
UPORABA BIOMETRIJE V VSAKDANJEM ŽIVLJENJU

UVOD

V modernem svetu je zanesljivo varovanje ena od najbolj zaželenih dobrin. Brez zanesljivega varovanja so ogrožene številne vsakdanje aktivnosti, kot na primer:

- Zaščita osebnih računalnikov, prenosnih računalnikov, mobilnih telefonov, internetnih storitev in podobnih pripomočkov pred uporabo nepooblaščenih oseb
- Zaščita motornih vozil, strojev in drugih vrednih predmetov pred nepooblaščenno uporabo ali dostopom
- Preprečevanje tatvine in poneverb pri finančnih transakcijah, še posebno elektronskih storitev, vključujoč plačila s kreditnimi karticami in plačili preko interneta
- Omogočanje dostopa do delovnih mest, skladišč in področij povišane varnosti, kot tudi vojaških področij, izključno pooblaščenim osebam
- Nadzor dostopa do storitev javnega prevoza, posebno v zračnem prometu
- Preverjanje identitete posameznika v vozniškem dovoljenju, kartici zdravstvenega zavarovanja, osebni izkaznici in podobnih dokumentih

Pomemben dejavnik pri zagotavljanju varnosti je identifikacija osebe ali pa preverjanje, če je oseba res ta, za katero se izdaja. Preverjanje mora biti zanesljivo, hitro, da ne posega v telo in za primerno ceno. V preteklosti je tovrstno preverjanje temeljilo na varnostnih karticah, obeskih, geslih, PIN kodah, podpisih ali celo na prepoznavanju osebe s strani varnostnika ali vratarja. Vsi ti načini so glede na zahteve v modernem svetu, postali nezanesljivi in zelo omejeni. Bodočnost je na strani *biometrije*. Biometrija nudi enostavno, zanesljivo in cenovno ugodno rešitev pri preverjanju identitete uporabnikov, ki jo lahko uporabimo tudi v nenadzorovanih in oddaljenih področjih.

Biometrični način identifikacije posameznika, pomeni individualno obravnavanje človekovih fizičnih lastnosti ali značilnosti obnašanja in zajem ter shranjevanje tega vzorca (imenovan tudi *živi vzorec*), v standardni podatkovni obliki. Ta vzorec se v postopku identifikacije primerja z vzorcem (imenovan tudi *shranjeni vzorec* ali *podpis*), ki temelji na istih značilnostih in je shranjen v varnostnem sistemu. Primerjava obeh vzorcev potrdi ali zavrže identiteto posameznika.

Pri tovrstni identifikaciji je pozornost usmerjena na majhno število fizičnih značilnosti, ki so lastne izključno eni osebi. Mednje spadajo barva glasu, način hoje, značilnosti obraza, vzorec šarenice, odtis dlani in prstov. (DNK pri tem ni vključena, ker je vzorčenje DNK počasno in pomeni poseg v telo) Najbolj dozorel, napreden in najrazvitejši način je preverjanje na osnovi prstnih odtisov.

Dolgoletne raziskave in izkušnje nam kažejo, da so prstni odtisi trenutno najzanesljivejši način preverjanja identitete oseb. Kljub nekaterim sodnim procesom v ZDA, so prstni odtisi še vedno nedvomen dokaz identitete posameznika. Večina današnjih biometričnih sistemov temelji na prepoznavanju prstnih odtisov.

Fiziološko je prstni odtis konfiguracija *grebenov* s porami, ki jih delijo *doline*. Ležijo na ožilju, neposredno pod kožo. Morfologija (oblika) prstnega odtisa je povezana s specifičnimi električnimi in toplotnimi značilnostmi kože. To pomeni, da svetlobo, toploto ali električno napetost (ali kombinacijo vseh) lahko uporabimo za zajem podobe prstnega odtisa. Prstni odtis nastane že pri razvoju zarodka in se ne spremeni s starostjo osebe, temveč raste v svoji prvotni obliki in po končani rasti osebe ostane v svoji velikosti nespremenjen. Prav tako se po poškodbi obnovi v prvotno obliko. Enojajčni dvojčki nimajo enakih prstnih odtisov.

