Počítačově podporované informační technologie

Computer Aided Identification Technologie

Bc. Erik Hrbáč

Diplomová práce
2013

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

ABSTRAKT

Diplomová práce pojednává o rozvoji identifikačních technologií s využitím výpočetní techniky. V první části se věnuji vývoji počítačových identifikačních technologií, konkrétně biometrii. Druhá část je věnována informacím, jejich ochraně, přenosu a šifrování. Ve třetí části popisuji identifikační úlohu v kriminalistice – identifikace pachatele trestného činu pomocí DNA. Další kapitola je o identifikačních metodách v současnosti. Závěr diplomové práce je o možnostech využití daktyloskopie s využitím výpočetní techniky.

Klíčová slova: identifikace, informace, informační technologie, daktyloskopie, kriminalistika, biometrie, stopa

ABSTRACT

The thesis discusses about the development of identification technologies by using computer technology. The first part is devoted to the development of computer identification technologies, particularly biometrics. The second part is devoted to information, protection, transfer and encryption. In the third part describes the role of the forensic identification - the identification of the offender through DNA. The next chapter is about identification methods currently. The final section is about how to use fingerprinting using computer technology

Keywords: identification, information, information technology, fingerprints, forensic, biometrics trace

Rád bych poděkoval mému vedoucímu diplomové práce panu JUDr. Josefu Čejkovi a mému konzultantovi panu JUDr. Vladislavu Štefkovi za pomoc a podporu při zpracování této diplomové práce.

Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové/bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že diplomová/bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové/bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji diplomovou/bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou/bakalářskou práci nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- beru na vědomí, že pokud bylo k vypracování diplomové/bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky diplomové/bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové/bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na diplomové práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně …….

podpis diplomanta

OBSAH

ÚVOD

Již od dávných dob si člověk uvědomuje své unikátní, biometrické vlastnosti. Důkazem jsou například otisky dlaní v jeskynních u maleb na stěnách, které měly sloužit jako „podpis“ autora pod dílo.

S rozvojem počítačově podporovaných technologií se biometrické rozpoznávání stává částečně automatizovaným procesem. Doba jde velmi rychle dopředu, tudíž v této oblasti zaznamenáváme s velkým rozvojem, který má za následek to, že se setkáváme v praxi se stále větší oblastí využití těchto systémů. Tyto systémy jsou velmi složité a proto často dochází k obavám, že se můžou zneužívat citlivé informace. K těmto obavám dochází z neznalosti propracovaných systémů, obavy jsou totiž zcela zbytečné. Vývoj by se měl ubírat takovým směrem, kdy budou přicházet stále nové identifikační metody, které budou více a více bezpečné, aby nás dokázaly chránit. Studijní text, který bude následovat pojednává o problematice identifikačních metod, které mají počítačovou podporu. V práci také zmiňuji doposud známé metody zabezpečení a přenosu dat, neboť bezpečnost před únikem informací sehrává v této problematice velkou roli.

Vývoj informačních technologií jde stále dopředu, nemožné věci se pomalu stávají skutečností. Počítače jsou stále výkonnější, jejich pořizovací cena jde dolů tudíž se systémy stávají dostupnějšími pro komerční sféru. Důkazem toho všeho je nedávná realizace, kdy se začaly vydávat biometrické pasy. Otázkou je, kdy se tento technologický vývoj zastaví, a s čím nás dokážou vědci a vývojáři v této oblasti překvapit.

1 HISTORICKÝ VÝVOJ POČÍTAČOVÝCH IDENTIFIKAČNÍCH TECHNOLOGIÍ

1.1 Historie biometrie

Slovo biometrie je odvozeno od dvou řeckých slov; „bio“ znamenající život a „metric“ vyjadřuje měření. Biometrie je věda, zabývající se měřením charakteristik člověka. V dnešní době se o biometrii převážně mluví v souvislosti s počítačovou bezpečností, ale její kořeny sahají hluboko do minulosti. Lidé od pradávna navzájem rozeznávají podle různých fyziologických rysů. Mezi nejčastější ukazatele patří vzhled tváře a hlas.

Nejznámější a nejstarší biometrickou technologií je otisk prstu. Znalost papilárních linií na lidské kůži se objevuje u řady civilizací. Ve státě Idiana byly nalezeny kameny s rytými obrazy, tzv. „petrglyfy“, které znázorňují lidskou ruku s vyznačenými papilárními liniemi. Vytvořily je indiánské kmeny a jejich stáří se odhaduje na několik tisíc let před naším letopočtem.

Také u Asyřanů se našly pozůstatky otisků prstů a můžeme se oprávněně domnívat, že se používaly pro účely identifikace, jako v dnešní době. Ve zříceninách asyrského města Ninive z 9. století před naším letopočtem, byly nalezeny na úlomcích hliněných tabulek kromě zajímavých textů také otisky prstů. Otisky se nacházely vedle jména autora a to vyvrátilo domněnky, že vznikly omylem během psaní textu. Autor textu tak zabránil falzifikaci. Obdobné využití otisků prstů se prokázalo na keramice při archeologických vykopávkách v Egyptě a Řecku. [1]

První písemně doložená zmínka o praktickém využití biometrické metody pochází od cestovatele jménem Joao de Barros, který popisuje užití otisku prstů ve středověké Číně 14-tého století. Popisuje, jak čínský kupec za pomocí inkoustu otiskuje dlaně a chodidla dětí na papír, aby dokázal malé děti od sebe rozeznat. V některých oblastech se tento zvyk udržel až do dněních do. [1]

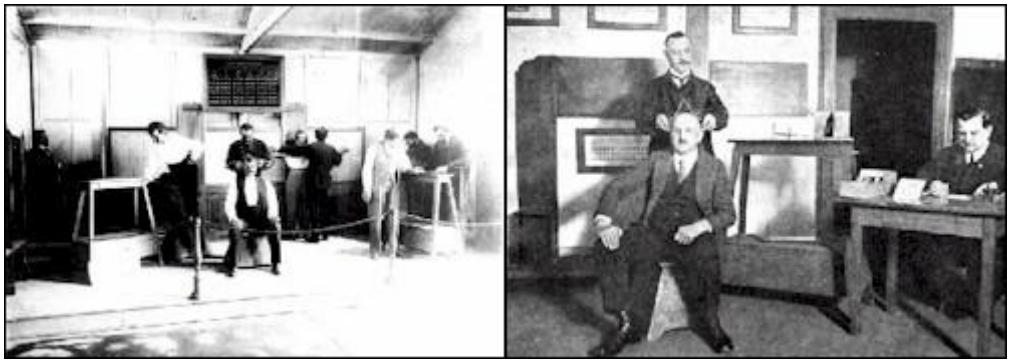
Počátky moderní biometrie se datují od roku 1882. Alphonse Bertillion, antropolog a šéf oddělení identifikace pachatelů pařížské police, hledal způsob, který by mu umožnil identifikovat již jednou odsouzené zločince. Hlavně jeho zásluhou se biometrie stala předmětem studií. Problém byl s opakované vězněnými zločinci, kteří při každém nové uvěznění uvedli falešné jméno a soudy jim nemohli opakovanou recidivitu prokázat.

Bertillion vynalezl metodu zvanou bertilionáž, která spočívala v měření fyzických znaků člověka. Zjistil, že některé charakteristické rysy, jako je velikost lebky nebo délka prstů zůstane stejná i když si daná osoba změní jméno, nechá se ostříhat vlasy nebo narůst vousy. Bertillionova metoda se rychle rozšířila po celém světě. Měření se zanášelo do antropologické karty, ve které byly délky hlavy dle různých tříd. Později k těmto údajům přibyly fotografie a otisky prstů. Po čase se však zjistilo, že různí dva lidé mohli mít tyto míry shodné, tudíž mohli být považováni za jednoho a toho samého člověka. Z toho důvodu se přestal Bertillionův systém používat. [1]



Obr. č. 1 - Alphonse Bertillion, Francis GaltonWilliam, James Herschel [1]

Biometrie samotná však nebyla zapomenuta. Anglický přírodovědec Francis Galton v roce 1988 publikoval svoji práci, v níž položil základy daktyloskopie. Pomocí matematických metod vypočítal, že existuje celkem 64 miliard variant uspořádání papilárních linií. Tím prakticky vyloučil možnost existenci dvou jedinců se stejným otiskem prstů. První základy daktyloskopické identifikace položil sir William James Herschel. Byl úředníkem žijícím v Indii a měl za úkol vyplácet důchody indickým vojákům, kteří neměli žádné osobní doklady. Domníval se, že vyplácí důchody i osobám, které již zemřeli, proto zavedl nový výplatní systém. Každá vyplacená osoba musela potvrdit příjem peněz otiskem ukazováčku a prostředníčku na výplatní listinu. Zabránil tak vzniku podvodů. Svoji metodu pak navrhl do vězeňství, aby se zamezilo záměnám těžkých zločinců za lehké případy. Jeho nápady však byly zavrhnuty a byly označeny za výplody fantazie. Problematice otisku prstů se věnovalo mnoho dalších osobností, například Dr. Henry Faulds, Juan Vucetich a český přírodovědec Jan Evangelista Purkyně, který jako první popsal jednotlivé papilární linie na koncových článcích prstů a klasifikoval je do devíti různých vzorů. [1]



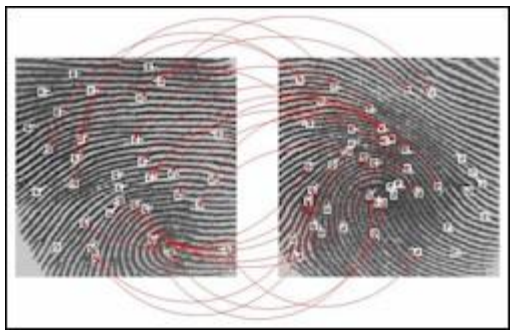
Obr. č. 2 - Ukázky měření v antropometrické laboratoři. [1]

Přes počáteční problémy se metoda otisku prstů nakonec dočkala uznání. I po nástupu nových technologií (DNA, oční duhovka) je i dodnes jednou z nejpoužívanějších metod pro identifikaci osob.

1.2 Biometrie s využitím informační technologie

Joseph T. James z univerzity v Miami v roce 1886 publikoval krátký článek, který pojednával o dvou hypotézách, na nichž do dnes stojí veškeré využití metody otisku prstu. První hypotéza předpokládala, že papilární linie se průběhu života nemění. Druhá předpokládala, že žádní dva lidé na světě nemají shodné obrazce papilárních linií. Problém byl v tom, že ani ze svých hypotéz nemohl vědecky podložit. S důkazem přišel až o dva roky později anglický přírodovědec Francis Galton. [2]

Metoda identifikace pomocí otisku prstů se od konce 19. století uplatňovala především v kriminalistice. Veškeré porovnávání otisků bylo prováděno policisty ručně, proces byl velmi zdlouhavý a náročný. Zlom nastal až v 60. letech 20. století s rozvojem výpočetní techniky. Výrazné zrychlení identifikačního procesu z rozsáhlých databází pomohl vývoj automatizovaných systémů, tzv. AFIS (Automated Fingerprint Identification Systems). Díky rozvoji osobních počítačů v 80. letech bylo možné využívat metodu otisku prstů i mimo sféru kriminalistiky. Začali vznikat aplikace, které kombinovaly techniku snímání otisků prstů s heslem nebo identifikační kartou. K masovému rozšíření došlo až v průběhu 90. let díky nižší ceně optických snímačů a rychlých srovnávacích algoritmů. Komerční sféra se však zaměřovala spíše na výpočetně snazší verifikaci, zatím co mnohem náročnější identifikace zůstává doménou systému AFIS. [3]



Obr. č. 3 - Porovnávání jednotlivých charakteristických bodů dvou otisků prstů. [2]

V kriminalistice nejznámější metodou získávání otisku prstů za pomocí inkoustu. Pro automatizované systémy je to však nevhodné, protože pro porovnávání je nutné otisk digitalizovat. Proto se nyní používají elektronické snímače otisků prstů, které mohou být optické, kapacitní, ultrazvukové nebo teplotní. Hlavní výhodou těchto snímačů je rychlost,

spolehlivost a uživatelská přívětivost. Rizikem této technologie může být krádež otisku prstů, který zanecháváme denně téměř všude. Kvalitní biometrické zařízení by mělo rozpoznat, zda se jedná o živý prst nebo o nějakou náhradu. Díky relativně nízké ceně a malým rozměrům jsou biometrická zařízení pro snímání otisků prstů i pro domácí použití – např. přístup k uživatelskému účtu v počítači nebo jako přístupový systém do domu. [3]

Mezi další metody, které se v poslední době začínají rozšiřovat, patří technologie založená na skenování oční duhovky. Jako snímací zařízení se využívají CCD kamery. Výhodou je, že není vyžadován blízký kontakt mezi uživatelem a snímačem. Snímek může být pořízen až do vzdálenosti jednoho metru. Duhovka může být zachycena i u osob se zhoršeným zrakem, pokud nemají poškozenou samotnou duhovku. Nevadí ani brýle či kontaktní čočky. Díky tomu, že metoda nevyžaduje žádný fyzický kontakt se snímačem, je tato metoda přijímána velmi kladně. [3]

Další používané metody vycházejí z geometrie ruky, dynamiky podpisu, rozpoznávání obličeje, dynamiky stisku kláves a mnoho dalších. Metody nejsou moc rozšířené, protože se dají jednodušeji obelstít. Třeba i takové metoda, jako je identifikace pomocí DNA, má svoji nevýhodu a tou je identita genetické informace u jednovaječných dvojčat. Některé nové výzkumy ovšem naznačují, že i jednovaječné dvojčata se na genetické úrovni liší. [3]

2 MOŽNOSTI ZPRACOVÁNÍ INFORMACÍ V BEZPEČNOSTNÍM SEKTORU

2.1 Co je to informace?

Slovo informace je běžnou součástí slovní zásoby, používáme ji tak často, že se vůbec nezajímáme o jeho významu. Nejsme schopni ji definovat, nicméně jsme schopni poukázat na konkrétní příklady a na nich dát najevo, že chápeme úlohu informace v každodenním životě. Není pochyb o tom, že člověk, jež neumí zacházet s informacemi, by neobstál v nynější společnosti, kterou máme ve zvyku nazývat společností informační. Pro běžný život si s tímto intuitivním chápáním vystačíme, nicméně informační profesionál potřebuje mnohem rozsáhlejší teoretické znalosti. [4]

Pojem informace zapadá mezi nejobecnější kategorii současné vědy i filosofie – řadí se mezi takové pojmy, jako jsou například pojmy hmota, myšlení, pohyb, poznání, vědomí, prostor, atd. Máme k dispozici různé způsoby jejího definování, záleží na tom, ve kterém vědním oboru či oblasti lidské činnosti se zabývá.

