalování plagiátů.

V Českých Budějovicích, 12. dubna 2019 .....

Ivona Váchová

Poděkování

Ráda bych touto cestou poděkovala vedoucímu své bakalářské práce Mgr. Jakubu Kothánkovi, LL. M. za vedení, pomoc při zpracování práce a čas věnovaný při konzultacích. Mé poděkovaní patří také mé rodině, která mě podporovala po celou dobu studia. Dále bych chtěla poděkovat paní Mgr. Zuzaně Veselé za odbornou konzultaci jazykové stránky práce.

Obsah

Úvod

V současném světě, kdy nám moderní a dostupné technologie dovolují setkávat se se spoustou nových lidí, věcí a jevů, kdy kontakt ani nemusí být přímý, roste potřeba identifikace. Identifikace byla dříve spojována především s oblastmi kriminalistiky a bezpečnosti. Aktuálně prostupují identifikační technologie i do civilního světa a každodenního dění obyčejných lidí.

Dochází k potřebě identifikace konkrétní, jako jsou osoby, živočichové, rostliny, předměty a jiné, a identifikace abstraktní, což jsou jevy, procesy, činnosti, chování a zájmy. (1, s. 36) Již dříve byly známé metody identifikace znalostí a vlastnictvím.

Třetí známou metodou identifikace je identifikace pomocí biometrik. Biometrická identifikace provází lidstvo sice již od počátku věků, ale až v současné době prožívá razantní rozvoj, a proto je třeba tomuto způsobu věnovat pozornost. Oproti dřívějšímu využití především v policejně-soudní oblasti se rozšiřuje používání biometrické identifikace do informačních a běžným uživatelům dostupných technologií.

Mnohá veřejnost má povědomí pouze o pár nejznámějších biometrických metodách, a proto je tato práce zaměřena na důkladnější vysvětlení aktuálních metod a seznámení s těmi méně známými a méně používanými.

Cílem práce je srozumitelně seznámit veřejnost s metodami biometrické identifikace, jejich dělením, pojmy důležitými k srozumitelnosti problematiky, zpracování historie tohoto oboru a dalšími relevantními informacemi, týkajícími se biometrie a jejího využití v různých oblastech každodenního dění.

Práce vysvětluje pojmy biometrice, identita, identifikace, verifikace a autentizace, seznamuje s historií a vyžitím biometrie. Představuje dělení biometrik a biometrické identifikace. V práci jsou vyloženy nejvyužívanější techniky s jejich výhodami a nevýhodami používání a stručně vysvětleny i metody ostatní. Je zde také zmíněn proces práce s biometrikami, kritéria biometrických technologií a chyby, které mohou vzniknout při používání biometrických systémů. Na závěr je také uvedeno využití biometrických vlastností v dokladech a kriminalistice, kde představuje jeho historii i současnost.

1 Biometrie

Původem řecké slovo biometrie se skládá ze dvou slov „*bio*“, znamenající život, a „*metric*“, což znamená měření. (2, s. 118) Dříve byla biometrie vymezována jako souhrn matematických metod, využívaných v lékařství a biologických vědách. (3, s. 7) V současnosti lze biometrii popsat jako vědu, která se zabývá měřením určitých charakteristik člověka. (2, s. 118) Pojem biometrie využívá v praxi více oborů, jako je IT nebo biomedicína. (4, s. 13) V IT tento pojem označuje systémy nebo postupy sloužící k automatické identifikaci nebo ověření identity člověka na základě unikátních, měřitelných fyziologických (např. otisk prstu, oční duhovka a sítnice) a behaviorálních vlastností (např. lokomoce, dynamika podpisu). (2, s. 118) V biomedicíně označuje statistické výpočty v biologii nebo medicíně (podklady pro genetické obory). (4, s. 13)

Jako každý způsob identifikace osob má i biometrie své výhody a nevýhody. Největší výhodou je jednoduchost, neboť biometrickou vlastnost nelze zapomenout, ztratit či přenést na jinou osobu. Dále také odrazení útočníka od podvodů a eliminace pokusů o popření identity osoby. Užití biometrie také zvyšuje stupeň zabezpečení a snadnost použití zvyšuje úroveň pohodlí identifikovaných osob. (4, s. 13) (2, s. 119)

Jednou z nevýhod je nepřesnost, která se ale s postupem času výrazně zlepšuje, ale i přesto stále biometrie není stoprocentní z důvodu nestejnosti dodávaných vzorků, které nikdy nebudou totožné jako ten uložený v šabloně. (5) Dalšími limity jsou nemožnost změny vlastnosti v případě prozrazení, potřeba kontroly životnosti osoby či nezachování soukromí. (4, s. 13) Mezi nevýhody patří i situace, kdy není osoba schopna nebo ochotna svou totožnost některým ze způsobů biometrické identifikace prokázat (např. němý není schopný identifikace hlasem), je tedy třeba počítat s náhradními řešeními. K nevýhodám se řadí i pomalost. V případě verifikace (kapitola 1.3.3), kdy se porovnává získaný vzorek se šablonou, se pomalost porovnávání neprojeví. Oproti tomu při identifikaci (kapitola 1.3.2), kdy se pro daný vzorek zjišťuje, zda existuje odpovídající šablona, se pomalost projeví, neboť jeden vzorek se porovnává i s miliony šablon. (5)

Rizikem používání biometrické identifikace je i samotný růst kvality biometriky – oční duhovku lze sejmou na dálku bez vědomí majitele, otisky prstů zanecháváme kdekoli se dotkneme, hlas lze nahrát do záznamníku, DNA lze získat ze slin zanechaných na skleničce,

fotografie sdílíme kdekoli na webu, v aplikacích a na sociálních sítích. Je proto třeba všechny tyto aspekty vzít v úvahu při tvorbě biometrických systémů. (5)

1.1 Historie

Pomocí biometrie se lidé identifikují již od dob počátku lidstva, kdy dítě rozpoznalo své rodiče po hlase, někdo známý mohl být identifikován podle lokomoce nebo vzhledu tváře.

Použití biometrických identifikačních metod, o kterém jsou záznamy, se datují až po faraonské dynastie v Egyptě. Mnoho dochovaných materiálů se zmiňuje o využití biometrické identifikace v údolí Nilu, kdy byli rolníci při výkupu obilí a vyplácení mzdy identifikováni podle unikátních jizev, barvy pleti a očí, rozměrů a vah těla. Dochovaly se také záznamy o faraonovi Khafre, který, aby vyloučil neoprávněné nebo násobné vydání mezd na stavbě pyramid, přikázal vést záznamy o všech, kteří se na stavbě podíleli. Vždy před vyplacením byl každý zaměstnanec zkontrolován podle vedených záznamů. O zaměstnancích zaznamenával, mimo základních osobních údajů a popisu obličeje a těla, i některé tělesné rozměry (např. délku lokte) a všechna viditelná zranění.

Další záznamy lze nalézt ve Starém zákoně, kde se píše o Izraelitech prchajících z Egypta. Tito uprchlíci byli vojskem identifikovaní na základě nesprávné výslovnosti slova „*shibboleth*“ a následně popravování. Identifikaci, založenou na daktyloskopii, znali již staří Číňané, Babyloňané a Peršané, kteří využívali otisk palce jako podpis při potvrzování obchodních smluv.

Roku 1686 popsal otisky prstů italský profesor Marcello Malpighi, aniž by znal jejich význam pro identifikaci. Podrobněji obrazce papilárních linií zkoumal v roce 1823 Jan Evangelista Purkyně, jehož zájem byl čistě přírodovědecký a lékařský, zasloužil se ale o návrh možnosti třídění obrazců papilár na základě jejich geometrických vlastností. (1, s. 90)

V praxi začal otisky prstů využívat roku 1858 William James Herschel, anglický guvernér v Indii, který pomocí nich identifikoval zaměstnance dráhy. Každý zaměstnanec při výplatě mzdy otiskoval svůj palec na výplatní pásku, čím potvrdil svou identitu a převzetí mzdy. Herschel později začal sbírat otisky pro vlastní zkoumání, na jehož základě sepsal knihu o původu otisků prstů. (4, s. 7)

Roku 1880 přišel Francis Galton s vědním oborem antropometrie (viz kapitola 7.1.1), na jejímž základě vyvinul Alphonse Bertillon (1882) postup zvaný Betillonáž (zabýval se jím již od roku 1879). (4, s. 8) V Japonsku začal v roce 1880 využívat daktyloskopické stopy

Dr. Henry Fauld, který je využíval k identifikaci předem vytipovaných osob, uvažoval také o zavedení daktyloskopických sbírek. Téhož roku vytvořili Francis Galton a Edward Henry třídící a registrační systém využitelný v daktyloskopické praxi. 1891 Juan Vucetich v Argentině poprvé cíleně snímá otisky prstů zločincům. (1, s. 91)

Do policejní praxe je daktyloskopie zavedena roku 1900, kdy je prosazena pro identifikační a verifikační účely. (4, s. 8) Pár let poté, 1924, americký Kongres založil oddělení FBI pro identifikaci otisky prstů. (1, s. 91) V roce 1965 byl poprvé použit daktyloskopický systém AFIS. (4, s. 8)

Již roku 1970 odstartoval využívání biometrické identifikace v komerční praxi systém Identimat, založený na měření geometrie ruky, který využívala investiční firma Shearson Hamil pro přístup do budov a kontrolu docházky zaměstnanců. V 70. letech 20. století se začala využívat pro zpracování otisků prstů v soudní praxi výpočetní technika.

Technologie AFIS začala být využívána i v civilním sektoru, kde byla využívána pro kontrolu přístupu do budov či počítačových zařízení.

Rozvoje se postupně dostává i dalším identifikačním biometrickým metodám. Roku 1980 byla do provozu uvedena první identifikační metoda založená na zkoumání struktury sítnice, byly také položeny základy pro využití oční duhovky. Mezi mladší techniky identifikace patří i rozpoznávání lidské tváře a podpisu. Na přelomu 20. a 21. století jsou vyvíjeny technologie využívající k identifikaci DNA. Tato metoda začala být později využívána mimo kriminalisticko-policejní a soudně-znalecké obory i pro civilní účely. Stejně jako AFIS byla později vyvinuta i databáze CODIS využívaná pro záznamy DNA. (1, s. 91)

1.2 Využití

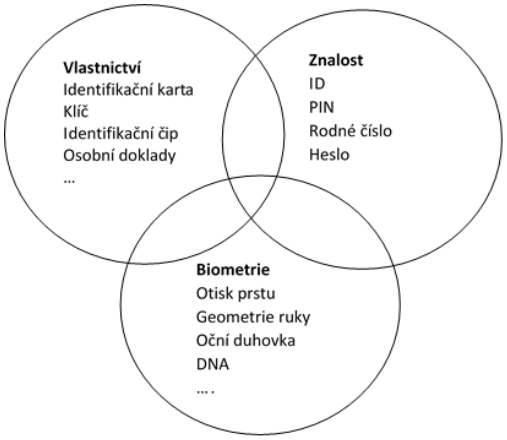
První využití zaznamenala biometrie v policejně-soudní sféře. V kriminalistice se biometrie využívá nejen k identifikaci pachatelů, ale i osob hledaných nebo obětí živelných katastrof. Později našla své uplatnění i v běžném životě. Otisky prstů nahrazují vstupní klíč domu, otisk prstu či geometrie ruky se využívají pro kontrolu vstupů a docházky osob do objektů a zaměstnání, nahrazují přístupová hesla do systémů, počítačů, místností či přestupově omezených zón objektů. V současné době se k trendu odemykání mobilního telefonu otiskem prstu přidala možnost identifikace tváří. (6) V roce 2017 využívalo biometrii v mobilních zařízení již přibližně 31 % osob ve věku 18-24 let a 8 % ve věku nad 65 let. (7) Uplatnění má biometrie i v osobních dokladech, jako jsou občanské průkazy a cestovní pasy. (6)

Rozšíření využití také nastává v bankovnictví, velké banky stále častěji nabízejí svým klientům, pro zvýšení bezpečnosti, možnosti využít k přihlášení ke svému účtu otisky prstů, hlas a jiné biometrické metody místo přístupových hesel. (7) Další využití biometrických identifikačních systémů zobrazuje Příloha č. 1.

1.3 Základní pojmy

1.3.1 Identita

Pojem identita (latinsky *indetitas*, odvozené od slova *idem* – stejný) znamená totožnost něčeho s něčím, sebe se sebou samým, používá se při porovnávání pojmů, objektů, které jsou záměnné tak, že mezi ně lze vložit znaménko rovnosti. (1, s. 37) Identita je založena na znalosti (něco vím), vlastnictví (něco mám), biometrii (něco jsem) (Obr. 1). (4, s. 11)



Obr. 1 Metody identifikace osob (4, s. 48 - vlastní úprava)

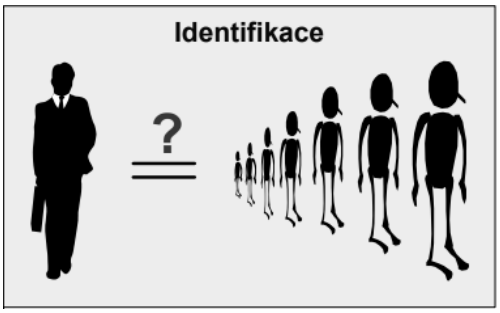
Každá osoba může mít dva druhy identity – fyzickou a elektronickou. Fyzická identita osoby je definována jejím vzhledem a chováním, tím, kdo je, a každá má pouze jednu. Tato identita je unikátní a nenajdeme dvě osoby s naprosto shodnou fyzickou identitou. Oproti tomu elektronická identita může ztvárňovat někoho, kým by osoba chtěla být. Těchto i zcela rozdílných identit si může jedinec vytvořit tolik, kolik chce (např. různé účty na sociálních sítích, emailových portálech). (4, s. 10)

1.3.2 Autentizace

S pojmem autentizace se setkáváme především u přístupových systémů. Při procesu autentizace jde o ověření identity. S autentizací se můžeme setkat při identifikaci i verifikaci, pro kterou se ale používá pojem častěji. (4, s. 11)

1.3.3 Identifikace

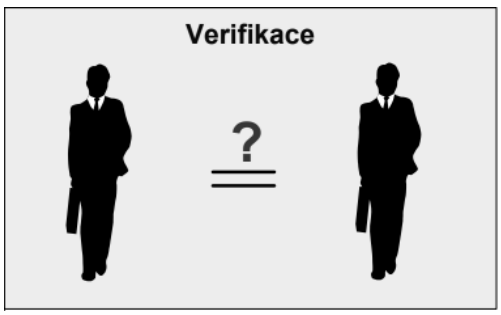
Identifikace se využívá ke zjištění identity osoby. Tento způsob získání identity se také nazývá *„One-To-Many Matching“*, jeden k mnoha, 1:n či rekognice. Při procesu identifikace uživatel předloží pouze biometrický vzorek bez předchozího sdělení identity a dochází tak k porovnávání vzorku se všemi šablonami v databázi (Obr. 2). Výsledkem je zjištění, jaká šablona (pokud existuje) odpovídá nasnímanému vzorku. (1, s. 128) Tento proces je časově náročný oproti verifikaci, neboť mnohé databáze jsou velmi rozsáhlé a obsahují velké množství šablon. Příkladem systému používaného pro identifikace je například AFIS. (4, s. 10)



Obr. 2 Identifikace – porovnání vzorku s více šablonami (8)

1.3.4 Verifikace

Verifikace se využívá k prověření, zda prověřovaná osoba je tou, za kterou se vydává. Tento způsob ověření identity se také nazývá *„One-To-One Matching“*, jeden k jedné, 1:1 či autentizace, porovnává se totiž jeden vzorek s jedou šablonou, uloženou v databázi, patřící prověřované osobě (Obr. 3). (1, s. 130) Oproti identifikaci osoba sděluje svoji elektronickou identitu a na základě ní je ověřována identita fyzická. Po sdělení identity je v databázi nalezen příslušný záznam, se kterým jsou vložená data porovnána. Neexistuje-li záznam, je přístup automaticky zamítnut. Výsledkem verifikace je potvrzení nebo vyvrácení identity osoby. (4, s. 10)



Obr. 3 Verifikace – porovnání vzorku se šablonou (8)

2 Dělení biometrik

Biometriky, lze dělit na anatomicko-fyziologické a behaviorální; jsou to měřitelné biometrické charakteristiky každého člověka, které se snímají, zpracovávají, vyhodnocují a uchovávají v procesech identifikace a verifikace. Behaviorální charakteristiky, lidské chování, jsou využívány v praxi méně často pro jejich menší objektivnost. (1, s. 105)

Podmínkou pro využití kterékoli charakteristiky je její jedinečnost, stálost, měřitelnost, výkonnost, akceptace – ochota osob nechat si vlastnost nasnímat, odolnost proti falšování a možnost dalšího zpracování pro vyhodnocení porovnání charakteristik. (4, s. 18)

2.1 Anatomicko-fyziologické biometrické charakteristiky

S těmito vlastnostmi se každý již narodí a jsou v průběhu života neměnné. Některé charakteristiky jsou často využívané v kriminalistice pro identifikaci osob a ohledání mrtvol při jejich identifikaci.

