SOFT BIOMETRIC AUTHENTICATION

Melisa Azizovic
Department of Computer Science, University of Novi Pazar, Serbia, melisa.azizovic@gmail.com
Emrus Azizovic
University of Novi Pazar, Serbia, e.azizovic@uninp.edu.rs

Abstract: Soft biometric authentication is the process of identifying or authenticating users based on characteristics that are less reliable than traditional biometric characteristics such as fingerprints or faces. Soft biometric authentication is a technology that uses different types of features and characteristics of users to determine whether they are a real user. These characteristics are commonly referred to as "soft" biometrics, as they differ from "hard" biometrics, which refer to physical characteristics such as fingerprints or the pupil of the eye. Examples of soft biometrics include characteristics such as handwriting, typing speed, voice characteristics, gestures, and other non-invasive and easily measurable characteristics. Soft biometric authentication is used in situations where traditional biometric characteristics are not reliable enough, or when the user does not want to provide personal information that is necessary for authentication. Soft biometric authentication plays an increasingly important role in the modern world, especially in the field of information technology. As technologies evolve, so do the risks of identity theft and hacker attacks. Soft biometric authentication provides an additional layer of security, helping to verify the user's identity based on various behavioral characteristics, making unauthorized access to the system difficult. This technology is increasingly used in banking, e-commerce, social media, health care and other areas where reliable user authentication is required. Soft biometric authentication also enables a better user experience, providing easier and faster access to systems and applications without the need for predefined passwords or other security codes. In addition, soft biometric authentication has the potential to be used in combination with other technologies such as machine learning and artificial intelligence to create advanced authentication systems that can adapt their actions based on user preferences and behavior. Soft biometric authentication has several advantages over traditional authentication methods. For example, users do not need to carry additional devices such as cards or keys, and they also do not need to remember passwords. This technology can also be useful in preventing fraud or hacking, as user behavior and environmental characteristics are difficult to fake. However, soft biometric authentication also has certain disadvantages, such as lower reliability compared to traditional authentication methods, the possibility of errors due to the variability of user characteristics and the environment, as well as the possibility of misuse of data on user characteristics. In this paper, we focused on the analysis of soft biometric authentication. First, we defined the term biometrics in order to follow the further content of the paper. We presented categories and analyzed security and privacy in soft biometric authentication.
Keywords: Biometrics, soft biometrics, authentication, social pattern, emotional pattern, behavioral pattern

SOFT BIOMETRIJSKA AUTENTIFIKACIJA

Melisa Azizović
Departman za računarske nauke Univerziteta u Novom Pazaru, Srbija, melisa.azizovic@gmail.com
Emruš Azizović
Univerzitet u Novom Pazaru,Srbija, e.azizovic@uninp.edu.rs

Rezime: Soft biometrijska autentifikacija predstavlja proces identifikacije ili autentifikacije korisnika na osnovu karakteristika koje su manje pouzdane od tradicionalnih biometrijskih karakteristika poput otiska prsta ili prepoznavanje lica. Soft biometrijska autentifikacija je tehnologija koja se oslanja na različite osobine i karakteristike korisnika kako bi se proverilo da li su oni pravi korisnik. Ove karakteristike se obično nazivaju "meke" biometrijske karakteristike, jer se razlikuju od "tvrde" biometrije koja se odnosi na fizičke karakteristike kao što su otisci prstiju ili zenica oka. Primeri soft biometrije uključuju karakteristike kao što su način pisanja, brzina kucanja, glasovne karakteristike, gestikulacije i druge neinvazivne i lakše merljive karakteristike. Soft biometrijska autentifikacija se koristi u situacijama kada tradicionalne biometrijske karakteristike ne pružaju dovoljno visok nivo pouzdanosti, ili kada korisnik ne želi da pruži lične informacije koje su neophodne za autentifikaciju. Soft biometrijska autentifikacija igra sve veću ulogu u savremenom svetu, posebno u oblasti informacionih tehnologija. Kao što se tehnologije razvijaju, tako i rizici od krađe identiteta i hakerskih napada postaju sve veći. Soft