Příklady definic informace: [4]

2.1.1 „Laický“ pohled na informaci

- Sdělení, zpráva
- Zformování, vnesení tvaru
- Znalost sdílená v komunikaci – to, co MY víme
- Jazykový projev, ve kterém se konstatují určitá fakta

2.1.2 Filosofické pojetí informace

- Vlastnost hmotné reality být uspořádán a její schopnost uspořádávat (forma existence hmoty vedle prostoru, času a pohybu) (ZEMAN)
- Vnímatelný obsah poznaného nebo předpokládaného obrazu skutečnosti, který je možno využít pro život člověka
- Potenciálně komunikovatelný poznatek o objektivní realitě

- Poznatek o určité skutečnosti, předmětu nebo jevu zachyceném ve zpřístupnitelné formě využitelný při přizpůsobování se člověka životnímu prostředí (CIGÁNIK)
- Význam přiřazený obrazům, údajům a z nich utvořeným lidským celkům. Informace představuje míru uspořádanosti systémů na rozdíl od entropie, tj. míry neuspořádanosti.
- Obecně vědní kategorie pro označení výsledku odrazu v systému (fyzikálním, biologickém, sociálním, technickém), jakož i prostředku přenosu resp. sdělování tohoto výsledku uvnitř systému a mezi systémy. Protože obsahem odrazu je varieta odráženého objektu, představuje informace po obsahové stránce odraženou varietu. (STRAKA)

2.1.3 Komunikační pojetí informace

- Obsah procesu lidské komunikace, odevzdávání a přijímání oznámení, jejich přenos osobním kontaktem, zvukem, signálem a prostředky masové komunikace
- Každý znakový projev, který má smysl pro komunikátora i příjemce (LAMSER)
- Objektivní obsah komunikace mezi souvisejícími hmotnými objekty, projevující se změnou stavu těchto objektů (BRILLOUIN)

2.1.4 Kybernetické pojetí informace

- Název pro obsah toho, co se vymění s vnějším světem, když se mu přizpůsobujeme a působíme na něj svým přizpůsobováním. Proces přijímání a využívání informace je procesem našeho přizpůsobování k nahodilostem vnějšího prostředí a aktivního života v tomto prostředí (WIENER)
- Zpráva o objektivní realitě, která funguje jako zpětná vazba
- Část poznání, která se používá k orientaci, k aktivní činnosti, k řízení - s cílem zachovat kvalitativní specifičnost systému a tento systém zdokonalovat a rozvíjet
- Proces, kdy určitý systém předává jinému systému pomocí signálů zprávu, která nějakým způsobem mění stav přijímacího systému

2.1.5 Matematický přístup k informaci

- Energetická veličina, jejíž hodnota je úměrná zmenšení entropie systému
- Poznatek, který omezuje nebo odstraňuje nejistotu týkající se výskytu určitého jevu z dané množiny možných jevů
- Obsah zprávy, který je definován jako záporný dvojkový logaritmus její pravděpodobnosti

2.2 Jak chránit informace?

Informace mají mnohdy nevyčíslitelnou hodnotu a proto je nutné je chránit, aby nedošlo k jejich zneužití či poškození. Existuje mnoho způsobů, jak docílit ochrany informací. Základ tvoří určení bezpečného a kvalitního úložiště. Dalším našim úkolem je stanovit, kdo může s informacemi přijít do styku. Krádež informace může mít mnohdy devastující následky. Je potřeba dbát na opravdu kvalitní přenosové trasy.

Možnosti ochrany informací:

- Bezpečné uložení informací
- Omezený přístup k informacím
- Šifrování a kódování informací
- Přenosové trasy

2.2.1 Bezpečné uložení informací:

Je důležité dbát na to, aby byly informace (data) správně skladována (uložena). Je také potřeba je zálohovat.

Datová média:

- Magnetické média – pevný disk, disketa, magnetooptický disk, magnetická páska
- Optická média – CD, DVD, Blu-ray
- Elektronická média – Flash paměť
- Externí datová úložiště – jedná se o online úschovny dat. V závislosti na finanční náročnosti nám nabízejí různé kapacity k uložení. Mezi nejznámější patří DropBox,

Google Drive, Box. Fungují na principu ozrcadlení, kdy si nainstalujete jejich klienta a na vlastním disku si vytvoříte složku. Tato složka se automaticky synchronizuje s externím úložištěm. V případě jakékoliv ztráty či poškození dat na Vašem disku, si můžete data kdykoliv stáhnout z této úschovny přes internetové rozhraní.

2.2.2 Omezený přístup k informacím:

Abychom předešli poškození, či zneužití informací, musíme k nim omezit přístup a chránit je tak. V případě, že se jedná o elektronickou formu informací, lze přístup k nim rozdělit na následující druhy:

Fyzický přístup k zařízení:

- Přístup k nosičům informací lze omezit za pomocí režimových opatření. Pomocí směrnic se stanoví, kdo a za jakých podmínek má přístup. Osoba musí prokázat totožnost (karty, heslo, biometrické údaje) a na jejím základě je jí umožněn přístup. Je potřeba vést evidenci přístupů, aby se mohly zpětně dohledat a identifikovat osoby, které měly naposledy přístup k zařízení.

Vzdálený přístup:

- Informace, které jsou uloženy na vzdáleném úložišti či serveru jsou běžně přístupné těm osobám, které znají přístupové údaje (nejčastěji jméno a heslo). Všichni uživatelé by měli mít své jedinečné přístupové údaje. Díky tomu se dá zpětně dohledat jakýkoliv nežádoucí počin s informacemi. Každý uživatel by měl mít kvalitní heslo, které nelze jen tak rozluštit. Doporučuje se použití alespoň 10 znaků. Opravdu kvalitní bezpečnostní heslo by mělo obsahovat 14 znaků a více. U hesla je dbán důraz na to, aby byly použity odlišné velikosti písmen, kombinace písmen a číslic, různá interpunkční znamínka, mezery, atd.

2.2.3 Kódování a šifrování informací

Kódování informací používáme proto, abychom chránili data při jejich přenosu před neoprávněným přístupem cizích osob a programů. Zaměříme se na zabezpečení dat.

2.2.3.1 Kódování

Jde o proces, který nám převádí text z jedné abecedy na text v druhé abecedě. U tohoto převádění je zapotřebí dbát na to, aby nebyl nijak pozměněn obsah dat, protože by pak příjemce text nerozluštil a z toho důvodu by kódování ztrácelo význam. Klasický příklad kódování je Morseova abeceda, znaky jsou nahrazeny tečkami a čárkami. V dnešní době se nejčastěji používá Huffmanova a aritmetická metoda kódování. Používají se při kompresi dat. [5]

2.2.3.1.1 Huffmanovo kódování:

Tento algoritmus byl vynalezen už v roce 1952, nicméně i přes jeho stáří je nadále jeden z nejpoužívanějších. Algoritmus si zakládá na pravděpodobnosti výskytu jednotlivých znaků. Těm znakům, které se vyskytují v textu nejméně je přidělován delší kód a více se vyskytujícím znakům se poté přidělují kratší kódy. Na témže principu byla vyvinuta telegrafní Morseova abeceda a to na samém začátku 19.století.

Princip této metody spočívá ve vytváření binárního stromu, jehož koncové uzly odpovídají symbolům původní abecedy, hrany jsou ohodnoceny symboly 0 a 1, uzly jsou ohodnoceny pravděpodobností výskytu. Pravděpodobnost vnitřního uzlu je přitom rovna součtu pravděpodobností jeho následníků. Uzly řadíme do posloupnosti a to podle rostoucí pravděpodobnosti. V každém kroku z ní odstraníme dva uzly s nejnižší prioritou, vytvoříme z nich následníky nového uzlu a ten zpět zařadíme do seznamu.

Huffmanův kód vlastní dvě důležité vlastnosti. Jedná se o kód s minimální délkou a je jednoznačně dekódovatelný. Nicméně jeho problémem je to, že musíme znát rozdělení pravděpodobností výskytu jednotlivých symbolů. Odhad můžeme v průběhu komprese upřesňovat. [5]

2.2.3.1.2 Aritmetické kódování

Aritmetické kódování oproti jiným metodám, neboť nepracuje principem nahrazování vstupního znaku zvláštním kódem. Namísto toho se kódovaný vstupní proud znaků nahradí pouze skutečným číslem z intervalu <0,1).

Na popud pravděpodobnosti výskytu jednotlivých symbolů vstupní abecedy, je každému všem symbolům přirazena odpovídající poměrová část intervalu <0,1). V průběhu kódování je poté celý interval <0,1) postupně omezován, a to z obou stran na základě postupně přicházejících symbolů. Všechny symboly si vyberou z aktuálního intervalu odpovídající poměrovou část a ta se poté stane novým základem pro v pořadí další symbol. Kódovaná hodnota se poté prezentuje libovolným, reálným číslem, jež leží ve výsledném intervalu získaném po přečtení všech symbolů na vstupu. V důsledku toho, že z takto reprezentované hodnoty není možné při dekódování určit konec zprávy, je zapotřebí navíc ke zprávě ještě přidat speciální znak, který nám označuje konec, eventuálně musí být uložena také délka původní posloupnosti. [5]

2.2.3.2 Šifrování

Jedná se o metodu, která mění podobu zdrojových dat a to do takové míry, že jej v ideálním případě nemáme možnost bez šifrovacího klíče rozluštit. Šifrování se používá pro přenos tajných informací, pro jejich uchování na veřejném místě, apod. Opakem šifrování je dešifrování. [5]

- Kryptografie – jedná se o obor, který se zabývá ochranou informací ve výpočetní technice (šifrování + dešifrování dat).

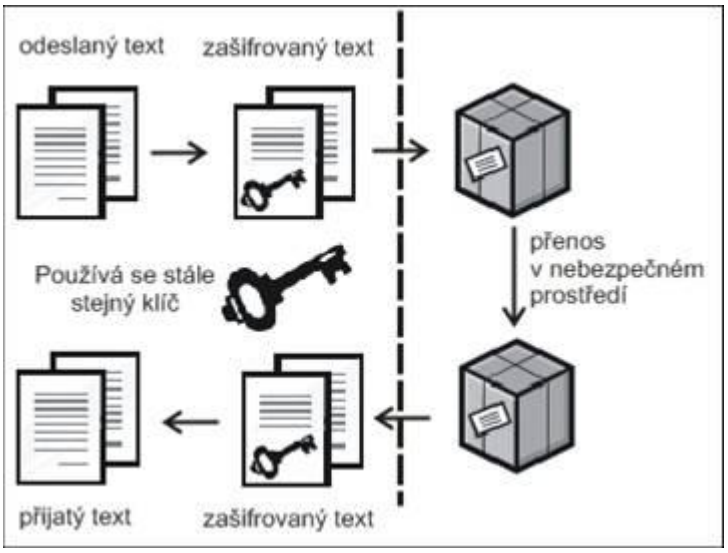
  Př. šifrování – pokud zaměníme písmena ve zprávě, jako např.: „A“ na „F“, „B“ na „G“, „C“ na „H“. Tak se nám celá abeceda posune o 5 znaků. Pomocí toho nám vznikne např. ze zprávy „Ahoj“ zpráva „Fmuo“, která působí utajeně.

Symetrická kryptografie

Symetrická kryptografie používá pouze jednoho klíče, který slouží jak pro šifrování, tak pro dešifrování.

V této metodě záleží tajnost zprávy na tajnosti klíče. Šifrování textu je velmi rychlé. Používá se také pro šifrování dokumentů, které nikam neposíláme, pouze chceme docílit zamezení jeho přečtení.

Tato metoda má mnoho nevýhod. Jednou z nich je počet klíčů, neboť tolik metod, aby měla každá dvojice na světě vlastní klič, není. Jednou z mnoha nevýhod je také ta, že pokud komunikujeme s nějakou osobou přes internet a potřebujeme jí tento klíč sdělit, hrozí jeho odhalení. [5]



Obr. č. 4 - Symetrická kryptografie [5]

Druhy symetrické kryptografie:

- Substituční metoda – tato metoda nahrazuje zvlášť každý symbol v textu jiným symbolem, nebo skupinou symbolů.

