# Přehled autentizačních biometrických metod

Vladimír Levek

Fakulta elektrotechniky a komunikačních technologií VUT v Brně
Email: levek@feec.vutbr.cz

***Abstrakt*** *– Tento dokument se zabývá problematikou spojenou s autentizací přístupu k elektronickým informacím a rozebírá biometrické metody jako prostředek autentizace. Popisuje možnosti jednotlivých technik a úskalí spojená s jejich využitím. Nejprve je popsána problematika autentizace včetně některých důležitých pojmů spojených s touto problematikou Následující kapitola rozebírá nedůležitější a nejčastější autentizační metody. Je zde rovněž zdůrazněna efektivita, náročnost nasazení na daný informační systém, a také perspektiva. Ve zbývající části článku jsou popsány biometrické metody nejčastěji používané v oblasti autentizace. Závěrem dokumentu je odůvodněna nutnost vícefaktorové autentizace.*

## 1 Úvod

Díky nástupu moderních informačních technologií je výrazně usnadněna činnost téměř ve všech oblastech ať komerčních, armádních, civilních, vládních, tak v oblastech veřejných služeb či zájmových organizací. Snadný přístup k informacím, má ovšem za následek zvýšenou možnost neoprávněného přístupu k důvěrným informacím, manipulací s těmito informacemi, či možnost záměrné modifikace dat. Snahy datových útočníků mohou být motivovány osobními zájmy, zájmy snadného obohacení, ale také zájmy s cílem průmyslové špionáže, či dokonce zájmy s politickými, nebo národními. Všechny aspekty možných neautorizovaných přístupů k informacím musí být řešeny v oblasti nazvané informační bezpečnost.

Pod pojmem informační bezpečnost lze chápat soubor opatření vedoucí k ochraně informací před zničením, ztrátou, nebo zneužitím. Přičemž ochrana informace je důležitá po celou dobu jejího životního cyklu, nebo alespoň do doby jejího odtajnění. Životní cyklus informace je zahájen jejím vznikem, pokračuje zpracováním, přenosem, uložením a je završen buď její likvidací, nebo ukončením její platnosti. Vzhledem ke stále se zvyšující hodnotě informace, je zcela logický rostoucí trend rozšiřování opatření vedoucích ke zvýšení její bezpečnosti ve všech formách a ve všech úsecích jejího životního cyklu. Protože informace existuje v nejrůznějších formách, způsob jejího zabezpečení se musí lišit. Informace uložená na papíře, popřípadě na nějakém fyzickém záznamovém mediu se musí chránit fyzickým zajištěním prostoru. Rovněž její zpracování, ukládání a distribuce musí spadat do oblasti fyzické ostrahy. Naproti tomu bezpečnost informace uložené v elektronické podobě musí zahrnovat výrazně širší nutnost ochrany a to z důvodu snadnějšího útoku. Opět musí být zajištěna fyzická ochrana prostor s datovým úložištěm, ale ve stejné míře musí být věnován prostor ochraně vzdáleného přístupu, ochraně přenosového vedení před neautorizovaným odposlechem, či neautorizovaným podvrhem modifikovaných dat. V další části práce bude pod pojmem informace míněna pouze informace v elektronické podobě, nazývaná též data.

Úkolem informační bezpečnosti je vytvoření opatření vedoucích k adekvátní ochraně celého informačního systému. Pod pojmem informační systém se rozumí nástroje sloužící k ukládání, zpracování a přenosu dat. V současné době jsou informační systémy nejčastěji tvořeny servery s datovými úložišti a s odpovídajícím programovým vybavením. Tyto servery jsou mezi sebou propojeny prostřednictvím počítačové sítě. Přístup k libovolným datům může být uskutečněn z libovolného místa počítačové sítě. V ideálním případě jsou data poskytnuta pouze konkrétnímu subjektu s právem přístupu ke konkrétním datům. Pro všechny ostatní případy je vyloučen jakýkoliv přístup, sdílení, či manipulace s daty. Snahou je, aby osobě s právem přístupu k určitým datům byl umožněn přístup k těmto datům prostřednictvím veřejné sítě, aby jí bylo umožněno data libovolně zpracovávat a následně je bezpečně uložit. Tato osoba musí být s jistotou identifikována a musí jí být umožněn přístup k datům na požadované úrovni. V praxi se ovšem nikdy nesetkáme s dokonale bezpečným systémem. Paradoxně tomu není bráněno technickými možnostmi zpracování či přenosu dat. Tyto nástroje informačního systému pracují spolehlivě a nejsou důvodem omezení informační bezpečnosti. Míra spolehlivost ochrany dat spočívá v lidském faktoru. Práva přístupu k datům a úroveň nakládáním s těmito daty zajišťuje člověk. Ten může pracovat nespolehlivě ať záměrně, z důvodu nevědomosti, či z důvodu pracovní nedbalosti. Osoba s právem přístupu ke konkrétním datům může být špatně vyhodnocena jako spolehlivá a opět může způsobit omezení informační bezpečnosti. Subjektem nejvíce ohrožujícím bezpečnost dat je útočník. Je to osoba s úmyslem neoprávněného přístupu k datům a to jakýmikoliv nelegálními prostředky. Data mohou být útočníkem buď zneužita, nebo mohou být záměrně podvržena. V odborné terminologii se tato narušení nazývají: ztráta důvěrnosti dat a ztráta autentičnosti dat, popřípadě lze hovořit o narušení integrity, či dostupnosti dat.

Biometrie je obor zabývající se měřením biologických vlastností člověka, popřípadě jeho chováním a reakcemi. Pro potřeby autentizace jsou výsledky biometrických měření používány pro rozlišení a identifikaci osob. Cílem není získání podrobného souboru obsahujícího nejrůznější výsledky měření, ale nalezení odlišností mezi jednotlivými osobami, které lze uplatnit při opakujících se měřeních. Problémem biometrické autentizace není nalezení rozdílů mezi jednotlivými osobami, ale uplatnění těchto rozdílů při automatickém procesu autentizace.

Jelikož absolutně bezchybná biometrická metoda neexistuje, je nutné stanovit míru efektivity dané metody. Na chybovost biometrických metod lze nahlížet z několika směrů a tak je důležité pro danou aplikaci vyhledat tu nejvhodnější meto-

du, která se vyznačuje nejpříznivějšími výsledky určitých statistických měření. Z důvodu rozlišení efektivnosti autentizačních metod jsou zavedeny statistické koeficienty:

- koeficient chybného odmítnutí,
- koeficient chybného přijetí,
- koeficient vyrovnané chyby,
- doba zápisu etalonu,
- doba ověření, atp.

V závislosti na úhlu pohledu, hloubce zkoumání či způsobu měření spolehlivosti může existovat mnohem více koeficientů kvantifikujících danou oblast autentizace. Pro získání informace o spolehlivosti daného autentizačního systému jsou nejdůležitější první dva koeficienty.