biometrijska autentifikacija pruža dodatni sloj sigurnosti, pomažući da se korisnikov identitet verifikuje na osnovu različitih karakteristika ponašanja, što otežava neovlašćeni pristup sistemu. Ova tehnologija se sve više koristi u bankarstvu, e-trgovini, društvenim medijima, zdravstvenoj zaštiti i drugim oblastima gde je potrebna pouzdana autentifikacija korisnika. Soft biometrijska autentifikacija takođe omogućava bolje korisničko iskustvo, pružajući lakši i brži pristup sistemima i aplikacijama bez potrebe za unapred definisanim lozinkama ili drugim sigurnosnim kodovima. Takođe, soft biometrijska autentifikacija može se kombinovati sa drugim tehnologijama poput mašinskog učenja i veštačke inteligencije kako bi se stvorili napredni autentifikacioni sistemi koji se mogu prilagoditi prema korisničkim preferencijama i ponašanju. U poređenju sa tradicionalnim metodama autentifikacije, ove karakteristike donose mnoge prednosti. Na primer, korisnicima nije potrebno nositi dodatne uređaje kao što su kartice ili ključevi, a takođe se ne moraju ni setiti lozinki.Ova tehnologija takođe može biti korisna u sprečavanju prevara ili hakovanja, jer se ponašanje korisnika i karakteristike okoline teško mogu lažirati. Međutim, soft biometrijska autentifikacija ima i određene nedostatke, kao što su manja pouzdanost u odnosu na klasične metode autentifikacije, mogućnost grešaka zbog varijabilnosti karakteristika korisnika i okoline, kao i mogućnost zloupotrebe podataka o karakteristikama korisnika. U radu smo se fokusirali na analizu soft biometrijske autentifikacije. Prvo smo definisali pojam biometrije kako bismo pratili dalji sadržaj rada. Predstavili smo kategorije i analizirali bezbednost i privatnost u soft biometrijskoj autentifikaciji.
Ključne reči: Biometrija, soft biometrija, autentifikacija, socijalni obrazac, emocionalni obrazac, ponašajni obrazac

1. UVOD

U današnje vreme, kada su online servisi postali neizostavni deo naše svakodnevnice, bezbednost i privatnost korisničkih podataka su postale od izuzetne važnosti. Tradicionalne metode autentifikacije, kao što su lozinke ili PIN kodovi, sve su manje efikasne zbog mogućnosti njihovog hakovana ili krađe. Zbog toga, razvijaju se nove tehnologije autentifikacije, a jedna od njih je soft biometrijska autentifikacija. Kao tehnologija autentifikacije, soft biometrijska autentifikacija se smatra manje invazivnom i diskretnijom za razliku od tradicionalnih biometrijskih metoda. Osim toga, prednosti soft biometrijske autentifikacije uključuju kontinuirano praćenje i analizu korisničkih karakteristika, što omogućava otkrivanje pokušaja zloupotrebe sistema, kao i poboljšanu prilagođenost i personalizaciju usluga za korisnike. Tradicionalna biometrijska autentifikacija koristi statičke fizičke karakteristike kao primer, možemo spomenuti otisak prsta, zenicu oka, oblik lica ili geometrijske karakteristike šake za autentifikaciju korisnika [8]. Sa druge strane, soft biometrijska autentifikacija se fokusira na dinamičke karakteristike korisnikovog ponašanja kao što su stil pisanja, brzina kucanja, karakteristike miša, ritam govora i slično. Tradicionalne biometrijske metode su relativno jednostavne za upotrebu, ali zahtevaju direktan kontakt između korisnika i senzora. Sa druge strane, soft biometrijska autentifikacija je manje invazivna i ne zahteva posebne senzore ili hardversku opremu. Osim toga, soft biometrijska autentifikacija može pružiti kontinuiranu autentifikaciju tokom celog korisničkog iskustva, dok tradicionalne metode mogu zahtevati da korisnik ponovo potvrdi svoj identitet nakon određenog vremena ili nakon izlaska iz sistema. Konačno, tradicionalne biometrijske metode obično se koriste za autentifikaciju jedne specifične karakteristike, dok soft biometrijska autentifikacija koristi kombinaciju različitih karakteristika kako bi se obezbedila veća sigurnost autentifikacije [5]. Ipak, soft biometrijska autentifikacija predstavlja inovativan pristup autentifikaciji koji se sve više koristi u modernim tehnološkim aplikacijama i sistemima. U ovom radu će biti detaljnije opisane karakteristike, prednosti i nedostaci soft biometrijske autentifikacije, kao i njena primena u različitim oblastima.

Cilj rada je da prikaže karakteristike soft biometrijske autentifikacije. Takođe cilj rada je da naglasi značaj i kategorije soft biometrijske autentifikacije kao što su socijalni, emocionalni i ponašajni obrazac, tehnologije koje se koriste u soft biometrijskoj autentifikaciji analiza lica, glasa i ponašanja kao i da ukaže na bezbednost i privatnost u soft biometrijskoj autentifikaciji. Posle uvoda u drugom delu rada je analiziran pojam biometrije, dok su u trećem delu objašnjene kategorije soft biometrijske autentifikacije. Četvrti deo rada opisuje bezbednost i privatnost u soft biometrijskoj autentifikaciji.

