LATVIJAS UNIVERSITĀTE
DATORIKAS FAKULTĀTE

AUTENTIFIKĀCIJAS METODES UN ALGORITMI

BAKALAURA DARBS

Darba autors: **Igors Matuls**
Studenta apliecības nr. : im10069
Darba vadītājs: profesors Dr. dat. Jānis Zuters

RĪGA 2015

ANOTĀCIJA

Autentifikācija ir viens no ikdienas procesiem mūsdienu pasaulē, kurš notiek katru reizi, kad cilvēkam ir nepieciešams pierādīt autentiskumu. Īsumā Autentifikācija ir autentiskuma pārbaudes procedūra: lietotāja ievadītās paroles un lietotājvārda pārbaude ar esošo datubāzē, vai elektroniskās vēstules pārbaude ar elektroniskā paraksta palīdzību. Autentifikāciju nevajadzētu jaukt ar autorizāciju (procedūra, kas piešķir subjektam noteiktas tiesības) un identifikāciju (procedūra, kas atpazīst subjektu pēc tā identifikatora), jo tās ir dažādas lietas.

Ar katru gadu drošības jautājums uzņēmumiem kļūst ar vien aktuālāks, un līdz ar to nāk vajadzība pēc atbilstoša līmeņa autentifikācijas. Krāpšana tīmeklī, identitātes zādzības un pīkšķerēšana rada bažas par finanšu iestādēm un to lietotājiem. Turklāt pašreizējām autentifikācijas sistēmām ir daudz trūkumu, piemēram lietotāji glabā savas paroles pierakstītā veidā, daži savukārt uzstāda ļoti banālas paroles, kuras var ļoti viegli atšifrēt izmantojot vārdnīcas principus.

Dotā darba ietvaros es piedāvāšu risinājumus, kas varētu izpētīšu esošo situāciju autentifikācijas jomā un piedāvāšu savus risinājumus, kas varētu uzlabot esošās autentifikācijas sistēmas. Šis darbs ir ļoti svarīgs, jo aizsargāt komerciālas transakcijas mūsdienās paliek arvien svarīgāk. Ja autentifikācijas process nebūs pietiekami drošs, tas var ietekmēt ne tikai pašu lietotāju, bet arī lielu organizāciju reputāciju.

ABSTRACT

Authentication methods and algorithms

Authentication is one of the everyday process in today's world, which happens every time, when it is necessary to prove authenticity. Briefly, authentication is procedure verifying the authenticity: when entered username and password are checked with database or emails are verified with token. Authentication should not be confused with authorization (function of specifying access rights to resources) or identification (the process of identifying the subject).

With each year, the issue of security, for firms are becoming more urgent, and with it comes the need for an appropriate level of authentication. Fraud via the web, identity theft, and phishing are raising concerns for users and financial organizations. In addition, current authentication methods, like passwords, have many problems - some users write them down, they forget them, or they make them easy to hack.

In the present work author examine the current situation in the field of authentication and purpose solutions that could improve the existing authentication systems. This research is important because the securing of e-commerce transactions is becoming increasingly important. If the authentication process is not sufficiently reliable, it can affect not only the users but also a large organization's reputation.

ATSLĒGVĀRDI

1. Autentifikācija
2. Autorizācija
3. Identifikācija
4. Drošība
5. Šifrēšana
6. E-Paraksts
7. Sertifikāti
8. Biometrija

SATURS

APZĪMĒJUMU UN TERMINU SARAKSTS

Apzīmējums	Paskaidrojums
IT	Informācijas tehnoloģijas
Bluetooth	Bezvadu datu savienojums
Forums	Diskusiju grupa kādā tiešsaistes pakalpojumu organizācijā
Captcha	Autentifikācijas tehnoloģija, kas paredzēta, lai noteiktu, vai datorsistēmas lietotājs ir cilvēks vai mašīna
Roboti	Automatizēta programmatūra, kas paredzēta kādu darbību izpildei
Urķis	Tehniski izglītots datoru entuziasts
Glitching	Programmatūras defektu izmantošana
Ports	Savienojums, ar kura starpniecību sinhronizē un vada datu plūsmu
Hiperteksta drošas pārsūtīšanas protokols HTTPS	Protokola HTTP paplašinājums, kas garantē drošu datu apmaiņu globālajā tīmeklī
Piekļuves vadības protokols	Autentifikācijas protokols, kas pārbauda lietotāja identitāti un atļauj piekļūt datoram vai sakaru tīklam
Provaiders	Pakalpojuma sniedzējs
Pīkšķerēšana	Neapdomīgu lietotāju aizvilināšana uz tīmekļa vietnēm, kas atdarina reālu organizāciju vietnes.
Pikselis	Vismazākais attēla elements, kam rastrgrafikā var tikt patstāvīgi piešķirti tādi raksturojumi kā, piem., krāsa un spilgtums
Ģenerēšana	Kādas informācijas masveida izveidošana.
Gradients	Plūstoša krāsas pāreja no vienas uz otru.

IEVADS

Jau kopš seniem laikiem cilvēces priekšā stāvēja diezgan sarežģīts uzdevums – pārliecināties par svarīgu ziņojumu ticamību. Tika izgudrotas mutiskas paroles, sarežģīti zīmogi. Kad parādījās pirmās mehāniskās autentifikācijas ierīces, jau palika daudz vieglāk, piemēram parasta slēdzene un atslēga tika izdomātas jau ļoti sen.

Mūsdienās, sakarā ar aktīvu tīkla tehnoloģiju izplatīšanos, automātiskā autentifikācija kļuva ļoti populāra. Jebkurš cilvēks izmanto interneta vietnes kurās ir nepieciešama autentifikācija – sociālie portāli, bankas, e-pasti, forumi, internet veikali un citas sistēmas. Autentifikācija ir viens no pirmajiem aizsardzības līmeņiem visās informācijas sistēmās, kas ir paredzēta, lai sistēma pārliecinātos, ka lietotājs tiešām ir tas par ko sevi uzdod. Neviens nevēlas, lai viņa personīgā informācija būtu pieejam trešajai personai, tādēļ izstrādājot informācijas sistēmu pie autentifikācijas jautājuma ir jāpieiet diezgan nopietni.

Identitātes nozagšana ir viens no mūsdienu populārākajiem noziegumiem, kas var radīt cilvēkam un organizācijām lielus finansiālus zaudējumus. Katru gadu identitātes zādzības pasaulē palielinās un rada ar vien lielākus finansiālus zaudējumus. Piemēram 2013 gadā finansiālie zaudējumi identitātes zādzību dēļ sasniedza 13 biljonus Eiropā un pat 38 biljonus ASV [1].

Tādēļ šajā darbā es centīšos aprakstīt un salīdzināt mūsdienu aktuālākās autentifikācijas iespējas, to plusus un mīnusus un izvēlēties labāko un drošāko variantu turpmākajai realizēšanai reālajā sistēmā, mēģināšu izveidot labāku pirkstu nospiedumu apstrādes algoritmu. Darba mērķis ir izveidot maksimāli drošu un ērtu autentifikācijas sistēmu reālam uzņēmumam, lai pēc iespējas samazināt privāto datu zādzību risku līdz minimumam un izmēģināt jaunu filtru pielietošanu pie pirkstu nospiedumu attēliem, lai palielinātu to kvalitāti.

Šis darbs ir turpinājums iepriekš izstrādātajam kursa darbam „Mūsdienu autentifikācijas iespējas", kura ietvaros tika apkopotas un klasificētas visas autentifikācijas iespējas, kas mūsdienās tiek izmantotas. Darba izstrādē tika izmantoti dažādi avoti – interneta vietnes, zinātniskie raksti, grāmatas kā arī esošā darba pieredze autentifikācijas sistēmu izstrādē iepriekš veiktajos projektos, tādos kā e-Veselība, Ārsta Birojs, NMPD EMY un citos mazākos projektos.

1. IESKATS AUTENTIFIKĀCIJAS METODĒS

1.1. Ievads

Pamata lietotāju reģistrācijas informācijas sistēmā tiek izmantota identifikācijas procedūra – atbildes saņemšana uz jautājumu „Kas Jūs esat?" un autentifikācija – fakta pierādīšana, kad Jūs tiešām esat tas, par ko uzdodaties. Nesankcionēta ļaundara pieeja pie informācijas sistēmas, pirmkārt ir saistīta ar autentifikācijas procedūras pārkāpumiem.

Pamata reģistrācijas procedūru ar EK ir identifikācijas procedūra - saņemtu atbildi uz jautājumu "Kas tu esi?" Un autentifikāciju - pierādījums, ka "jums ir viens, kas piedāvā". Pacēlums no uzbrucējs piekļuvi IP dēļ, pirmkārt, pārkāpjot autentifikācijas procedūru.

Autentifikācija princips pamatā sastāv no slepeno datu, kurus iedeva lietotājs, salīdzināšanas ar jau esošajiem datiem sistēmas datubāzē. Atkarībā no datu tipa, tos var iedalīt 4 pamata faktoros vai arī to kombinācijās.

1.2. Zināšanu faktors (paroles autentifikācija)

Pirmais un pats izplatītākais autentifikācijas mehānisms uz doto brīdi, ievadīt kaut ko, kas ir zināms tikai lietotājam, piemēram parole vai atbilde uz kādu jautājumu. Teorētiski tas ir pats vienkāršākais un drošākais autentiskuma pārbaudes veids, tādēļ, ka to ir grūti uzlauzt (pieņemot, ka parole nav triviāla), kā arī to ir vienkārši realizēt, un viss kas ir nepieciešamas no lietotāja – atcerēties 8-12 burtu un ciparu kombināciju.

Tomēr praksē viss ir savādāk. Pirmkārt cilvēki bieži vien veido vieglas paroles, kas ir saistīts ar cilvēka fizioloģiju, pareizāk sakot ar smadzeņu darbību – mēs domājam asociatīvi un tēlaini un tādēļ izvēlamies paroles tādā veidā kuras būtu vieglāk atcerēties, piemēram telefona numurs, vārds, uzvārds, automašīnas nosaukums, mājdzīvnieka vārds utml. Tādēļ daudzas no lietotāju parolēm ir iespējams atrast parastā vārdnīcā un tad tos ir viegli atminēt veicot pilnu vārdnīcas pārlasīšanu. Par lietotāju vāju kriptogrāfijas paroles izvēli ir uzrakstīti daudz raksti. Viena no vecākajam skaitās 1990 gada Daniela Kleina raksts par to, ka viņam izmantojot vārdnīcu ar 62 727 vārdiem izdevās piekļūt pie 3340 lietotāju profiliem, kas bija 24,2 % no kopējā profilu skaita sistēmā. Pie tam ir vērts atzīmēt divus faktorus: pirmais - kopš tā laika, cilvēki nesāka veidot sarežģītākas paroles un otrais – ņemot vērā „Mūra likumu", skaitļošanas mašīnas kopš tā laika ir kļuvušas vairāk kā 16 000 reizes ātrākas

SafeNet un PasswordResearch pētījumi norāda, ka vairāk kā 30% lietotāju aizmirst savas paroles gada laikā [2][11], pie tam palielinoties paroles sarežģītībai arī palielinās to kļūdainās ievadīšanas skaits. Tādēļ pēc dažiem veiktajiem pētījumiem daudzas informācijas sistēmas nomainīja savu drošības politiku un pieļāva lielāku kļūdainas paroles ievadīšanas skaitu pirms pieejas bloķēšanas.

Nākamā izplatītā metode ir „slepenais jautājums", kurā lietotājam ir jāsniedz atbilde uz jautājumiem kuri viņam tika uzdoti iepriekš un ja atbilde būs pareiza viņam tiks atļauta piekļuve. Šis autentifikācijas veids ir vel sliktāks, jo 2012. gadā IEEE Security and Privacy konferencē tika publicēts pētījums, kurā piedalījās 130 cilvēki, un tika pierādīts, ka 28 % gadījumā cilvēki, kas pazina savu oponentu varēja atminēt atbildes uz dotajiem jautājumiem, bet ja oponents bija pilnīgi nepazīstams, tad atbildes atminēja 17% cilvēku[3]. Beigu beigās rezultāts ir stipri atkarīgs no izvēlētā jautājuma, piemēram jautājums par mīļāko futbola komandu, vai mājdzīvnieka vārdu nekļūs par lielu problēmu, jo šādu informāciju var viegli uzzināt kaut vai no sociālajiem tīkliem. Pie tam pēc 5-6 mēnešiem 16% aptaujāto eksperimenta dalībnieku nevarēja atcerēties atbildes uz šiem jautājumiem.

1.3. Īpašuma faktors (aparatūras autentifikācija)

Otrais populārākais faktors. Pirmām kārtām zem šī faktora tiek domāti aparatūras vai programmatūras sistēmas identifikācija, vai arī identifikācijas pazīmju ievades ierīces. Tās var būt iButton, Smart kartes, USB atslēgas vai USB taloni, RFID identifikatori un līdzīgas ierīces.

iButton ir elektroniskā datoru mikroshēma, kurā ir ieprogrammēta lietotāja personīgā informācija un tas ir ielikts tērauda iepakojumā, kas aizņem ļoti maz vietas. Izstrādātāji garantē tā darbību 10 gadus, pie temperatūras no -40 līdz +70 grādiem pēc celsija. Kā vienu no mīnusiem iButton var atzīmēt to, ka tas nesatur nekādas šifrēšanas metodes, tādēļ to bieži vien izmanto kopā ar speciālu programmatūru kas šifrē datus.

Protams Smart kartes, kas ir veidotas no plastika nav tik drošas pret fiziskiem bojājumiem, kā tērauda iButton, bet arī to izmaksas ir daudz zemākas. Līdz ar to daudzi izvēlas tieši Smart kartes savu autentifikācijas sistēmu veidošanai.

Zibatmiņas atslēgas lielākā problēma ir tā pieslēgvieta. Izstrādātāji pat ietver to specifikācijās, piemēram e-Talona zibatmiņas identifikatoram ir garantēts 5000 reižu pieslēgums.

RFID bezvadu identifikatori un Smart kartes ir pozitīvās puses ir tas, ka viņas satur enerģijas neatkarīgu atmiņu ar kriptogrāfisku procesoru, kas ļauj pastiprināt datu aizsardzību.

Tomēr uzbrūkošā puse neguļ un izdomā visnotaļ dažādus veidus kā piekļūt pie šifrētās informācijas.

Ir publicēti vairāki darbi, kas apraksta dažādus uzbrukumus čipiem-identifikatoriem. Šie pētījumi parāda gan teorētiskas, gan praktiskas metodes čipu atkodēšanai. Pie teorētiskajām metodēm attiecas Bellcore uzbrukumi, diferenciāla analīze DFA, bet pie praktiskajām metodēm var nosaukt glitching metodi – programmatūras defektu, kļūdu izmantošana, un fiziskos uzbrukums, kas tiecas uz meklējamo datu izgūšanu un atkodēšanu.

Rezumējot iepriekš rakstīto, var droši teikt, ka izmaksu dēļ aparatūras autentifikācija tiek izmantota pārsvarā biznesa sektorā. Un no mīnusiem ir tikai divi: tos var nozaudēt vai nozagt un tie var salauzties.

1.4. Sociālais faktors (sociālā autentifikācija)

Kā vel vienu faktoru var izmantot kādu, kas Jūs pazīst, protams ne kādu parastu cilvēku, bet gan tādu sistēmu, kas ir pilnvarota Jūs autentificēt. Piemēram organizācijās kurās lietotājs ir aizmirsis paroli, bieži vien atbildība tiek pārlikta uz administratoru vai palīdzības dienestu. Piemēram Microsoft diezgan ilgu laiku izmantoja šādu metodi – ja lietotājs nozaudēja savu paroli, tad viņa kolēģis varēja no viņa vārda pieprasīt paroles nomaiņu. Šāda pieeja bieži vien pieprasa cita cilvēka iejaukšanos un tiek izmantota nelielos un vidējos uzņēmumos, kur administrators var atrast laiku, jaunas paroles izveidošanai. Lielākās organizācijās ir veselas nodaļas kas nodarbojas ar šāda tipa problēmām. Tomēr Facebook ir līderis šajā jomā[12], jo viņi pirmie izdomāja automatizētu sociālās sistēmas autentifikāciju ar nosaukumu „uzticamais draugs", līdz ar to noteikti ietaupīja lielu naudas summu uz tehniskā palīgdienesta [4].