### Koeficient pravděpodobnosti chybného odmítnutí (False Rejection Rate - FRR)

Koeficient FRR představuje pravděpodobnost odmítnutí oprávněného uživatele. Jedná se o případ, kdy osoba mající oprávněný přístup, je na základě vyhodnocení autentizačního systému odmítnuta [2]. Tento koeficient nemá vliv na bezpečnost chráněné oblasti, ale určuje komfortnost přístupu. Pokud není oprávněná osoba rozpoznána, může se většinou ještě několikrát pokusit o přístup. Další pokusy ovšem vedou k prodloužení odezvy systému. V extrémních případech může opakované zamítnutí přístupu vést k zablokování uživatele spojeného se zásahem správce systému a nutností opětovného zavedení přístupových údajů. Koeficient FRR je též označován jako chyba I. druhu. Ta se obecně vyznačuje jako chybné rozhodnutí na základě výsledku testu, který odmítne pravdivou hypotézu. Číselně lze vyjádřit koeficient FRR jako poměr chybovosti k počtu všech pokusů oprávněných osob.

$$FRR = \frac{N_{FR}}{N_{EIA}} 100 \quad [\%], \tag{1}$$

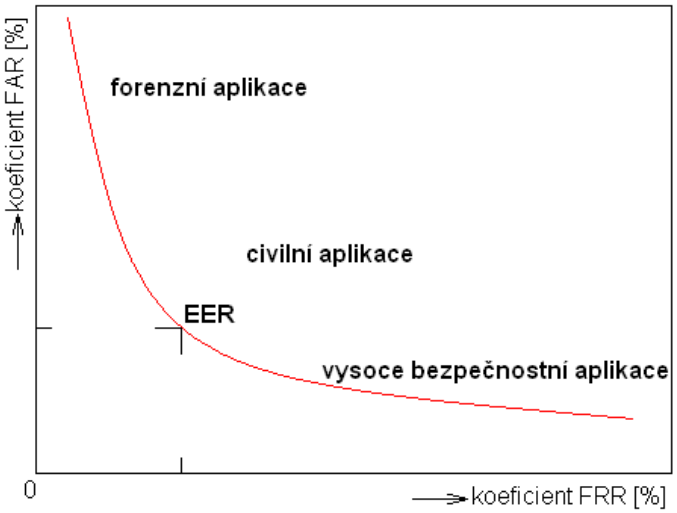
kde $N_{FR}$ (Number of False Rejection) je počet chybných odmítnutí a $N_{EIA}$ (Number of Enrolle Identification Attemps) je počet všech pokusů oprávněných osob.

### Koeficient pravděpodobnosti chybného přijetí (False Acceptance Rate - FAR)

Koeficient FAR určuje pravděpodobnost přijetí neoprávněného uživatele. V tomto případě je neoprávněné osobě, často útočníkovi, umožněn přístup do chráněné oblasti, což má za následek bezpečnostní incident [2]. Tento koeficient ukazuje bezpečnostní míru dané autentizační metody. Koeficient FAR lze označovat za chybu II. Druhu. Tato chyba vznikne na základě testu, který přijme falešnou hypotézu. Číselně je tento koeficient vyjádřen poměrem chybovosti k počtu všech neoprávněných osob.

$$FAR = \frac{N_{FA}}{N_{IIA}} 100 \quad [\%], \tag{2}$$

Pro stanovení vhodného autentizačního systému je důležité nalézt kompromis mezi koeficientem FAR a koeficientem FRR. Pro rozhodování při výběru systému je důležitý tzv. křížový koeficient EER (Equal Error Rate) [2], který určuje pravděpodobnost chybovosti při rovnosti koeficientů FRR a FAR. Na obrázku 1 je zobrazena křivka ROC (Receiver Operating Characteristic), která znázorňuje kompromis mezi pravděpodobnostními koeficienty FAR a FRR.




Obrázek 1: Křivka ROC (Receiver Operating Characteristic)

Uprostřed křivky je znázorněn křížový koeficient EER. Směrem nahoru po křivce nastává situace, kdy autentizační systém více akceptuje neoprávněné osoby, zatímco málo odmítá oprávněné osoby. Takové autentizační systémy jsou vhodné v oblasti kriminalistiky, či forenzních aplikacích. Zde se klade rozhodující důraz na rozpoznání osoby. Kladen je důraz na co nejnižší koeficient FRR (málo chybných odmítnutí oprávněné osoby). Koeficient FAR je zde vysoký (mnoho akceptování neoprávněných osob), ale ten nehraje významnou roli a může být eliminován na základě šetření užšího výběru osob. V každém případě systémy s vyšším koeficientem FAR je vhodné doplnit kontrolou za pomocí lidského faktoru. Naproti tomu systémy s vysokým koeficientem FRR a malým koeficientem FAR jsou vhodné pro automatické autentizační systémy pracující bez přispění dozoru lidského faktoru. Tato situace je znázorněna v dolní části křivky. Vysoký koeficient FRR (mnoho chybných odmítnutí oprávněné osoby) může být eliminován možností opakování pokusu o přístup a nehraje tedy prvořadou roli z hlediska bezpečnosti. Důležitějším faktorem je nízký koeficient FAR (malé množství akceptování neoprávněných osob). Tento parametr je důležitý pro volbu automatických autentizačních systémů [2].

## 2 Autentizace

Autentizace je proces vedoucí k ověření identity subjektu. Jedná se o legalizaci daného subjektu s případnou možností přístupu ke chráněné oblasti. Cílem tohoto procesu je ověření hodnověrnosti a pravosti zkoumaného subjektu se zamezením falšování identity. V oblasti informačních technologií se autentizovaný subjekt rozlišuje na autentizace osoby a autentizace dat. V další části textu se pod pojmem autentizace bude výhradně považovat autentizace osob. Zatímco autentizace dat

či programového vybavení plně spadá do oblasti kryptografie, autentizace osob může zabírat mnohem širší oblast vedoucí napříč několika vědními obory, jako jsou:

- biomedicína (biometrická měření),
- mikroelektronika (biometrické senzory),
- počítačové inženýrství (vyhodnocení dat, databáze uživatelů)
- kryptografie (zabezpečení vyhodnocených dat), atd.

V souvislosti s užitím autentizačních metod rozlišujeme dva významné procesy. Jejich odlišení spočívá ve způsobu přístupu k databázím autentizovaných subjektů.

### Identifikace osoby

Při tomto procesu se určuje totožnost neznámé osoby. Anglicky je tento proces označen jako one-to-many. V praxi je tento proces většinou uplatňován v kriminologii. Sejmutý biometrický vzorek, videozáznam z kamery, pachová stopa, atp. jsou porovnávány s databází všech dostupných vzorků a tím lze docílit získání totožnosti osoby. V souvislosti s identifikací osoby je nutné rozlišovat pojmy, jako jsou identita a shodnost. Zatímco identita osoby je v čase neměnná a zůstává v platnosti po celou dobu života, shodnost je aktuální právě v jednom okamžiku a neustále se mění vlivem plynutí času, stárnutí verifikované osoby [1]. Identifikovat osoby lze na základě antropologických metod, nebo pomocí vnějších znaků osob [10].

