Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačního inženýrství

Bakalářská práce

Biometrický podpis a jeho bezpečnost

Lucie Šeredová

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Lucie Šeredová

Informatika

Název práce

Biometrický podpis a jeho bezpečnost

Název anglicky

Biometric signature and its security

Cíle práce

Cílem práce je zkoumání bezpečnosti dynamických biometrických podpisů.

Metodika

-Prostudujte problematiku snímání biometrických pasů.

-Na základě rešerše definujte přijatelné a nepřijatelné (mezní) odchylek u biometrických podpisů.

-Následně stanovením dané hranice bezpečného přijetí a odmítnutí (meze).

-Proveďte základní měření a ověřte validnost stanovených odchylek.

-Definujte závěry a doporučení.

Doporučený rozsah práce

30-40

Klíčová slova

Biometrický podpis, biometrie, dynamika podpisu

Doporučené zdroje informací

Doc. Mgr. Ing. Radomír Ščurek, Ph.D.: BIOMETRICKÉ TECHNOLOGIE, Technické prostředky bezpečnostních služeb

---

Předběžný termín obhajoby

2021/22 LS – PEF

Vedoucí práce

Ing. Josef Pavlíček, Ph.D.

Garantující pracoviště

Katedra informačního inženýrství

Elektronicky schváleno dne 1. 3. 2022

Ing. Martin Pelikán, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 7. 3. 2022

doc. Ing. Tomáš Šubrt, Ph.D.

Děkan

V Praze dne 09. 03. 2022

Čestné prohlášení

Prohlašuji, že svou bakalářskou práci "Biometrický podpis a jeho bezpečnost" jsem vypracovala samostatně pod vedením vedoucího bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu použitých zdrojů na konci práce. Jako autorka uvedené bakalářské práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušila autorská práva třetích osob.

V Praze dne 15. 3. 2022 _____

Poděkování

Ráda bych touto cestou poděkovala vedoucímu práce Ing. Josefu Pavlíčkovi, Ph.D. za odborné vedení, ochotu, cenné rady a vstřícnost při konzultacích bakalářské práce. Dále bych ráda poděkovala účastníkům testování za jejich čas a ochotu.

Biometrický podpis a jeho bezpečnost

Abstrakt

Bakalářská práce je zaměřena na dynamický biometrický podpis, na jeho bezpečnost a použití v praxi. Biometrický podpis je prostý elektronický podpis a slouží pro stvrzování akcí a pro autentizaci.

V teoretické části jsou objasněny základní pojmy biometrie a typy podpisů. Část je věnována právě vlastnostem biometrického podpisu jako je rychlost podpisu, doba trvání podpisu, přítlak, a další. U bezpečnosti je i základně vysvětleno šifrování, které patří k biometrickým podpisům.

V praktické části jsou u biometrických podpisů zkoumány a testovány odchylky ve snímaných datech v rámci jedné osoby. Dále respondenti ve dvojicích simulují své podpisy navzájem po krátkém odpozorování původního podpisu, zde se porovnávají odchylky podpisů pravých a padělaných.

Klíčová slova: Dynamický biometrický podpis, Autentizace, Verifikace, Biometrie, Odchylky, Čtečky, Šifrování

Biometric signature and its security

Abstract

The bachelor thesis is focused on dynamic biometric signature, its security and use in practice. A biometric signature is a simple electronic signature and is used for event confirmation and authentication.

The theoretical part clarifies the basic concepts of biometrics and types of signatures. A part is devoted to the properties of the biometric signature, such as signature speed, signature duration, pressure, and more. For security, there is also a basic explanation for encryption, which belongs to biometric signatures.

In the practical part, deviations in the scanned data of biometric signature are examined and tested within one person. Furthermore, the respondents in pairs simulate their signature to each other after a short observation of the original signature, here the deviations of genuine and forged signatures are compared.

Keywords: Dynamic biometric signature, Authentication, Verification, Biometrics, Deviations, Readers, Encryption

Obsah

Seznam obrázků

Seznam grafů

Seznam tabulek

Seznam zkratek

DBP	Dynamický biometrický podpis
ÚOOÚ	Úřad pro ochranu osobních údajů
GDPR	General Data Protection Regulation (Ochrana osobních údajů)
FAR	False Acceptance Rate (Chybné přijetí)
FRR	False Rejection Rate (Chybné odmítnutí)
ERR	Equal Error Rate
DTW	Dynamic Time Warping (Dynamická časová deformace)
HMM	Hidden Markov Model (Skrytý Markův model)
GMM	Gaussian Mixture Model (Gaussův smíšený model)
HASH	hašovací funkce
MD5	Message-Digest algorithm (hašovací funkce)
SHA	Secure Hash Algorithm
DES	Data Encryption Standard
AES	Advanced Encryption Standard
RSA	iniciály autorů Rivest, Shamir, Adleman
eIDAS	nařízení Evropské unie č.910/2014
ZEP	Zaručený elektronický podpis
ZAREP	Uznávaný podpis - ZEP založený na kvalifikovaném certifikátu
KEP	Kvalifikovaný elektronický podpis

1 Úvod

Dynamický biometrický podpis je kombinace behaviorálních, ale i fyziologických vlastností člověka používaný k ověřovaní a zejména stvrzování, jako je tomu u klasického statického podepisování perem na papír. Nejedná se pouze o vizuální stránku podpisu, jsou snímány i další faktory jako tlak, čas a přesné souřadnice bodů X a Y. Je nutné nezaměňovat dynamický (biometrický) a elektronický podpis. Elektronický podpis, je používán také k ověření identity nebo stvrzování dokumentů, ovšem jedná se pouze o určitý elektronický údaj (číslo), který neobsahuje žádné biometrické osobní údaje.

Tématem této bakalářské práce je dynamický biometrický podpis a jeho bezpečnost pomocí měření odchylek jeho vlastností u jednotlivých snímaných podpisů. Dynamický podpis poskytuje bezpečnější autentizaci v porovnání se statickým podpisem, právě kvůli osobním biometrickým údajům, které umožňují lépe rozpoznat pravost podpisu. Pro případné padělatele je mnohem náročnější zvládnout napodobit nejen vzhled podpisu, ale také jeho rychlost v jednotlivých částech a tlak na podepisovací podložku.

Teoretická část práce je zaměřena především na objasnění pojmu biometrik a zanesení dynamického biometrického podpisu do kontextu. Důležitou částí je představení podpisů, jejich vlastností a technologií snímání. Zmíněné vlastnosti a charakteristiky podpisů nás budou provázet zejména do praktické části. Součástí teoretické části je i náhled do elektronické bezpečnosti podpisů, jenž zahrnuje především šifrování podpisů a případné propojení podpisů s dokumenty a zachování jejich integrity pomocí zašifrování. Závěr je věnován právním omezením biometrických osobních údajů.

Praktická část je založena na zpracování a zkoumání nasnímaných dat pro účel této bakalářské práce. Proces probíhal ve spolupráci s Československou obchodní bankou, která poskytla patřičné hardwarové i softwarové technologie. Podepisování respondentů probíhalo ve dvojicích. Respondenti poskytli 4 podpisové vzory pro vyhodnocení míry rozptylu, dále se pak druhý z dvojice pokusil dvakrát napodobit podpis prvního z dvojice, pro ukázku obtížnosti snahy padělání podpisů. V rámci shromážděných dat následuje určení vlastní hranice shodnosti podpisů, tím pádem jejich přijetí či odmítnutí.

2 Cíl práce a metodika

2.1 Cíl práce

Cílem práce je zkoumání bezpečnosti dynamických biometrických podpisů.

2.2 Metodika

- Prostudujte problematiku snímání biometrických podpisů.
- Na základě rešerše definujte přijatelné a nepřijatelné (mezní) odchylky u biometrických podpisů.
- Následně stanovením dané hranice bezpečného přijetí a odmítnutí (meze).
- Proveďte základní měření a ověřte validnost stanovených odchylek.
- Definujte závěry a doporučení.

3 Teoretická východiska

3.1 Biometrie

Biometrie se skládá ze slov „bio“ a „metric“. Pojem je vyvozený z řečtiny, kde slovo „bios“ znamená „život“ a slovo „metron“ značí „měření“. Biometrie je tedy vědní obor, jenž se zabývá zkoumáním živých organismů a měří biologické vlastnosti nebo behaviorální charakteristiky. [2]

Biometrii lze rozdělit na dvě základní odvětví podle charakteristických rysů použitých pro měření. Jedná se o statické a dynamické rysy. Statickou biometrií je myšlena fyziologická a anatomická (tělesná) stránka člověka. Pod statické charakteristiky se řadí nejznámější otisk prstu dále pak sken obličeje, oční duhovky, oční sítnice, krevní řečiště v ruce (termogram ruky), termogram obličeje, tvar ucha, dentální obraz a DNA. Dynamická biometrie se zabývá chováním člověka, tím pádem jeho behaviorálními charakteristikami. Pod dynamickou biometrii tedy patří hlas, chůze, gestikulace obličeje, stisk kláves a dynamika podpisu. [6]

Biometrické vlastnosti mají nastavené určité ukazatele (kritéria), podle kterých se lze rozhodovat. Například jaký typ biometrických charakteristik je vhodný při požadovaném ověření. Dynamické charakteristiky jsou často ovlivněny momentálním rozpoložením člověka jako je psychický a fyzický stav, proto je důležité stanovení těchto ukazatelů. [6]

- univerzálnost: Vlastnost musí mít každá osoba.
- jedinečnost (unikátnost): Nemožnost nalézt dvě osoby se shodou.
- konstantnost (stálost): V čase vlastnost zůstává neměnná.
- získatelnost (dostupnost): Je možné kvantitativní měření vlastnosti.
- výkonnost: Nestárnutí a nezměnění vlastnosti.
- akceptace (etika): Ochota lidí poskytnout dané biometrické vlastnosti.
- bezpečnost: Nízké riziko vytvoření padělku.
- finance: Výše financí vyložených na zavedení daného systému pro snímání údajů.

V následující tabulce č. 1 jsou uvedena vybraná biometrická kritéria.

Tabulka 1 - Kritéria vybraných biometrických prvků [3]

biometrický prvek	univerzálnost	jedinečnost	konstantnost	získatelnost	výkonnost	akceptace	bezpečnost	finance
obličej	vysoká	nízká	střední	vysoká	nízká	vysoká	nízká	nízké
otisk prstu	střední	vysoká	vysoká	střední	vysoká	střední	vysoká	nízké
geometrie ruky	střední	střední	střední	vysoká	střední	střední	střední	střední
žíly ruky	střední	střední	střední	střední	střední	střední	vysoká	střední
duhovka	vysoká	vysoká	vysoká	střední	vysoká	nízká	vysoká	vysoké
sítnice	vysoká	vysoká	střední	nízká	vysoká	nízká	vysoká	vysoké
podpis	nízká	nízká	nízká	vysoká	nízká	vysoká	nízká	nízké
hlas	střední	nízká	nízká	střední	nízká	vysoká	nízká	nízké
termogram	vysoká	vysoká	nízká	vysoká	střední	vysoká	vysoká	vysoké

Z tabulky vyplývá, že uvedená kritéria lépe splňují statické biometrické charakteristiky oproti dynamickým. Ve statických vlastnostech si nejlépe vede otisk prstu, který finančně není příliš nákladný jako například snímání duhovky, a zároveň obstojně splňuje zbylá kritéria.

Biometrické prvky se dají rozdělit na přístupové a forenzní. Přístupové biometrické prvky slouží především k rozpoznání člověka po dřívějším dobrovolném zanesením do systému. Příkladem mohou být docházky nebo přístupy do hlídaných budov. Biometrické prvky ve forenzním odvětví slouží k nalezení totožnosti člověka, například z policejní databáze. [6]

Důležité je objasnit základní pojmy používané v biometrii, které se často mohou zaměňovat nebo považovat za synonyma. Jedná se o pojmy verifikace a identifikace dále pak i pojem autentizace. [2]

3.1.1 Verifikace

Verifikace (anglicky verification) je ověření pomocí principu one-to-one (1:1), kdy osoba nejdříve zadá svou identitu pomocí čipové karty či hesla, a pak se prokazuje biometrickým údajem. Porovnání je tedy pouze v rámci právě nasnímaného údaje a uložené šablony. Dříve

zapsaný vzorek je uložený v databázi nebo pro větší bezpečnost právě na zmiňované čipové kartě. [2][1][15]

3.1.2 Identifikace

Identifikace (anglicky identification) stojí na principu one-to-many (1:N), zde osoba neprokazuje svou identitu, ale pouze poskytuje biometrický údaj. Biometrická informace je pak porovnávána s celou databází uložených šablon, dokud není nalezena shoda. Pokud shoda nalezena není uživatel není identifikován a jeho přístup je odmítnut. [2][15]

3.1.3 Autentizace

Autentizace je další z důležitých pojmů užívaných v biometrii. Autentizace je způsob ověření neboli rozpoznání identity. Uživatel na konci celého procesu získá status. Může se jednat o status přijetí/odmítnutí nebo oprávněný/neoprávněný a další. Autentizaci lze provést například ověřením fotografie, hlasu nebo přihlášením do systému. Nejčastějším a nejznámějším způsobem autentizace, ale zároveň i nejzranitelnějším je heslo. Nevýhodou ale zároveň i výhodou hesel je možnost sdělení či vyzrazení další osobě. Způsob autentizace pomocí biometrických vlastností tuto vlastnost postrádá. Je to především výhoda zejména u systémů, kde je nežádoucí, aby si uživatelé předávali přihlašovací údaje. Existují tedy tři základní metody a způsoby autentizace uživatele založené na prokázání znalosti, vlastnictví nebo vlastnosti, případně na kombinaci zmíněných. [2][12]

3.1.3.1 Znalost

U autentizace prokázáním znalosti musí uživatel znát určité heslo či frázi. Hlavní nevýhodou je možnost sdělení další osobě. Někdy tento faktor může být v osobním životě přínosný, ovšem z hlediska bezpečnosti je velmi nežádoucí. [2][12]

Jak již bylo zmíněno, heslo je stále nejpoužívanější způsob autentizace, ovšem je také velmi zranitelné. Hesla jsou v systémech ukládána v databázích. V dnešní době by se neměla ukládat ve formě prostého (čitelného) textu (plain text), kvůli případnému průniku útočníka do databáze. Hesla se šifrují pomocí hash funkce. Nadstavbou pak je pak tzv. „solení“, kdy se k heslu přidá náhodný text a teprve pak je heslo zašifrováno. [2][12]

U hesel je často doporučováno užívat silná dlouhá hesla s čísly a speciálními znaky a také jejich častá obměna. Ovšem uživatelé či administrátoři systému musí vyhodnotit, zda příliš složité heslo není naopak nevýhodou, kdy hrozí, že si jej uživatel bude poznamenávat a zvyšovat tak riziko odcizení hesla. I častá obměna hesla nucená systémem nemusí být jen

přínosem, uživatelé často jen mění čísla na konci hesla, takže když se útočník dostane k heslu minulému není problém se dopracovat k heslu současnému. [2][12]

3.1.3.2 Vlastnictví

Autentizace prokázáním vlastnictví je založena na principu vlastnictví speciálního předmětu. Může se jednat o token, čipovou kartu, telefon apod. Nevýhodou těchto zařízení je možnost přenášení a předávání. Může zde tedy hrozit větší riziko odcizení, proto se často využívá s kombinací autentizace pomocí znalosti. Příkladem mohou být platební karty, které vyžadují i zadání pinu. [2][12]

3.1.3.3 Vlastnost (biometrie)

Autentizace pomocí biometrické vlastnosti je v dnešní době již velmi běžná. Jedná se o prokázání speciální vlastnosti těla jako je rozpoznání obličeje, otisk prstu, dynamika podpisu a další. Tělesné biometrické vlastnosti vynikají svou jedinečností. Není tedy možné, jako u autentizace pomocí vlastnictví nebo znalosti, přenášet či předávat biometrická data další osobě. Další velkou výhodou biometrické autentizace je neměnnost těchto vlastností, zároveň nehrozí jejich zapomenutí jak fyzické, tak psychické. [2][12]

Je vhodné používat autentizační metody v kombinacích, tzv. více faktorová autentizace. Samotné metody autentizace znalostí (heslem) a vlastnictvím (tokenem) jsou snadno odcizitelné a přenositelné. Kombinace těchto prvků přináší vyšší stupeň bezpečnosti, ovšem stále může dojít ke ztrátě, úniku či vyzrazení. Biometrická autentizace zaručuje použití pouze danou osobou a její použití je také vhodné v kombinaci s heslem či tokenem. Příkladem může být placení mobilním telefonem, kdy je vyžadováno vlastnictví telefonu a zároveň ověření biometrického údaje jako otisk prstu nebo rozpoznání obličeje. [2][12]

3.2 Podpisy

Podpis je behaviorální metoda biometrické identifikace a je brán jako součást rukopisu. Ruční písmo je specifikací každé osoby, jenž umí psát tedy podpis nevyjímaje.

Původní funkcí podpisů nebyla identifikace člověka, a tak tomu převážně není ani dnes. Podpisy jsou brány především jako projev vlastní vůle, souhlasu a stvrzení určitého dokumentu či formuláře. V dnešní době v průmyslově rozvinutých zemích, kde se umí většina lidí podepsat, je podpis používán u spousty úkonů především právních či bankovních jako jsou například právní smlouvy, kupní smlouvy, bankovní šeky, půjčky, hypotéky atd. To by byly především hmotné transakce, ovšem podpisem můžeme stvrdit i nehmotné jako je udělení souhlasu, seznámení se s určitou skutečností či potvrzení autorství. Právě zde slouží podpis jako stvrzovací a souhlasný nástroj. [1]

Především kvůli stvrzovací vlastnosti podpisů dochází ke snahám o jeho falzifikaci nebo napodobení. Podpis je v nynější době pouze subjektivně porovnáván tzn., že například pracovník banky při podpisu smlouvy pouze vizuálně porovnává podpisy. Se subjektivním porovnáním se nejčastěji setkáváme při kontrole identity pomocí občanského průkazu, kde daná osoba pouze vizuálně porovnává náš obličej a fotkou na průkazu mnohdy mnoho let starou. Nebezpečí falzifikace je proto vyšší, než by bylo u podrobného rozebrání počítačem. [1]

Podpis je autentizace založená na kombinaci znalosti a vlastnosti. Znalostí je myšlena především znalost písma samotného (gramotnost), jenž jsme se v průběhu života naučili a zautomatizovali. Vlastnost je pak biometrická část, to jsou specifické a jedinečné vlastnosti našeho písma. [11]

V dnešní době se setkáváme s více druhy podpisů, proto je důležité si vymezit, co jednotlivé typy podpisů znamenají.