1.5. Biofaktors (biometriskā autentifikācija)

Tā ir autentifikācija kurā ir nepieciešama speciāla aparatūra, tā saucamais biometriskais skeneris, kas varētu nolasīt lietotāja biometriskos rādītājus. Tie atšķiras pēc nolasāmās informācijas rakstura.

Pirkstu nospiedumu lasītājs – viss biežāk izmantotā biometriskā autentifikācija, kuras pamatā atrodas unikāls cilvēka pirksta nospiedums. Cilvēka pirksta nospieduma attēls kurš tika nolasīts ar skeneri tiek pārvērts par ciparu kodu un salīdzināts ar iepriekš ievadīto šablonu vai šablonu kopu.

Rokas ģeometrija – šī metode arī ir balstīta uz unikālas cilvēka rokas atpazīšanas metodes, kur ar speciālas ierīces palīdzību tiek iegūta trīsdimensionāls rokas modelis un salīdzināts ar iepriekš veidotu šablonu. Daži ražotāji veido tikai pirkstu modeļus.

Atpazīšana pēc acs varavīksnes – šī metode ir balstīta uz unikāla acs varavīksnes zīmējuma atpazīšanas. Priekš tā ir nepieciešama kamera ar pietiekami lielu izšķirtspēju, lai varētu iegūt acs varavīksnes attēlu, kā arī programmatūra, kas spētu izgūt acs varavīksnes zīmējumu pēc kura tiktu uzbūvēts ciparu identifikācijas kods.

Atpazīšana pēc balss – dotajā brīdī šīs tehnoloģijas attīstība sāka strauji virzīties uz priekšu, jo tiek plānota tās izmantošana veidojot tā saucamās „gudrās mājas". Eksistē diezgan daudz dažādu koda piemēru priekš balss atpazīšanas, lielākoties tie ir balstīti uz frekvenču diapazona un dažādām statistiskām vērtībām.

Kopumā visām šim metodēm ir nepieciešama pietiekami dārga aparatūra un ne mazāk dārga programmatūra. Ir diezgan labi izstrādājumi šajās jomās, bet tās vel ne tik drīz kļūs tik populāras kā iepriekš aprakstītas metodes. Esmu pārliecināts kad nākotnē biometrijas metodes būs ikdienas cilvēku sastāvdaļa, jo jau tagad tās uzsāk strauju attīstību.

1.6. Secinājumi

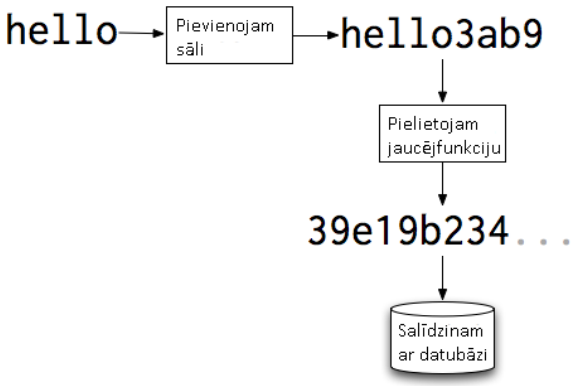
Rezumējot visu augstāk aprakstīto, mēs varam saprast, ka visas autentifikācijas metodes var klasificēt 3 daļās - pēc to automatizācijas pakāpes, izmantošanas prioritātes un autentifikācijas faktora. Katrai no klasificētās kategorijas ir savi plusi un mīnusi un to izmantošana ir stipri atkarīga no dažādiem faktoriem, tādiem kā finanses, uzņēmuma lieluma un vajadzībām.

2. PAPILDUS AIZSRDZĪBAS SLĀŅI

2.1. Ievads

Nav iespējams izveidot drošu autentifikācijas sistēmu neizmantojot papildus aizsardzības slāņus, tādus kā kriptogrāfiskā datu šifrēšana, sīkdatnes un daudzi citi. Šajā sadaļā tiks aprakstītas populārākās autentifikācijas aizsardzības metodes un to reālo pielietošanas piemēri.

2.2. Autentifikācijas šifrēšana

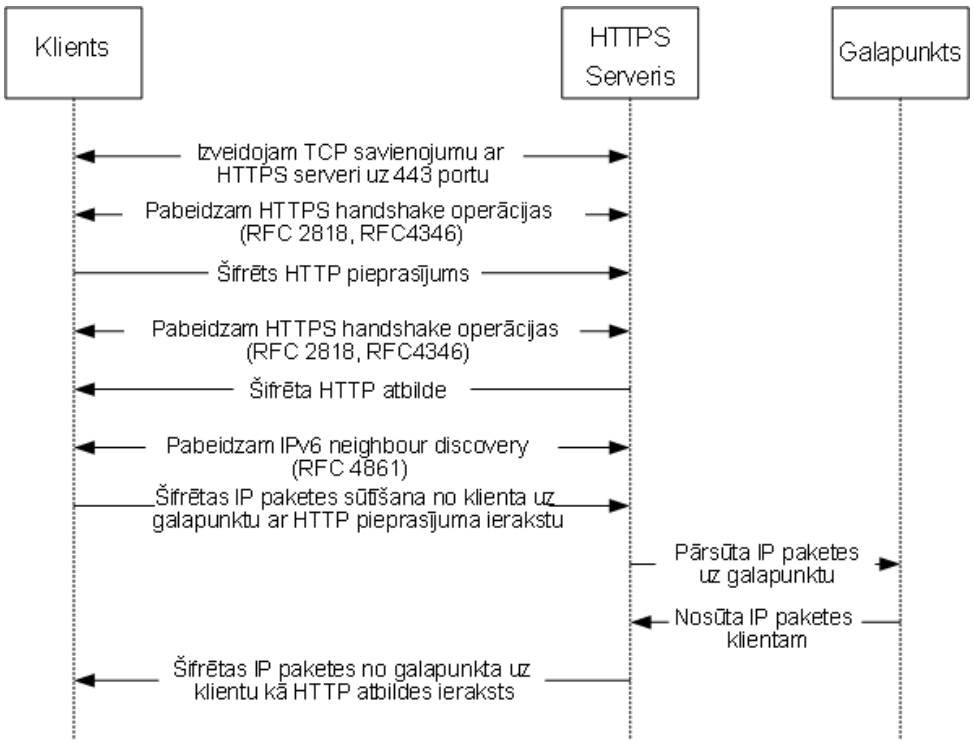


Attēls 2.1. - Šifrēšanas ideja

Jebkurā daudz maz nopietnā sistēmā autentifikācijas procesā nosūtītie un saņemtie dati tiek šifrēti ar dažāda veida algoritmiem. Par šiem algoritmiem var uzrakstīt veselu diplomdarbu, tādēļ šajā paragrāfā stipri neiedziļināsimies un apskatīsim tikai šifrēšanas ideju un dažus piemērus.

Šifrēšanas princips ir ļoti vienkāršs – paņemam saņemto autentifikācijas informāciju, pievienojam tai tā saucamo sāli un izmantojot kriptogrāfiskos paņēmienus nošifrējam. Pēc tam salīdzinām iegūto kodu ar datubāzē saglabāto informāciju. Protams ir vairāki šifrēšanas paveidi, bet princips ir līdzīgs.

Šobrīd visbiežāk paroles šifrēšanai tiek izmantota vienpusēja jaucējfunkcija MD5, kas nozīmē, ka no apstrādātās paroles iegūt oriģinālo paroli nav iespējams. Tomēr, ja parole ir pārāk vienkārša, tad ir iespējams veikt pilno datu pārlasi mēģinot ievadīt vairākas paroles un atrast īstos pieejas datus, to sauc par brutālā spēka metodi (*Brute – force*)



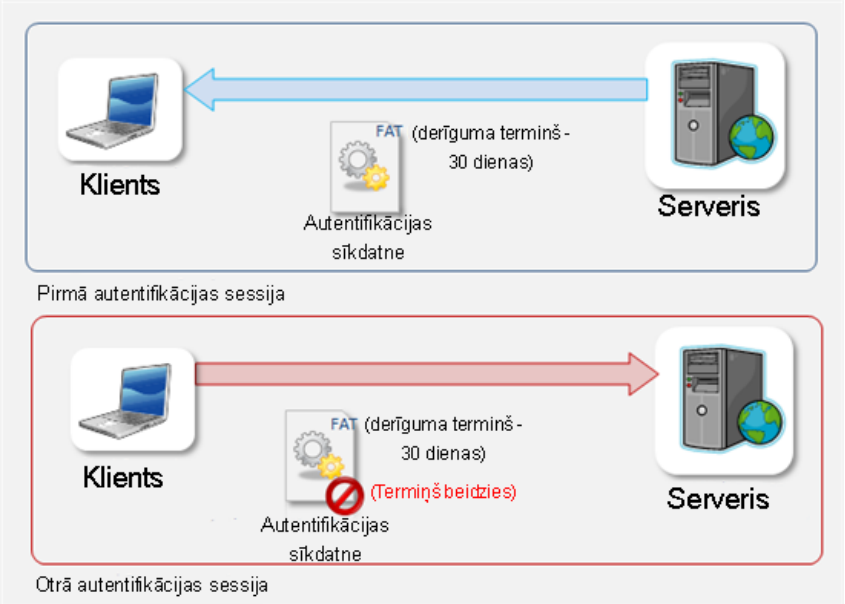
Attēls 2.2. - Hiperteksta HTTPS pieprasījuma shēma

Hiperteksta pārsūtīšanas (HTTPS) protokols palīdz šifrēt visus datus, kuri tiek sūtīti starp pārlūkprogrammu un serveri, nevis tikai lietotāja vārdu un paroli. Protokols tika izstrādāts 1994 gadā ar Netscape Communications kompāniju, speciāli priekš Netscape Navigator pārlūkprogrammas. Šobrīd tas tiek plaši izmantots visā pasaulē un to atbalsta visas pārlūkprogrammas.

HTTPS nav atsevišķs protokols, tas ir HTTP protokola papildinājums, kurā visi sūtītie dati tiek „iepakoti" kriptogrāfiskā drošligzdu slānī (*SSL - Secure Sockets layer*) vai transporta drošības slānī (*TLS - Transport Layer Security*) protokolā. Atšķirībā no HTTP, priekš HTTPS protokola tiek izmantots 443 TCP ports. Šādu protokolu vajadzētu izmantot tādos gadījumos, kad lietotājam ir jāievada svarīgi personiski dati – adresi, kredītkartes numuru vai bankas datus.

Viņš aizsargā no tādiem uzbrukumiem, kuri ir balstīti uz tīkla savienojuma noklausīšanos, piemēram trafika analizatoru uzbrukumiem (*sniffering attack*) – kad kāds lietotājs pārķer tīklā sūtītos ziņojums un var tos analizēt, vai starpnieku uzbrukumiem (*man-in-the-middle attack*) – kad kriptogrāfijas analītiķis (uzbrucējs), spēj lasīt un rediģēt ziņojumus, kurus nosūta citi korespondenti, pie tam neviens no tiem, nav spējīgs uzzināt par to. Diemžēl šī protokola izmantošana stipri palēnina piekļuves ātrumu.

2.3. Sīkdatnes (*Cookies*)



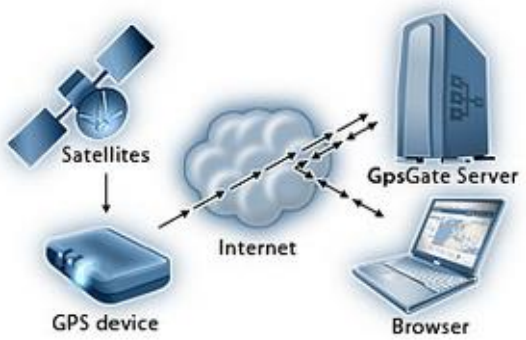
Attēls 2.3. - Sīkdatņu autentifikācijas shēma

Diezgan daudz dažādu mājaslapu kā autentifikācijas līdzekli izmanto sīkdatnes (*cookies*), pārsvarā tās ir tērzētavas (*chatroom*), spēles un forumi. Sīkdatnes ir neliela izmēra datnes, kuras serveris izveido uz klienta datora un ieraksta tajos nepieciešamo informāciju un turpmāk lasa tos pie katras autentifikācijas (skatīt attēlu nr. 10).

Ja sīkdatnes izdodas nozagt, tad, viltojot to, var autentificēties cita lietotāja lomā. Gadījumā kad ievadītie dati tiek nekorekti filtrēti vai netiek filtrēti vispār, nolaupīt sīkdatnes nav nemaz tik grūti. Lai uzlabotu esošo situāciju tiek izmantota aizsardzība pēc IP adreses, tas nozīmē, ka sīkdatnes ir piesaistītas pie noteiktas IP adreses, no kuras lietotājs no paša sākuma autentificējās sistēmā. Tomēr IP adresi var viltot, tādu viltošanas paņēmienu sauc par Interneta protokola viltošanas metodi (*IP-spoofing*), tādēļ uzticēties IP adreses aizsardzībai pilnībā arī nedrīkst.

Uz doto brīdi lielākā daļa pārlūkprogrammu izmanto sīkdatnes tikai ar *HTTP-only* pazīmi, kas aizliedz pieeju pie sīkdatnēm dažāda veida skriptiem. Bet lai vel vairāk nodrošinātu aizsardzību, sīkdatnēm ir derīguma termiņš, un lai tas būtu maksimāli efektīvs, parasti derīguma termiņu uzstāda uz neilgu laiku. Pēdējā laikā arī sīkdatnēs tiek izmantoti kriptogrāfijas paņēmieni, lai šifrētu ierakstītos datus un padarītu tos grūtāk pieejamus noziedzniekiem.

2.4. Lietotāja atrašanās vieta



Attēls 2.3. - Globālās pozicionēšanas sistēma (GPS)

Kā vienu no pēdējā laika jaunākajām tendencēm gribētos pieminēt lietotāja atrašanās vietas noteikšanas sistēmu izmantošanu, lai uzlabotu autentificēšanās drošību.

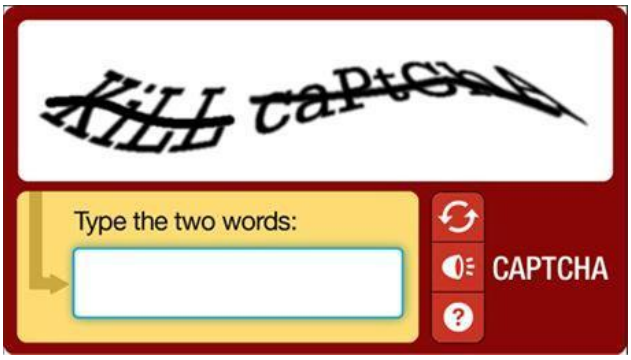
Sistēmas pirms autentificēšanās nosaka lietotāja atrašanās vietu un salīdzina ar iepriekšējām piekļuves vietām, un gadījumos kad autentificēšanās vieta ir stipri izmainījusies, piemēram lietotājs parasti autentificējās no Latvijas, bet pēkšņi autentifikācija notiek no Indijas, tas ir aizdomīgi un tad sistēma pieprasa papildus autentifikācijas parametrus, lai pārliecinātos kad tā ir īstā persona. Kā papildus parametri var būt slepenie jautājumi, e-pasta adrese vai var nosūtīt īsziņu uz reģistrēto tālruņa numuru ar kodu, kurš turpmāk būs jāievada sistēmā.

Pēdējā laikā, noteikt lietotāja atrašanās vietu palika ļoti vienkārši, to var izdarīt izmantojot ierīcēs iebūvēto globālo pozicionēšanas sistēmu (*GPS*), vai arī atsekojot lietoto interneta protokola (*IP*) adresi.

2.5. IP adrešu datu bāze

Ne tik populāra, bet arī izmantota metode ir IP adrešu datubāze, kuras pamatā autentifikācijas serverim ir datubāze ar lietotāju adresēm, kā arī ļaundaru adresēm, līdz ar to, ja piekļuve pie notiek vai nu no jaunas IP adreses, vai no ļaundaru reģistrētās adreses, serveris var attiecīgi reaģēt uz šādiem gadījumiem un veikt papildus identitātes pārbaudes.

