Jegyzőkönyv

Biztonság és védelem az informatikában c. tárgy

4. feladat

Készítette:

Csomor Bence, TVIK4I

2021.03.10.

**Biometrikus azonosítás**

A biometrikus azonosítások, az emberi szervezet egyedi jellemzőjének felismerésén alapulnak. Ezek az arc-, hang-, írisz- retina-, kéz- és ujjlenyomat azonosítás, DNS elemzés, de ide sorolhatjuk az aláírást, amellyel nap, mint nap azonosítsuk saját magunkat.

A biometrikus azonosítási módszerek egy mintaillesztő algoritmuson alapulnak. A beléptető rendszer az adatbázisban rögzített mintát az egyén be- vagy kilépésekor összehasonlítja az aktuális adattal, vagyis felismeri azt. A megbízhatóságot ezek az úgynevezett nem átadható adatok jelentik, ezeket sem ellopni, sem elveszíteni, sem átadni nem lehet, mint egy PIN kódot, vagy beléptető kártyát. Az adatbázisban eltárolt mintasablon személyes adatnak minősül, tehát adatvédelem alatt áll. Az azonosítás sebessége az eszközök fejlődésével együtt, egyre rövidebb ideig tart.

A mobilokon és a notebookokon legelterjedt biometrikus azonosítási módszerek az arcfelismerés és az ujjlenyomat azonosítás.

*Arcfelismerés:*

Az arcfelismerés egy olyan biztonsági funkció, ami inkább kényelmi, mintsem, hogy biztonsági funkció lenne. Ez azért van mert ez a funkció, ugyan gyors és egyszerű, de ugyanakkor sokszor pontatlan és könnyen kijátszható. Az arcfelismerés 2000:1 arányban(FAR) pontatlan. További probléma lehet az arcfelismerésnél a napszemüveg, manapság a maszk viselése és legtöbbször a sötét. Ez utóbbira megoldás szokott lenni pár telefonnál az a módszer, mikor a kijelző fehér lesz és a fényerejét felviszi az arcfelismerés sikeressége érdekében. Ez a funkció minden előlapi kamerával rendelkező telefonban elérhető manapság és azokra a notebookokra is, amelyeken van kamera. Fontos kitérni arra, hogy az egy előlapi kamera könnyebben árverhető, akár egy kinyomtatott arcképpel is könnyedén feloldhatóak ezek az eszközök. A mobiltelefonok általában rendelkeznek elől is infra szenzorral, ami már nehezebben verhető át, mivel ennek segítségével az eszköz érzékelni tudja, ha egy lapos képet lát. Az IOS-es telefonokon „face ID” néven érhető el.

*Ujjlenyomat azonosítás:*

Az ujjlenyomatok terén tény, hogy barázdáltsága mindenkinek egyedi mintázatú. Tulajdonképpen ez teszi azonosításra alkalmassá. A barázdáltságot az úgynevezett fodorszálaknak köszönhetjük, amelyek a verejtékmirigyek láncolatai. Az ujjlenyomat azonosítási módszerek azonban nem ezeknek a barázdáknak a tulajdonságaira, hanem azok találkozására, elágazásaikra, csomópontjaira fókuszál.

Az ujjlenyomat azonosítására szolgáló rendszerek lényegében ezeknek a pontoknak a távolságából, elhelyezkedéséből képeznek egy úgynevezett minuta ábrát. Az egész ábrából pedig egy számot generálnak. Ezzel a számmal történik az azonosítás.

*Ujjlenyomat azonosítási technikák:*

Lényegében kétféle ujjlenyomat azonosítási technológiát alkalmaznak jelenleg: a gyakoribb módszer az ujjbarázda struktúra elemzése. Ezen felül azonban létezik az ujjlenyomat globális struktúrájának elemzése.

*Optikai szenzoros ujjlenyomat azonosítás:*

Optikai szenzor használatakor az érzékelő felületre helyezett ujjat LED világítja meg. Az ujjlenyomat képe egy prizmán és egy lencserendszeren keresztül jut el a képérzékelőhöz. Az olvasást befolyásolja az alkalmazott szűrők és érzékelő felbontása.

*Thermo szenzoros ujjlenyomat azonosítás:*

Thermo szenzoros hőmérsékletmérő pixelsorokból áll, melyek az ujj felületének redői és az alacsonyabb hőmérsékletű, völgyekben található levegő hőkülönbsége alapján rajzolja fel az ujjlenyomatot. Az ujjlenyomat érzékeléséhez az ujjat át kell húzni a szenzor felett. Érzékelő felület helyett egy csík látható és e felett kell adott irányban áthúzni az ujjat.