Mezi tyto charakteristiky podle částí těla patří:

- oko – oční duhovka, sítnice oka,
- hlava – obličej, tvar vnějšího ucha, termogram obličeje, dentální obraz,
- končetiny – daktyloskopické otisky prstů, dlaní a chodidel, geometrie prstů a ruky, topografie žil ruky, dlaně a prstu, snímek lůžka nehtu, termogram ruky,
- celé tělo – pach lidského těla, obsah soli v těle, rozměry a váhy těla, DNA. (4, s. 16) (1, s. 104) (2, s. 118)

Metodě analýzy anatomicko-fyzických vlastností se říká statická metoda. (4, s. 17)

2.2 Behaviorální biometrické charakteristiky

Identifikace na základě těchto charakteristik je založena na poznatcích o lidském chování. Tyto vlastnosti jsou sice unikátní, ale nejsou neměnné, jsou ovlivněny chováním a stavem osob, každý nasnímaný vzorek vlastnosti může být odlišný. Metodě analýzy behaviorálních vlastností se říká dynamická metoda. (4, s. 17) K těmto vlastnostem se řadí hlas, lokomoce (pohyb těla), písmo, podpis, dynamika stisku kláves a pohybu myší a také mimika obličeje a pohyb rtů. (4, s. 17) (1, s. 104)

3 Biometrická identifikace

Pro různou přesnost, spolehlivost, objektivnost a způsob využití metod identifikace a verifikace lze metody rozdělit na identifikaci:

- policejně-soudní,
- bezpečnostně komerční,
- ezoterickou.

Hlavní rozdíly mezi policejně-soudní a bezpečnostně-komerční identifikaci jsou uvedeny v Příloze č. 2.

3.1 Policejně-soudní (forenzní) identifikace

Tento druh identifikace, označovaný *„High Biometrics“*, je nejčastěji používán bezpečnostními složkami, kriminalisty a OČTŘ. Jedná se o nejnáročnější, nejvyspělejší a nejspolehlivější technologie z těchto tří skupin identifikace. Používané metody zaručují zjištění jednoznačné totožnosti mezi miliony osob, převažuje zde proto identifikace nad verifikací.

Z důvodu předkládání výsledků této identifikace u soudního řízení je kladen důraz na vyloučení chyb a objektivitu závěrů a metody používané pro policejně-soudní identifikaci musí být vědecky podložené a dlouhodobě prověřené na velkém množství vzorků, aby jakákoli chyba nemohla negativně ovlivnit lidský osud. Veškeré zpracování je uskutečňováno ve specializovaných pracovištích, kterých je omezené množství, pomocí laboratorních a počítačových technologií se speciálním SW vybavením, výsledek však vždy vyhodnocuje člověk – specialista, soudní znalec, který jej obhajuje před soudem. Mezi používané metody patří daktyloskopické otisky, DNA, hlas, písmo, podpis a dentální obraz. (1, s. 107)

3.2 Bezpečnostně-komerční identifikace

S rozvojem technologií a nárůstem potřeb obyčejných lidí se z metod používaných kriminalisty, vyvinuly metody a technologie vhodné pro bezpečnostně-komerční identifikaci, označované *„Lesser Biometrics“*. Systémy založené na těchto principech jsou na trhu pro své rozšíření a levnější výrobní ceny velmi dostupné a využívané především pro obecné

bezpečnostní potřeby, jako jsou zabezpečení počítačů, bankovní bezpečnost nebo ochrana citlivých osobních údajů.

Technologie pracující s biometrickými údaji jsou uzpůsobené častěji pro verifikaci než identifikaci, výsledkem verifikačního procesu proto bývá, na rozdíl od policejně-soudní identifikace, pouze povolení nebo odmítnutí přístupu. Zpracování a vyhodnocování je plně automatizované, což způsobuje nižší přesnost výsledků, pro vyhodnocování oprávnění vstupu a zamezení použití jedné identity více osobám je ale přesnost dostačující. Metodami používanými k bezpečnostně-komerční identifikaci jsou otisky prstů, geometrie ruky, oční duhovka a sítnice, tvář, hlas, podpis a dynamika psaní na klávesnici. (1, s. 108)

3.3 Ezoterická identifikace

Třetí a nejméně využívanou skupinou metod identifikace je ezoterická. Pojem ezoterický má významy jako jsou utajovaný, skrytý nebo přístupný jen zasvěceným, z čehož vyplývá, že tyto způsoby identifikace jsou známé pouze úzkému zasvěcenému okruhu lidí – specialistům. Tato kategorie obsahuje postupy identifikace, které nejsou zatím příliš rozšířené a prověřené na dostatečně velkém množství vzorků pro využívání v praxi, je jim ale věnována značná pozornost při vývoji a zkoumání.

Nejčastěji využívanou metodou ze skupiny ezoterických je identifikace pomocí pachu těla, pro kterou jsou využíváni speciálně vycvičení psi, schopní rozpoznat osoby a látky. Bohužel není možné tuto metodu realizovat do technologických postupů a pro policejně-soudní potřeby je používána pouze jako stopa, nikoli důkaz použitelný k usvědčení pachatele.

K těmto metodám se dále řadí lokomoce, tvar vnějšího ucha, topologie žil na zápěstí, obsah soli v lidském těle, snímek lůžka nehtu, mimika obličeje a pohyb rtů. (1, s. 108)

4 Biometrické systémy

Při práci s biometrickými technologiemi je třeba si ujasnit používané pojmy, potřebné k pochopení fungování celého automatizovaného systému.

Biometrický vzorek je odraz biometrických charakteristik do vnějšího světa. Vzorkem je daktyloskopický otisk, kapka krve, hlasový záznam nebo fotografie osoby.

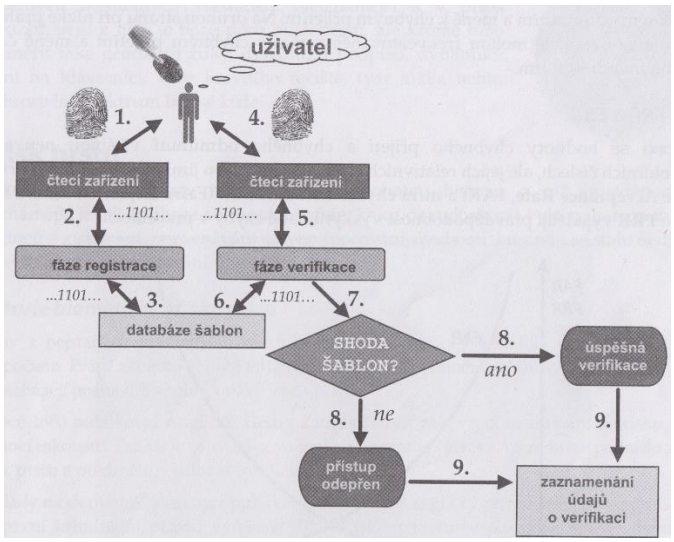
Biometrická charakteristika je měřitelný a popsatelný údaj z biometrického vzorku (papilární linie na otisku prstu).

Biometrickým markantem jsou ty části biometrických charakteristik, které se využívají pro identifikaci/verifikaci (konec a začátek nebo zakřivení papilární linie).

Biometrická šablona obsahuje naměřené hodnoty, charakteristiky, funkční závislosti minimálního počtu markantů, které jsou potřeba pro jednoznačnou identifikaci/verifikaci, je to výsledek formalizace a optimalizace biometrického vzorku, na jejím základě probíhá vyhodnocování procesu identifikace/verifikace. (1, s. 121)

4.1 Proces práce s biometrikami

Biometrické systémy pracují ve dvou fázích, registrace a verifikace, při kterých se provádějí různé úkony vedoucí k zařazení osoby do systému nebo k jejímu porovnání s obsahem uloženým v databázi. (9) Zjednodušený model fungování biometrického systému představuje obr. 4.



Obr. 4 Model biometrického systému (1, s. 121)

4.1.1 Fáze registrace

V této fázi procesu se zařazuje nová osoba do systému biometrické technologie. Osobě jsou sejmuty biometrické charakteristiky ze vzorku, který bývá odebrán několikrát, aby se pro vytvoření šablony mohl použít ten nejlepší. Po sejmutí a výběru vzorku následuje jeho zpracování měřením a extrahování nejdůležitějších charakteristik, které se ve formě matematického kódu uloží do nově vytvořené šablony.

Šablony mohou být uloženy více způsoby – přímo v zařízení, na token (čipová karta) nebo do centrální databáze, kdy je třeba zajistit zabezpečenou komunikaci mezi oběma zařízeními, v každém případě by měla být v šifrované podobě. (9) (2, s. 120)

4.1.2 Fáze verifikace a identifikace

V etapě, kdy se ověřuje totožnost, opět uživatel zadává vzorek, kde jsou měřeny a snímány dané charakteristiky, ty jsou zpracovány a vloženy do nové šablony, která je buď porovnávána s danou šablonou, nebo je odpovídající šablona hledána v databázi systému. V případě dokazování totožnosti biometrickou charakteristikou nikdy není získána stoprocentní shoda mezi šablonami, stanovuje se prahová hodnota, která určuje procentuální míru shody, kdy jsou šablony považovány za shodné, tato hodnota musí být zvolena vhodně, aby nedocházelo k nesprávnému akceptování nebo odmítnutí identifikované osoby.

Jsou zde rozlišovány dvě varianty identifikace – negativní a pozitivní. Během pozitivní identifikace uživatel chce dokázat, že někým je, a data získaná od něj, jsou porovnávána s referenční šablonou. Při negativní identifikaci osoba prokazuje, že někým není, tudíž zadává svůj vzorek, kterým dosvědčuje, že není známa systému a není uložena v databázi šablon. (9) (2, s. 120)

4.2 Kritéria biometrických technologií

Biometrické systémy jsou vyráběny na základě různých požadavků, jejichž splnění je podstatné pro úspěšnost systému. Uživatelé mají různé nároky z hlediska zabezpečení, spolehlivosti, praktičnosti, přijatelnosti i finančních možností, pro každé prostředí je vhodná jiná technologie. (10)

Kritéria pro hodnocení biometrických technologii jsou děleny do pěti skupin – operační, výrobní, technická, finanční a metodologická, algoritmická a bezpečnostní kritéria – která jsou rozebraná v následujících podkapitolách (4.2.1–4.2.5). (1, s. 113)

4.2.1 Operační kritéria

Mezi tato kritéria se řadí:

- **jedinečnost** – pro zaručení odlišitelnosti osob od sebe s vysokou přesností a spolehlivostí je třeba, aby biometrické charakteristiky dané metody byly naprosto unikátní,
- **neměnnost** – aby byla charakteristika vhodná pro použití identifikační metodou, je třeba, aby si markanty dané charakteristiky zachovávaly svoji neměnnost, a tudíž měly stálou podobu celou dobu života osoby, optimální je absolutní stálost identifikačních znaků,
- **měřitelnost** – každá charakteristika musí být měřitelná a symbolicky vyjádřitelná, ještě před uvedením metody do užívání, musí být zjištěna chybovost měření.
- **uchovatelnost** – naměřené charakteristiky se archivují, aby se předešlo ztrátě jejich kvality,
- **spolehlivost –** proces, při kterém se měří, zpracovávají, vyhodnocují a ukládají biometrické charakteristiky, musí splňovat dostatečnou spolehlivost a možnost opakování se shodnými výsledky,
- **exkluzivita** – metoda biometrické identifikace musí být úplná, aby se zamezilo potřebě další podpůrné identifikační činnosti,
- **praktičnost** – způsob, jakým je identifikace prováděna, musí být pro uživatele praktický, tzn. potřeba minimálního kontaktu se zařízením, rychlost identifikace, minimální množství potřebných úkonů, jednoduchost měření, minimum tréninku uživatele na používání,
- **přijatelnost –** všechny etapy práce se systémem by měly pro většinu lidí splňovat podmínky přijatelnosti, jak osobní, tak společenské, sociální, náboženské i etické a další. Nesmí být využity metody, které jakýmkoli způsobem uživatele poškozují, diskriminují nebo narušují soukromí,
- **lidskost –** výběr a realizace identifikační technologie je velmi citlivou psychologickou záležitostí, je třeba zajistit její uživatelskou přívětivost. Proces metody nesmí být vtíravý a rušivý, nesmí diskriminovat. (1, s. 114–115)

4.2.2 Výrobní kritéria

Výrobní kritéria se zohledňují při výběrových řízeních. Je důležité vybrat dostatečně kvalitního dodavatele či výrobce technologií, který je schopný zajistit efektivní a cenově dostupnou **podporu** při provozu zařízení, je **perspektivní**, má dobrou **záruku** a jeho práce má dobré **reference** od jiných uživatelů. V potaz je třeba brát i možnou **kompatibilitu** s dalšími využívanými technologiemi. (1, s. 118)

4.2.3 Technická kritéria

V této oblasti je kladen důraz na:

- **časová náročnost** – měří se čas přípravy uživatele a zařízení, samotný proces identifikace (snímání, zpracování, uložení, prověření),
- **chybovost** – testuje se a vyhodnocuje pravděpodobnost chybného přijetí neoprávněného (FAR – kapitola 4.3.1) nebo odmítnutí oprávněného (FRR – kapitola 4.3.2) uživatele a schopnost se s těmito situacemi vypořádat,
- **flexibilita –** biometrický systém by měl být přizpůsobitelný aktuálním potřebám vlastníka nebo uživatelů,
- **odolnost** – zařízení a jeho systém musí být odolné, aby nebyl při nesprávném užívání jednoduše poškozen,
- **efektivnost –** používáním by se mělo dosáhnout nejvyššího možného přínosu,
- **výkonnost**,
- **standardizace** – kompatibilita a schopnost užívání částí jiných systémů je další z důležitých vlastností,
- **skladovatelnost identifikačních charakteristik** – možnost archivace,
- **vlastnosti šablony** – velikost ukládaných dat by měly být minimální, aby se snížily nároky na kapacitu paměti, diskových či fyzických prostorů. Je vhodné, aby snímané hodnoty byly redukovatelné do minimálních kapacit pro efektivnost dalších postupů,
- **přesnost** – pro akceptovatelnost použití systému je důležitá jeho přesnost, aby nedocházelo k častým chybám,
- **jednoduchost** – používání technologie nesmí být pro uživatele složité,
- **rychlost**,
- **nezávislost na vnějším prostředí** – technologii nesmí ovlivnit vnější prostředí (hluk, světlo, teplota, …). (1, s. 117)

4.2.4 Finanční kritéria

Finanční možnosti odběratele technologie mívají rozhodující roli při vývoji a výběru vhodné technologie. Je důležité, aby technologie splňovala požadavky, které jsou posuzovány z krátkodobého i dlouhodobého hlediska. Jsou to:

- pořizovací cena,
- cena instalace,
- náklady spojené s uvedením technologie do provozu (školení),
- ceny upgradů a modifikací,
- ceny návazných systémů (počítače, fyzická ostraha, …),
- cena logistické podpory provozu,
- cena dalšího rozvoje sytému (další zařízení),
- cena obsluhy zařízení. (1, s. 118)

Ceny biometrických systémů se podle využívaných technologií liší. Hlavním rozdílem v ceně je, zda se kupuje pouze biometrický prvek (zařízení na snímání otisků) nebo celý systém, kdy může být implementováno i více metod dohromady. Další veličinou, která ovlivňuje cenu produktu, je jeho dostupnost v dané oblasti. (10)

4.2.5 Metodologická, algoritmická a bezpečnostní kritéria

Aby byl systém spolehlivý a přijatelný, záleží na jeho efektivitě a zabezpečení. Systém má být chráněn proti nepovoleným zásahům a modifikacím a být schopen rozpoznat zneužívání. Kromě těchto kritérií rozhodují o jeho kvalitě i algoritmy, kódování, protokoly a použité databáze. Při hodnocení těchto kritérií se posuzují:

- **správnost teorie** – pokud by algoritmus, se kterým metoda pracuje, byl založen na špatné teorii, technologie by byla nepoužitelná,
- **správnost algoritmů** – identifikační algoritmy musí být sestaveny na základě matematické teorie, která odpovídá dané identifikační metodě, použitá matematická metoda musí být otestována a certifikována specialistou,
- **bezpečnost algoritmů –** v případě, kdy je použitý algoritmus chybný nebo neobsahuje všechna dostupná řešení nežádoucích situací, tak aby nedošlo k ovlivnění výsledků, není algoritmus bezpečný. Za bezpečný algoritmus je považován ten, kdy úsilí potřebné k jeho překonání má vyšší cenu než chráněná data. Rozlišují se dvě úrovně bezpečnosti – absolutní bezpečnost nebo bezpečnost s vypočitatelnou mírou rizika,

- **správné markanty,**
- **efektivita a zabezpečení kódování biometrických dat –** zabezpečená nebo kódovaná data musí být skryta před neoprávněnou osobou, aby se zabránilo poznání skutečného obsahu
- **zabezpečení databáze –** data musí být uložena v databázi, která je dostatečně zabezpečená proti zásahům cizích osob a útočníků,
- **bezpečnost protokolů –** ke komunikaci a přenášení dat mezi zařízením a úložištěm je třeba využít protokolů, které zajistí bezpečný přenos,
- **bezpečnost síťového a distribuované prostředí –** pozornost je věnována i prostředí, ve kterém dochází k přenosu a využívání dat. (1, s. 116–117)

4.3 Chyby systémů

Jak již bylo dříve zmíněno, žádný biometrický systém není stoprocentní a podle nastavení prahové hodnoty se vyskytují různé hodnoty nejčastějších chyb biometrických systémů – chybného přijetí a chybného odmítnutí. Je-li prahová hodnota příliš vysoko, dochází častěji k chybnému odmítnutí, v opačném případě nastává častěji chybné přijetí, je proto třeba najít vhodné nastavení, aby bylo přívětivé pro majitele i uživatele systému. (2, s. 122)

4.3.1 FRR

Chyba systému, pravděpodobnost chybného odmítnutí (False Rejection Rate), označovaná jako chyba I. druhu, udává pravděpodobnost, s jakou zařízení odmítne identifikovat/verifikovat uživatele oprávněného. (10) Toto odmítnutí nemusí být způsobeno pouze chybou biometrického systému, ale i nesprávným zacházením uživatele (křivě přiložený prst na čtecí zařízení při snímání daktyloskopického otisku). (11)

Chybné odmítnutí je v komerční sféře nežádoucí především pouze z uživatelského hlediska, kdy klesá důvěra v zařízení. Z hlediska policejně-soudní identifikace může mít FRR fatální následky, kdy osoba zodpovědná za trestný čin není správně identifikována a uniká spravedlnosti.