2.6. Drošības kodi (*CAPTCHA*)



Attēls 2.4. - Drošības kodi (CAPTCHA)

Esmu pārliecināts, kad praktiski jebkurš zina kas ir drošības kodi (*CAPTCHA*), jeb HIP drošības uzdevumi. Tie ir teksti, kurus sistēma piedāvā ievadīt pirms veikt kādu darbību, lai pārliecinātos par to, kad lietotājs, kas veic darbību sistēma, nav robots, kurš mēģina ļaunprātīgi iegūt pieeju pie slēgtās informācijas ar iepriekš aprakstīto spēka metodi (*Brute-force*).

Drošības kodi parasti ir izveidoti tādā veidā, lai ļaunprātīgā programmatūra nevarētu tos atpazīt ar teksta atpazīšanas tehnoloģijām, tādēļ bieži vien tie ir uzrakstīti tik nelasāmi, kad arī cilvēkam ir grūti tos atpazīt un pārrakstīt.

2.7. Secinājumi

Neskatoties uz to, kad kompānijas mēģina viss dažādākajos veidos aizsargāt savus lietotājus un to personīgos datus, lauži atrod veidus kā apiet šīs sistēmas un ar katru gadu parādās jaunas tehnoloģijas, algoritmi un idejas kā pasargāt savus un citu datus no nelikumīgas piekļuves. Es personīgi uzskatu, kad šajā nozarē ir vel ļoti daudz iespēju, kā var uzlabot autentifikācijas drošības līmeni.

Kā nelielu piemēru varētu minēt divu studentu izpētes darbu[5], kurā viņi veica peles kustību analīzi un izveidoja algoritmu, kas bija spējīgs noteikt kad mainās datora lietotājs atkarībā no lietotāja peles izmantošanas pieradumiem. Šādas tehnoloģijas pielietojums varētu būt ļoti aktuāls praktiski jebkurā sistēmā. Pieņemsim Jūs veicat bankas pārskaitījumu kādā publiskā vietā un Jums nozog datoru tajā brīdī kad Jūs esat autentificēts, pateicoties šādai aizsardzībai bankas sistēma varētu noteikt kad ir nomainījies lietotājs un piedāvāt pa jaunam ievadīt pieejas paroles, līdz ar to aizsargāt Jūsu kontu.

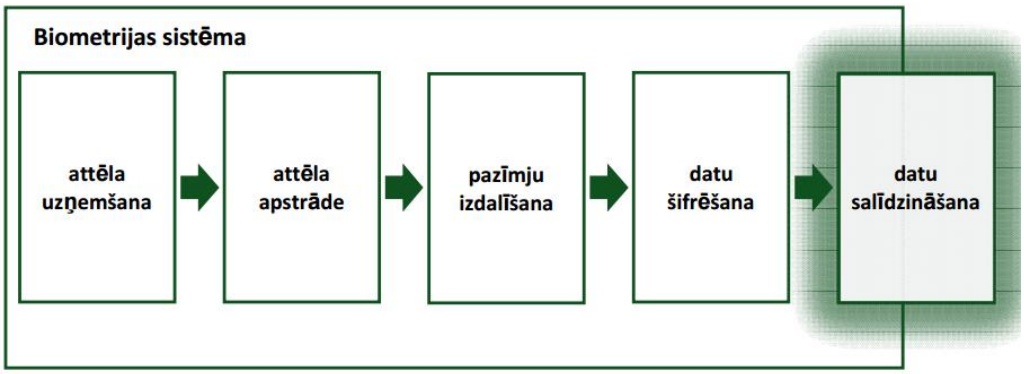
3. IZVĒLĒTAIS AUTENTIFIKĀCIJAS VEIDS

3.1. Ievads

Pēc visu iespējamo autentifikācijas metožu analīzes, tika nolemts izveidot divu faktoru autorizācijas sistēmu, pamatā balstītu uz biometrijas autentifikācijas faktora, jo pēc vairāku rakstu un izpētes darbu analīzes, kā arī autora domām, šis autentifikācijas veidam jābūt viss drošākajam un ērtākajam no visiem, kā arī nākotnē tas var kļūt par vienu no populārākajiem pasaulē, kaut arī pagaidām vel nav tik izplatīts.

Kā otru iemeslu, kādēļ tika izvēlēta biometrijas autentifikācijas metode bija iespēja praksē to realizēt esošajā uzņēmumā un veikt pienācīgus testus, lai saprastu tās darbības principus un to, vai tā ir pietiekami droša un stabila ar mūsdienās pieejamo tehniku un izstrādātajiem algoritmiem.

3.2. Ieskats biometrijā



Attēls 3.1. - Biometrijas autentifikācijas sistēmas pamatprincips

Atšķirībā no esošajām autentifikācijas metodēm, kuras ir balstītas uz tā, ka mums kaut kas pieder, vai arī mēs kaut ko zinām – piemēram magnētiskā karte vai parole, bet gan to, kas ir personai. Tas nozīmē, ka ar biometrijas autentifikācijas metodi lietotājam vairs nevajadzēs atcerēties sarežģītas paroles, domāt par to saglabāšanu un drošību un maiņu, kā tas ir parasti. Tādēļ, ka tiek izmantoti unikāli indivīda parametri, kas ir cilvēka neatņemama sastāvdaļa un kurus ir diezgan sarežģīti viltot.

Vārds autentifikācija šajā gadījumā satur sevī vairāk nekā parasti, jo tas ietver arī identificēšanas (identitātes noteikšanas) un verificēšanas (vai sakrīt reālā un deklarētā identitāte) procesus.

Visas biometriskās sistēmas strādā pēc līdzīga principa. Pirmkārt sistēma iegaumē lietotāja biometriskos paraugus (to sauc par ieraksta procesu). Ierakstīšanas brīdī dažas sistēmas var palūgt ievadīt vairākus paraugus, lai izveidotu precīzāku biometrijas pazīmes attēlu, tad saņemtā informācija tiek algoritmiski apstrādāta un pārvērsta matemātiskā kodā. Autentifikācija parasti notiek četrās stadijās: Ierakstīšana – sistēma nolasa un iegaumē lietotāja fizisko vai uzvedības paraugu; Izšķiršana – no parauga tiek izņemta unikālā informācija un tiek izveidots biometriskais paraugs; Salīdzināšana – kad saglabātais paraugs tiek salīdzināts ar iesniegto; „Sakrišana/nesakrišana" – sistēma nolemj, vai iesniegtais paraugs sakrīt ar datubāzē esošo paraugu un atgriež lēmumu.

Diezgan ilgu laiku biometriskā identitātes noteikšanas tehnoloģijas ieviešana tika aizkavēta dēļ pietiekami precīzas aparatūras neesamības un programmatūras līdzekļu, kas ļautu automatizēt šo procesu. Pēdējā laikā tehnoloģijas ir strauji attīstījušās un ir parādījušās jaunas tehnoloģijas, kas atrisina šīs problēmas. Kā arī aparatūras cenas ir strauji kritušās un plašam lietotāju lokam kļuva pieejamas biometriskās identifikācijas sistēmas, kuras agrāk bija pieejamas tikai nelielam pilnvarotam personu lokam.

Dotajā sadaļā analizējot mūsdienu stāvokli biometrijas tehnoloģiju jomā tiek lietots termins „identifikācija", kā neatņemama sastāvdaļa no ilgtspējīgas izteiksmes „*biometric identification*", kas apraksta biometrijas pārbaudi plašā vārda nozīmē, iekļaujot arī autentifikāciju.

3.3. Pirksta nospiedumu atpazīšana

Pirkstu nospiedumus izmantoja, lai identificētu personību, jau Senajā Ēģiptē, Asīrijā, Ķīnā, Japānā. Pirmais zinātniskais raksts (1823. gads) par pirkstu nospiedumiem pieder Braslavas Universitātes profesoram J.E. Purkinjē. Viņš aprakstīja pirksta nospiedumu modeļus kas tiek izmantoti vel joprojām. Ārsts Henrijs Folds iepazīstināja cilvēci ar pirksta nospiedumu uz papīra, kā cilvēka identifikācijas metodi jau 1824 gadā. Viņš to arī pirmais izmantoja praksē, kad pēc pirkstu nospieduma atpazina noziedznieku. Bet pašas pirmās komerciālās pirkstu nospiedumu atpazīšanas sistēmas parādījās iepriekšējas simtgades 60-tajos gados.

Šīs biometriskās identifikācijas metodes pamatā atrodas katra cilvēka pirksta unikālais papillāru modelis. Priekšrocības – viegla izmantošana, ātrums un drošība. Sociālie pētījumi[6]

arī ir parādījuši, ka lietotājiem tas ir arī pats ērtākais autentifikācijas veids. Pie tam biometriskais pirkstu nospiedumu skeneris ir pietiekami kompakts un iekļaujas pat parastā klaviatūrā.

Katrā pirkstu nospiedumā ir iespējams atrast divu veidu pazīmes – globālās un lokālās. Globālās pazīmes – tās, kuras var redzēt ar neapbruņotu aci:

- Papillāru zīmējums;
- Attēla platība – fragmenta, kurā atrodas visas unikālās pazīmes, izdalīšana;
- Kodols – punkts, kas atrodas pirksta nospieduma vidū vai arī kādā iezīmētā platībā.
- Delta punkts – sākuma punkts. Vieta kurā notiek līniju sadalīšanās vai savienošanās, vai arī ļoti īsa līnija (varbūt pat punkts)
- Līnijas tips – divas lielākās līnijas , kas sākas paralēli un tad apiet apkārt visa pirksta zīmējumam.
- Līniju skaitītais – līniju skaits, kas atrodams attēlā, vai arī starp kodolu un deltu.

Otrā pirkstu nospiedumu pazīme – lokālā. Tās ir katra pirksta nospieduma unikālās pazīmes, kuras arī sauc par munīcijām. Tās nosaka līniju struktūras izmaiņas punktus (beigu, sadalīšanās, pārrāvumu punkti utt.), šo līniju orientāciju un šo punktu koordinātes. Katrs pirkstu nospiedums satur ap 70 munīcijām.

Pirksta nospieduma attēls, kuru iegūst ar speciāla skenera palīdzību, tiek pārvērsts par ciparu kodu un tiek salīdzināts ar iepriekš ievadītu etalonu. Eksistē divi pamata algoritmi saņemtā koda salīdzināšanai ar esošo šablonu datubāzē, pēc raksturīgajām pazīmēm un pēc visa pirksta nospieduma virsmas. Pirmajā gadījumā tiek identificētas raksturīgās pazīmes un to savstarpējā atrašanās vieta. Otrajā gadījumā tiek iegaumēts viss pirksta nospiedums. Dažkārt arī tiek izmantota algoritmu kombinācija, kas ievērojami palielina sistēmas drošību.

Bieži vien datubāzē glabā vairākus etalona piemērus, kas palīdz uzlabot identifikācijas precizitāti. Tie var atšķirties ar nobīdi un pagriezienu, maksimālais pirksta nospieduma pagrieziens no vertikālā stāvokļa var būt ne vairāk kā 15 grādi. Mērogs netiek mainīts, jo visi pirkstu nospiedumi tiek iegūti no vienas ierīces.

Vidēji negatīvais identifikācijas procents legāliem lietotājiem sastāda aptuveni 3%, bet kļūdaini pozitīvo reakciju ir mazāk nekā viens pret miljonu. Šāda varbūtība ir daudz mazāka salīdzinot ar citām biometrijas metodēm, it īpaši ja ņemt vērā, kad vidējā pirkstu nospiedumu atpazīšanas varbūtība kriminālistiem ir aptuveni 70%, kaut arī daktiloskopija tiek izmantota jau vairāk kā 100 gadus un skaitās pietiekami droša. [7]

Kā šīs metodes pozitīvās puses gribētos atzīmēt ļoti labu cenas un kvalitātes attiecību, kā arī nelielus skenera izmērus, kas pieļauj to izvietošanu pat portatīvās ierīcēs. Pie trūkumiem var atzīmēt to, ka eksistē negatīva attieksme no lietotāju puses, iespēja diezgan viegli izgatavot pirkstu kopijas, tā pat skenēšana ir stipri atkarīga no pirkstu tīrības un var būt problēmas, ja cilvēkam ir kādi pirksta bojājumi. Bet visām no šīm problēmām ir savi risinājumi – ja cilvēkam ir bojāts pirksts – ir iespēja ieskanēt vairāku pirkstu kopijas un lietot jebkuru no tiem. Attiecībā uz pirkstu kopiju izveidošanu – jau kādu laiku ir pieejami skeneri kas spēj pārbaudīt vai tas ir reāls pirksts (termiskā analīze, bioloģiskā analīze utt.).

3.4. Plaukstas formas atpazīšana

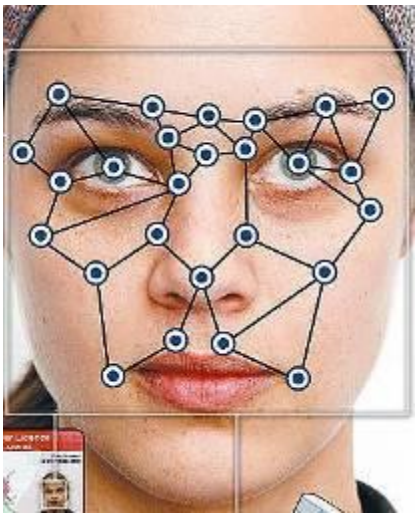
Šī ir salīdzinoši jauna metode, kas ir attīstījusies no kriminālistikas nozares, tiek veikta identifikācija pēc plaukstas skenēšanas. Dotajās biometrijas sistēmās tiek izmantota plaukstas ģeometriskā forma (vai dažu pirkstu), un papildus arī zemādas kapilāru un plaukstas līniju atrašanās vietas, pie tam ir iespējamas dažādas metodes.

Identifikācija pēc rokas ģeometrijas pēc savas tehnoloģijas struktūras un drošības līmeņa ir salīdzināma ar daktiloskopijas identifikāciju. Bieži vien šīs metodes tiek lietotas kopā, kaut arī plaukstas nolasīšanas ierīces aizņem vairāk vietas. Lai iegūtu trīsdimensionālu plaukstas attēla kodu, tiek izmantotas speciālas ierīces, vai arī video kameru, uzņem plaukstas iekšpuses un sāna skata attēlus.

Ir divas pieejas kuras izmanto plaukstas formas atpazīšanā. Pirmā (eksistē kopš 1976. gada) ir balstīta uz plaukstas ģeometriskām īpašībām, kuras katram indivīdam ir savādākas. Otrs princips (mūsdienīgs) izmanto izņemot ģeometriskās formas izmanto arī rokas struktūras pazīmes (zīmējumus starp pirkstu falangu locīšanas vietām, asinsvadu zīmējumus)

Dotā metode nepiestāda nekādas prasības pret roku tīrību, mitrumu un temperatūru. Tomēr plaukstas forma diezgan stipri mainās ar laiku un ir iespējamas nesakritības pēc noteikta laika perioda, tādēļ nāksies atjaunot datubāzē esošos etalonus. Pie nopietniem trūkumiem varētu atzīmēt milzīgas skenējošās ierīces (izņemot dažus modeļus), kā arī viegli izgatavojamas roku kopijas priekš pirmā tipa ierīcēm (kas izmanto tikai ģeometrijas pazīmju principu).

3.5. Sejas atpazīšana



Attēls 3.2. - sejas atpazīšanas metožu ilustrācija

Tas ir pats intuitīvi saprotamākais identifikācijas veids, kas ir vistuvākais cilvēkam. Dotajā identifikācijas metodē tiek veidots cilvēka sejas tēls, un tajā tiek izceltas individuālās pazīmes. Daudzums, kvalitāte un nolasīto tēlu dažādība (galvas pagriešanas leņķis, apakšējās sejas daļas izmaiņas, noteiktu vārdu izrunas kustības utt.) var variēties atkarībā no algoritmiem un sistēmas funkcijām, kas realizē tekošo metodi.