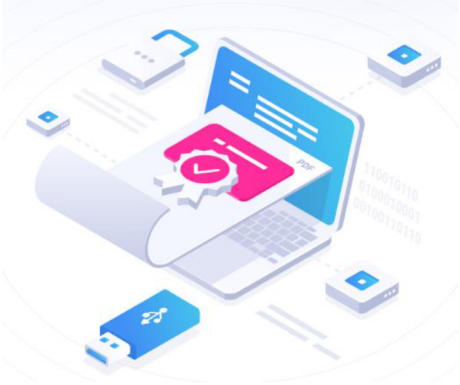
3.2.1 Statický podpis

Statický podpis je tzv. „offline“ podpis a jedná se o klasický ručně psaný podpis na papír tužkou, který může být například naskenován nebo ofocen a přidán do dokumentu. [11]

Obrázek 1 - Statický podpis [11]

3.2.2 Elektronický podpis

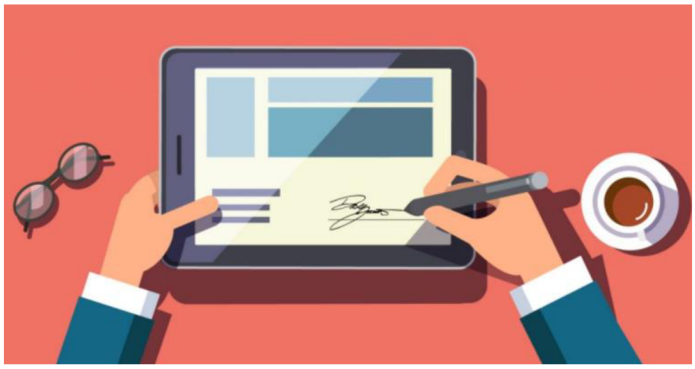
Elektronický podpis je často zaměňován s podpisem dynamickým, ovšem jedná se o naprosto odlišné podpisy. Elektronický podpis prakticky nemá nic společného s ručně psaným podpisem. Jedná se o číselný údaj, obsahující šifrované klíče, jenž jednoznačně stvrzuje identitu osoby. Elektronický podpis využívá asymetrickou kryptografii, díky které je zajištěna integrita dokumentů. [11][12][16]



Obrázek 2 - Elektronický podpis [20]

3.2.3 Dynamický podpis

Jedná se o vlastnoruční (statický) podpis, ke kterému jsou přidané informace o procesu vytváření podpisu. Dynamický biometrický podpis se tedy skládá ze dvou částí, ze statického podpisu a z dynamických vlastností podpisu. [1][13]



Obrázek 3 - Dynamický podpis [21]

Dynamický podpis neboli také „online“ podpis je zaznamenáván pomocí tabletu, kde je snímán nejen finální vzhled podpisu, ale také proces jeho vytváření. Data potom obsahují informace o souřadnicích X a Y pro jednotlivé body a dále i čas a tlak v těchto bodech. [11]

U DBP je využíváno behaviorálních i anatomických vlastností člověka, a má na něj také vliv momentální psychický i fyzický stav člověka. [2]

Dynamický podpis je využíván jako projev vůle u právního jednání nebo jiných úkonů s nutností přítomnosti podpisu. Jedná se tedy o formu autentizace dokumentů, a především o zachování integrity (nepopiratelnosti) dokumentů. [13]

3.3 Dynamika podpisu

„Tato metoda je datována k roku 1977 využívá jedinečnosti kombinace anatomických a behaviorálních vlastností člověka, které se projeví, když se podepisuje.“ [2]

Dynamika podpisu rozšiřuje obyčejný statický podpis o elektronicky snímané vlastnosti. Jak již bylo zmíněno biometrické údaje lze použít k identifikaci (1:N) nebo k verifikaci (1:1). U DBP je vhodné užívat pouze verifikační metodu autentizace. Aby byla verifikace možná, v první řadě je nutno vytvořit podpisový vzor z několika podpisů po ověření identity osoby například prokázáním občanského průkazu. Po vytvoření podpisového vzoru (referenční podpis) je možné po ověření identity osoby verifikovat nově nasnímaný podpis právě s podpisovým vzorem. [14]

3.3.1 Vlastnosti biometrického podpisu

Nadstavbou DBP oproti obyčejnému statickému podpisu na papír jsou dynamické charakteristiky člověka, které určují biometrickou stopu podepisujícího, která nelze být padělána. Mezi vlastnosti tedy patří i statické charakteristiky obrazu podpisu, kde lze zkoumat vrcholy písmen, překřížení tahů, různé křivky a smyčky a zároveň oblasti co jsou uzavřené. Tyto vlastnosti jsou v datech vyjádřeny souřadnicemi os X a Y, které určují umístění jednotlivých bodů podpisu na snímané ploše. Vyšší úroveň zabezpečení ale představuje právě dynamická část podpisu a proces jeho vzniku. Mezi dynamické charakteristiky pak patří délka trvání podpisu a čas v jednotlivých bodech, tlak podepisujícího perem na podložku, rychlost podepisování, zároveň rychlost mezi jednotlivými úseky, akcelerace nebo kolikrát a na jak dlouho bylo pero zvednuto. Dynamická část má tolik faktorů, že pro případného padělatele je nemožné napodobit biometrický podpis i s dostupným obrazem originálu. [7][13]

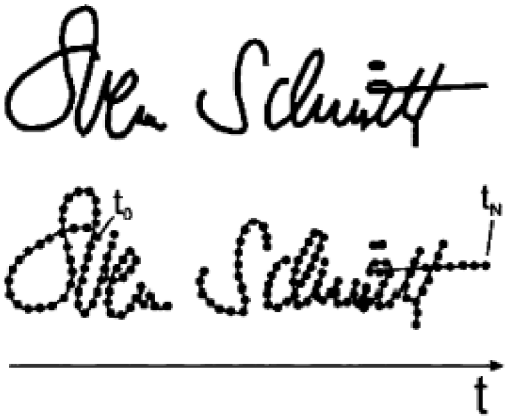
Další faktor DBP je, že jeho vlastnosti vychází nejen z anatomických rysů, ale i z behaviorálních, tím pádem závisí také na momentálním stavu člověka ať fyzickém, tak psychickém. Vzorky jsou tím pádem pokaždé jiné, proto lze přijít na případné použití jednoho vzorku dvakrát, jelikož by došlo ke sto procentní shodě, a to by poukazovalo na zneužití podpisu. Zároveň nízká procentuální shodnost charakteristik naznačuje snahu o falzifikaci. Proto je nutné hodnotit vzorky pomocí pravděpodobnosti shodnosti. [16]

3.3.1.1 Souřadnice X, Y

Souřadnice os X a Y zastávají klasickou podobu podpisu. Určují souřadnice jednotlivých bodů podpisu na podpisové ploše. Pomocí těchto dat lze určit rychlost tahů a jejich směr. [2]

3.3.1.2 Doba podpisu

Čas vyhotovení podpisu je jedním z hlavních faktorů. Je ovšem nutné brát v potaz, že je rozdíl mezi celkovým časem podpisu od jeho zahájení (bodu t_0) do jeho skončení (bodu t_n) a časem mezi jednotlivými úseky/body podpisu. Kombinací informací o umístění bodů podpisu v určitém čase nám umožňuje zjistit rychlost v jednotlivých částech a zároveň i lokální zrychlení či zpomalení. [1] [5]

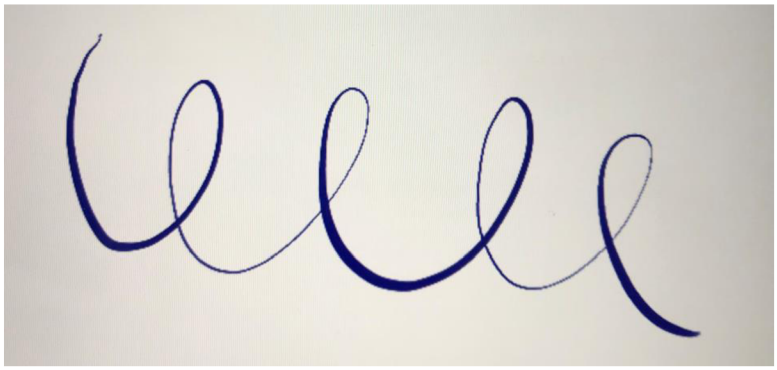


Obrázek 4 - Dynamická hodnota času podpisu v jednotlivých bodech [1]

3.3.1.3 Přítlak podpisu

Tlak, jenž podepisující osoba vyvíjí perem na podložku je další dynamická vlastnost, kterou lze získat právě díky digitalizačním snímačům. V průběhu podepisování se přítlak mění, a to je další typická behaviorální vlastnost osob. [5]

Na následující ukázce lze vidět v jakých částech podpisu byl přítlak menší a větší podle tloušťky tahu v jednotlivých fázích.



Obrázek 5 - Znázornění tlaku v podpisu

3.4 Biometrické čtečky

Princip vytváření dynamických biometrických podpisů je založen na snímání vlastnoručních podpisů pomocí tabletů či čteček (digitizérů) s použitím stylusu (speciální dotykové pero) nebo jiným nástrojem, kupříkladu prstem. [13]

Existují různé typy digitalizačních snímacích zařízení dynamického biometrického podpisu. K zachycení lze využít tradiční tablety nebo specializované čtecí zařízení určené přímo pro podepisování (sing-pady). Ve většině případech je k podpisu používán, spolu s tabletem, stylus. Jsou dva základní typy stylusů, a to levnější verze, která neměří přítlak podpisů a nepotřebuje tedy žádné napájení. Dražší variantou je pak pero s přítlakem, jenž je nutné nabíjet a zajistit komunikaci s tabletem. Pera, která měří přítlak nám zajišťují větší míru zabezpečení, jelikož poskytuje více biometrických charakteristik. Některé dříve užívané tablety bohužel neposkytovaly vizuální obraz při podepisování a podpis šlo vidět pouze na počítači monitoru. Dalším rozdílem mezi některými tablety a speciálními stylusy je, zda snímají pouze dotek pera a uživatel má tedy možnost opřít si ruku na tabletu a dosáhnout tak většího pohodlí při podepisování, anebo tablet snímá i vše ostatní a dochází tak k obtížnějšímu zaznamenání podpisu, jelikož se méně podobá klasickému podpisu na papír. Pro mnoho lidí je tato varianta velmi nepohodlná. [7][11]

3.4.1 Čtečky

Na trhu je v dnešní době mnoho firem nabízejících podpisové tablety i softwarové řešení. Jedním z poskytovatelů softwarového řešení je firma Kofax zabývající se digitalizací dokumentů, jenž nabízí například řešení Kofax SoftPro. [22]

Obrázek 6 - SignoTec čtecí zařízení [23]

Německá firma SignoTec nabízí hardwarové i softwarové řešení pro elektronické podepisování. [11][23]

Dalším příkladem je švýcarská firma SignPlus, která poskytuje řešení elektronického podepisování především ve finančních odvětvích. [24]

Dynamický podpis je ovšem možné s vhodným softwarem a aplikacemi snímat z klasického tabletu s digitálním perem, příkladem mohou být tablety od firmy Samsung nebo Apple.

Obrázek 7 - Tablet a stylus od společnosti Apple

3.5 Verifikační metody

Rozeznávají se dvě základní metody ověřování podpisů podle toho, zda se jedná o pouhý statický podpis nebo o dynamický podpis. U obyčejného statického podpisu psaného na papír se používá off-line systém (tzv. statický systém), kdy je naskenován ručně psaný podpis a jeho obraz je pak porovnán s podpisovým vzorem. Na druhé straně pak tedy stojí on-line verifikace (tzv. dynamický systém), která je používána u dynamických podpisů zaznamenávaných na tablety. Zde jsou předmětem verifikace statické i dynamické vlastnosti. [1]

Při srovnávání biometrických dat hledáme tzv. skóre které určuje míru shodnosti dvou vzorků. Vzorky nejsou nikdy na sto procent stejné. Zároveň je nutné určit tzv. mez, která určuje, jak vysoké musí skóre být, aby byl vzorek vyhodnocen jako přijatelný. [15]

U biometrických charakteristik jsou dva ukazatele, které určují míru chybovosti: FAR a FRR. V bodě, kde se kříží se nachází hodnota ERR (equal error rate). [7]

Obrázek 8 - Graf biometrických chyb [15]

3.5.1 Chybné přijetí (FAR – False Acceptance Rate)

Pravděpodobnost chybného přijetí je vypočítána poměrem uživatelů, kteří byli chybně akceptováni do systému k celkovému počtu testovaných osob. Znamená to tedy, že je povolen přístup neoprávněné osobě, což je vážný bezpečnostní problém. [1][15]

3.5.2 Chybné odmítnutí (FRR – False Rejection Rate)

Pravděpodobnost chybného odmítnutí je ta „lepší“ varianta. Vypočítá se jako poměr uživatelů, kterým byl přístup chybně odepřen k celkovému počtu testovaných osob. Znamená to tedy, že autorizovaná osoba je vyhodnocena jako neoprávněná. Není to z pohledu bezpečnosti takový problém, ovšem musí se dbát i na použitelnost a přístupnost systému. [1][15]

Mezi těmito pravděpodobnostními klasifikacemi platí nepřímá úměrnost. Snažíme se tedy najít ideální bod, kdy FAR a FRR budou co nejnižší.

3.5.3 Off-line verifikace

Off-line systém verifikace ověřuje klasické statické podpisy psané rukou na papír. Následně po podepsání je podpis digitalizován, a to naskenováním optickým skenem nebo vyfotografováním. Získaná data se pak skládají pouze ze souřadnic x a y. Off-line verifikace

osoby má tři základní etapy: předzpracování, extrakce biometrických charakteristik, vyhodnocení. [1][4]

3.5.4 On-line verifikace

On-line systém verifikace je systém pro dynamické podpisy, které zaznamenávají i průběh podpisu v závislosti na čase, a proto pokusy o falzifikaci jsou mnohem složitější. Mezi měřené anebo dopočítávané charakteristiky patří rychlost podpisu jako celku, rychlost psaní jednotlivých částí, tlak pera na podložku, pořadí jednotlivých částí podpisu a další. Výstup z dynamického podpisu není pouze obraz podpisu, ale především data reprezentující dynamické vlastnosti, ke kterým se lze dostat po dešifrování DBP. Získaná data jsou reprezentována jako matematická časová funkce F(t), kde je počáteční bod v t_0 a koncový bod v t_n. On-line verifikace má také základní etapy jimiž jsou: **předzpracování a extrakce charakteristik, verifikace, metody porovnávání, určení prahu citlivosti**. [1][4][9][10]

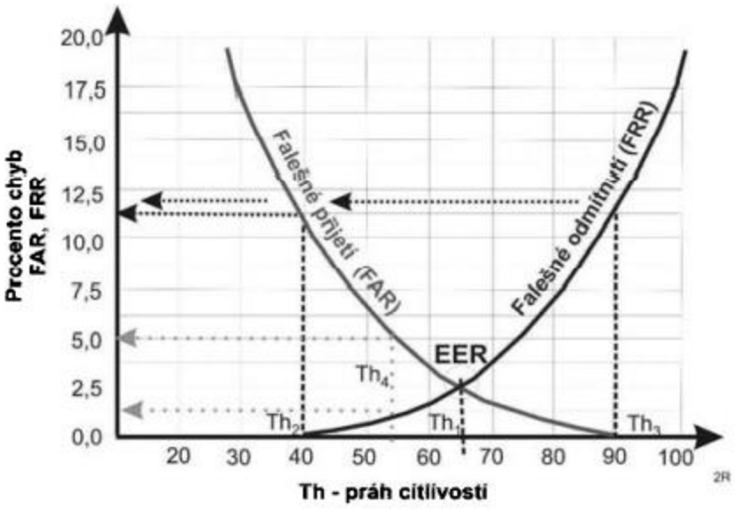
3.5.5 Metody porovnávání:

Uvedeme si několik metod používaných pro porovnání podpisů vzorových/referenčních a právě pořízených.