FFR je definována jako poměr počtu falešných odmítnutí k počtu pokusů o identifikaci:

$$FRR = \frac{N_{FR}}{N_{EIA}} = \frac{N_{FR}}{N_{EVA}},$$

kde:

- NFR – počet chybných odmítnutí (Number of False Rejection)
- NEIA/NEVA – počet pokusů oprávněných osob o identifikaci/ verifikaci (Number of Enrolle Identification/Verification Attemps). (1, s. 138)

4.3.2 FAR

Tato chyba, pravděpodobnost chybného přijetí (False Acceptance Rate), označovaná jako chyba II. druhu, udává pravděpodobnost, s jakou zařízení identifikuje/verifikuje uživatele, který k tomu není oprávněný. (10)

Na rozdíl od FFR je FAR nejzávažnější z chyb, které mohou v biometrickém systému nastat, a může mít fatální následky i v komerčním sektoru, zde je nutno brát neoprávněné přijetí osoby jako bezpečnostní incident, který může vést například k finančním či majetkovým ztrátám.

FAR je definována jako poměr počtu falešných přijetí k počtu pokusů o identifikaci:

$$FAR = \frac{N_{FA}}{N_{IIA}} = \frac{N_{FA}}{N_{IVA}},$$

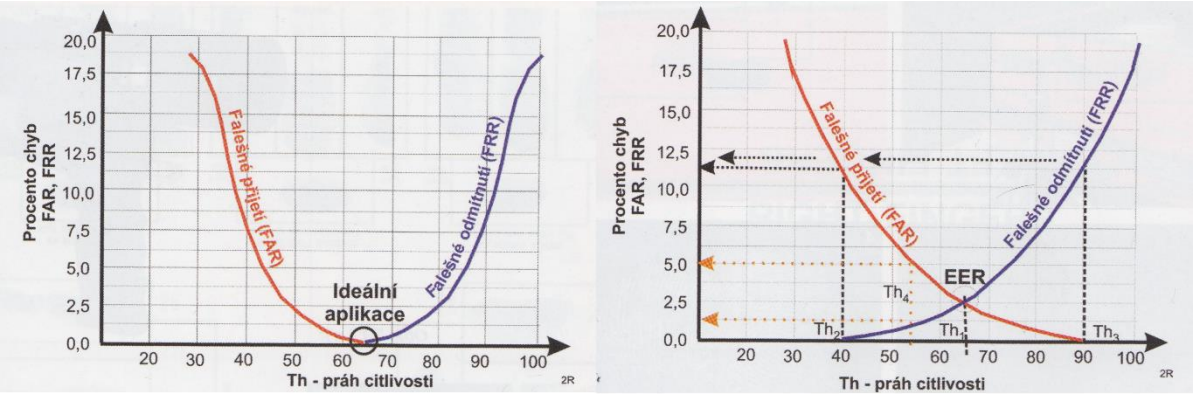
kde:

- NFA – počet chybných přijetí (Number of False Acceptance)
- NIIA/NIVA – počet pokusů neoprávněných osob o identifikaci/ verifikaci (Number of Impostor Identification/Verification Attemps). (1, s. 139)

4.3.3 EER

Případem ideální aplikace je taková, která nevykazuje žádnou chybovost, křivky hodnot FFR i FAR se neprotínají, jsou ve vhodném prahovém místě oddělitelné (Obr. 5). Tento stav je bohužel nereálný a hledá se tak umístění prahu, které bude vyhovující požadavkům a vhodné k použití, aby žádná z chyb nedosahovala extrémů (Obr. 5). (10)

EER (Equal Error Rate) je algoritmus sloužící k předurčení prahových hodnot pro FAR a FFR a porovnání dvou aplikací. V tomto bodě dosahují obě chyby stejných hodnot a jejich křivky se protínají. (12)



Obr. 5 Porovnání ideální a reálné biometrické aplikace (1, s. 140)

5 Biometrické identifikační prostředky

V následujících podkapitolách jsou rozebrány a vysvětleny jednotlivé biometrické metody, rozdělené do dvou skupin – aktuálně využívané a vybrané ostatní, které jsou méně aplikované v praxi a neznámé pro většinu lidí.

Aktuální metody obsahují jejich popis, způsob fungování, jakým se podřizují normám, kde v praxi nacházejí využití a také jaké výhody a nevýhody jejich používání v praxi přináší.

Nejpoužívanějšími normami sloužícími ke standardizaci biometrických metod jsou normy ISO/IEC a ANSI/INCITS. Standardy ISO/IEC jsou pro normy formátu výměny biometrických dat vydávány od roku 2005 a obsahují popis normy šablony pro umožnění interoperability (schopnost různých systémů vzájemně spolupracovat). Staršími normami jsou ANSI/INCITS, vydávané pro biometrii již od roku 2002. (4, s. 65 – 69)

Norma ISO/IEC 19794-1: 2011 Framework obsahuje popis obecných aspektů a požadavků pro definování formátů výměny biometrických dat. Tato norma definuje běžně používané formáty dat, standardizuje společný obsah, význam a reprezentaci datových formátů jednotlivých biometrik, které jsou specifikovány v dalších částech ISO/IEC 19794. (13)

Metodologii testování shody pro biometrické formáty výměny dat obsahuje standard ISO/IEC 29109-X, který je vydán i pro jednotlivé metody. Testování a vyhodnocení výkonnosti biometrik podléhá normám ISO/IEC 19795-X. (14)

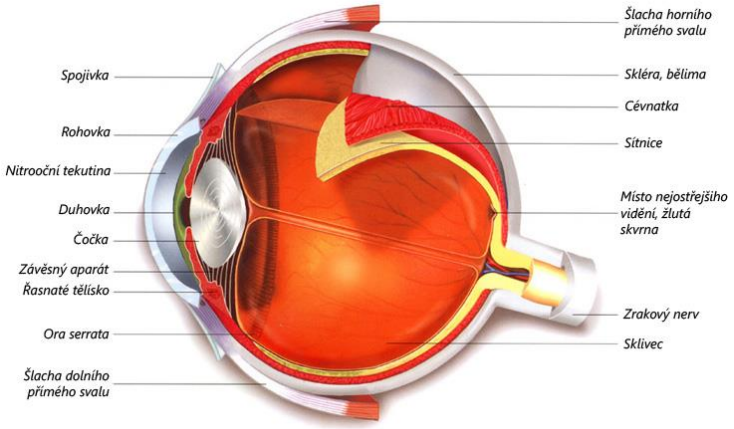
INCITS 358-2002[R2017] BioAPI Specification definuje jednotné rozhraní vhodné pro biometrické technologie. Nezahrnuje požadavky na bezpečnost biometrických aplikací, ale uvádí některé informace, které vysvětlují jak API podporuje správné bezpečnostní postupy. (15)

ANSI/INCITS 398-2005 Common Biometric Exchange Formats Framework specifikuje soubor datových prvků nezbytných pro podporu běžných biometrických technologií a prvky potřebné k zajištění spolupráce mezi aplikačními programy a systémy od různých dodavatelů. (16)

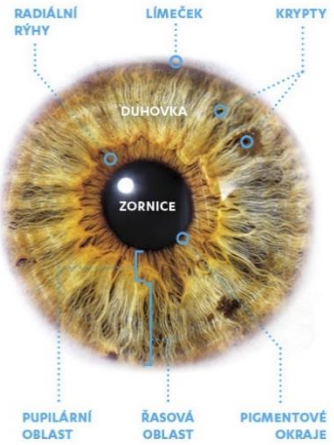
5.1 Oční duhovka

Jedna z metod biometrické identifikace je založena na snímání duhovky lidského oka. Duhovka leží v přední části oka (Obr. 6) a má tvar kruhového terčíku s kruhovým otvorem uprostřed – zornice (pupila), je to barevná část oka pozorovatelná pouhým pohledem. V duhovce jsou pigmentové buňky (melanin), které svým množstvím a hloubkou uložení určují její barvu. (17) Duhovka se dá rozdělit na vnitřní (pupilární) a vnější (řasovou) oblast. V obou lze nalézt krypty, límečky, rýhy a další znaky (Obr. 7), které dohromady tvoří unikátní strukturu. (18)

Duhovka oka každého jedince se vyznačuje svou jedinečností vůči ostatním osobám, dokonce i obě duhovky osoby jsou rozdílné a nalezení dvou identických duhovek je mnohonásobně méně pravděpodobné než nalezení dvou identických daktyloskopických otisků prstu, tudíž neexistuje spolehlivější a více rozlišovací metoda. (19)



Obr. 6 Anatomie lidského oka (17)



Obr. 7 Struktura duhovky (20)

Normy

Identifikace oční duhovkou podléhá normám ISO/IEC 19794-6:2011 Iris image data a ANSI/INCITS 379-2004 Iris Image Interchange Format.

ISO/IEC 19794-6:2011 a její doplňky specifikují dva formáty pro výměnu dat duhovky. První umožňuje ukládat téměř nezpracovaná data, druhý se zabývá daty, která prošla zpracováním. Norma nestanovuje požadavky na optické specifikace kamer, na fotometrické vlastnosti obrázků duhovky a na proces zápisu, pracovní postup a používání zařízení pro duhovku. (21)

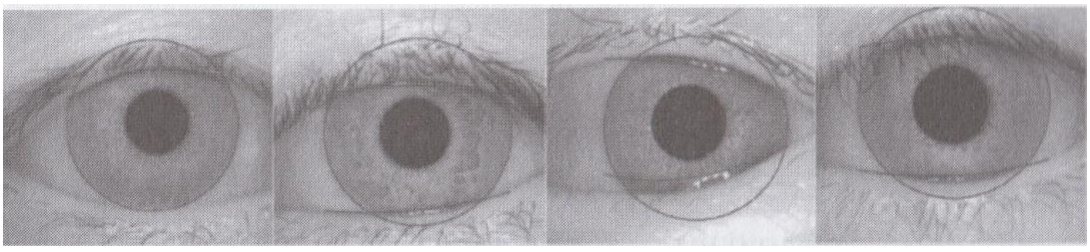
ANSI/INCITS 379-2004 udává dva formáty pro výměnu snímků využívaných k rozpoznání duhovky. Jeden je založen na přímočarém (kartézském) a druhý na polárním souřadnicovém systému. (22)

Postup autentizace

Pro zachycení snímku oka se využívá zařízení obsahující kameru s IR osvětlením, které melanin odráží a na snímku se tak vytvářejí detailní obrazy struktury duhovky, toto osvětlení je také pro uživatele příjemnější než viditelné světlo. (23) Získaný snímek je černobílý, vyznačující se vysokým rozlišením. (2, s. 136)

V prvním kroku zpracování systém lokalizuje ve fotografii duhovku (hranice křivky) (Obr. 8), která musí být velmi kvalitně nasnímána, aby mohla být namapována do fázových diagramů, kde jsou obsaženy informace o pozicích, orientaci a počtu specifických identifikačních rysů. (4, s. 182)

Dalším krokem je lokalizace víčka (Obr. 8), provádí se obdobným způsobem jako vyhledání duhovky, v tomto případě jsou ale zjišťovány pozice horního a dolního víčka. Následně je každý bod uvnitř duhovky mapován do polárních souřadnic a realizuje se kódování duhovky. Kód obsahuje 256 bytů a jeho velikost je 8 x 32 bytů. (4, s. 182, 186)

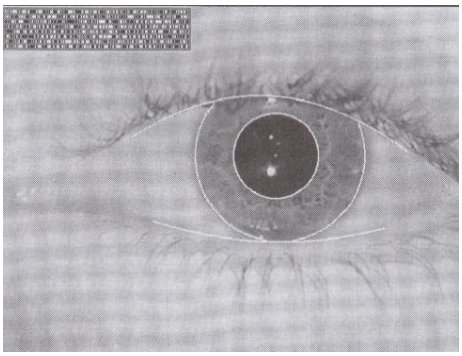


Obr. 8 Příklady lokalizovaných duhovek a víček (4, s. 184)

Porovnání je provedeno výpočtem Hammingovy vzdálenosti mezi oběma kódy duhovek, tato vzdálenost je dána jako suma exkluzivních součtů (XOR) mezi jednotlivými byty:

$$HD = \frac{1}{N}\Sigma_{j=1}^{N} A_j \otimes B_j,$$

kde N = 2048 (8x256), pokud není duhovka zastíněna víčkem. Pokud ano, jsou pro výpočet použity pouze platné oblasti kódu. Jsou-li oba porovnávané vzorky získané z jedné duhovky shodné, je Hammingova vzdálenost rovna či blízká nule. (4, s. 186) Příklad kódu duhovky zobrazuje obr. 9.



Obr. 9 Příklad kódu duhovky (1, s. 494)

Využití v praxi

Metoda identifikace duhovkou oka je velmi hojně využívaná na letištích, pro svou vysokou bezpečnost jsou tyto systémy nasazovány pro řízení přístupu v jaderných elektrárnách, věznicích nebo bankovních trezorech. Některá zařízení mohou být použita i pro umožnění vstupu do domu a informačních systémů. (1, s. 510)

Výhody a nevýhody

Výhodami použití duhovky v biometrických systémech jsou:

- stabilnost a neměnnost duhovky během života,
- uživatelská přijatelnost pořizování snímku,
- chráněnost duhovky proti vnějším vlivům,
- vysoká míra biometrické entropie (míra neuspořádanosti) informace,
- přirozená obrana vůči podvodům, systém nelze přelstít fotografií ani skleněným okem,

- malá velikost šablon. (4, s. 187) (19)

Nevýhodami jsou:

- nezahrnuje-li systém zjištění životnosti, systém může být podveden fotografií,
- předsudky uživatelů,
- nutná spolupráce uživatele,
- vysoké náklady na pořízení systému,
- možnost zneužití naskenovaného vzorku ke zjištění zdravotního stavu osoby,
- některé nemoci a operace mohou změnit vzhled duhovky. (4, s. 187)

5.2 Tvář

Obličej obsahuje poměrně velké množství specifických znaků, které obličeje od sebe navzájem odlišují. Problém použití této metody nastává při stárnutí osoby a u jednovaječných dvojčat s téměř identickými obličeji. (24) Při identifikací tváří jsou využívány dva možné způsoby získání obrazu obličeje, 2D a 3D. Metody jsou založeny na měření vzdáleností mezi specifickými body, 3D využívá ještě hloubky bodů. (25)

Normy

Identifikace tváří podléhá normám ISO/IEC 19794-5:2011 Face Image Data a ANSI/INCITS 385-2004[R2014] Face Recognition Format For Data Interchange.