Sejas atpazīšanas tehnoloģijas nav uzkrītošas (atpazīšana notiek no vairāku metru attāluma, bez aizturēm un uzmanības pievēršanas), kā likums, pasīvas (nepieprasa nekādas darbības no cilvēka puses), neierobežo cilvēku pārvietošanos un ir pietiekami lētas.

Pēc cilvēka sejas var uzzināt viņa vēsturi, simpātijas un antipātijas, slimības, emocionālo stāvokli, jūtas un nodomus pret apkārtējiem. Visas šīs lietas ir ļoti interesantas priekš automātiskās sejas atpazīšanas sistēmas (piemēram, lai identificētu potenciālos noziedzniekus).

Viss biežāk tiek izmantotas trīs sejas atpazīšanas metodes:

1. Korelācijas (saskaņotas filtrēšanas metode)
2. Metode kas ir balstīta uz Karunena-Lojeva konversijām un „pašu seju" („EigenFace") jēdziena.
3. Metode kas ir balstīta uz lineāras diskriminantanalīzes un „Fisherface" jēdziena

Sejas identifikācijas sistēmas bieži vien tiek lietotas lidostās ejot caur pases kontroles punktiem, pieblīvētās vietās meklējot noziedzniekus, azartspēļu vietās krāpnieku identificēšanai, kā arī pie ieejas svarīgos pasākumos, lai nepieļautu „melnajā sarakstā" esošo personu iekļūšanu.

Identifikācija pēc sejas pazīmēm ir viena biometrijas industrijas ātrākajām attīstības nozarēm, tomēr vairums no izstrādātājiem pagaidām nav sasnieguši pietiekami augstu sistēmas darbības drošību, lai to izmantotu priekš identifikācijas un autentifikācijas.

Šādu metožu priekšrocība pirmkārt ir tas, ka nav nepieciešamas nekādas darbības no lietotāju puses. Pie trūkumiem noteikti jāmin tas, ka šāda tipa sistēmas nespēj atšķirt dvīņus.

3.6. Acs varavīksnes atpazīšana

Šajā gadījumā notiek acs krāsainās riņķa līnijas, kas atrodas apkārt zīlītei, izmēru noteikšana un analīze. Fakts par to, ka neeksistē divi cilvēki ar vienādu acs varavīksnes (pat vairāk – vienam un tam pašam cilvēkam acs zīlītes atšķiras) bija pierādīts vel 1950 gados. Tomēr acs varavīksnes atpazīšanas tehniskā metodes realizācija parādījās salīdzinoši nesen – 1994 gadā. Šīs tehnoloģijas unikalitāte ir tas, ka acs varavīksnē atrodas vairāk informācijas nekā jebkurā citā cilvēka orgānā (266 unikāli punkti, salīdzinot ar 10-60 punktiem citās metodēs). Pie tam ir zināms, kad acs varavīksne pabeidz savu attīstības ciklu jau pirmajos divos gados un paliek praktiski nemainīga līdz pašai nāvei (Acs varavīksne var izmanīties tikai sakarā ar retām slimībām).

Nav nepieciešamības pēc speciāliem apstākļiem, piemēram, lai lietotājs nokoncentrētos uz kādu noteiktu punktu, jo varavīksne atrodas acs virspusē. Redzes problēmas vai acs kristāla bojājums (katarakta) nekādā veidā neietekmē skenēšanas precizitāti. Patentētais kods, kuru pieņemts izmantot visās komerciālās identifikācijas sistēmās garantē kļūdu attiecību 1 pret 1,2 miljonu. Mūsdienu aparatūras risinājumi atļauj identificēt lietotāju pat pie bojātas acs varavīksnes, ja ir pieejama vismaz 1/3 no varavīksnes attēla ar kļūdas varbūtību 1 pret 100 tūkstošiem. Līdzīgu drošību nevar nodrošināt neviena no esošajām biometrijas tehnoloģijām.

Metodes realizācijai ir nepieciešama tikai kamera, kas ļauj iegūt attēlu ar pietiekamu izšķirtspēju un specializēta programmatūra, kas spēj izgūt no attēla acs varavīksnes attēlu, pēc kura tālāk tiek izveidots ciparu kods priekš cilvēka identifikācijas. Faktiski ar mūsdienu kameru palīdzību acs var tikt noskanēta no viena metra attāluma, kas stipri paplašina metodes izmantošanas iespējas.

Dotajā brīdī tiek izmantotas divas pamata pieejas, kuras atšķiras ar attēla apstrādes algoritmu. Pirmajā pieejā acs varavīksne tiek izņemta no acs attēla. Tālāk eksistē divi acs varavīksnes attēlošanas veidi:

- Riņķa līniju veidā, kas attiecas uz acs varavīksnes zonu
- Taisnstūra veidā, kas tiek iegūts pārveidojot Dekarta koordinašu sistēmu uz polāro.

Sākumā tiek noteikts acs zīlītes centrs un divi rādiusi attiecībā pret to – zīlītes rādiuss un acs varavīksnes rādiuss līdz ārējai malai. Pie tam zīlītes un acs varavīksnes robežas nav apaļas. Tās kļūst tādas tikai pēc papildus apstrādes. Pēc kā, tālāk notiek attēla precizitātes palielināšana.

Otrā pieejā par attēlu tiek pieņemta kodu matrica kas atbilst acs varavīksnei. Acs attēls tiek izdalīts no sejas attēla, pēc tam uz acs varavīksnes tiek uzlikta īpaši izveidota kodu maska, kā rezultātā tiek izveidots etalona attēls, kura izmērs ir 512 baiti.

Pie dotās tehnoloģijas priekšrocībām var pieskaitīt augstu atpazīšanas līmeni un zemu kļūdu iespējamību, bez kontakta iespējamo skenēšanu, kā arī iespēju skenēt cilvēkus, kas nēsā brilles un vienaldzību pret vairumu izplatītām acs slimībām. Starp nepilnībām var konstatēt tikai nepieciešamību „pierast" pie sistēmas.

3.7. Acs tīklenes atpazīšana

Acs tīklenes skenēšana notiek izmantojot infrasarkano starojumu, kas tiek virzīta cauri zīlītei pie asins kapilāriem kas atrodas uz aizmugurējās acs sienas. Acs tīklenes attēlam ir jābūt ļoti precīzam, tādēļ katarakta negatīvi ietekmēt personības identifikācijas precizitāti. Lai ieraudzītu acs dobuma kapilārus cilvēkam ir jāskatās uz attālinātu gaismas punktu, un šādā veidā apgaismots acs dobums var tikt noskenēts ar īpaši tam izveidotu kameru.

Acs tīklenes kameras ir ieguvušas lielu izplatību pieejas kontroles sistēmās, kas atrodas īpaši slepenos objektos, jo tiem ir viss zemākais legālo lietotāju atteikumu procents un praktiski nekad nenotiek kļūdaina piekļuves atļauja. Pēc precizitātes tās ir sliktākas tikai par DNS analīzi.

Neskatoties uz līdzību un praktiski vienādu drošību, šī metode nav tāda pati kā acs varavīksnes skenēšana, jo tiek izmantota pavisam cita aparatūra, sensori ar daudz augstākām prasībām pret saņemamo attēlu.

Galvenā problēma, kādēļ šī metode nav tik izplatīta ir diezgan augsta aparatūras cena un lietošanā radītās neērtības (ir nepieciešams noņemt brilles, pielikt aci pie okulāra un uz nelielu brīdi izjust nepatīkamas sajūtas, kuras rada fokusēts infrasarkanais starojums), kā arī neiespējamība lietot šo tehnoloģiju lietotājiem, kam ir dažādas acs ābola slimības.

3.8. Rokraksta atpazīšana (pēc paraksta)

Parasti priekš šīs metodes tiek izmantots kāds slepenais vārds vai cilvēka parakts. Ciparu identifikācijas kods tiek veidots pēc cilvēka rokraksta dinamiskajiem rādītājiem (ātrums,

spiediens, kustību asums) un pēc grafiskajiem paraksta rādītājiem, atkarībā no nolasīšanas ierīces iespējām.

Priekš paraksta identifikācijas var tikt izmantotas speciāli izveidotas pildspalvas, kas ir jūtīgas pret virsmas spiedienu, vai arī to kombinācijas. Ierīces ar īpaši izgatavotām pildspalvām ir daudz lētākas un aizņem mazāk vietas, bet tajā pašā laikā to darbības laiks ir daudz zemāka.

3.9. Balss atpazīšana

Balss ir pilnīgi unikāla katram cilvēkam un tiek veidota pēc fizioloģiskiem un psiholoģiskiem uzvedības faktoriem. Eksistē diezgan daudz metodes kā izveidot balss identifikācijas kodu, kā likums, tās pārsvarā ir dažādu frekvenču biežums un citas statiskas balss pazīmes.

Biometriskā pieeja, kas ir saistīta ar balss identifikāciju, ir viena no vecākajām tehnoloģijām, un tajā pašā laikā ir ļoti ērti pielietojama. Bet galvenais šīs metodes trūkums ir zema identifikācijas precizitāte, dēļ daudzu neatkarīgu ārējo faktoru (piemēram kakla slimības). Bet kaut arī identifikācija pēc balss nav tik pat droša, kā pārējās aprakstītās biometriskās metodes, šī problēma kļūst arvien mazāk nopietna, jo pēdējā laikā parādās ar vien vairāk ierīču, kas spēj atpazīt un identificēt papildus jaunas cilvēka balss un izrunas pazīmes [8] .

3.10. DNS atpazīšana

Teorētiski dotā metode atļauj viennozīmīgi identificēt lietotāju. Šādas tehnoloģijas priekšrocības ir acīmredzamas, tomēr mūsdienās izmantojamās metodes priekš DNS iegūšanas un apstrādes ir tik ilgi, ka šādas sistēmas tiek izmantotas tikai īpašām ekspertīzēm. Pie tam izmaksas kuras ir nepieciešamas lai veiktu dotā veida atpazīšanas procedūru arī neveicina šīs metodes plašu izplatību.

3.11. Biometrijas atpazīšanas tehnoloģiju salīdzināšana

Statiskā un dinamiskā biometrija ir divas savstarpēji papildinošas nozares. Galvenā statiskās biometrijas priekšrocība ir salīdzinošā neatkarība no lietotāju psiholoģiskā stāvokļa, zemas piepūles izmaksas un līdz ar to arī spēja organizēt lielu cilvēku plūsmu biometrisko

identifikāciju. Toties dinamisko metožu priekšrocības ir to vieglā realizācija un izmantošana, kā arī zemās naudas izmaksas to realizācijai.

Lai izmantotu biometrijas īpašības autentifikācijas sistēmās, tām ir jābūt unikālām, pastāvīgām, un izmērāmām, pie tam tām ir jābūt grūti viltojamām.

- Unikalitāte – nozīmē, ka nedrīkst būt divu cilvēku ar identiskām pazīmēm.
- Pastāvīgums – pazīme nedrīkst manīties ar laiku.
- Izmērāmība – iespēja ātri un viegli iegūt detalizētu pazīmi no indivīda.

Tabula 3.1. – Cilvēku biometrijas pazīmju novērtējums

Pazīme	Unikalitāte	Pastāvīgums	Izmērāmība	Noturība pret viltošanu
Rokraksts	+	+	+++++	+
Rakstīšanas dinamika	+++	+	+++++	+++
Klaviatūras rokraksts	++	+	+++++	++
Balss	+++	++	++++	+
Pirksta nospiedums	++++	+++++	+++	+++
Plaukstas forma	+++	+++	++++	+
Acs tīklene	+++++	++++	++	++++
Acs varavīksne	+++++	+++++	++++	++++
Sejas forma	+++	+++	++++++	+
Sejas termogramma	++++	++++	++++	++++
DNS	+++++	+++++	+	+++++

Kā var redzēt pēc ekspertu viedokļa veiktās biometrijas pazīmju novērtēšanas, ne viena no pazīmēm neapmierina visas prasības pilnā mērā [8].

3.12. Svarīgākie parametri

Kā jau mēs zinām, paroles autentifikācijas sistēmās vienmēr norādot korektu paroli tiks apstiprināta identitāte un veikta autentifikācija. Bet ja biometriskā sistēmā ir iesniegti legāli biometriskie rādītāji, tas vel negarantē, kad notiks korekta autentifikācija. Pirmkārt tas ir saistīts ar neiespējamību iegūt pilnīgi identisku ciparu attēlu pie katras biometriskās īpašības nolasīšanas. Tā iemesls ir „trokšņi", dažāda slīpuma leņķi cilvēka ķermeņa daļām veicot skenēšanu. Otrkārt ir biometrisko īpašību izmaiņas iespējas, jo lielākā daļa no biometrijas īpašībām var mainīties dēļ emocionālā vai fiziskā personības stāvokļa. Nogurums, kairinājums, alkohola reibuma stāvoklis un tamlīdzīgi. Tas viss var ļoti stipri ietekmēt cilvēka biometriskos rādītājus. Statisko pazīmju gadījumā tās ir daudz noturīgākas pret izmaiņām, bet

arī tās var mainīties ar laiku, cilvēkam novecojot, vai apdedzinot pirkstu, kas novedīs pie papillāru līniju bojājumiem, plaukstas ievainojums arī var uz laiku izmainīt tās formas, dažas no acs slimībām var liegt saņemt legālu biometrisko attēlu.

Kā arī ir iespēja, kad nelegāla lietotāja identitāte var tikt apstiprināta izmantojot legālā lietotāja datus. Tas ir saistīts ar to, ka dažādu cilvēku biometrijas dati tomēr var būt ļoti līdzīgi, piemēram dvīņiem ir apbrīnojami līdzīgas biometrijas pazīmes.

Tādēļ papildus pie visiem iepriekš minētajiem biometrijas tehnoloģiju aprakstīšanas parametriem lieto arī citus:

- FAR (*False accept rate*) – cik daudz procentu gadījumu tiek atzīti par vienādiem
- FRR (*false reject rate*) – cik daudz procentu gadījumu tiek atzīti par dažādiem
- FER (*failure to enroll*) – cik daudz procentu paraugu nav iespējams iegūt pietiekamā kvalitātē
- FTC (*failure to capture*) – šīs parametrs pārsvarā tiek lietots automātiskajās sistēmās un norāda cik daudz procentu gadījumu sistēmai nesanāk nolasīt korektu paraugu.

Bieži vien ir svarīgi noanalizēt FAR un FRR attiecību dažādos darbības apstākļos. Kvalitātes parametrus norāda arī algoritmu iestatījumi un ārējie apstākļi. Plašākā risinājuma kontekstā būtu jāvērtē arī sistēmas vispārējā drošība, tāda kā datu pārsūtīšana, glabāšana utt., kā arī iekārtu specifikācija. Piemēram tālajā 2002 gadā veiktais gumijas pirksta eksperiments[8] , kuru nesen arī atkārtoja kādi Krievijas zinātnes universitātes studenti, pierāda, ka joprojām daļu no mūsdienu lētajiem pirkstu nospiedumu lasītājiem var apmānīt ar lētu gumijas pirksta nospieduma kopiju. Tajā testā tika pārbaudīti vairāk nekā 10 komerciāli pirkstu nospiedumu lasītāji, un mājas apstākļos izgatavotu mākslīgu pirkstu visas ierīces atzina par derīgu un atrada sakritību ar parauga etalonu 67-100% pārbaudes mēģinājumos. Tas nozīmē tikai to, kad paļauties uz to, kad FAR parametrs ir tikai 1%, nekādā gadījumā nedrīkst. Protams ir jautājums par to, vai patērētais laiks un resursi ir adekvāti iegūtajam, nevis par kādiem principiāliem ierobežojumiem.

Vairumam biometrijas autentifikācijas sistēmām ir iespēja samazināt vienas kļūdas gadījumus uz otras kļūdas rēķina – tā saucamā sistēmas „jūtība". Pilnībā tikt vaļa no viena tipa kļūdas var tikai uzstādot otras kļūdas varbūtību uz 100%, kas saprotami ir nepieņemami.