- Metoda vážené distance – vážená distance dvou podpisů vyjadřuje míru ztotožnění. Dané váhy jsou získávány z referenčních podpisů. [1]
- Statistické metody – pracují s pravděpodobností ztotožnění snímaného podpisu s referenčním. [1]
- Neuronová síť – využívá charakteristiky parametrické a funkční. Má menší chybovost FAR a FRR než metoda vážené distance nebo statistické metody. [1]
- Dynamická časová deformace (DTW – Dynamic Time Warping) a skrytý Markův model (HMM – Hidden Markov Model) – využívají funkční charakteristiky, zpracovávají signály s časovou návazností a stačí pouze jeden referenční podpis. [1]
- Dynamická časová deformace (DTW – Dynamic Time Warping) a Gaussův smíšený model (GMM – Gaussian Mixture Model) – jedná se o míry podobnosti. U GMM je odhadováno pravděpodobnostní rozdělení modelu. Metoda DTW porovnává referenční, a právě nasnímaný podpis pomocí matic. [14]

3.5.6 Práh citlivosti

Volba prahu citlivosti je důležitým faktorem. Práh citlivosti *Th (Threshold)* určuje hranici, kdy je vyhodnoceno přijetí či odmítnutí. Pokud by byla hranice *Th* příliš nízká docházelo by k většímu počtu FAR (chybných přijetí), naopak kdyby byla hranice příliš vysoká zvyšovalo by se číslo FRR (chybné odmítnutí). Tuto vlastnost popsuje níže uvedený obrázek grafu. [1]



Obrázek 9 - Práh citlivosti [1]

U verifikace biometrických vlastností nikdy nedojde ke 100% shodě, a to ani u statických charakteristik. Je logické, že se nikdy nezvládneme dvakrát totožně podepsat, ale například otisk prstu také nepřiložíme dvakrát úplně stejně za stejných podmínek. Pokud dojde při verifikaci ke 100% shodě značí to padělání použitím absolutní kopie vlastnosti. Často jsou zaváděny tzv. prvky životnosti zejména u statických vlastností. Snímá se tedy další faktor, jenž určí, že se nejedná například o fotografii. U otisku se může jednat o snímání toku krve v prstu. Jelikož je dynamický podpis behaviorální charakteristika, tak už ve své podstatě obsahuje prvky životnosti a není potřeba žádné přidávat. [1][8][9][10]

3.6 Bezpečnost biometrického podpisu

Biometrická data jsou osobní údaje, a proto se musí zajistit jejich bezpečnost a integrita. Vedle hardwaru je tedy nutné mít i odpovídající software. Dynamický podpis slouží především pro autentizaci dokumentu, proto je na prvním místě provázání dokumentu s dynamickým biometrickým podpisem a zajištění jejich spojení a integrity. Jinými slovy musíme mít jistotu, že dokument nebyl od jeho podepsání pozměněn. K tomu slouží šifrování dokumentů s biometrickými daty. [12][13]

3.6.1 Kryptografie

Pro zajištění bezpečnosti biometrických dat je využívána kryptografie. Kryptografie je nauka o skrývání informací a zabývá se šiframi. Šifrování sahá do daleké historie, kde se jednalo o substituční šifry jako je Polybiův čtverec nebo Cézarova šifra. Věk počítačů přinesl zároveň nový věk pro šifrování. Kryptografie používá dva druhy šifer: jednosměrné a obousměrné. [12]

- **Jednosměrné šifry** nelze dešifrovat, lze pouze porovnávat to, co je již zašifrované. Příkladem jednosměrné šifry je HASH funkce, kterou lze například používat při ukládání hesel. [12]

  Hash funkce šifruje libovolně dlouhý text na vstupu do textu s přesně danou délkou na výstupu (konkrétně 32 znaků). Hlavní důležitou charakteristikou hash funkce je změna velké části hash při minimální změně na vstupu. Mezi konkrétní hashovací funkce patří MD5, SHA-1 a aktuálně doporučená SHA-2 kam patří verze SHA-224, SHA-256, SHA-384, SHA-512. Právě funkce SHA-2 je využívána u certifikátů a elektronických podpisů. [12]

- **Obousměrné šifry** jsme schopni dešifrovat pomocí klíče a dostat se tak k originální zprávě/dokumentu. [12]

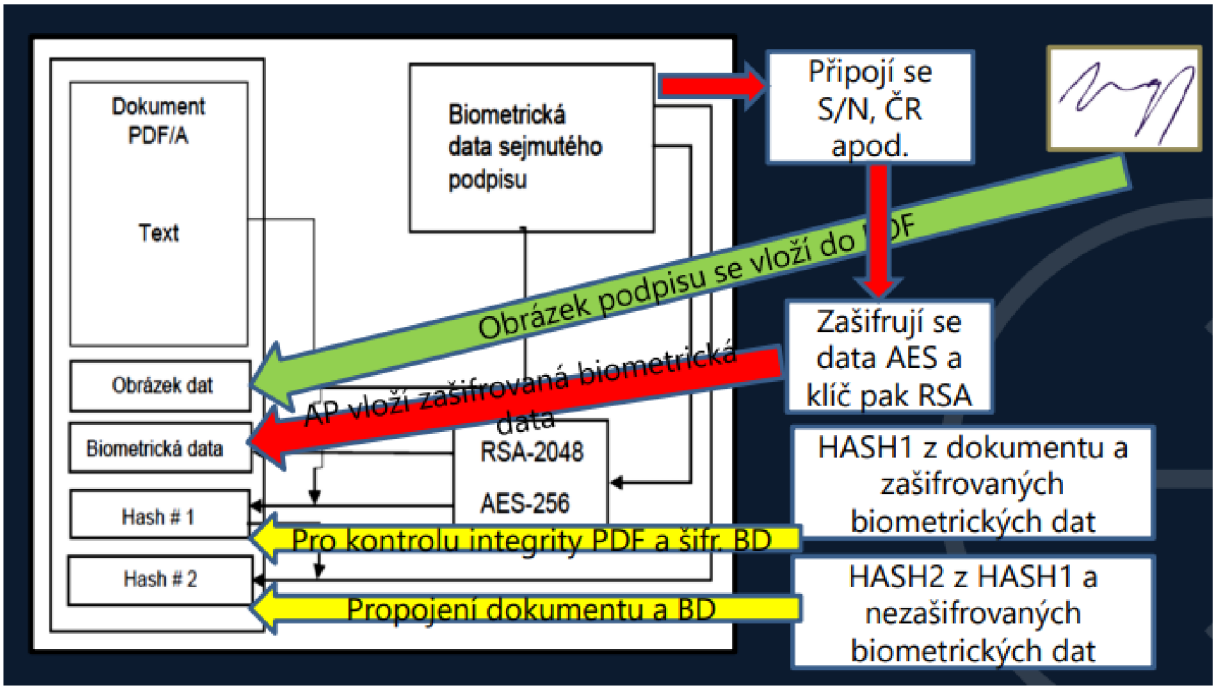
Obousměrné šifry tedy obsahují klíč a lze je dále rozdělit podle toho, zda používají jeden sdílený klíč nebo dva klíče. [12]

- **Jeden klíč** používají **symetrické šifry**. Jednou z prvních šifer v počítačovém věku byla šifra proudová – šifra DES, která se ovšem dnes již nepoužívá, jelikož lze zjistit šifrový klíč při dostatečné znalosti nešifrovaného a šifrovaného textu. Jejím nástupcem je šifra AES v dnešní době používána pro šifrování přenosů dat. [12]

- **Dva klíče**, tzv. páry klíčů, používá **asymetrická kryptografie**. Asymetrie je založena na privátním a veřejném klíči. Na počátku se na zabezpečeném hardwaru vygeneruje vysoké prvočíslo, z nějž se vypočte privátní klíč, dále je z privátního klíče vytvořen veřejný klíč. Hlavními vlastnostmi asymetrického šifrování je, že z privátního klíč lze odvodit veřejný klíč, ovšem z veřejného klíče nelze odvodit privátní klíč. Další důležitá charakteristika zajišťuje možnost dešifrování dat opačným klíčem, než kterým byla zašifrována. V takovém případě data šifrovaná veřejným klíčem lze dešifrovat pouze privátním klíčem a naopak. Příkladem asymetrické kryptografie je RSA šifrování. [12]

3.6.2 Šifrování biometrického podpisu

Biometrická data opouští čtecí zařízení již v zašifrované podobě. Biometrický podpis se bezprostředně připojuje k danému podepsanému dokumentu a zajišťuje se tak jeho integrita. Zde se používají kryptografické metody. [5]



Obrázek 10 - Schéma provázání DBP s dokumentem typu PDF [13]

V tomto schématu popisuje Vladimír Smejkal postup zabezpečování DBP po podepsání dokumentu. [5]

Biometrická data nasnímaného podpisu jsou bezpečným kanálem přesunuta do aplikace. Viditelný obraz podpisu je uložen do dokument pro vizuální účely. Aby podpis byl skutečně

použit pouze jednou a v určeném dokumentu, je k podpisu připojeno sériové číslo zařízení a časové razítko zajišťující integritu. [5]

Biometrická data jsou nejdříve zašifrována symetricky (AES-256) dále pak je symetrický klíč zašifrován veřejným klíčem asymetricky (RSA-2048). Biometrická data podpisu jsou následně propojena s dokumentem. [5][8]

Nyní máme dokument se zašifrovanými biometrickými údaji. Pomocí funkce HASH1, provedenou algoritmem SHA-256, zajistíme integritu dokumentu se zašifrovaným DBP. Máme tedy možnost ověření, že data nebyla pozměněna. Funkce HASH1 je podepsána veřejným klíčem spolu s kterým je vložena do dokumentu. [5]

Dále je pak spočítána funkce HASH2 obdobným algoritmem. HASH2 je spočítána z nezašifrovaných biometrických dat s HASH1 a tím pádem zajišťuje spojení dokumentu s DBP. [5]

3.7 Právní normy

Na úvod je důležité si zařadit dynamický biometrický podpis do kategorie elektronického podpisu podle právních úprav.

Unijní právo definuje elektronický podpis jako: „data v elektronické podobě, která jsou připojena k jiným datům v elektronické podobě nebo jsou s nimi logicky spojena, a která podepisující osoba používá k podepsání“. [18]

Nařízení eIDAS má základ právě v unijním právu. Nařízení eIDAS je nařízení Evropské Unie (Evropského parlamentu a Rady) č. 910/2014, o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu. Některé oblasti mohou být, podle nařízení eIDAS, doformulovány jednotlivými národy. Proto Česká republika přijala zákon č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce. [18]

Na základě těchto nařízení identifikujeme 4 typy elektronických podpisů:

- Prostý elektronický podpis

Nejjednodušší forma elektronického podpisu je prostý elektronický podpis. Tento základní typ zahrnuje mnoho metod, a to například i pouhé zaškrtnutí políčka souhlasu s obchodními podmínkami na webových stránkách, patří sem také napsání jména na konci emailu. Právě do této kategorie se zařazuje i ručně psaný podpis ať už pouze naskenovaný/vyfocený podpis vložený do dokumentu, tak i vzor podpis vytvořený na elektronickém snímači. Prostý elektronický podpis nemá základ v asymetrickém šifrování. [18][19]

- Zaručený elektronický podpis (ZEP)

Připojení zaručeného elektronického podpisu k dokumentu zajišťuje identifikaci podepisující osoby zároveň lze zjistit, zda dokument nebyl od doby podepsání změněn. Nevýhoda ZEP a zároveň důvod proč je často tento princip nevyhovující v praxi je neznalost autora podpisu. ZEP si totiž podepisující osoba vytváří sama, takže není zaručené, že data jsou pravdivá. [18]

- Uznávaný podpis (ZEP založený na kvalifikovaném certifikátu (ZAREP))

Tento typ podpisu je specifikovaný v zákoně č. 297/2016 Sb. Uznávaný podpis je zaručený elektronický podpis, který musí být založený na kvalifikovaném certifikátu tzn. že tento podpis musí obsahovat certifikát (potvrzení) od uznávané certifikační autority. V České republice jsou tři certifikační autority. Jedná se o: První certifikační autorita, a.s., Česká pošta, s.p., eIdentity a.s. [18]

- Kvalifikovaný podpis (KEP)

„Nařízení eIDAS definuje tento typ jako zaručený elektronický podpis, který je vytvořen kvalifikovaným prostředkem pro vytváření elektronických podpisů a který je založen na kvalifikovaném certifikátu pro elektronické podpisy“. [18] Hlavním faktorem vysoké bezpečnosti tohoto typu je nutnost vlastnění USB tokenu, jenž je kvalifikovaným prostředkem pro vytvoření elektronického podpisu. Podpis je uložený pouze na tomto tokenu a nelze ho přenést na jiné zařízení. Lze to chápat jako například kreditní kartu, jsme jejím vlastníkem, známe PIN, v případě ztráty bychom ji měli co nejdříve zablokovat a nechat si vystavit novou, ovšem zároveň není způsob, jak kontrolovat, zda svou kartu (token) nepředá daná osoba osobě další i s přístupovými údaji. [18]

Dynamický biometrický podpis je tedy sám o sobě, pouhý prostý elektronický podpis. Je důležité rozlišovat v jaké sekci českého práva se pohybujeme. V českém veřejném právu jsou vyžadovány vyšší úrovně elektronického podpisu, čímž je uznávaný podpis a kvalifikovaný podpis. Veřejné právo tedy neumožňuje užívání dynamických biometrických podpisů. Oproti tomu české soukromé právo není svázáno tímto omezením a forma soukromoprávních jednání je na samotných jednajících stranách. Samotný DBP ovšem nezahrnuje identifikační údaje o osobě, jenž podpis patří. Tímto problémem se zabývá zákon č. 250/2017 Sb., o elektronické identitě. [19]

3.7.1 GDPR a Úřad pro ochranu osobních údajů

ÚOOÚ v roce 2019 zpochybnil DBP a jeho zpracování označil jako nadbytečné zpracování osobních dat. Nicméně pokud je DBP používán v soukromoprávním sektoru a obě strany souhlasí s touto formou stvrzení dokumentu, není tento čin v rozporu s právem. Není totiž výslovně zakázáno zpracování této zvláštní kategorie osobních údajů. Důležitým

faktorem je tedy svobodnost souhlasu s udělením DBP, aby jeho zpracování nebylo v rozporu s GDPR. [19]

Biometrická data spadají pod zákon č. 101/2000 Sb., o ochraně osobních údajů, protože se jedná o silně citlivé osobní údaje [6]. Tyto biometrické údaje jsou speciální osobní údaje, které spadají pod nařízení Evropského parlamentu a Rady (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů (GDPR). V praxi je tedy DBP prostý elektronický podpis, který lze zpracovávat pouze s výslovným souhlasem. [17]

4 Vlastní práce

4.1 Postup při podepisování

V praktické části byla ve skupině 12lidí testována bezpečnost dynamických biometrických podpisů z hlediska pokusu o falzifikaci vlastnoručních podpisů.

Testování probíhalo ve věkové skupině 20-26 let. Podepisování respondentů vždy probíhalo po dvojicích, kdy se první testovaný podepsal 4krát za sebou, přičemž druhý testovaný se snažil odpozorovat daný podpis, dále měl i možnost si podpis prohlédnout a následně se jej pokusil zfalšovat.

4.2 Sběr dat

Hardware a software použitý k získání dat byl zajištěn ve spolupráci s Československou obchodní bankou. K nasnímání podpisů byl použit iPad Air a Apple Pencil od společnosti Apple.

Obrázek 11 - iPad Air s Apple Pencil

Nasnímaná data jsou ihned v zařízení šifrována, proto byla potřeba všechna data nejdříve dešifrovat. Po rozšifrování byla získala surová data DBP, ve formátu „csv“, která obsahovala čtyři parametry v určitém bodě. Jedná se o čas v milisekundách (T), souřadnice X, souřadnice Y a tlakovou sílu (F).

Na následujících obrázcích je příklad prvních a posledních deseti řádků dešifrovaných dat.

	A	B	C	D	E
1	#	Time	X	Y	Pressure
2	0	0	171	58	81
3	1	4	171	57	81
4	2	8	171	57	81
5	3	13	172	57	81
6	4	17	172	57	81
7	5	21	172	56	46
8	6	25	172	56	26
9	7	29	173	56	13
10	8	33	173	56	1
11	9	38	173	56	0

Obrázek 13 - Prvních 10 řádků dešifrovaných dat

922	920	4566	468	71	80
923	921	4571	466	73	86
924	922	4575	464	76	92
925	923	4579	462	78	82
926	924	4583	460	79	72
927	925	4587	458	81	69
928	926	4591	456	82	65
929	927	4596	455	82	42
930	928	4600	453	83	0
931	929	4600	453	83	0

Obrázek 12 - Posledních 10 řádků dešifrovaných dat

Ze získaných dat vyplývá, že tlaková síla je vždy na začátku tahu na hodnotě 81 bez ohledu na skutečný přítlak. Ovšem tento stav je pouze v rámci milisekund. Jak můžeme vidět na Obr.13 tak v bodě 5 po 21 milisekundách je tlak již bez problému snímán.

4.3 Verifikace dat

Postup probíhal dle etap on-line verifikace. Nejdříve byla data předzpracována a extrahována, následovala verifikace a porovnání dat, na závěr po vyhodnocení dat byl definován práh citlivosti.

Zmíněné čtyři parametry DBP (čas, osa X, osa Y, tlak) byly analyzovány jednotlivě, v závěru jim byla přidělena čtvrtinová váha z celku (25 %) a výsledná data pro jednotlivé charakteristiky byla spojena.

Ve fázi předzpracování dat byl ze tří pravých podpisů respondenta vytvořen podpisový vzor u každého parametru. Podpisový vzor se skládal z průměru těchto tří podpisů a ze směrodatných odchylek.

Ve fázi verifikace bylo podle průměrné směrodatné odchylky vyhodnoceno kolik procent bodů podpisu splňuje danou směrodatnou odchylku. Takto bylo postupováno pro jeden pravý podpis a pro dva falzifikáty. Tento postup byl jednotný pro tlak, osu X a osu Y. U charakteristiky času byl brán v potaz celkový čas vyhodnocení podpisu, tj. od prvního doteku perem tabletu do posledního. Celkový čas u tří pravých podpisů podpisového vzoru byl zprůměrován a byla nalezena směrodatná odchylka a maximální odchylka. Následně byly také nalezeny odchylky pro porovnávaný pravý podpis a falzifikáty. Ve vyhodnocení dat pak hrálo roli, zda odchylka porovnávaného podpisu splňuje hranici směrodatné odchylky nebo hranici maximální odchylky, anebo alespoň hranici dvojnásobné směrodatné odchylky.

Pro vyhodnocení dat bylo nutné spojit všechny čtyři parametry, proto každému parametru byla přidělena čtvrtinová váha ze 100 % a data byla spojena. Výsledné procento představuje celkovou procentuální podobnost k podpisovému vzoru.