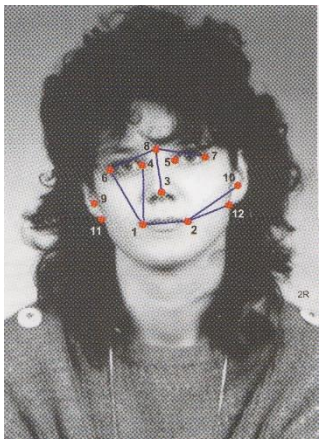
ISO/IEC 19794-5:2011 specifikuje formát záznamu pro ukládání, nahrávání a přenos informací z jednoho nebo více obrazů obličeje nebo krátkého videa. Určuje také omezení scény obrazu obličeje, jeho fotografické vlastnosti, vlastnosti digitálního obrazu a poskytuje nejlepší postupy pro fotografování tváří. (26)

ANSI/INCITS 385-2004[R2014] určuje definice vlastností fotografií (pozadí, postoj, ohnisko, aj.), vlastnosti digitálního obrazu a formát pro výměnu dat. (27)

Postup autentizace

Při užití 2D identifikace se využívá znalostí antropometrie (viz kapitola 7.1.1). V první fázi rozpoznání je detekování obličeje na snímku, je zde třeba brát v úvahu různé osvětlení, barvy, pozice i výrazy, také může být na snímku více osob. Následně jsou vzorky pro vyšší spolehlivost porovnání normalizovány, tj. výřezy jsou navzorkovány do stejných rozměrů, obličej je extrahován z pozadí, jsou nalezeny význačné body. (4, s. 155, 160)

Jednou z metod rozpoznání je nalezení 12 bodů nacházejících se na očích, ústech, nosu a uších (vnitřní a vnější koutky očí, horizontální koutky rtů, špička nosu, přechod nosu do čela, spojení ušního lalůčku a tváře, body na chrupavce ucha) (Obr. 10). Tyto body se spojí úsečkami, kterým se změří délka, podle poměrů těchto bodů a délek se vytvoří šablona obsahující body a hrany mezi nimi. Tyto šablony se porovnávají pro následné rozpoznání tváře. (28)



Obr. 10 Nalezené markanty obličeje (1, s.309)

Pro 3D identifikaci se využívají speciální zařízení, fungující na bázi 2,5D skeneru. Z toho je získán 2D obraz, který má pro každý bod uloženou informaci o jeho hloubce a reprezentují se tak prostorová data. Z více skenů je následně sestaven plný 3D model. K identifikaci pak může sloužit i hloubková mapa – shluk bodů, kde jejich intenzita odpovídá vzdálenosti v prostoru. I při této metodě je třeba obraz normalizovat – detekováním nosu a koutků očí.

Identifikace se následně provádí porovnáním podobností 3D modelů, tvaru a vzhledu nebo hloubkových map. (4, kap. 8.4)

Využití v praxi

Metoda identifikace tváří je využívána na letištích a hraničních kontrolách (pasy, doklady), pro přístup k výpočetním a telekomunikačním systémům, jako přístupové systémy do budov a docházkové systémy, ochrana vládních objektů, finančních institucí, hotelů, aj.. Kriminalistika rozpoznání tváře aplikuje v bezpečnostních aplikacích nebo při sledování osob. (1, s. 13) Běžní uživatelé technologií se s touto metodou setkávají při odemykání svých mobilních telefonů (iPhone, Samsung, Xiaomi, Huawei, LG, Asus, aj.) nebo na sociálních sítích (automatické návrhy označování osob na Facebooku).

Výhody a nevýhody

Výhodami jsou:

- přijatelnost pro uživatele,
- jednoduchost snímání,
- u 2D nízká cena,
- proveditelnost snímání na dálku. (29)

Nevýhody zahrnují:

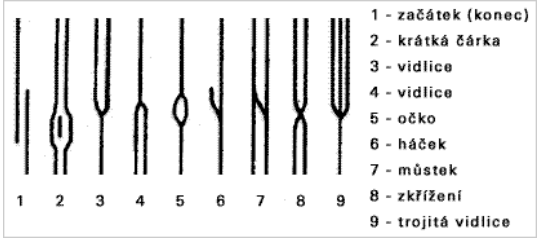
- možnost oklamat 2D identifikaci, která nevyužívá mimiku, fotografií,
- nemožnost nasazení metody v zemích zakazujících fotografování nebo přikazujících zahalení obličeje (25)

5.3 Daktyloskopické otisky

Tato metoda je nejspíš pro veřejnost nejznámější ze všech. Na dlaních, bříškách prstů ruky a na ploskách a prstech nohou se nacházejí vyvýšené reliéfy kůže, tzv. papilární linie. Jejich průběh je jedinečný u každé osoby (i u jednovaječných dvojčat). Papilární linie se vyvářejí během vývoje plodu, po narození již zůstává jejich struktura stejná, jejich velikost je závislá na pohlaví a věku, proto lze z otisku zjistit informace o pohlaví a přibližném věku osoby. (30)

Při identifikaci otiskem prstu jsou využívány jeho markanty. Otisk prstu má tři základní vzory seskupení papilár, jsou jimi oblouk (arch), smyčka (loop) a vír (whorl) (Obr. 11). Dalšími markanty jsou menší obrazce, které linie vytváří (Obr. 12). (31)

Obr. 11 Základní vzory seskupení papilárních linií (32)



Obr. 12 Základní znaky vytvářené papilárními liniemi (33)

Otisk lze získat různými způsoby – pomocí inkoustu a papíru, statickým snímáním (přiložení prstu k senzoru) nebo snímáním šablonováním (přejetí prstem přes senzor). (31) Také existují různé druhy snímačů, které obraz otisku získávají. Jsou jimi:

- **optoelektronické –** princip založený na rozdílném odrazu světla, snímač zachycuje zobrazení otisku pomocí viditelného světla (fosfor), které osvětluje plochu prstu, od papilárních linií se světlo odráží, od rýh nikoli, čímž vznikne výsledný obraz otisku,
- **kapacitní** – tyto snímače využívají rozdílu kapacity mezi deskou snímače a povrchem prstu, jelikož papiláry k podložce přiléhají více než rýhy a mají vyšší kapacitní odpor, pro načtení obrazu se prst přikládá na citlivou plochu osazenou velkým množstvím elektrod, které převedou otisk na digitální obraz,
- **teplotní** – pro získání otisku teplotním snímačem se využívá malý citlivý čip (pyrodetektor), který snímá rozdíl teplot mezi papilárními liniemi a prostorem mezi nimi, přes který je třeba přejíždět prstem, tím se získá obraz ve formě digitálních pásů, které se seskládají do výsledného obrazu otisku,
- **elektroluminiscenční** – zde se využívá speciální vrstva reagující na tlak způsobený luminiscenčním efektem, tato vrstva je světlo-eliminující a filtruje světlo z míst, kde je tlak papilárních linií,
- **radiofrekvenční** – způsob fungování spočívá v připojení generátoru střídavého signálu na dvě rovnoběžné desky (plocha snímače a plocha otisku), odrazem od otisku dopadá signál na senzory různou silou signálu, čímž se získá obraz otisku,
- **multispektrální** – tato technologie je schopna snímat vlastnosti i pod povrchem kůže, systém se skládá ze zdroje světla a zobrazovacího systému, který využívá více osvětlovacích soustav o rozdílných vlnových délkách, světlo projde pod povrch kůže a umožní tak získat více identifikačních údajů z prstu. (34)

Normy

Identifikace oční duhovkou podléhá normám ISO/IEC 19794-3:2006 Finger pattern, ISO/IEC 19794-4:2011 Finger image data, ISO/IEC 19794-2:2011 Finger minutiae data, INCITS 377- 2009[R2014] Finger Pattern Data Interchange Format, ANSI/INCITS 378-2004 Finger Minutiae Format For Data Interchange a ANSI/INCITS 381-2004 Finger Image-Based Data Interchange Format.

ISO/IEC 19794-3:2006 specifikuje požadavky na reprezentaci lokálních nebo globálních spektrálních dat odvozených z obrazu otisků prstů. (35)

ISO/IEC 19794-2:2011 popisuje pravidla pro určování markantů na otiscích prstů, případně doplňujících informací, zabývá se třemi formáty výměny dat – záznamový, normální a kompaktní pro ukládání dat na smart karty. (36)

ISO/IEC 19794-4:2011 specifikuje formát výměny dat obrazu jednoho nebo více otisků prstů či otisku dlaně. (37)

INCITS 377- 2009[R2014] specifikuje formát výměny dat pro otisky prstů, popisuje také proces zpracování dat. (38)

ANSI/INCITS 378-2004 obsahuje popis reprezentace otisku prstu založený na markantech, definuje umístění markantů v otisku, formát záznamu a nepovinné informace. (39)

ANSI/INCITS 381-2004 definuje formát výměny obrazových dat otisku prstu a dlaně. (40)

Postup autentizace

Prvním krokem zpracování obrazu otisku je zvýraznění papilárních linií, upravený obraz se převede do černobílé škály, následuje ztenčení linií na tloušťku pod 1 pixel. Následně jsou stanoveny markanty.

Množinu markantů může systém porovnat s jinou množinou a stanovit pravděpodobnost shody dvou otisků prstů. Je třeba brát v úvahu i možné změny způsobené opotřebením, nemocí či mechanickým poškozením. Jednou z vlastností, která také určuje možnost přijetí nebo odmítnutí je životnost snímané části. (30)

Využití v praxi

Tato metoda identifikace je velmi často využívána výrobci mobilních telefonů (iPhone, Samsung, Xiaomi, Huawei, LG, Asus, aj.) a notebooků a počítačů, kteří zařazují snímač otisku prstů pro řízení přístupu do zařízení. Další využití má otisk prstu v kriminalistice při identifikaci nejen osob spojených s trestnou činností. Otisky se využívají i v komerční sféře jako docházkové či přístupové systémy do objektů, mohou nahradit i klíč od bytu či domu. Otisky prstů jsou obsaženy i v nově vydávaných cestovních pasech a mohou být kontrolovány na letištích. (4, s. 116)

Výhody a nevýhody

Výhodami jsou:

- uživatelská akceptovatelnost,

- spolehlivost,
- vysoká biometrická entropie,
- vyspělost technologie,
- minimální velikost. (4, s. 122)

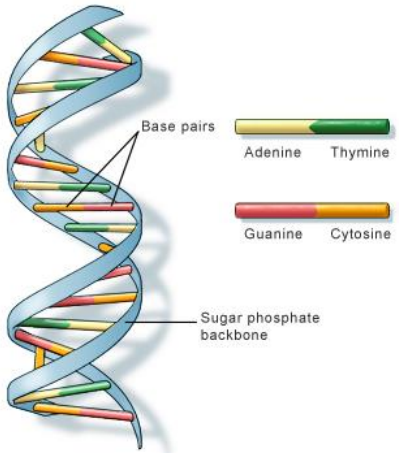
Nevýhody zahrnují:

- nutnost kontaktu se zařízením,
- zanechávání otisku na statických snímačích,
- snadnost získání otisku.

5.4 DNA

DNA, dvojitě točená spirálová molekula tvořící kroucený žebřík (Obr.13), je nejspolehlivějším biometrickým údajem, jež nachází v současné době využití především v oblasti kriminalistiky a nikoli komerční sféře a nese naše genetické informace. K identifikaci lze využít krev, sliny i jiné tělesné tekutiny, z nichž lze poznat, kdo osoba je, barva vlasů, přibližný věk, výška postavy nebo barva očí. (41)

K rozlišení se využívá tzv. regionů – STR (Short Tandem Repeats), složených z opakujících se sekvencí (posloupnost písmen, A C G T, představujících strukturu vlákna DNA). V současnosti je těchto regionů 13. (4, s. 270)



Obr. 13 Struktura DNA (42)

Normy

Identifikace pomocí DNA podléhá normě ISO/IEC 19794-14:2013[2013] DNA data, která je ve stejném znění využívána i pro normu INCITS.

INCITS/ISO/IEC 19794-14:2013[2013] specifikuje formát výměny dat pro výměnu dat DNA pro identifikační a verifikační technologie využívající tuto biometrickou vlastnost. Tento standard umožňuje také reprezentaci dat pro více DNA technik v jediném záznamu pro daný subjekt, není určen pro jiné účely než výměna DNA pro biometrické ověřování a identifikaci jednotlivců; zejména nevyměňuje lékařské a jiné zdravotní informace. (43)

Postup autentizace

Proces autentizace pomocí DNA zahrnuje tři části – extrakci, kopírování a sekvencování. Při extrakci se různými metodami získá a izoluje vzorek DNA, který je následně kopírován, aby se počet vzorků zvýšil na množství dostatečné pro sekvencování. Sekvencování je krok, při kterém se získá unikátní kód nukleové kyseliny z DNA vzorku. Následný obraz vzorku je získán pomocí genetického analyzátoru, do kterého je získaná DNA nahrána, tento analyzátor má fluorescenčně označené komponenty A, T, C a G. K systému je připojen elektrický proud a části DNA rostou kolem laseru, ty části, které pošly laserem, jsou nahrány a výsledně je vytvořen profil DNA, který může být porovnáván s dříve získanou šablonou. (4, kap. 13.3) V současnosti existují již zařízení, která proces identifikace za pomoci DNA provedou i za kratší dobu než dříve, přibližně 90 minut. (44)

Využití v praxi

Hlavní využití nachází DNA ve forenzních vědách a to nejen k identifikaci osob, ale i ke zjištění příbuzenských vztahů, zjištění některých přibližných vzhledových vlastností osob. Možnost zjištění příbuzenských vztahů využívají i lidé v běžném životě, např. při zjištění paternity nebo pro dědické řízení. Další oblastí, kde se uplatňuje genetická analýza DNA, je archeologie, kdy se ověřují různé hypotézy. (1, kap. 18.5)

Výhody a nevýhody

Výhodami jsou:

- vysoká individualita a unikátnost,
- vysoká spolehlivost,
- snadná dosažitelnost vzorku,
- neměnnost,
- velmi špatná falzifikovatelnost. (4, kap. 13.3)

Nevýhody zahrnují:

- špatná akceptovatelnost uživateli,
- nepřijatelná doba identifikace pro komerční sféru,
- možný zásah do soukromí osob (fyzický stav, nemoci, aj.),
- nemožné provedení identifikace v reálném čase,
- proces zpracování není zcela automatizován,
- jednovaječná dvojčata mají stejnou DNA,
- zanechávání vzorků. (4, kap. 13.3)

5.5 Hlas

Hlas, zvuk vytvářený hlasivkami, je jedinečnou biometrickou vlastností, jejíž individualita je dána tvarem hlasivek, ústní dutiny, jazyka a zubů. (45) Existují dva způsoby autentizace:

- nezávislá na textu (text independent) – kdy hlasové ověření není závislé na vyřčeném obsahu,
- závislá na textu (text dependent) – analýza se provádí na předem uložené frázi, která je při každém ověřování stejná, nebo systémem určené frázi, kdy je vytvářena náhodná přístupová fráze.

Na získaném vzorku se analyzují jedinečné vokální vlastnosti, jako jsou doba trvání, intenzita nebo dynamika. (46)

Normy

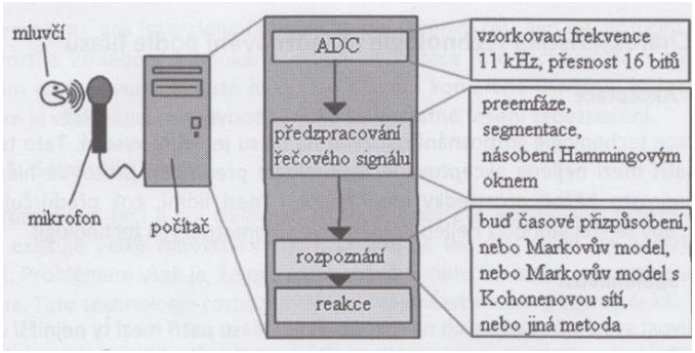
Identifikace pomocí hlasu podléhá normě ISO/IEC 19794-13:2018 Voice data.

ISO/IEC 19794-13:2018 specifikuje formát výměny dat, který může být použit pro ukládání, nahrávání a přenos digitalizovaných akustických dat lidského hlasu (řeči), o nichž se předpokládá, že pocházejí od jedné osoby a jsou nahrané během jedné relace. (47)

Postup autentizace

Vzorek pro porovnání, který se dále analyzován, je získán nahráním uživatelova hlasu do mikrofonu. Prvním krokem zpracování řečového signálu je segmentace, stanoví se maximální délka signálu a signál je následně rozdělen na segmenty, které mají právě maximální stanovenou délku. Důležité je, aby se segmenty překrývaly, aby nezanikly některé krátké nebo nevýrazné hlásky. Další fází je preemfáze, což je předzpracování signálu

za pomoci digitální horní propustnosti, kdy se posiluje oblast vyšších frekvencí a snižuje se vliv základního tónu řeči u znělých hlásek. Následně se signál vahuje – násobí oknem (signál se z obou stran ořízne). Pro další analýzu se využívají ještě základní příznaky, jako jsou energie signálu nebo počet průchodů nulou. Proces zpracování signálu zobrazuje obr. 14.