Příklad šifry:

- Proces šifrování „posun písmene v abecedě“ – klíč „5|10|2“ – délka klíče = 3.

5	10	2	5	10	2		
N	A	Z	D	A	R	=	NAZDAR
S	J	B	CH	J	T	=	SJBCHJT

Obr. č. 5 - Substituční metoda šifrování [5]

Každé písmeno je šifrováno zvlášť. Posun prvního písmene je o 5, druhého o 10 a třetí se posunuje o 2, následuje posun písmene opět o 5. Dešifrování probíhá obdobně.

- Transpoziční metoda – tato metoda mění pořadí znaků obsažených ve zprávě, nicméně nemění samotné symboly.
  Příklad šifry:
- Zapisování znaku tabulky, jež má stejně sloupců, jako klíč písmen.

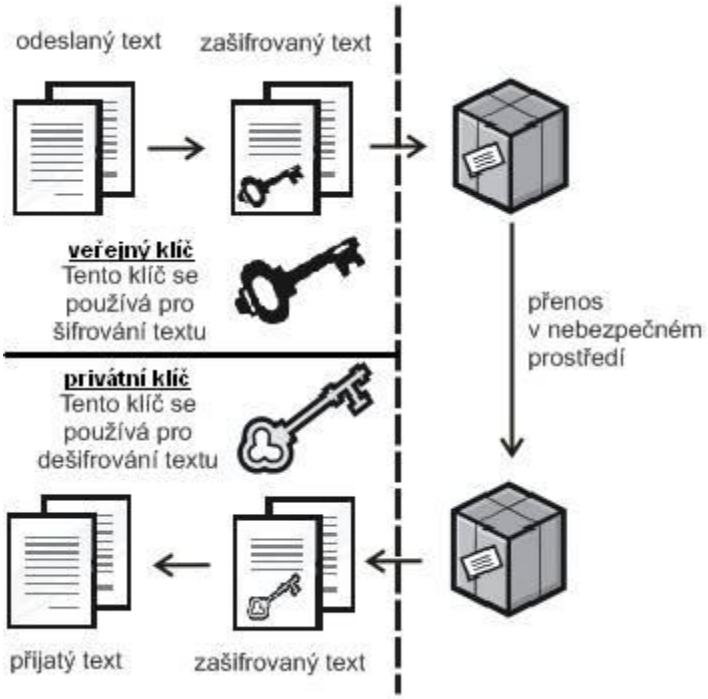
3	4	2	1
K	L	I	C
T	A	J	N
A		Z	P
R	A	V	A

Obr. č. 6 - Transpoziční metoda šifrování [5]

V této tabulce se poté čte šifra po sloupcích, začíná se tím sloupcem, ve kterém má klíč písmeno nejblíže začátku abecedy.
Věta „Tajna zprava“ byla díky klíči „klic“ zašifrována na zprávu „NPAJZVTARA A“.

Asymetrická kryptografie

Asymetrická kryptografie používá dva klíče. Jeden klíč slouží k zašifrování (tzv. klíč veřejný) a druhý slouží k dešifrování zprávy (tzv. klíč privátní). Použití klíčů: jedna osoba vlastní oba dva klíče. V případě, že mu někdo chce poslat zprávu, obdrží pouze jeho veřejný klíč, privátní klíč nikomu nedá, ten používá POUZE pro sebe. Tímto docílíme toho, že výsledný text si přečte pouze on, nikoliv kdokoliv jiný včetně odesílatele. Dostáváme se tedy k hlavní výhodě, lidé si mohou měnit klíče pomocí internetu, a to i s rizikem, že se tento klíč prozradí. Jedná se totiž o klíč veřejný. Není tedy potřeba tolik klíčů. Bohužel tato metoda má i svá negativa, je zhruba 1000x pomalejší, než metoda symetrická.



Obr. č. 7 - Asymetrická kryptografie [5]

Kryptoanalýza

Kryptoanalýza slouží k dešifrování textů. V případě, že aspoň tušíte, co chcete hledat (text v angličtině, zdrojový kód v programovacím jazyce, atd.), máte schopnost pomocí kryptoanalýzy, na základě četnosti výskytu jednotlivých znaků, statistických údajů pro daný jazyk, dešifrovat text. To v praxi znamená, že „nesmysl“ v podobě „asdfkhlahe“ by nedokázala ani kryptoanalýza dešifrovat. Z čehož plyne, že vlastnost zakódování stejného textu jinak nám znesnadní kryptoanalýzu. Je důležité se držet hesla, čím je klíč delší, tím je to lepší.

2.2.3.3 Digitální podpis

V dnešní době plné bankovních transakcí prováděných přes internet, posílání důležitých emailových zpráv, bychom se nemohli obejít bez digitálního podpisu. Podle digitálního podpisu poznáme pravost dokumentu a také to, zda nám zprávu zasílá opravdu ten, od koho ji očekáváme.

Digitální podpis využívá vlastností asymetrické kryptografie, kdy autor podpisu má u sebe privátní klíč a pokud se chce podepsat pod dokument, tak ho použije. Každý, kdo má jeho druhý veřejný klíč, si může ověřit, zda je podpis správný.

Základními algoritmy, které se k podpisu datových zpráv používají, jsou algoritmy RSA, u kterých je bezpečnost založena na obtížnosti rozkladu velkých čísel, dále pak DSA, vycházející z algoritmu postaveném na matematickém aparátu diskrétních logaritmů.

Z praktických důvodů se takto nezpracovává celý dokument, ale pouze jeho otisk (tzv. hash), velické krátký výtah vytvořený specializovaným algoritmem z celého dokumentu. Tento hash je poté zašifrován tajným klíčem a vzniká podpis. Ověření podpisu docílíme dešifrováním hashe za pomocí veřejného klíče autora, nezávislého výpočtu hashe z dokumentu a porovnání obou hodnot. V případě, že si odpovídají, tak je podpis ověřen a dokument je považován za důvěryhodný. Autor nemůže popřít jeho autorství, neboť k jeho tajnému klíči nikdo jiný nemá přístup a naopak, nikdo jiný nemůže zašifrovat hash dokument tak, aby po aplikaci autorova veřejného klíče vznikla správná hodnota. Dokument po podepsání nemůžeme změnit, protože pak hash vychází jinak. [5]

2.2.4 Přenosové trasy

Ať už pro přenos informací, ukládání informací, či pro přenos poplachových signálů potřebujeme zabezpečit bezpečné a kvalitní přenosové trasy. Máme následující druhy přenosových tras: [6]

2.2.4.1 Metalické

Jedná se většinou o telefonní linku, nebo internet vedený UTP kabelem. U větších firem nastává riziko odposlechu dat, a to tehdy, když se někdo napojí ilegálně na interní

počítačovou síť. V tomto případě nám nezbývá nic jiného, než se proti tomu bránit šifrováním dat.

2.2.4.2 Optické

Jedná se o novější technologii. Tyto kabely jsou výbornou přenosovou trasou. Přenos dat je velmi rychlý a spolehlivý. Optické kabely se nedají odposlouchávat a jsou odolné vůči elektromagnetickému rušení. Jedinou nevýhodou jsou poněkud dražší pořizovací náklady.

2.2.4.3 Rádiové

Pro jejich realizaci používáme elektromagnetických vln o takových kmitočtech, aby se efektivně šířily volným prostorem. Rádiové systémy se skládají z vysílací části s anténou, která vysílá elektromagnetické vlny a přijímací částí zpracovávající elektromagnetický signál vzniklý na přijímací anténě. Můžeme se setkat s distribucí signálu pomocí rozhlasových nebo televizních vysílačů, kde probíhá přenos pouze v jednom směru, nebo s obousměrným přenosem.

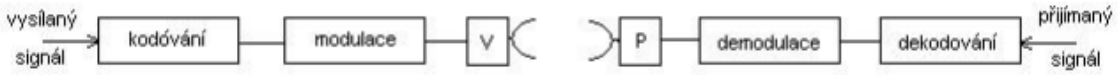
Abychom mohli díky radiovým vlnám přenášet užitečnou informaci, musíme u vysílání ovlivnit některý, z jejich parametrů a poté na přijímací straně informaci zpátky dekódovat, tomu se říká modulace. Amplitudová modulace spočívá v tom, že se přenášený signál projevuje jako obálka amplitudy nosné vlny harmonického průběhu o stálém kmitočtu. Kmitočtová modulace zase působí okamžitou změnu v kmitočtu nosné vlny, se stabilní amplitudou. U radiového přenosu digitálních signálů musíme u modulace vyjádřit několik stavů z konečné množiny hodnot. Při použití více stavů u dané přenosové rychlosti snížíme rychlost modulační a signál po modulaci zabere užší pásmo v radiovém spektru.

Použitá modulace je poté charakterizována počtem stavů a také typem. Zde jsou nejpoužívanější varianty těchto modulačních metod:

- Modulace fázová – PSK (nejčastěji se používá 4PSK)
- Modulace kvadraturní amplitudová – QAM (nejčastěji se používá 64QAM)

Vysílaný signál se překóduje, moduluje příslušnou metodou do vysokofrekvenčního pásma a vyslán anténou pomocí výkonových vysílacích obvodů V.

Strana přijímací provádí opačnou funkci. Klíčovou roli hraje funkce přijímacích obvodů P, jež obsahují filtr propouštějící jen potřebné pásmo a nízkofrekvenční zesilovač. [6]



Obr. č. 8 – Blokové schéma rádiového přenosu [6]

Jednotlivé vysílače rádiového přenosu mají předělené radiové kanály, jež jsou určené nosnou frekvencí a také šířkou přenášeného pásma. Volba této frekvence se musí provézt tak, aby se nerušily vysílače, které pracují na shodných nosných kmitočtech. Toho docílíme dostatečnou vzdáleností jednotlivých vysílačů od sebe.

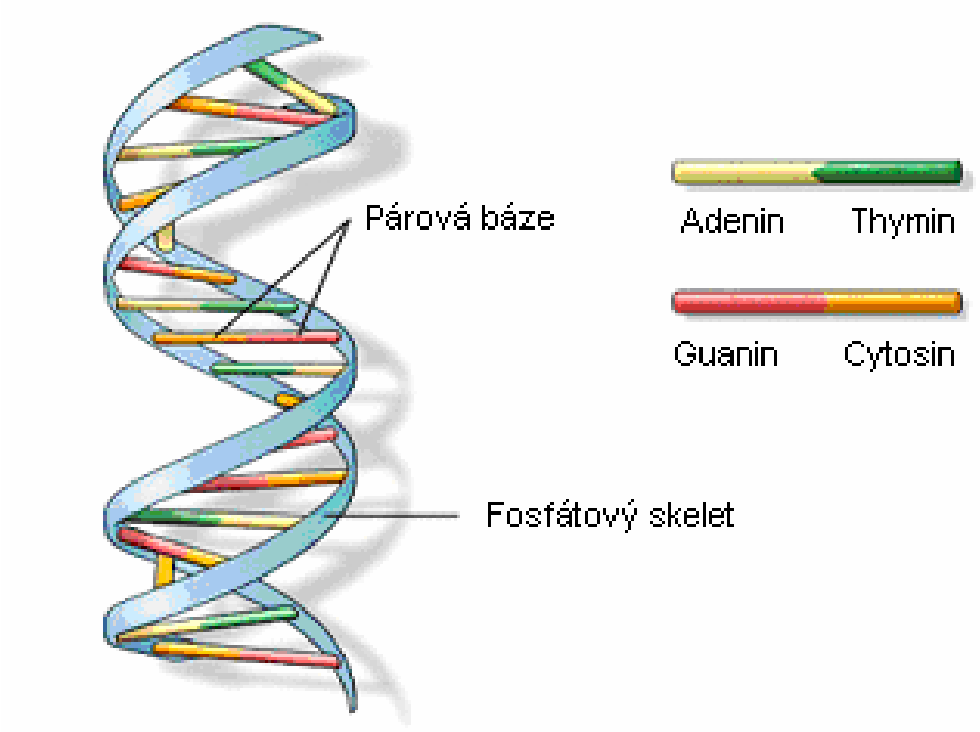
Nevýhodou rádiového přenosu je vysoká pořizovací cena. Hlavní výhodou jsou nízké provozní náklady a velmi vysoká spolehlivost. [6]

3 IDENTIFIKAČNÍ ÚLOHA V KRIMINALISTICE: IDENTIFIKACE PACHATELE TRESTNÉHO ČINU ZA POMOCÍ DNA

3.1 DNA = kyselina deoxiribonuleová

Jedná se o chemickou sloučeninu tvořenou dvěma spojenými polynukleotidovými řetězci. Tyto řetězce jsou svinuty do tvaru dvoušroubovice, patří mezi tzv. nukleoidové kyseliny. U eukaryotických organismů (rostliny, živočichové) je DNA uložena vždy uvnitř buněčného jádra, kdežto u prokaryot (např. bakterie) se DNA nachází volně v cytoplazmě. DNA je označována jako nositelka genetických informací pro všechny buněčné organismy. [7]

DNA je biologická makromolekula: polymer, dvoušroubovice, jež je tvořena dvěma řetězci nukleoidů v obou vláknech.