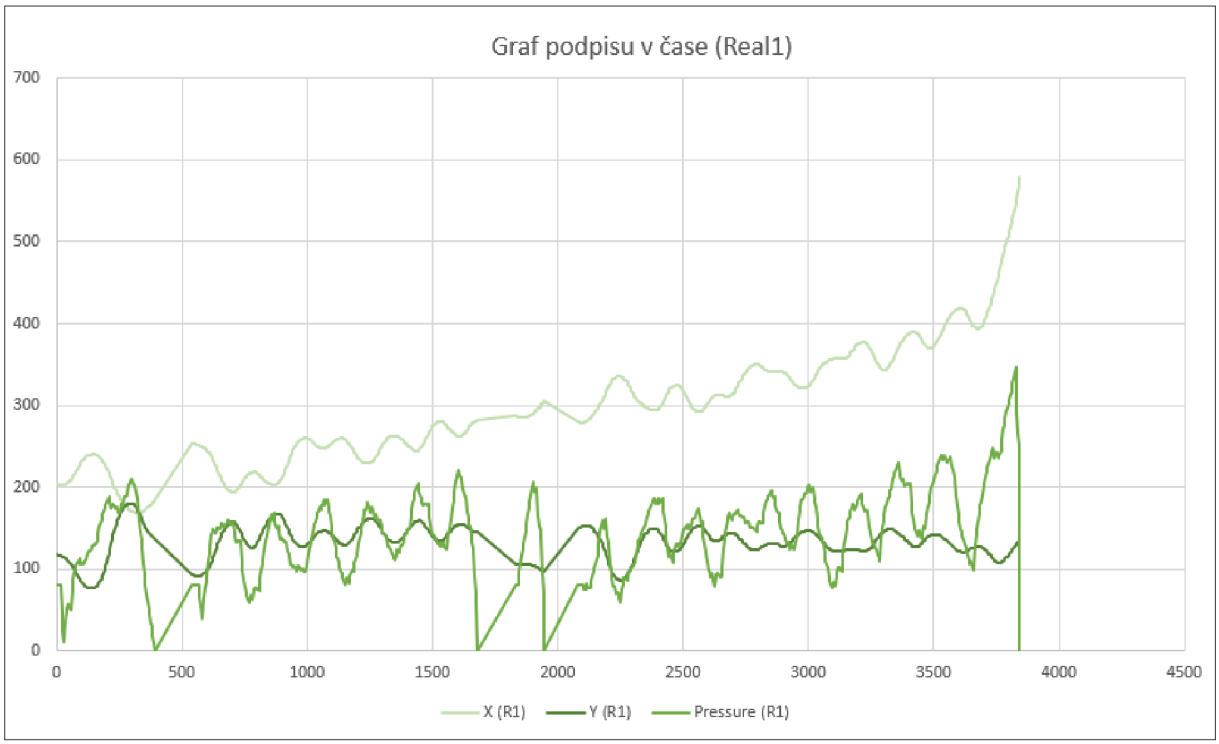
5 Testování

Testování probíhalo na 12respondentech za stejných podmínek a vyhodnocení dat bylo u každého provedeno pomocí stejné analýzy. Podrobněji bude popsán jeden takovýto test. Na základě všech testů proběhlo vyhodnocení dat a určení prahu citlivosti.

5.1 Předzpracování dat

Dešifrovaná biometrická data byla přesunuta do prostředí Microsoft Excel, kde probíhal celý proces analýzy, verifikace a vyhodnocení dat.

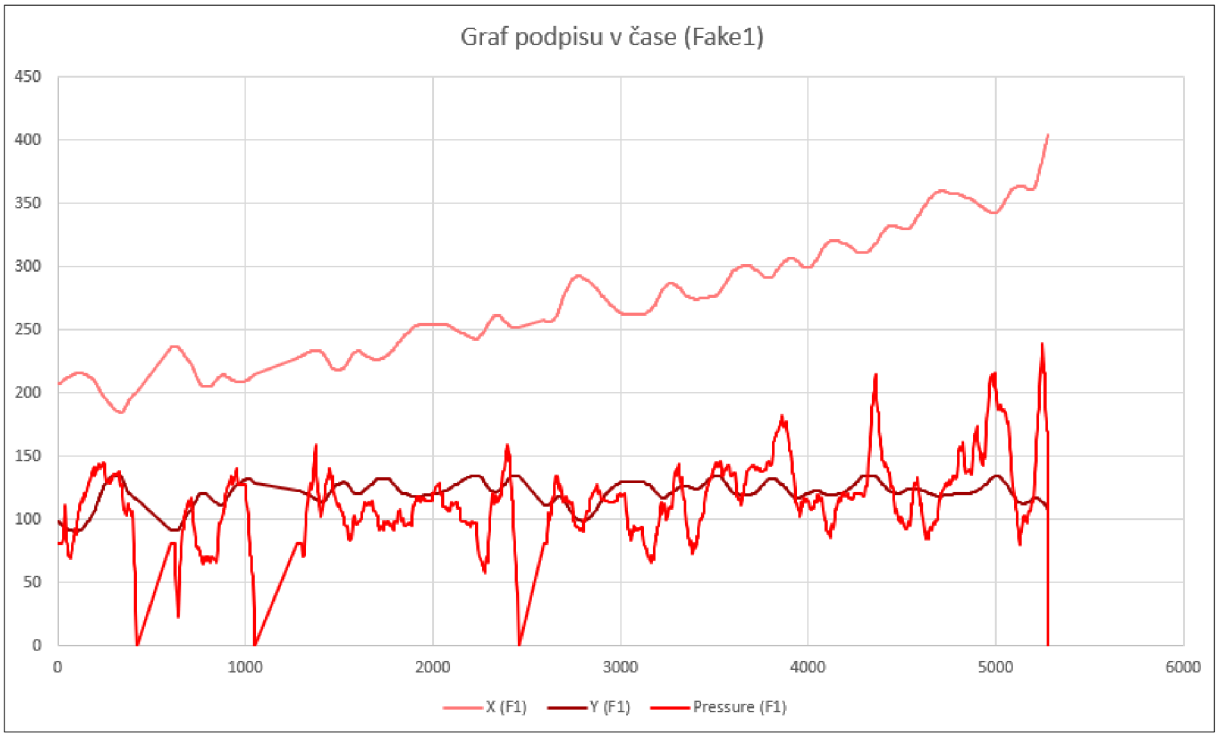
Jeden sešit Excel v příloze představuje jeden test, tzn. čtyři pravé podpisy a dva falešné. Pravé podpisy jsou značené Real1, Real2, Real3, Real4, falešné podpisy jsou pak značené Fake1 a Fake2. Každý podpis má vlastní list v Excel sešitu, kde jsou zdrojová biometrická data a grafy na nichž jsou porovnávané měřené charakteristiky.



Graf 1 - Graf pravého podpisu v čase (Real1)

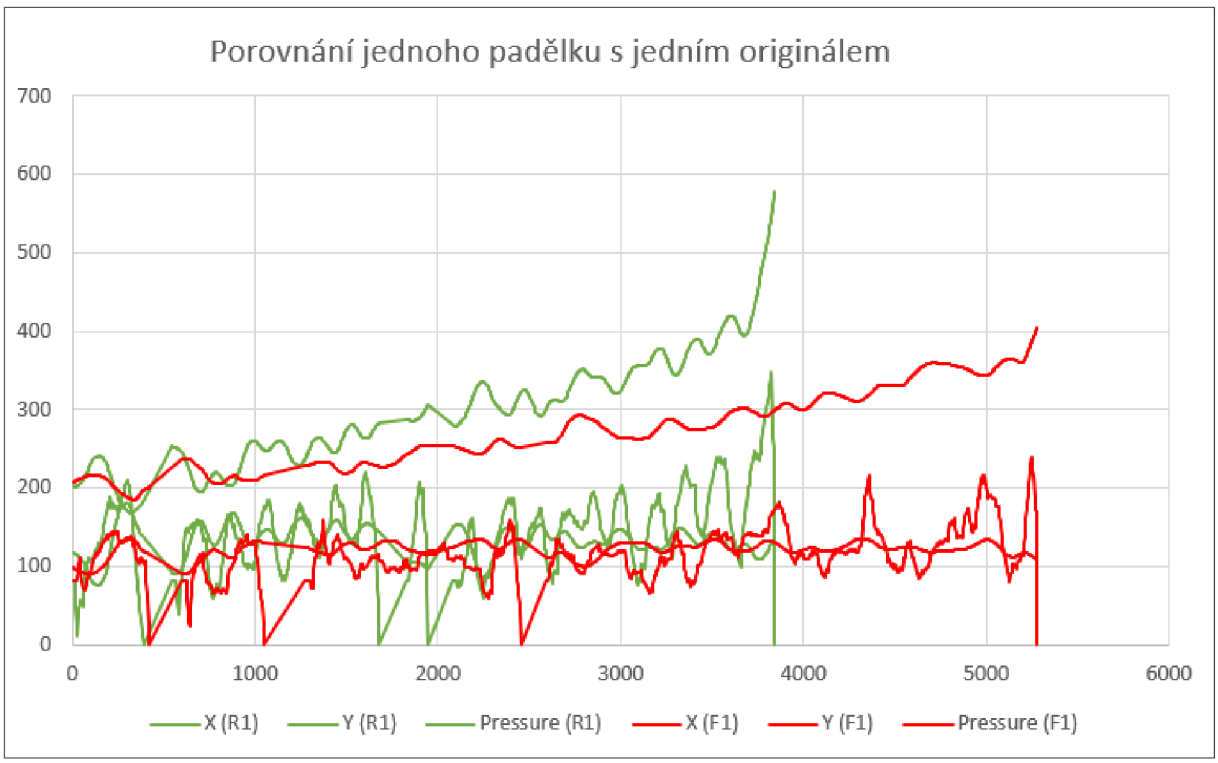
V grafu č.1 vidíme charakteristiky osy X (X (R1)), osy Y (Y (R1)) a talku (Pressure (R1)) v závislosti na čase, jenž je na X ose zobrazeného grafu (čas se blíží ke 4000 ms).

Stejné charakteristiky jsou i u falešných podpisů, jak můžeme vidět na grafu č. 2.



Graf 2 - Graf falešného podpisu v čase (Fake1)

Grafy na první pohled nevypadají příliš odlišně, ovšem je nutné brát v úvahu rozsah grafu. Proto je zde žádoucí provést porovnání těchto dvou grafů, jako je tomu v grafu č.3.



Graf 3 - Porovnání jednoho padělku s jedním originálem

Zde již můžeme pozorovat značné odchylky a časovou neshodu až o přibližně jednu sekundu.

5.1.1 Referenční tlak

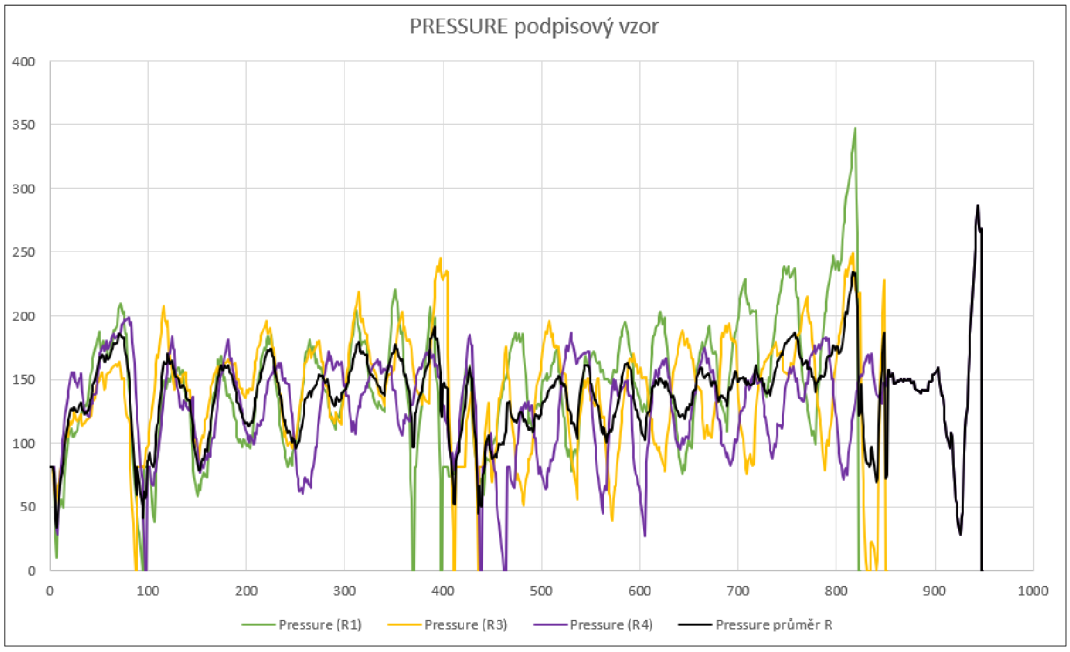
Hlavní fází předzpracování dat je hledání směrodatných odchylek a nalezení průměrné směrodatné odchylky zvlášť pro každý podpisový vzor a zvlášť pro každý parametr.

#	Pressure (R1)	Pressure (R3)	Pressure (R4)	Pressure průměr R	Rozptyl Real podpisů - podpisový vzor	Směrodatná odchylka Real podpisů - podpisový vzor	Průměrná směrodatná odchylka	
0	81	81	81	81	0	0	**25,99**	
1	81	81	81	81	0	0		
2	81	81	81	81	0	0		
3	81	81	81	81	0	0	MAX SO	96,63102791
4	81	66	81	76	50	7,071067812	MIN SO	0
5	46	58	58	54	32	5,656854249		
6	25	50	45	40	116,666667	10,8012345		
7	10	58	32	33,33333333	384,888889	19,61858529		
8	35	67	28	43,33333333	288,222222	16,97710877		
9	47	69	55	57	82,6666667	9,092121131		
10	51	77	71	66,33333333	123,555556	11,11555467		
11	56	81	81	72,66666667	138,888889	11,78511302		
12	54	84	91	76,33333333	257,555556	16,04853749		
13	52	87	102	80,33333333	438,888889	20,94967515		

Tabulka 2 - Podpisový vzor pro tlak

V tomto konkrétním testu vyšla průměrná směrodatná odchylka pro tlak ***25,99*** a určuje tak rozmezí ve kterém jsou přijatelné jednotlivé body porovnávaného podpisu. Tato hranice je vždy vypočítána zvlášť u každého podpisového vzoru pro parametry tlaku, osy X a osy Y.

Na níže uvedeném grafu je zobrazen podpisový vzor pro tlak, jenž se skládá ze tří pravých podpisů a jejich průměru.



Graf 4 - Graf pro talk podpisového vzoru

5.1.2 Referenční souřadnice osy X

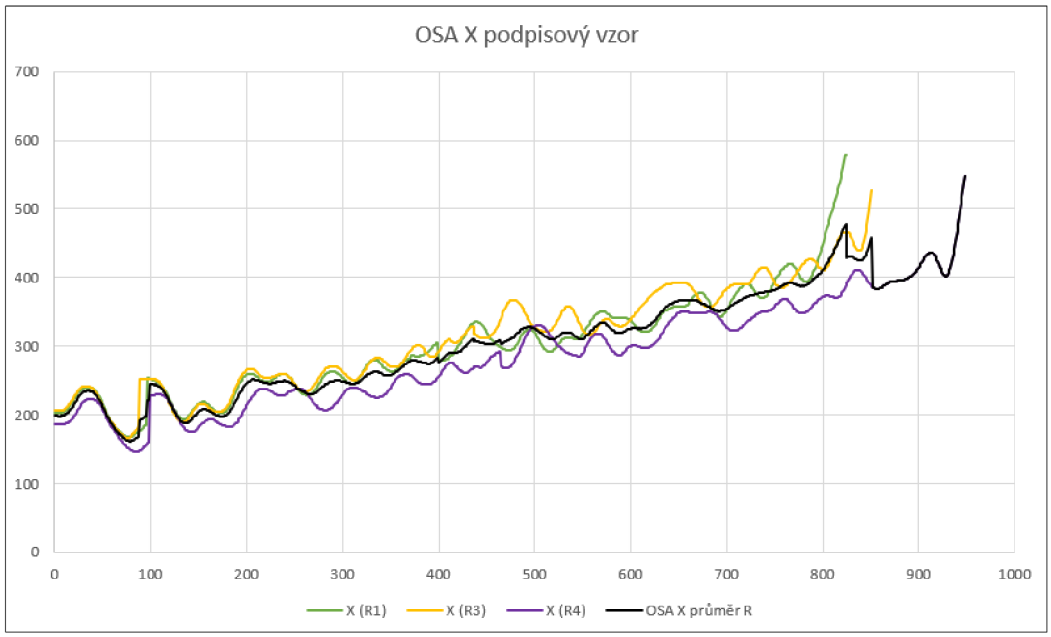
Data byla obdobně předzpracována i pro souřadnice osy X za použití průměru a odchylek.

#	X (R1)	X (R3)	X (R4)	OSA X průměr R	Rozptyl Real podpisů - podpisový vzor	Směrodatná odchylka Real podpisů - podpisový vzor	Průměrná směrodatná odchylka	
0	203	206	187	198,6667	69,55555556	8,339997335	**16,60**	
1	203	206	187	198,6667	69,55555556	8,339997335		
2	202	206	187	198,3333	66,88888889	8,178562764		
3	202	206	187	198,3333	66,88888889	8,178562764	MAX SO	79,17491185
4	202	206	186	198	74,66666667	8,640987598	MIN SO	0
5	202	206	186	198	74,66666667	8,640987598		
6	202	206	186	198	74,66666667	8,640987598		
7	203	206	186	198,3333	77,55555556	8,806563209		
8	203	207	186	198,6667	82,88888889	9,104333522		
9	204	207	187	199,3333	77,55555556	8,806563209		
10	205	208	187	200	86	9,273618495		
11	206	209	187	200,6667	94,88888889	9,741092797		
12	207	210	188	201,6667	94,88888889	9,741092797		
13	208	212	188	202,6667	110,2222222	10,49867717		

Tabulka 3 - Podpisový vzor pro osu X

Průměrná směrodatná odchylka ***16,60*** vyšla pro souřadnice osy X a určuje tak rozhas přijatelnosti bodů souřadnic osy X porovnávaného podpisu.