### Verifikace osoby

Při tomto procesu se ověřuje totožnost známé osoby. Anglicky je tento proces označen jako princip one-to-one. Tento proces se uplatňuje k zabezpečení přístupu osob do chráněných prostor, k přístupu ke chráněným datům, k přístupu do bankovního sektoru, atd. V databázi jsou uložena identifikační data, která se porovnávají s daty uživatele žádajícího o oprávněný přístup. Tato databáze je vytvořena vždy před prvním užitím.

Prokázat totožnost lze několika způsoby, z nichž každý má jinou míru bezpečnosti, jinou míru uživatelského komfortu a také jiné požadavky na vybavení autentizačního systému. Autentizaci lze provést na základě vlastnictví unikátního autentizačního předmětu, na základě znalosti tajné informace, nebo na základě měření vlastní fyziologické, nebo behaviorální charakteristiky. Metody autentizace tedy lze rozdělit do tří základních skupin:

- autentizace předmětem - uživatel "něco má",
- autentizace tajnou informací - uživatel "něco ví",
- autentizace pomocí biometrické charakteristiky - uživatel "něco je".

Každý z těchto způsobů autentizace přináší kompromis mezi uživatelským komfortem a mírou bezpečnosti a proto každý ze zmíněných způsobů autentizace bude mít vždy jiné opodstatnění pro nasazení pro různé bezpečnostní aplikace.

## 2.1 Autentizace předmětem

Relativně nejbezpečnější způsob prokázání totožnosti v současné době je autentizace na základě vlastnictví autentizačního předmětu. V současné době není problém vytvořit elektronický obvod, který dokáže generovat unikátní autentizační informaci, a nelze jej zkopírovat, uživatelsky ovládat, či přeprogramovat. Vzhledem k tomu, že zabezpečení dat mezi autentizačním předmětem a autentizačním systéme spadá do oblasti kryptografie, lze očekávat, že v horizontu blízké budoucnosti nebude problém s jejich důvěryhodností. Aktuální kryptografické systémy nemají výrazné problémy s prolamováním dat a jiný trend se v blízké budoucnosti nepředpokládá. Autentizační předměty se většinou používají v kombinaci s bezpečnostním kódem - PIN (Personal Identification Number). Pro autentizační předmět tedy platí tyto zásady:

- nesmí být zkopírován,
- smí být přeprogramován pouze známou autentizační autoritou,
- nesmí poskytnout žádné informace při násilném vniknutí.

Velká nevýhoda autentizačních předmětů spočívá v jejich přenositelnosti. Pokud je tento předmět zcizen, nebo ztracen a poté použit neoprávněnou osobou, nastává bezpečnostní konflikt. Ten může být při autentizaci ztížen vyžádáním přístupového hesla - PIN. Další nevýhodou autentizačních předmětů je nízký uživatelský komfort, jelikož uživatel jej musí mít na paměti a neustále jej střežit před zcizením, či ztrátou. Další nevýhoda spočívá v distribuci. Pokud má být celý autentizační systém bezpečný, je většinou vyžadováno osobní převzetí autorizačního předmětu u konkrétní autentizační autority.

### Čipová karta (Smart Card)

Plastová karta v kontaktním či bezkontaktním provedení, je asi nejrozšířenějším autentizačním předmětem. Tato karta umožňuje oboustrannou komunikaci se čtečkou a je schopna poskytnout šifrované autentizační informace. Používá se běžně při bankovních operacích, při komunikaci GSM jako verze karty SIM, pro přístupové a docházkové systémy a v mnoha dalších bezpečnostních systémech.


Obrázek 2: Ukázka čipové karty

Na obrázku 2 je ukázka běžného provedení čipové karty. Z hlediska bezpečnosti se jedná o velmi důvěryhodné autentizační zařízení, proto je její užití běžné v bankovním sektoru pro přístup k účtům. Její velkou nevýhodou je její křehká konstrukce. Tato vlastnost omezuje její životnost, ale také usnadňuje možnost útoku. Většina zaznamenaných útoků na bezpečnost čipové karty se týkala narušení jejího obalu a pro-

vedení některé ze známých hardwarových kryptoanalýz mikrokontroléru jako jsou:

- měření okamžité spotřeby mikrokontroléru při kryptoanalytických operacích,
- ozařování paměťové buňky mikrokontroléru pod mikroskopem,
- působením nadstandardních provozních podmínek mikrokontroléru, atd.

Tyto útoky nejsou příliš četné a tak největším bezpečnostním problémem čipových karet bývá jejich ztráta a v některých případech dokonce i ztráta spolu se zaznamenanou hodnotou kódu PIN.

### USB token

Tento autentizační prostředek o velikosti a tvaru běžného úložiště USB je vybaven konektorem USB pro připojení k osobnímu počítači. Pracuje na podobném principu jako čipová karta. V počítači je spuštěna aplikace, která v paměti tokenu USB vyhledává přístupová práva, popř. certifikát. Jiným způsobem než prostřednictvím přístupové aplikace nelze s tokenem USB komunikovat. Jeho výhoda spočívá v jednoduchosti aplikace bez nutnosti pořizování čtečky, nebo snímače.


Obrázek 3: Ukázka USB tokenu, získáno z www.windowsecurity.com

Na obrázku 3 je zobrazena jedna z mnoha variant tvaru autorizačního tokenu USB. Jeho funkce, užití, výhody popř. nevýhody jsou obdobné jako u použití čipových karet. Na rozdíl od čipové karty, která může komunikovat i bezkontaktním způsobem, je zde autentizace podmíněna zasunutím tokenu do zdířky USB.

### Autentizační kalkulátor

Tento autentizační prostředek pracuje na principu synchronizace s autentizačním systémem. Ve stejném okamžiku je na kalkulátoru vygenerováno na základě neznámé posloupnosti jednorázové heslo, které je autentizačnímu systému známé. Toto číslo je po určitou dobu platné a dalším vygenerováním nového čísla platnost starého kódu končí. Synchronizace může být uskutečněna na základě měření přesného času, popř. komunikace po utajeném komunikačním kanále. Tyto autentizační prostředky mohou být konstruovány různým způsobem, musí však mít k dispozici klávesnici popř. tlačítko a displej.


Obrázek 4: Ukázka autentizačního kalkulátoru, získáno z www.atlasltd.cz

Na obrázku 4 je fotografie konkrétního autentizačního kalkulátoru. Tato autentizační metoda představuje nejvyšší stupeň zabezpečení, ale i v tomto případě její nevýhoda spočívá v nutnosti mít tento předmět neustále v patrnosti.