Obr. č. 9 – Struktura DNA [7]

3.2 Získání DNA stop

Biologický materiál můžeme rozdělit do následujících základních skupin:

- Biologický materiál, který pochází z lidského organismu
- Biologický materiál, který pochází ze zvířete
- Biologický materiál, jež je rostlinného původu

Pro kriminalistiku je nejdůležitější první skupina, kde biologický materiál pochází z lidského organismu. Tuto skupinu poté můžeme ještě rozdělit z hlediska odloučení od organismu: [8]

- **Materiál, jež byl samovolně odloučen** – moč, stolice, pot, slzy, sliny, chlupy, vlasy, nosní sekret, zvratky, placenta, plodová voda, atd. V tomto případě není použito násilí.
- **Materiál, který byl odloučen od těla zevním násilím** – krev, části tkání a orgánů, vytržené či oddělené vlasy, zuby, část pokožky, nehty.
- **Biologický materiál již zaniklého organismu** (smrt osoby) – těla mrtvol (částečná, celá), kosterní nálezy.

S biologickým materiálem, který pochází od zvířat, či rostlin se kriminalisté setkávají pouze v rámci mikrostop zajištěných na daném místě činu. Zkoumá se zpravidla jen pro rozlišení, že se nejedná o stopu pocházející z člověka. Pouze v určitých případech, kdy se jedná např. o krádež, či týrání zvířat je biologická stopa od zvířete považována za důkazní materiál. [8]

3.3 Místo činu

Biologické stopy pro nás mají velký význam a proto je nutné dbát na dodržování určitých pravidel v místě činu a to z důvodu, abychom stopu nijak neznehodnotili. Kontaminovaný materiál by poté mohl být vyloučený jakožto důkazní materiál, což by bylo pro řešení trestného činu nepřístupné.

Základní pravidla k zajišťování stop biologického původu: [8]

- Vyvarovat se dotyku s biologickou stopou rukou – U kontaktu pokožky se stopou se skupinové substance přenáší z potu na biologickou stopu. V důsledku tohoto přenášení poté dochází k mylnému závěru při zkoumání této stopy. Mnohdy také může přicházet k přenosu choroboplodných zárodků na člověka a díky tomu může dojít k infekci.
- V případě možnosti zajistit celý předmět s biologickou stopou – Zajištění celého předmětu s biologickou stopou je pro nás podstatně výhodnější, neboť popis a zajištění stopy provádí přímo znalec a tím se razantně zvýší možnost, že biologická stopa nebude poškozena.
- V případě, že tuto možnost nemáme, je zapotřebí biologickou stopu snímat nástroji, které jsou naprosto čisté, do naprosto čistých obalů a nádob – Opět je to z toho důvodu, aby nedošlo ke kontaminaci biologické stopy, protože by poté mohlo docházet k mylnému závěru.
- Je zapotřebí zajištěné biologické stopy a jejich nosiče bezprostředně vysušit, ke zkoumání se odesílají suché – Vysoušení biologických stop, a také jejich nosičů se provádí z toho důvodu, aby při následném skladování nedocházelo k jejich znehodnocování v důsledku spojeném s plísněmi, či napadením mikroorganizmy.
- Zajistit veškeré vyhledané biologické stopy – toto je jedno z dalších pravidel, které není mnohdy lehké splnit, jelikož se na místě činu může nacházet velké množství biologických stop. Veškeré zajištěné stopy se nemusí posílat ihned na analýzu, nicméně je dobré je mít pro případ, že bychom je v budoucnu potřebovali.
- Zajistit srovnávací biologický materiál – Tento druh materiálu určujeme podle druhu zajištěných stop. Ve většině případů se jedná o vzorek krve, vlasů a slin zúčastněných osob. Srovnávací materiál umožňuje znalci rozlišit biologické stopy dle vztahu jejich zůstavitele k tč. a případně tak upozorní na nutnost, že se musí provést další (doplňující) vyšetření.

Obr. č. 10 – Pracovní oděv [10]

Obr. č. 11- Zajištěný vzorek krve [11]

Obrázek 12 - Kriminalistický kufřík pro odběr biologického materiálu [12]

3.4 Odběr vzorku DNA u podezřelého

DNA můžeme získat víceméně z jakékoliv tělní tkáně. Je dokázáno, že DNA kterou získáme ze stěru ústní dutiny bude po informační stránce naprosto shodná s DNA získanou z krve, nebo vlasového kořínku.

Při odběru biologického materiálu se postupuje za pomocí bukálního stěru. Samotný odběr se provádí standardní odběrovou soupravou ze sliznice dutiny ústní. Není zapotřebí otvírat osobě ústa, stačí pouze odstavit dolní ret a jeho setření pomocí sterilního tamponu z vnitřní strany. V případě, že by podezřelá osoba kladla odpor, je zapotřebí souhlas státního zástupce. [13]

3.5 Analýza odebraných vzorků DNA

Molekuly kyseliny deoxyribonukleové (DNA) v chromozomech jsou získávány pomocí bukálního stěru. DNA je u všech jedinců jedinečné a neopakovatelné (výjimku tvoří jednovaječná dvojčata). Metodu, jež policie k následné analýze DNA používá, nedospívá k žádným novým výsledkům, vyjma alfanumerického kódu, ze kterého lze zjistit pohlaví – průkaz X a Y chromozomu. Je možné osobu díky kódu identifikovat, nicméně nelze zjistit další informace (vlastnosti charakteru, dědičné předpoklady, nemoci, atd.). [13]

K identifikaci osoby dochází pomocí porovnání vzorku DNA s kriminalistickými stopami. Můžeme tak identifikovat osobu, jejíž stopy byly nalezeny na místě činu, nebo také tělo mrtvého jedince. Díky genetické analýze je možno odhalit pachatele, který spáchal několik let starý zločin.

Nutno také zmínit, že ze stop DNA se po jejich vyschnutí nedá poznat jejich stáří, tím pádem osoba, jejichž DNA se našlo na místě činu, nemusí být nutně pachatelem trestného činu. Je také možnost si na několik hodin „změnit“ DNA, např. pokud se jedná o vzorek slin. Změnit DNA se dá také pomocí transplantace kostní dřeně, konkrétně tak u genetického profilu, jež byl získán ze vzorku z krevního obrazu.

Kromě standardní analýzy, se také provádí speciální analýzy Y chromozomu a mitochondriální DNA. Nicméně tyto dvě metody neumožňují individuální identifikaci a proto se také provádí jako doplňkové.

3.6 Genetický profil

Analýzou pořízených biologických vzorků nedostáváme informace o čisté DNA, nicméně jen o tzv. genetickém profilu, tj. o unikátní řadě čísel a písmen. Pomocí této informace můžeme jednoznačně identifikovat osobu a určit její pohlaví. Žádnou jinou informaci z tohoto profilu získat nemůžeme. Genetický profil je neměnný vlivem narůstajícího věku osoby. Toho by se dalo docílit pouze za pomocí transfuze krve, či transplantaci kostní dřeně. [13]

Za zmínku stojí ten fakt, že pro získání dalších informací z DNA je zapotřebí technické vybavení, které je drahou záležitostí. Policie ČR tvrdí, že nevlastní žádné takové zařízení, jelikož na ně nemají prostředky.

3.7 Databáze DNA

3.7.1 Právní základ databáze DNA

V roce 2002 na základě závazného pokynu policejního prezidenta u nás vznikla národní databáze DNA. Tento závazný pokyn č. 88/2002 pojednává o naplňování, provozování a také využívání národní databáze DNA. Obsahuje již přes 40tisíc genetických profilů. [13]

Právní základ databáze DNA upravuje zákon o policii a trestní řád. Samotná databáze DNA však zákonem upravena není a tudíž není ani pod žádným subjektem registrována tak, jak vyžaduje zákon o ochraně osobních údajů. Závazný pokyn prezidenta policie slouží jen pro tzv. „ vnitřní potřebu“ a tudíž pro širší veřejnost, ani pro osoby ve výkonu trestu není znám. [13]

3.7.2 Obsah národní databáze DNA tvoří:

Genetické profily, jež byly získány na místech doposud neobjasněných trestních činů a těch osob, které byly odsouzeny za spáchání zvláště závažné trestné činy, nebo proti nim bylo za tyto trestné činy vedeno stíhání. [13]

Genetické profily těch osob, které byly obviněny ze spáchání trestného činu, nalezených osob, na které bylo vyhlášeno pátraní, nemajících způsobilost k právním úkonům v plném rozsahu.

Genetické profily mrtvých těl, kosterních nálezů či ostatků lidských těl, které nemají známou totožnost.

Policie ČR hlásá, že genetické profily podezřelých, ani poškozených osob nejsou součástí databáze.

Biologický materiál se odebírá na všech služebnách policie, nicméně k přečtení odebraného genetického profilu a následujícím expertizám slouží Kriminalistický ústav v Praze. Tento ústav má pro tyto účely konkrétní zvláštní oddělení genetických expertíz. Genetické profily se uschovávají v části národní databáze, ve formě alfanumerického kódu. Tato část je nazývána CODIS (Comibned DNA Index Systém). Jedná se o SW, který byl vyvinut ve spojených státech a je poskytován FBI státním institucím na celém světě. Díky tomu je zaručen standardní provoz a jednotná správa dat. CODIS je používán zhruba 40státy. [13]

Policií ČR je uváděno, že do systému databáze může vstupovat pouze určitý počet vyškolených policistů, jejichž veškerá činnost v databázi je monitorována. Smazat vložený genetický profil může pouze certifikovaný pracovník Kriminalistického úřadu v Praze, tato činnost je také zaznamenána. V okamžiku, kdy byla osoba zproštěna obvinění, obdrží ústav cestou orgánů činných v trestním řízení požadavek, aby zlikvidovali genetický profil z databáze, který musí následně splnit. [13]

3.7.3 Další možnosti využití genetického profilu

Genetické profily, jež jsou se souhlasy daných osob ukládány do mezinárodních databází, jsou využívány mimo oblast práva např. v rámci výzkumu původu lidských populací. Jsou také veřejně přístupné databáze, ve kterých lze pomocí číselných hodnot Y haplotypu určité osoby vyhledávat nositele shodných, nebo téměř totožných genetických profilů. Díky tomu se nacházejí vzdálení příbuzní. Příkladem jsou neziskové organizace jako Sorenson Molecural Genealogy Foundation, která má kolem 20 000 záznamů, databáze Falily Tree DNA, která vlastní již přes 30 000 záznamů. Pro ČR již od úplného

začátku 21. století funguje společnost Genomac International, která se specializuje na genové testování. [13]

3.7.4 Genetický profil podle zákona o osobních údajích

Genetický profil je osobní údaj dle zákona o ochraně osobních údajů 101/2000 sb. Na sběr a starání se o genetické profily se vztahuje úprava tohoto zákona. Na vedení databáze se vztahuje oznamovací povinnost podle § 16, zákona o ochraně osobních údajů. Výjimkou u oznamovací povinnosti zákon připouští tehdy, pokud se v databází shromažďují osobní údaje, které ukládání správci databáze umožňuje zvláštní zákon, nebo je u takových osobních údajů zapotřebí k uplatnění práv a povinností, které vyplívají ze zvláštního zákona. Národní databáze DNA ovšem není pod žádným subjektem registrována. [13]

4 OBLAST VYUŽITÍ IDENTIFIKAČNÍCH METOD V SOUČASNOSTI

Oblasti využití identifikačních metod v současnosti

- **Bezpečnostní oblast**
  - Kriminalistika
  - Pátrání po pohřešovaných osobách
  - Bezpečnostní zpravodajství
  - Vězeňství
  - Boj proti zločinu
- **Oblast státní správy**
  - Vydávání řidičských oprávnění, pasů, víz.
  - Sociální a zdravotní pojištění
  - Zdravotnictví
  - Školství
- **Komerční sféra**
  - Bankovnictví
  - Docházkové a přístupové systémy ve firmách
  - Ochrana proti podvodům a zpronevěrám

Kvalita kteréhokoliv automatizovaného přístupového systému závisí pouze na kvalitě autentizačního mechanismu. V případě, že je identita autorizovaného uživatele ověřena v povolené odchylce, je systémem zprostředkován vstup do prostředí s řízeným přístupem, jinak je přístup zamezen. Je známých mnoho metod, které zabezpečují přístup uživatele a tvoří tak základ přístupových systémů. [13]

4.1 Autentizační metody:

- **Autentizace heslem** – jedná se o autentizaci, která je založena na faktu, že známe heslo
- **Autentizace předmětem** – jedná se o autentizaci, která je založena na vlastnictví daného předmětu
- **Biometrická autentizace** – jedná se o autentizaci, která je založena na biometrických charakteristikách člověka

4.1.1 Ověření heslem

Jedná se o tradiční metodu pro autentizaci uživatele, za použití tajného hesla. Toto heslo musí uživatel sdělit přístupovému systému, žádá-li o povolení vstupu do prostředí s řízeným přístupem. Hlavní výhodou tohoto řešení je technická nenáročnost a s tím spojené nízké pořizovací náklady. Tato varianta není ovšem moc bezpečná, jelikož má mnoho nevýhod. [13]

Autentizace, která je založena na hesle velmi často selže a to z několika důvodů. V případě, že si člověk vybírá heslo sám, volí si takové, které si lehce zapamatuje – tím pádem není heslo nijak složité a je lehké ho odhalit. V případě, že je heslo uživateli automaticky přiřazeno, hrozí zde riziko, že si jej někam poznačí a tím pádem ho může někdo nalézt. Je zapotřebí, aby byl zabezpečen mechanismus ke generaci, distribuci a použití hesel. [13]

Charakteristikou dobrého hesla:

- je distribuováno zabezpečeným způsobem
- je zapotřebí, aby heslo obsahovalo různé znaky, malá a velká písmena, kombinace číslic a písem
- má dostatečnou délku
- nemělo by se jednat o známou frázi či slovo
- nemělo by jej být schopno odvodit z údajů o člověku
- je zapotřebí toto heslo měnit

- nezaznamenávat si jej na přístupná místa

Jak je vidět, tak mít opravdu kvalitní heslo, které si člověk jednoduše zapamatuje je obtížné. Je zde mnoho negativ, kdy může být heslo rozluštěno. Z toho důvodu se doporučuje určitý druh šifrování, kdy uživatel její rozšifrování provede pomocí tajného klíče.