V následujícím grafu je zobrazení podpisového vzoru pro osu X, což znamená, že se jedná o referenční podpisy a jejich průměr.



Graf 5 - Graf pro souřadnice osy X podpisového vzoru

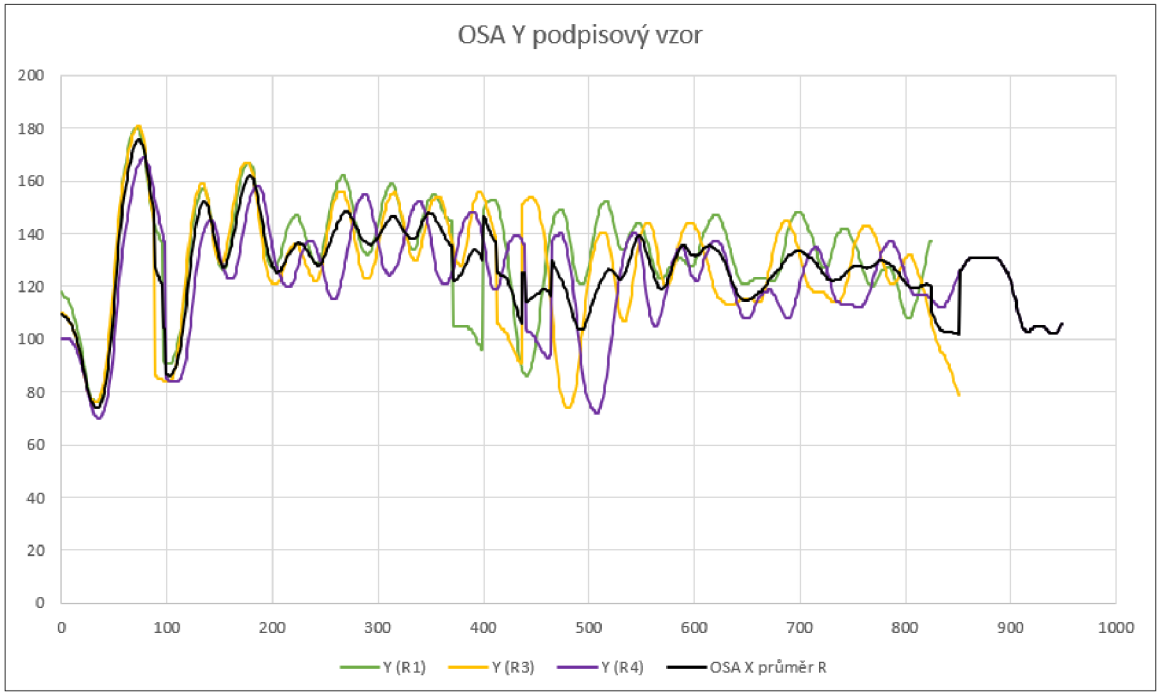
5.1.3 Referenční souřadnice osy Y

Posledním takto předzpracovaným parametrem jsou souřadnice osy Y.

#	Y (R1)	Y (R3)	Y (R4)	OSA X průměr R	Rozptyl Real podpisů - podpisový vzor	Směrodatná odchylka Real podpisů - podpisový vzor	Průměrná směrodatná odchylka	
0	118	110	100	109,3333	54,22222222	7,363574011	**9,59**	
1	117	110	100	109	48,66666667	6,976149845		
2	117	110	100	109	48,66666667	6,976149845		
3	116	109	100	108,3333	42,88888889	6,548960901	MAX SO	33,71778298
4	116	109	100	108,3333	42,88888889	6,548960901	MIN SO	0
5	115	108	100	107,6667	37,55555556	6,12825877		
6	115	108	100	107,6667	37,55555556	6,12825877		
7	114	107	100	107	32,66666667	5,715476066		
8	113	106	100	106,3333	28,22222222	5,31245915		
9	112	106	99	105,6667	28,22222222	5,31245915		
10	111	105	99	105	24	4,898979486		
11	110	104	98	104	24	4,898979486		
12	108	103	98	103	16,66666667	4,082482905		
13	107	101	97	101,6667	16,88888889	4,109609335		

Tabulka 4 - Podpisový vzor pro osu Y

Z referenčních podpisů byl vypočítán průměr, rozptyl a jednotlivé směrodatné odchylky, jejichž průměr je ***9,59*** a určuje možné odchylky od průměru.



Graf 6 - Graf pro souřadnice osy Y podpisového vzoru

Na grafu č. 6 můžeme pozorovat vzorové podpis s jejich průměrem, které dohromady určují podpisový vzor.

5.1.4 Referenční čas

Analýza času probíhala oproti zpracování dat předchozích charakteristik odlišně. Při vyhodnocování časových údajů byl brán v úvahu pouze finální celkový čas vyhotovení podpisu. Tím pádem nás zajímalo ze získaných dat pouze maximum, které logicky je zároveň poslední údaj. Z jednotlivých časů nasnímaných vzorových podpisů byl vypočítán průměrný čas a z něho pak také směrodatná odchylka.

#	Time (R1)	Time (R3)	Time (R4)		Time (R1)	Time (R3)	Time (R4)	Průměrný čas podpisového vzoru
0	0	0	0	MAX =	3843	3856	4234	3977,666667
1	4	4	4					
2	9	9	8	Směrodatná odchylka		181,3327		
3	13	13	12					
4	17	17	16					MAX
5	21	21	21	Odchylky	134,6667	121,6667	256,3333	**256,3333333**
6	25	25	25					
7	29	29	29					
8	34	34	33					
9	38	38	37					
10	42	42	41					
11	46	46	46					
12	50	50	50					
13	54	54	54					

Tabulka 5 - Podpisový vzor pro čas

Směrodatná odchylka v tomto testu vyšla ***181,33 ms***, ovšem nás současně zajímá i maximální odchylka od průměru jenž vyšla ***256,33***, jelikož se jedná o podpisy pravé.

U porovnávaných podpisů s podpisovým vzorem (průměrem) nás pak zajímá, zda jejich odchylka spadá do směrodatné odchylky nebo alespoň do maximální odchylky. Je také možnost, že i pravý porovnávaný podpis bude delší, než je maximální z referenčních, proto je ve vyhodnocení dat času také zohledněna odchylka, které splňuje dvounásobnou směrodatnou odchylku.

5.2 Porovnávání dat

Porovnávání dat nasnímaných s daty referenčními bylo prováděno pomocí směrodatných odchylek těchto podpisů. Ve fázi předzpracování dat byly určené průměrné směrodatné odchylky k jednotlivým parametrům, tyto odchylky si přenášíme s sebou i do verifikační fáze. Podle stanovených odchylek je určeno kolik jednotlivých bodů porovnávaného podpisu toto kritérium splňuje. Tento počet je následně přepočítán, v závislosti na celkovém počtu bodů, na procenta. V závěru tedy získáme procentuální přijatelnost daného parametru. Tento postup je znovu jednotný u parametru tlaku, souřadnic os X a souřadnic os Y.

Pro charakteristiku času byl použit trochu odlišný způsob především, protože je zde počítáno s menším objemem dat. U parametru času si z fáze předzpracování přenášíme průměrný čas podpisu, směrodatnou odchylku a maximální odchylku. Ve fázi verifikace dat pak pouze vypočítáme odchylku času porovnávaného a průměrného podpisu.

5.2.1 Porovnání tlaku

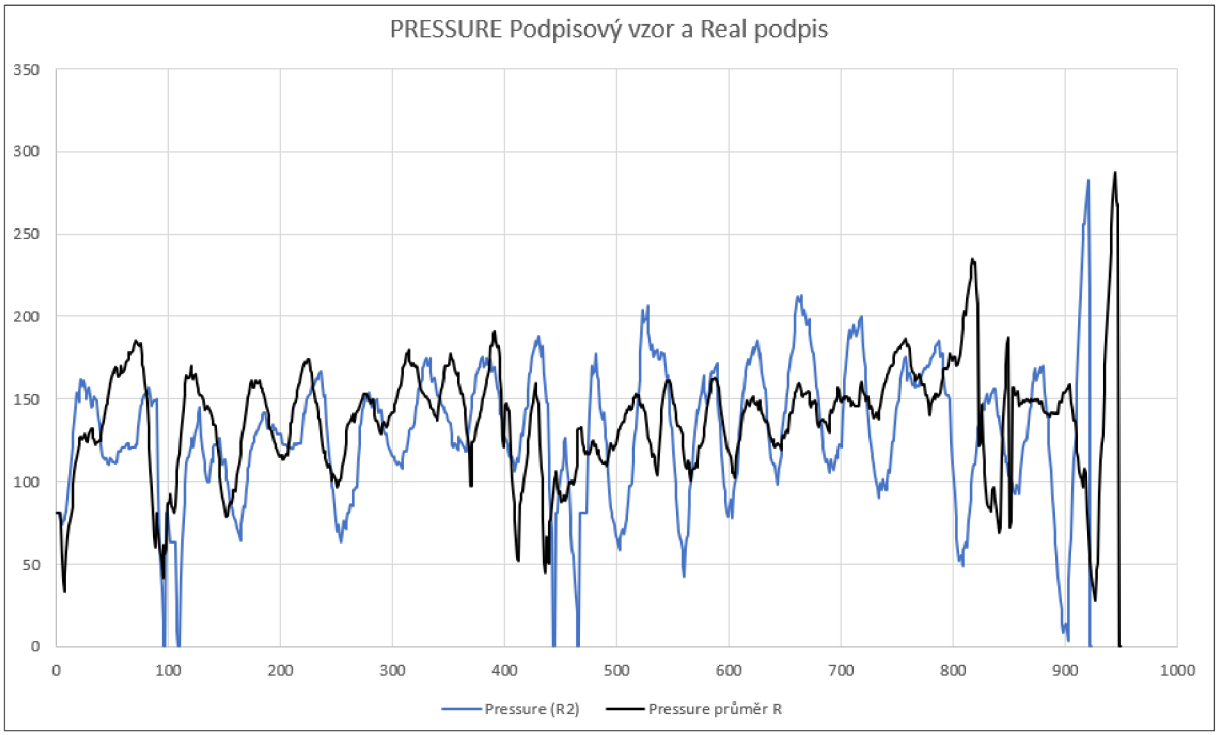
V předchozí kapitole bylo řečeno, že průměrná směrodatná odchylka tlaku referenčních podpisů je ***25,99***, což nám určuje hranice pro tento konkrétní test, kde budou jednotlivé body brány jako přijatelné.

#	Pressure (R2)	Pressure průměr R	Směrodatná odchylka PV a Real		Procento bodů v průměrné směrodatné odchylce
0	81	81	0		78,42%
1	81	81	0		
2	81	81	0		
3	81	81	0	MAX SO	143,5
4	81	76	2,5	MIN SO	0
5	74	54	10		
6	76	40	18		
7	77	33,33333333	21,8333333	SO nad průměr	205
8	79	43,33333333	17,8333333		
9	82	57	12,5	100%	950
10	90	66,33333333	11,8333333	21,5789474%	205
11	98	72,66666667	12,6666667		
12	105	76,33333333	14,3333333		
13	113	80,33333333	16,3333333		

Tabulka 6 - Porovnání referenčního tlaku s pravým podpisem

Pomocí určené průměrné směrodatné odchylky bylo spočítáno, že ***205*** bodů tuto odchylku nesplňuje (SO nad průměr). Následným převedením tohoto výsledku na procenta a odečtením od celku (100 %) bylo zjištěno kolik procent bodů splňuje danou směrodatnou odchylku. Tedy výsledné číslo ***78,42 %*** nám říká, na kolik procent je parametr tlaku přijatelný.

Z grafu je možno také vizuálně porovnat tlak průměrný (referenční) a tlak dalšího pravého podpisu. Můžeme vidět různé vychýlení, ovšem celkově jsou tlaky více podobné.



Graf 7 - Graf porovnání referenčního a pravého podpisového tlaku

Podle referenční odchylky ***25,99*** budeme porovnávat a počítat i další dva podpisy, kde víme, že se jedná o falzifikáty. U prvního padělku vyšlo ***430*** bodů nad danou směrodatnou odchylku. To tedy po dopočítání dá pravděpodobnost ***62,48 %*** přijatelnosti parametru tlaku. Jedná se o nižší hodnotu, než bylo předchozích ***78,42 %*** ovšem ne příliš výrazně. Můžeme zde tedy konstatovat, že padělatel si vedl v parametru tlaku poměrně dobře.

Je nutné zdůraznit, že nezáleží pouze na jednom parametru, ale je nutné brát v úvahu všechny čtyři. Spojení parametrů bude až ve fázi vyhodnocení dat.

#	Pressure (F1)	Pressure průměr R	Směrodatná odchylka PV a Fake		Procento bodů v průměrné směrodatné odchylce
0	81	81	0		62,48%
1	81	81	0		
2	81	81	0		
3	81	81	0	MAX SO	119,5
4	81	76	2,5	MIN SO	0
5	81	54	13,5		
6	81	40	20,5		
7	85	33,33333333	25,83333333	SO nad průměr	430
8	93	43,33333333	24,83333333		
9	103	57	23	100%	1146
10	111	66,33333333	22,33333333	37,5218150%	430
11	90	72,66666667	8,666666667		
12	82	76,33333333	2,833333333		
13	80	80,33333333	0,166666667		

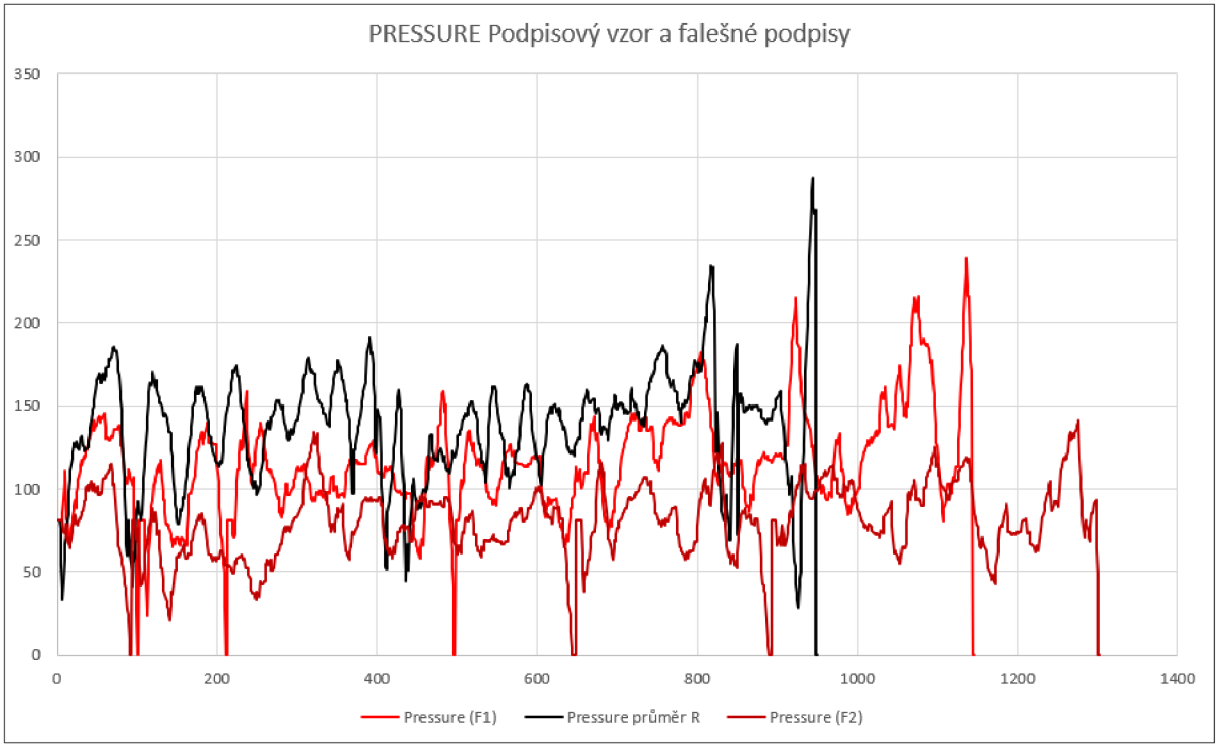
Tabulka 7 - Porovnání referenčního tlaku s falešným podpisem

Na první pohled je vidět, že druhý falzifikát si již tak dobře nevedl. Podle průměrné směrodatné odchylky (*25,99*) bylo zjištěno ***981*** nevyhovujících bodů a tím pádem pravděpodobnost přijetí parametru tlaku pouze ***24,71 %***.

#	Pressure (F2)	Pressure průměr R	Směrodatná odchylka PV a Fake		Procento bodů v průměrné směrodatné odchylce
0	81	81	0		24,71%
1	81	81	0		
2	81	81	0		
3	81	81	0	MAX SO	96,5
4	81	76	2,5	MIN SO	0
5	81	54	13,5		
6	81	40	20,5		
7	81	33,33333333	23,8333333	SO nad průměr	981
8	74	43,33333333	15,3333333		
9	73	57	8	100%	1303
10	73	66,33333333	3,33333333	75,2877974%	981
11	79	72,66666667	3,16666667		
12	71	76,33333333	2,66666667		
13	69	80,33333333	5,66666667		

Tabulka 8 - Porovnání referenčního tlaku s druhým falešným podpisem

Graf průměrného tlaku a padělaných tlaků ukazuje značnější odchýlení oproti minulému pravému podpisu. Můžeme si především všimnout, že tlaky falešné podpisy trvaly déle, a proto mají i více zapsaných bodů s tlakem, zároveň oba padělané podpisy mají tlaky především pod průměrem a téměř se neprolínají, což také způsobuje větší odchylky.