### Mobilní telefon

Bezesporu největší výhodou při nasazení mobilního telefonu jako autentizačního předmětu je skutečnost, že jej vlastní téměř každý a je běžně používán při každodenní činnosti. Proto se lze domnívat, že v tomto případě není narušen uživatelský komfort, tak jak je tomu v případě užití ostatních autentizačních prostředků. Mobilní telefony jsou využívány neustále a tak uživateli nečiní potíže mít jej v patrnosti a v neustálé ochraně. Mobilní telefon jako prostředek k autentizaci může využívat volání, popř. službu SMS na poskytovatele datových služeb, nebo na autentizační autoritu a tím realizovat identifikaci. Další možností je vybavení mobilního telefonu patřičnou aplikací a telefon může být použit jako autentizační kalkulátor umožňující vygenerování jednorázových hesel. Někdy se využívá karta SIM mobilního telefonu jako autentizační prostředek. Tato metoda není ovšem tak bezpečná jako u ostatních autentizačních předmětů, protože z principu nelze zaručit, že klíč uložený v její paměti nelze kopírovat, vyjmout, či modifikovat.

## 2.2 Autentizace na základě vědomostí uživatele

Nejčastější způsob autentizace je realizován právě na základě znalosti tajné sekvence - kódu. Na první pohled se zdá, že tento způsob autentizace je nejbezpečnější, nejlevnější a nejpohodlnější. Průzkumy ukazují, že opak je pravdou. Hlavní důvod vytvářející z této autentizační metody poměrně málo odolný druh ochrany dat opět zapříčiňuje lidský faktor. Běžný uživatel příliš nemění přístupová hesla, používá sekvence, které jsou mu blízké a dobře pamatovatelné a také používá omezený počet přístupových hesel pro velké množství přístupů. Dalším nešvarem bývá zápis přístupového hesla někam poblíž místa autentizace, zápis hesla přímo na čipovou kartu, nebo prozrazení hesla další osobě. Při kterémkoliv hrubém porušení pravidel bezpečného zacházení s kódem si uživatel většinou neuvědomí, jaké následky může mít následný bezpečnostní incident.

Pokud by tento autentizační způsob měl být opravdu funkční a odolný, měl by uživatel dodržovat alespoň tyto zásady:

- přístupové heslo za určité období obměňovat,
- bezpečnostní heslo nikomu nesdělovat a nikam nezapisovat,

- pro jednotlivé přístupy k jednotlivým poskytovatelům dat používat jiné přístupové heslo,
- požívat složitější sekvence přístupových hesel,
- nepoužívat pro sekvence hesel vlastní iniciály, či data mající jednoduchou souvislost s uživatelem, atp.

Při pohledu na výše zmíněný výčet základních pravidel pro správu bezpečnostních hesel, je na místě tvrzení ověřené průzkumy, že autentizace na základě přístupových hesel není příliš bezpečná. Většina uživatelů používá pro autentizaci k různým systémům stejné heslo, aniž mají jistotu, zda může být toto heslo použito pro podvodnou autentizaci k jinému a mnohem rizikovějšímu poskytovateli dat.

Pokud by však uživatel dodržoval všechny výše zmíněné zásady, ztratil by tento druh autentizace svou uživatelskou přívětivost a pohodlí. Běžný uživatel si totiž není schopen zapamatovat více než několik málo jednoduchých sekvencí. Na základě tohoto zjištění byly v malé míře rozvíjeny způsoby autentizace na základě zapamatování určitého obrazu, určitého místa na obrazu, popř. určité sekvence obrazů [10]. Při této formě autentizace je uživatel schopen použít a hlavně zapamatovat si větší množství informací než v případě použití běžných přístupových hesel. Všechny podobné druhy autentizace využívají epizodické paměti člověka, která je efektivnější než paměť na sekvence alfanumerických posloupností (sémantická paměť) [11]. Množství kombinací při použití tohoto vizuálního přístupu je vyšší než při použití běžných bezpečnostních hesel. Obrazů může být velké množství a na každém obraze je spousta bodů sloužících k identifikaci. Navíc může být využita sekvence více obrazů po sobě následujících. Při tomto druhu autentizace je uživatel vyzván, aby si kupříkladu zvolil určitý obraz a na něm si zvolil určité místo. Označením tohoto místa při každém přístupu je uživatel autentizován. Takových způsobů autentizace je popsáno spoustu, nicméně v praxi se příliš neuplatňují. Teoreticky by tento způsob autentizace mohl být pohodlnější a bezpečnější, nicméně jsou s ním spojena další úskalí, jako jsou kvalita obrazu, rozlišení displeje a různých autentizačních zařízení, nebo snížená možnost utajení patřičného místa obrazu či sekvence obrazů při autentizaci ve veřejných prostorách.

Do kategorie autentizace pomocí znalosti identifikační charakteristiky osoby patří také užití jména a příjmení, rodného čísla, popř. dalších podobných identifikačních znaků. Autentizace na základě zmíněných identifikátorů není bezpečná a její používání se předpokládá pouze v procesech s nízkým bezpečnostním rizikem. Jméno a příjmení není unikátní informace, naopak ve všech národech existuje mnoho příjmení a jmen s velkou četností. Podle [1] 20 nejfrekventovanějších příjmení představuje v některých národech 40 až 60% veškerého obyvatelstva. O možnosti podvrhu v souvislosti s autentizací na základě jména a příjmení nelze hovořit, neboť jméno a příjmení není tajnou informací. V nedávné době bylo užití identifikace a v některých případech i autentizace pomocí rodného čísla prosazováno. Rodné číslo má velmi vysoký stupeň jednoznačnosti a mělo se za to, že lze tento identifikační údaj uchovávat v tajnosti. Nicméně v současné době nelze považovat použití rodného čísla za bezpečnou autentizační metodu, protože jeho obsah lze u většiny obyvatel zjistit.

## 2.3 Biometrická autentizace

Zdánlivě nejlepší a nejspolehlivější biometrické metody mohou být obtížně měřitelné, či nesnadno zpracovatelné. Na straně druhé některé biometrické metody mají vysokou míru přesnosti, či dobré měřitelnosti a přesto jsou méně použitelné. Osoby se mezi sebou navzájem rozpoznávají podle vzhledu obličeje, vzhledu celého těla, stylu chůze, podle hlasu, atp. a právě tyto biometrické vlastnosti člověka jsou v automatickém procesu velmi obtížně zpracovatelné a míra spolehlivosti jejich měření je často ovlivňována mnoha faktory, které nehrají roli při rozpoznání osob navzájem. Při automatických metodách souvisejících například s rozpoznáním obličeje mohou hrát roli chybové faktory měření, jako jsou: úhel pootočení obličeje, míra dopadu světla na obličej, případná kožní vyrážka, atp. Osoby při vzájemném rozpoznávání většinou tyto faktory zohlední. Naproti tomu biometrické metody pracující například na principu snímání otisku prstů jsou velmi vhodné pro automatizační způsoby autentizace. Jsou poměrně dobře zpracovatelné, snadno se ukládají do databází a vykazují vysokou spolehlivost při automatizovaném procesu identifikace.