4.1.2 Ověření předmětem

Obecné označení pro autentizační předmět, jež potvrzuje identitu svého vlastníka je token, který musí být jedinečný a velmi těžce napodobený. Tokeny jsou používány v automatizovaných autentizačních systémech. Jsou vybaveny informací, která se používá při provádění autentizačního protokolu. Jelikož je informace, která je uložena na autentizačním předmětu jedinečná, musí se zabezpečit její ochrana proti duplikaci nebo krádeži. Z bezpečnostního hlediska je síla autentizace založená na vlastnictví předmětu v tom, že předmět, který obsahuje informaci, jež prověřuje identitu uživatele, je přenosný. Z toho plyne, že autentizační informace může být vlastnictvím uživatele. [13]

Největší hrozbou tohoto typu systému spočívá v tom, že autentizační předmět nám může někdo ukrást, případně padělat. Tuto hrozbu zmírníme tak, že autentizační systém požaduje token v kombinaci s heslem. Tím pádem musí daná osoba jak vlastnit předmět, tak znát heslo, jinak bude autentizačním systémem odmítnut. [13]

Používané autentizační předměty jsou:

- Tokeny s pamětí – magnetické, optické či elektronické karty – paměť vlastní jednoznačný řetězec k identifikaci.
- Tokeny, jež udržují hesla – tyto tokeny vydají určený vhodný klíč po zadání jednoduchého hesla
- Tokeny s logikou – umí zpracovávat jednoduché podněty (vydej: následující klíč, vydej cyklickou sekvenci klíčů).
- Inteligentní tokeny – můžou mít svoje vlastní vstupní zařízení určené ke komunikaci s uživatelem, vlastní časovou základnu, mohou šifrovat a generovat náhodná čísla, atd. Jedná se o tzv. „chytré karty“.

Obr. č. 13 – Token – Fortinet [15]

Hlavní nevýhodou této metody je opět jejich přenositelnost. S čím úzce souvisí, že v případě znalosti hesla a odcizení předmětu, se může osoba vydávat za někoho, kdo ve skutečnosti není.

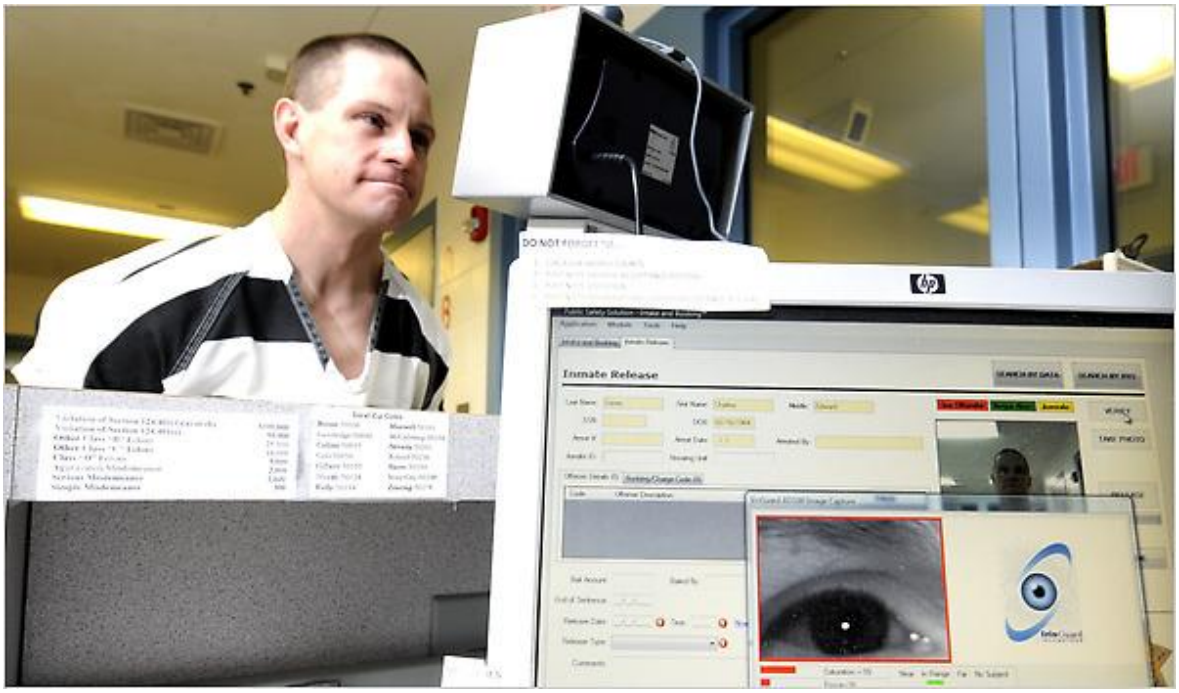
4.1.3 Biometrická autentizace

Biometrická autentizace je založena na automatizované zjišťování a porovnávání jedinečných biometrických charakteristik uživatelů přístupového systému. Jedná se o měřitelné fyziologické nebo chování se týkající vlastnosti, jež mohou být využitelné pro ověření identity jednotlivce. [13]

Biometrické prostředky identifikace člověka jsou např.:

- Otisky prstů
- Geometrie ruky
- Skladba oční sítnice
- Hlas
- Skladba oční duhovky

- Portrétní identifikace
- Skladba deoxyribonukleové kyseliny (DNA)



Obr. č. 14 – Identifikace pomocí skladby oční sítnice [16]

4.2 Použití biometrie v praxi

V dnešní době je jednoznačným trendem návrat biometriky do praxe. Biometrie má před sebou velkou budoucnost, jelikož neexistuje žádná metoda, která by byla takto blízce spojena s identifikací konkrétní osoby. Německo v roce 2004 vydalo na biometriku 12 milionů eur, v roce 2009 dokonce 377 milionů eur. [17]

Největším světovým zastupitelem biometriky jsou v dnešní době Spojené státy. Již od roku 2005 chtěli zavést biometrické pasy, nicméně zatím museli od tohoto kroku ustoupit. Důvodem byly nejasnosti v mezinárodní sféře, jaká data by měla být shromažďována a také v jaké podobě. Každý stát hájí své zájmy a bez konsenzu podstatné většiny se projekt velmi těžko podaří zrealizovat. [17]

Turisté a také běžní občané se ve Spojených státech setkávají s tím, co dříve bylo vyhrazeno pouze podezřelým a kriminálníkům. USA navíc dnes vydávají pro každého legálního pracovníka ze zahraničí identifikační kartu. Tato karta by v budoucnu měla

obsahovat biometrické prvky. Tato rozšíření budou snadnější než v případě pasů, jelikož nebude zapotřebí mezinárodního souhlasu, jedná se o vnitřní věc Spojených států. [17]

Obr. č. 15 – Snímaní otisku prstů v USA [18]

Od roku 2004 byly odebrány v USA otisky prstů a fotografie 23 milionů zahraničních návštěvníku na 115 amerických letištích. Náklady na veškerou americkou biometriku dosahují 8 miliard dolarů ročně. [17]

Ministerstvo obrany Spojených států používá pro všechny vojenské osoby identifikační kartu CAS (Common Access Card). Tato karta obsahuje biometrické data a také digitalizované fotografie držitelů, navíc pak jako ochranný prvek proti padělání hologramy. Doposud se vystavilo již přes 10 milionů kusů. [17]

V USA je flotila o stu nákladních vozidel, které slouží k dopravě nebezpečných materiálů (biologické, chemické, radioaktivní). Vstup do těchto flotil je možný pouze skrze biometrické systémy. Řidiči těchto flotil jsou sledování, zda nejsou pod stresem. Je zde i mnoho dalších systémů, které sledují dodržování tras těchto vozidel, plánované ale i neplánované zastávky, atd. [17]

Biometrika si našla cestu i do komerční sféry. Třeba hotel Ceasars Palace v Las Vegas ji používá pro přístup hostů do pokojů. A jak Disney Land (Kalifornie), tak Walt Disney World (Florida) používají biometriku - k tomu, aby osoby, které si zakoupily nepřenosný lístek, jej nemohli prodat dále. [17]

V květnu 2005 schválila horní komora parlamentu v Německu vydávání ePassu, jež obsahuje biometrickou technologii. ePass je vydáván od listopadu 2005, od března 2007 bude obsahovat i biometrické prvky – otisky prstů (jeden z každé ruky). Stejně tak musí mít všichni návštěvníci země, kteří mají dobu pobytu delší než tři měsíce biometrickou identifikační kartu. A na olympijských hrách v roce 2004 v Athénách byl přístup všem hostům do Německého domu umožněn pouze na základě biometrické identifikace. [17]

Biometricky nesmírně rozvinutým státem je Izrael. Hranice s pásmem Gazy denně překračuje za prací devadesát tisíc Palestinců, jež mají speciální identifikační dokumenty vydané izraelskou armádou. Obsahují biometrické údaje otisků prstů, dále také tváře a siluety ruky. Kromě toho je na nich nejen vytištěná fotografie, ale v digitalizované podobě je umístěná i na čipu. [17]

Obr. č. 16 - Identifikační karta v Izraeli [19]

Letiště Bena Guriona v Tel Avivu má pro časté cestující jakožto součást programu "frequent flyer" kartu rychlého odbavení. Tato karta obsahuje informace o siluetě ruky a otisky všech prstů cestovatele. Přístup do uzavřených prostor díky ní trvá jen cca deset sekund. [17]

V Iráku se vydává identifikační karta s biometrickými prvky, která je imunní vůči falšování. Při vytvoření šablony je tato odeslána i do centrální databáze – takže pokud je karta ztracena, data se dají z této databáze ověřit. Databáze obsahuje i další doplňkové informace, zvláště pak osobní historii dotyčné osoby – např. zda už někdy měla konflikt s vojenskými či policejními jednotkami. [17]

Obr. č. 17 – Identifikace pomocí oční sítnice v Iráku [18]

V Japonsku zase došlo k zavedení bankomatů, které pracují na principu biometrické identifikace dlaně. Podle zkušebního provozu dochází jen v 0,01 procentech k odmítnutí oprávněného uživatele a jen v 0,00008 procentech k akceptaci neoprávněné osoby. [17]

Obr. č. 18 – Identifikace pomocí otisků prstů v Čině [18]

5 DAKTYLOSKOPIE S VYUŽITÍM VÝPOČETNÍ TECHNIKY

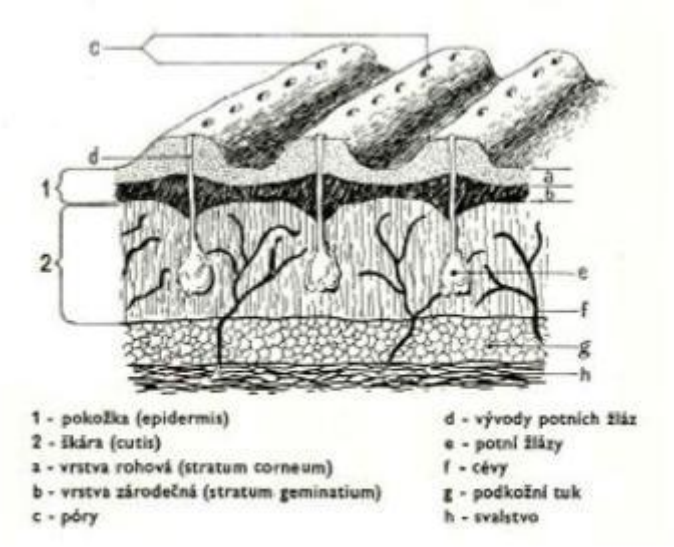
5.1 Co to je daktyloskopie?

Daktyloskopie je jedna z nejstarších kriminalistických metod, která se zabývá identifikací osob. Principy daktyloskopie byly používány již u starých lidských kultur. Identifikace osob v této oblasti vychází z existence papilárních linií, jež jsou vytvořeny na různých částech povrchu lidského těla. Tyto papilární linie se vyskytují pouze na vnitřní straně prstů horních končetin, dlaně obou rukou, dále pak prsty a chodidla nohou. Významnou roli zde hraje ten fakt, že papilární linie nejsou v dnešní době vytvořeny u jiných živočichů, než u člověka. V tomto důsledku můžeme díky nalezeným daktyloskopickým stopám zcela jistě určit přítomnost člověka, což je v kriminalistice velmi žádané. [8]

Daktyloskopie je nauka o obrazcích papilárních linií. Jedná se o metodu, která nám umožňuje identifikaci osob.