Graf 8 - Graf porovnání referenčního tlaku a falešných podpisových tlaků

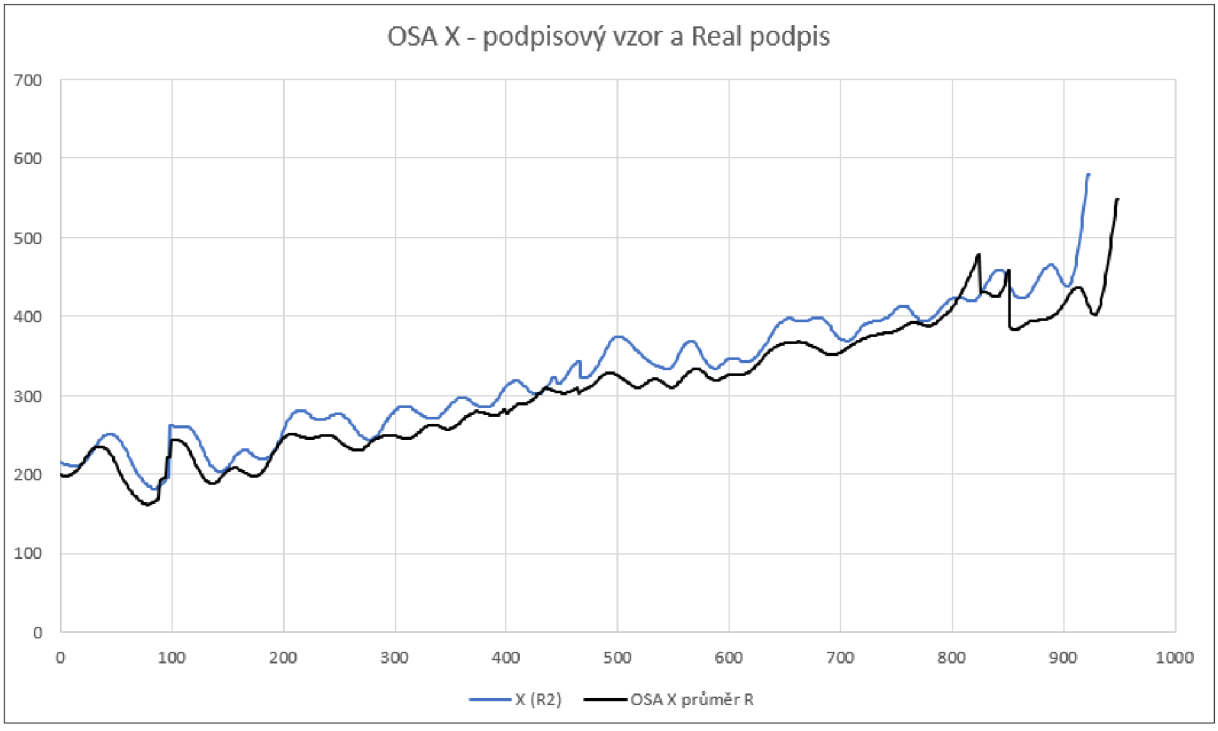
5.2.2 Porovnání souřadnic osy X

Porovnávání souřadnic osy X bylo prováděno stejným postupem jako porovnávání tlaku. Spočítaná průměrná směrodatná odchylka ***16,60*** udává hranice přijatelnosti pro odchylky porovnávaných podpisů. U porovnávaného pravého podpisu bylo směrodatných odchylek nad průměrnou ***231*** z ***950*** bodů, takže konečné procento přijatelnosti tohoto parametru je ***76 %***.

#	X (R2)	OSA X průměr R	Směrodatná odchylka PV a Real		Procento bodů v průměrné směrodatné odchylce
0	216	198,6667	8,666666667		76%
1	215	198,6667	8,166666667		
2	214	198,3333	7,833333333		
3	213	198,3333	7,333333333	MAX SO	274
4	213	198	7,5	MIN SO	0,166666667
5	212	198	7		
6	212	198	7		
7	212	198,3333	6,833333333	SO nad průměr	231
8	211	198,6667	6,166666667		
9	211	199,3333	5,833333333	100%	950
10	211	200	5,5	24%	231
11	211	200,6667	5,166666667		
12	211	201,6667	4,666666667		
13	211	202,6667	4,166666667		

Tabulka 9 - Porovnání referenčních souřadnic osy X s pravým podpisem

V grafu je znázorněný průměr souřadnic osy X (podpisový vzor ze tří pravých podpisů) a porovnávaný pravý podpis. Je vidět, že podpisy mají minimální odchýlení, proto lze brát výsledných 76 % jako dostačující míru přijatelnosti pro parametr souřadnic osy X.



Graf 9 - Graf porovnání referenčních a pravých podpisových souřadnic osy X

Padělaná část podpisu pro souřadnice osy X je na tom výrazně hůře, než tomu bylo u tlaku. Do malé průměrné směrodatné odchylky ***16,60*** se nevešlo ***732*** bodů z ***1146***, což znamená *64%* neúspěch, takže pouze ***36%*** přijatelnost odchylek souřadnic osy X.

#	X (F1)	OSA X průměr R	Směrodatná odchylka PV a Fake		Procento bodů v průměrné směrodatné odchylce
0	207	198,6667	4,166666667		36%
1	208	198,6667	4,666666667		
2	208	198,3333	4,833333333		
3	208	198,3333	4,833333333	MAX SO	202,5
4	208	198	5	MIN SO	0
5	209	198	5,5		
6	209	198	5,5		
7	210	198,3333	5,833333333	SO nad průměr	732
8	210	198,6667	5,666666667		
9	211	199,3333	5,833333333	100%	1146
10	211	200	5,5	64%	732
11	211	200,6667	5,166666667		
12	212	201,6667	5,166666667		
13	212	202,6667	4,666666667		

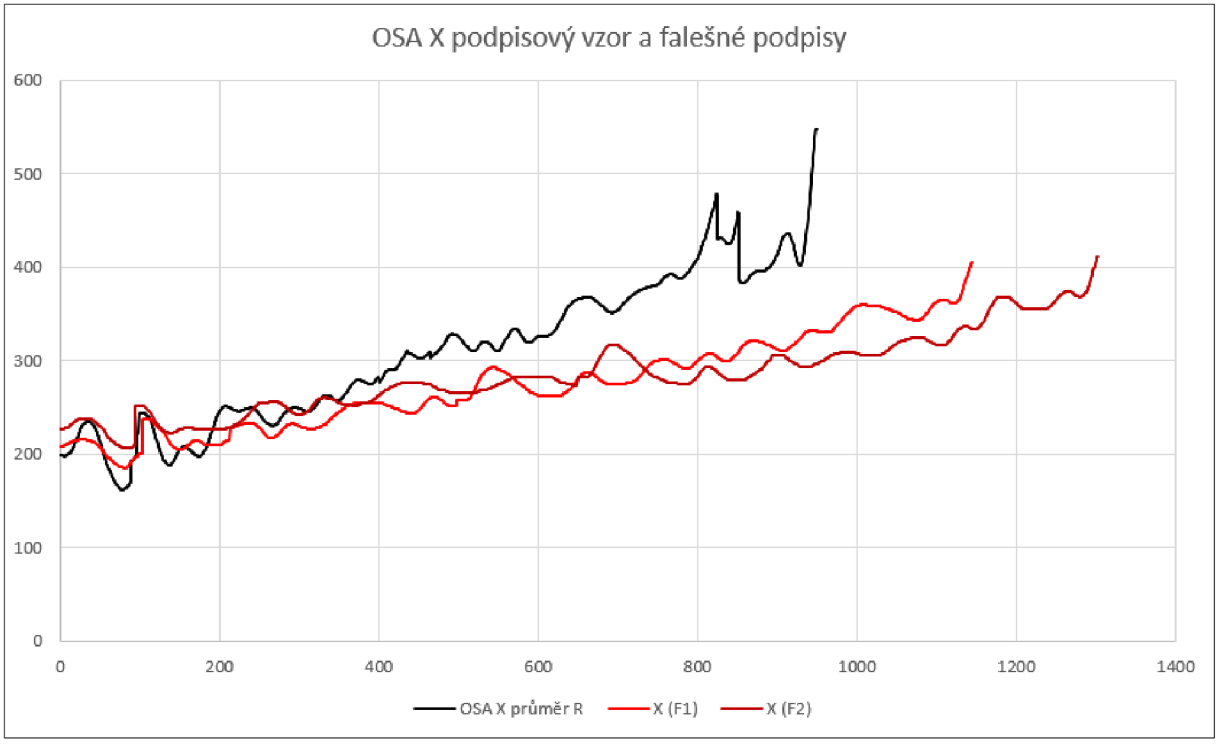
Tabulka 10 - Porovnání referenčních souřadnic osy X s falešným podpisem

U druhého falzifikátu vypadaly výsledky obdobně. Pouhých ***33 %*** přijatelných odchylek souřadnic osy X jasně říkají, že se pravděpodobně jedná o falzifikát (nutné další parametry).

#	X (F2)	OSA X průměr R	Směrodatná odchylka PV a Fake	Průměrná směrodatná odchylka	Procento bodů v průměrné směrodatné odchylce
0	227	198,6667	14,16666667	64,9717319	33%
1	227	198,6667	14,16666667		
2	227	198,3333	14,33333333		
3	227	198,3333	14,33333333	MAX SO	205,5
4	227	198	14,5	MIN SO	0
5	227	198	14,5		
6	228	198	15		
7	228	198,3333	14,83333333	SO nad průměr	877
8	228	198,6667	14,66666667		
9	229	199,3333	14,83333333	100%	1303
10	229	200	14,5	67%	877
11	230	200,6667	14,66666667		
12	231	201,6667	14,66666667		
13	231	202,6667	14,16666667		

Tabulka 11 - Porovnání referenčních souřadnic osy X s druhým falešným podpisem

Z grafu lze dobře vidět, jak se postupně souřadnice osy X u falzifikátů odchylují od podpisového vzoru (průměru). Přesto, že na začátku se padělatel držel reálných souřadnic postupem času se více vzdaloval, což se také projevilo na procentuálním výsledku pouhým úspěchem ***33 %*** a ***36 %***.



Graf 10 - Graf porovnání referenčních a falešných podpisových souřadnic osy X

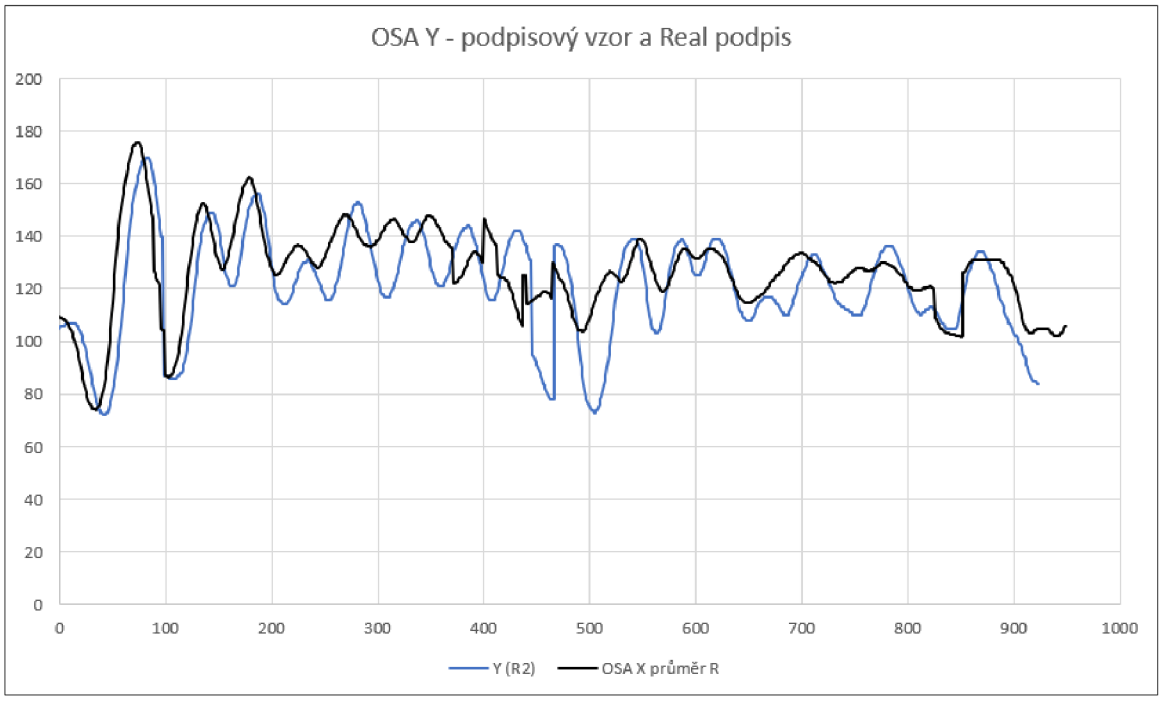
5.2.3 Porovnání souřadnic osy Y

Předposlední porovnávaný parametr, souřadnice osy Y, je znovu porovnáván stejným způsobem jako předchozí dva parametry. Z předzpracování dat víme, že průměrná směrodatná odchylka pro tento test je ***9,59***. Porovnávaný pravý podpis tuto podmínku nesplňuje pouze ve ***212*** bodech z ***950***, takže se dostáváme na ***78 %*** přijatelnosti parametru souřadnic osy Y. Znovu se jedná o poměrně vysoké číslo, což je u pravého podpisu také žádané a bude hrát roli u celkového vyhodnocení dat.

#	Y (R2)	OSA X průměr R	Směrodatná odchylka PV a Real		Procento bodů v průměrné směrodatné odchylce
0	105	109,3333	2,166666667		78%
1	106	109	1,5		
2	106	109	1,5		
3	106	108,3333	1,166666667	MAX SO	53
4	106	108,3333	1,166666667	MIN SO	0
5	106	107,6667	0,833333333		
6	107	107,6667	0,333333333		
7	107	107	0	SO nad průměr	212
8	107	106,3333	0,333333333		
9	107	105,6667	0,666666667	100%	950
10	107	105	1	22%	212
11	107	104	1,5		
12	107	103	2		
13	107	101,6667	2,666666667		

Tabulka 12 - Porovnání referenčních souřadnic osy Y s pravým podpisem

Graf podpisového vzoru v porovnání s pravým podpisem nás utvrzuje v procentuální shodnosti, jelikož vidíme, že ve většině bodech jsou odchylky minimální a pouze v několika místech dochází k většímu vychýlení, což je u podpisů normální a důležitá je celková shodnost všech parametrů dohromady.



Graf 11 - Graf porovnání referenčních a pravých podpisových souřadnic osy Y

I pro padělané podpisy platí stejná průměrná směrodatná odchylka 9,59, jenž nesplnilo u prvního padělaného podpisu 437 bodů, takže procento přijatelnosti souřadnic osy Y je 62 % a jedná se tedy o poměrně dobré napodobení souřadnic osy Y ovšem pro přijetí jakožto pravého podpisu by byla ideální vyšší hodnota. Stále ovšem záleží na součtu všech pravděpodobností jednotlivých vlastností.

#	Y (F1)	OSA X průměr R	Směrodatná odchylka PV a Fake		Procento bodů v průměrné směrodatné odchylce
0	98	109,3333	5,666666667		62%
1	98	109	5,5		
2	97	109	6		
3	97	108,3333	5,666666667	MAX SO	67
4	96	108,3333	6,166666667	MIN SO	0
5	96	107,6667	5,833333333		
6	95	107,6667	6,333333333		
7	95	107	6	SO nad průměr	437
8	95	106,3333	5,666666667		
9	94	105,6667	5,833333333	100%	1146
10	94	105	5,5	38%	437
11	93	104	5,5		
12	93	103	5		
13	93	101,6667	4,333333333		

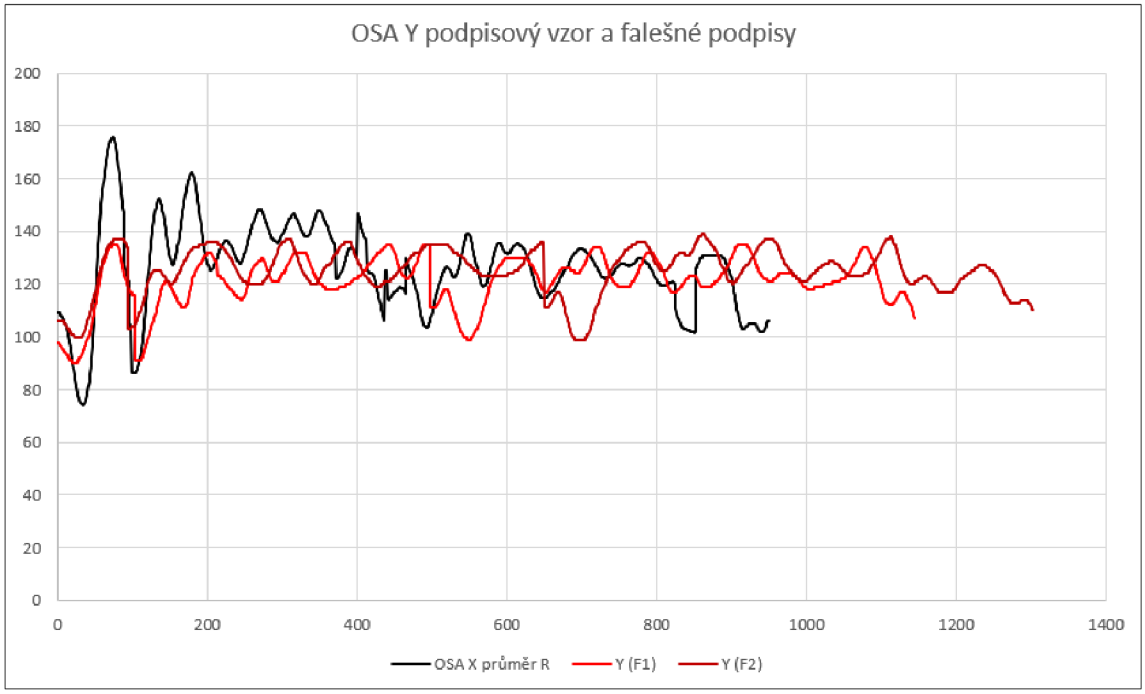
Tabulka 13 - Porovnání referenčních souřadnic osy Y s falešným podpisem

Druhý padělaný podpis je na tom i o trochu hůře a celkově je pouhých ***53 %*** bodů splňujících průměrnou směrodatnou odchylku (*9,59*) pro souřadnice osy Y.