2. POJAM BIOMETRIJE

Izraz biometrija dolazi od grčkih reči bios, što znači život, i metron, što znači mera. Ovde se radi o merenju određenih telesnih i ponašajnih karakteristika živih bića, posebno ljudi [3]. Postoji debata u vezi sa biometrijom i metodama identifikacije, gde jedna grupa autora tvrdi da su sve (klasične) metode identifikacije zapravo biometrijske, a da se radi o klasičnim metodama u novom, digitalnom okruženju. Druga grupa autora prihvata savremene tehnološke mogućnosti koje omogućuju jednostavniju primenu "klasičnih" metoda identifikacije, ali i razvoj novih metoda temeljenih na identifikacijskim obilježjima koja se nisu mogla prepoznati i koristiti u ranijem periodu, kada su tehnološke mogućnosti bile ograničene. Ipak, bez obzira na ove različite stavove, biometrija se smatra metodama identifikacije koji su primarno određene informaciono-digitalnim okruženjem. Biometrija je nauka

o automatizovanim postupcima za jedinstveno prepoznavanje ljudi na osnovu jednog ili više urođenih telesnih obeležja ili obeležja čovekovog ponašanja [4]. Biometrijske metode se zasnivaju na klasičnim, standardnim metodama identifikacije koje datiraju iz davne istorije čovečanstva. U novije vreme biometrija je doživela punu afirmaciju i procvat, a razlog tome leži ponajviše u vrtoglavom razvoju tehnologije koja klasičnim biometrijskim metodama daje novu dimenziju, a posebno, kao što je kazano u uvodu, razvoju računarske industrije (hardverskih, tehničkih mogućnosti, ali i softverskih alata) čime se mogućnosti primene otvaraju do neslućenih granica, koje su u bliskoj prošlosti bile nezamislive. Biometrijska identifikacija koristi fizičke i ponašajne osobine osobe za prepoznavanje njenih biometrijskih karakteristika i upoređivanje istih sa uzorkom prethodno sačuvanim u bazi podataka. Biometrijski sistem se sastoji od ulazne jedinice, ekstraktora, baze podataka i jedinice za verifikaciju i poređenje. Metode telesne biometrije zasnivaju se na individualnosti i nepromenljivosti dimenzija pojedinih delova ljudskog tela i njihovih međusobnih odnosa [2]. U savremenom svetu, pouzdana zaštita sigurnosti osoba, predmeta i sistema je imperativ. To uključuje zaštitu ličnih računara, mobilnih uređaja, motornih vozila, mašina i drugih vrednih predmeta od neovlašćene upotrebe ili pristupa, krađe i falsifikovanja prilikom finansijskih transakcija, pristup radnim mestima i skladištima povećane sigurnosti, kao i proveru identiteta u ličnim dokumentima [11]. Biometrijske metode identifikacije postale su najpouzdanije i najprimenljivije metode identifikacije.

3. SOFT BIOMETRIJSKA AUTENTIFIKACIJA

Soft biometrijska autentifikacija predstavlja jedan od najnovijih pristupa u oblasti biometrije koji omogućava autentifikaciju korisnika korišćenjem različitih karakteristika osim fizičkih, kao što su ponašanje, socijalni i emocionalni obrasci [1]. Ova tehnologija se koristi u cilju poboljšanja sigurnosti, praktičnosti i udobnosti korisnika. Ključna prednost soft biometrijske autentifikacije jeste mogućnost da se obavlja u pozadini, bez ometanja korisnika, čime se smanjuje mogućnost krađe identiteta i drugih zloupotreba. Takođe, ova tehnologija pruža fleksibilnost, jer se može prilagoditi različitim aplikacijama i uređajima, uključujući pametne telefone, tablete i računare. Međutim, kao i sa svim tehnologijama, postoje i određeni izazovi koji se odnose na soft biometrijsku autentifikaciju, kao što su pouzdanost i privatnost. Neke karakteristike, poput emocionalnih obrasci, mogu biti teško merljive i često podložne promenama. Takođe, potrebno je osigurati da se informacije prikupljene tokom procesa autentifikacije čuvaju sigurno i da se koriste samo u svrhu autentifikacije. Soft biometrijska autentifikacija predstavlja značajan napredak u oblasti biometrije i obećava poboljšanje sigurnosti i praktičnosti korišćenja različitih aplikacija i uređaja. Soft biometrijska autentifikacija se oslanja na ponašajne, emocionalne i socijalne obrazce kako bi identifikovala korisnika. Korišćenje ovih obrazaca pruža dodatni nivo sigurnosti i smanjuje mogućnost zloupotrebe sistema [6]. Tehnologije koje se najčešće koriste u soft biometrijskoj autentifikaciji uključuju analizu obrasca kucanja, prepoznavanje glasa, prepoznavanje lica, analizu obrasca ponašanja kao i tehnologija prepoznavanja otiska prsta [11]. Ove tehnologije mogu se primenjivati nezavisno ili u kombinaciji sa drugim metodama autentifikacije, kao što su lozinke ili čip kartice, kako bi se povećao nivo sigurnosti. Soft biometrijska autentifikacija sve više dobija na značaju u svetu tehnologije, jer omogućava jednostavniju i sigurniju identifikaciju korisnika u digitalnom svetu. Postoje raznovrsne karakteristike koje se mogu iskoristiti za soft biometrijsku autentifikaciju.