Obr. 14 Cyklus zpracování hlasového signálu (4, s. 227)

Jelikož řeč je dynamická, hodí se pro její rozpoznávání dynamické metody (skryté Markovovy modely, neuronové sítě). (4, kap. 10)

Využití v praxi

Růzností hlasových projevů osob se využívá v kriminalistické audioexpertize. Při té může docházet k identifikaci neznámé osoby (výhružné telefonáty), typování pachatele, identifikaci obsahu nahrávky nebo určení její autentičnosti. (1, s. 459) V komerční sféře nachází verifikace hlasem uplatnění při řízení přístupu.

Výhody a nevýhody

Výhodami jsou:

- nízká cena,
- dostupnost v mobilních telefonech,
- možnost integrace do zařízení (automobily, domácí spotřebiče),
- vysoká akceptovatelnost uživateli,
- bezkontaktnost.

Nevýhody jsou:

- vysoká míra nepřesnosti,
- nutnost detekce životnosti,
- vliv okolního prostředí na kvalitu vzorku. (46)

5.6 Podpis

Podpis je z části statickou a z části dynamickou biometrickou vlastností, záleží na druhu snímání. Rozlišují se dva typy systémů – off-line a on-line. V případě off-line systému předává osoba vzorek svého podpisu systému napsanou na papíře, z něhož je následně digitalizován. Při verifikace v on-line systému jsou charakteristiky podpisu získány v reálném čase pomocí speciálního tabletu, snímacího pera nebo jiného snímacího HW. (1, s. 439)

Normy

Identifikace pomocí podpisu podléhá normám ISO/IEC 19794-7:2007 Signature/sign time series data, ISO/IEC 19794-11:2013 Signature/sign processed dynamic data a ANSI/INCITS 395-2005 Signature/Sign Data.

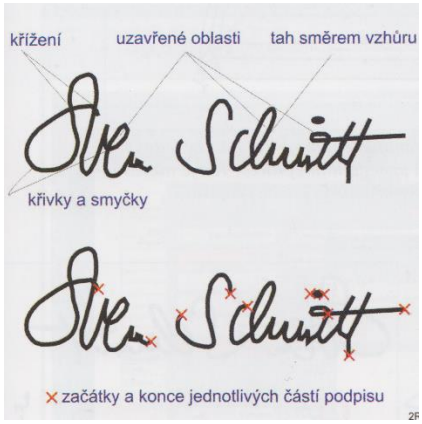
ISO/IEC 19794-7:2007 popisuje dva formáty výměny dat pro podpis a písmo. První je obecný formát, druhý je kompaktní, který lze využít pro smart karty. (48)

ISO/IEC 19794-11:2013 pro účely biometrického porovnání specifikuje obecný formát výměny dat pro zpracované podpisové/znakové údaje o chování získané z časové řady zachycené pomocí zařízení. (49)

ANSI/INCITS 395-2005 specifikuje formát výměny dat pro digitalizované písmo nebo podpis pro účely biometrického zápisu, verifikace nebo identifikace. Tento formát je obecný a může být využit v široké škále aplikací využívajících elektronický podpis. (50)

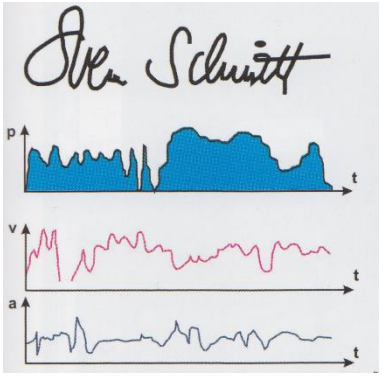
Postup autentizace

Verifikace v off-line systému se skládá ze tří etap – předzpracování, extrakce biometrických charakteristik a vyhodnocení. Během předzpracování jsou provedeny některé algoritmy, jako jsou vyhlazování, zjednodušení, či normalizace. Extrakce probíhá různými způsoby, jedním z nich je zjištění geometrických a topologických rysů – uzavřené smyčky, speciální body nebo místa křížení (Obr. 15). Výsledné vyhodnocení je založeno na vyhodnocování vektorů charakteristik, může být provedeno porovnáním významových bodů, klasifikátorem sousedů nebo neuronovou sítí. (1, kap. 13.7)



Obr. 15 Statické charakteristiky podpisu (1, s. 441)

V případě on-line verifikace jsou pomocí HW získány kromě statických i dynamické charakteristiky – rychlost psaní, tlak pera, pořadí psaní jednotlivých částí apod. Již v průběhu psaní podpisu jsou získávány informace o průměrné a maximální rychlosti psaní, měření vlastností zakřivení tahů, poměr dlouhých a krátkých tahů, různé délky segmentů podpisu aj.. V každém časovém okamžiku vzniku podpisu jsou popisovány časovou funkcí další dynamické charakteristiky – souřadnicové pozice hrotu psacího nástroje, rychlost (v), zrychlení (a) a tlak hrotu na podložku (p) (Obr. 16). Následně jsou získané charakteristiky porovnávány se šablonou uloženou v databázi, získá se tak míra ztotožnění. (1, kap. 13.8)



Obr. 16 Dynamické vlastnosti podpisu: p - tlak pera, v - rychlost, a - zrychlení (1, s. 445)

Využití v praxi

Autentizace podpisem může být prováděna na denním pořádku, nejen za použití elektronických zařízení. Často ji provádí notáři, při ověření pravosti podpisů nebo závětí a jiných důležitých ručně psaných dokumentů. Písmoznalectví, expertiza ručního písma, nachází uplatnění i v kriminalistice nebo historických vědách při zjišťování a potvrzování autorů podpisů a psaných textů.

Výhody a nevýhody

Výhodami jsou:

- míra přijatelnosti uživateli,
- bezproblémovost z právního a náboženského hlediska,
- nízká náročnost na vybavení.

Nevýhodami jsou:

- nepřesnost,
- ovlivnění psychickým a zdravotním stavem osoby,
- off-line identifikaci lze podvrhnout fotografií podpisu. (4, s. 244)

5.7 Geometrie ruky

Systémy založené na geometrii ruky využívají poznatku, že ruka každého jedince je jinak tvarovaná a tento tvar se nemění. Tato zařízení pracují s 2D nebo 3D obrazem ruky a k rozlišení jedinců se používají charakteristiky ruky – délka, šířka a výška prstů, zakřivení a lokální anomálie.

Geometrie využívá pohled shora a z boku, k zachycení snímku se nejčastěji využívá běžná kamera s podložkou, na které jsou kolíky sloužící k přesnému umístění prstů. Tato podložka také reflektuje dopadající světlo a zvyšuje kontrast mezi rukou a podložkou. Některá zařízení využívají ještě zrcadlo, které pod úhlem 45° promítá do kamery i boční profil ruky. (4, s. 126)

Normy

Identifikaci geometrií ruky jsou nadřízené normy ISO/IEC 19794-10:2007 Hand geometry silhouette data a ANSI/INCITS 396-2005 Hand Geometry Interchange Format.

ISO/IEC 19794-10:2007 specifikuje formát dat pro 2D geometrii ruky, sestává se z množství povinných i volitelných dat (parametry při snímání geometrie, standardizovaná pozice ruky, aj.) (51)

ANSI/INCITS 396-2005 norma určuje formát pro výměnu dat geometrie ruky ve formátu siluety. Definuje obsah, formát a jednotky měření pro tyto informace. (52)

Postup autentizace

Metod rozpoznávání osob podle geometrie ruky je více, patří sem přímé měření, zarovnání rukou, analýza šířky prstů nebo 3D geometrie ruky.

Metoda založená na přímém měření zjišťuje všechny významné rozměry na snímku. Ze snímku musí být nejprve odstraněny distanční kolíky, následně jsou měřeny délky prstů, šířky prstů v různých místech, šířka dlaně aj., jednotlivé délky slouží jako konečné příznaky, z nichž je vytvořena šablona. (4, s. 128)

Při metodě, jejíž princip je zarovnání rukou, jsou ruce natočeny do předem definované polohy a měří se rozdíly mezi vzorem a šablonou. Postup je prováděn v několika krocích – odstranění distančních kolíků, extrakce kontury, extrakce a zarovnání prstů, výpočet párových vzdáleností a samotná verifikace. (4, s. 130)

Třetí metoda využívá analýzu šířek jednotlivých prstů lidské ruky. Postup je následovný – obraz ruky se oddělí od pozadí a nalezne se hlavní osa ruky, která se vypočítá pomocí vlastních vektorů matice setrvačnosti. Druhá osa, kolmá na hlavní, rozděluje ruku na prstovou oblast a zbylou část. Následně je provedena analýza okraje prstu, jsou nalezeny špičky prstů a údolí mezi prsty, na jejichž základě je obraz rozdělen na jednotlivé prsty. Každý bod na okraji prstu je promítnut na osu prstu a jsou spočítány všechny vzdálenosti bodů od osy, z nichž je vytvořen histogram, který musí být normalizován. Výsledkem procesu je pravděpodobnostní rozložení těchto délek. (4, s. 130, 131)

U způsobu, který pracuje s 3D obrazem ruky, dochází k extrakci rysů na celém povrchu ruky, reprezentovaném množinou parametrů popisujících geometrii ruky. Snímek se získává za pomoci strukturovaného světla a běžné kamery. Z deformace linií jsou odhadnuty polohy bodů v prostoru. Po zrekonstruování jsou extrahovány příznaky, k čemuž se v současnosti používají povrchy jednotlivých prstů. Prsty jsou lokalizovány a následně jsou určeny jejich šířky a průměrné zakřivení v různých částech. Porovnání se nejčastěji provádí výpočtem vzdáleností vektorů příznaků. (4, s. 133)

Využití v praxi

Tato metoda je využívána výhradně v bezpečnostně-komerční sféře pro účely verifikace, pro využití k identifikaci obsahuje příliš málo informací. Je nasazována pro řízení přístupu nebo jako docházkový systém v prostorách a objektech s omezeným a známým počtem osob,

jako jsou režimová pracoviště, výrobní závody, obchodní domy, sportovní a jiné kluby nebo zábavní průmysl. (1, s. 272)

Výhody a nevýhody

Výhodami jsou:

- dobrá akceptovatelnost uživateli,
- lehká použitelnost,
- odolnost vůči vlivům prostředí,
- relativně nenákladné zařízení.

Nevýhodami jsou:

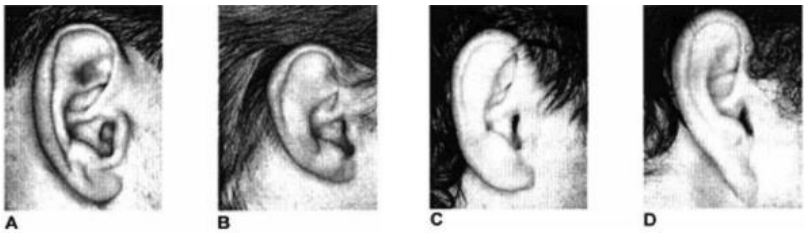
- nízká rozlišovací schopnost,
- vhodné využití je pro menší počet osob,
- velikost zařízení,
- nošení šperků snižuje kvalitu rozpoznání. (4, s. 134)

5.8 Ostatní metody

5.8.1 Tvar vnějšího ucha

Vnější ucho se skládá z chrupavky, jejíž růst probíhá v prvních 4 měsících vývoje plodu, poté se pouze zvětšují proporce. Každý jedinec má ucho specificky tvarované a jedinečné, vnější ucho se tak stává biometrikou vhodnou pro použití k identifikaci nebo verifikaci. Jsou rozlišovány čtyři základní tvary vnějšího ucha – oválný, kulatý, obdélníkový a trojúhelníkový (Obr. 17).

Podle Iannarellisova systému se při použití vnějšího ucha k identifikaci vytvoří snímek, který se rozdělí na 8 částí po 22,5 stupních, kdy střed se nachází v centru zvukovodu a vyhodnocuje se dvanáct charakteristik (vzdálenosti od bodu 10) (Obr. 18). Další metody využívající ucho k identifikaci jsou termogram, grafový model a 3D tvar ucha. (53) (4, s. 253) (25) (41)



Obr. 17 Základní tvary vnějšího ucha (53)

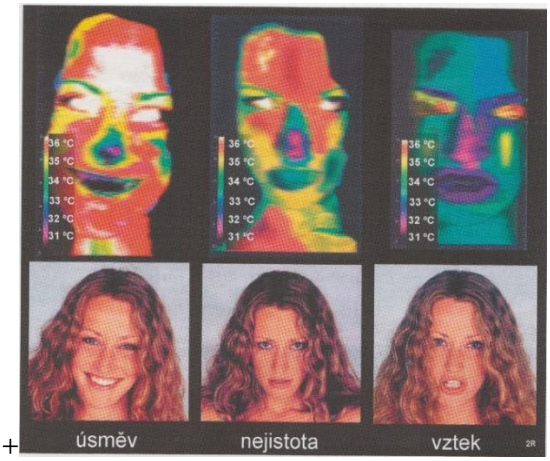
Obr. 18 Udávané geometrické charakteristiky dle Iannarilliho (53)

5.8.2 Termogram obličeje

Tvář každého jedince obsahuje husté krevní řečiště (cévy, žíly, kapiláry), které mají výrazně vyšší teplotu než jeho bezprostřední okolí, k identifikaci se tak používají snímky obličeje, které zobrazují rozložení tepla v obličeji. (1, s. 343) Pro snímání termosnímků jsou využívány termokamery, při jejichž použití je třeba dodržovat předepsané parametry – konstantní vzdálenost, pro správné zaostření, relativní vlhkost a teplota okolí. (4, s. 174)

Termokamera vytvoří záznam, tzv. termomap, ve kterém se hledá pozice očí, úst, nosu a hran obličeje, k čemuž je využíván právě odraz tepla. Po nalezení pozic, se získaný snímek v překryvu porovnává s dříve získanou šablonou a je hledána shoda. (4, s. 174) Stejný princip lze využít i u krevního řečiště na ruce. (1, s. 343)

Výhodou termosnímku je získání stejné kvality obrazu i při špatných světelných podmínkách a velká složitost vytvoření falzifikátu. Bohužel jsou snímky závislé na proměnlivosti teplot v obličeji v závislosti na aktuální aktivitě, emocích (Obr. 19) i teplotě okolí. Výrazně lepších výsledků v používání se dosahuje v kombinaci s běžnými snímky obličeje. (4, s. 175)



Obr. 19 Snímky tváře při různých emocích (1, s.384)

5.8.3 Topografie žil ruky

Tuto metodu lze provádět pomocí snímaní krevního řečiště na hřbetu, dlani nebo prstu ruky. (54) Jednou z vlastností, která umožňuje použití krevního řečiště jako biometrické metody, je neměnnost v průběhu života, další je uložení žil pod kůží, což ztěžuje vytvoření funkčního falzifikátu. (25)

Osoba při identifikaci přikládá snímanou část ruky ke scanneru s infračerveným zářením, který partii ozáří (IR záření umožňuje získání snímku bez ohledu na světelné podmínky či špínu). (25) Systém získá obraz zachycující rozložení žil, které se v obrazu projevují tmavou barvou (pohlcují dopadající záření) (Obr. 20). Z obrazu se získávají vlastnosti, jako jsou úhly mezi žílami, vzdálenosti, délky a jiné, které slouží pro biometrickou analýzu a identifikaci či verifikaci. (54)

Obr. 20 IR snímek dlaně (4, s. 146)

5.8.4 Dentální obraz

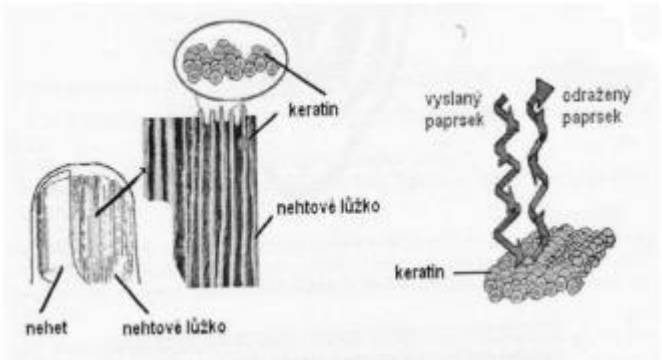
Identifikace osob na základě chrupu je způsob využívaný především v případech mrtvol, kdy nelze tělo identifikovat jinou biometrickou metodou. Člověk má obvykle 32 zubů, které se v průběhu života mohou poškodit, zkazit a zaplombovat, odstranit a nahradit zubní náhradou. Jakékoli zásahy do chrupu zvyšují množství kombinací a různých sestav zubů v čelisti, ale i pouhé rozdíly ve velikostech, tvarech, orientaci či počtu a tvaru kořenů jsou dostatečné k rozlišení různých osob. Identifikace může být prováděna pomocí rentgenových snímků (Obr. 21), 3D snímků zubů nebo otisků zubů po skousnutí. (4, s. 261–263)

Obr. 21 Rentgenový snímek části chrupu s viditelnými anomáliemi (55)