#	Y (F2)	OSA X průměr R	Směrodatná odchylka PV a Fake	Průměrná směrodatná odchylka	Procento bodů v průměrné směrodatné odchylce
0	106	109,3333	1,666666667	21,50537222	53%
1	106	109	1,5		
2	106	109	1,5		
3	106	108,3333	1,166666667	MAX SO	69
4	106	108,3333	1,166666667	MIN SO	0
5	106	107,6667	0,833333333		
6	106	107,6667	0,833333333		
7	106	107	0,5	SO nad průměr	608
8	106	106,3333	0,166666667		
9	105	105,6667	0,333333333	100%	1303
10	105	105	0	47%	608
11	104	104	0		
12	104	103	0,5		
13	103	101,6667	0,666666667		

Tabulka 14 - Porovnání referenčních souřadnic osy Y s druhým falešným podpisem

Na grafu porovnání podpisového vzoru a falzifikátů si můžeme hned všimnout jiné délky souřadnic osy Y v určitých bodech, to souvisí především i s časem vyhotovení podpisu na který se blíže zaměříme v další kapitole. Ovšem větších odchylek si můžeme povšimnout hned na začátku grafu, kde falzifikáty zdaleka nejdou do takového rozsahu jakožto podpisový vzor. Pokud bychom se podívali zpět na porovnání podpisového vzoru s pravým podpisem viděli bychom, že pravý podpis přesně opisoval průměr což značí pravost daného podpisu.



Graf 12 - Graf porovnání referenčních a falešných podpisových souřadnic osy Y

5.2.4 Porovnání času

Závěrečné porovnání času se od předchozích verifikací liší. Pracuje se zde pouze s maximální hodnotou, tzn. pouze s celkovým časem vyhotovení podpisu. V kapitole předzpracování jsme došli k průměrnému času podpisového vzoru ***3977,67 ms*** (necelé 4 sekundy) se směrodatnou odchylkou ***181,33 ms*** a maximální odchylkou ***256,33 ms***.

MAX =	3843	3856	4234	3977,666667
Směrodatná odchylka		181,3327		
				MAX
Odchylky	134,6667	121,6667	256,3333	**256,3333333**

Tabulka 15 - Odchylky času podpisového vzoru

Porovnávaný čas pravého podpisu s referenčním podpisem měl odchylku ***202,33 ms***, což však znamená, že není zahrnut směrodatnou odchylkou. Splňuje ovšem alespoň maximální odchylku ***256,33 ms*** a můžeme ho tak stále považovat za potencionálně pravý (v kombinaci s dalšími parametry).

#	Time (R2)		Time (R2)	
0	0		4180	
1	4			
2	8	Odchylka	202,3333	
3	12			
4	16			
5	20			

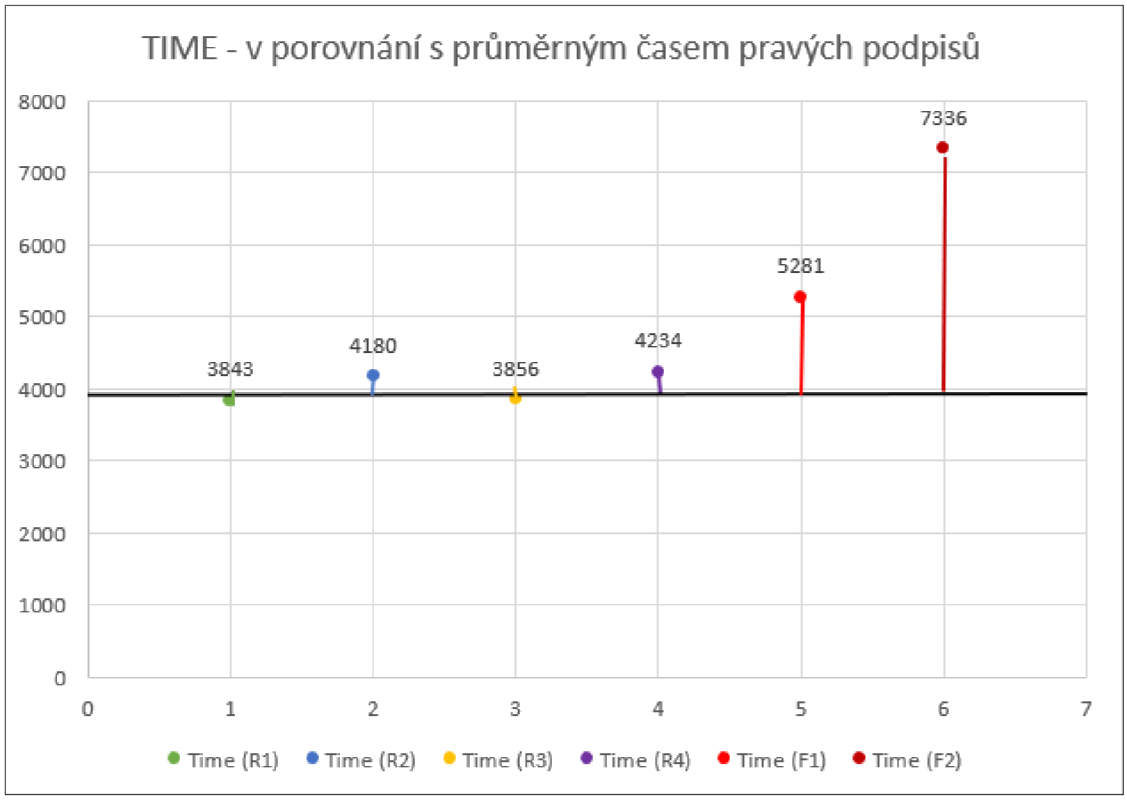
Tabulka 16 - Odchylka času mezi referenčním a pravým podpisem

U dalších dvou porovnávaných podpisů vysoká čísla odchylek značí, že se již jedná o falzifikáty. Směrodatná (***181,33 ms***) ani maximální odchylka (***256,33 ms***) nemají zdaleka blízko odchylkám ***1303,33 ms*** ani ***3358,33 ms***. Pokud se odchylka ve vyhotovení pohybuje okolo 3 sekund, přičemž vyhotovení samotného podpisu trvá okolo 4 sekund, tak už nelze podpis považovat za pravý.

#	Time (F1)	Time (F2)		Time (F1)	Time (F2)
0	0	0		5281	7336
1	4	5			
2	8	9	Odchylky	1303,333	3358,333
3	13	13			
4	17	17			
5	21	21			

Tabulka 17 - Odchylka času mezi referenčním a falešnými podpisy

Vychýlené odchylky falešných podpisů také můžeme pozorovat na níže uvedeném grafu. Černá přímka naznačuje průměrný čas vyhotovení podpisu vypočítaný ze tří referenčních podpisů. Na první pohled je zřetelné vychýlení padělaných podpisů. Delší doba vyhotovení podpisu je častým a běžným ukazatelem falzifikátů, jelikož se pro podepisujícího nejedná o naučený zafixovaný pohyb, ale podpis po něm vyžaduje soustředění, což zabírá více času.



Graf 13 - Graf odchylek času od průměru

5.3 Vyhodnocení dat

Všech 12 testů bylo předzpracováno a porovnáno stejně jakož tomu bylo v konkrétním příkladě rozebíraným v předchozích kapitolách. Výsledky všech testů byly shromážděny do jednoho materiálu, kde byly porovnány i mezi sebou.

Každý test, tzn. tři referenční podpisy, jeden podpis pravý a dva falzifikáty, obsahuje čtyři parametry – tlak, souřadnice osy X, souřadnice osy Y a čas. V rámci jednotlivých charakteristik byla pro přehled shromážděna všechna důležitá data z jednotlivých testů.

Shromážděná data tlaku ukazují, že není příliš těžké napodobit určitý podpis, pokud máme možnost pozorovat jeho psaní, zároveň také není příliš jednoduché nebo běžné zvládnout svůj vlastní podpis se stejným tlakem ve stejných bodech. Například u Testu5 vidíme přesný opak, než je předpokládán. Pravděpodobnostně nejpodobnější tlak má falešný podpis, a to s vysokou shodností ***82,67 %***. Ovšem právě proto je nutná celková pravděpodobnost podobnosti, jelikož právě Test5 má v parametrech souřadnic osy Y a v čase velmi vzdálené hodnoty od průměrů a díky tomu v celkovém hodnocení není přijat jakožto pravý podpis. Podobným příkladem je Test8.

Na druhou stranu pozorujeme i anomálii opačného typu, a to v Testu1, kde tlak pravého podpisu zcela neodpovídá tlaku podpisového vzoru. Podpis z Testu1 se velmi vymyká i v dalších parametrech, čímž se budeme ještě zabývat.

č. Testu	PRESSURE			
	Průměrná směrodatná odchylka podpisového vzoru	Procento bodů v průměrné směrodatné odchylce pravého podpisu	Procento bodů v průměrné směrodatné odchylce falešného podpisu	Procento bodů v průměrné směrodatné odchylce falešného podpisu
Test12	51,11	74,64%	15,25%	22,76%
Test11	49,38	82,02%	41,74%	32,35%
Test10	71,45	81,46%	77,90%	57,12%
Test9	55,90	74,04%	60,54%	66,89%
Test8	27,24	60,78%	83,39%	78,01%
Test7	28,90	70,87%	56,50%	44,73%
Test6	27,50	79,95%	49,87%	55,14%
Test5	59,83	73,36%	79,71%	82,67%
Test4	23,43	66,87%	36,14%	37,28%
Test3	25,99	78,42%	62,48%	24,71%
Test2	50,93	69,34%	59,47%	67,64%
Test1	25,43	19,69%	66,97%	75,45%

Tabulka 18 - Vyhodnocení – Tlak

U parametru souřadnic osy X jsou až na pár výjimek odpovídající procenta přijatelnosti tohoto parametru dle toho, zda se jedná o pravý podpis či falzifikát. Dokonce pravý podpis v Testu12 splňuje danou průměrnou směrodatnou odchylku na ***100 %***. Naši pozornost zároveň opět přitahuje Test5, jelikož i hodnoty padělků jsou vysoké jakož tomu bylo u tlaku, jenže jak již bylo zmíněno podmínky značně nesplňují u osy Y a u času a kvůli tomu je nelze celkově přijmout za pravé podpisy. A také znovu pozastavení u Testu1, kde i pravý podpis má velmi nízké procento přijatelnosti parametru souřadnic osy X a již nyní lze říct, že i přes to, že se jedná o pravý podpis nebyl by přijat.

č. Testu	OSA X			
	Průměrná směrodatná odchylka podpisového vzoru	Procento bodů v průměrné směrodatné odchylce pravého podpisu	Procento bodů v průměrné směrodatné odchylce falešného podpisu	Procento bodů v průměrné směrodatné odchylce falešného podpisu
Test12	28,25	100,00%	54,20%	72,98%
Test11	24,66	95,51%	77,88%	27,06%
Test10	9,81	74,15%	22,79%	20,70%
Test9	10,69	91,04%	0,86%	0,00%
Test8	11,31	87,63%	8,13%	6,16%
Test7	10,25	82,74%	28,29%	29,99%
Test6	15,32	79,65%	30,52%	49,13%
Test5	21,06	90,00%	72,79%	88,72%
Test4	8,34	93,67%	0,00%	0,00%
Test3	16,60	75,68%	36,13%	32,69%
Test2	33,87	86,79%	39,94%	65,09%
Test1	18,05	47,67%	49,39%	46,06%

Tabulka 19 - Vyhodnocení – Osa X

Parametr souřadnic osy Y je na tom obdobně, ne-li lépe, než je tomu u osy X. Už i u Testu5 je vidět značný rozdíl mezi pravým podpisem a falzifikáty. Dokonce pravděpodobnost přijetí u pravého podpisu Testu1 je poměrně vysoká, ovšem to už nebude pro celkové přijetí rozhodně stačit, zde by již nestačilo ani *100 %*.

č. Testu	OSA Y			
	Průměrná směrodatná odchylka podpisového vzoru	Procento bodů v průměrné směrodatné odchylce pravého podpisu	Procento bodů v průměrné směrodatné odchylce falešného podpisu	Procento bodů v průměrné směrodatné odchylce falešného podpisu
Test12	13,78	95,26%	57,14%	69,35%
Test11	7,12	75,28%	28,04%	29,12%
Test10	8,63	72,21%	22,10%	11,74%
Test9	7,05	77,89%	17,08%	5,78%
Test8	15,92	81,63%	42,05%	51,61%
Test7	9,62	73,57%	0,40%	11,42%
Test6	15,04	80,15%	54,59%	43,92%
Test5	9,97	76,64%	48,89%	62,19%
Test4	5,68	73,45%	20,18%	16,80%
Test3	9,59	77,68%	61,87%	53,34%
Test2	19,39	86,32%	48,82%	66,18%
Test1	22,17	70,21%	53,94%	47,58%

Tabulka 20 - Vyhodnocení – Osa Y

Čas je poslední vyhodnocovaný parametr, jenž nesmí být v celkovém součtu opomenut.

č. Testu	TIME				
	Směrodatná odchylka času podpisového vzoru	Maximální odchylka v podpisovém vzoru od průměru	Odchylka pravého podpisu od podpisového vzoru	Odchylka falešného podpisu od podpisového vzoru	Odchylka falešného podpisu od podpisového vzoru
Test12	23,68	29	5	92	129
Test11	49,41	61,33333333	7,333333333	569,3333333	2352,333333
Test10	249,37	347	36	6553	6229
Test9	124,61	156	53	335	195
Test8	68,56	96,33333333	48,66666667	55,33333333	338,3333333
Test7	258,96	362	367	1234	755
Test6	82,83	113,6666667	115,6666667	39,66666667	1006,333333
Test5	251,39	348	73	8616	1739
Test4	60,60	83	47	13363	6465
Test3	181,33	256,3333333	202,3333333	1303,333333	3358,333333
Test2	57,25	79,66666667	10,33333333	795,3333333	378,3333333
Test1	12,26	15,33333333	247,6666667	69,33333333	128,3333333

Tabulka 21 - Vyhodnocení – Čas

Vyhodnocení času bylo obtížnější, než dosavadní charakteristiky zejména jelikož jsou žádané co nejnižší hodnoty a jsou v milisekundách na rozdíl od předchozích požadovaných vysokých hodnot procent přijetí. Proto bylo nutné převést jednotky času do procentuálních hodnot.

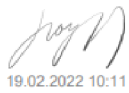
Byly určené čtyři rozmezí pro nasnímaný čas:

- čas je menší než směrodatná odchylka = **100%** přijetí parametru čas
- čas je menší než maximální odchylka = **90%** přijetí parametru čas
- čas je menší než dvounásobná směrodatná odchylka = **60%** přijetí parametru čas
- čas je delší než dvounásobná směrodatná odchylka = **0%** přijetí parametru čas

č. Testu	TIME							
	Směrodatná odchylka času podpisového vzoru	Maximální odchylka v podpisovém vzoru od průměru	Odchylka pravého podpisu od podpisového vzoru	Odchylka falešného podpisu od podpisového vzoru	Odchylka falešného podpisu od podpisového vzoru	Odchylka pravého podpisu od podpisového vzoru	Odchylka falešného podpisu od podpisového vzoru	Odchylka falešného podpisu od podpisového vzoru
Test12	23,68	29	5	92	129	100%	0%	0%
Test11	49,41	61,33333333	7,333333333	569,3333333	2352,333333	100%	0%	0%
Test10	249,37	347	36	6553	6229	100%	0%	0%
Test9	124,61	156	53	335	195	100%	0%	60%
Test8	68,56	96,33333333	48,66666667	55,33333333	338,3333333	100%	100%	0%
Test7	258,96	362	367	1234	755	60%	0%	0%
Test6	82,83	113,6666667	115,6666667	39,66666667	1006,333333	60%	100%	0%
Test5	251,39	348	73	8616	1739	100%	0%	0%
Test4	60,60	83	47	13363	6465	100%	0%	0%
Test3	181,33	256,3333333	202,3333333	1303,333333	3358,333333	90%	0%	0%
Test2	57,25	79,66666667	10,33333333	795,3333333	378,3333333	100%	0%	0%
Test1	12,26	15,33333333	247,6666667	69,33333333	128,3333333	0%	0%	0%

Tabulka 22 - Vyhodnocení – Čas převedený na procenta

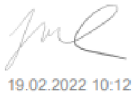
Nyní se dostáváme ke spojení jednotlivých parametrů. Jelikož jsou parametry čtyři každému z nich je přidělena čtvrtinová váha z celku, tzn. ***25 %*** ze ***100 %***. Každý parametr tedy bude přispívat svou pravděpodobností přijetí do maximální výše ***25 %***. Postupně byla spočítána čtvrtina za všech výsledných dat a tyto čtvrtiny byly sečteny pro jednotlivé Testy.



Obrázek 14 - Test1 pravé podpisy

	Pravý	Falešný	Falešný
Test12	92%	32%	41%
Test11	88%	37%	22%
Test10	82%	31%	22%
Test9	86%	20%	33%
Test8	83%	58%	34%
Test7	72%	21%	22%
Test6	75%	59%	37%
Test5	85%	50%	58%
Test4	83%	14%	14%
Test3	80%	40%	28%
Test2	86%	37%	50%
Test1	34%	43%	42%

Tabulka 23 - Vyhodnocení spojených parametrů



Obrázek 15 - Test1 padělané podpisy

Ve výše uvedené tabulce jsou zeleně zvýrazněny hodnoty nad ***70 %*** a červeně jsou zvýrazněny hodnoty pod ***50 %***.

