Biometrikus azonosítás

A biometrikus azonosítás során az embert nem az azonosítja, amit tud (pl. jelszó), és nem az, hogy mije van (pl. bankkártya), hanem az ember maga (pl. az ujjlenyomata). Ebben a feladatban egy tájékoztató anyagot kell elkészítenie a biometrikus azonosításról.

1. Töltse be a szövegszerkesztőbe az ismertető szövegét az UTF-8 kódolású **bio.txt** állományból! Munkáját **biometrikus** néven mentse a program alapértelmezett formátumában! Az elkészített dokumentum ne tartalmazzon felesleges szóközöket és üres bekezdéseket!
2. A tájékoztató A4-es méretű, álló tájolású legyen, és mind a négy oldalmargót állítsa 2 cm nagyságúra!
3. A tájékoztatóban – ahol a feladat nem ír elő mást – a következő beállításokat alkalmazza!
    a. A betűtípus Times New Roman (Nimbus Roman) legyen, a betű mérete pedig 11 pontos!
    b. A bekezdések legyenek sorkizártak, alkalmazzon szimpla sorközt, a bekezdések első sora 0,8 cm-rel beljebb kezdődjön!
    c. A címet követő bevezetés, a felsorolás, a számozott lista és a tabulátorokkal kialakítandó rész kivételével a bekezdéseket 6 pontos térköz kövesse!
4. 4. A tájékoztató címe legyen 18 pontos betűméretű, az alcímek 14 pontos betűméretűek! A cím betűstílusát állítsa félkövérre, az alcímekét félkövérre és kiskapitálisra! A cím előtt ne legyen térköz, de 18 pontos térköz kövesse! Az alcímek előtt 18, az alcímek után 12 pont térköz legyen! A cím és az alcímek bal behúzását állítsa 0 cm-re!
5. A címet követő bevezető legyen dőlt betűstílusú 2 cm-es bal behúzással, bal oldalán 6 pont széles szürke vonallal! A bevezetőt követő bekezdés elé állítson be 12 pontos térközt!

6. Az első alcímet követő képeket egy kétsoros, négyoszlopos, szegély nélküli táblázat kialakításával rendezze el! A táblázat sorait állítsa 3 cm magasra! A cellákba a mintának megfelelő sorrendben, vízszintesen középre igazítva, az oldalarányok megtartásával 2,5 cm magasra átméretezve szúrja be a **11.jpg**, **12.jpg**, **13.jpg**, **14.jpg**, **21.jpg**, **22.jpg**, **23.jpg** és **24.jpg** képet! A táblázatot megelőző bekezdés után, valamint a táblázatot követő bekezdés előtt 12 pontos térközt alkalmazzon!
7. A táblázatot követő felsorolásban felsorolásjelként – a mintának megfelelően – a „👁” szimbólum vagy a **jel.png** kép jelenjen meg!
8. A második alcím alatt – a mintának megfelelően – alkalmazzon számozott listát!
9. Gondoskodjon arról, hogy a harmadik alcím új oldalra kerüljön!
10. A harmadik alcím alatti részt tabulátorokkal alakítsa ki! A tabulátorpozíciók helyei rendre 1 cm, 3,5 cm, 6 cm, 8 cm, 11 cm, valamint 13,5 cm legyenek! Valamennyi tabulátorpozíció legyen balra zárt, azokat pontozott vonal kösse össze! Az első sorban alkalmazzon félkövér betűstílust!
11. A tabulátoros elrendezésben a „FAR” kulcsszó után „*” szimbólum hivatkozással szúrjon be egy lábjegyzetet „A FAR (False Accept Rate) mutató azt mondja meg, hány helyes azonosításra jut egy téves.” szöveggel! Ügyeljen arra, hogy a lábjegyzet betűformátuma egyezzen meg a főszövegével!
12. A két utolsó alcím közötti részbe – a mintának megfelelően – szúrja be a **magyar.jpg** képet a méretarányok megtartásával 6 cm szélesre átméretezve, a jobb margóhoz igazítva! Képaláírásként írja be a „Magyar biometrikus útlevél” szöveget dőlt betűstílussal, egyébként a főszöveg betűformátumával azonos formai jellemzőkkel! A képet szegélyezze 1 pont vastagságú vékony fekete színű vonallal!
13. A dokumentumban a mintának megfelelő szövegrészeknél állítson be félkövér betűstílust!
14. A dokumentumban alkalmazzon automatikus elválasztást!

Minta:

Biometrikus azonosítás

> *A biometrikus azonosítás különböző fajtáinak működése egyaránt azon alapul, hogy a rendszer az emberi szervezet vagy viselkedés valamely egyedi sajátosságáról mintát vesz, azt digitális adattá konvertálja és adatbázisban tárolja, majd az aktuálisan levett mintát összeveti az ebben az adatbázisban tárolt mintákkal.*

A hivatalos definíció szerint **a biometria az alapján azonosít, ami az ember maga, nem pedig az alapján, amit tud** (kód, jelszó), **vagy amije van** (kártya, távirányító). Ez utóbbiak a megfejtésük vagy eltulajdonításuk esetén azok már valójában nem azt a személyt fogják azonosítani, akihez eredetileg hozzárendelték.

A BIOMETRIKUS AZONOSÍTÁS VÁLTOZATAI

A biometriai azonosítás során használnak **fizikai jellemzőket:** ujjlenyomat-, kéz- írisz-, arcazonosítást és DNS-elemzést, valamint azonosíthatnak **viselkedésbeli jellemzők** pl. gépelési stílus, aláírás vagy hang.