5.8.5 Snímek lůžka nehtu

Rýhování je vlastnost nacházející se na každém prstu každého člověka a nese záznam o detailních genetických informacích a individualitě jedince. Nehet vyniká svou stabilitou v různém prostředí a snadnou dekontaminací, vyznačuje se také různým vzorkováním u každé osoby a i každého prstu, a je tedy naprosto jedinečný. Proces zkoumání rýhování je, na rozdíl od některých metod, neinvazivní a nedestruktivní metodou. (56)

K samotné identifikaci lůžkem nehtu se nevyužívá přímo rýhování viditelné na nehtu, ale prostor mezi nehtem a nehtovým lůžkem, tvořený keratinem, který způsobuje zvrásnění nehtu samotného a mění orientaci dopadajícího světla (Obr. 22). Ke snímání struktury se používá zdroj polarizovaného světla, kterým se ozáří nehet a zachycují se změny paprsku po odrazu od nehtu (Obr. 22). Po zpracování se získá obraz podobný čárovému kódu, který se porovnává se šablonami uloženými v databázi. (31)



Obr. 22 Struktura nehtu a způsob odrazu paprsku (31)

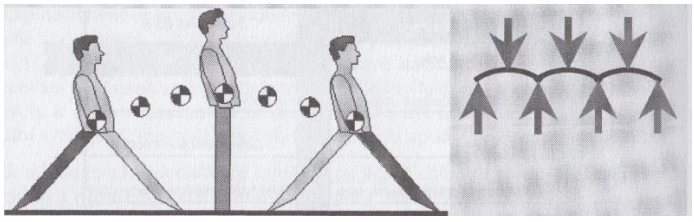
5.8.6 Pach lidského těla

Identifikací osob podle pachu se zabývá obor zvaný odorologie. Pachy jsou tvořeny atomy a molekulami, které se za určitých podmínek odpařují nebo sublimují z různých látek, to způsobuje obtížnosti kriminalisticko-technického zkoumání a tato metoda se v praxi používá velmi omezeně. Pachové stopy jsou v současnosti využívány při práci se speciálně vycvičenými psy, kdy pes může po čichu identifikovat osobu, není ale možné v soudním řízení použít identifikaci psem jako přímý důkaz. (57)

5.8.7 Lokomoce těla

Způsob, jakým člověk chodí – bipedální lokomoce (pohyb dolních končetin), se ustaluje kolem sedmého roku života jedince, kdy každý získá svůj jedinečný styl, který se v průběhu let nemění, neutrpí-li osoba nějakou újmu nebo změnu stavu (těhotenství), která by zapříčinila změnu ve stereotypu chůze. (58)

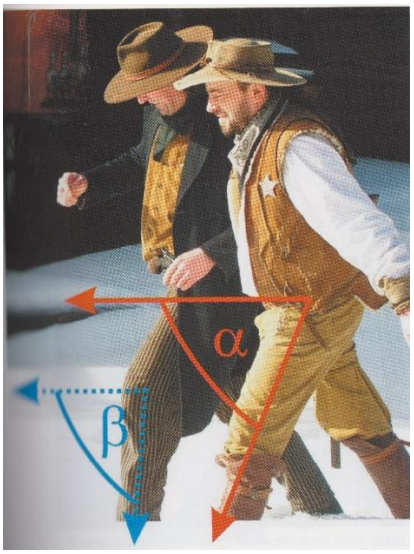
Jednou z metod využití lokomoce k identifikaci je sledování trajektorie těžiště osoby. Důsledkem stavby lidského těla je neschopnost udržet těžiště při chůzi v jedné linii a těžiště tak opisuje vlnící se křivku, to napomáhá rozlišit chůzi jednotlivých osob (Obr. 23). (1, s. 572) Při identifikaci lze ale také využít sledování i jiných částí těla, které se pohybují v podobné trajektorii jako těžiště, jako jsou ucho či hlava nebo středy velkých kloubů (kyčel, koleno, …). (59)



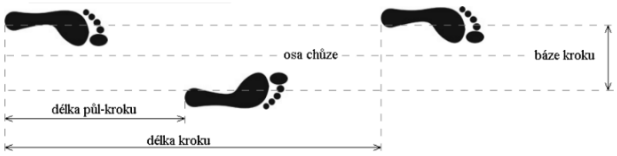
Obr. 23 Zjednodušený pohyb trajektorie těžiště těla (1, s. 572)

Další způsob identifikace se zabývá sagitální kinematikou, měřením úhlu odklonu určité části končetiny od kloubu směrem dolů od předozadní osy, která prochází daným kloubem (Obr. 24). Úhly jsou měřeny po dobu jednoho celého cyklu chůze (Obr. 25) a jsou zaznamenávány do grafů, tyto grafy tak definují charakteristiku chůze osoby. (1, s. 574)

Osoby lze identifikovat i podle siluety, kterou při chůzi vytvářejí, zde se vyhodnocují například délky kontur siluety. (1, s. 577)



Obr. 24 Měření úhlu pohybu v sagitálním směru (1, s. 574)



Obr. 25 Cyklus chůze (60)

5.8.8 Dynamika stisku kláves

Způsob, jakým člověk píše na klávesnici, je jedinečný a často se proto využívá při vícefaktorové autentizaci (spojení dvou ze tří způsobů identifikace – vlastnost, znalost, biometrie). Při identifikaci se analyzuje přirozený rytmus psaní každého jedince, není proto třeba žádné další HW vybavení. (61)

Při zkoumání není důležitý obsah psané zprávy, ale způsob, jakým osoba píše. Zkoumanými rysy jsou celková rychlost psaní, doba stisku klávesy, doba mezi stisky po sobě jdoucích kláves a tlak vyvinutý při stisku na klávesu. (61) (4, s. 246)

Rozlišují se dva druhy verifikace – statická, kdy jsou klávesy analyzovány pouze ve specifikovaný čas a průběžná, kdy se sleduje chování uživatele po celou dobu práce. (4, s. 246)

5.8.9 Oční sítnice

Sítnice je povrch zadní strany oka citlivý na světlo, skládá se z obrovského počtu nervových buněk, které převádějí světelné paprsky na nervové signály a poskytují barevné vidění. (19) Analýza sítnice je jednodušší než u duhovky, zde se hledají pouze vidličky a křížení tvořené cévami, které sítnicí procházejí (Obr. 26). Pozice těchto útvarů je jedinečná pro každou osobu, kterou tak identifikuje. (18)

Obr. 26 Snímek cév za oční sítnicí (62)

Pro získání obrazu se používá zdroj světla s nízkou intenzitou záření a opto-elektrický systém. Naskenovaný obraz se převede do podoby 40 bitového čísla, v tomto formátu se následně sítnice porovnávají. (31)

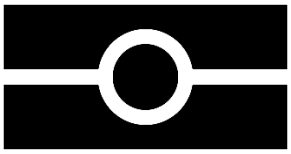
6 Doklady obsahující biometrii

Podle nařízení Rady EU č. 2252/2004 byly všechny členské státy EU povinny zavést do cestovních dokladů první biometrické prvky. Nově vydávané pasy měly do konce srpna 2006 začít obsahovat na čipu biometrického cestovního pasu (ePas) obličej, do konce února 2008 měly přibýt ještě otisky prstů. Tyto biometrické vlastnosti jsou využívány pro ověření autenticity pasů a víz a pro ověření identity držitele pasu. (63)

Cestovní pas (Obr. 27) je cestovním dokladem typu knížka a obsahuje 34 stran, současně vydávané cestovní pasy obsahují nosič dat (čip) s biometrickými údaji. (64) Biometrický pas má tyto následující tři znaky:

- datum vydání po 1. září 2006,
- stránka s osobními informacemi je vyrobena z tuhého plastu,
- přední strana desek obsahuje mezinárodní symbol pro biometrický pas (Obr. 28). (65)

Obr. 27 Biometrický pas (64)



Obr. 28 Mezinárodní symbol biometrického pasu (66)

Obličej

Snímek osoby je pořizován v předním čelném pohledu, tak aby pohled směřoval do objektivu digitálního fotoaparátu. Zobrazení obličeje musí také splňovat technické parametry podle přímo použitelného předpisu Evropských společenství (Čl. 2 písm. c) a čl. 5 odst. 2 nařízení Rady (ES) č. 2252/2004, ve znění nařízení Evropského parlamentu a Rady (ES) č. 444/2009). Fotografie zachycuje osobu s neutrálním výrazem, zavřenými ústy a otevřenýma očima, které nesmí překrývat vlasy. (67)

Otisky prstů

Biometrický cestovní pas obsahuje otisk jednoho prstu z každé ruky. Snímání se provádí nejprve u pravé ruky, začíná se ukazovákem, pokud není vzorek dostatečně kvalitní, pokračuje se palcem, prostředníkem a prsteníkem, dokud není vzorek vyhovující. Stejný postup následuje i u levé ruky. Otisky také musí splňovat technické parametry podle předpisu Evropských společenství a musí se shodovat s otisky prstů pořízenými pro účely ztotožnění bezprostředně po pořízení otisků. V nosiči dat je obsažen údaj o tom, ze kterého prstu byl otisk pořízen a údaje o jeho kvalitě. (67)

7 Biometrie v kriminalistice

Kriminalistika patří mezi vědy, které se významně zasluhují o boj proti kriminalitě, není to ale jediná její funkce. Poznatků kriminalistiky se využívá i při pátrání po osobách, při identifikaci obětí přírodních katastrof nebo dopravních nehod.

Kriminalistika zkoumá zákonitosti vzniku a zániku stop a důkazů a jiných kriminalisticko-relevantních informací, dále také zkoumá zákonitosti shromažďování a využívání důkazů a stop k odhalování, vyšetřování a předcházení trestné činnosti. Tato věda má velmi blízko k trestnímu právu, k technickým a přírodním vědám. (68)

Důležitou roli při objasňování trestné činnosti má již zmiňovaná biometrie, jejíž vývoj má pro kriminalistiku značný přínos. Pro forenzní využití jsou vhodné ty biometrické charakteristiky, které lze zanechat na místě činu – otisky prstů, dlaní, uší, záznam obličeje, pach, vzorek DNA v krvi, písmo nebo záznam hlasu. (69)

7.1 Historie biometrie v kriminalistice

První biometrickou metodou užívanou v kriminalistice byla antropometrie (kapitola 7.1.1), která jako první umožnila určitým způsobem identifikovat zločince. (1, s. 146)

Druhou nejstarší metodou, využívanou pro identifikaci osob v kriminalistické praxi, je daktyloskopie (nauka o obrazcích papilárních liniích), která postupně antropometrii nahradila. (70) Roku 1901 byla daktyloskopická identifikace zavedena ve Velké Británii, o dva roky později i v Německu, postupně daktyloskopii jako významnou identifikační metodu uznala i Francie, v českých zemích byla oficiálně zavedena roku 1908. (71)

Roku 1890 navrhl Alphonse Bertillon další metodu, která získala své místo v kriminalistické identifikaci, fotografování hlavy zločinců z různých stran. Tento návrh se ujal a byl zaveden do praxe. První pachatel v českých zemích byl fotografován v Praze 14. října 1895. Pomocí fotografie lze pak zjistit podobnost s pachatelem. (72)

Další metodou často využívanou v kriminalistice je analýza DNA, která byla pro tyto účely poprvé využita roku 1986 ve Velké Británii k identifikaci vraha dvou mladých dívek, poté se metoda rozšířila i do dalších zemí. Na území České republiky byla poprvé uplatněna v roce 1992. (73)

První případ, kdy bylo ucho, jehož otisk se řadí k trasologickým stopám, použito a uznáno soudem jako důkaz, byl někdy kolem roku 1910, kdy byla prokázána totožnost vězně na fotografii díky zvláštnosti jeho ucha. (74)

Jedny z prvních audioexpertizních zkoumání pro soudní účely se začaly objevovat v 60. letech 20. století v USA a Velké Británii. (1, s. 456) Počátky těchto zkoumání v Kriminalistickém ústavu Praha se nacházejí v roce 1975, kdy Ing. Jan Málek položil základy samostatného pracoviště, definoval metody a specifikoval techniku pro provádění tohoto zkoumání. (75) Využití má tato metoda převážně při odposleších nebo při identifikaci volající osoby.

V první polovině 20. století se začaly objevovat práce, věnující se problematice využívání ručního písma k identifikaci osob. (76) Na KÚP přibyla písmoznalecká expertiza jako samostatný forenzní obor, roku 1950. Do té doby se této metodě věnovali pouze soukromí znalci. (77)

Využití v kriminalistice našla i identifikace pachem (odorologie) či podle chrupu.

7.1.1 Alphonse Bertillon

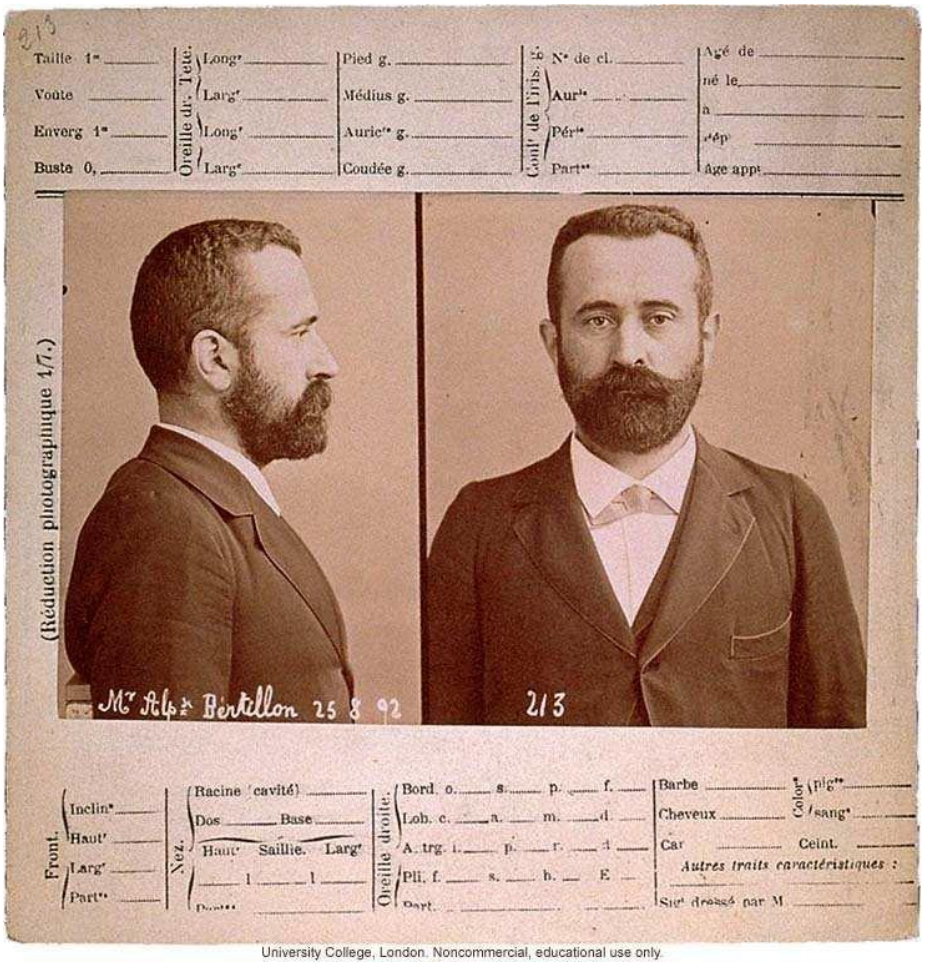
Alphonse Bertillon, jedna z významných osobností historie kriminalistické identifikace, byl francouzský vědec, který se zasloužil o vznik první biometrické metody postavené na vědeckých základech. Metoda se zakládala na měření rozměrů jednotlivých částí lidského těla, antropometrii. (1, s. 146) Počátek Bertillonovy metody se datuje v roce 1879, pařížská policie ji začala v praxi využívat až roku 1883. Poté se rozšířila do celého světa, ale po několika letech byla nahrazena efektivnější a přesnější daktyloskopií. (1, s. 148)

Identifikační metoda byla podložena Quételetovu teorií, která určovala pravděpodobnost shody tělesné výšky dvou lidí poměrem 1:4, při přidání dalších měr se poměr zmenšuje geometrickou řadou a při měření 11 rozměrů dvou zločinců se sníží na 1:4 191 304. (1, s. 151)

Pro svůj způsob identifikace navrhl:

- stručný metodický návod k přesnému měření zvolených částí lidského těla,
- zvláštní záznamový arch pro záznam délek na konkrétní osobě,
- klasifikační strukturu pro řazení záznamů, klasifikaci a rychlé hledání již vytvořených záznamů podle antropometrických měření. (1, s. 149)

Tento způsob identifikace umožnil policistům identifikovat recidivisty, kteří by unikli těžšímu trestu. Během krátké doby mohli vyšetřovatelé porovnat míry zločince s již zaevidovanými a zjistit, zda jsou registrovány či ne. Nejprve měřil 13 tělesných rozměrů, které byly později redukovány na 11. Měřilo se výška těla ve stoje a v sedě, šířka rozpětí paží, délka a šířka hlavy, délka a šířka pravého ucha, délka prostředníku a prsteníku levé ruky, délka předloktí levé ruky a levého chodidla. (1, s. 150) Tyto rozměry se s dalšími údaji zapisovaly do identifikačních karet, ke kterým se přidával popis a fotografie zločince (Obr. 29). (1, s. 152)



Obr. 29 Identifikační antropometrická karta Alphonse Bertillona (78)

Pro snadnější orientaci vytvořil Bertillon vlastní indexový systém. Každá karta byla očíslována a zařazena do příslušné oddělené kategorie. Podle měr se osoby rozřazovaly do jedné z 243 kategorií. Další dělení, které zahrnovalo i barvu vlasů a očí, tvořilo 1701 skupin. (1, s. 151)

7.2 Současnost

V současnosti, stejně jako dříve, napomáhá biometrie v kriminalistice k objasňování trestné činnosti. Stále se vyvíjejí nové technologie, které by její využití zjednodušily. Jednou z technologií, která přispívá k jednoduššímu a efektivnějšímu používání biometrických charakteristik k identifikaci osob jsou informační systémy.