3.13. Standarti

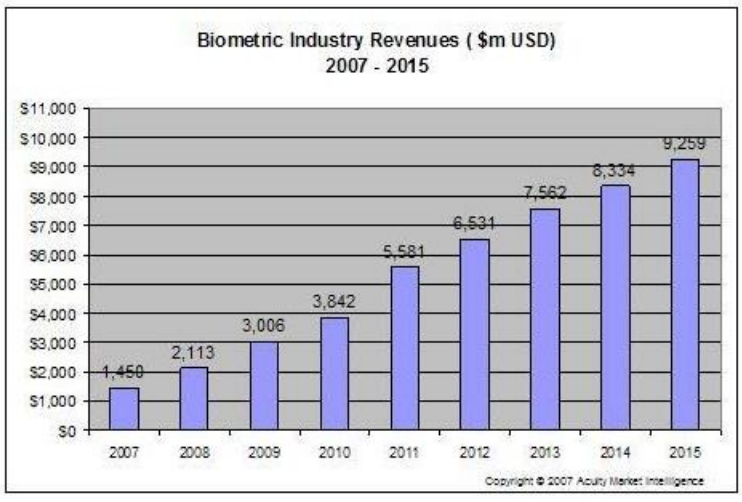
Biometrijas standartizācijas jomas iesācēji bija un joprojām ir ASV, līderpozīcijas aizņem ANSI/NIST standarti [9]. Šie standarti aptver vairākas jomas, sākot ar sistēmu API prasībām

un datu apmaiņas formātiem līdz pat vis dažādākām tehniskajām un testēšanas prasībām. Lielākoties ietverot ANSI standarta saturu, kopš 1990. gadu vidus ir pieejami arī ISO standarti, kas sagrupēti četrās kategorijās: 1) tehniskās saskarnes (ISO/IEC 19784 un ISO/IEC 19785), 2) datu apmaiņa (ISO/IEC 19794), 3) kvalitāte jeb efektivitāte (ISO/IEC 19795) un 4) atbilstības pārbaudes (ISO/IEC 24709).

3.14. Tirgus izpēte

Līdzīgi kā tas notiek citās nozarēs, lai izpētītu pasaules biometrijas tirgus tehnoloģijas ir nepieciešams veikt veselu analītisko un statistisko metožu kompleksu, veikt patērētāju un ražotāju aptaujas un tamlīdzīgas lietas. Bet eksistē organizācijas kas specializējas uz zinātniski-tehnisko organizāciju analīzes un izpētes, kas seko līdzi tirgus attīstībai un novērtē tā izaugsmi. Izmantosim datus, kurus mums piedāvā dažas no šādām organizācijām, lai veiktu savu analīzi mūsdienu biometrijas identifikācijas tirgū. Bet vajadzētu ņemt vērā, kad dažādos avotos dati var manīties uz līdz pat 15-20%, tādēļ šī analīze būs tikai kā uzskates novērtēšana.

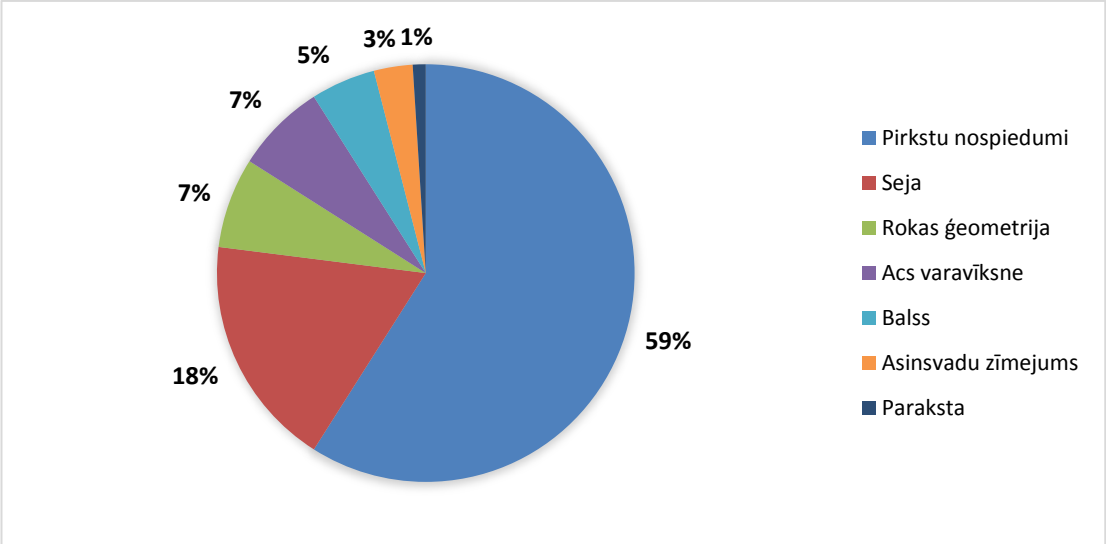
3.14.1. Mūsdienu attīstība un tekošais stāvoklis



Attēls 3.3. - Biometrijas tehnoloģiju tirgus daļa (miljoni dolāru) [10]

Pašos pirmsākumos biometrijas tehnoloģijas bija nesamērīgi dārgas un nepieejamas parastiem lietotājiem un pārsvarā tos izmantoja slepenajos objektos, armijās spēkos un tamlīdzīgas vietās. Bet kā jau redzams Attēlā nr. 6. ar katru gadu tirgus daļa biometrijas tehnoloģijām aug un līdz ar to parādās diezgan nedārgas un pieejamas tehnoloģijas kuras jau tagad veiksmīgi lieto ikdienā vairākās organizācijās, lai nodrošinātu drošu personu

identifikāciju un piekļuvi pie aizsargātiem datiem un objektiem. Daļu no šī tirgus aizņem ne tikai aizsardzības tehnoloģijas, bet arī atsekošanas, jeb monitoringa tehnoloģijas, kas piemēram ļauj kontrolēt darbinieku darba laika uzskaiti.



Attēls 3.4. - Biometriskās drošības sistēmu tirgus daļas [10]

Kā jau mēs redzam, lielāko tirgus daļu aizņem daktiloskopiskās sistēmas (pirkstu nospiedumi). 2011 gadā uz šo segmenta daļu attiecās summa 5 miljardu dolāru apmērā un uz 2015 gadu tā sastāda divtik daudz – 10 miljardi dolāru.

Pie tam pēc GIA novērtējumiem kopējais pārdošanas apjoms visām pārējām identifikācijas sistēmām kā sejas, acs varavīksnes un vēnu zīmējuma ir aptuveni 2 miljardi dolāru.

Kā lielāko šī segmenta lietotāja daļu GIA atzīmēja bija un joprojām ir ASV. Kas savukārt attiecas uz biometrijas tehnoloģijas attīstības līmeni – šajā pozīcijā līderis ir Āzija klusā okeāna reģions, kur ik gadu šajā jomas attīstībā tiek ieguldīts ap 500 miljoniem dolāru un ar katru gadu šis cipars paliek ar vien lielāks. Šāda biometrijas autentifikācijas tehnoloģijas attīstība šajā reģionā ir tik augsta dēļ tā, ka tiek ievestas nacionālās identifikācijas infrastruktūras sistēma un robežkontroles sistēma. Kā arī ir sākusies identifikācijas karšu sistēmas izveide, kas satur biometriskos identitātes parametrus.

3.14.2. Populārākie ražotāji

- Pirkstu nospiedumu nolasīšanas aparatūra – neskatoties uz to, kad eksistē liels vairums kompāniju, kas ražo pirkstu nospieduma nolasīšanas tehnoloģijas, lielāko tirgus daļu, aptuveni 80% aizņem viena kompānija – Identix (*http://www.identix.com*)

- Sejas atpazīšanas aparatūra – Kā piemēru var minēt diezgan izplatītu sistēmu ASV, kas darbojas vairākos štatos pie bankas aparātu vietām – Mr. Payroll. Kā arī vairākas lidostās un dažas Anglijas pilsētās strādājošā sistēma Facelt. Kā arī diezgan lielu daļu no tirgus aizņem Āzijā izstrādātās sistēmas – AcSys Biometric, A4Vision.
- Atpazīšana pēc plaukstas – vel 10 gadus atpakaļ šī metode bija diezgan izplatīta un bija cerība uz tās attīstību nākotnē, bet pēdējos gados tās tirgus daļa samazinās. Iespējams tās apvienos kopā ar citām metodēm, piemēram pirkstu nospiedumiem. Lielākie ražotāji – BioMet Partners, Recognition Systems, Palmetrics un BTG.
- Acs varavīksnes autentifikācija – šī metode skaitās ne tikai pati drošākā, bet arī pati dārgākā. Pie tam šīs metodes tehnoloģijas izplatība ir strikti noteikta ar ASV patentu no uzņēmuma Iridian. Līdz ar to var saprast kādēļ pasaulē ir ļoti neliels piedāvāto iekārtu klāsts. Šo metodi pārsvarā lieto valsts organizācijās, cietumos, kodolieroču ražošanas vietās. Lielākais aparatūras ražotājs dotajā brīdī ir kompānija Iridian, uz kuru risinājumiem arī ir bāzētas visas pārējās izstrādes. Izņemot šo kompāniju ar izstrādi nodarbojas vel vairāk kā 20 kompānijas tai skaitā British Telecom, Sensar, Saflink, LG, Panasonic, Oki.
- Balss atpazīšanas iekārtas – tā ir viena no vecākajām biometrijas tehnoloģijām. Pēdējā laikā tā ir sākusi strauji attīstīties, jo tiek plānots izmantot balss kontroli privātmājās un sadzīves tehnikas kontrolei. Bet pagaidām, dēļ sliktas kvalitātes, tiek lietota tikai eksperimentālās laboratorijās un mobilajās ierīcēs.

3.15. Nākotnes problēmas un to risinājumi

Biometrijas autentifikācijas metodes ir ļoti ērtas, tomēr tās atrodas ilgās attīstības ceļa sākumā, un eksistē vesela rinda ar problēmām, kas ir saistītas ar salīdzinošu šīs tehnoloģijas jaunumu.

- Pirkstu nospiedumu metodei ir iespējamas šādas ievainojamības:
  1. Pirksta kopijas izveidošana no lateksa un želatīna. Šāda kopija var nostrādāt uz lētajiem skeneriem.

     Risinājums: uzstādīt vairāku faktoru autentifikācijas sistēmu, kas fiksēs ne tikai pirkstu nospiedumu, bet arī temperatūru un svīšanu.
  2. Signāla pārķeršana izmantojot skenerus ar vadu interfeisu
  3. Risinājums: izmantot kriptogrāfijas metodes jau pie datu pārsūtīšanas no skenera.
  4. Kondensācija (silta gaisa plūsmas raidīšana uz skeneri, kā rezultātā tiek atgūts pēdējais pirkstu nospiedums).

Risinājums: šī problēma ir saglabājusies tikai uz lētajiem optiskajiem skeneriem, uz pusvadītājiem šī metode vairs nestrādā.

5. Pie tam eksistē vel arī problēma ar bojātu pirkstu nolasīšanu, kuru var apiet ar vairāku pirkstu nospiedumu nolasīšanu.

- Sejas autentifikācijas sistēmas problēmas:

1. Izmaiņas apgaismojumā, mīmikā, apmatojumā, kosmētikas daudzumā un citas lietas kas kavē atpazīšanu.

   Risinājums: Dārgākās sistēmās tiek papildus izmantota arī infrasarkanā diapazona skenēšanas iespēja (sejas termogrāfija). Tādā veidā kvalitāte ir tīri proporcionāli atkarīga no cenas.

2. Sistēmas apmuļķošana ar reģistrētas personas sejas fotogrāfijas izmantošanu, vai arī dažādu tipu seju fotogrāfiju izmēģināšana arī var nostrādāt uz vairāku portatīvo datoru sejas atpazīšanas iekārtām.

   Risinājums: izmantot 3D-atpazīšanu (kas nav lēti).

3. Sistēma nevar atpazīt dvīņus.

   Risinājums: Izmantot vairāku faktoru autentifikācijas sistēmu – sejas ģeometrija un pirksta nospiedums/rokraksts/balss/parole.

- Autentifikācija pēc cilvēka acs varavīksnes:

Pamata sistēmas apejas variants ir acs varavīksnes mulāžu izgatavošana un novietošana sensora priekša.

Risinājumi var būt dažādi: var reģistrēt acs patvaļīgās kustības – metode ir efektīva, bet ir iespējamas problēmas ar dažu cilvēku fizioloģiskām īpašībām. Dažiem šādu kustību nav un ir iespējama sistēmas atteikšana. Acs atstarošanas spektra analīze – tā ir balstīta uz dzīvas acs un mulāžas mitruma noteikšanas, bet šādu sistēmu ir diezgan viegli apiet ieeļļojot vai izmērcējot mulāžu želatīnā. Vel kā labs variants ir gaismas stara novirzīšana uz acs zīlīti, jo īsta acs zīlīte sašaurināsies, bet mulāža to izdarīt nevarēs, tomēr šāda metode rada diskomfortu lietotājam un aizņem vairāk laika.

Vairumam sistēmu pārskaitītās metodes būs pietiekami drošas, bet ir viena lieta. Ir zināms, kad cilvēki ar lēcām veiksmīgi iziet šo autentifikācijas procesu. Tas nozīmē, kad ir iespējams izgatavot lēcas ar legālā lietotāja acs varavīksnes zīmējumu.

- Autentifikācija pēc balss. Pamata problēmas šim autentifikācijas veidam:

1. Balss izmaiņas (emocijas, veselības stāvoklis)
2. Traucējumi mikrofonā vai sakaru līnijās
3. Konfidenciālas informācijas pārķeršana no ļaundaru puses.

Risinājums: izmantojot laringofonu (līdzīgs mikrofonam, tikai izmanto balss vibrācijas kas rodas kakla reģionā) var iedot pilnīgi individuālu skaņas signālu katram cilvēkam, kuru būtu grūti diskreditēt.

Neskatoties uz visiem pārskaitītajiem trūkumiem un problēmām, biometrijas iekārtas skaitās ļoti perspektīvs attīstības virziens priekš pieejas kontroles un autentifikācijas sistēmām, jo tās stipri atvieglo procesu un ļauj ļoti viegli izpildīt grūtus uzdevumus.

3.16. Secinājumi

Eksistē arī daudzi citi, mazāk pazīstami novirzieni biometrijas jomā, tādi kurus vairs nelieto, un tādi kas ir perspektīvā attīstīties spējīgi, bet šobrīd vel ir uzskatāmi kā eksotiski. Piemēram, atpazīšana pēc sirds darbības ritma, sejas termogrammas, smakas un daudzi citi. Daudzas no šīm tehnoloģijām atrodas pagaidām tikai izpētes stadijā un dotajā brīdī to daudzums nav spējīgs ietekmēt biometrijas attīstību.

Katram no parametriem ir savas priekšrocības un trūkumi skatoties no identifikācijas tehnoloģijas viedokļa puses. Pēdējā laikā notiek aktīva personības identifikācijas izstrāde, uzlabošana kā arī modificēšana, tiek meklētas jaunas pieejas un cilvēka individualitātes pazīmes, kā arī fizioloģisko un uzvedības faktoru kombinācijas, kas turpmāk varētu palīdzēt attīstīt biometrijas nozari.

Bet jebkurā gadījumā, vairums no prognozēm nonāk pie secinājuma, kad nākotnē biometriskās sistēmas tiks integrētas it visur. Meklējumos pret cīņu ar terorismu, jebkurā gadījuma novedīs pie šīs jomas attīstības. Kā arī vel viens no faktoriem kādēļ biometriskā identifikācijas tehnoloģija strauji attīstīsies tuvākajā laikā ir tas, ka jau tagad dažas valstis uzsāk centralizētu biometrisko identifikācijas karšu projektu izstrādi un ieviešanu dzīvē. Eiropa plāno tuvāko gadu laikā izveidot biometriskās vīzas lai kontrolētu migrācijas plūsmas. ASV jau kopš 2005 gada ir noslēguši bez vīzu režīmu ar 27 valstīm, kura ietvaros šo valstu pilsoni drīkst uz 90 dienu laiku, bez vīzas iebraukt ASV, ja viņiem ir biometriskie dokumenti.