Mi szükséges ahhoz, hogy az emberi szervezet vagy viselkedés bizonyos tulajdonsága alkalmas legyen a biometrikus azonosításra?

- egyediség (mindenkinek van, de különbözik másokétól)
- permanencia (a korral, betegséggel járó változások során nem változik)
- mérhetőség (adattá konvertálható)
- gyors azonosíthatóság (elvárt teljesítmény)
- elfogadhatóság (a mintavételt ne utasítsák el pl. higiéniai okból)
- megbizhatóság (hamisítás, kikerülés elkerülésére)

A BIOMETRIKUS AZONOSÍTÁSI METÓDUS 4 LÉPÉSE

1. Mintavétel az adatbázishoz: ujjlenyomat, kéz, tenyér, hang stb. beolvasása mindenkiről, aki az azonosítási rendszerben érintett lesz.
2. Adatbázis létrehozása: a fiziológiás jellemzőkről beolvasott mintákat, illetve az azokból készült bináris kódot nevesítve, személyhez rögzítve eltárolja a rendszer.
3. Felhasználói mintavétel: a rendszer beolvassa az aktuális mintát az azonosítandó személyről, és ezt kódolja, ha szükséges.
4. Ellenőrzés vagy azonosítás: a beolvasott aktuális mintát a szoftver összeveti az adatbázisban rögzített adatokkal.

A BIOMETRIKUS BELÉPTETŐ RENDSZEREK BIZTONSÁGI MUTATÓI

Az alábbiakban összehasonlítjuk néhány biometrikus beléptető rendszer jellemzőit:

Azonosítás	FAR*	Idő (s)	Megbízhatóság	Állandóság	Higiénia
Arc	2000:1	1	alacsony	nem	megfelelő
DNS	n.a.	órák	magas	igen	mintától függ
Érminta	n.a.	0,4	közepes	igen	megfelelő
Hang	500:1	5	alacsony	igen/nem	kitűnő
Írisz	12 000 000:1	n.a.	nagyon magas	igen	megfelelő
Kéz	700:1	<5	alacsony	nem	alacsony
Retina	10 000 000:1	10-15	nagyon magas	igen	megfelelő
Ujjlenyomat	1 000 000:1	0,2-0,4	közepes	igen	alacsony

ADATVÉDELEM ÉS AGGÁLYOK

Az Európai Unió már 2004-ben úgy döntött, hogy az útleveleknek tartalmazniuk kell az ujjlenyomatot. (Magyarországon 2006-ban kezdték kibocsátani a biometrikus útleveleket.) Ezzel akkora nemzetközi adatbázis jött létre, amelynek a kezelése rendkívül komoly biztonsági követelményeket támaszt.

Szeptember 11. után a biztonságra való törekvés még jobban megerősödött, olyan méreteket öltve, amelyet előtte el sem tudtak képzelni. Például a rabosítás során levett ujjlenyomatok (vagy egyes országokban az írisz) adatai eredetileg csupán a büntetőeljárásban, illetve a bűnügyi nyilvántartóban voltak megtalálhatóak, de ma már a terrorizmus elleni harc intézkedéseinek következtében a mindennapok részévé váltak.

A modern kor azonosítási procedúrája automatizálódik, berendezések és szoftverek végzik a beérkezett és a tárolt információk összevetését, nem pedig a határőr vagy rendőr ellenőrzi a fotót és a személyt. Ezzel együtt 2012-re már több százezer hamis biometrikus útlevél került forgalomba az EU-ban, és több százezer olyan, amelynek az ujjlenyomat mintája értékelhetetlen. Főleg gyermekek és idősek ujjlenyomatai bizonyultak megbízhatatlannak, de az EP már végzi a biometrikus útlevelek felülvizsgálatát.



Magyar biometrikus útlevél

VIGYÁZAT, CSALNAK!

A biometrikus beléptető rendszer biztonságosságát is a legsebezhetőbb pontja határozza meg. Ezért a műszaki fejlesztők és a csalók egyaránt a gyenge pontot keresik, nyilvánvalóan különböző okokból, de minden bizonnyal egymással versenyezve.

Már jó ideje nem számít komoly ujjlenyomat olvasó rendszernek a nemzetbiztonságban az, amelyet át lehet vágni egy levágott ujjal, de még a fejlettebbeket is becsaphatja ma még egy jól elkészített szilikon ujjlenyomat.

Kezdetben még egy nyomtatott fotó az íriszről vagy egy mesterséges szem elegendő volt a rendszerbe való illetéktelen bejutáshoz, majd javultak a leolvasók és jöttek a speciális kontaktlencsékkel való sikeres támadások. Ezek használata viszont ma már egyértelműen lebukáshoz vezet. A szemgolyó sejtjei olyan gyorsan halnak el, hogy értelmetlen próbálkozás lenne egy biometrikus azonosítás miatt eltávolítani azt a természetes helyéről.

Az arcfelismerő rendszereket ideiglenes álcákkal, sminkkel nem lehet befolyásolni, de maszkokkal (itt is a szilikon a nyerő) sikerülhet a csalás egyes esetekben. A legbiztosabb átvágás persze a plasztikai sebészet alkotta új arc, de orvosi okokból ez is korlátozott mértékben lehet hatásos. Esetleg meg kell kérni az egypetéjű ikertestvért, mert a tökéletesen egyforma ikerpárokat egyelőre még nem sikerült megkülönböztetni.

---

* A FAR (False Accept Rate) mutató azt mondja meg, hány helyes azonosításra jut egy téves.