Cílem ideální biometrické autentizační metody tedy není nalezení co největších rozdílů mezi lidskými jedinci, ale nalezení takových charakteristických prvků, které umožňují spolehlivé použití v automatizačním procesu. Jedná se především o tyto vlastnosti:

- přesně měřitelné význačné biometrické body,
- neměnnost těchto bodů po celou dobu vývoje člověka,
- snadný způsob měření,
- nízké působení chybových faktorů měření,
- obtížný způsob získání kopie či podvrhů…

Při hledání vhodné biometrické metody autentizace by neměla být zanedbána ani jedna z těchto klíčových vlastností. Sebespolehlivější biometrická metoda, vykazující se vysokým stupněm spolehlivosti může být bezcenná, pokud lze její výsledek snadno podvrhnout, nebo pokud se měřená biometrická vlastnost člověka často mění v každém stádiu jeho vývoje [2].

# 3 Biometrické metody

Biometrická měření lze aplikovat pro získání fyzických parametrů člověka (fyziognomie), nebo některých jeho vlastností, či způsobu chování (behaviometrie). Fyziognomie člověka je určena na základě dědičnosti, vývojem, popř. prostředím a jen velmi málo může být modifikována osobními návyky, životním stylem atp. Do této skupiny biometrie patří zejména:

- rozpoznání otisků prstů,
- rozpoznání duhovky, nebo sítnice oka,
- rozpoznání tvaru ušního boltce,
- rozpoznání tvaru obličeje,
- rozpoznání podélného rýhování nehtů,
- rozpoznání tvaru cévní struktury dlaně,
- rozpoznání geometrie ruky,
- rozpoznání bioelektrického pole,

- další málo uplatňované metody: vlastnosti zubů, spektroskopie kůže, DNA, atd.

Behaviorální biometrické metody bývají často ovlivněny osobními návyky, životním stylem, životosprávou, manuální zručností, fyzickým potenciálem atp. Patří se zejména tyto biometrické metody:

- analýza psaní na klávesnici,
- analýza dynamiky podpisu,
- rozpoznání hlasu,
- analýza dynamiky chůze,
- analýza pohybu očí, atd.

Ne každá z výše uvedených metod je vhodná pro automatizovaný proces autentizace. Každá z těchto uvedených metod je na jiném stupni pokročilosti z hlediska zpracování.

## 3.1 Rozpoznání otisků prstů

Nejvíce rozšířená biometrická metoda autentizace je založena na snímání otisků papilárních linií prstů. Tato identifikační metoda je používána už od konce 19. století, s rozvojem mikroelektroniky se rozšířila i do oblastí mimo kriminalistiku. Její výhoda spočívá v poměrně snadném snímání, ve stálosti po větší část doby vývoje člověka a také v jedinečnosti. Je prokázáno, že každý jedinec má jinou papilární kresbu prstů s charakteristickými rysy - markantami rozmístěnými ve specifické topologii [10]. Spolehlivost této metody tedy úplně závisí na způsobu snímání a na použité algoritmizaci při zpracování snímaných dat. Při zpracování se většinou neukládá do databáze obrazová podoba otisku prstu, ale vektory naměřených markant spolu s informací o jejich orientaci, odstupem od papilárií atp. Většina algoritmů počítá s určitým poměrem shody výsledku s předlohou, nikdy se nehledá dokonalá shoda.

Pokud je pominuta metoda snímání otisku prstu pomocí inkoustu a papíru, existují dvě základní metody snímání:

- statické snímání,
- snímání protažením.

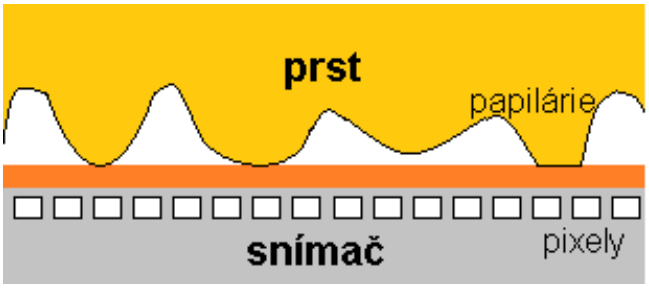
Statické snímače slouží k nasnímání celého otisku prstu v jednom kroku. Tyto snímače mohou být vybaveny snímačem teploty, tepu, tvaru cévního řečiště, popř. dalšími snímači biometrických vlastností prstu. Jejich nevýhoda spočívá v možnosti zanechání otisku prstu na skeneru, či v možnosti zkreslení vlivem znečištěné snímací části. Tyto snímače bývají většinou větší a tak je omezena jejich možnost použití u miniaturních autentizačních systémů. Z hlediska principu snímání nelze je realizovat v robustním provedení zabraňující mechanické poškození a proto není běžné jejich užití ve veřejných nechráněných prostorách.

Štěrbinové snímače pracují na principu snímání protažením prstu s následným seskládáním výsledného obrazu. Tyto snímače mají příčné rozlišení o velikosti několika jednotek pixelů a vyžadují jistou rutinu při snímání. Existuje větší nespolehlivost snímání spojená s nestandardním pohybem prstu. Jejich výhoda spočívá v menších rozměrech v nemožnosti zanechání otisku prstu po měření a v menší míře zkreslením měření díky znečištění snímače. Každým protažením prstu se ze snímače odstraní minulý otisk. Tyto snímače nelze většinou kombinovat s dalšími biometrickými metodami a mohou se tak snadněji stát terčem podvrhu.

Snímače zachycující papilární linie mohou pracovat na těchto principech:

- optické,
- kapacitní,
- teplotní,
- tlakové.

Každá ze zmíněných metod snímá za pomocí jiné technologie rozdíl mezi papilární čarou a mezerou měřeného prstu. Tyto hodnoty jsou získány maticovým snímačem (kapacitním, CCD – Charge Coupled Device, TFT – Thin Film Transistors…)[3]




Obrázek 5: Ukázka snímání papilárních linií

Na obrázku 5 je znázorněno snímání otisku prstů pomocí maticového snímače. Při jakémkoliv měření jsou získány rozdílné výsledky na patřičných pixelech maticového snímače mezi papilární čarou a mezerou.

## 3.2 Rozpoznání duhovky oka

Duhovka je oční orgán ovlivňující velikost čočky na základě intenzity dopadajícího světla. Zatímco některé optické vlastnosti duhovky jsou geneticky ovlivněné, jiné vlastnosti, zejména její kresba se vyvíjejí během vývoje plodu a jsou geneticky nezávislé. Je prokázáno, že každý jedinec má každou duhovku jinou a neexistuje žádná shoda duhovky mezi jakkoliv spřízněnými osobami. Tato skutečnost činí z biometrické metody snímání oční duhovky nejpřesnější ze všech.