Vznik a trvání obrazců papilárních linií na končetinách se řídí následujícími zákonitostmi: [8]

- Na světě nejsou dva jedinci, jež by vlastnili shodné obrazce papilárních linií. Toto tvrzení nám potvrzuje i fakt, že za celou dobu existence daktyloskopické metody v kriminalistice nebyly dosud objeveny dva, do nejmenších detailů totožné obrazce papilárních linií.
- Člověk má po celou dobu svého života téměř neměnné obrazce papilárních linií. Je dokázáno, že obrazce papilárních linií se u člověka tvoří již v embryonálním životu. Tvoří se zde základ papilární linie, která zůstává po celý život člověka nezměněna. Dělaly se pokusy, kdy se v různých věkových odstupech snímaly otisky člověka a dospělo se k závěru, že se tyto obrazce nemění. Mírné změny byly způsobeny v důsledku stáří, kdy jsou tyto obrazce narušeny vráskami stárnoucí kůže. Jedná se ale pouze o narušení, nikoliv změnění.



Obr. č. 19 - Průřez lidské kůže [8]

- Papilární linie jsou relativně neodstranitelné, v případě, že není odstraněna i zárodečná vrstva kůže. K lidem se často dostávají mylné informace, že se dají pomocí spálení, sedření či seříznutí povrchové vrstvy papilární linie trvale odstranit, což není pravda. Dalo by se toho docílit pouze tehdy, když by byla odstraněna zárodečná vrstva kůže. V jiném případě se kůže zahojí a jsme zpět tam, kde jsme byli před poraněním.

Uvedené zákonitosti měly za následek to, že se daktyloskopie dostala na přední pozici identifikačních metod v kriminalistice. Přelomový rok, pro zavedení daktyloskopie je uváděn rok 1896. Pro daktyloskopii hrál do karet hlavně ten fakt, že snímání a uchování otisků je relativně snadnou záležitostí, samozřejmostí je dodržení základních pravidel.

5.2 Vznik daktyloskopických stop:

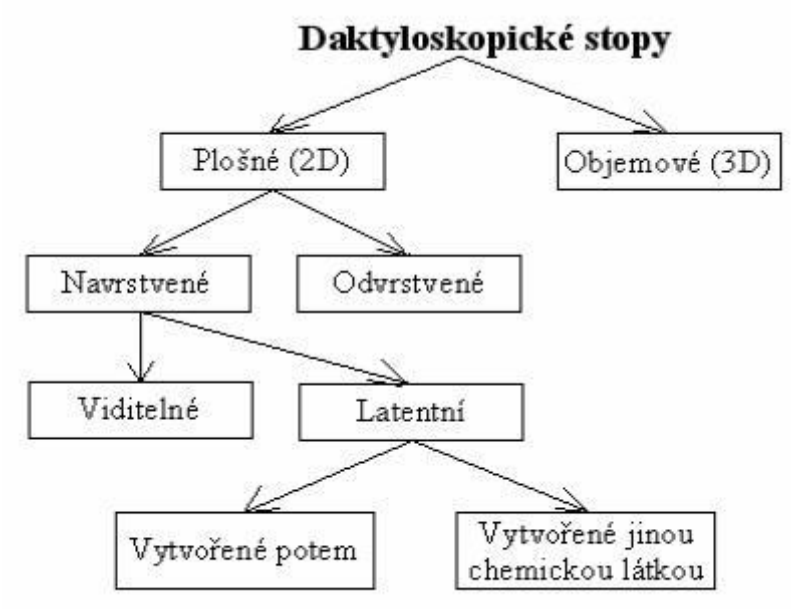
Daktyloskopické stopy vznikají v momentu styku člověka s jiným předmětem. Tento předmět je schopen přijmout a po nějakou dobu stopy (papilární linie) uchovat.

Vznik daktyloskopické stopy probíhá několika způsoby: [8]

- Vytvoří se ozrcadlený reliéf povrchové struktury papilárních linií. K tomuto jevu dochází zejména tehdy, pokud materiál, se kterým přicházíme do styku je schopen plastické deformace tlakem. Mohou to být také hmoty, jež jsou měkké za standardních klimatických podmínek, a v důsledku dotyku se na nich vytvoří reliéf, který si jsou schopny udržet (např.: pečetní plastelína, jejichž použití je v dnešní době rozšířené u pečetění trezorů). Dále jsou to hmoty, které změní své fyzikální vlastnosti díky teplotě končetin při doteku a na povrchu vznikne reliéf (např.: čokoláda, parafín, tuk, atd.). Daktyloskopické stopy můžou vzniknout také v průběhu fyzikální změny u objektů, jako například při tuhnutí vosku, usychání určitých druhů lepidel či laků. Takto vzniklé stopy zanikají tehdy, když dojde k razantní změně fyzikálních veličin – úplné roztavení. V určitých případech můžeme docílit toho, že stopy se vzniknou i na těle člověka. Daktyloskopické stopy, jež vznikají tímto způsobem řadíme do plastických daktyloskopických stop.

- Daktyloskopická stopa vznikne tak, že na papilární linie se přenese látka z povrchu předmětu a tím dojde k narušení povrchové struktury nosiče stopy. V místech odpovídajícím mezipapilárním prostorům zůstane původní povrch nosiče neporušen. Mechanismus vzniku tohoto druhu daktyloskopických stop může být různý. Působením vodní složky potu se rozpustí miniaturní množství látky, která má tu schopnost ulpět na vrcholcích papilárních linií (např.: na lepících páskách, lepidlech, atd.). Takto vznikají kvalitní daktyloskopické stopy, jež jsou vyhovující pro identifikaci. Obdobně mohou vznikat stopy na zledovatělém povrchu, nicméně za předpokladu, že okolní teplota je vyhovující. V případě styku papilárních linií s čerstvým nátěrem laku, barvy či krve vznikají rovněž daktyloskopické stopu a to tím, že se poruší souvislá vrstva nanesené látky, zatímco v mezipapilárním prostoru zůstane látka neporušena. Stejně tak v důsledku existence potu na papilárních liniích dochází ke vzniku daktyloskopické stopy při styku s mírně zaprášeným povrchem (např.: nábytek, sklo, apod.). V případech, kdy jsou ruce příliš suché, víceméně nedochází ke vzniku těchto stop. Takto vzniklé stopy jsou nazývány odvrstvené daktyloskopické stopy.

- Daktyloskopické stopy vzniknou tak, že se na vhodný nosič přenese látka, jež se nachází na vrcholcích papilárních linií. Jedná se o opak výše zmíněných daktyloskopických stop. Na vrcholcích papilárních linií nám ulpí určitá látka (krev, pot, barva, lak, apod.), která se poté přenese za pomocí dotyku na určitý předmět. Tyto stopy poté můžeme dělit na viditelné a neviditelné (latentní). Takto vzniklé daktyloskopické stopy se nazývají navrstvené daktyloskopické stopy.



Obr. č. 20 - Druhy daktyloskopických stop [8]

Nejrozšířenější skupinu daktyloskopických stop tvoří stopy, jež vzniknou přenosem potu, který vylučuje pokožka z vrcholků papilárních linií na vhodný nosič. Tyto stopy spadají do skupiny latentních stop, kdy pouhým běžným okem nemůžeme vypozorovat existenci stopy. Proto byla vymyšlena řada metod, které nám umožňují stopy zviditelnit. Metody jsou závislé zejména na vlastnostech daného nosiče. [8]

Daktyloskopické stopy představují rozšířenou skupinu kriminalistických stop. K jejich vyhledání, vyhodnocení, zajištění a následnému znaleckému zkoumání je zapotřebí technického vybavení a odborné znalosti. Další neocenitelnou vlastností existence daktyloskopické stopy je ten fakt, že díky nim můžeme mnohdy zjistit celý průběh objasňované události a to za pomocí rozmístění stop. [8]

Při stanovení kritérií, podle nichž je možné a účelné daktyloskopické stopy dělit, je proto nutné vzít v úvahu nejen hledisko technické, ale i kriminalisticko taktické. Významným kritériem, podle kterého se daktyloskopické stopy dělí, je počet identifikačních znaků obsažených ve stopě. Dle tohoto hlediska mohou být zajištěné stopy: [8]

- Upotřebitelné k identifikaci - sem patří stopy, jež obsahují nejméně 10 identifikačních znaků a mohou sloužit jako důkazní prostředek po provedeném identifikačním zkoumání.
- Částečně upotřebitelné stopy – tyto stopy obsahují 7-9 identifikačních znaků. Nemůžou být použity jako důkazní prostředek, případně jen výjimečně, ale poskytují informace taktického charakteru, kdy díky nim můžeme řadu podezřelých osob vyloučit.
- Neupotřebitelné stopy – jsou to stopy, které obsahují 6 a méně identifikačních znaků. Takto vzniklé stopy jsou vytvořeny odrazem velmi malé části prstu, případně byly nějak poškozeny. Špatná struktura podkladního materiálu, rozmazanost. Nicméně i takto vzniklé stopy mohou mít pro kriminalistiku velký význam. Díky nim můžeme zjistit, o který prst se jedná a následně jednoduše vyloučit podezřelé osoby s odlišným vzorem papilárních linií na prstu.

Daktyloskopické stopy jsou poměrně malé objekty, které jsou náchylné na znehodnocení či úplné zničení neodborným zásahem. Jejich výskyt na kriminalistických místech je běžný. Mohou se vyskytovat na různých předmětech. Uvedeme si zde ty nejběžnější:

- Na jednotlivých částech budov – okna, dveře, mříže, stěny
- Na jednotlivých věcech napadené osoby
- Na nástrojích použitých k trestnému činu – zbraně, páčidla, kleště, dopravní prostředky
- Na odcizených věcech – zboží, věci od postižených osob
- Na těle postižené osoby

5.3 Metody odhalení daktyloskopické stopy:

Kriminalistická technika vypracovala celou řadu metod pro zviditelňování latentních (neviditelných) daktyloskopických stop, zajišťování a také pro jejich ukládání. Pro správnou volbu metody je zapotřebí brát v potaz druh stopy, její stáří, nosič a některé další faktory. Lze použít následující metody:

5.3.1 Fyzikální metody

Jedná se o nejpoužívanější metodu, díky které se zajišťuje nejvíce daktyloskopických stop. Využívají poznatku, že odparek potu, jež tvoří vlastní stopu, má lepkavý charakter. Na odparku ulpívají jemné práškovité hmoty, které zviditelňuje obrazec papilárních linií. V kriminalistické praxi se používá mnoho velmi jemně práškovaných, ve vodě nerozpustitelných materiálů. Zástupci těchto materiálů jsou např.: argentorát, železo, mosazné a bronzové prášky, grafit, karborafin, tkanol a další. Výběr prášku se volí podle podkladního materiálu a dbá se na to, aby byl zabezpečen kontrast mezi vyvolanou stopou a podkladem. [8]

Obr. č. 21 - Prostředky pro odhalování stop [8]

Zviditelnění latentní daktyloskopické stopy se provádí tak, že se za pomocí jemných vlasových štětečků nanese prášek na prověřované místo. Štěteček se lehce přetírá jedním směrem tam, kde se předpokládá latentní stopa. Prášek se na tuto stopu zachytí a tím ji zviditelní. Je nutno dbát na to, aby se prášek nanášel pomocí štětečku velmi lehce a

jemně, aby nedošlo k poškození stopy. V dnešní době je dostupná již řada sprejů a rozprašovačů, díky nimž se rozprašuje prášek.

Vyvolaný daktyloskopický otisk se po fotografickém zadokumentování zajišťuje na daktyloskopickou fólii. Po vyvolání se odstřihne fólie tak, aby měla velikost pouze o něco větší, než je stopa. Odstřihne se růžek a sejme se ochranný list. Fólie se poté valivým způsobem přitiskne želatinovou vrstvou na vyvolanou stopu. Díky želatinové vrstvě dokážeme otisknout stopu se všema jejíma podrobnostmi, avšak v zrcadlovém provedení. Po sejmutí otisku se tento zakryje ochranným listem tak, aby mezi želatinovou vrstvou a ochranným listem nebyly vzduchové bublinky. Tato vrstva se poté označí na rubové straně číslem. [8]

Seznam látek a jejich použití:

- **Argentorát** – Používá se pro vyvolání stopy na pevných, hladkých a lesklých předmětech (sklo, porcelán, leštěné plochy nábytku, okenní rámy, kliky atd).
- **Saze, grafit, kovové prášky** – Používá se pro vyvolání stopy na papíru, kde je potřeba zachovat nepoškozený stav předmětu (bankovky, cenné papíry, doklady, známky, šeky.
- **Vosk, asfalt, xeroxový barvící prášek** – Použití tam, kde nám nevadí mírná povrchová změna nosiče stopy (papír).
- **Tkanol** – Používá se pro sejmutí daktyloskopických stop z textilií.

Další skupinu tvoří duální prostředky – Jedná se o prostředky, jež se na světlém podkladě jeví jako tmavošedé a na tmavém zase jako světlešedé. Dále jsou to fluorescenční prášky. Tyto prášky jsou v různě barevné a jejich aplikace probíhá pomocí mechanického nanášení. Po vystavení světla tyto prášky fluoreskují.