Socijalni obrazac

Socijalni obrazac u soft biometrijskoj autentifikaciji se odnosi na karakteristike ponašanja korisnika na društvenim mrežama, aplikacijama i drugim internet platformama koje mogu biti korišćene kao dodatni faktor za autentifikaciju. Ove karakteristike uključuju preferencije pregledavanja, obrasce korišćenja, interakciju sa drugim korisnicima i drugo [7]. Jedan primer socijalnog obrasca koji se može koristiti u soft biometrijskoj autentifikaciji je način na koji korisnik pregledava internet stranice. Na primer, neki korisnici mogu više vremena provoditi na određenim vrstama sadržaja, kao što su vesti, dok drugi korisnici više vremena provode na društvenim mrežama. Ova preferencija pregledavanja može se koristiti kao način autentifikacije, pored drugih metoda kao što su lozinke, otisci prstiju i drugo. Jedna od prednosti korišćenja socijalnog obrasca u soft biometrijskoj autentifikaciji je to što se ova karakteristika može lako pratiti i analizirati putem softverskih alata za praćenje aktivnosti korisnika. Ovo omogućava jednostavniju autentifikaciju korisnika bez potrebe za dodatnim hardverskim uređajima. Pored toga, socijalni obrasci mogu pružiti dodatni sloj sigurnosti, posebno ako se koriste u kombinaciji sa drugim oblicima autentifikacije. Međutim, postoji i nekoliko nedostataka korišćenja socijalnog obrasca u soft biometrijskoj autentifikaciji. Na primer, neki korisnici mogu imati različite obrasce ponašanja u različitim vremenima, u zavisnosti od situacije u kojoj se nalaze. Takođe, neki korisnici mogu aktivno pokušavati da izmene svoj socijalni obrazac kako bi zaobišli sistem autentifikacije[10]. Socijalni obrazac predstavlja značajnu karakteristiku u soft biometrijskoj autentifikaciji, koja može pružiti dodatni sloj sigurnosti i olakšati autentifikaciju korisnika. Međutim, potrebno je uzeti u obzir i nedostatke i pažljivo prilagoditi korišćenje socijalnog obrasca u zavisnosti od specifičnih potreba korisnika i sistema autentifikacije.

Ponašanje korisnika na internetu

Način na koji korisnik koristi internet i interaguje sa digitalnim uređajima može biti jedinstven za svakog korisnika. Ovo ponašanje korisnika može biti praćeno i analizirano korišćenjem različitih tehnologija poput softverskih alata za analizu ponašanja korisnika. Na primer, softver može pratiti način na koji korisnik klikće na dugmad, kako pomeraju miš, koliko vremena provode na pojedinim stranicama ili koliko dugo koriste različite aplikacije[6]. Ove informacije mogu da se koristite za autentifikaciju korisnika. Na primer, ako se korisnik prijavi na račun sa novog uređaja ili sa nove lokacije, softver može uporediti način ponašanja korisnika sa prethodnim navikama korišćenja interneta. Ako se način ponašanja korisnika ne poklapa sa prethodnim navikama, softver bi mogao da upozori na moguću prevaru ili da traži dodatnu autentifikaciju, kao što je unos lozinke ili koda za potvrdu. Važno je napomenuti da ponašanje korisnika ne bi trebalo da bude jedina karakteristika koja se koristi za autentifikaciju, jer se navike korišćenja interneta i digitalnih uređaja mogu promeniti tokom vremena. Međutim, ova karakteristika može biti korisna u kombinaciji sa drugim karakteristikama soft biometrijske autentifikacije za jačanje sigurnosti pri autentifikaciji korisnika.