Obrázek 6: Ukázka rozdílných kreseb očních duhovek u jedné osoby

Problém této metody spočívá v nutnosti použít vysoce přesnou digitální kameru. V současné době však technologický pokrok čím dál více usnadňuje nasazení kamer s velmi vysokým rozlišením. Větší problém spočívá ve zpracování získaného snímku duhovky. Při algoritmizaci se porovnávají předlohy s obrazem a jsou podrobeny testu statistické nezávislosti. I přes vysokou bezpečnost ochrany není tato autentizační

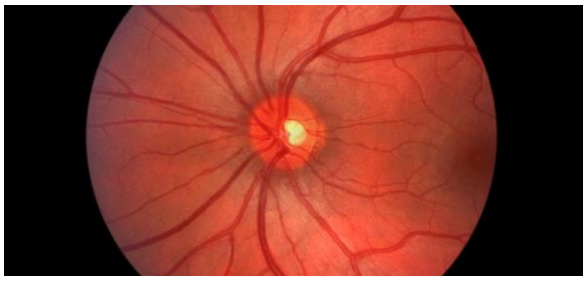
metoda běžně rozšířena a na svůj komerční rozkvět teprve čeká.

Na obrázku 6 je ukázka poměrně velkého rozdílu kresby očních duhovek jedné osoby [6].

## 3.3 Rozpoznání sítnice oka

Tato metoda využívá rozpoznání specifických cévních kreseb na pozadí lidského oka. Tyto cévy jsou nejvíce charakteristické v oblasti slepé skvrny, kudy sem vstupuje zrakový nerv, který se dělí do několika větví. Tak jako kresba na oční duhovce, je i kresba očního nervu a cév na pozadí lidského unikátní. Její snímání vyžaduje, aby se osoba podrobující se měření dívala do určitého místa a její zrak byl osvětlen infračerveným světlem.

Z hlediska přesnosti je tato metoda považována za jednu nejbezpečnějších metod. Jejímu masovému využití brání složitost snímání a malá účinnost u lidí se sníženou zrakovou schopností.

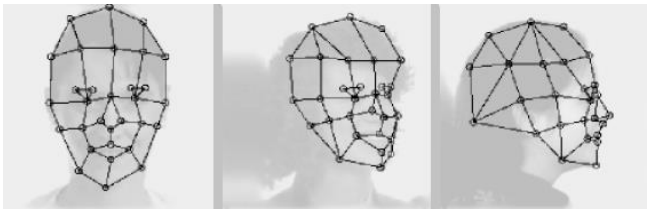


Obrázek 7: Ukázka sítnice lidského oka, získáno z http://cs.medixa.org

Na obrázku 7 je ukázka sítnice lidského oka. Tato metoda zdánlivě podobná s metodou snímání oční duhovky klade vyšší nároky na snímání a rovněž automatizační proces této autentizace je odlišný.

## 3.4 Rozpoznání tvaru obličeje

Jak bylo výše uvedeno, rozpoznání obličeje patří k nejběžnějším způsobům identifikace při styku mezi dvěma osobami. Lidská paměť a způsob vyhodnocení vnějších podnětů je však velmi odlišný od jakéhokoliv způsobu algoritmizace a proto patří metody pro rozpoznání obličeje k nejsložitějším. Obličej každého jedince je odlišen velkým množstvím charakteristických rysů, ať geometrických, či jasových. Jejich zpracování patří k nejsložitějším, nicméně v dnešní době nejvíce zkoumaným. V případě nalezení vysoce účinné metody identifikace obličeje by tato metoda zcela jistě vytlačila spoustu dalších metod, neboť její nasazení by nevyžadovalo žádné zvýšené náklady. Jako snímač poslouží obyčejná kamera, jejíž užívání je v dnešní době zcela běžné. Nyní však tato metoda vykazuje nízkou efektivitu a její nasazení se v automatizovaných autentizačních systémech neuplatňuje. Výhoda této metody by spočívala také v možnosti kontinuálního ověřování identity – tedy během celé doby práce s daty v chráněné oblasti informačního systému. Tuto možnost nemá každá z biometrických metod.

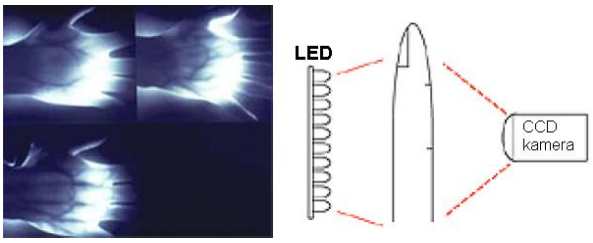


Obrázek 8: Ukázka sítě vytvořené elastickým mapováním, získáno z [4]

Metod pro vyhodnocení obrazu obličeje existuje mnoho. Jsou založeny na měření charakteristických vzdáleností na lidském obličeji a následném vytvoření sítě 3D naměřených bodů - obrázek 8. Rozměry jednotlivých bodů jsou porovnávány s předlohou a na základě složitých algoritmů vyhodnoceny. Míra spolehlivosti je navíc ovlivněna pootočením tváře, nestejným nasvícením obličeje, či možnými změnami vznikajících pod vlivem např. kožních vyrážek, atd. [4].

## 3.5 Rozpoznání tvaru cévní struktury dlaně

Jedná se o poměrně spolehlivou metodu, která se však vyznačuje poměrně složitým a nepohodlným snímáním. Její výhoda spočívá ve velmi malé pravděpodobnosti povrhu, protože snímané zápěstí je většinou podrobeno snímání proudu krve v cévním řečišti v kombinaci se snímáním teploty popř. s dalšími biologickými měřeními. Pro potencionálního útočníka je velmi obtížné zkonstruovat model ruky i s funkčním cévním řečištěm. Snímání dlaně se provádí pomocí čipu CCD. Před tento snímač je položena dlaň, která je z druhé strany prosvětlena nejčastěji pomocí několika diod LED. Pomocí velmi intenzivního světla je ruka částečně prosvětlena a na snímači CCD lze zaznamenat strukturu cévního řečiště, jeho větvení, a tloušťku. To vše je viditelné v infračerveném spektrálním záření. Výsledkem snímání, je potlačení obrazu ruky a zvýraznění cévního řečiště. Výsledný obraz je podroben dalšímu zpracování.

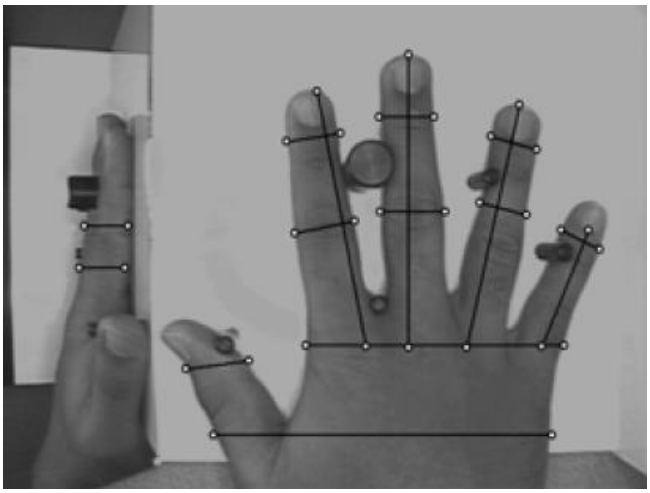



Obrázek 9: Ukázka snímku a princip snímání struktury cévního řečiště, získáno z [7]

Výhoda této metody spočívá v neměnnosti a unikátnosti struktury krevního řečiště dlaně. Je známo, že tato struktura je u každého jedince jiná. Další výhoda spočívá ve velmi snížené možnosti podvrhu. Struktura řečiště je skrytá, lze ji tedy sledovat pouze speciálními snímači, a navíc v krevním řečišti musí téct teplá krev, což je v infračerveném spektru dobře viditelné. Výroba jakéhokoliv falsifikátu k případnému podvrhu je extrémně náročná. Z tohoto důvodu se jedná o velmi bezpečnou biometrickou autentizační metodu. Na obrázku 9 je patrná úprava obrazu dlaně a zároveň je zde znázorněn princip snímání [7].