Majhen odstotek populacije (npr. rudarji in majhno število glasbenikov) ima prstne odtise, zaradi stalnega trenja, poškodovane. V razvitih državah je ta odstotek zanemarljiv in ne predstavlja omembe vredne težave za identifikacijske sisteme, ki temeljijo na prstnih odtisih.

Za zajem značilnosti vzorca prstnega odtisa, obstaja več algoritemskih metod.



Najbolj razširjene metode temeljijo na *prepoznavanju vzorca* ali izvlečku *minucij*. V primeru algoritmov, ki temeljijo na minucijah, je prstni odtis sestavljen iz grobih značilnosti, kot so *loki*, *zanke* in *zasuki*, ter drobnih značilnosti (minucije) kot so predvsem *bifurkacije* (razdelitve), *delt*e (združevanja v obliki črke Y) in *zaključki* grebenov. Prstni odtis ima med 30 in 40 minucij. Značilnost vsake od njih je položaj (koordinate), tip (bifurkacija, delta ali zaključek) in usmerjenost (orientacija). Skupek značilnosti minucij lahko da predlogo za prstni odtis. Če so značilnosti natančno zajete, je možnost, da bi imela dva prstna odtisa enake značilnosti, izjemno nizka.

Slika 1. Minucije tipičnega prstnega odtisa

Elektronski zajem slik in algoritmi za razpoznavanje vzorcev, so danes dovolj razviti, da vzorec prstnega odtisa avtomatsko obdelajo in shranijo. V več primerih za ta postopek obstojajo tudi standardi. Ti standardi obstojajo za vzorce, ki temeljijo na minucijah. Najbolj uporabljan je standard, ki ga v ZDA predpisuje NIST (National Institute of Standards and Technology). Kljub temu je oklepanje standardov ovira za fleksibilnost razvijalcev algoritmov in omejuje njihovo intelektualno lastnino. Tako naletimo na razkorak med oklepanjem standarda in med natančnostjo in hitrostjo, ko gre za standardizacijo procesa.

TEHNOLOGIJE ČITALCEV PRSTNIH ODTISOV

Za zajem prstnih odtisov, so na trgu številne tehnologije. Najbolj znane so; optična, kapacitivna, radijska, tehnologija tlaka, mikro-elektro-mehanična in toplotna.

Optična

Za odčitavanje podobe prstnega odtisa so uporabljene digitalne kamere. Prst položimo na ustrezno osvetljeno stekleno ploščo. Za približanje objekta snemanja služijo posebne leče. Slika je zajeta z CMOS ali CCD množico točk, ustrezne ločljivosti in spremenjena v sive odtenke (od 2 do 16 tonov). Pomanjkljivost te tehnike je prstni odtis, ki ostane na stekleni plošči in ga lahko ponovno uporabimo (zlorabimo) in dejstvo izredno težavnega razločevanja med živim prstom in dobro oblikovano imitacijo.

Kapacitivna

Ko položimo prst na množico točk, občutljivih na spremembe električne napetosti, se razlike v napetosti med grebeni (pretežno voda) in dolinami (pretežno zrak) zapišejo kot slika. Kljub občutljivosti tega načina na elektrostatične motnje v okolju in ostala električna polja, je ta tehnika ena od najbolj razširjenih. Prav tako jo je dokaj enostavno zaobiti z imitacijami prstov in latentnimi odtisi.

Radijska

Če prst obsevamo z radijskimi valovi nizke intenzitete, deluje kot oddajnik in razlike v oddaljenosti med grebeni in dolinami so razpoznavne kot množica ustrezno usmerjenih točkovnih anten. Prst mora biti v stiku z oddajno površino senzorja. Ker ta način temelji na fizioloških značilnostih kože, je radijski senzor težko prevarati z umetnim prstom. Slaba točka te tehnike je stik med prstom in oddajnim obročem, ki lahko postane neprijetno vroč.