Emocionalni obrazac

Emocionalni uzorak u soft biometrijskoj autentifikaciji se odnosi na analizu emocionalnog stanja korisnika kao faktora autentifikacije. Ovaj uzorak koristi senzore za merenje bioloških reakcija korisnika, kao što su brzina otkucaja srca, nivo znoja, izraz lica i druge parametre, kako bi se utvrdilo da li se korisnik koji se prijavljuje poklapa sa onim koji se autentifikuje. Primeri emocionalnog obrasca u soft biometrijskoj autentifikaciji uključuju analizu govora i gestova korisnika, analizu facijalnih karakteristika i praćenje očiju kako bi se utvrdio nivo pažnje korisnika i njegov emocionalni odgovor na datu situaciju [7]. Prednosti korišćenja emocionalnog obrasca u soft biometrijskoj autentifikaciji su to što se mogu koristiti kao dodatni sloj sigurnosti u kombinaciji sa drugim oblicima biometrijske autentifikacije. Takođe, oni su korisni u situacijama gde je potrebna brza autentifikacija bez potrebe za dodatnom opremom, poput senzora otiska prsta ili skenera lica. Nedostaci emocionalnog obrasca u soft biometrijskoj autentifikaciji mogu biti povezani sa nesavršenošću tehnologije, kao i sa individualnim varijacijama u emocionalnom odgovoru korisnika. Takođe, neki korisnici mogu biti osetljivi na otkrivanje svojih emocija putem senzora, što može uticati na njihovu spremnost da koriste ovaj obrazac autentifikacije.

Analiza glasa

Biometrijski sistem govora je vrsta softverskog biometrijskog sistema koji koristi karakteristike govora za identifikaciju ili autentifikaciju korisnika. Prepoznavanje glasa koristeći tehnologije kao što su govorni prepoznavači i modeli dubokog učenja. Glas, odnosno obrazac govora, može biti korišćen kao karakteristika soft biometrijske autentifikacije. Svaki govornik ima jedinstvenu karakteristiku u načinu na koji izgovara reči, što se naziva vokalnim potpisom. Vokalni potpis se zasniva na karakteristikama kao što su ton glasa, brzina govora, ritam, naglašavanje reči i slično [5]. Sistem biometrijske autentifikacije zasnovan na glasu koristi različite tehnike za prepoznavanje vokalnog potpisa. Najčešće se primenjuje tehnologija automatskog prepoznavanja govora (ASR) koja se zasniva na prepoznavanju zvukova koji formiraju reči. ASR tehnologija analizira vokalne karakteristike korisnika i upoređuje ih sa prethodno snimljenim uzorcima glasa korisnika, kako bi se utvrdilo da li je korisnik legitimni ili ne. Osim ASR tehnologije, postoje i druge tehnike za prepoznavanje vokalnog potpisa, kao što su tehnike zasnovane na analizi govornog spektra ili tehnike zasnovane na analizi vokalnih odlika kao što su formantne frekvencije [7]. Međutim, postoji i nekoliko izazova u primeni tehnologija za prepoznavanje vokalnog potpisa. Na primer, moguće je da se kvalitet snimka razlikuje u zavisnosti od uređaja na kojem se vrši snimanje, što može uticati na tačnost prepoznavanja. Takođe, neki ljudi mogu imati problema sa govorom ili mogu govoriti različitim jezicima, što takođe može uticati na tačnost prepoznavanja.

Brzina i ritam otkucaja srca

Brzina i ritam otkucaja srca mogu biti iskorišćeni kao karakteristike soft biometrijske autentifikacije. Svaka osoba ima jedinstvenu brzinu otkucaja srca i ritam koji se može koristiti za autentifikaciju korisnika. Kod soft biometrijske autentifikacije putem brzine i ritma otkucaja srca, korisnik će nositi senzore koji će pratiti brzinu i ritam otkucaja srca. Ove karakteristike se zatim mogu koristiti za utvrđivanje identiteta korisnika i autentifikaciju korisnika, uz visok nivo pouzdanosti [10]. Postoji nekoliko prednosti korišćenja brzine i ritma otkucaja srca kao karakteristike soft biometrijske autentifikacije. Na primer, ovaj metod autentifikacije je vrlo pouzdan, jer su karakteristike srčanog ritma jedinstvene za svaku osobu i teško ih je falsifikovati. Osim toga, ova karakteristika ne zahteva nikakve dodatne uređaje, osim senzora koji mogu biti integrisani u pametne satove, narukvice i druge uređaje.Od nedostataka navodimo na primer, senzori koji se primenjuju za merenje ove karakteristike mogu biti skupi i neudobni za nošenje, što može smanjiti prihvatljivost ovog metoda autentifikacije kod korisnika. Takođe, neki korisnici mogu biti zabrinuti zbog privatnosti i sigurnosti podataka o brzini i ritmu otkucaja srca, što može smanjiti njihovu spremnost za korišćenje ovog metoda autentifikacije.