4. PRAKTISKĀ DAĻA

4.1. Ievads

Šis darbs tika izveidots ar tādu domu, lai balstoties uz teorētisko materiālu, kuri tika iznalizēti šī darba ietvaros, varētu izveidot reālu autentifikācijas sistēmu, kas darbosies reālā uzņēmumā. Es tiku nozīmēts kā atbildīgā persona par mūsdienīgas autentifikācijas sistēmas izveidi uzņēmuma kurā strādāju, līdz ar to bija nolemts pieiet pie šīs prasības ļoti nopietni un pie reizes arī padalīties ar pieredzi šādas sistēmas izveidē savā bakalaura darbā. Pateicoties šajā darbā veiktajam pētījumam man veiksmīgi izdevās realizēt biometriskās identifikācijas sistēmas ieviešanu vienā no Latvijas lielākajiem programmatūras izstrādes un tehnoloģijas attīstības uzņēmumiem.

4.2. Sistēmas prasības

Uzņēmumam bija nepieciešama vienota autentifikācijas sistēma, kura nodrošinātu nepieciešamo funkcionalitāti:

- Personāla darba laika uzskaiti un integrāciju ar esošo laika uzskaites sistēmu (CRM)
- Piekļuves tiesību izveidošanu pie noteiktām telpām, datoriem un informācijas
- Centralizēta tiešsaistes programmatūra, kas dod iespēju no jebkuras vietas apskatīt visu nepieciešamo informāciju kas ir pieejam sistēmā.
- Plašu atskaišu sistēmu

Ņemot vērā to, ka uzņēmums darbojas tehnoloģijas attīstības jomā, bija vēlēšanas izmantot jaunākos izgudrojumus autentifikācijas jomā, tādēļ bija nolemts pielietot biometrijas identifikācijas metodes, jo šobrīd šī ir viena no aktuālākajām tendencēm autentifikācijas jomā un tas ne tikai ir ērti – nav vajadzīgas nekādas viedkartes, taloni, paroles, bet tas izskatīsies arī ļoti mūsdienīgi un prestiži, kā arī nevar aizmirst par pašu galveno lietu, drošības līmeni – biometrijas tehnoloģijas ir ieguvušas savu plašo atzinumu pateicoties acīmredzamam efektam, kas tika sasniegts, jo šīs sistēmas vairāku gadu garumā izmantoja valstu drošības struktūras.

4.3. Sistēmas izvēle

Izpētot Latvijā pieejamo biometrijas ierīču un programmatūras tirgus daļu, tika nolemts izmantot populārāko pasaulē pirkstu nospiedumu lasītājus no Identix uzņēmuma. Identix piedāvā tādus biometrijas risinājumus kā biometriskā personu atpazīšana, objektu atpazīšana attēlos un video, biometriskā piekļuves kontrole, biometrijas datu sistēma, biometrijas datu ieguves programma.

Pēc piedāvāto produktu izpētes tika iegādāti četri Identix K21 pirkstu nospiedumu lasītāji, kas darbojas caur bezvadu interneta pieslēgumu un ir viegli integrējams ar jebkuru programmatūru un 5 zemāka līmeņa pirksta nospiedumu lasītāji Ekey F60.

Attēls 4.1. - Identix K21 un Ekey F60 pirkstu nospiedumu lasītāji

Abu iekārtu ražotāju solītie parametri izskatās ļoti apmierinoši:

- FAR: <= 0,0001%
- FRR: <= 1%
- Identifikācijas ātrums: mazāk par 1 sekundi

4.4. Sistēmas izveide

4.4.1. Sistēmas specifikācija

Kad aparatūra bija uzstādīta un nokonfigurēta sākās programmatūras izstrādes process. Lai izpildītu uzņēmuma prasības bija nepieciešamas izveidot programmatūru, kas būs spējīga darboties ar jau esošo aparatūru un atbilst visām uzņēmuma prasībām.

Tika izdalīta nepieciešamā sistēmas funkcionalitāte:

- Izveidot drošu aizsardzības līmeni visai datu sistēmai
- Veikt lietotāju darba laika uzskaiti
- Integrēt laika uzskaiti ar grāmatvedības programmatūru
- Kontrolēt lietotāju piekļuves tiesības pie uzņēmuma telpām
- Kontrolēt lietotāju piekļuves tiesības pie uzņēmuma serverī esošajiem dokumentiem un lokācijām
- Izveidot tiešsaistes portālu, kurā būs pieejama visa statistika par lietotāju autentificēšanos sistēmā un darba laikiem, ar iespēju rediģēt sistēmas uzstādījumus un tiesības.

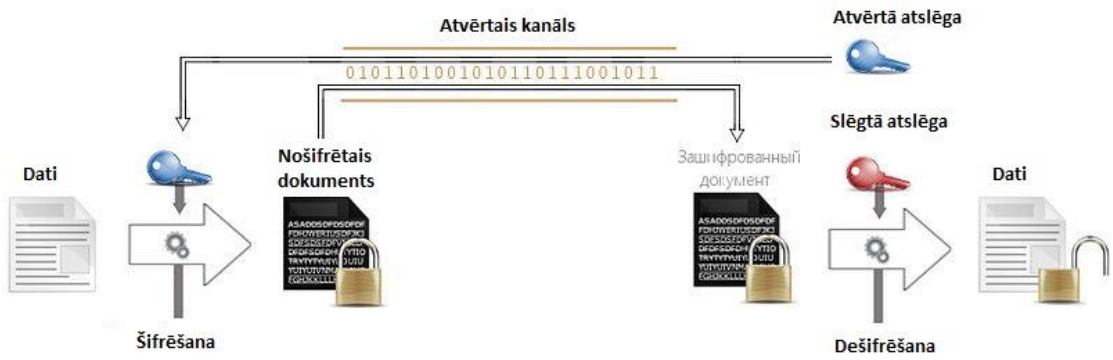
Ņemot vērā, ka šajā darbā tiek aprakstītas autentifikācijas sistēmas un to algoritmi, zemāk tiks aprakstītas izveidotās sistēmas sadaļas, kas atbilst tekošajam tematam.

4.4.2. Datu aizsardzības līmenis

Lai nodrošinātu sistēmā esošo datu drošību, tika nolemts izveidot atsevišķu datu aizsardzības līmeni, kurš tiks izmantots visas informācijas šifrēšanai. Datu šifrēšana ir nepieciešama trīs informācijas drošības parametrus:

- Konfidencialitāti – šifrēšana tiek izmantota, lai paslēptu informāciju no neautorizētām personām veicot datu pārsūtīšanu vai glabāšanu.
- Integritāti – šifrēšana tiek izmantota, lai to nebūtu iespējams izmainīt pie datu nosūtīšanas un glabāšanas
- Identificējamību – šifrēšana tiek izmantota priekš informācijas avota autentifikācijas un pierādīšanas, kad dati nāca tieši no šī avota.

Lai nolasītu nošifrēto informāciju, saņēmēja pusei ir nepieciešama atslēga un dekodētājs (ierīce kas realizē atšifrēšanas algoritmu pēc padotās atslēgas). Šifrēšanas ideja ir ļoti vienkārša – ja ļaundaris pārķer šifrēto informāciju, vai arī kādā citā veidā iegūst piekļuvi pie tās, bez dešifrēšanas atslēgas viņš nevarēs nolasīt informāciju, ne arī izmanīt. Pie tam, bija nolemts izmantot mūsdienīgu kriptogrāfijas sistēmu ar atvērto atslēgu – tas nozīmē, kad datu šifrēšanai un dešifrēšanai var būt izmantotas pilnīgi dažādas atslēgas.



Attēls 5 - Asinhronā šifrēšana

Pie algoritma realizācijas tika pielietota uzlabotā metode, kuru sauc par Difi-Helmana protokolu [18]:

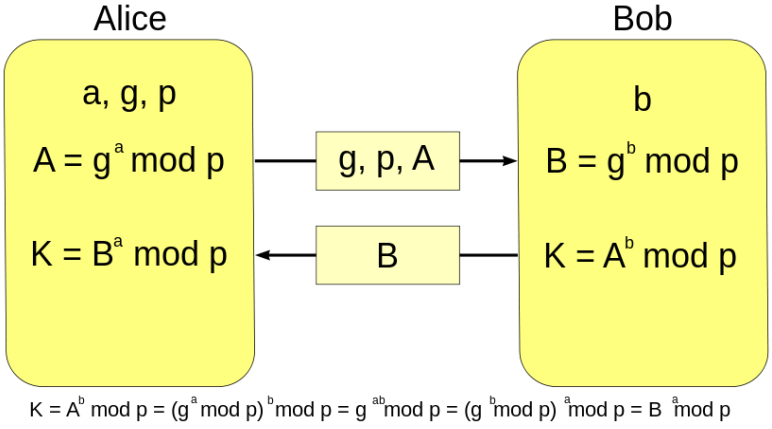
1. Izveido gadījuma naturālo skaitli a – aizvērto atslēgu
2. Kopā ar attālināto pusi tiek uzstādīti atvērtie parametri p un g
    a. p ir parasts gadījuma skaitlis
    b. g ir sakne pēc moduļa no p
3. Tiek aprēķināta atvērtā atslēga A, izmantojot atvērtās atslēgas izmaiņas pēc pārveidošanas, kur $A = g^a \bmod p$
4. Notiek atvērtās atslēgas apmaiņa starp abām pusēm
5. Tiek aprēķināta kopējā slēptā atslēga K, izmantojot atvērto atslēgu no attālinātās puses B un sava slēgtā atslēga a.

   $K = B^a \bmod p$

   K iznāk vienāds abām pusēm, jo:

   $B^a \bmod p = (g^b \bmod p)^a \bmod p = g^{ab} \bmod p = (g^a \bmod p)^b \bmod p = A^b \bmod p$

a un b vietā, praktiskajā realizācijā tika izmantoto skaitļi 10^{100} un p lielums 10^{300}. Bet skaitlim g nav obligāti jābūt lielam un parasti tā vērtība svārstās pirmajā desmitniekā.



Attēls 4.3.6 - Difi-Helmana protokols

Paša algoritma realizācija ir pieejam *pielikumā nr. 1*.

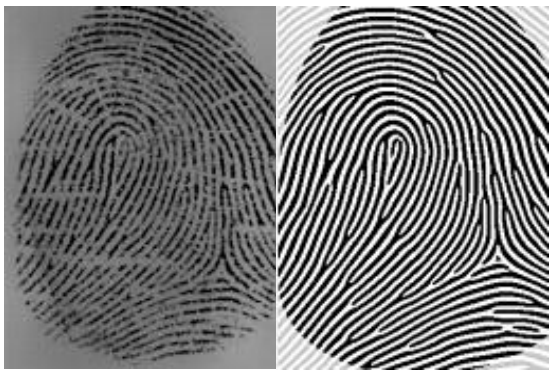
4.4.3. Pirkstu nospieduma attēla apstrāde

Autentifikācijas sistēmas pamatā, kā jau mēs noskaidrojām iepriekš, tiek lietoti Identix un Ekey ražojuma pirkstu nospiedumu skeneri. Pēc dziļākas šo skeneru izpētes, tika noskaidrots, kad iegūtie pirkstu nospiedumi no Ekey skeneriem, ir daudz sliktākas kvalitātes līmenis, salīdzinoši ar Identix ražojumu. Tas savukārt palēnina sistēmas darbību un arī var radīt drošības problēmas nākotnē.

Veicot pētījumu un sazinoties ar Ekey ražotājiem, tika noskaidrots, kad pēc skenēšanas, Ekey aparatūras izveidotie attēli tiek apstrādāti ar telpiskas filtrēšanas metodi. Metode balstās uz gaismas atstarošanas un absorbēšanas procesu fiziskās realizācijas. Rezultātā tiek iegūts attēlā numur 16 redzamais uzlabojums.

Attēls 4.5. - Pirkstu nospiedumu apstrāde Ekey skenerim

Atšķirība neapstrīdami ir diezgan liela – papillāru zīmējums noteikti ir kļuvis daudz izteiktāks un labāk saskatāms, līdz ar to arī vieglāk atrast identificējošās pazīmes un izveidot bināro kodu kurš turpmāk tiks salīdzināts. Bet salīdzinot to ar attēlu, kas tika iegūts no Identix ražotā skenera, var saprast, kādēļ ir tik milzīga cenas starpība.



Attēls 4.6.7 - Pirkstu nospiedumu apstrāde Identix skenerim

Tādēļ bija uzsākta daudz veiksmīgāku filtru meklēšana, nekā Ekey skeneri izmantotā telpiskā filtrēšanas metode. Veicot vairāku filtru izpēti, atradu informāciju par Gabora filtru, kurš ir domāts lai atpazītu objektu robežas – mūsu gadījumā objekti ir pirkstu nospiedumu

celiņi. Pēc vairāku pielietojumu un piemēru aplūkošanas bija nolemts veikt mēģinājumu papildināt esošo skenera nolasīšanas sistēmu ar Gabora filtra pielietojumu pie nolasītajiem pirkstu nospiedumiem.

4.4.3.1. Realizācijas valodas izvēle

Realizācijas valodas izvēle tika veikta balstoties uz tā, lai būtu viegli strādāt ar matricām, kuras izmanot Gabora filtra algoritms, kā arī lai būtu gatavas bibliotēkas priekš darba ar attēliem. Ņemot vērā iepriekš minētās prasības bija izvēlēta valoda Mathlab. Šī valoda atļauj izpildīt lielu vairumu dažādu operāciju ar matricas tipa datiem, kā arī satur sevī jaudīgu iebūvēto attēlu apstrādes bibliotēku.

4.4.3.2. Virzienu noteikšana

Lai izveidotu kvalitatīvu pirksta nospieduma attēlu mēs realizēsim algoritmu, kurš noteiks pirksta nospiedumu papillāru zīmējuma kustības virzienu.

Virzienveidīgais attēls tiek viedots pēc sākuma attēla gradienta. Gradients tiek atrasts pēc Sobela operatora pielietošanas. Sobela operators – tas ir diskrēti differenciāls operators, kas aprēķina aptuvenu attēla gradienta spilgtumu. Gradienta attēla aprēķināšana notiek pielietojot divdimensionālas operācijas starp attēlu un Sobela operatoru [14].

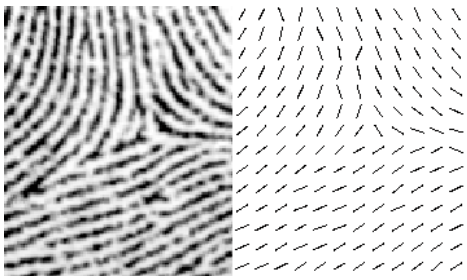
$$G_y = \begin{bmatrix} -1 & -2 & -1 \\ 0 & 0 & 0 \\ +1 & +2 & +1 \end{bmatrix} * A, \quad G_x = \begin{bmatrix} -1 & 0 & -1 \\ -2 & 0 & +2 \\ -1 & 0 & +1 \end{bmatrix} * A ,$$

Kur A – sākuma attēls, G_x un G_y - attēls, kur katrs punkts satur pietuvinātus x un y atvasinājumus. Leņķis, kas norāda gradienta virzienu tiek rēķināts pēc formulas:

$$\alpha = \arctan \frac{G_y}{G_x}$$

Šo formulu realizācijas kods ir pieejams *pielikumā numur 2*.

Attēls 4.7. - Pirksta nospiedums pēc apstrādes ar virzienu veida metodi



Attēls 4.8. - Pirksta nospiedums pēc apstrādes ar virziena veida metodei - pietuvināts

4.4.3.3. Attēla pārveidošana binārajā kodā

Pēc virzienu aprēķināšanas mums ir nepieciešams pārvērst iegūto attēlu binārajā kodā. Binārais kods – tas ir attēls, kur katrs pikselis ir vai nu bedrītes pikselis, vai pikselis kas apraksta izcēlumu. Lai izveidot bināru attēlu, iepriekš normalizētajam attēlam tiek pielietota sliekšņa apstrāde (*treshholding*) – katram attēla pikselim tiek piešķirta nulles (izcēluma) vērtība, ja tā ir zemāka par sliekšņa vērtību, vai vienīnieks (bedrītes) pretējā gadījumā.

$$R(i,j) = \begin{cases} 1, \textit{если } G(i,j) > R_0 \\ 0, \textit{иначе} \end{cases},$$

kur $G(i,j)$ - maskēšanas slieksnis, bet R_0 - pikseļa intensitāte [15].