## 3.6 Rozpoznání geometrie ruky

Metoda pro rozpoznání geometrie ruky není příliš perspektivní. Je založena na principu měření rozměrů dlaně ve třídimensionální oblasti. Geometrie ruky není obecně příliš unikátní, ale pomocí měření mnoha polohových bodů na ruce lze dospět k uspokojivým výsledkům měření. Snímání ruky je prováděno na speciální podložce, na které je měřená dlaň fixována pomocí přesně rozmístěných kolíků. Obraz dlaně je snímán kamerou CCD. Do databáze není ukládán obraz, ale pouze rozměry přesně stanovených rozměrů ruky. Toto je bezesporu největší výhoda této autentizační metody. Výsledná identifikační informace je velmi malá a umožňuje snadnou manipulaci s databází biometrických vzorků.



Obrázek 10: Ukázka snímání geometrie ruky, získáno z [5

Na obrázku 10 je ukázána snímací podložka s přesně umístěnými fixačními kolíky. Na výsledném obrazu ruky lze přes 31 000 bodů a lze zde provést 90 různých měření vzdáleností. I přes toto velké množství rozměrů je po zpracování výsledná hodnota autentizační informace velmi malá. Nevýhoda této metody spočívá v malé unikátnosti geometrie ruky, a proto se příliš nepředpokládá její další vývoj [5].

## 3.7 Analýza psaní na klávesnici

Tato biometrická metoda spadá do oblasti behaviorálního měření. Styl psaní na počítačové klávesnici není ovlivněn fyziognomií člověka, ale jeho návyky, manuální zručností a podobnými vlastnostmi. Analýza psaní na klávesnici je poměrně nenáročná analytická metoda, při níž je měřena délka stisku klávesy a délka prodlevy mezi jednotlivými úhozy. Výsledky měření nelze získat jednorázovým měřením jako je tomu u ostatních biometrických metod, ale musí být podrobeno delšímu měření stylu psaní na klávesnici.

Velkou výhodou této metody je její hardwarová nenáročnost a také možnost provádění analýzy po celou dobu činnosti v chráněné datové oblasti. Další výhodou tohoto měření je zisk poměrně malého výstupního souboru a tím snadná manipulace s databází. Nevýhodou této metody je bezesporu její časová nestálost a rovněž poměrně malá unikátnost. Dynamika psaní na klávesnici se může měnit za poměrně krátkou dobu. Rozdíly dynamiky psaní u jednoho člověka mohou být ovlivněny četností psaní na klávesnici, osvojením určitých návyků, popř. zlozvyků při psaní, motorickou změnou pohybového ústrojí ruky, popř. únavou, špatnou viditelností klávesnice, požitím alkoholu či tlumících prostředků, atp. Faktorů ovlivňujících dynamiku psaní existují celé spousty a záleží na vhodné algoritmizaci, která je schopna tyto faktory do jisté míry eliminovat. Další velkou nevýhodou této metody je poměrně velká pravděpodobnost záměny. Protože naměřených údajů nebývá potřebné množství a jejich přesnost není příliš vysoká, mají dosažené výsledky poměrně malou pravděpodobnost jednoznačnosti. Z toho důvodu bude mít tato metoda vždy vyšší koeficient FAR, než FRR, což ji znevýhodňuje pro použití v automatizovaných autentizačních systémech. A právě pro automatizovanou identifikaci by byla tato metoda velmi vhodná [2].

## 3.8 Analýza dynamiky podpisu

Metoda pro analýzu ručního podpisu využívá podobných principů jako analýza psaní na klávesnici. Prostředky k dosažení cíle jsou jiné, ale i zde se jedná o metodu měření jistého návyku při ručním psaní. Obvykle se zde neposuzují pouze statické parametry, jako jsou tvar písma, tloušťka čar apod. Posuzují se rovněž dynamické parametry, jako jsou síla přitlačení pera na podložku v určitých bodech a také rychlost psaní. Pro snímání ručního psaní může sloužit zápisník PDA či jiný běžný dotykový displej s jemným rozlišením. Vzhledem k tomu že měřených kritérií je oproti předchozí metodě více, je tato metoda rozhodně bezpečnější, mající tedy poměrně nižší koeficient FAR. Její velká nevýhoda spočívá ve složité algoritmizaci, jejímž výsledkem je poměrně rozsáhlá identifikační informace. Stejně jako u předchozí metody je toto biometrické měření obtížně napodobitelné. Z praxe jsou běžně známy případy podvrhu statického podpisu, tedy tvaru písmen, ovšem dynamiku podpisu, tedy rychlost, přítlak, či určité nespojitosti napodobit lze napodobit pouze za velmi obtížných podmínek [9].

## 3.9 Rozpoznání hlasu

Díky snadné možnosti snímání se jeví analýza rozpoznání hlasu jako velmi perspektivní metoda. Díky složitosti algoritmizace však nejsou výsledky této metody v současné době spolehlivé a tato metoda zatím nedošla svého masového nasazení. Jejími výhodami jsou:

- autentizace po telefonu na dálku,
- autentizace po celou dobu setrvání v chráněné datové oblasti,
- možnost nasazení v jakémkoliv prostoru,
- malá pravděpodobnost podvrhu,
- implementační nenáročnost.

V dnešní době se metody rozpoznání hlasu nejvíce využívá v oblasti kriminalistiky. V komerční sféře či v automatizovaných autentizačních procesech se prozatím běžně nevyužívá. Většina systémů pro rozpoznání hlasu srovnává naměřený vzorek s uloženým při užití tajné sekvence slov. Tato skutečnost není příliš praktická pro užití ve veřejném prostoru. Jakmile bude známá algoritmizační metoda pro

rozpoznání jakékoliv slovní kombinace, bude tento systém určitě užíván v mnohem větší míře [8].