Ponašajni obrazac

Ponašajni obrazac u soft biometrijskoj autentifikaciji odnosi se na jedinstveni način na koji korisnik koristi uređaj i interaguje s njim, kao i na specifičan stil korišćenja različitih funkcija uređaja. Ovo obuhvata karakteristike kao što su brzina kucanja, način na koji korisnik drži uređaj, brzinu skrolovanja ekrana i slično. Ove karakteristike mogu biti prilično jedinstvene za svakog pojedinca, što omogućava da se koriste kao faktor autentifikacije. Primeri ponašajnog obrasca u soft biometrijskoj autentifikaciji uključuju jedinstvene obrasce kucanja na tastaturi, način na koji se korisnik kreće kroz menije na ekranu, brzinu pritiska na ekran, brzinu otvaranja aplikacija i slično [9]. Prednosti korišćenja ponašajnog obrasca u soft biometrijskoj autentifikaciji uključuju činjenicu da se ne zahteva dodatna oprema poput senzora otiska prsta, što može smanjiti troškove i poboljšati praktičnost autentifikacije. Osim toga, ponašajni obrazac je teško falsifikovati i lako se može koristiti kao dodatni faktor autentifikacije. Nedostaci korišćenja ponašajnog obrasca u soft biometrijskoj autentifikaciji uključuju činjenicu da neki korisnici mogu imati promenjive obrasce ponašanja, što može dovesti do pogrešnih autentifikacija ili odbijanja pristupa. Takođe, mogućnost lažiranja ponašajnog obrasca postoji i može se koristiti za prevaru sistema autentifikacije.

Obrasci kucanja na tastaturi

Obrasci kucanja na tastaturi su jedna od karakteristika soft biometrijske autentifikacije koja se može koristiti za identifikaciju i autentifikaciju korisnika. Svaki korisnik ima jedinstven način kucanja na tastaturi, koji se može koristiti za autentifikaciju korisnika sa visokim stepenom pouzdanosti [7]. Kod soft biometrijske autentifikacije putem obrasca kucanja na tastaturi, softver za autentifikaciju snima karakteristike kretanja prstiju koje korisnik ostvaruje tokom kucanja na tastaturi. Ove karakteristike se zatim mogu uporediti sa prethodno registrovanim karakteristikama kucanja na tastaturi kako bi se utvrdila autentičnost korisnika. Postoji nekoliko prednosti korišćenja obrasci kucanja na tastaturi kao karakteristike soft biometrijske autentifikacije. Na primer, ovaj metod autentifikacije je vrlo prijatan za korisnika, jer se proces autentifikacije odvija tokom normalnog korišćenja računara. Osim toga, ovaj metod autentifikacije ne zahteva nikakve dodatne uređaje ili posebnu obuku korisnika, što je čini veoma praktičnom za upotrebu.Od nedostataka navodimo da ovaj metod autentifikacije nije uvek dovoljno precizan, jer se karakteristike kretanja prstiju mogu razlikovati u zavisnosti od okolnosti, kao što su umor, stres ili druge fizičke ili emocionalne faktore. Osim toga, ovaj metod autentifikacije nije jednako efikasan kao drugi metodi kada se koristi sa više korisnika na jednom računaru, jer se karakteristike kucanja na tastaturi mogu mešati i preklapati između različitih korisnika.

Obrazci pisanja

Potpis se može koristiti kao karakteristika soft biometrijske autentifikacije. Svaki potpis ima jedinstvene karakteristike, kao što su pritisak olovke, brzina pisanja, stil pisanja i druge specifičnosti. Ove karakteristike potpisa mogu se iskoristiti za autentifikaciju korisnika, čak i kada korisnik koristi različite uređaje ili računarske mreže. Kod soft biometrijske autentifikacije putem potpisa, korisnik će u procesu autentifikacije morati potpisati digitalni dokument, a zatim će se karakteristike njegovog potpisa uporediti sa prethodnim potpisima koje je korisnik napravio [7]. Navedene karakteristike mogu se is koristiti za utvrđivanje identiteta korisnika i autentifikaciju korisnika, uz visok nivo pouzdanosti. Postoji nekoliko prednosti korišćenja potpisa kao karakteristike soft biometrijske autentifikacije. Na primer, proces potpisivanja je relativno jednostavan i ne zahteva nikakve dodatne uređaje, već samo digitalnu olovku ili ekran na kome korisnik može da potpiše dokument. Osim toga, potpisivanje se često koristi za zakonski važne dokumente, pa se stoga može koristiti i za autentifikaciju. Nedostaci su da se potpis može lako falsifikovati, što može dovesti do neovlašćenog pristupa nečijem računu. Takođe, potrebno je uzeti u obzir da se karakteristike potpisa mogu promeniti tokom vremena, zbog čega se proces autentifikacije putem potpisa može pokazati manje pouzdanim za razliku od drugih karakteristika [5].