5.3.2 CHEMICKÉ METODY

Tyto metody jsou založeny na chemické reakci. V důsledku této reakce mezi potem a chemikálií vznikají barevné látky. Používají se nejčastěji pro papír. Jejich použití je náročné a proto se zpravidla neprovádí na místě činu. Mezi nejčastěji používané chemické metody patří použití dusičnanu stříbrného a ninhydrinu. Tyto metody jsou časově náročné. Za normálních okolností dostáváme viditelnou daktyloskopickou stopu za 24 – 48 hodin.

Záleží na vlastnostech potu. Stopa se dá urychlit a to zahřátím nosiče (papír max. 80°C), nicméně je to na úkor její kvality.

5.3.3 FYZIKÁLNĚ-CHEMICKÉ METODY

Zde se nejčastěji používá metoda založena na využití par jódu. Zviditelněná stopa je pouze dočasná a musíme ji zdokumentovat fotograficky. Podstata této metody je založena na tom, že jód sublimuje z pevného skupenství do plynného a ulpívá tak na místech, kde došlo ke kontaktu prstu s papírem. Efektivnost této metody spočívá v tom, že za pomocí skleněné rourky, uprostřed vyduté, s náplní jódových krystalků, je možné na kterémkoliv místě vyvolat daktyloskopickou stopu, aniž bychom museli převážet předmět do laboratoří. [8]

S popsaným prostředkem se pracuje tak, že se ústy nahání vzduch do skleněné rourky, jež spolu s jódovými parami vychází na nosič, kde ulpí na daktyloskopické stopě.

Dále se nám rozvíjí metoda, která pro zviditelnění používá kyanoakrylátu. Ten naprosto dokonale vyvolává daktyloskopickou stopu a co je pro nás nejdůležitější, na široké škále materiálu. Nejvhodnější je použití na plastických hmotách, ale výborné vlastnosti má i na zbraních, střelivech, dřevu, kovech, sklech. Vyvolaný otisk je bílý, pevný a vcelku stálý. Nejčastěji se jeho zajištění provádí pomocí fotodokumentace, nicméně za použití určitých prášků se dá zajistit i na fólii.

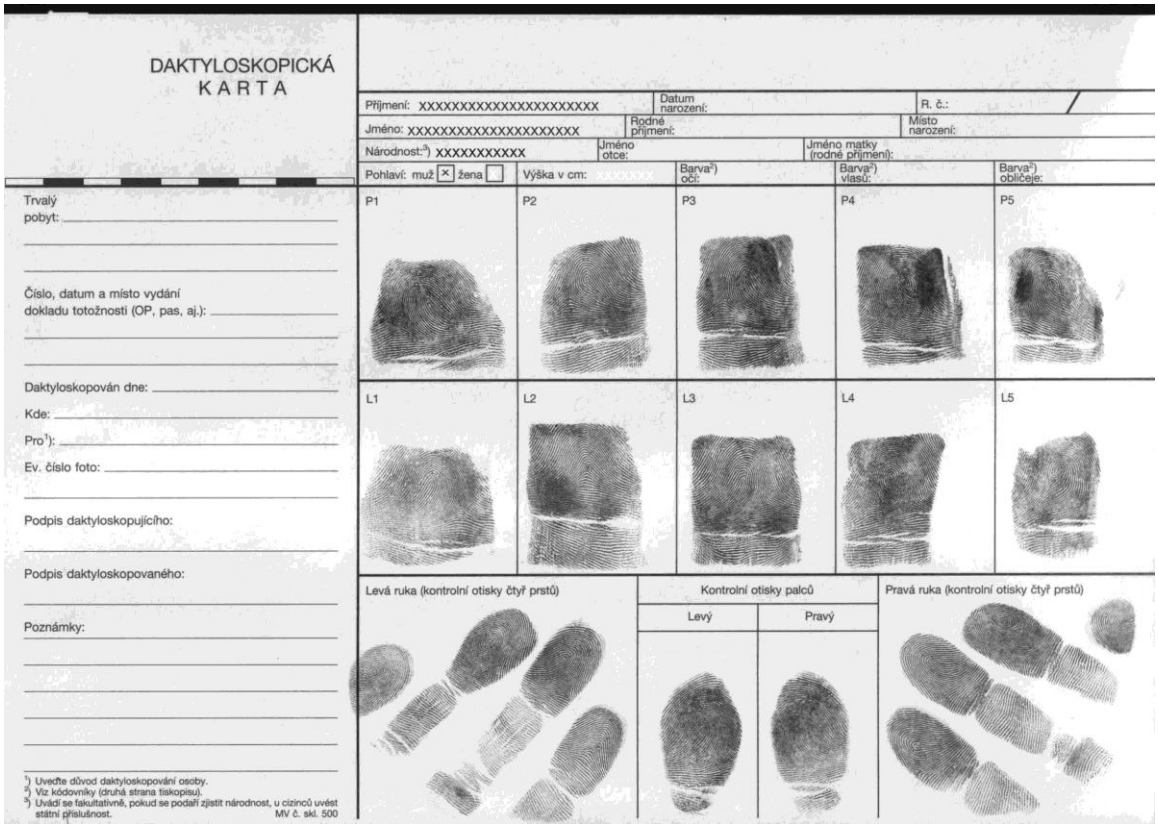
Máme ještě další řadu metod, nicméně ty nejsou v běžné kriminalistické praxi používány. Jedná se například o metodu využívající radioaktivního záření.

Pro vyhledávání viditelných daktyloskopických stop potřebujeme pouze pečlivou práci, neboť tyto stopy jsou běžně viditelné pouhým okem. V určitých případech si můžeme pomoci osvětlením, případně lupou či jinými prostředky. Po jejich vyhledání musíme stopu zajistit. Tyto stopy se zajišťují in natura a to buď na daktyloskopickou fólii, fotodokumentace, či případně odléváním.

In natura se zajišťují takové stopy, které lze včetně jejich nosiče snadno odeslat ke zkoumání. Jedná se například o zbraně, listinné materiály, či jiné drobnější předměty. Hrozí zde nebezpečí znehodnocení daktyloskopických stop, které jsou způsobené pomocí nesprávné manipulace.

5.4 Získávání otisku prstů

Dříve bylo možné získávání otisků prstů pouze za použití metody s inkoustem. Na požadované prsty byl nanesen černý inkoust a prst byl přitištěn na papírovou kartičku. Tato karta byla poté naskenována obyčejným skenerem a vzniknula tak digitální podoba.



Obr. č. 22 – Daktyloskopická karta [20]

V dnešní době se pořizují přímo naskenované digitální otisky, které získáme pomocí elektronického skeneru otisku prstů. U této metody není potřeba žádného inkoustu, stačí pouze přiložit prst ke čtečce otisků.

Obr. č. 23 - Scanování otisku prstu [8]

Mezi nejpoužívanější a zároveň nejstarší techniku přímého snímání otisku prstů patří metoda FTIR (Frustrated Total Internal Reflection). Zatímco se prst dotýká horní strany skleněného (plastového) hranolu, vrcholky papilárních linií jsou v přímém kontaktu s hranolem a mezery mezi papilárními liniemi jsou v určité vzdálenosti. Levá strana hranolu je osvětlena difusním světlem. Světlo, které vstupuje do hranolu je odraženo v mezerách papilárních linií a náhodně rozptýleno na vrcholcích papilárních linií. Nedostatečný odraz umožňuje vrcholkům papilárních linií odlišení od mezer mezi papilárními liniemi. Paprsky světla dopadající na pravou stranu hranolu jsou zaostřeny pře optickou čočku na CCD snímač (nebo také CMOS). Hlavní výhodou této metody je to, že zařízení FTIR snímají 3D povrch prstu, tím pádem nemohou být jednoduše oklamány za pomocí plochých fotografií otisku prstu. [8]

5.5 Skenery pro přímé snímání

Používají vysoce kvalitní fotoaparát, který je přímo zaostřený na otisk prstu. Nedochází zde ke kontaktu prstu s povrchem. Skener může mít mechanickou podporu, která uživateli usnadní správnou pozici pro prst. Toto zařízení může být považováno za více hygienické, neboť se jedná o bezdotykové snímání. Nedochází zde k nelineární deformaci způsobené při dotyku prstu s povrchem. Není zapotřebí periodického čištění dotekové plochy.

5.6 Rozpoznání daktyloskopických stop:

Spolehlivé rozpoznání otisku je velmi složitým úkolem a to hlavně z důvodů velké variability jednoho otisku prstu. Tato variabilita je zapříčiněna např. posunutím, rotace, nelineární deformace způsobené tlakem, šum, chyby, změna vlastnosti kůže, atd. Díky tomu můžou otisky jednoho prstu mnohdy vypadat rozdílně a odlišné prsty poté mohou zase vypadat podobně. [8]

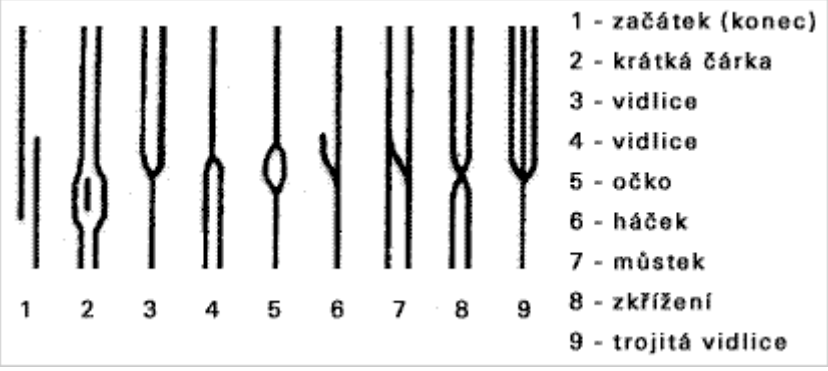
V procesu kriminalistické identifikace osob dle daktyloskopických stop je potřeba v souladu s teorií identifikace porovnávat objekty identifikované a identifikující (daktyloskopické stopy a srovnávací materiály). Vlastní identifikace je prováděna pomocí daktyloskopických markantů, což jsou individuální znaky. Jednoznačně vyjádřená individualita papilárních linií se projevuje tak, že mají velký počet markantů, které nám umožňují snadno navzájem odlišit jednotlivé obrazce. Rozmístění markantů (začátek a konec papilárních linií, vidlice, očko, háček, můstek, atd.) se navzájem liší jak svým geometrickým tvarem, tak i četností výskytu. I konkrétní markanty mohou vykazovat rozdíly.

Identifikační hodnotu znaku (markantu) lze vypočítat pomocí následujícího vzorce:

$l = -\log n$ kde l – identifikační hodnota znaku

n – četnost výskytu znaku na ploše 1 mm2

Význam určení identifikační hodnoty jednotlivých daktyloskopických znaků spočívá v tom, že se na jejímž základě určí minimální počet znaků, které je potřeba pro vyslovení spolehlivého kategorického závěru o totožnosti objektu. Pro identifikaci je rozhodující celkový součet jejich identifikačních hodnot.



Obr. č. 24 - Daktyloskopické markanty [8]

Proces daktyloskopické identifikací se skládá ze tří následujících stádií:

V prvním stádiu má za úkol znalec prozkoumat, zda jsou objekty identifikace vhodné pro identifikační zkoumání. Zjišťuje, zda tyto objekty obsahují vhodné identifikační znaky, jejich počet a také kvalitu. Určuje (pokud je to v jeho silách) pomocí které končetiny (prstu) byla daktyloskopická stopa vytvořena. Toto stádium hraje velkou roli také pro taktickou stránku, neboť můžeme objasnit podmínky, za kterých mohla stopa vzniknout a další podrobnosti, které souvisí s událostí trestného činu.

Ve druhém stádiu daktyloskopické identifikace provádí znalec vlastní srovnávací zkoumání, jehož principem je vědecky přesné a logicky zdůvodněné hodnocení jednotlivých daktyloskopických identifikačních znaků obsažených v identifikujících objektech jak z hlediska jejich kvality, tak kvantity, která je určena jejich polohou ve vztahu k jiným okolním znakům nebo ke zvolenému souřadnému systému. Hodnocení daktyloskopických identifikačních znaků se provádí souběžně u obou identifikujících objektů. Výsledky se poté porovnají a vyvodí se závěry o shodnosti, či rozdílnosti znaků. Současně se konstatuje odůvodněné vysvětlení zjištěných rozdílů pro vyslovení některého ze druhů kategorických soudů.