Attēls 4.9. - Normalizētais attēls pa kreisi un tā binārais attēlojums pa labi

4.4.3.4. Gabora filtra pielietošana

Pēdējais attēla apstrādes posms ir Gabora filtra pielietošana. Kura pirmais solis ir Gabora filtra ģenerācija un parametru atlase.

Zemāk tiek attēlots funkcijas kods, kura realizē Gabora filtra ģenerāciju pēc uzdotā leņķa theta [16].

```
function gb=gabor_fn (theta)
    bw = 2;
    gamma = 1;
    psi = 1;
    lambda = 6;
    theta = (theta+90) *pi/180;
    sigma = lambda/pi*sqrt (log (2) /2) * (2^bw+1) / (2^bw-1);
    sigma_x = sigma;
    sigma_y = sigma/gamma;
    sz = 9;
    if mod (sz,2) ==0, sz=sz+1; end
    [x y] =meshgrid (-fix (sz/2): fix (sz/2),fix (sz/2): - 1: fix (-
sz/2));
    x_theta=x*cos (theta) +y*sin (theta);
    y_theta=-x*sin (theta) +y*cos (theta);
    gb=exp (-0.5* (x_theta. ^2/sigma_x^2+y_theta. ^2/sigma_y^2)). *cos
(2*pi/lambda*x_theta+psi);
end
```

Zemāk ir attēloti uzģenerētie Gabora filtra piemēri.

Attēls 4.10. – Iegūtie Gabora filtra piemēri

Nākamais etaps ir Gabora filtra uzklāšana uz attēla. Zemāk ir attēlots programmas kods, kas realize doto etapu[17]:

```
function [img] = gabor_filter (img, orient)
    img_m = zeros (19, size (img,1),size (img,2));
    for c = 0: 10: 180
        gab = gabor_fn (c);
        img_m ( (c) /10+1,:,:) = imfilter (img, gab);
    end
    for a = 1: size (img, 1)
        for b = 1: size (img,2)
            if (orient (a,b) >=175)
                orient (a,b) = 1;
            end
        end
    end
    for a = 1: size (img, 1)
        for b = 1: size (img,2)
            img (a,b) = img_m (round (orient (a,b) /10) +1,a,b);
        end
    end
end
```

Attēla nr. 19 tiek attēlots iepriekš veiktās procedūras rezultātā izveidotais pirksta nospiedums pēc tā normalizēšanas, bet attēlā numur 20 ir attēlots pirksta nospiedums, kurs ir apstrādāts ar Gabora filtru.

Attēls 4.11. – Binārais pirksta nospieduma attēls

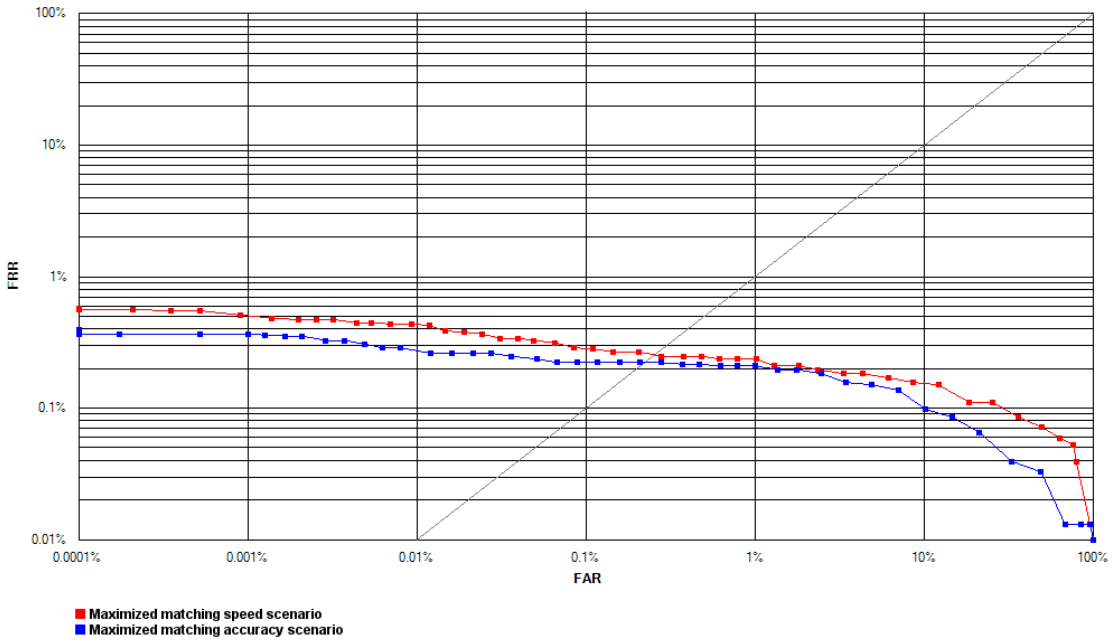
Attēls 4.12. - Apstrādāts ar Gabora filtru pirksta nospiedums

4.4.3.5. Secinājumi

Kā var redzēt pēc iepriekšējiem attēliem, mums izdevās stipri uzlabot pirkstu nospiedumu attēlu, pielietojot Gabora filtra īpašības. Uz šāda attēla ir daudz vienkāršāk atrast nepieciešamās pazīmes un salīdzināt tās, līdz ar to arī identifikācijas ātrumam un arī precizitātei mūsu sistēmā vajadzētu paātrināties.

4.5. Testēšana

Pēc gandrīz viena mēneša testēšanas, kurā piedalījās 32 sistēmā reģistrēti darbinieki un vairāk nekā 100 sistēmā nereģistrēti lietotāji (uzņēmuma viesi), var droši pateikt, kad sistēma savu darbu izpilda teicami un to apstiprina 15. attēlā redzamais grafiks ar FAR un FRR attiecības statistiku. Grafikā ir attēlotas divas līknes, zilā nozīmē, kad aparāti strādāja maksimālās precizitātes režīmā, bet sarkanā nozīmē, kad aparāts strādāja maksimālajā ātruma režīmā. Kā var redzēt atšķirība nav liela un pilnībā apmierinoša abiem gadījumiem.



Attēls 4.13. - FAR un FRR attiecība rezultāti pēc viena mēneša testēšanas

Kā var redzēt abos gadījumos kļūdainu rezultātu procents ir vienādi zems, līdz ar to var apgalvot kad sistēma ir pietiekami droša, lai to izmantotu informācijas aizsargāšanai. Visas testēšanas laikā neviens no nereģistrētajiem lietotājiem nebija iekļuvis aizsargājamajās telpās, kā arī bija tikai daži gadījumi kad reģistrēts lietotājs ar pirmo reizi nevarēja iegūt piekļuvi, bet tas drīzāk notika dēļ nekorekta pirksta novietošanas uz sensora. Šādi gadījumi pārsvarā bija tikai pašā sākumā, kad sistēma tika uzstādīta, pēc tam, kad darbinieki ieguva vairāk pieredzes pirkstu nospiedumu iekārtas izmantošanā, šādu problēmu vairs nebija.

Testēšanas rezultātā iegūtā FRR un FAR statistika palīdzēja iegūt optimālo uzstādījumu izmēru, to var redzēt pēc slīpās svītras uz grafika. Viss optimālāko FAR un FRR attiecību sanāca iegūt uzstādot FAR 0,15% un FRR uz 0,5%.

4.6. Secinājumi

Sistēma ir uzstādīta vairāk nekā mēnesi atpakaļ un pagaidām ir tikai pozitīvas atsauksmes. Darbiniekiem vairs nav jāpilda laika atskaites sistēma, jo tā tiek aizpildīta automātiski pēc saņemtās autentifikācijas informācijas. Vadība vairs neuztraucas par drošības jautājumiem, jo tagad katram lietotājam ir savas piekļuves tiesības pie noteiktām telpām un noteiktā laika periodā. Grāmatvedības nodaļai ir daudz vienkāršāk aprēķināt darbinieku algu un sekot līdzi darba stundām, veidot dažāda veida atskaites, jo biometriskā autentifikācijas sistēma ir integrēta grāmatvedības uzskaites programmatūrā. Uzņēmuma viesi ir pārsteigti redzot šādu autentifikācijas sistēmu, līdz ar to arī kompānijas izskats klientu un sadarbības partneru acīs palielinās.

Laikam ejot uz priekšu iespējams atklāsies arī kādas negatīvās šīs tehnoloģijas puses, bet uz doto brīdi sistēma pilnībā apmierina uzņēmuma vajadzības un atbilst ieguldītajiem līdzekļiem.

REZULTĀTI UN DISKUSIJA

Daudzās dažādās nozarēs vienmēr bija uzdevumi, kur nepieciešams atpazīt konkrēto cilvēku. Viss biežāk tas ir nepieciešams veicot kontroli, drošības nodrošināšanu, lai kontrolētu cilvēku darbības un aizsargātu personīgo informāciju.

Pēdējā desmitgadē cilvēka identitātes noteikšanai izmanto arvien jaunākas tehnoloģijas metodes, un viss pieprasītākās no tām ir biometriskās personības atpazīšanas metodes, kad pats cilvēks ir atslēga, izmantojot savas unikālās fiziskās vai uzvedības pazīmes. Pēdējā laikā šīs jomas specializācija ir stipri palielinājusies salīdzinot to ar sākuma gadiem: identifikācija tiek izmantota ne tikai tradicionālos uzdevumos, lai nodrošināto drošību un piekļuves tiesības, bet arī kā piemēru var minēt tirdzniecības sistēmas, kur tiek veikta individuālā pieeja katram klientam., vai statistikas pētījumos un vel daudz kur citur.

Ir pierādīts, kad katram cilvēkam ir daudz unikālu pazīmju, sākot ar daudziem pazīstamajām (piemēram pirkstu nospiedumi), līdz pat diezgan eksotiskām (auss formas, sejas temperatūras karte). Lai veiktu identifikāciju pēc vairākiem no šiem principiem jau tagad ir izveidoti tehniski risinājumi, kā arī ir pilnība automatizētas sistēmas, kas veic cilvēka personības biometrisko identifikāciju.

Prakse pierāda, kad tradicionālo autentifikācijas sistēmu nomaiņa uz barometriskajām, jebkurā gadījuma palielina kopējo sistēmas drošības līmeni pateicoties neapšaubāmām šīs pieejas priekšrocībām. Korekta ekspluatācija un pareizo līdzekļu izmantošana (piemēram, dažreiz var būt nepieciešama krusteniskā biometrija) praksē nodrošina gandrīz 100% identifikācijas precizitātes līmeni, kas savukārt palīdz veikt secinājums par pareizās sistēmas izvēli.

Starp daudzām citām metodēm, kas jau tagad ir kļuvušas tradicionālas, viena no nākotnes perspektīvākajām metodēm varētu būt personības atpazīšana pēc sejas. Šai metodei ir daudz neapšaubāmu priekšrocību citu priekšā: pie pietiekami lielas precizitātes šī tehnoloģija atļauj veikt pārbaudes no lielāka attāluma, personai par to pat nenojaušot, un aparatūras gadījumā ir nepieciešama tikai video kamera ar pietiekami labu kvalitāti, kas ir brīvi pieejamas tirgū plašam klientu klāstam. Šo īpašību kombinācija noteikti izraisīs strauju šīs tehnoloģijas attīstību, un tas drīzumā kļūs tik pat izplatīts kā pirkstu nospiedumu pārbaude.

Pēc viss izplatītāko programmatūru priekš privātās izmantošanas analīzes, var redzēt, ka tehniskais lēciens jau ir noticis – biometrija ir pagājusi lielu soli uz priekšu veicot plaša spektra uzdevumu risināšanu. Ejot laikam uz priekšu biometriskās tehnoloģijas attīstīsies un aizstās jau sen eksistējošās tehnoloģijas. Pie tam attīstību var gaidīt ne tikai pēc skaita, bet arī

pēc kvalitātes – biometrija tiks integrēta arī jaunās nozarēs (kā piemēram tas notiek ar balss kontroli) un parādīsies pilnīgi jaunas un cilvēkam intuitīvi saprotamas metodes. Tai skaitā var arī droši prognozēt turpmāk plašu sejas atpazīšanas tehnoloģijas integrāciju (piemēram teroristu meklēšanā ar novērošanas kameru palīdzību). Un ņemot vērā, kad jau tagad daudzās valstīs, tai skaitā Latvijā, ieviestas masveida biometrijas tehnoloģijas (piemēram pases ar biometrijas datiem), drīzumā tās kļūs daudz izplatītākas un atliks tikai tās pielāgot pēc gala lietotāju atsauksmēm.

Klasiskas vairākkārt lietojamas paroles izmantošana ir vājākais autentifikācijas veids, tādēļ mūsdienās, kad informācijas aizsardzība ir ļoti nopietns jautājums, ņemot vērā izanalizēto informāciju, nebūtu prātīgi turpināt lietot tikai tās, ir vērts apdomāt to apvienošanu ar citām autentifikācijas metodēm un vairāku faktoru autentifikācijas sistēmas izveidi.

SECINĀJUMI

Mūsdienu lielākā autentifikācijas problēma ir pieejas datu zādzība, kas var būt pasniegts dažādi. Tas nozīmē, ka paroli noziedznieks var iegūt pielietojot pīkšķerēšana metodi (fishing method), vai arī parole tiek ieraudzīta ievadīšanas brīdī, vai pierakstīta uz papīra un nokļūst citu acīs, vai kādā citā veidā tiek nozagta. Tādēļ ir vērts pievērst vairāk uzmanības autentifikācijas sistēmas izstrādei, kas nepieļautu personīgo datu zādzību, pat ja lietotājs ir nozaudējis savus pieejas datus.

Šobrīd lieli resursi tiek ieguldīti tieši biometriskās autentifikācijas attīstīšanā, jo tas ir viens no ērtākajiem autentifikācijas veidiem, nav jāatceras paroles, identifikatori, nav jānēsā līdzi nekādas ierīces. Viens no pēdējiem biometriskās autentifikācijas izgudrojumiem ir speciāli veidots skeneris, kurš ar speciāla gaismas stara palīdzību nolasa zemādas kapilāru struktūru, kura katram cilvēkam, tā pat kā pirkstu nospiedums ir sava. Vienīgi atšķirībā no pirksta nospieduma, kuru ir iespējams viegli nokopēt, šī pieeja ir drošāka, jo šādu informāciju saņemt ir daudz grūtāk, atšķirībā no pirkstu nospieduma, kurus mēs atstājam uz visām lietām, kurām pieskaramies. Vel ir atklāts, kad katra cilvēka sirds veidotās mikro vibrācijas ir unikālas katram cilvēkam – to arī varētu izmantot jaunas autentifikācijas metodes izveidošanai. Vienīgi šādu parametru nolasīšanai būs nepieciešami zemādas sensori. Es uzskatu, ka nākotnes autentifikācijas sistēmas būs balstītas uz biometrijas līdzekļiem.

Es personīgi uzskatu kad viss drošākā autentifikācijas sistēma ir divu faktoru autentifikācijas sistēma ar biometrisko faktoru, piemēram pirkstu nospiedumu metodi var viegli apvienot ar plaukstas ģeometrijas metodi un sanāks ļoti droša un ērta autentifikācijas sistēma, vai arī acs varavīksnes pārbaude kopā ar sejas atpazīšanas algoritmu – varbūt atsevišķi nav tik precīzas, bet lietojot tās kopā tās dos praktiski 100% precīzu rezultātu.

Pasaulē, kurā mums visapkārt ir dažādi sensori, saslēgtas ierīces, sociālie tīkli kuri ar vien vairāk satur personīgo informāciju par mūsu dzīvi, tagadējās autentifikācijas metodes ir nepietiekami drošas un vienkāršas, tieši tādēļ industrija vel joprojām smagi strādā, lai atrastu viss optimālāko autentifikācijas variantu, kas būtu viegli izmantojams, viegli aizsargājams un grūti uzlaužams.