4. BEZBEDNOST I PRIVATNOST U SOFT BIOMETRIJSKOJ AUTENTIFIKACIJI

Soft biometrijska autentifikacija donosi nove mogućnosti u oblasti autentifikacije, ali sa sobom nosi i određene rizike. Korišćenje ovakve tehnologije može dovesti do potencijalnih problema sa sigurnošću i privatnošću podataka korisnika. Rizici korišćenja soft biometrijske autentifikacije uključuju mogućnost krađe biometrijskih podataka, zloupotrebu istih, kao i potencijalnu povredu privatnosti korisnika. Takođe, moguće su greške u identifikaciji, što može dovesti do problema sa pristupom korisničkim računima. Kako bi se smanjili ovi rizici, preduzimaju se određene mere. Jedna od njih je enkripcija biometrijskih podataka kako bi se sprečio neovlašćeni pristup istima [11]. Takođe, podaci se čuvaju na sigurnim serverima i pristup istima je moguć samo uz odgovarajuće ovlašćenje. Isto tako, korisnici treba da budu upoznati sa načinom na koji se njihovi biometrijski podaci koriste i obrađuju, a treba im pružiti i mogućnost da kontrolišu svoje podatke i da odluče koji će biti korišćeni za autentifikaciju [6]. U cilju smanjenja grešaka u identifikaciji, koriste se različiti algoritmi koji mogu prepoznati nepravilnosti u uzorcima biometrijskih podataka. Takođe, koriste se višestruki faktori autentifikacije kako bi se smanjila mogućnost zloupotrebe podataka.

Međutim, upotreba soft biometrije podrazumeva i brojne izazove u pogledu privatnosti i bezbednosti korisnika [1]. Prvo, prikupljanje i obrada biometrijskih podataka podrazumeva rizik od krađe identiteta i zloupotrebe podataka. Stoga, organizacije koje koriste soft biometriju moraju imati jasnu politiku privatnosti i postupak zaštite podataka. Drugo, soft biometrija podrazumeva neprekidnu prikupljanje podataka o korisniku, što može predstavljati ozbiljan rizik za njihovu privatnost. Na primer, analiza obrasca kucanja može otkriti detalje o korisnikovom zdravstvenom stanju ili emocionalnom stanju. Stoga, organizacije koje koriste soft biometriju moraju osigurati da se prikupljeni podaci koriste samo u svrhu autentifikacije, a ne za bilo koju drugu svrhu. Treće, soft biometrijska autentifikacija podrazumeva korišćenje algoritama koji obrađuju i porede biometrijske podatke korisnika. Međutim, ovi algoritmi mogu biti skloni greškama i diskriminaciji, posebno prema određenim grupama ljudi, kao što su starije osobe ili osobe sa invaliditetom. Stoga, organizacije koje koriste soft biometriju moraju osigurati da su algoritmi pravični i da ne diskriminišu određene grupe ljudi. Takođe, soft biometrija može se primenjivati u kombinaciji sa drugim metodama autentifikacije, poput lozinki ili čip kartica. Međutim, ovo može dovesti do rizika u pogledu bezbednosti, ako se jedan od metoda autentifikacije kompromituje. Na primer, ako korisnik izgubi svoju čip karticu, neko drugi može koristiti soft biometriju da bi pristupio njihovom računu. Zbog toga, organizacije koje koriste soft biometriju u kombinaciji sa drugim metodama autentifikacije moraju se pobrinuti da su svi metodi autentifikacije sigurni i pouzdani [3].Bezbednost i privatnost u soft biometrijskoj autentifikaciji su od velike važnosti kako bi se korisnicima pružio siguran i pouzdan način autentifikacije, koji će istovremeno zaštititi njihove podatke i privatnost. U mnogim zemljama postoje zakonska ograničenja u pogledu korišćenja biometrijskih podataka, zbog pitanja privatnosti i bezbednosti. Iako postoje navedeni nedostaci, primena soft biometrijske autentifikacije sve više raste, a očekuje se da će se dalje proširivati u budućnosti.