# 4 Vícefaktorová autentizace

Při stávající úrovni vývoje biometrických metod nelze použít při žádosti o přístup k citlivým datům, či k cenným informacím pouze jednu autentizační metodu. V současnosti, žádná ze známých autentizačních metod nevylučuje možnost podvrhu, nebo neoprávněného přístupu. Zatímco autentizační předměty nelze oklamat, kopírovat, nebo modifikovat v útočníkův prospěch, lze je poměrně snadno zcizit. Naopak biometrické vlastnosti nelze od oprávněné osoby využít, ale lze autentizační biometrické systémy do jisté míry oklamat. Z toho důvodu je u většiny přístupů s vyšší mírou bezpečnosti vyžadována více faktorová autentizace. V praxi se běžně setkáváme při autentizaci kombinace užití přístupového hesla PIN a autentizačního předmětu. Tato kombinace násobně zvyšuje bezpečnost přístupu, protože případný útočník musí pro neautorizovaný přístup získat jak autentizační předmět, tak i přístupové heslo. Pokud oprávněná osoba dodržuje pravidlo, že tajné heslo uchovává odděleně od autentizačního předmětu, je pravděpodobnost bezpečnostního incidentu výrazně nižší. Z tohoto důvodu je pomocí více faktorové autentizace ověřován přístup k bankovním účtům či k dalším informacím s nejvyšší až kritickou mírou bezpečnosti.

Tabulka 1 Přehled jednotlivých biometrických metod ve vztahu k autentizaci

| systém | míra spolehlivosti | míra bezpečnosti |
|---|---|---|
| Rozpoznání otisků prstů | vysoká | vysoká |
| Rozpoznání duhovky oka | vysoká | vysoká |
| Rozpoznání sítnice oka | vysoká | vysoká |
| Rozpoznání tvaru obličeje | nízká | střední |
| Rozpoznání tvaru cévní struktury dlaně | vysoká | velmi vysoká |
| Rozpoznání geometrie ruky | střední | střední |
| Analýza psaní na klávesnici | střední | nízká |
| Analýza dynamiky podpisu | střední | střední |
| Rozpoznání hlasu | nízká | nízká |

Tabulka 2 Přehled jednotlivých biometrických metod ve vztahu k autentizaci - pokračování

| systém | perspektiva pro masové užití | pořizovací náročnost | výpočetní náročnost | zpracování v databázi |
|---|---|---|---|---|
| Rozpoznání otisků prstů | perspektivní | střední | střední | střední |
| Rozpoznání duhovky oka | méně perspektivní | střední | vysoká | náročné |
| Rozpoznání sítnice oka | perspektivní | vyšší | vysoká | náročné |
| Rozpoznání tvaru obličeje | velmi perspektivní | nižší | velmi vysoká | náročné |
| Rozpoznání tvaru cévní struktury dlaně | neperspektivní | vyšší | střední | nenáročné |
| Rozpoznání geometrie ruky | perspektivní | nízká | nízká | nenáročné |
| Analýza psaní na klávesnici | perspektivní | vyšší | střední | nenáročné |
| Analýza dynamiky podpisu | velmi perspektivní | nízká | vysoká | náročné |
| Rozpoznání hlasu | | | | |

Závěrem popisu biometrických metod je v tabulce 1 uveden jejich přehled s vyznačením důležitých ukazatelů [2]. Každá ze zmíněných metod je v současné době využívána s větším či menším objemem a každá ze zmíněných metod je vhodná pro různé účely. Kritéria výběru vhodných autentizačních metod jsou:

- míra bezpečnosti chráněné oblasti (bankovní účty, vojenská data, výrobní data…),
- resort užití (armáda, zdravotnictví, bankovnictví, školství, výzkum…)
- způsob autentizace (dálkový přístup, veřejné prostory, veřejné prostory s dozorem…)
- míra automatizace (autonomní systémy, systémy s osobní kontrolou, forenzní aplikace…)
- frekvence autentizace (přístupové systémy na frekventovaných místech, specializované přístupy, individuální přístupy…).

Kritérií určujících použití vhodné autentizační techniky může být mnoho. Vždy bude při výběru vhodné autentizační metody záležet na požadavcích správce datového přístupu.

# 5 Závěr

Úvod článku se zabýval popisem autentizačních technik a možností biometrie. Všechny popsané oblasti byly prostudovány z několika zdrojů a byly vyextrahovány nejdůležitější poznatky a problémy dané oblasti. Zároveň byly do práce přidány vlastní náhledy na danou problematiku, vlastní organizace některých metod a komentáře k některým oblastem.

Problematika spojená s autentizačními systémy je popsána v následující kapitole. Jsou zde naznačeny metody pro kvantifikaci spolehlivosti a bezpečnosti autentizačních technik. V této kapitole jsou jmenovány vědní obory, kterých se autentizace dotýká, popř. jak tyto obory mezi sebou souvisejí. Jsou zde popsány autentizační prostředky pomocí autorizačních předmětů, nebo možnosti užití biometrie v oblasti autentizace.

Ve třetí kapitole jsou popsány biometrické metody. Každá z autentizačních metod má svoji bezpečností úroveň, svoji spolehlivost a také jistou míru komfortnosti či uživatelské přívětivosti. Některé nejvýznačnější biometrické způsoby autentizace jsou popsány podrobněji.

# 6 Seznam použité literatury


[1] RAK et al. *Biometrie a identita člověka: ve forenzních a komerčních aplikacích*. Praha: Grada, 2008, 664 s. ISBN 978-80-247-6392-7.

[2] ŠČUREK, Radomír. *Biometrické metody identifikace osob v bezpečnostní praxi Studijní text* [online]. [cit. 2012-11-03]. Dostupné z: http://www.fbi.vsb.cz

[3] Fingerprint Recognition. In: *Http://www.biometrics.gov* [online]. [cit. 2012-11-03]. Dostupné z: http://www.biometrics.gov/Documents/FingerprintRec.pdf

[4] Face Recognition. In: *Http://www.biometrics.gov* [online]. [cit. 2012-11-03]. Dostupné z: http://www.biometrics.gov/Documents/FaceRec.pdf

[5] Hand Geometry. In: *Http://www.biometrics.gov* [online]. [cit. 2012-11-03]. Dostupné z: http://www.biometrics.gov/Documents/HandGeometry.pdf

[6] Iris Recognition. In: *Http://www.biometrics.gov* [online]. [cit. 2012-11-03]. Dostupné z: http://www.biometrics.gov/Documents/IrisRec.pdf

[7] Vascular Pattern Recognition. In: *Http://www.biometrics.gov* [online]. [cit. 2012-11-03]. Dostupné z: http://www.biometrics.gov/Documents/VascularPatternRec.pdf

[8] Speaker Recognition. In: *Http://www.biometrics.gov* [online]. [cit. 2012-11-03]. Dostupné z: http://www.biometrics.gov/Documents/SpeakerRec.pdf

[9] Dynamic Signature. In: *Http://www.biometrics.gov* [online]. [cit. 2012-11-03]. Dostupné z: http://www.biometrics.gov/Documents/DynamicSig.pdf

[10] Kriminalistické metody identifikace osob. In: [online]. [cit. 2012-11-25]. Dostupné z: : www.prf.cuni.cz/dokumenty-download/1404044797/

[11] Paměť a učení. In: *Psychologie.ff.cuni.cz* [online]. [cit. 2013-01-14]. Dostupné z: psychologie.ff.cuni.cz/studium/prf/pamet.pdf