*Kapacitív szenzoros ujjlenyomat azonosítás:*

Amikor a kapacitív szenzor érzékelő felülete egy ujjat észlel, a felület minden pixelében megméri a kapacitást. A kapacitáskülönbségek mutatják, merre vannak az ujjlenyomatunkat alkotó egyedi redők és völgyek. Ezzel az ujjlenyomatszenzorral az olyan apró, mindennapos esetek – mint a vágás, piszok, daganat – okozta ujjlenyomat változások sem okoznak problémát.

Az ujjlenyomat alapú azonosítás egy az arcfelismerésnél már sokkal biztonságosabb módja az eszközünk biometrikus védelmére. Ennek a módszernek a hibaaránya(FAR), már 1,000,000:1 -hez, ezért személy szerint én ezt a biometrikus azonosítást preferálom eszközeimnél. Az ujjlenyomat alapú azonosítást már nehezebb átverni is, erre talán a legjobb módszer, ha a tulaj egy teljes ujjlenyomatát megtalálja az illető, aki fel akarja oldani az adott eszközt és azt egy gumikesztyűre ragasztva feloldja a telefont. Ennél az aronosításnál hátrány lehet, ha télen kesztyűt hordunk vagy ha vizes a kezünk és a kapacitív szenzoros azonosítást leszámítva a kosz és az ujjlenyomaton esett sérülések is meggátolhatják az azonosítást. Az IOS-es mobilok az utóbbi években nem bővelkedtek ujjlenyomat olvasókban. Például az iPhone 12 -ben csak a már korábban említett face ID volt elérhető.

Manapság mind az arcfelismerők, mind az ujjlenyomatolvasók igen gyorsan működnek. A különbség két eszköz feloldási ideje között körülbelül 1 másodperc szokott lenni. Általában pillanatok alatt feloldanak az eszközök ezekkel a biometrikus azonosítási módszerekkel.

Biometrikus rendszerekbiztonságának mérésére két mutatót használunk:

FAR (False Acceptance Rate):

téves elfogadási hányad (jogosultként ismer fel nem jogosult személyt).

FRR (False Rejection Rate):

téves visszautasítási hányad (nem jogosultként ismer fel jogosult személyt).

Régebben a biometrikus azonosítás nem volt biztonságos annyire, hogy az emberek nap mint nap használják, de az elmúlt 10-12 évben a technológia fejlődésével ezek a módszerek egyre gyorsabbá és pontosabbá váltak, ezért sokan használják a mindennapokban a kódok és jelszavak írogatása helyett. Egy átlagember, aki megpróbálja feltörni másnak a telefonját, az nem tud vagy nem akar belefektetni annyi erőt és időt, hogy kijátssza ezeket a rendszereket. Általában alkatrésznek adják el a lopott vagy talált telefonokat, ezért ezek a biometrikus azonosítási formák elég biztonságosnak mondhatók. Cégek és átlagemberek is szeretettel használják ezeket a módszereket. Ha egy komolyabb módszert szeretne egy vállalat a biztonságos belépésre, akkor talán a retinaazonosítás a legjobb mód erre, ugyanis ennek a módszernek a FAR mutatója már 10,000,000:1 -hez. Viszont ez az azonosítási mód nem elterjedt az átlagfelhasználók köreiben.

A mobilunkkal azonosíthatjuk magunkat például, ha egy idegen gépről lépünk be a google fiokunkba. Ez egy biztonsági funkció a google-től, nehogy észrevétlenül tudják használni a fiokunkat. Sok hasonló online rendszer használ hasonló azonosítási formákat. Ha a számítógépen jelentkezünk be az internetbankunkba, akkor általában a telefonszámunkra küldenek egy biztonsági azonosító kódot. Hasonló módon megy az HBO GO alkalmazás aktiválása okos TV-re vagy számítógépre is. Ilyenkor a mobilon meg kell nyitni az hbogo.hu/activate weboldalt ahol az eszközön látható kóddal aktiválhatjuk azt.

források: <http://www.logintrade.eu/index.php/belepteto-rendszer/biometrikus-azonositas>

<https://biometrikus.hu/mik-az-ujjlenyomat-azonositasi-pontok/>