5. ZAKLJUČAK

Soft biometrijska autentifikacija predstavlja inovativan pristup autentifikaciji korisnika koji se bazira na neinvazivnom prikupljanju i analizi biometrijskih podataka koji se ne odnose direktno na fizičke karakteristike korisnika. U ovom radu su detaljno opisani socijalni, emocionalni i ponašajni obrasci koji se koriste u soft biometrijskoj autentifikaciji, kao i tehnologije koje se koriste za njihovo prikupljanje i analizu. Značaj soft biometrijske autentifikacije ogleda se u mogućnosti da se prevaziđu ograničenja tradicionalne autentifikacije koja se bazira na fizičkim karakteristikama korisnika. Zahvaljujući napretku tehnologije i razvoju veštačke inteligencije, soft biometrijska autentifikacija ima potencijal da se dalje razvija i poboljšava u budućnosti. Međutim, postoji i nekoliko nedostataka u korišćenju soft biometrijske autentifikacije, kao što su niski nivoi pouzdanosti u nekim situacijama, rizici od krađe identiteta, i nedostatak standardizacije u prikupljanju i obradi biometrijskih podataka. Potrebno je nastaviti sa istraživanjem i razvojem soft biometrijske autentifikacije kako bi se prevazišli ovi nedostaci i osigurala maksimalna bezbednost i privatnost korisnika.U budućnosti, istraživači mogu razvijati nove tehnologije i metode za prikupljanje i analizu biometrijskih podataka, a takođe je važno uspostaviti standarde i smernice za korišćenje soft biometrijske autentifikacije u različitim sektorima. Kao jedan od najnovijih i najperspektivnijih pristupa autentifikaciji korisnika, soft biometrijska autentifikacija će nastaviti da privlači pažnju istraživača i da se dalje razvija u budućnosti. Soft biometrija je efikasan način autentifikacije korisnika u digitalnom svetu.

LITERATURA

Ashbourn, J. (2000). Biometrics: Advanced Identity Verification: The Complete Guide, Springer-Verlag, London,

Bigun, J., Fierrez, J., & Ortega-Garcia, J. (2009)."Biometrics and Identity Management", Springer,

Islam, M. T., & Kabir, A. B. M. A. H. (2019). "Soft Biometric Traits in Multimodal Biometric Systems: A Survey", Journal of Information Processing Systems, vol. 15, no. 2, pp. 327-356,

Iyengar, S. S., & Singh, S. K. (2018). "Behavioral Biometrics: A Comprehensive Survey", ACM Computing Surveys, vol. 51, no. 2, pp. 1-36,

Li, B., Xiong, X., & Noman, A. N. M. (2018). "Soft Biometrics: A New Approach to Enhance User Authentication", Future Internet, vol. 10, no. 1, pp. 1-16,

Patil, P. R., Karode, A. H., & Suralkar, D. S. R. (2017). Human skin detection using image fusion. International Journal of Electronics and Communication Engineering and Technology, 8(4), 13–21.

Rajasekar, V., Saračević, M., Hassaballah, M., Karabasevic, D., Stanujkic, D., Zajmovic, M., Tariq, U., Jayapaul, P. (2002). Efficient Multimodal Biometric Recognition for Secure Authentication Based on Deep Learning Approach, International Journal on Artificial Intelligence Tools, World Scientific.

Rhien-Lien, H., Mohamed Abdel - Mottabel, & Jain, A. K.. (2002). “Face Detection in Color Images”, IEEE Trans. Pattern Analysis and Machine Intelligence, vol. 24, no. 5, pp. 696.706, May

Schneider, J., Franke, K., & Nickolay, B. (2000). Konzeptstudie - Biometrische Authentifikation. Technical report, Fraunhofer IPK Berlin, (in German).

Sobabe, A.-A., Djara, T., & Vianou, A. (2019). A Framework for Combination of Sequential Architecture and Soft Biometrics in Multibiometric Scores Fusion [Conference paper] 3rd International Conference on Bio-engineering for Smart Technologies, Paris, France. https://ieeexplore.ieee.org/abstract/document/8734247 .

Yan, J., Ross, A., & Noman, A. N. M. (2012). "Soft Biometrics for Personal Recognition Systems: A Survey", IEEE Transactions on Systems, Man, and Cybernetics, Part C ,vol. 42, no. 6, pp. 1241-1251,