Lze zřetelně vypozorovat, že většina pokusů o padělek se nachází pod ***50 %*** škálou shodnosti, což je velmi nízké procento. Pouze tedy čtyři podpisy překročily hranici ***50 %*** a dokonce pouhé tři podpisy se lehce blíží k ***60 %***. Je tedy především důležité, že žádný z uvedených falzifikátů se neblíží procentům přijatelnosti pravých podpisů (nepočítaje Test1). Nehrozí zde tedy FAR, což je významně nepřijatelná varianta. Proto je i nutné nastavit práh přijatelnosti tak, aby tato varianta hrozila co nejméně.

Jedinou výjimku tvoří Test1, který se značně vymyká. Procenta shodnosti pravého podpisu s podpisovým vzorem jsou dokonce nižší než ne příliš dobré falzifikáty. Zde by se tedy jednalo o případ FRR, což je přijatelnější varianta, jelikož značí určité zabezpečení. A rozhodně je výhodnější odmítnout pravý podpis a zkusit nechat napsat podpis znovu než přijmout padělek za pravý podpis. Proto je nutné najít balanc mezi těmito chybami a správně určit hranici přijetí a odmítnutí.

5.3.1 Práh citlivosti

Práh citlivosti nebo také hranice přijatelnosti byla na základě analýzy dat určena na **70 %**. Volba této hranice souvisí s minimálním procentem přijatelnosti pravého podpisu v testování, nepočítaje anomální Test1. Porovnávaný pravý podpis u Testu7 má hodnotu ***72 %***. Zároveň maximální hodnota shodnosti falzifikátu je u Testu6 ***59 %***, proto bylo třeba zvolit hranici nacházející se mezi těmito dvěma procenty.

S ohledem na požadavek co nejnižších hodnot FAR a FRR, a také skutečnost, že ideálně by žádná FAR nastat neměla, byla zvolena zaokrouhlená hodnota blížící se k minimální procentuální shodnosti pravého podpisu – **70 %**. Tím tedy oddalujeme možnost přijetí falešného podpisu.

	Pravý	Falešný	Falešný
Test12	92%	32%	41%
Test11	88%	37%	22%
Test10	82%	31%	22%
Test9	86%	20%	33%
Test8	83%	58%	34%
Test7	72%	21%	22%
Test6	75%	59%	37%
Test5	85%	50%	58%
Test4	83%	14%	14%
Test3	80%	40%	28%
Test2	86%	37%	50%
Test1	34%	43%	42%
	> 70%		< 50%
	Přijatelná hranice 70%		

Tabulka 24 - Hranice přijetí

6 Výsledky a diskuse

Výsledkem zkoumání vlastní práce je stanovení prahu citlivosti neboli také mezní hranice. Po analýze a zkoumání všech naměřených dat jsem došla k závěru ideální meze 70 % shodnosti. Hranice 70 % určuje, na kolik procent se musí porovnávaný dynamický biometrický podpis shodovat s referenčním podpisem podle individuálně určené odchylky u daného podpisového vzoru. Pokud je procentuální shodnost podpisů nad 70 % je přijat jako pravý podpis, naopak pokud této hranice nedosahuje je považován za falzifikát a je odmítnut. K volbě této hranice jsem přihlížela i z pohledu FAR a FRR, kde se snažím obě chyby co nejvíce minimalizovat, a kde zároveň má větší bezpečnostní prioritu minimalizace chybného přijetí (FAR). Proto jsem při volbě hranice mezi minimální hodnotou pravého podpisu (72 %) a maximální hodnotou falešného podpisu (59 %) z provedeného testování zvolila zaokrouhlené procento s většími nároky na shodnost porovnávaného podpisu s referenčním a zároveň s malou rezervou pro další odchýlení pravého podpisu.

Je nutné interpretovat výsledky až po sloučení a vyhodnocení všech parametrů podpisu, jelikož jsme mohli výjimečně pozorovat velmi dobré hodnoty shodnosti padělaných podpisů u jednotlivých charakteristik, podle čehož by se mohlo zdát, že se jedná o pravý podpis. Překvapivé rozhodně mohly být vyšší hodnoty falzifikovaného tlaku a současně nižší hodnoty tlaku pravého. Tlak je tedy méně stálá vlastnost v porovnání s ostatními parametry.

Jelikož pro každý referenční podpis byly vytvářeny individuální průměrné směrodatné odchylky, není tento systém vhodný pro identifikaci uživatele, tedy pro porovnávání podpisu s celou řadou referenčních podpisů v určité databázi. Ideálně by se měly dynamické biometrické podpisy využívat pro verifikaci. Jinými slovy DBP by byl používán v kombinaci s jiným autentizačním prostředkem, jakož by mohlo být pouze obyčejné jméno a příjmení, průkaz totožnosti, čipová karta či heslo. Pomocí tohoto prostředku by byla zjištěna uživatelova identita a dále by se autentizoval pomocí DBP. Jednalo by se tak o více faktorovou autentizaci.

7 Závěr

Bakalářská práce se zabývala problematikou dynamického biometrického podepisování. Cílem práce bylo především zkoumání bezpečnosti DBP s ohledem na stanovení mezních odchylek přijetí a odmítnutí.

Analýze získaných dat předcházelo prostudování odborných textů a zdrojů souvisejících s tématem biometrických podpisů. V teoretické části práce jsem tedy nejprve přiblížila problematiku biometrik obecně, kde jsou představeny fyziologické i behaviorální vlastnosti člověka a dále jsou upřesněny základná pojmy identifikace, verifikace a autentizace. U autentizace jsem pak popsala její druhy a možnosti kombinace těchto druhů. Ve výsledcích práce, doporučuji tuto možnost kombinace, používat DBP s jinou autentizační metodou, aby se dosáhlo více faktorového ověření a byla zajištěna větší bezpečnost podpisů. Důležitou částí jsou kapitoly o typech podpisů, jelikož dynamický podpis může být často zaměňován za elektronický podpis, ovšem také se již nejedná o klasický podpis na papír, podpis statický. Zde se zároveň dostávám k bližšímu popisu jednotlivých parametrů dynamického biometrického podpisu – času, souřadnicím a přítlaku. Klíčovým oddílem, především pro následující praktickou část, je pak kapitola o verifikačních metodách, kde vysvětluji průběh porovnávání podpisů a další důležité parametry jakož je chybné přijetí a odmítnutí (FAR a FRR). V závěrečné části teoretických východisek přibližuji také technické zabezpečení a právní normy jenž zaštiťují tuto oblast.

Vlastní práce spočívala ve zkoumání odchylek dynamických biometrických podpisů. Praktická část probíhala testováním těchto podpisů. V první řadě tedy proběhl sběr dat od dvanácti testovaných subjektů. Respondenty jsem rozdělila do dvojic, ve kterých se navzájem pokusili zfalzifikovat podpis toho druhého. Každý se nejprve 4x podepsal, přičemž druhý „padělatel“ měl možnost tento proces sledovat a vzápětí se pokusil dvakrát tento podpis napodobit. Po rozšifrování dat jsem postupovala dle fází on-line verifikace. Nejdříve jsem data předzpracovala a vytvořila referenční podpisy ze tří pravých podpisů pro jednotlivé parametry. Následovalo již samotné porovnání dat, a to vždy dat referenčních a jednoho pravého podpisu a dvou padělaných podpisů. Z porovnání jednotlivých charakteristik vyšla určitá procenta shodnosti, která jsem následně sloučila do celkové shodnosti podpisového vzoru a porovnávaného podpisu. Po vyhodnocení všech testů bylo nutné určit procentuální mezní práh shodnosti podpisů pro jejich přijetí či odmítnutí. Tento práh citlivosti jsem vyhodnocovala ze všech získaných a vypočtených dat. Po analýze těchto dat, kde jeden pravý

podpis měl anomální výsledek, a tedy jsem s ním nepočítala v rozhodování o prahu citlivosti, jsem došla k ideální hranici přijatelnosti při 70% shodnosti podpisů. Zmíněný vychýlený pravý podpis byl vyhodnocen za FRR a jednalo by se tedy o chybné odmítnutí, kdy by se uživatel pro autentizaci musel podepsat znovu. Ovšem vyšší prioritu má minimalizace chybného přijetí čehož bylo docíleno právě vyšším nárokem na procentuální shodnost podpisů.

Dynamický biometrický podpis se v posledních letech velmi rozšířil a já věřím, že i do budoucna jeho pole působení bude stále širší. Na závěr bych už jen chtěla říct, že tento výzkum a testování pro mne bylo velmi přínosné a zajímavé, a dokážu si i v budoucnu představit další práci v této oblasti. Zároveň doufám, že i čtenářovi byl tento text jakkoli přínosný a obohatil jej.

8 Seznam použitých zdrojů

Seznam knižních zdrojů

[1] RAK, Roman, MATYÁŠ, Václav, ŘÍHA, Zdeněk. Biometrie a identita člověka ve forenzních a komerčních aplikacích. Praha, 2008. Copyright © Grada Publishing, a.s.. 664 s. ISBN 9788024763927.

[2] ŠČUREK, Radomír. *Biometrické technologie – technické prostředky bezpečnostních služeb.* [online verze]. 1. vydání. Ostrava: Vysoká škola báňská – Technická univerzita, 2015. ISBN 978-80-248-3786-4. Dostupné z: https://www.fbi.vsb.cz/export/sites/fbi/060/.content/galerie-souboru/studijni-materialy/BiometrickeTechnologie.pdf

Seznam sériových publikací

[3] DRAHANSKÝ, Martin. Identita v nás ukrytá (detailní rozbor biometrických systémů). *CONNECT!,* Brno: Computer Press, 2007, č. 4, s. 24-25. ISSN 1211-3085.

[4] HORTAI, František. *Possibilities of dynamic biometrics for authentication and the circumstances for using dynamic biometric signature*. [online]. Brno University of Technology, Faculty of Business and Management, Department of Informatics. EMI, Vol. 9, Issue 2, 2017. ISSN: 1805-353X (Online). Retrieved from: https://pdfs.semanticscholar.org/9ffd/12440ec9b1ac23f0e321afd3ca38ec68288a.pdf

[5] SMEJKAL, Vladimír. *Dynamický biometrický podpis a nařízení GDPR.* [online] Revue pro právo a technologie. Ústav práva a technologií Právnické fakulty Masarykovy univerzity. Brno. Roč. 8, č. 16, 2017. Tato práce je licencována pod Mezinárodní licencí Creative Commons Attribution ShareAlike 4.0. Copyright © 2017 Vladimír Smejkal. ISSN: 1805-2797 (online). Dostupné z: https://doi.org/10.5817/RPT2017-2-5

[6] PAVLÍK, Pavel. *Biometrie jako základ současné i budoucí identifikace a autentizace.* [online verze]. Jihočeská univerzita v Českých Budějovicích, Zdravotně sociální fakulta, katedra informačních systémů. S. 427-430. 2007. ISSN 1212-4117. Dostupné z: https://kont.zsf.jcu.cz/pdfs/knt/2007/02/34.pdf

Seznam online zdrojů

[7] ŘÍHA, Zdeněk, MATYÁŠ, Václav. *Biometric Authentication Systems*. [online verze] FI MU Report Series. Faculty of Informatics Masaryk University. November 2000. Copyright © 2000, FI MU. Retrieved from: https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.32.7232&rep=rep1&type=pdf

[8] SMEJKAL, Vladimír a KODL, Jindřich. *Dynamic Biometric Signature – an Effective Alternative for Electronic Authentication*. Advances in Technology Innovation, vol. 3, no. 4, 2018, pp. 166-178. Copyright © TAETI. Retrieved from: https://www.researchgate.net/profile/Vladimir-Smejkal/publication/327052225_Dynamic_Biometric_Signature_-_an_Effective_Alternative_for_Electronic_Authentication/links/5b75417592851ca6506420c8/Dynamic-Biometric-Signature-an-Effective-Alternative-for-Electronic-Authentication.pdf

[9] ZALASIŃSKI, Marcin, ŁAPA, Krystian, CPAŁKA, Krzysztof. *Expert Systems With Applications. Prediction of values of the dynamic signature features*. Institute of Computational Intelligence, Częstchowa University of Technology, Al. Armii Krajowej 36, 42.200 Częstchowa, Poland. 86-96 s. © 2018 Elsevier LTD. All rights reserved. Retrieved from: https://reader.elsevier.com/reader/sd/pii/S0957417418301738?token=B46830132A8A968ED50281C4B86F5A649DF5EFCE5CBCF54195CFEBC13C62450434ECE1F562D76A9E7746AF87FCD02AAF&originRegion=eu-west-1&originCreation=20220228094044

[10] LAI, Songxuan, JIN, Lianwen, LIN, Luojun, ZHU, Yecheng, MAO, Huiyun. *SynSig2Vec: Learning Representations from Synthetic Dynamic Signatures for Real-World Verification*. School of Electronic and Information Engineering, South China University of Technology. 2020. Vol. 34 no. 01. Retrieved from: https://doi.org/10.1609/aaai.v34i01.5416

[11] DRYGAJLO, Andrzej. *Dynamický podpis.* [prezentace]. Praha: ČVUT FEL [b.r.]. Dostupné z: https://cw.fel.cvut.cz/b181/_media/courses/a6m33bio/ulohy/dynamicky_podpis.pdf

[12] HAVRÁNEK, Martin. *Autentizace.* [videozáznam prezentace]. Praha, 16.11.2021.

[13] SMEJKAL, Vladimír. *Dynamický biometrický podpis a nařízení GDPR*. [prezentace] Moravská vysoká škola Olomouc. Vysoké učení technické v Brně, Fakulta podnikatelská. Dostupné z: https://www.law.muni.cz/dokumenty/40736

[14] WILD, Jiří a SCHNEIDER, Jakub. *Cvičení z předmětu Biometrie, Úloha: Verifikace osoby pomocí dynamického podpisu.* [online]. Praha: ČVUT FEL: 05.10.2015. Dostupné z: https://cw.fel.cvut.cz/b191/_media/courses/a6m33bio/ulohy/podpis-zadani.pdf

[15] BIOMETRIC LINE. *Biometriky* [online]. ©2011-2022 ABAS, a. s. [Cit. 2022-02-09]. Dostupné z: http://www.biometricke-ctecky.cz/biometriky/

[16] PETERKA, Jiří. Jak rozumět dynamickým biometrickým podpisům? In: *Lupa.cz* [online]. 2014. [Cit. 2022-02-09]. Dostupné z: https://www.lupa.cz/clanky/jak-rozumet-dynamickym-biometrickym-podpisum/

[17] KORBEL, František, KOVÁŘ, Dalibor, NEŠPŮREK, Robert a OTEVŘEL, Richard. Dynamický biometrický podpis nově vždy jako zvláštní kategorie osobních údajů. In: *pravniprostor.cz* [online]. 10.06.2019 [Cit. 2022-02-09]. Dostupné z: https://www.pravniprostor.cz/clanky/pravo-it/dynamicky-biometricky-podpis-nove-vzdy-jako-zvlastni-kategorie-osobnich-udaju

[18] HANÁK, Jakub, PRUŠKA, Lukáš. Elektronický podpis pohledem aktuální právní úpravy. In: *epravo.cz* [online]. LAWYA, advokátní kancelář s.r.o. 22.01.2020 [Cit. 2022-02-26]. Dostupné z: https://www.epravo.cz/top/clanky/elektronicky-podpis-pohledem-aktualni-pravni-upravy-110560.html

[19] KORBEL, František, KOVÁŘ, Dalibor, JAROŠ, Ján. Pojistný obzor: Aktuální právní přístup k dynamickému biometrickému podpisu. In: *opojisteni.cz* [online]. Advokátní kancelář HAVEL & PARTNERS. 24.06.2021 [Cit. 2022-02-27]. Dostupné z: https://www.opojisteni.cz/pojistny-trh/pojistny-obzor-aktualni-pravni-pristup-k-dynamickemu-biometrickemu-podpisu/c:21090/

[20] ELEKTRONICKÝ PODPIS. *Elektronický podpis PostSignum*. [online]. Elektronický podpis s.r.o. [Cit. 2022-02-28]. Dostupné z: https://www.elektronickypodpis.cz/

[21] PODNIKATEĽSKÉ CENTRUM. *Elektronický podpis: Môžem podpisovať zmluvy a robiť úkony elektronicky?* [online]. NEPLAT-POKUTY s.r.o. Lighthouse Media Solutions. [Cit. 2022-02-28]. Dostupné z: https://podnikatelskecentrum.sk/elektronicky-podpis-mozem-podpisovat-zmluvy-a-robit-ukony-elektronicky/

[22] INFORMATIC. *Jak funguje biometrický podpis?* [online]. © 2011–2022 INFORMATIC s.r.o. [Cit 2022-03-01]. Dostupné z: https://www.infomatic.cz/zona/uzitecne/temata/jak-funguje-biometricky-podpis

[23] SIGNOTEC. E-signature solution. [online]. SignoTec GmbH. Dostupné z: https://www.signotec.com/portal/startseite.html

[24] SIGNPLUS. GSN Global Signature Net AG. Dostupné z: https://www.signplus.ch/

9 Přílohy

Biometrický podpis a jeho bezpečnost – výpočty.zip obsahující:

- Test1.xlsx
- Test2.xlsx
- Test3.xlsx
- Test4.xlsx
- Test5.xlsx
- Test6.xlsx
- Test7.xlsx
- Test8.xlsx
- Test9.xlsx
- Test10.xlsx
- Test11.xlsx
- Test12.xlsx
- VyhodnoceniTestu.xlsx

Poznámka

Po dohodě se školitelem bylo rozhodnuto, že data obsahující konkrétní identifikační osobní údaje nebudou zahrnuty do připojených příloh.