Tlačna

Točkovna množica, občutljiva na tlak, je sestavljena iz piezo-električnih elementov, ki zajemajo vzorec grebenov, ko nanjo položimo prstni odtis. Kljub številnim pomanjkljivostim te tehnike (slaba občutljivost, nezmožnost razlikovanja med pravim in umetnim prstom, občutljivost na premočan pritisk) kar nekaj proizvajalcev razvija prototipe.

Mikro-elektro-mehanična

Mikro-elektro-mehanična metoda je ostala na stopnji med raziskavo in razvojem ter med uporabo v različnih aplikacijah. V laboratorijih so naredili množico mikro-mehaničnih tipal, ki zaznavajo grebene in doline prstnega odtisa, vendar ne morejo zagotoviti robustnosti in široke uporabnosti. Prav tako je nemogoče ločevanje med živim prstom in imitacijo.

Termična

Piro-električni material lahko razliko v temperaturi spremeni v določeno napetost. Ta način je zelo razširjen in je uporabljen tudi v infrardečih kamerah. Termični čitalec prstnega odtisa, ki temelji na uporabi tega materiala, meri temperaturno razliko med točkami, ki so v stiku (grebeni) in med tistimi, ki niso (doline).

Termični pristop ima številne prednosti. To je neobčutljivost na statično elektriko in odsotnost signala poslanega iz čitalca na prst. Termični način deluje tako v skrajnih, kot v normalnih temperaturnih pogojih. Prav tako je praktično nemogoča zamenjava živega prsta z imitacijo.

Slabost termičnega načina je, da slika hitro izgine. Ko prst položimo na senzor, je v začetku velika razlika v temperaturi, vendar že po kratkem času (manj kot ena sekunda) slika izgine, ker se temperatura izenači. To je tudi eden od razlogov, zakaj se uporablja način zajema slike, opisan v nadaljevanju.

Statična ali odčitavana slika

Večino zgoraj opisanih tehnik lahko uporabljamo na dva načina. *Kot statično sliko*, ki jo zajemamo na okencu enake velikosti kot je prstni odtis tako, da na površino pritisnemo prst za toliko časa, kolikor je potrebno za zajem slike. Prednost te tehnike je, da zajame celotno sliko v enem koraku. Pomembna pomanjkljivost pa je velikost čitalca in dejstvo, da na površini čitalca ostane prstni odtis. Drugi način je uporaba pravokotnega okenca širine enake širini slike in le nekaj točk višine, preko katerega navpično potegnemo s prstom. Ta način zahteva, da sliko zajemamo sekcijsko in jo programska oprema rekonstruira v celoto. Prednost je gotovo v majhnosti, stabilnosti slike zaradi termičnega odčitavanja in dejstvu, da je čitalec samočistilen. Na njem ne ostajajo latentni odtisi. Zaradi kratke obstojnosti termične razlike, je to tudi edina metoda, ki jo lahko uporabimo pri termičnih čitalcih.

NAČINI PREPOZNAVANJA PRSTNIH ODTISOV

Prepoznavanje prstnih odtisov lahko uporabljamo v zelo velikem številu različnih aplikacij, vendar vse zahtevajo osnoven postopek. Ta ni odvisen od tehnologije, uporabljene za zajem slike ali pa od programske opreme namenjene obdelavi, shranjevanju in primerjanju vzorcev.