K mezinárodním systémům, využívaným i v České republice, se řadí AFIS a CODIS, tyto dva informační systémy jsou spravovány FBI Spojených států amerických. K českým informačním systémům patří FODAGEN, PORIDOS. (79)

AFIS – specializovaný identifikační systém sloužící k vyhodnocování otisků prstů. V současnosti ho nahradila novější verze AFIS-BIS, která umožní navíc zpracovávat otisky dlaní. (80) Jsou zde obsaženy otisky osob, stopy z neobjasněných a objasněných případů. (81)

CODIS – zde jsou uchovávány genetické profily osob. Tato databáze má vysoký stupeň ochrany před zneužitím, jsou zde uchovávány profily osob obviněných, odsouzených, profily dosud neztotožněných stop. (82)

FODAGEN – tento systém je využíván ke zpracování informací o provedených identifikačních úkonech, jako jsou popis, fotografování osoby, odebrání daktyloskopických otisků či biologického vzorku a získaných osobních údajů. (83)

PORIDOS – počítačový systém vytvořený KÚP, zavedený do praxe v 90. letech 20. století, umožňuje intuitivně sestavovat portréty osob s fotografií jednotlivých obličejových částí. (84)

Závěr

Současné trendy a rozšiřující se vývoj informačních technologií s sebou přinášejí potřebu vyššího zabezpečení. Za tímto účelem lze velmi efektivně využít biometrických charakteristik lidí, které zaručují vysokou míru zabezpečení a díky zkoumání a vývoji nových technologií dokáží míru bezpečnosti v budoucnosti udržet, dokonce i zvýšit. Technologie a systémy využívající biometrik nacházejí široké využití nejen v kriminalistice, velmi rychle se rozšířily a rozšiřují také na trhu pro komerční využití. Bohužel se tyto metody autentizace z důvodů malého povědomí a znalostí veřejnosti často setkávají s velkou nedůvěrou osob, které je mají využít, převážně z hlediska možného zásahu do soukromí nebo možného získání charakteristiky a prolomení zabezpečení. Proto je třeba se tomuto tématu stále věnovat a vylepšovat technologie a získávat nové znalosti a informace.

Tato bakalářská práce vznikla právě za účelem splnění cíle, shromáždění aktuálních a nových informací, aby mohla dostatečně a srozumitelně informovat. Práce vysvětluje téma biometrie, mapuje její historii, vysvětluje důležité pojmy, popisuje také dělení biometrických charakteristik a biometrické identifikace, seznamuje s technologiemi a systémy využívajícími biometrických vlastností osob. Hlavním bodem bylo vysvětlení jednotlivých nejvyužívanějších metod, kde jsou metody popsány spolu s informacemi o některých normách, kterým podléhají, s postupy autentizace, možnostmi využití a jejich výhodami a nevýhodami. Dále byly uvedeny vybrané méně využívané metody, které jsou podle mého názoru zajímavé, je dobré o nich vědět a představit je veřejnosti. V práci jsou zmíněny i české doklady obsahující biometrické charakteristiky jejich majitelů a možnosti, jak lze využít charakteristik v kriminalistice.

Mým přínosem je sepsání důležitých a aktuálních informací oproti rozsáhlým a dříve vydaným knihám a jiným tištěným dokumentům. Dalším přínosem je srozumitelnost a komplexnost informací, které čtenář získá a tím je obeznámen s tématem, čím může narůst jeho důvěra v nové a moderní technologie využívající biometrik, které se v současnosti vyvíjejí a uvádějí do provozu.

Seznam použité literatury

[1] RAK, Roman a kolektiv. Biometrie a identita člověka ve forenzních a komerčních aplikacích. Praha: Grada Publishing, 2008. ISBN 978-80-247-2365-5.

[2] BITTO, Ondřej. Šifrování a biometrika aneb tajemné bity a dotyky. Kralice na Hané: Computer Media, 2005. ISBN 80-86686-48-5.

[3] KOMENDA, Stanislav. Základní biometrické metody. Olomouc: Universita Palackého, 1968.

[4] DRAHANSKÝ, Martin a Filip ORSÁG a kolektiv. Biometrie. Brno: Computer Press, 2011. ISBN 978-80-254-8979-6.

[5] PŘIBYL, Tomáš. Výhody a nevýhody biometrických systémů (1). *Scienceworld* [online]. [cit. 2019-02-01]. Dostupné z: https://www.scienceworld.cz/biologie/vyhody-a-nevyhody-biometrickych-systemu-1-515/?switch_theme=mobile

[6] Letmý pohled do světa biometrie: Otisk prstu zatím převládá. *IT Systems* [online]. 2014, 2014(6) [cit. 2019-02-02]. Dostupné z: https://www.systemonline.cz/it-security/letmy-pohled-do-sveta-biometrie.htm

[7] KYNĚRA, Jan. Samá hesla. Jaká je biometrická budoucnost bankovnictví?. *Roklen 24* [online]. [cit. 2019-02-02]. Dostupné z: https://roklen24.cz/a/itGJX/sama-hesla-jaka-je-biometricka-budoucnost-bankovnictvi

[8] DRAHANSKÝ, Martin. *Přehled biometrických systémů a testování jejich spolehlivosti* [online]. VUT V BRNĚ, FIT, ÚITS, 2007 [cit. 2019-02-03]. Dostupné z: https://data.security-portal.cz/clanky/113/odborne_prednasky/Prezentace.pdf. VUT V BRNĚ, Fakulta informačních technologií, ÚITS.

[9] PUŽMANOVÁ, Rita. Biometrické systémy v praxi. *IT Systems* [online]. 2004, 2004(3) [cit. 2019-02-25]. Dostupné z: https://www.systemonline.cz/clanky/biometricke-systemy-v-praxi.htm

[10] SULOVSKÁ, Kateřina. Biometrické systémy zaměřené na rozpoznávání tváře, jejich spolehlivost a základní metody pro jejich tvorbu. *Posterus* [online]. 2011, 4(9), 15 [cit. 2019-02-26]. ISSN 1338-0087. Dostupné z: http://www.posterus.sk/?p=11511&output=pdf

[11] FRR – false rejection rate. *Webopedia* [online]. [cit. 2019-02-26]. Dostupné z: https://www.webopedia.com/TERM/F/false_rejection.html

[12] EER – equal error rate. *Webopedia* [online]. [cit. 2019-02-26]. Dostupné z: https://www.webopedia.com/TERM/E/equal_error_rate.html

[13] ISO/IEC 19794-1:2011: Information technology -- Biometric data interchange formats -- Part 1: Framework. *International Organization for Standardization* [online]. 2011-07 [cit. 2019-03-04]. Dostupné z: https://www.iso.org/standard/50862.html

[14] Standards catalogue: 35.240.15 - Identification cards. Chip cards. Biometrics. International Organization for Standardization [online]. [cit. 2019-03-04]. Dostupné z: https://www.iso.org/ics/35.240.15/x/

[15] INCITS 358-2002[R2012]: Information technology - BioAPI Specification (Version 1.1). *International Committee for Information Technology Standards* [online]. 2012-09-17 [cit. 2019-03-04]. Dostupné z: https://standards.incits.org/apps/group_public/project/details.php?project_id=847

[16] ANSI INCITS 398-2005: Information Technology - Common Biometric Exchange Formats Framework (CBEFF). ANSI Webstore [online]. [cit. 2019-03-04]. Dostupné z: https://webstore.ansi.org/standards/incits/ansiincits3982005

[17] ŠAFARIKOVÁ, Hana. Anatomie lidského oka. Optika Hana Šafariková [online]. [cit. 2019-03-04]. Dostupné z: http://www.optika-safarikova.cz/oko.html

[18] DRAHANSKÝ, Martin. Tajemství biometrie 3: Duhovka a sítnice. ABC [online]. 2018, 2018(2018/13) [cit. 2019-03-04]. Dostupné z: https://www.abicko.cz/clanek/precti-si-technika/23576/tajemstvi-biometrie-3-duhovka-a-sitnice.html

[19] Biometrie oka. Biometric Line [online]. [cit. 2019-03-04]. Dostupné z: http://www.biometricke-ctecky.cz/biometriky/oko/

[20] DRAHANSKÝ, Martin. Tajemství biometrie 3: Duhovka a sítnice. ABC [online]. 2018, 2018(2018/13) [cit. 2019-03-04]. Dostupné z: https://www.abicko.cz/galerie/precti-si-technika/45641/tajemstvi-biometrie-3-duhovka-a-sitnice?foto=4

[21] ISO/IEC 19794-6:2011: Information technology -- Biometric data interchange formats -- Part 6: Iris image data. International Organization for Standardization [online]. 2011-10 [cit. 2019-03-04]. Dostupné z: https://www.iso.org/standard/50868.html

[22] INCITS Announces the Approval of Five Biometric Data Interchange Format Standards. International Committee for Information Technology Standards [online]. [cit. 2019-03-04]. Dostupné z: http://www.incits.org/news-events/press-releases/incits-announces-the-approval-of-five-biometric-data-interchange-format-standards

[23] THAKKAR, Danny. Top Five Biometrics: Face, Fingerprint, Iris, Palm and Voice. Bayometric [online]. [cit. 2019-03-04]. Dostupné z: https://www.bayometric.com/biometrics-face-finger-iris-palm-voice/

[24] DRAHANSKÝ, Martin. Tajemství biometrie 2: Rozpoznávání obličeje. ABC [online]. 2018, (2018/7) [cit. 2019-03-05]. Dostupné z: https://www.abicko.cz/clanek/precti-si-technika/23285/tajemstvi-biometrie-2-rozpoznavani-obliceje.html

[25] ČERMÁK, Miroslav. Autentizace: biometrické metody. CLEVER AND SMART [online]. 07.12.2009 [cit. 2019-03-05]. Dostupné z: https://www.cleverandsmart.cz/autentizace-biometricke-metody/

[26] ISO/IEC 19794-5:2011: Information technology -- Biometric data interchange formats -- Part 5: Face image data. International Organization for Standardization [online]. 2011-11 [cit. 2019-03-05]. Dostupné z: https://www.iso.org/standard/50867.html

[27] INCITS 385-2004[R2014]: Information Technology - Face Recognition Format For Data Interchange. ANSI Webstore [online]. [cit. 2019-03-05]. Dostupné z: https://webstore.ansi.org/Standards/INCITS/INCITS3852004R2014

[28] Biometrie obličeje. Biometric Line [online]. [cit. 2019-03-05]. Dostupné z: http://www.biometricke-ctecky.cz/biometriky/oblicej/

[29] Měření biometrických údajů. VUT V BRNĚ, FEKT, ÚAMT [online]. [cit. 2019-03-05]. Dostupné z: http://www.uamtold.feec.vutbr.cz/vision/TEACHING/MAPV/10%20-%20Biometrie%20a%20medicina.pdf

[30] DRAHANSKÝ, Martin. Tajemství biometrie 1: Otisky prstů. ABC [online]. 2017, 29. listopadu 2017, (22/2017) [cit. 2019-03-05]. Dostupné z: https://www.abicko.cz/clanek/precti-si-technika/22381/tajemstvi-biometrie-1-otisky-prstu.html

[31] ŠČUREK, Radomír. VŠB TU OSTRAVA, Fakulta bezpečnostního inženýrství, Katedra bezpečnostního managementu, Oddělení bezpečnosti osob a majetku. Biometrické metody identifikace osob v bezpečnostní praxi: Studijní text [online]. VŠB TU OSTRAVA, Fakulta bezpečnostního inženýrství, červen 2008 [cit. 2019-03-05]. Dostupné z: http://www.rucnepsanypodpis.cz/PDF/biometricke_metody.pdf

[32] Do you have unusual fingerprints?. Headlines on Human Hands [online]. SEPTEMBER 20, 2005 [cit. 2019-03-05]. Dostupné z: http://handlines.blogspot.com/2005/09/do-you-have-unusual-fingerprints.html

[33] Obrazce a znaky kůže. Krimi-spk.sweb.cz [online]. [cit. 2019-03-05]. Dostupné z: http://krimi-spk.sweb.cz/02_exper/expertiz/02a_dakt/02a_kuze.htm

[34] Biometrie otisku prstu. Biometric Line [online]. [cit. 2019-03-05]. Dostupné z: http://www.biometricke-ctecky.cz/biometriky/otisk-prstu/

[35] ISO/IEC 19794-3:2006: Information technology -- Biometric data interchange formats -- Part 3: Finger pattern spectral data. International Organization for Standardization [online]. 2006-08 [cit. 2019-03-05]. Dostupné z: https://www.iso.org/standard/38747.html

[36] ISO/IEC 19794-2:2011: Information technology -- Biometric data interchange formats -- Part 2: Finger minutiae data. International Organization for Standardization [online]. 2011-12 [cit. 2019-03-05]. Dostupné z: https://www.iso.org/standard/50864.html

[37] ISO/IEC 19794-4:2011: Information technology -- Biometric data interchange formats -- Part 4: Finger image data. International Organization for Standardization [online]. 2011-12 [cit. 2019-03-05]. Dostupné z: https://www.iso.org/standard/50866.html

[38] INCITS 377-2009[R2014]: Information Technology - Finger Pattern Data Interchange Format. ANSI Webstore [online]. [cit. 2019-03-05]. Dostupné z: https://webstore.ansi.org/Standards/INCITS/INCITS3772009R2014

[39] ANSI INCITS 378-2004: Information Technology - Finger Minutiae Format For Data Interchange. ANSI Webstore [online]. [cit. 2019-03-05]. Dostupné z: https://webstore.ansi.org/Standards/INCITS/ANSIINCITS3782004

[40] ANSI INCITS 381-2004: Information Technology - Finger Image-Based Data Interchange Format. ANSI Webstore [online]. [cit. 2019-03-05]. Dostupné z: https://webstore.ansi.org/Standards/INCITS/ANSIINCITS3812004

[41] JAVŮREK, Karel. 10 biometrických technologií, které vás identifikují. VTM [online]. [cit. 2019-03-06]. Dostupné z: http://vtm.e15.cz/aktuality/10-biometrickych-technologii-ktere-vas-identifikuji

[42] What is DNA?. U. S. National Library of Medicine: Genetics Home References [online]. March 5, 2019 [cit. 2019-03-06]. Dostupné z: https://ghr.nlm.nih.gov/primer/basics/dna

[43] ISO/IEC 19794-14:2013: Information technology -- Biometric data interchange formats -- Part 14: DNA data. International Organization for Standardization [online]. 2013, 2013-03 [cit. 2019-03-06]. Dostupné z: https://www.iso.org/standard/50872.html

[44] DNA Biometrics. IBIA - International Biometrics + Idnetity Association [online]. [cit. 2019-03-06]. Dostupné z: https://www.ibia.org/biometrics-and-identity/biometric-technologies/dna

[45] HINNER, Jiří. Biometrické metody v bezpečnostní praxi (1). TŘÍPÓL [online]. 17. října 2006 [cit. 2019-03-06]. Dostupné z: https://www.3pol.cz/cz/rubriky/bez-zarazeni/363-biometricke-metody-v-bezpecnostni-praxi-1

[46] Voice authentication. Aware [online]. [cit. 2019-03-06]. Dostupné z: https://www.aware.com/voice-authentication/

[47] ISO/IEC 19794-13:2018: Information technology -- Biometric data interchange formats -- Part 13: Voice data. International Organization for Standardization [online]. 2018-03 [cit. 2019-03-06]. Dostupné z: https://www.iso.org/standard/72276.html

[48] ISO/IEC 19794-7:2007: Information technology -- Biometric data interchange formats -- Part 7: Signature/sign time series data. International Organization for Standardization [online]. 2007-06 [cit. 2019-03-07]. Dostupné z: https://www.iso.org/standard/38751.html

[49] ISO/IEC 19794-11:2013: Information technology -- Biometric data interchange formats -- Part 11: Signature/sign processed dynamic data. International Organization for Standardization [online]. 2013-02 [cit. 2019-03-07]. Dostupné z: https://www.iso.org/standard/51824.html

[50] ANSI INCITS 395-2005: Information Technology - Biometric Data Interchange Formats - Signature/Sign Data. ANSI Webstore [online]. [cit. 2019-03-07]. Dostupné z: https://webstore.ansi.org/Standards/INCITS/ANSIINCITS3952005

[51] ISO/IEC 19794-10:2007: Information technology -- Biometric data interchange formats -- Part 10: Hand geometry silhouette data. International Organization for Standardization [online]. 2007-06 [cit. 2019-03-07]. Dostupné z: https://www.iso.org/standard/43638.html

[52] ANSI INCITS 396-2005: Information Technology - Hand Geometry Interchange Format. ANSI Webstore [online]. [cit. 2019-03-07]. Dostupné z: https://webstore.ansi.org/Standards/INCITS/ANSIINCITS3962005

[53] RAK, Roman a Viktor PORADA. Identifikace a verifikace osoby na základě tvaru ucha a jeho otisků. Soudní inženýrství [online]. 17/2006(5/2006) [cit. 2019-02-21]. ISSN 1211-443X. Dostupné z: http://www.sinz.cz/archiv/docs/si-2006-05-255-268.pdf

[54] Biometrie krevního řečiště. Biometric Line [online]. [cit. 2019-02-22]. Dostupné z: http://www.biometricke-ctecky.cz/biometriky/krevni-reciste/

[55] GHIDRAI, George. THE DENTAL RADIOGRAPHY OR DENTAL X-RAY. Infodentis [online]. November 2017 [cit. 2019-02-23]. Dostupné z: https://www.infodentis.com/fixed-prosthodontics/dental-radiography.php

[56] LOVELEEN. Role of Nail Striation in Forensic Identification. INTERNATIONAL JOURNAL OF RESEARCH CULTURE SOCIETY [online]. 2017, May - 2017, 1(3), 33 [cit. 2019-02-18]. ISSN 2456-6683. Dostupné z: http://ijrcs.org/wp-content/uploads/201705004.pdf

[57] MUSIL, Jan a kolektiv. Kriminalistika. Praha: Naše vojsko, 1994. ISBN 80-206-0423-5.