IZMANTOTĀ LITERATŪRA UN AVOTI

1. InfoSec Institute, Pierluigi Paganini, „The Impact of Cybercrime", februāris 2014. URL:http://resources.infosecinstitute.com/2013-impact-cybercrime/
2. SafeNet-Inc, Andrew Gertz, Data Breaches by the Numbers, aprīlis, 2014, URL:http://data-protection.safenet-inc.com/2014/04/infographic-data-breaches-by-the-numbers-q1-2014-26-people-fall-victim-to-a-data-breach-every-second/
3. „The Science of Guessing: Analyzing an Anonymized Corpus of 70 Million Passwords", Bonneau, J. ; Comput. Lab., Univ. of Cambridge, Cambridge, UK, 2012 URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6234435
4. M. Just. Designing authentication systems with challenge questions. In L. F. Cranor and S. Garfinkel, editors, Security and Usability: Designing Secure Systems that People Can Lapas nr. 143–155, Sebastopol, CA, 2005. O'Reilly Media, Inc.
5. Zach Jorgensen and Ting Yu, Department of Computer Science North Carolina State University „On Mouse Dynamics as a Behavioral Biometric for Authentication", oktobris 2012 URL: http://www4.ncsu.edu/~tyu/pubs/asiaccs11-jorgensen.pdf
6. Sophie Curtis, The Thelegraph, „Young people 'ready to ditch passwords for biometric security'" janvāris 2015 URL: http://www.telegraph.co.uk/technology/internet-security/11343040/Young-people-ready-to-ditch-passwords-for-biometric-security.html
7. Kevin Mitnick with William L. Simon. „The Art of Decepton: Controlling the Human Element of Security", oktobris 2002
8. Y. Dodis, L. Reyzin, and A. Smith. „Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data" Proceedings from Advances in Cryptology EuroCrypt. — 2004
9. NSTC Policy for Enabling the Development, Adoption and Use of Biometric Standards URL: http://www.biometrics.gov/standards/
10. Louisville, CO (PRWEB) „Biometrics Market will Exhibit Sustained Growth Through 2020 as Revenues Approach $10 Billion Annually" marts, 2007 URL: http://www.prweb.com/releases/2007/03/prweb514374.htm
11. B. Sullivan. 'Forgot your password?' may be weakest link, decembris, 2013. URL: http://www.zonealarm.com/blog/2013/12/how-your-email-account-could-be-the-weakest-link-to-your-online-accounts/
12. Social Authentication. Alex Rice, janvāris, 2011, URL:blog.facebook.com/blog.php?post=486790652130
13. Igors Matuls, kursa darbs „Mūsdienu autentifikācijas iespējas", Rīga, 2014
14. Javier R. Movellan (Ed) Tutorial on Gabor Filters. 2008. URL: http://mplab.ucsd.edu/tutorials/gabor.pdf
15. Van Gogh Hogan „Алгоритмы для классификации отпечатков пальца на основе применения фильтра Габора, вейвлет-преобразоваия и многослойной нейронной сети" Известия Томского политехнического университета, 2012 gads

16. Asker M. Bazen, „Systematic methods for the computation of the directional fields and singular points of fingerprint” Asker M. Bazen, Sabih H. Gerez, IEEE Transactions on pattern analysis and machine intelligence, 2002 gads
17. Jie Zhou, „Singular Points Analysis in Fingerprints Based on Topological Structure and Orientation Field” Jie Zhou, Jinwei Gu, David Zhang Department of Computing, the Hong Kong Polytechnic University, Kowloon, Hong Kong
18. Wikipedia, „Diffie–Hellman key exchange”, 2013 gada, marts; URL: http://en.wikipedia.org/wiki/Diffie%E2%80%93Hellman_key_exchange

PIELIKUMI

1. pielikums. Difi-Helmana protokols datu aizsardzībai

```
using System;
using System.Collections.Generic;
using System.Text;
using System.Security.Cryptography;

namespace DiffieHellman
{
    /// <summary>
    /// Difi-Helmana protokola klase
    /// </summary>
    public class DiffieHellman : IDisposable
    {
        #region - papildus funkcionalitāte -
        static StrongNumberProvider _strongRng =
       new StrongNumberProvider();
        #endregion

        #region - Lauki -
        /// <summary>
        /// Bitu skaits kurus ģenerēt
        /// </summary>
        private int bits = 256;

        /// <summary>
        /// Kopējais pamatskaitlis.
        /// </summary>
        BigInteger prime;
        /// <summary>
        /// Kopējais bāze]]
        /// </summary>
        BigInteger g;
        /// <summary>
        /// privātais pamatskaitlis
        /// </summary>
        BigInteger mine;

        /// <summary>
        /// Beigu astlēga
        /// </summary>
        byte[] key;
        /// <summary>
        /// Simbolu attēlojums
        /// </summary>
        string representation;
        #endregion

        #region - Properties -
        /// <summary>
        /// Atgriež beigu atslēgu, kuru lietot
        /// </summary>
        public byte[] Key
        {
```

```
        get { return key; }
    }
    #endregion

    #region - Ctor -
    public DiffieHellman()
    {
    }

    public DiffieHellman(int bits)
    {
        this.bits = bits;
    }

    ~DiffieHellman()
    {
        Dispose();
    }
    #endregion

    #region - Realizācijas metodes -
    #region Plūsma

    /// <summary>
    /// Izveido pieprasījumu.
    /// </summary>
    /// <returns></returns>
    public DiffieHellman GenerateRequest()
    {
        // Izveido parametrus
        prime = BigInteger.GenPseudoPrime(bits, 30,
                _strongRng);
        mine = BigInteger.GenPseudoPrime(bits, 30,
                _strongRng);
        g = (BigInteger)5;

        // Izveido simbolu virkni
        StringBuilder rep = new StringBuilder();
        rep.Append(prime.ToString(36));
        rep.Append("|");
        rep.Append(g.ToString(36));
        rep.Append("|");

        // Izveido lielu gadījuma skaitli BigInteger
        using (BigInteger send = g.ModPow(mine, prime))
        {
            rep.Append(send.ToString(36));
        }

        representation = rep.ToString();
        return this;
    }

    /// <summary>
    /// Izveido atbildi
    /// </summary>
    /// <param name="request">Pieprasījuma simbolu
    /// virkne</param>
    /// <returns></returns>
    public DiffieHellman GenerateResponse(string request)
    {
```

```
        string[] parts = request.Split('|');

        // Izveido nepieciešamos mainīgos
        using (BigInteger prime = new BigInteger(parts[0],
                                        36))
        using (BigInteger g = new BigInteger(parts[1], 36))
        using (BigInteger mine =
         BigInteger.GenPseudoPrime(bits, 30, _strongRng))
        {
            // Izveido atslēgu
            using (BigInteger given =
               new BigInteger(parts[2], 36))
            using (BigInteger key = given.ModPow(mine,
                                        prime))
            {
                this.key = key.GetBytes();
            }
            // Izveido atbildi
            using (BigInteger send = g.ModPow(mine, prime))
            {
                this.representation = send.ToString(36);
            }
        }

        return this;
    }

    /// <summary>
    /// Izveido atslēgu, pēc atbildes saņemšanas.
    /// </summary>
    /// <param name="response">Simbolu virknes attēlojums
    ///  atbildei</param>
    public void HandleResponse(string response)
    {
    // Veic moduļa sadalīšanu ar skaitli
    // kas ir kāpināts ar citā skaitlī.
        using (BigInteger given = new BigInteger(response,
                36))
        using (BigInteger key = given.ModPow(mine, prime))
        {
            this.key = key.GetBytes();
        }
        Dispose();
    }
    #endregion

    public override string ToString()
    {
        return representation;
    }
    #endregion

    #region IDisposable Members
    /// <summary>
    /// Pabeidz skaitļošanu, un atslēga vel joprojām ir
    /// pieejama
    /// </summary>
    public void Dispose()
    {
        if (!Object.ReferenceEquals(prime, null))
            prime.Dispose();
```

```
            if (!Object.ReferenceEquals(mine, null))
                mine.Dispose();
            if (!Object.ReferenceEquals(g, null))
                g.Dispose();

            prime = null;
            mine = null;
            g = null;

            representation = null;
            GC.Collect();
            GC.Collect();
        }

        #endregion
    }
}
```

2. Pielikums. Gabora filtra realizācija

```
%Virziena aprēķināšanas funkcija
function [orient] = orient_grad (img)
    [mod, dir] = imgradient (img);
    for a = (1: size (mod,1))
        for b = (1: size (mod,2))
            if (dir (a,b) >=0)
                line_dir (b) = dir (a,b) - 90;
            else
                line_dir (b) = dir (a,b) +90;
            end
        end
        if a==1
            dir_new = line_dir;
        else
            dir_new = cat (1, dir_new, line_dir);
        end
    end
    win_size = 9;
    for a = (fix (win_size/2) +1: win_size: size (dir_new,1) -
       fix
   (win_size/2))
        for b = (fix (win_size/2) +1: win_size: size (dir_new,2)
   -
        fix (win_size/2))
            count_plus = 0; %krustpunktu skaitītājs
            count_min = 0; %pazīmju skaitītais
            for c = (1: win_size)
                for d = (1: win_size)
                    if dir_new (a- (fix (win_size/2) +1) +c,
                           b- (fix (win_size/2) +1) +d) >=0
                        count_plus = count_plus + 1;
                    else
                        count_min = count_min + 1;
                    end
                end
            end
            aver = 0; %vidējais leņķis
            for c = (1: win_size)
                for d = (1: win_size)
                    if count_plus>count_min
                        if dir_new (a- (fix (win_size/2) +1) +c,
                               b- (fix (win_size/2) +1) +d) >=0
                               aver = aver+ double (dir_new (a-
                          (fix (win_size/2) +1) +c, b- (fix
                          (win_size/2) +1) +d));
                        end
                    else %else
                        if dir_new (a- (fix (win_size/2) +1) +c,
                               b- (fix (win_size/2) +1) +d) <0
                            aver = aver + double (dir_new (a-
                        (fix (win_size/2) +1) +c, b- (fix
                        (win_size/2) +1) +d));
                        end
                    end
                end
            end
            % aprēķinam vidējo leņķi
```

```
            if count_plus>count_min
                aver = aver/count_plus;
            else
                aver = aver/count_min;
            end
            % saglabājam vērtību matricā
            orient_line (fix (b/win_size) +1) = aver;
        end
        if a==fix (win_size/2) +1
            orient = orient_line;
        else
            orient =cat (1, orient, orient_line);
        end
    end
end

%Virziena vizualizācijas funkcija
function [output_img] = show_orient (img)
    img = img*pi/180;
    for x= (1: size (img,1) /5)
        img_line = show (img,x);
        if (x==1)
            output_img = img_line;
        else
        output_img = cat (1, output_img, img_line);
        end
    end
    imtool (output_img)
end

function [img_out] = show (img, x)
    line = zeros (15,15);
    for a = (3: 13)
        line (8,a) = 255;
    end
    a = (x-1) *5+3;
    for b = (3: 5: size (img,2) - 2)
        sum = 0
        for c = (1: 5)
            for d = (1: 5)
                sum = sum + img (a-3+c, b-3+d);
            end
        end
        sum = sum/25; % leņķu vidējais aritmētiskais
        orient = imrotate (line, sum*180/pi, 'crop');
        orient = imadjust (orient, [0 1], [1 0]);
        if (b==3)
            for c = (1: 15)
                for d = (1: 15)
                    img_out (c, (b-3) *3+d) = orient (c, d);
                end
            end
        else
            img_out = cat (2, img_out, orient);
        end
    end
end


%Parametra pielasīšanas funkcija
function [output_args] = test_gabor (img, orient)
```

```
    bw = 0.3;
    for a = 1: 24
        test_im = gabor_filter (img, orient,bw+a/20);
        imtool (test_im);
    end
end

%Virziena funkcijas veidošanas kods
function [orient] = orient_grad (img)
    [mod, dir] = imgradient (img);
    for a = (1: size (mod,1))
        for b = (1: size (mod,2))
            if (dir (a,b) >=0)
                line_dir (b) = dir (a,b) - 90;
            else
                line_dir (b) = dir (a,b) +90;
            end
        end
        if a==1
            dir_new = line_dir;
        else
            dir_new = cat (1, dir_new, line_dir);
        end
    end
    win_size = 9;
    for a = (fix (win_size/2) +1: win_size: size (dir_new,1) -
       fix (win_size/2))
        for b = (fix (win_size/2) +1: win_size: size (dir_new,2)
             - fix (win_size/2))
            %uzskaita cik krustojumu ir attēlā
       count_plus = 0;
            %uzskaita cik individuālās pazīmes ir attēlā
       count_min = 0;
            for c = (1: win_size)
                for d = (1: win_size)
                    if dir_new (a- (fix (win_size/2) +1) +c,
                                b- (fix (win_size/2) +1) +d) >=0
                        count_plus = count_plus + 1;
                    else
                        count_min = count_min + 1;
                    end
                end
            end
            aver = 0; %vidējas leņķis
            for c = (1: win_size)
                for d = (1: win_size)
               % ja krustojumu ir vairāk nekā pazīmes
                    if count_plus>count_min
                        if dir_new (a- (fix (win_size/2) +1) +c,
                                b- (fix (win_size/2) +1) +d) >=0

                         aver = aver+ double (dir_new (a- (fix
                    (win_size/2) +1) +c, b- (fix (win_size/2) +1)
                    +d));
                        end
                    else %else
                        if dir_new (a- (fix (win_size/2) +1) +c,
                                b- (fix (win_size/2) +1) +d) <0
                         aver = aver + double (dir_new (a- (fix
                    (win_size/2) +1) +c, b- (fix (win_size/2) +1)
                    +d));
```

```
                    end
                end
            end
        end

        % aprēķinam vidējo leņķi
            if count_plus>count_min
                aver = aver/count_plus;
            else
                aver = aver/count_min;
            end
            % saglabājam vērtības matricā
            orient_line (fix (b/win_size) +1) = aver;
        end
        if a==fix (win_size/2) +1
            orient = orient_line;
        else
            orient =cat (1, orient, orient_line);
        end
    end
end

%Attēla virzienu vizualizācijas kods
function [output_img] = show_orient (img)
    img = img*pi/180;
    for x= (1: size (img,1) /5)
        img_line = show (img,x);
        if (x==1)
            output_img = img_line;
        else
             output_img = cat (1, output_img, img_line);
        end
    end
    imtool (output_img)
end

function [img_out] = show (img, x)
    line = zeros (15,15);
    for a = (3: 13)
        line (8,a) = 255;
    end
    a = (x-1) *5+3;
    for b = (3: 5: size (img,2) - 2)
        sum = 0
        for c = (1: 5)
            for d = (1: 5)
                sum = sum + img (a-3+c, b-3+d);
            end
        end
        sum = sum/25; %leņķu vidējais aritmētiskais
        orient = imrotate (line, sum*180/pi, 'crop');
        orient = imadjust (orient, [0 1], [1 0]);
        if (b==3)
            for c = (1: 15)
                for d = (1: 15)
                    img_out (c, (b-3) *3+d) = orient (c, d);
                end
            end
        else
            img_out = cat (2, img_out, orient);
        end
```

```
    end
end

%Parametra piemeklēšanas funkcijas kods
function [output_args] = test_gabor (img, orient)
    bw = 0.3;
    for a = 1: 24
        test_im = gabor_filter (img, orient,bw+a/20);
        imtool (test_im);
    end
end
```

DOKUMENTĀRĀ LAPA

Bakalaura darbs „Autentifikācijas metodes un algoritmi” izstrādāts LU Datorikas fakultātē.

Ar savu parakstu apliecinu, ka pētījums veikts patstāvīgi, izmantoti tikai tajā norādītie informācijas avoti un iesniegtā darba elektroniskā kopija atbilst izdrukai.

Autors: Igors Matuls I.Matuls 01.06.2015.

Paraksts _____

Rekomendēju darbu aizstāvēšanai
Vadītājs: Jānis Zuters asociētais profesors Dr.sc.comp.

Paraksts _____

Recenzents: Juris Vīksna profesors Dr.sc.comp.

Darbs iesniegts Datorikas fakultātē 01.06.2015.
Metodiķe: Ārija Sproģe

Darbs aizstāvēts bakalaura gala pārbaudījuma komisijas sēdē

_____

Komisija: _____