Registracija in primerjanje

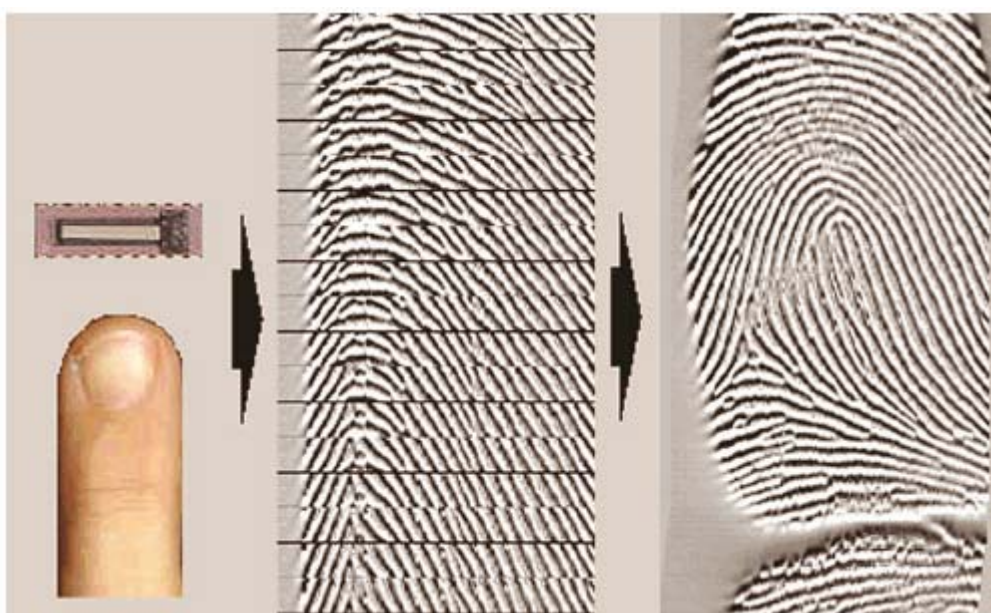
Kot začetni korak, je potrebno *registrirati* prstne odtise oseb. Registracija je sestavljena iz zajema in shranjevanja vzorčnega prstnega odtisa določene osebe. Ni potrebno omenjati, da je postopek potrebno opraviti v ustrezno varovanem okolju. Odvzet prstni odtis ali zbir izvlečka podatkov o prstnem odtisu, se imenuje *predloga* (tudi *registrirana predloga*) osebe. Med delovanjem sistema, čitalci prstnih odtisov, podatke ali *vzorke* (tudi *vzorčena predloga*) zajemajo in obdelujejo tako kot med registracijo. Programska oprema vzorec primerja s predlogo ali s predlogami. Če sta skladna, je s tem potrjena istovetnost (identifikacija) osebe. (če vzorec primerjamo z eno predlogo, npr. pri potrditvi istovetnosti uporabnika pametne kartice, se proces imenuje avtentifikacija ali ugotavljanje pristnosti).

Zajem slike

Je pridobivanje točkovne slike celotnega prstnega odtisa, ob ustrezni ločljivosti. Se- stavljena je iz sosledja vodoravnih okvirov velikosti 8 x 280 pixel pri 4-bit ločljivosti.

Rekonstrukcija slike

Ob predpostavki, da je bilo preko čitalca s prstom potegnjeno v razumnem času, prekrivanje sledečih se slik omogoča rekonstrukcijo slike prstnega odtisa. Slika 2. Programska oprema, potrebna za rekonstrukcijo, je že vgrajena v čitalcu. Rekonstruirana slika ima ločljivost 8-bit, zaradi izboljšanja ločljivosti med rekonstrukcijo okvirjev, kar je skladno z FBI IQS specifikacijami.



Slika 2. Rekonstrukcija slike prstnega odtisa

Izvleček predloge ali vzorca

Zaradi varnostnih razlogov, kot tudi zaradi velikosti in omejitev podatkovne baze, ni primerno shranjevanje slik celotnih prstnih odtisov. (na varovan kraj lahko sicer shranimo primerjalno sliko prstnega odtisa, vendar ta ni potrebna za delovanje sistema) Normalen postopek pomeni izvleček edinstvene *predloge* iz slike prstnega odtisa, z uporabo prepoznavanja vzorca minucij, kot že prej opisano. Med registracijo tako dobimo registrirano predlogo, med preverjanjem pa vzorčeno predlogo. Postopek je v obeh primerih enak. Za to so številni razlogi:

- tipični nabor 36 minucij, od katerih ima vsaka 4 byte, zaseda zgolj 144 byte.
- Iz predloge ne moremo rekonstruirati slike prstnega odtisa. To bistveno zmanjša možnost zlorab, poneverb, vdoru v baze podatkov ipd.
- Vzorec lahko še nadalje stiskamo z vsakim standardnim algoritmom za stiskanje podatkov. Če je potrebno, ga lahko tudi šifriramo. Ta oblika je pomembna predvsem pri uporabi čitalcev pametnih kartic, ki so opremljeni s čitalcem prstnih odtisov, kjer sta zasedanje podatkovnega prostora in varnostna stopnja, ključna dejavnika.