[58] STRAUS, Jiří. Kriminalistický a biometrický aspekt identifikace osoby [online]. Policejní akademie ČR - Katedra kriminalistiky [cit. 2019-02-24]. Dostupné z: http://files.svses.webnode.cz/200004811-8ab3a8ca3d/strauss.pdf

[59] Přesná identifikace osob podle dynamického stereotypu lokomoce. Technický portál [online]. 1. leden 2006 [cit. 2019-02-24]. Dostupné z: https://www.technickytydenik.cz/rubriky/archiv/presna-identifikace-osob-podle-dynamickeho-stereotypu-lokomoce_11049.html

[60] HORÁK, Karel a Miloslav RICHTER. Segmentace obrazu pro identifikaci osob pomocí bipedální lokomoce. Technický portál [online]. Fakulta elektrotechniky a komunikačních technologií, Vysoké učení technické v Brně, 2009, October 2009 [cit. 2019-02-24]. Dostupné z: https://www.researchgate.net/publication/237496605_Segmentace_obrazu_pro_identifikaci_osob_pomoci_bipedalni_lokomoce

[61] ČERMÁK, Miroslav. Autentizace: analýza způsobu psaní na klávesnici. CLEVER AND SMART [online]. 15.12.2011 [cit. 2019-02-19]. Dostupné z: https://www.cleverandsmart.cz/autentizace-analyza-zpusobu-psani-na-klavesnici/

[62] DRAHANSKÝ, Martin. Tajemství biometrie 3: Duhovka a sítnice. ABC [online]. 2018, 2018(2018/13) [cit. 2019-03-09]. Dostupné z: https://www.abicko.cz/galerie/precti-si-technika/45641/tajemstvi-biometrie-3-duhovka-a-sitnice?foto=1

[63] Cestovní doklady s biometrickými prvky (CDBP). Ministerstvo vnitra České republiky [online]. [cit. 2019-03-12]. Dostupné z: https://www.mvcr.cz/clanek/cestovni-doklady-s-biometrickymi-prvky-cdbp.aspx?q=Y2hudW09MQ%3d%3d

[64] Vyhláška č. 400/2011 Sb.: vyhláška, kterou se provádí zákon o občanských průkazech a zákon o cestovních dokladech. In: Sbírka zákonů ČR. 2011, částka 139, číslo 400. ISSN 1211-1244. Dostupné také z: https://www.zakonyprolidi.cz/cs/2011-400

[65] Biometrický pas. CESTOVNI-PAS.CZ [online]. [cit. 2019-03-12]. Dostupné z: https://www.cestovni-pas.cz/biometricky-pas/

[66] EPassport logo. Wikipedie [online]. [cit. 2019-03-12]. Dostupné z: https://cs.wikipedia.org/wiki/Biometrick%C3%BD_pas#/media/File:EPassport_logo.svg

[67] Vyhláška č. 415/2006 Sb.: vyhláška, kterou se stanoví technické podmínky a postup při pořizování a dalším zpracovávání biometrických údajů obsažených v nosiči dat cestovního dokladu. In: Sbírka zákonů ČR. 2006, částka 133, číslo 415. ISSN 1211-1244. Dostupné také z: https://zakonyprolidi.cz/cs/2006-415

[68] JEDLIČKA, Miloslav. Kriminalistika. Kriminalistika a příbuzné obory [online]. [cit. 2019-03-14]. Dostupné z: http://kriminalistika.eu/menu/kr_obory0.html

[69] BUSTARD, John D., Xingjie, Xingjie NIXON a Chang-Tsun LI. On Forensic Use of Biometrics. HO, Anthony T.S. a Shujun LI. Handbook of Digital Forensics of Multimedia Data and Devices. Wiley - IEEE, 2015. ISBN 978-1-118-64050-0. Dostupné také z: https://www.researchgate.net/publication/269037172_On_Forensic_Use_of_Biometrics

[70] Kriminalistická daktyloskopie. Policie ČR [online]. [cit. 2019-03-14]. Dostupné z: https://www.policie.cz/clanek/celorepublikove-utvary-kriminalisticky-ustav-praha-zpravodajstvi-test-2.aspx?q=Y2hudW09MQ%3d%3d

[71] JEDLIČKA, Miloslav. Kriminalistická daktyloskopie. Kriminalistika a příbuzné obory [online]. [cit. 2019-03-14]. Dostupné z: http://kriminalistika.eu/daktyl/daktyl.html

[72] JEDLIČKA, Miloslav. Z historie kriminalistické fotografie. Kriminalistika a příbuzné obory [online]. [cit. 2019-03-14]. Dostupné z: http://kriminalistika.eu/krim_foto/krim_foto.html

[73] JEDLIČKA, Miloslav. Genetika ve službách kriminalistiky. Kriminalistika a příbuzné obory [online]. [cit. 2019-03-14]. Dostupné z: http://kriminalistika.eu/dna/dna.html

[74] VAN DER LUGT, Cor. (EARS AND) EARPRINTS, INDIVIDUALISING CRIME SCENE MARKS?!. Problems of Forensic Sciences [online]. 2001 [cit. 2019-03-14]. Dostupné z: http://www.forensicscience.pl/pfs/46_lugut.pdf

[75] Kriminalistická dokumentace. Policie České republiky [online]. [cit. 2019-03-14]. Dostupné z: https://www.policie.cz/clanek/kriminalisticka-dokumentace?fbclid=IwAR11w-kBRP-madh0cpk-_n1s8MLEvZGbUi0tQGifmxGs4mHfdd0HTYGrG9k

[76] Kriminalistické identifikace. Policie ČR [online]. [cit. 2019-03-14]. Dostupné z: https://www.policie.cz/clanek/kriminalisticke-identifikace-618304.aspx?q=Y2hudW09Ng%3D%3D

[77] Historický vývoj KÚP. Policie ČR [online]. [cit. 2019-03-14]. Dostupné z: https://www.policie.cz/clanek/historicky-vyvoj-kup.aspx?q=Y2hudW09Mg%3d%3d

[78] Anthropometry card of Alphonse Bertillon who originated the criminal identification. ResearchGate [online]. [cit. 2019-01-28]. Dostupné z: https://www.researchgate.net/figure/Anthropometry-card-of-Alphonse-Bertillon-who-originated-the-criminal-identification_fig5_282008384

[79] JANDEČKA, Aleš. Informační systémy Policie České republiky. Praha, 2019. Dostupné také z: https://is.cuni.cz/webapps/zzp/detail/76126/. Diplomová práce. Univerzita Karlova v Praze, Filozofická fakulta, Ústav informačních studií a knihovnictví.

[80] AFIS. Policie ČR [online]. [cit. 2019-03-14]. Dostupné z: https://www.policie.cz/clanek/celorepublikove-utvary-kriminalisticky-ustav-praha-zpravodajstvi-test-2.aspx?q=Y2hudW09Mg%3d%3d

[81] DENNY. Daktyloskopie. Kriminalistika - Vše o vědních disciplínách [online]. [cit. 2019-03-14]. Dostupné z: http://krimi2000.blogspot.com/2013/03/daktyloskopie.html

[82] DENNY. Policie ČR nezneužívá DNA. Policie ČR [online]. [cit. 2019-03-14]. Dostupné z: https://www.policie.cz/clanek/informacni-servis-zpravodajstvi-policie-cr-nezneuziva-dna.aspx

[83] Pořizování identifikačních fotografií. Policie ČR [online]. [cit. 2019-03-14]. Dostupné z: https://www.policie.cz/clanek/porizovani-identifikacnich-fotografii.aspx

[84] Sestavování portrétů z kosterních pozůstatků. Policie ČR [online]. [cit. 2019-03-14]. Dostupné z: https://www.policie.cz/clanek/pripady-na-kterych-se-kup-podilel.aspx?q=Y2hudW09NQ%3D%3D

[85] ONDRŮŠEK, Roman. Identifikační biometrické prostředky. Zlín, 2006. Dostupné také z: https://digilib.k.utb.cz/handle/10563/743. Bakalářská práce. Univerzita Tomáše Bati ve Zlíně, Fakulta aplikované informatiky.

Seznam obrázků

Seznam použitých zkratek

2D	Dvourozměrný (Two-dimensional)
2,5D	Dva a půl rozměrný (Two-and-a-half-dimensional)
3D	Trojrozměrný (Three-dimensional)
AFIS	Daktyloskopický identifikační systém (Automated Fingerprint Identification System)
ANSI/INCITS	ANSI (Americká národní standardizační organizace – American National Standards Institute) a INCITS (Mezinárodní výbor pro standardy informačních technologií – International Committee for Information Technology Standards)
API	Rozhraní pro programování aplikací (Application Programming Interface)
CODIS	Národní databáze DNA Spojených států amerických vytvořená FBI (Combined DNA Index System)
DNA	Deoxyribonukleová kyselina (Deoxyribonucleic Aacid)
EER	Míra spolehlivosti (Equal Error Rate)
FAR	Míra chybného přijetí (False Acceptance Rate)
FBI	Federální úřad pro vyšetřování (Federal Bureau of Investigation) - vyšetřovací orgán amerického ministerstva spravedlnosti
FRR	Míra chybného odmítnutí (False Rejection Rate)
HW	Hardware (veškeré fyzicky existující technické vybavení počítače)
IR	Infračervené záření (Infrared radiation)
ISO/IEC	Společná technická komise ISO (Mezinárodní organizace pro normalizaci – International Organization for Standardization) a IEC (Mezinárodní elektrotechnická komise – International Electrotechnical Commission)
IT	Informační technologie
KÚP	Kriminalistický ústav Praha
OČTŘ	Orgány činné v trestním řízení
STR	Krátké tandemové repetice (Short Tandem Repeats) – sekvence repetitivní DNA
SW	Software (sada všech počítačových programů používaných v počítači provádějících nějakou činnost)

Přílohy

Příloha 1 Oblasti využití biometrických identifikačních systémů (85 – vlastní úprava)

Bezpečnostní oblast	Oblast státní zprávy	Výpočetní technika obecně a komerční sféra
• Kriminalistika • Boj proti zločinu obecně • Osoby v pátrání a pohřešované • Vězeňství • Sledování zájmových osob • Fyzická ostraha a zabezpečení strategických objektů (letiště, nádraží, banky, vládní instituce, …) • Zpravodajství	• Vydávání řidičských oprávnění, osobních dokladů, ID karet, pasů a víz • Zdravotní pojištění • Sociální pojištění • Oprávněnost přistupovat k volbám, účastnit se referenda, sčítání lidu atd. • Zdravotnictví • školství	• Bankovnictví, finančnictví a pojišťovnictví • Personální agendy • Přístup k prostředkům počítačových informačních systémů a telekomunikačních zařízení • Obecná ochrana proti podvodům a zpronevěrám • Řízení přístupu k platebním kartám a bankomatům • Identifikace zákazníků, zaměstnanců, návštěvníků • Zvýhodněné služby pro stálé zákazníky • Elektronické transakce, elektronický podpis • Různé služby a marketing

Příloha 2 Porovnání bezpečnostně-komerční a policejně-soudní identifikace (1, s. 109 – vlastní úprava)

Biometrická identifikace nebo verifikace		
Sledovaná charakteristika	**Bezpečnostně-komerční (lesser biometrics)**	**Policejně-soudní (forenzní) (high biometrics)**
Rozlišovací schopnost metody	Nižší – $1{:}10^4$ až 10^6	Vysoká – $1{:}10^7$ až 10^9
Automatizace	Úplná	Vysoká, pouze podpůrná role
Identifikační nebo verifikační závěr realizován	Zcela automaticky zařízením nebo aplikací	Silná podpora automatizovaných prostředků, rozhodující závěr vyslovují soudní znalci
V praxi převládá	Verifikace	Identifikace
Chybné ztotožnění (odmítnutí) registrované osoby znamená	Nespokojený oprávněný uživatel, opakování identifikačního/verifikačního procesu, nízký uživatelský komfort, nedůvěra v zařízení	Podezřelý nebo pachatel uniká z dosahu policejně-soudních orgánů, spokojený pachatel, nespokojené OČTŘ, špatný směr vyšetřování
Ukládání referenčních šablon do databáze	Pouze známé osoby	Osoby známé, ale i neznámé s cílem pozdější identifikace nebo dokazování souvislostí
Možnost opětovného sejmutí vzorku	Prvotní zavádění do databáze lze opakovat v případě nedostačující kvality	Nelze zvyšovat kvalitu stop nalezených na místě trestných činů, stopa může být vyhovující nebo nevyhovující
Ukládání biometrických vzorků a referenčních šablon do databáze	Uchovávány pouze referenční šablony pro porovnávací účely	Kromě šablon u některých metod uchovávány i původní vzorky, pro možnost generace nových šablon
Doba zpracování	Sekundy, důležitá je akceptovatelnost pro uživatele a provozovatele	Vteřiny až dny, rychlost není tak rozhodující
Akceptovatelnost použití	Nezávislé, posuzovatelské instituce, provozovatelé, uživatelé	Stát, policejně-soudní teorie a praxe
Právní regulace používání biometrických aplikací	Nutný souhlas osoby, která metodu používá, zařízení – interní směrnice, podnikové normy, které musí být v souladu s legislativou (pokud pro tuto oblast existuje)	Vždy zakotveno v národní legislativě
Akceptovatelnost metody uživatelem	Rozhodující	Nerozhoduje, osoba může být i přinucena poskytnout vzorek (v souladu s platnou legislativou, etikou a hygienou)
Oblast využití	Široká, obecná	Velmi specializovaná, omezená na instituce pověřené státem
Komerční dostupnost	Pro všechny zájemce	Zpravidla pouze pro instituce pověřené státem

Cena	Nízká, daná technologií a jejím masovým rozšířením	Vysoká, nemusí být pro nákup rozhodující, důraz kladen na vysokou rozlišovací schopnost, objektivnost, spolehlivost a vědeckou transparentnost metody
Nároky na zabezpečení technologie nebo zařízení	Spíše průměrné, v závislosti na požadavcích provozovatelů	Vysoké, zařízení provozovány na režimových pracovištích s různě vysokým stupněm zabezpečení, minimalizace přístupu neoprávněných osob
Rozměry zařízení	Malé, snaha o miniaturizace	Mohou být velké, miniaturizovat ano, ale není podmínkou
Vlastnictví zařízení a jejich využití	Vlastníky jsou státní orgány i privátní instituce, využití veřejné nebo privátní	Vlastníky jsou zpravidla státní orgány, využití neveřejné