Ve třetím stádiu daktyloskopické identifikace provádí znalec na základě analytického a syntetického zkoumání zhodnocení všech dílčích závěrů. Podle kvality a kvantity daktyloskopických identifikačních znaků rozhodne o shodnosti, případně rozdílnosti zkoumaných objektů z hlediska původu jejich vzniku. Může vyslovit čtyři druhy kategorických soudů. [8]

- **Kategoricky kladný soud** - stopa z místa činu i srovnávací otisk byly vytvořeny jednou osobou
- **Kategoricky záporný soud** – stopa a srovnávací otisk byly vytvořeny dvěma osobami
- **Částečně kladný a částečně záporný soud** – ve stopě a srovnávacím otisku byly nalezeny odlišnosti, které musí znalec nejdříve objasnit, než vynese verdikt

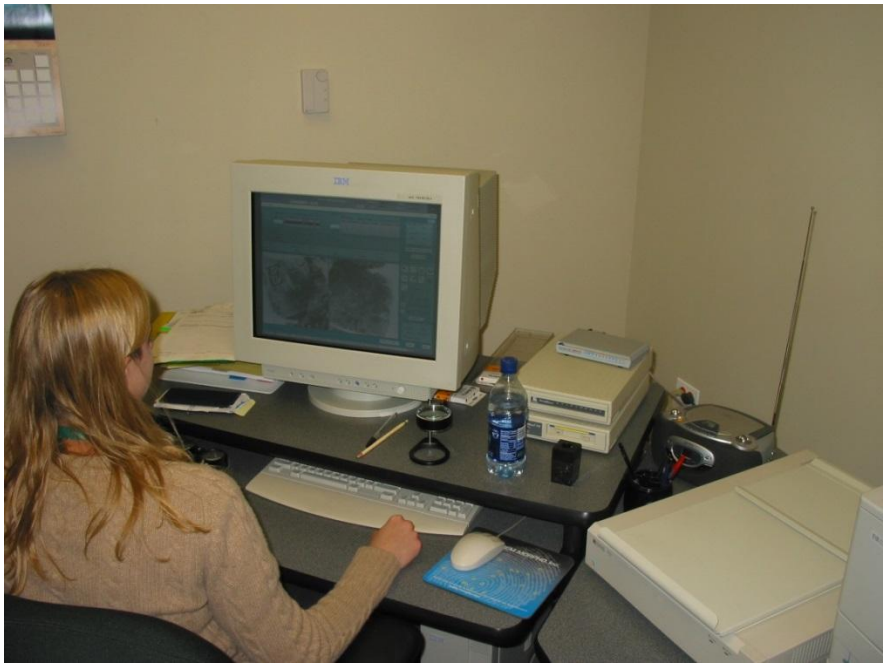
5.7 Automatizace v daktyloskopii:

Hlavním důvodem nasazení výpočetní techniky je zvětšení produktivity a kvality práce. Manuální vyhodnocování otisků prstu, bez účasti výpočetní techniky pro experty v daktyloskopii časově, odborně a také fyzicky náročné. Jelikož narůstá kriminalita, logicky narůstá čas na jejich manuální zpracování a vyhodnocení, protože se zvětšují samotné daktyloskopické fondy, jež mají být v případě vyhodnocování otisku kompletně znovu a znovu sekvenčně prohledávány a porovnávány. Z tohoto důvodu roste doba, která je potřebná pro vyhodnocení každé daktyloskopické stopy.

S rozvojem informační technologie byly vymyšleny a zkonstruovány automatizované daktyloskopické systémy, jež umožňují velmi rychlé vyhledávání nejpodobnějších otisků se stopou z místa činu. Systém po vyhodnocení nabídne několik nejpodobnějších otisků a předloží je daktyloskopickému expertovy, který poté porovná tyto otisky a zpracuje znalecký posudek. Hlavní výhoda této automatizace je rychlost a přesnost. [8]

5.8 AFIS

Automated Fingerprint Identification Systém – v překladu – Automatický systém pro identifikaci podle otisku prstu.

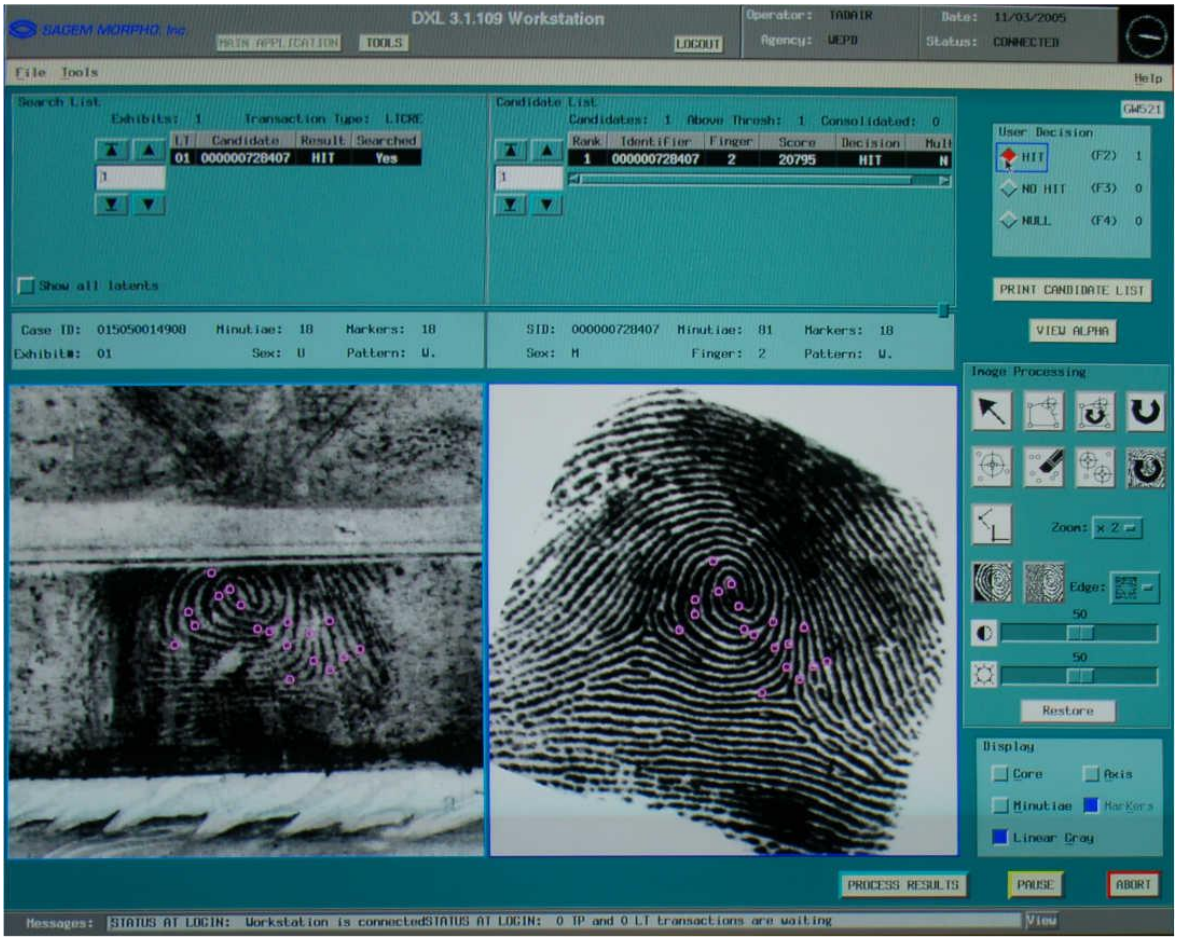


Obr. č. 25 – Pracovnice se systémem AFIS [21]

Vyvinula jej vláda Spojených států v úzké spolupráci s FBI. Tento systém je používán i v ČR. Je nainstalován v praze a pořizovací náklady přesáhly 100mil. Kč.

Při přechodu z papírových evidenci na počítačové registry AFIS, je nutné mít naskenované všechny jednotlivé, daktyloskopické karty. Tento proces může být také automatizován za pomocí moderních skenerů, které již dnes dokážou pracovat s podavači karet, tím pádem převod probíhá po dávkách.

Být objektivní, je snahou všech orgánů činných v trestním řízení. Z toho důvodu nelze svěřit veškeré rozhodování jen technice. Otisk může být nekvalitní a tudíž by mohl vézt k mylnému závěru. Z toho důvodu rozhoduje o otisku znalec. [22]



Obr. č. 26 – AFIS [21]

ZÁVĚR

Rozvoj informačních technologií jednoznačně ovlivnil identifikační technologie. S rozvojem výpočetní techniky vznikly nové identifikační metody. Vysoce výkonné počítače jsou schopny zpracovávat velké množství dat a řešit nespočet algoritmů.

Cílem mé diplomové práce bylo předvést ucelený materiál, který se bude týkat identifikačních metod a jejich podpory informačními technologiemi. Součástí je také vysvětlení základních pojmů, abychom si dokázali utvořit představu, jak tento proces probíhá.

Biometrickou identifikaci nepochybně čeká skvělá budoucnost. Nebude trvat dlouho a zcela určitě se s nimi budeme setkávat na každém kroku. Většina technických a technologických překážek je dnes již vyřešena, ale tu největší překážku mají teprve před sebou – musí je lidé přijmout a musí jim důvěřovat.

ZÁVĚR V ANGLIČTINĚ

The development of information technology clearly influenced identification technology. With the development of computer technology has created new identification method. High performance computers are able to process large amounts of data and solve countless algorithms.

The aim of my thesis was to perform a comprehensive material, which will involve identification methods and their support of information technology. Also included is an explanation of basic concepts, we have managed to form an idea of how this process occurs.

Biometric identification undoubtedly expect a great future. It will not take long, and certainly with them we meet at every step. Most of the technical and technological barriers is now resolved, but there are still the biggest obstacle in front of you - the people must accept and must trust them.

SEZNAM POUŽITÉ LITERATURY

[1] VACH, Martin. Historie biometrik a jejich využití ve výpočetní technice. [online]. 2003 [cit. 2013-06-02]. Dostupné z: http://www.fi.muni.cz/usr/jkucera/pv109/2003/xvach_biometriky.htm

[2] ŘÍHA, Zdeněk. *Biometric authentication systems* [online]. Brno, 2001 [cit. 2013-06-02].

[3] JAIN, A. K., R. BOLLE a S. PANKARI. *Biometrics – Personal identification in Network Society*. Kluwer Academic Publisher, 1999.

[4] Definice informace. Data - informace - znalosti. [online]. 2013 [cit. 2013-06-02]. Dostupné z: http://web.sks.cz/users/ku/ZIZ/inform1.htm

[5] KÓDOVÁNÍ A ŠIFROVÁNÍ INFORMACÍ. [online]. 2012 [cit. 2013-06-02]. Dostupné z: http://spsprerov.draksoft.net/rocprace/Modsite/stranky/09.htm

[6] PŘENOSOVÉ CESTY A JEJICH CHARAKTERISTIKA. [online]. 2012 [cit. 2013-06-02]. Dostupné z: http://sdelovacka.kbx.cz/data/statnice/BEST/26.pdf

[7] VACULKA, Tomáš. *Identifikace osob pomocí DNA*. Zlín, 2010. Bakalářská práce. UTB ve Zlíně. Vedoucí práce JUDr. Vladislav Štefka.

[8] PORADA, Viktor a kolektiv. Kriminalistika. Praha : CERM 2001. 746 s. ISBN 8072041940.

[9] HAMRLOVÁ, Andrea. Identifikace osob pomocí DNA. Brno, 2007. 48 s.Bakalářská práce. Masarykova Univerzita.

[10] Girl of 15 found stabbed to dead in lift at London block on flats [online]. 2008 [cit. 2010-05-07]. Guardian. Dostupné z WWW: <http://www.guardian.co.uk/uk/2008/jun/03/knifecrime.ukcrime1>

[11] Crime Scene Photos [online]. 2009 [cit. 2010-05-01]. Brebeuf Jesuit Biotechnology. Dostupné z WWW: < http://bjpsbiotech.edublogs.org/csi-2010/crime-scene-photos/>

[12] Evidence collection [online]. 2009 [cit. 2010-05-16]. RexCoffey. Dostupné z WWW: <http://www.rexcoffey.com>

[13] VESELÁ, MGR., Hana. Odebírání vzorků DNA, nakládání s nimi a následná identifikace osob. [online]. 2009 [cit. 2013-06-02]. Dostupné z: www.psp.cz/sqw/text/orig2.sqw?idd=53957

[14] JANEČEK, Tomáš. Biometrika [online]. [cit. 2008-05-25]. Dostupný z WWW: http://www.nula.wz.cz/biometrika/biometrika.rtf

[15] FortiToken-200 Hardware (OTP) Token. [online]. 2012 [cit. 2013-06-02]. Dostupné z: http://www.fortinet.com/products/fortitoken/200.html

[16] Jails Hope Eye Scanners Can Provide Foolproof Identification System for Inmates. [online]. 2012 [cit. 2013-06-02]. Dostupné z: http://www.nytimes.com/2010/02/28/us/28eyes.html?_r=1&

[17] MGR. ING. ŠČUREK, PH.D, Radomír. Biometrické metody identifikace osob v bezpečnostní praxi. Ostrava, 2008. Dostupné z: http://www.fbi.vsb.cz/export/sites/fbi/040/.content/sys-cs/resource/PDF/biometricke_metody.pdf. Studijní text. VŠB TU Ostrava.

[18] Biometric applications for immigration. [online]. [cit. 2013-06-02]. Dostupné z: http://fingerchip.pagesperso-orange.fr

[19] Israel's biometric database. [online]. [cit. 2013-06-02]. Dostupné z: www.bioenabletech.com

[20] Dobrodružství kriminalistiky – Daktyloskopie. [online]. [cit. 2013-06-02]. Dostupné z: http://www.geocaching.com/seek/cache_details.aspx?guid=061eb58e-b5de-40e2-9686-95e54ad6352a

[21] AFIS: The Automated Fingerprint. [online]. [cit. 2013-06-02]. Dostupné z: Identification Systemhttp://forensics4fiction.com/2011/09/01/afis-the-automated-fingerprint-identification-system/

[22] RAK Roman, MATYÁŠ Václav, ŘÍHA Zdeněk a kol. Biometrie a identita člověka [ISBN 9788024763927]

SEZNAM OBRÁZKŮ