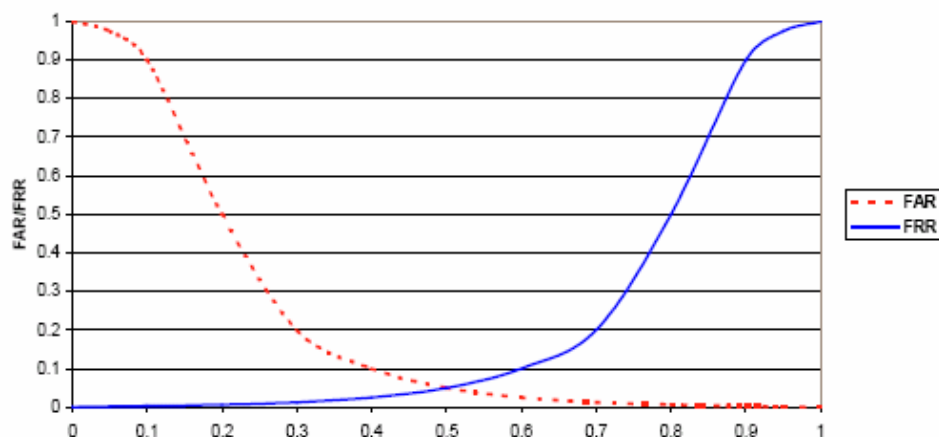
Primerjava predloge in vzorca

Zadnji korak v postopku primerjanja je primerjava vzorca z več predlogami in ugotavljanje istovetnosti (identifikacija) ali z eno predlogo in ugotavljanje pristnosti (avtentifikacija). Praktično neverjetno je, da bi se vzorec in predloga povsem skladala. Razlog temu so približki v postopku odčitavanja odtisa (pri 50 μm ločljivosti je to daleč od točnosti), zamiki slike in sam postopek izdelave izvlečka minucij. Za primerjavo predloge in vzorca uporabljamo primerjalni algoritem, ki preverja in primerja različne usmeritve slike in stopnjo skladnosti z minucijami, ter jo izrazi v številčni vrednosti ustrežanja. Nad določenim nivojem, je potrjena skladnost.

Tu nastaneta dve možni vrsti napak:

- **Napačna potrditev**, kjer neustrezen vzorec in predloga dajeta dovolj visoko vrednost, da sta označena kot skladna. To dovoljuje nepooblaščenim osebam da vstopi v sistem. Verjetnost tega dogodka določa stopnja **FAR** (False Acceptance Rate).
- **Napačna zavrnitev**, kjer ustrezen vzorec in predloga ne dajeta dovolj visoke vrednosti in sta označena kot neskladna. Zavrnitev prepreči uporabo pooblaščenim osebam. Verjetnost tega dogodka določa stopnja **FRR** (False Rejection Rate).

Presek je točka, kjer se sekata vrednosti FAR in FRR.



Slika 3. FAR/FRR in njuno presečišče

Cilj proizvajalcev sistemov čitalcev prstnih odtisov, sta čim nižji vrednosti FAR in FRR, vendar je v praksi med njima razkorak. Zmanjšanje FAR pomeni zvišanje FRR in obratno. Smislen cilj je točka, ko obe vrednosti in posledice napak, ne predstavljajo omembe vrednega ogrožanja varnosti. Posledice napačne zavrnitve (FRR) segajo od nadležnih do življenjsko nevarnih, odvisno od področja uporabe. Nekateri sistemi so dovolj napredni, da vključujejo različna varovala pred posledicami napačne zavrnitve. Npr. oseba mora ponoviti postopek odčitavanja odtisa ali pa je za isto osebo vnesenih več predlog.

Sam postopek preverjanja skladnosti predloge in vzorca je stvar programske opreme in ni odvisen od načina zajema prstnega odtisa. Kljub temu pa je visoko kvalitetna slika pogoj za čim nižjo stopnjo FAR in FRR.